Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity

Platform **Talent** voor **Technologie**

dialogic
innovatie • interactie

In opdracht van Ministerie van Economische Zaken en Klimaat

Managementsamenvatting

Nederland en de EU werken hard aan een digitaal veilige samenleving. De aanwezigheid van voldoende goed geschoolde cybersecurity professionals is hiervoor een essentiële voorwaarde. De huidige krapte op de totale arbeidsmarkt, nieuwe technologische ontwikkelingen en de intensivering van cybercriminaliteit zijn bepalend voor de steeds groter wordende behoefte aan diverse typen cybersecurityspecialisten[1].
Het Ministerie van Economische Zaken en Klimaat krijgt graag een goed beeld van de **huidige kwantitatieve en kwalitatieve tekorten op de Nederlandse cybersecurity arbeidsmarkt, de verwachte groei en de mogelijkheden om onderwijs en arbeidsmarkt beter op elkaar aan te sluiten** (ook beschreven als actie in het Actieplan Nederlandse Cybersecuritystrategie 2022 -2028[2]).

Platform Talent voor Technologie (PTvT) en Dialogic hebben van september 2023 tot februari 2024 antwoord gegeven op een negen- tal onderzoeksvragen die zich richten op het in kaart brengen van vraag en aanbod (arbeidsmarkt en opleidingsmogelijkheden). Dit moet leiden tot een **onderbouwd advies, inclusief implementatieplan, over welke (beleids-)instrumenten op de korte en op de lange termijn** ingezet kunnen worden om de cybersecurity arbeidsmarkt te versterken.

In dit onderzoek zijn middels verschillende dataverzamelingswijzen de arbeidsmarkt en opleidingsmogelijkheden in kaart gebracht. Middels de analyse van de data uit verschillende landelijke bronnen zijn vraag en aanbod kwantitatief weergegeven. Deze data zijn geverifieerd en kwalitatief aangevuld middels vragenlijsten, interviews en workshops, uitgevoerd met leden uit het onderwijsveld en van de arbeidsmarkt. Ook hebben partijen betrokken bij de huidige Human Capital-activiteiten meegewerkt aan de kwalitatieve dataverzameling en duiding van de resultaten.

Onderwijs

Binnen het mbo worden de eisen waaraan een student moet voldoen om een mbo- diploma te halen landelijk vastgelegd in het betreffende kwalificatiedossier. De minister van Onderwijs, Cultuur en Wetenschap (OCW) stelt de kwalificatiedossiers vast. In het opleidingsaanbod zien we dat er op **mbo-niveau in de drie huidige kwalificatiedossiers** voor het ICT-domein de afgelopen jaren aandacht voor cybersecurity is: ICT support (niveau 2), Software Development (niveau 4) en ICT Systems & Devices (allroud medewerker niveau 3 en expert IT Systems & Devices niveau 4). In de **vernieuwing van deze kwalificatiedossiers**, die ingaan per 1 augustus 2024, is **nog explicieter uitgewerkt** wat studenten moeten kennen en kunnen op het gebied van cybersecurity. Daarnaast zijn er **drie mbo-initiatieven** gevonden waarvan de opleiding **in ontwikkelingsfase, accreditatiefase, of opstartfase is**.
Inhoudelijke focus van de mbo-opleidingen ligt vooral op de **technische aspecten en in enige mate op management en organisatie aspecten**. Door de variatie in hoe de ICT-opleidingen invulling geven aan het onderwijs, is niet mogelijk gebleken precies te achterhalen hoe groot het aandeel cybersecurity in de opleiding is. Navraag bij de opleidingsmanagers leert in ieder geval dat bij een aantal mbo-instellingen **cybersecurity een standaard onderdeel van de ICT-opleiding** is, terwijl anderen meer gebruik maken van de mogelijkheden die de **keuzedelen** bieden. Het totaal aantal studenten van deze betreffende opleidingen blijft ongeveer gelijk aan rond 23.000 studenten per jaar. Over de afgelopen jaren stromen er jaarlijks gemiddeld 6.000 gediplomeerde ICT-studenten uit.
Als knelpunten en/of uitdagingen geven de opleidingsdirecteuren aan [1] het up to date brengen van de docenten, [2] het tekort aan studenten, [3] ontoereikende faciliteiten en [4] de snelle opkomst van nieuwe thema's op het gebied van AI bijvoorbeeld.
Behalve bij de ICT-opleidingen is er bij de rest van de mbo-opleidingen nauwelijks of nog geen aandacht voor cybersecurity. De eerste aanzetten in vorm van **pilots** worden gedaan, zoals bijvoorbeeld binnen de opleiding beveiliger.
Op **hoger onderwijs niveau (hbo en wo) zijn** er, binnen de NVAO-geaccrediteerde opleidingen, **10 studies geïdentificeerd die volledig in het teken staan van cybersecurity (5 hbo, 5 wo), 29 studies die een specialisatie-/ keuzerichting cybersecurity aanbieden (18 hbo, 11 wo) en 13 studies (6 hbo, 7 wo) die een verplicht onderdeel cybersecurity in hun programma** hebben geïntegreerd, (groter dan 6 ECTS). Tevens zijn er **9 hoger onderwijs- studies** (8 hbo, 1 wo) aan het licht gekomen die nog **in ontwikkelingsfase, accreditatiefase, of opstartfase zijn**.
De instroom van studenten met een relevant onderdeel cybersecurity in hun studie blijft de laatste **drie jaren redelijk gelijk**; rond de 3000 studenten jaarlijks. **Het aantal afgestudeerde studenten neemt jaarlijks toe** bij met name studies die volledig in het teken staan van cybersecurity, danwel bij studenten die binnen hun studie een specialisatie-/ keuzerichting cybersecurity gekozen hebben. Over de opleidingen heen lijken de **hbo- en wo-opleidingen meer multidisciplinair ingestoken**. In alle studies (mbo en ho) is er geen- weinig aandacht aan competentieontwikkeling op het gebied van onderwijs, waarmee studenten didactische kennis en vaardigheden kunnen ontwikkelen.

1. https://www.cybersecurityraad.nl/documenten/brieven/2023/12/22/informerende-brief-van-de-cyber-security-raad-over-onderwijsversterking-en-kennisontwikkeling
2. https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

In de interviews en vragenlijsten met docenten, hoogleraren en management komen verschillende **knelpunten** naar voren zoals: [1] tekort aan docenten met voldoende kennis, [2] de inhoud van het curriculum waarin zowel een breed profiel en specialistische profilering binnen het cyberdomein dient te worden aangeboden, [3] de snelheid waarin de security wereld zich ontwikkelt in combinatie met het gebrek aan vermogen om hier flexibel op te reageren, [4] de beeldvorming rondom cybersecurity onderwijs als technische studie dat invloed heeft op de werving en het verwachtingsmanagement van (potentiële) studenten en [5] het gebrek aan middelen voor bijv. onderwijsmateriaal, hybride leerwerkplekken etc.)

Binnen het **Leven Lang Ontwikkelen-aanbod** (LLO-aanbod) zien we een zo op het oog uitgebreid niet-bekostigd onderwijsaanbod[3] (aanbod niet gesubsidieerd door de ministeries van OCW en EZK. De kosten van de opleiding komen voor rekening van degene die de opleiding volgt, van de werkgever of van de uitkeringsinstantie opleidingen aan een particulier instituut, schriftelijke cursussen of bedrijfsopleidingen), waarvan **ongeveer 20% gericht is op de meest gevraagde cybersecurity certificaten** op de arbeidsmarkt. Naast veel aanbieders, zien we één aanbieder met een groot portfolio aan aanbod.
Op meerdere manieren is het onderwijs beschikbaar, waarbij hybride vormen steeds meer voorkomen. Ook voor mkb-ondernemers en burgers zijn er veel – vaak regionale – activiteiten en aanbod. Bereik en impact zijn nog moeilijk in te schatten.
Particuliere opleiders geven aan dat mensen in de **om-, bij- en nascholing in cybersecurity de nodige belemmeringen ervaren (onvoldoende tijd krijgen van werkgever, geen toegang tot opleidingssubsidies)**.

Arbeidsmarkt

De vraag op de arbeidsmarkt is in kaart gebracht door de huidige vacatures te analyseren. Niet de gehele vraag zal hiermee in kaart zijn gebracht; de verwachting is dat posities ook zonder vacaturestelling vervuld worden.
In de vacatureanalyse is een **groeiende vraag** naar cybersecurity expertise te zien op de arbeidsmarkt: van circa 8.000 in 2018 tot circa 19.000 in 2022, voor zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt. Deze vraag is **verschillend per provincie** en kent een zwaartepunt op de **vraag naar medior en senior functies waarvoor een hbo of wo-opleidingsniveau** gevraagd wordt. De meeste vraag naar cybersecurity expertise komt van de **overheid en de IT-sector**, met de meeste cybervacatures bij organisaties zoals de Politie, PWC, CGI, EY, Belastingdienst, ING, ABN AMRO, Capgemini, KPMG en het Ministerie van Defensie. Organisaties die relatief meer doen met cybersecurity hebben ook meer vraag naar specialistische profielen.

De populatie cybersecurity professionals kenmerkt zich als een relatief jonge populatie, waarvan tweederde man is en eenderde vrouw. **Immigratie en arbeidsmigranten** lijken belangrijk te zijn voor de sector: circa 5-10% van de instroom is toe te schrijven aan werknemers uit het buitenland die in Nederland komen werken. In 2021 was er een **uitstroom** van bijna 25% van de populatie, waarvan ~2% van de uitstromers met pensioen ging en nog eens ~2% emigreerde. Ongeveer driekwart van de uitstromers gaat werken bij een organisatie die buiten de scope van dit onderzoek valt. Dat wil niet zeggen dat ze een ander beroep gaan uitoefenen; ze kunnen ook hetzelfde beroep of een vergelijkbaar beroep uitoefenen bij een andere werkgever. Ongeveer 2,5% van de populatie maakte een switch naar een ander bedrijf binnen de onderzoekspopulatie.

Over de hele linie is er relatief **veel technische kennis** vereist om actief te zijn binnen de cybersecurity, maar de benodigde **vaardigheden en uit te voeren taken** zijn daarentegen voor een groot deel **niet-technisch** van aard. Bij vacatures die in hun teksten refereren aan de European Cybersecurity Skills Framework (ECSF) profielen weegt de technische component zwaarder dan bij de andere typen cybersecurity profielen. De vraag naar cybersecurity expertise en onderliggende bouwstenen kent een **sterke groei in absolute zin**, maar in relatieve zin is de **verhouding tussen verschillende typen kennis en vaardigheden stabiel**.
In **15% van de vacatures wordt expliciet gevraagd naar een cybersecurity certificaat**. De meest gevraagde certificaten zijn de CISSP, CISM, en CISA[4]. **Binnen de specialistische cybersecurity profielen wordt vaak een certificaat gevraagd**; zo treffen we voor het profiel behorende bij de Chief Information Security Officers (CISO) in 77% van de vacatures de vraag naar een certificaat aan en voor de Penetratietester, die computersystemen en apps test op kwetsbaarheden in de beveiliging, is dat in 58% het geval.

3. https://www.ocwincijfers.nl/sectoren/onderwijs-algemeen/niet-bekostigd-onderwijs/deelnemers-niet-bekostigd-onderwijs
4. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA)

Toekomstige ontwikkelingen

De komst van de NIS2 richtlijn (Network and Information Security), de Cyber Resilience Act (CRA) en de verdere ontwikkeling van AI zal een grote rol gaan spelen op de cybersecurity arbeidsmarkt. De verwachting is dat de **NIS2 de vraag naar cybersecurity professionals in de breedte zal doen toenemen**, van de ECSF profielen Chief Information Security Officers (CISO) tot aan Implementers, Analisten, Auditors en Pentesters. Door de **CRA zal de vraag naar cybersecurity professionals naar verwachting in de breedte toenemen**, met vermoedelijk de grootste impact voor de cyberintegrators. Door de verdere ontwikkeling en inzet van AI zal de vraag naar de uitvoering van bepaalde taken door mensen afnemen, maar tegelijkertijd zullen er ook nieuwe taken ontstaan en zullen nieuwe competenties benodigd zijn. Bij de ECSF-profielen **Penetration Tester, Cyber Threat Intelligence Specialist en de Digital Forensics Investigator** bestaat de **grootste kans dat AI een significante rol gaat spelen**. Organisaties die marginaal met cybersecurity bezig zijn, waar cybersecurity een relatief kleine rol speelt, en die niet onder de NIS2 en/of CRA vallen zullen vermoedelijk blijven kiezen voor **de 'hybride' functies in combinatie met externe inhuur/inkoop/organisatie van cybersecurity expertise**.

Aansluiting onderwijs- arbeidsmarkt

Het idee dat onderwijs en (alle) concrete vacatures op de arbeidsmarkt perfect zouden kunnen matchen is een misconceptie, omdat er meerdere jaren en in verschillende contexten (werkomgeving, trainingen e.d.) bijgeleerd moet worden. In dit onderzoek is derhalve gekeken naar de vraag op de arbeidsmarkt naar junior functies en de aansluiting met de opleidingen. Bij het hoger onderwijs zien we **relatief te weinig hbo en wo-gediplomeerden met een specialistisch cybersecurity profiel** afstuderen ten opzichte van de vraag op de arbeidsmarkt. Het aantal ho-gediplomeerden dat een **'substantiële' component cybersecurity in de opleiding heeft gehad is echter op peil** met de vraag. Net als de kwantitatieve vraag naar **mbo cybersecurity junior personeel: deze is op peil met de uitstroom** in de twee betreffende mbo-4-opleidingen.
Inhoudelijk gezien wordt er op de arbeidsmarkt veel gevraagd naar de **competenties van het type 'Technisch' en 'Management & Organisatie'**. Deze bouwstenen zien we ook terug bij de opleidingen met een specialisatierichting cybersecurity. De **focus op 'legal'** competenties vinden we met name terug bij de opleidingen waar cybersecurity **geen specialisatierichting** is. De **competenties op het gebied van 'onderwijs' (bijv. lesgeven) zien we echter nergens terugkomen** - niet bij de opleidingen en niet in de vacatures op juniorniveau.

Een grote opgave voor de cybersecurity arbeidsmarkt lijkt dus met name te liggen in het Leven Lang Ontwikkelen, bij zowel het **aantrekken als het behouden** van de (huidige) cybersecurity professionals. Hierbij dient rekening gehouden te worden met het verschil tussen de functie waar iemand vandaan komt en de functie waar iemand bij in moet stromen. Dit verschil kan niet te groot zijn; er moet een 'overbrugbare stap' zijn. Het is zaak om secuur te kijken naar **welke achtergronden voldoende basis hebben om de stap te overbruggen**. Het belang van certificaten op de cybersecurity arbeidsmarkt is groot, met name bij de meer specialistische cybersecurity profielen. Deze **certificaten en bijbehorende trainingen zijn een manier om de stap te overbruggen**.
Daarnaast is het van belang de **genoemde knelpunten in het onderwijs** aan te pakken; de instroom van de reguliere opleidingen wordt hiermee kwantitatief en kwalitatief verbeterd om zo beter aan te sluiten op de vraag van de arbeidsmarkt.

Advies

De uitkomsten van dit onderzoeksrapport vormen de basis van waaruit een advies inclusief een implementatievoorstel opgesteld zullen worden. Via meerdere bijeenkomsten in begin 2024 wordt samen met het onderwijs, bedrijfsleven en samenwerkende partners bepaald welke (beleids-) instrumenten op de korte en op de lange termijn ingezet kunnen worden om de cybersecurity arbeidsmarkt te versterken. Deze adviezen worden gebundeld in een rapport dat eind februari/begin maart 2024 opgeleverd zal worden.

Inhoudsopgave

Leeswijzer

In dit rapport zal een overzicht geboden worden van de aanpak en de resultaten van het onderwijs- en arbeidsmarkt onderzoek op het gebied van cybersecurity.
Hoofdstuk 1 beschrijft de *aanleiding en aanpak van het onderzoek*, waarin ook de onderzoeksvragen gesteld door het ministerie van Economische Zaken en Klimaat aan bod komen. In **Hoofdstuk 2** wordt de *methodologie van het onderzoek* toegelicht, zowel wat betreft het onderwijsdeel als het arbeidsmarktdeel. Vervolgens worden in **Hoofdstuk 3** *de resultaten* toegelicht van de onderzoeksvragen die betrekking hebben op het *onderwijs* en geeft **Hoofdstuk 4** de *resultaten* weer van de *arbeidsmarktanalyse*. De *getrokken conclusies* zijn terug te lezen in **Hoofdstuk 5**. Tot slot kijken we vooruit naar het advies in **Hoofdstuk 6**: welk denkkader en welke aanpak nemen we vanuit deze resultaten mee richting het advies?

1. Aanleiding en aanpak van het onderzoek

1.1 Aanleiding

In Nederland en de EU wordt hard gewerkt aan een digitaal veilige samenleving. De aanwezigheid van voldoende goed geschoolde cybersecurity professionals met expertise is hiervoor een essentiële voorwaarde. Het Ministerie van Economische Zaken en Klimaat krijgt graag een goed beeld van de huidige kwantitatieve en kwalitatieve tekorten op de Nederlandse cybersecurity arbeidsmarkt en de verwachte groei. In het Actieplan Nederlandse Cybersecuritystrategie 2022 -2028[5] zijn de volgende acties op het gebied van Human Capital opgenomen:

- De kwalitatieve en kwantitatieve tekorten op de cybersecurity arbeidsmarkt worden onderzocht, met aanbevelingen over hoe deze tekorten aan te pakken;
- Verkend wordt of de initiatieven voor inzicht in ICT- brede tekorten en de ontwikkeling van een onderwijs en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity specialisten.

Om uitvoering te geven aan bovengenoemde acties heeft het Ministerie van Economische Zaken en Klimaat een uitgebreid onderzoeksvoorstel geschreven. De onderzoeksvragen richten zich op vraag en aanbod (arbeidsmarkt en opleidingsmogelijkheden) en moeten leiden tot een onderbouwd advies, inclusief implementatieplan, over welke (beleids-)instrumenten op de korte en op de lange termijn ingezet kunnen worden om het geconstateerde tekort op de cybersecurity arbeidsmarkt te verkleinen. De voorgaande jaren is op meerdere manieren het onderwijs en de arbeidsmarkt rondom cybersecurity in kaart gebracht. Middels dit multidisciplinair onderzoek zijn we aanvullend en verdiepend op de bestaande inzichten door:

- het onderzoek specifiek te richten op cybersecurity
- de probleemstelling te verdiepen: over welke tekorten hebben we het precies?
- aandacht te hebben voor specifieke kennis, vaardigheden en taken binnen cybersecurity
- aandacht te hebben voor verschillende doelgroepen/typen organisaties
- te werken aan een methodiek-ontwikkeling, die ook in de toekomst gebruikt kan worden.

In dit hoofdstuk wordt stil gestaan bij de volgende onderwerpen:

- De onderzoeksvragen gesteld door het Ministerie van Economische Zaken en Klimaat;
- De aanpak zoals deze opgesplitst is in een onderzoeksrapport en adviesrapport;
- De aanpak om te komen tot een onderbouwd advies.

1.2 Onderzoeksvragen

De onderzoeksaanvraag van het Ministerie van Economische Zaken en Klimaat bevat een negental onderzoeksvragen:

Aanbod

1. Breng de relevante Nederlandse opleidingen (mbo-4- t/m wo-niveau) en omscholingsinitiatieven in kaart (o.a. wiskunde, AI, data science, ICT). Bouw hierbij verder op bestaande initiatieven zoals de Nationale Cybersecurity Research Agenda (NCSRA) en het Platform Talent voor Technologie (PTvT);
2. Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) wat de huidige in- en uitstroom is van het opleidings- en omscholingsaanbod;
3. Op basis van (1) en (2), maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) welk soort cybersecurity expertise, in welke hoeveelheid, wordt aangeboden;
4. Geef inzicht in de knelpunten inzake cybersecurityopleiding-en omscholing. Denk hierbij aan factoren die de instroom en doorstroom beïnvloeden.

Vraag

5. Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) hoe groot de vraag naar cybersecurity experts is, en welke expertise gevraagd wordt. Doe dit op basis van:
    - Een overzicht van de openstaande vacatures bij Nederlandse organisaties waar cybersecurity professionals in dienst (gaan) zijn;
    - Een overzicht van het soort cybersecurity expertise dat gevraagd wordt;
    - Inzicht in de sectorale en regionale verdeling van de vraag naar cybersecurity expertise binnen Nederland: waar komt de vraag vandaan?

5. https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

6. Maak een beargumenteerde schatting van de te verwachten groei (heden – 2028) in de vraag naar cybersecurity expertise (in termen van aantal en soort expertise). Doe dit op basis van toekomstige ontwikkelingen en historische groei.

Tekort

7. Maak inzichtelijk (kwantitatief en kwalitatief) welke discrepantie er zit tussen de vraag naar en het aanbod van cybersecurity expertise. Analyseer welke factoren deze discrepantie veroorzaken. Sta onder andere stil bij (ervaren) kwaliteitsverschillen tussen verschillende opleidingen en certificering.
8. Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) wat de uitstroom is van cybersecurity expertise op de Nederlandse arbeidsmarkt en waar dit door komt.

Advies

9. Geef een onderbouwd advies, inclusief implementatieplan, over welke (beleids-)instrumenten op de korte en op de lange termijn ingezet kunnen worden om het geconstateerde tekort op de cybersecurity arbeidsmarkt te verkleinen. Maak hierbij ook inzichtelijk welke partijen hierbij een rol kunnen/moeten spelen. Besteed specifiek, maar niet uitsluitend, aandacht aan:
    - Het instrumentarium van de Human Capital Agenda-ICT;
    - Het publiek-private samenwerkingsplatform dcypher;
    - Beschikbare beleidsinstrumenten van EZK, OCW en SZW (incl. NGF, Actieplan groene en Digitale banen, UWV).

1.3 Aanpak

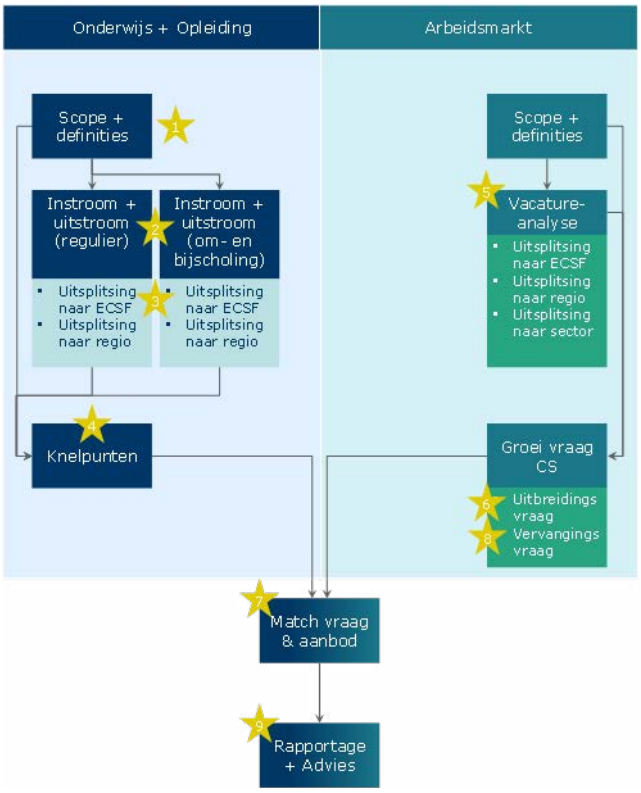
1.3.1 Onderzoeks- en adviesrapport

Om uiteindelijk te komen tot een gedragen advies, inclusief implementatievoorstel is het onderzoek op onderstaande wijze aangepakt. In figuur 1 is de flowchart van het onderzoek terug te vinden. De sterren wijzen op de onderzoekvragen die in die blokken beantwoord worden. Vanuit onderzoek en opleiding zijn de instroom en uitstroom in kaart gebracht, om vervolgens uit te komen op knelpunten.

In het arbeidsmarktdeel is een vacature- analyse uitgevoerd en antwoord gegeven op de groeivraag van de cybersecurity arbeidsmarkt.

Beide stromen leveren data en input op waarmee de match tussen onderwijs en arbeidsmarkt bepaald kan worden. Dit geheel heeft als output het onderzoeksrapport.

Naast het onderzoeksrapport wordt er nog een apart adviesrapport opgesteld, inclusief een implementatievoorstel waarin aangegeven wordt welke adviezen op welk niveau opgepakt kunnen worden.



Figuur 1: flowchart onderzoek

1.3.2 Aanpak: op hoofdlijnen

Zoals hierboven beschreven zijn er twee delen in dit onderzoek: het onderzoeksdeel dat antwoord geeft op onderzoeksvragen 1 tot en met 8 (waarvan in deze rapportage verslag wordt gedaan) en het adviesdeel dat antwoord heeft op onderzoeksvraag 9, dat op basis van de uitkomsten van het onderzoeksdeel begin 2024 wordt opgesteld.

Om te komen tot een gedragen advies, dat gebaseerd is op empirisch onderzoek en goed aansluit op alle huidige initiatieven is tijdens het onderzoek zoveel mogelijk het betrokken werkveld geraadpleegd:

- Middels interviews met vertegenwoordigers van onderwijs, bedrijfsleven, branches en betrokken instellingen hebben we input opgehaald en de onderzoeksresultaten geverifieerd.
- Door verschillende vragenlijsten uit te zetten hebben we zowel bij het onderwijs als bij het bedrijfsleven kwalitatieve input opgehaald over de huidige opleidingen en vacatures, en ook over de toekomstige ontwikkelingen en verwachtingen.
- Middels een posterpresentatie en een pitch op de ONE conference hebben we gecommuniceerd over het onderzoek en input opgehaald.
- Door aan te sluiten bij de Cyber Security Raad hebben we het onderzoek en de aanpak kunnen toelichten en veel input op kunnen halen over de aanpak, uitkomsten, positionering en vervolg van het onderzoek.
- Via (online) workshops hebben we aanpak en tussentijdse resultaten gedeeld en veel input opgehaald waarmee de aanpak van het onderzoek en duiding van de resultaten aangescherpt is.

In hoofdstuk 2 is terug te lezen op welke manier de onderzoeksdata voor onderwijs en arbeidsmarkt verzameld zijn, welke afbakening er plaats heeft gevonden en op welke manier de data zijn geanalyseerd.

Middels een workshop en verschillende bijeenkomsten met onderwijs en bedrijfsleven halen we de input op voor het advies en implementatiedeel. Dit zal beschreven worden in het adviesrapport.

2. Methodologie onderzoek

In dit hoofdstuk beschrijven we hoe we de inventarisatie van het opleidingsaanbod en wat er speelt in het onderwijs hebben aangepakt. Hetzelfde doen we voor de analyse van de vraag vanuit de arbeidsmarkt.
De focus van het onderzoek ligt op dat deel van de opleidingen dat opleidt voor functies die in de HSD Human Capital Agenda in het kwadrant "Occupations for Safety & Security of data and information systems" zijn geplot.[6]
Zowel de gegevens uit de onderwijs- als de arbeidsmarktanalyse zijn in de vorm van workshops bij een brede groep van stakeholders en experts gecheckt.

2.1 Methodologie onderwijs mbo

Voor het mbo-onderwijs worden op landelijk niveau de eindtermen (wat moeten de studenten aan het eind van de opleiding kennen en kunnen) voor de opleidingen met het afnemend werkveld afgestemd. Dit wordt vastgelegd in een kwalificatiedossier.
Als eerste hebben we de kwalificatiedossiers van de vier ICT-opleidingen (huidig en vanaf 2024) en de keuzedelen geanalyseerd op relevantie voor cybersecurity. Volledigheidshalve is ook nog gekeken naar opleidingen binnen Zakelijke Dienstverlening en Veiligheid.

De invulling van het onderwijs kan variëren. Daarom hebben de opleidingen de nodige ruimte in de keuze voor werkvormen en inhoud. Daartoe is een enquête onder de directeuren ICT-opleidingen uitgezet om zicht te krijgen op hoe cybersecurity in het onderwijs wordt opgepakt.

Deze acties zijn uitgezet in samenspraak en met hulp van onze contactpersonen bij de SBB Sectorkamer ICT en de MBO Raad bedrijfstakgroepen ICT & Creatieve Industrie en Zakelijke Dienstverlening en Veiligheid.

Tot slot hebben we via deskresearch en binnen het Katapultnetwerk gezocht naar mbo-instellingen met een duidelijke cybersecurity profilering op het gebied van initieel onderwijs.

2.2 Methodologie hoger onderwijs

Binnen het hoger onderwijs hebben hogescholen en universiteiten veel ruimte om te bepalen welke opleidingen ze aanbieden, met welke beoogde uitkomsten en met welke inhoud. De instelling schrijft een opleidingsplan, dat een beeld geeft van de beoogde leerresultaten van de gehele opleiding, de inrichting van het curriculum, de leeromgeving en de toetsing en het docententeam dat de opleiding zal gaan verzorgen. Dit leerplan wordt gekeurd door een panel van onafhankelijke deskundigen van de Nederlands-Vlaamse Accreditatieorganisatie (NVAO).

Voor wat betreft het hbo-onderwijs in het ICT–domein is nog relevant te vermelden dat er een landelijk kader is voor de eindkwalificaties op Associate degree, bachelor en professional master-niveau. Deze domeinbeschrijving wordt onderhouden door de HBO-i stichting en door de Vereniging Hogescholen vastgesteld. Opleidingen kunnen hun eigen opleidingsprofiel, leerdoelen en curricula afleiden uit de domeinbeschrijving. Expliciete koppeling van het eigen opleidingsprofiel aan de domeinbeschrijving borgt inhoud en eindniveau van de opleiding. Momenteel wordt gewerkt aan een IT security framework binnen de domeinbeschrijving om de link tussen opleiding en bedrijfsleven te versterken.

Voor het in kaart brengen van de relevante Nederlandse opleidingen op het gebied van cybersecurity op hbo- en wo-niveau is, met behulp van pr-eDICT, een selectie gemaakt van alle cybersecurity- en veiligheid-gerelateerde opleidingen en alle ICT-opleidingen die instroom hadden in de jaren 2020-2022. Door middel van desk research zijn al deze opleidingen geanalyseerd en ingedeeld in drie categorieën: [1] opleidingen zonder cybersecurity, [2] deels cybersecurity opleidingen en [3] opleidingen die volledig in het teken staan van cybersecurity (kijkwijzer: ECSF profielen). Opleidingen die als deels cybersecurity beoordeeld zijn, zijn vervolgens verder opgesplitst in de volgende categorieën: [1] opleidingen met een specialisatie-/keuzerichting cybersecurity, [2] opleidingen met een verplicht onderdeel cybersecurity (meer dan 6 ECTS) en [3] opleidingen met één (keuze)vak van 6 ECTS. Opleidingen uit de eerste twee categorieën zijn hierbij als relevant beschouwd binnen dit onderzoek.

Met behulp van de open DUO-data zijn de in- en uitstroom cijfers opgehaald van alle opleidingen die volledig in het teken staan van cybersecurity en van de categorie 2 deels cybersecurity opleidingen. Waar deze data niet beschikbaar waren (categorie 1 deels cybersecurity opleidingen, niet-bekostigd onderwijs, recent gestarte opleidingen), zijn de in- en uitstroom cijfers opgevraagd bij de program director of onderwijsmanager van de desbetreffende opleiding.

6. Figure 7: Safety and security occupations, HSD, 2018, blz 28, Human Capital Agenda Security 2023 – 2026

Bij deze program directors en onderwijsmanagers is tevens een enquête uitgezet om inzicht te krijgen in de huidige ontwikkelingen en trends van het onderwijs, de aansluiting en samenwerking met de arbeidsmarkt en de knelpunten binnen cybersecurity onderwijs.

Tot slot ziin gedurende het proces van in kaart brengen van de relevante Nederlandse cybersecurity opleidingen in het hoger onderwijs, de interviews met vertegenwoordigers van het onderwijs en de (online) workshops, de specifieke cybersecuritystudies geïnventariseerd die nog in de ontwikkelingsfase, accreditatiefase of opstartfase zijn.

2.3 Methodologie LLO-aanbod (onbekostigd onderwijs)

Gestart is met een scraping van data via www.leeroverzicht.nl met cybersecurity–gerelateerde zoektermen. Dit heeft 2.409 hits opgeleverd, die op basis van de beschrijvingen zijn ingedeeld in 1. volledig cybersecurity, 2. deels cybersecurity en 3. geen cybersecurity. Bij deze lijst is ook nagegaan hoeveel van de opleidingen gericht zijn op cybersecurity certificaten. Dit is met behulp van een automatische analyse van opleidingsbeschrijving en titel gedaan en vervolgens heeft nog een handmatige check op fout positieven plaatsgevonden. Tevens is bij de vacatureanalyse gekeken naar welke certificaten hoe vaak worden gevraagd in vacatures.

Voor de inventarisatie van regionale, sectorale en landelijke activiteiten en initiatieven voor ondernemers en burgers is de Regioscan digitalisering mkb gebruikt. Binnen dit overzicht is geselecteerd op cybersecurity (240 hits) en dit is nog aangevuld met activiteiten die zijn verkregen via een uitvraag onder de HCA-ICT regiocontactpersonen.

De Katapultnetwerkkaart met een overzicht van duurzame samenwerkingsverbanden ICT is nagelopen op voorbeelden op het gebied van (om)scholing ICT en specifiek richting cybersecurity.

2.4 Methodologie arbeidsmarkt

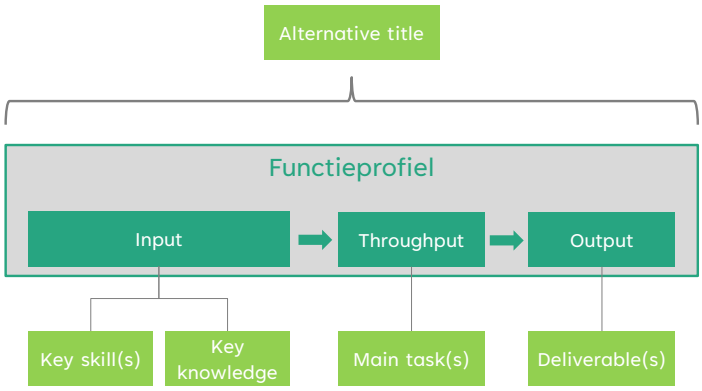
In onderstaande paragraaf beschrijven we de afbakening van het begrip cybersecurity, op welke wijze er gebruik is gemaakt van het European Cybersecurity Skills Framework (ECSF) en hoe de vacature-analyse uitgevoerd is. Een gedetailleerde beschrijving van de methodologie is opgenomen in Bijlage 1.
Cybersecurity is een breed concept. Het gaat om digitale veiligheid in de brede zin van het woord, waar onderwerpen als techniek, wet- en regelgeving, bestuur en organisatie allemaal een rol spelen. De breedte van het concept 'cybersecurity' wordt logischerwijs ook weerspiegeld in de expertise die professionals (moeten) hebben om werkzaam te zijn op dit gebied. Om op een zinvolle manier te spreken over 'cybersecurity expertise' (hierna: cybersecurity expertise) is het derhalve relevant om scherp te hebben wat we exact verstaan onder deze expertise.
Wanneer we naar cybersecurity expertise op de arbeidsmarkt kijken, kunnen we het op verschillende 'aggregatieniveaus' benaderen. Het meest directe en duidelijke aggregatieniveau is het niveau van **functietitels- en profielen**. Er wordt bijvoorbeeld gevraagd naar een Chief Information Security Officer (CISO), een Pentester of een Cyber Incident Responder. Binnen dit onderzoek is het European Cybersecurity Skills Framework (ECSF)[7] van ENISA als basis genomen voor twaalf relevante (doch illustratieve) cybersecurity profielen (figuur 2).

Figuur 2: De twaalf functieprofielen binnen het ECSF

7. Voor meer informatie kan worden gekeken op de website van ENISA. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Belangrijke voordelen van spreken over functieprofielen zijn dat [1] men zich er doorgaans wel iets bij voor kan stellen en [2] het direct een integraal beeld geeft van wat een persoon in die functie op hoofdlijnen doet. Belangrijke nadelen zijn echter dat [i] de invulling van hetzelfde functieprofiel of -titel kan verschillen tussen of zelfs binnen organisaties en [ii] dat cybersecurity expertise ook terug kan komen in (individuele) taken die gekoppeld zijn aan functieprofielen die men doorgaans niet als sec cybersecurityprofiel zou classificeren. **Cyberexpertise laat zich immers niet vangen in enkele functies, maar kan onderdeel zijn van een grote variëteit aan beroepen op de arbeidsmarkt**. Denk bijvoorbeeld aan een data engineer of projectleider ICT die wel degelijk verstand moet hebben van cybersecurity, zonder dat zij een 'puur' cybersecurity profiel vertegenwoordigen. Het is derhalve ook relevant om niet enkel naar functieprofielen te kijken, maar op een aggregatieniveau 'lager' ook te kijken naar individuele taken, kennis en vaardigheden. Het belang van dit 'inzoomen' op cybersecurity expertise wordt ook door anderen in het veld onderstreept, waaronder bijvoorbeeld de HSD in hun Human Capital Agenda[8].

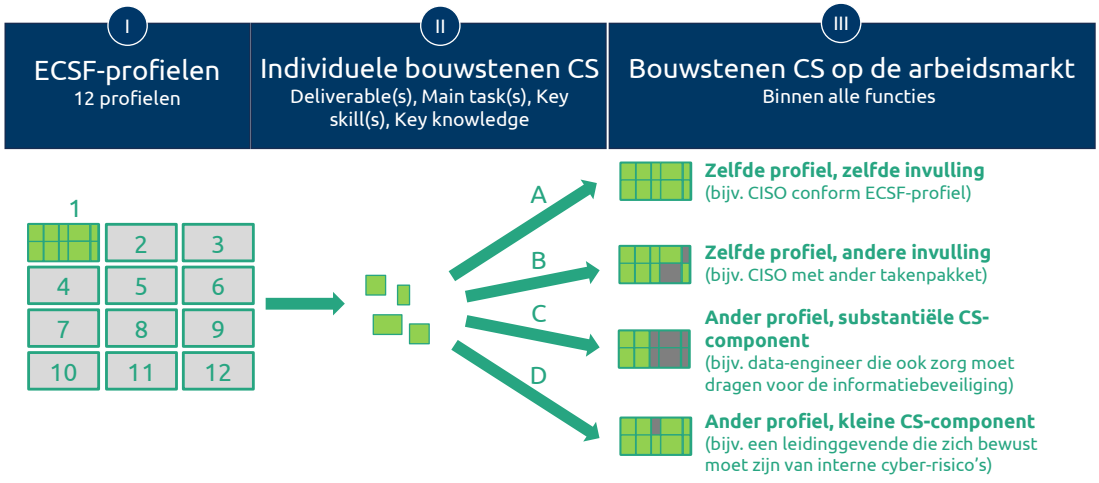
Relevante taken, kennis en vaardigheden op het gebied van cybersecurity zijn in dit onderzoek geïdentificeerd aan de hand van hetzelfde ECSF. De twaalf genoemde functies zijn gedetailleerd beschreven en opgebouwd aan de hand van 'Deliverables', 'Main task(s)', 'Key skills' en 'Key knowledge'. Deze **bouwstenen** kunnen als volgt gevisualiseerd worden (figuur 3):



Figuur 3: Bouwstenen ECSF-profielen

De twaalf profielen komen overeen met 385 onderliggende bouwstenen, wat overeenkomt met gemiddeld 30-35 bouwstenen per profiel. Hoewel de twaalf profielen op zichzelf geenszins dekkend zijn voor de cybersecurity arbeidsmarkt in brede zin, verwachten wij als onderzoekers wel dat de onderliggende 385 bouwstenen (deliverables, taken, kennis en vaardigheden) wel een vrij compleet beeld schetsen van wat er onder cybersecurity expertise verstaan kan worden.

In dit onderzoek kijken we dus naar cyberexpertise op het niveau van profielen, maar onderzoeken we ook de vraag naar individuele bouwstenen. Deze individuele bouwstenen kunnen we vervolgens aantreffen in de 12 (illustratieve) ECSF-profielen, maar we kunnen hen ook aantreffen in andere functieprofielen. Schematisch ziet dit er als volgt uit (figuur 4):



Figuur 4: cybersecurity bouwstenen op de arbeidsmarkt

8. HSD (2023), Human Capital Agenda Security 2023 – 2026

In dit onderzoek is er dus aandacht voor beroepen waarin cybersecurity expertise de hoofdmoot vertegenwoordigt (typen A en B in figuur 4), maar wordt er ook gekeken naar beroepen waarin cybersecurity expertise wel degelijk een rol speelt en tegelijkertijd niet per se de hoofdmoot vertegenwoordigt (typen C en D in figuur 4).

Voor het analyseren van de vraag naar cybersecurity expertise op de arbeidsmarkt is een vacature-analyse uitgevoerd op vacatures in de periode 2018-2022. De vacaturedata zijn afkomstig van het bedrijf Jobdigger. De vacature-analyse volgt een zekere gelaagdheid:

- Er is beoordeeld in welke vacatures überhaupt naar cybersecurity expertise gevraagd wordt. Dit is gedaan door te zoeken naar een lijst van 'generieke cybersecuritytermen'. Een overzicht van deze generieke termen is opgenomen in Bijlage 1.
- Vervolgens is bepaald of de relevante vacature behoort tot één van de twaalf ECSF-profielen.
- Indien de vacature niet behoort tot één van de 12 ECSF-profielen, is het 'gehalte cybersecurity' bepaald. Hiervoor zijn drie categorieën gebruikt, verwijzend naar een hoog cybersecurity gehalte, een middelhoog cybersecurity gehalte of een laag cybersecurity gehalte.
- Binnen de relevante vacatures is ook gezocht naar individuele taken, kennis en vaardigheden die relevant zijn voor cybersecurity. Deze individuele 'bouwstenen' zijn gebaseerd op alle bouwstenen die in het ECSF benoemd zijn. Het gaat om 385 bouwstenen, verdeeld over 12 ECSF-profielen.
- Voor iedere bouwsteen zijn twee operationaliseringsroutes gehanteerd: [1] het handmatig opstellen van een query die de desbetreffende bouwsteen moet kunnen vinden in een vacaturetekst en [2] het laten genereren van zoektermen door ChatGPT middels een separaat prompt per type bouwsteen. In de tweede route zijn circa 20.000 zoektermen handmatig bekeken en gescoord op precision ("als deze term gevonden wordt, hoe groot is de kans dat het dan ook gaat om bouwsteen X?") en recall ("hoeveel van de bouwstenen op de arbeidsmarkt worden gevonden met deze zoekterm"). Na controle van de twee methoden is gesteld dat een bouwsteen X in vacature Y is aangetroffen als minimaal één van de twee methoden een positief resultaat oplevert.

Naast het uitvoeren van een uitgebreide vacature-analyse is een analyse op CBS-microdata uitgevoerd. Het doel van deze analyse is om zicht te krijgen op de uitstroom van cybersecurity professionals. Voor deze analyse is vertrokken vanuit een lijst bedrijven die (deels) actief zijn in de cybersecurity sector c.q. betrokken zijn bij de 'productie' van cybersecurity goederen-en diensten. Deze lijst is eerder opgesteld in het kader van het onderzoek 'De economische kansen van de cybersecuritysector (Dialogic, 2023)'. De mensen die bij deze bedrijven werkzaam zijn en hoogopgeleid zijn, zijn de populatie van de analyse. Hoewel dit niet allemaal cybersecurity professionals zijn, is er geen registratie om cybersecurity professionals aan te duiden en is dit een second-best optie om op hoofdlijnen zicht te krijgen op de (relatieve) uitstroom.

3. Resultaten Onderwijs

Onderzoeksvraag 1:
Breng de relevante Nederlandse opleidingen (mbo- t/m wo-niveau) en omscholingsinitiatieven in kaart (o.a. wiskunde, AI, data science, ICT). Bouw hierbij verder op bestaande initiatieven zoals de Nationale Cybersecurity Research Agenda (NCSRA) en het Platform Talent voor Technologie (PTvT);

In het opleidingsaanbod zien we dat er op mbo-niveau in de drie huidige kwalificatiedossiers voor het ICT-domein de afgelopen jaren aandacht voor cybersecurity is: ICT support (niveau 2), Software Development (niveau 4) en ICT Systems & Devices (allroud medewerker niveau 3 en expert IT Systems & Devices niveau 4). In de vernieuwing van deze kwalificatiedossiers, die ingaan per 1 augustus 2024, is nog explicieter uitgewerkt wat studenten moeten kennen en kunnen op het gebied van cybersecurity. Daarnaast zijn er drie mbo-initiatieven gevonden waarvan de opleiding in ontwikkelingsfase, accreditatiefase, of opstartfase is.
Op hoger onderwijs niveau (hbo en wo) zijn er, binnen de NVAO-geaccrediteerde opleidingen, 10 studies geïdentificeerd die volledig in het teken staan van cybersecurity (5 hbo, 5 wo), 29 studies die een specialisatie-/keuzerichting cybersecurity aanbieden (18 hbo, 11 wo) en 13 studies (6 hbo, 7 wo) die een verplicht onderdeel cybersecurity in hun programma hebben geïntegreerd, (groter dan 6 ECTS). Tevens zijn er 9 hoger onderwijs-studies (8 hbo, 1 wo) aan het licht gekomen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn.
Binnen het Leven Lang Ontwikkelen-aanbod (LLO-aanbod) zien we een zo op het oog uitgebreid niet-bekostigd onderwijsaanbod, waarvan ongeveer 20% gericht is op de meest gevraagde cybersecurity certificaten op de arbeidsmarkt. Naast veel aanbieders, zien we één aanbieder met een groot portfolio aan aanbod.
Op meerdere manieren is het onderwijs beschikbaar, waarbij hybride vormen steeds meer voorkomen. Ook voor mkb-ondernemers en burgers zijn er veel – vaak regionale – activiteiten en aanbod.

Onderzoeksvraag 2:
Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) wat de huidige in- en uitstroom is van het opleidings- en omscholingsaanbod);

Het totaal aantal mbo ICT-studenten blijft ongeveer gelijk aan rond 23.000 studenten per jaar. Over de afgelopen jaren stromen er jaarlijks gemiddeld 6.000 gediplomeerde ICT-studenten uit.
De instroom van hbo – en wo studenten met een relevant onderdeel cybersecurity in hun studie blijft de laatste drie jaren redelijk gelijk; rond de 3000 studenten jaarlijks. De uitstroom aan studenten neemt jaarlijks echter duidelijk geleidelijk toe bij met name studies die volledig in het teken staan van cybersecurity, danwel bij studenten die binnen hun studie een specialisatie-/keuzerichting cybersecurity gekozen hebben.
In- en uitstroomcijfers van de particuliere scholingsmarkt zijn om voor de hand liggende redenen (concurrentiegevoelig, privacy van deelnemers) niet beschikbaar.
Bereik en impact van regionale initiatieven voor mkb-ers en burgers zijn vanwege het heterogene karakter zijn nog moeilijk in te schatten.

Onderzoeksvraag 3:
Op basis van (1) en (2), maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) welk soort cybersecurity expertise, in welke hoeveelheid, wordt aangeboden;

Uitgaande van een globale indeling in soorten expertise in technisch, management & organisatie, legal, onderzoek en onderwijs zien we het volgende in het bekostigd onderwijs:
Inhoudelijke focus van de mbo-opleidingen ligt vooral op de technische aspecten en in enige mate op management en organisatie aspecten. Door de variatie in hoe de ICT-opleidingen invulling geven aan het onderwijs, is niet mogelijk gebleken precies te achterhalen hoe groot het aandeel cybersecurity in de opleiding is.
Over de opleidingen heen lijken de hbo- en wo-opleidingen meer multidisciplinair ingestoken. In alle studies (mbo en ho) is er geen- weinig aandacht aan competentieontwikkeling op het gebied van onderwijs, waarmee studenten didactische kennis en vaardigheden kunnen ontwikkelen.
Vanwege het grote aanbod aan opleidingen in het particuliere segment is het plotten van het categoriseren van het aanbod niet goed doenlijk. Wel is ingezoomd op de opleidingen die voor een cybersecurity-certificaat opleiden. Ongeveer 20% van alle onbekostigde cybersecurity opleidingen is gericht op de meest gevraagde cybersecurity certificaten op de arbeidsmarkt.
Hetzelfde geldt voor de regionale initiatieven voor mkb-ers en burgers. Aanbod daar lijkt globaal genomen met name gericht op vergroten van awareness en cyberweerbaarheid.

Onderzoeksvraag 4:
Geef inzicht in de knelpunten inzake cybersecurity opleiding en omscholing. Denk hierbij aan factoren die de instroom en doorstroom beïnvloeden.

Als knelpunten en/of uitdagingen geven de ICT-opleidingsdirecteuren in het mbo aan [1] het up to date brengen van de docenten, [2] het tekort aan studenten, [3] ontoereikende faciliteiten en [4] de snelle opkomst van nieuwe thema's op het gebied van AI bijvoorbeeld.
In de interviews en vragenlijsten met docenten, hoogleraren en management van ho-instellingen komen verschillende knelpunten naar voren zoals: [1] tekort aan docenten met voldoende kennis, [2] de inhoud van het curriculum waarin zowel een breed profiel en specialistische profilering binnen het cyberdomein dient te worden aangeboden, [3] de snelheid waarin de security wereld zich ontwikkelt in combinatie met het gebrek aan vermogen om hier flexibel op te reageren, [4] de beeldvorming rondom cybersecurity onderwijs als technische studie dat invloed heeft op de werving en het verwachtingsmanagement van (potentiële) studenten en [5] het gebrek aan middelen voor bijv. onderwijsmateriaal, hybride leerwerkplekken etc.)
In het onbekostigde onderwijssegment geven opleiders als belemmerende factoren aan dat mensen bij de om-, bij en nascholing in cybersecurity geen toegang hebben tot opleidingssubsidies of onvoldoende tijd krijgen van de werkgevers om een leergang goed te doorlopen.

3.1 Introductie

Het onderwijs op het gebied van cybersecurity is volop in ontwikkeling. In dit hoofdstuk wordt een overzicht geboden van het opleidingen, in- en uitstroom van studenten op het gebied van mbo (paragraaf 3.3) en het hbo en wo onderwijs (paragraaf 3.4). In paragraaf 3.5 wordt inzicht gegeven in de inhoud van deze opleidingen.
Het Leven Lang Ontwikkelen aanbod wordt beschreven in paragraaf 3.6, waarna de conclusies en gevonden knelpunten in paragraaf 3.7 besproken worden.

3.2 Ordeningskader/kijkwijzer

Bij het mbo zijn zowel type opleidingen als eindtermen landelijk afgestemd. Daarbinnen heeft een onderwijsinstelling wel ruimte voor eigen invulling van het onderwijs. Voor mbo is daarom gekeken naar de omschrijving van eindtermen van alle vier de ICT-opleidingen. Tevens zijn opleidingen binnen Zakelijke Dienstverlening in ogenschouw genomen.

Bij het hbo en wo is gezocht op een aantal trefwoorden binnen DUO en pre-DICT. Vervolgens is er gekeken naar beschikbare online-informatie over opleiding en op basis daarvan zijn opleidingen ingedeeld in:

- Volledige cybersecuritystudies
- Studies met een specialisatie-/keuzerichting cybersecurity
- Studies met een verplicht onderdeel cybersecurity (> 6 EC)
- Opleidingen met 1 (keuze)vak van 6EC
- Geen cybersecurity studies

Voor de LLO-analyse is gezocht op een aantal trefwoorden op het gebied van cybersecurity en veiligheid binnen overzichten met niet-bekostigd onderwijs en publiek private initiatieven.
Vervolgens zijn opleidingen gelabeld en zijn vergelijkbare activiteiten geclusterd om enig beeld te krijgen van waar zwaartepuntvorming in het aanbod is. Bij de opleidingen is ook specifiek gekeken naar welke en hoeveel er opleiden voor cybersecurity certificaten.

3.3 Mbo

3.3.1 Opleidingsaanbod

Mbo-scholen bieden opleidingen aan op vier niveaus. Wat mbo-studenten aan het eind van hun opleiding moeten kennen en kunnen, staat in kwalificatiedossiers. Op basis van deze eisen stelt de mbo-opleiding onderwijsprogramma's en examens op. Vertegenwoordigers van werkveld en onderwijs werken mee aan de ontwikkeling van de kwalificatiedossiers. De minister van Onderwijs, Cultuur en Wetenschap (OCW) stelt de kwalificatiedossiers vast. De kwalificatie-eisen om het mbo-diploma te behalen, liggen dus landelijk vast.
Voor de hand ligt dat de mbo-opleidingen ICT veruit de meeste raakvlakken hebben met het thema cybersecurity in vergelijking met andere mbo-opleidingen.
Daarom zijn deze opleidingen als eerste onder de loep genomen. De kwalificatiedossiers bieden een eerste ingang om zicht te krijgen op de aandacht voor cybersecurity. Er zijn momenteel drie kwalificatiedossiers.
In tabel 1 is in steekwoorden omschreven wat de eisen zijn die een link hebben met cybersecurity:

Huidige kwalificatiedossiers ICT	
ICT support Medewerker ICT support (niveau 2)	Kan security-issues (zoals firewall, virusscanner, WPA 2) toepassen Aanvullend voor niveau 3: Voorziet gebruikers van handreikingen mbt security-issues https://kwalificatie-mijn.s-bb.nl/

Software development Software developer (niveau 4)	Past wetgeving op het gebied van o.a. computercriminaliteit toe op software Kan principes van Secure Software Development Life Cycle toepassen Kan controleren en toelichten of een softwareontwerp voldoet aan beveiligingseisen https://kwalificatie-mijn.s-bb.nl/
IT systems & devices Allround medewerker IT systems & devices medewerker (niveau 3) Expert IT systems & devices (niveau 4)	Werkt volgens geldende securityrichtlijnen Aanvullend voor niveau 4: Geeft securityadvies en verbetert de security Reageert op security incidenten https://kwalificatie-mijn.s-bb.nl/

Tabel 1: eisen met een link met cybersecurity binnen de huidige mbo kwalificatiedossiers

De twee niveau 4-opleidingen (software developer en expert IT system & device) raken het meest aan cybersecurity.

Met ingang van 1 augustus 2024 treden nieuwe kwalificatiedossiers voor ICT Support (niveau 2) en Software Developer in werking. Per 1 augustus 2025 volgt het kwalificatiedossier ICT Support & Systems het dossier IT Systems & Devices op. Deze nieuwe dossiers zijn ook bekeken.

Deze kwalificaties zijn vernieuwd, waarbij cybersecurity een explicietere uitwerking heeft gekregen (tabel 2).
Wat meteen opvalt en ook in de lijn der verwachtingen ligt is dat er veel meer aandacht is voor cybersecurity. Er is een apart profieldeel binnen de opleiding ICT-system engineer.

Nieuwe kwalificatiedossier ICT	
ICT support Medewerker ICT niveau 2	Heeft basiskennis van nieuwe ontwikkelingen op het gebied van (netwerk)-security Kan regels, afspraken en procedures toepassen die betrekking hebben op veiligheid en privacy https://kwalificatie-mijn.s-bb.nl/
Software development Software developer niveau 4	Heeft kennis van security & privacy passend bij het eigen vakgebied Heeft brede kennis van cybersecurity en bedreigingen van netwerken en systemen Heeft brede kennis van wetgeving mbt computercriminaliteit en kan conform werken Volgt geldende protocollen en regelgeving rondom veiligheid van software en laat dit in het ontwerp zien https://kwalificatie-mijn.s-bb.nl/
IT support and systems ICT support technician niveau 3 ICT system engineer niveau 4	Heeft kennis van eenvoudige securitymaatregelen Kan instructies geven aan gebruikers mbt security Heeft kennis over de beveiliging van informatievoorzieningen Werkt conform SLA's, procedures en bedrijfsafspraken mbt security Toont zicht bewust van security door veiligheidsmaatregelen in informatie/instructies op te nemen Profieldeel voor niveau 4: Een belangrijk aandachtspunt in het werk van de ICT system engineer is security. Hierbij gaat het zowel om de beveiliging van systemen als om de reactie op cybersecurityaanvallen In het profieldeel wordt dit gedetailleerd uitgewerkt. (per maart 2024 openbaar)

Tabel 2: eisen met een link met cybersecurity binnen de nieuwe mbo kwalificatiedossiers

De opleiding ICT system engineer niveau 4 besteedt de meeste aandacht aan (cyber)security. Deze beginnend beroepsbeoefenaar wordt opgeleid om de security te kunnen controleren en te verbeteren en om op cybersecurity incidenten te kunnen reageren.
Binnen de opleiding Software Development wordt de beginnend beroepsbeoefenaar vooral bijgebracht dat principes van security in alle contexten van software development aanwezig zijn en dat je hiermee dus rekening houdt bij alle (deel)ontwerpen.

Onderstaande tabel 3 bevat de gegevens hoeveel mbo's welke ICT opleidingen aanbieden. De opleidingen tot software developer en expert systems & devices hebben de meeste raakvlakken met cybersecurity. Bijna alle mbo's bieden deze 2 opleidingen.

Combinatie van ICT-opleidingen	Aantal mbo's
Medewerker ICT niveau 2 Software developer niveau 4 Allround medewerker IT systems & devices niveau 3 Expert IT systems & devices niveau 4	32
Software developer niveau 4 Allround medewerker IT systems & devices niveau 3 Expert IT systems & devices niveau 4	5
Software developer niveau 4 Allround medewerker IT systems & devices niveau 3	1
Software developer niveau 4	2

Tabel 3: Welke ICT-opleidingen worden aangebodenen aangeboden

Daarnaast zijn er op dit moment voor het mbo nog drie opleidingen, specifiek gericht op cybersecurity, die in de ontwikkelingsfase, accreditatiefase, of opstartfase zijn:

- MBO Rijnland : Cyber education
- ROC Aventus : Safety & Security
- ROC Mondriaan : Cyber education

Naast de ICT-opleidingen is ook gekeken of er binnen de opleiding Zakelijke Dienstverlening en Veiligheid expliciet kennis en vaardigheden op het gebied van cybersecurity aan de orde zijn.

- Binnen de opleiding Beveiliger van ROC Aventus is het keuzedeel Basis cybercriminaliteit en cyberveiligheid ontwikkeld. Aventus is aangesloten bij het Centrum voor Veiligheid en Digitalisering en werkt samen met Politie Oost Nederland om een eenjarige opleiding op maat te kunnen aanbieden voor nieuwe politie-collega's. Het doel van deze opleiding is om kennis te maken met de mogelijkheden, dreigingen en kwetsbaarheden van de digitale wereld bij uitvoering van werkzaamheden en actie te ondernemen als er een digitaal incident dreigt of in uitvoering is. Er is ook een nieuwe kwalificatie in ontwikkeling met de werknaam Safety en Security. Dit is een kwalificatie voor een 1 –jarige kopopleiding (niveau 4) als aanvulling op niveau 3 beveiliger.
- Wat betreft de juridisch-administratieve opleiding: daar is de bedrijfstakgroep nu bezig om bij de financiële dienstverlenende bedrijven op te halen waarin de opleidingen moeten worden geactualiseerd. Thema's als Duurzaamheid en cybersecurity zitten daar zeker bij. Maar dit verkeert nog in het stadium van een eerste gedachtenvorming hoe deze thema's in de opleiding een plek moeten krijgen.

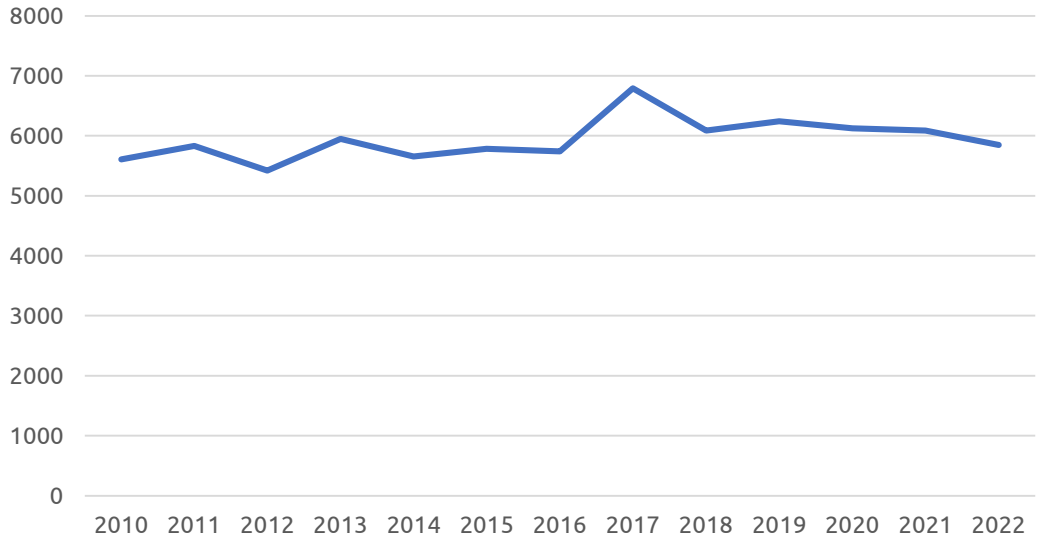
3.3.2 In- en uitstroom

Om een gevoel te geven van de omvang van de potentiële HCA-pool voor cybersecurity in het mbo is gekeken naar het aantal bekostigde studenten in de schooljaren 2017/2018 t/m 2022/2023 per kwalificatiedossier (tabel 4).

	2017-18	2018-19	2019-20	2020-21	2021-22	2022- 23
Medewerker ICT niveau 2	2.457	2.496	2.340	2.348	2.405	2.330
Software developer niveau 4	8.018	8.718	9.011	9.251	9.486	9.553
Allround medewerker IT systems & devices niveau 3	4.631	4.272	3.979	3.437	3.006	2.715
Expert IT systems & devices niveau 4	8.219	8.398	8.601	8.684	8.151	7.472
Totaal	23.325	23.884	23.931	23.720	23.398	22.532

Tabel 4: aantal bekostigde studenten in de schooljaren 2017/2018 t/m 2022/2023 per kwalificatiedossier
Bron: DUO, bewerkt door SBB, 7 februari 2023

Deze aantallen ICT-studenten over alle opleidingen leveren jaarlijks een uitstroom op van ongeveer 6.000 gediplomeerde mbo ICT-studenten (figuur 5).



Figuur 5: Jaarlijkse uitstroom gediplomeerde bekostigde mbo ICT-studenten over de tijd
Bron: HCA ICT, 2023 (gegenereerd op 18/01/2024 09:58 uit pr-eDICT)

Natuurlijk zijn deze gediplomeerde mbo-ers, ook de niveau 4-studenten, direct na diplomering nog geen breed inzetbare cybersecurityspecialisten. Maar het is qua aantallen natuurlijk wel een substantiële bron van cybertalent. Jaarlijks komen er immers ongeveer 6.000 nieuwe ICT'ers bij die ieder geval kunnen bijdragen aan de technische, operationele aspecten van cybersecurity en die je op het pad naar cybersecurityexpert zou kunnen zetten.
Daarom is het zeker relevant om de ontwikkelingen van deze aantallen mbo-studenten te blijven volgen. Bijvoorbeeld valt op dat er tussen 2017 – 2023 een overall daling is van aantallen ICT mbo-studenten. En ook dat in het afgelopen jaar er een duidelijke daling te zien is bij studenten expert IT system, de opleiding die in het nieuwe kwalificatiedossier gegeven het profieldeel het meest voorsorteert op cybersecurity (tabel 4).

Tevens is ook nog gekeken naar het aantal studenten die de keuzedelen volgen[9] die specifiek een link hebben met cybersecurity. Tot nu toe gaat het om twee keuzedelen die worden gegeven binnen de opleidingen ICT & Mediabeheer, Smart Building en Smart Industry:

- Het keuzedeel Security in systemen en netwerken 1 gaat in op het preventief signaleren van afwijkingen van beleid, kwetsbaarheden en bedreigingen en het evalueren van de oorzaken en risico's voor systemen en netwerken. Op basis hiervan worden voorstellen gedaan voor beveiligingsmaatregelen. In het studiejaar 2022-2023 wordt dit keuzedeel door 19 mbo's, bij 34 opleidingen aan 1.004 studenten gegeven.

9. Bron: S-BB Dasboard keuzedelen en mbo-certificaten. Nota bene: het gaat om het minimaal aantal studenten. Niet alle instellingen hebben (volledige) informatie aangeleverd. Wel geeft het dashboard een representatief beeld, 60 - 70%.

- Het keuzedeel Security in systemen en netwerken 2 gaat in op het volgen van technologische ontwikkelingen om een beeld te krijgen van de actuele dreigingen en beveiligingsmogelijkheden, het vergelijken van gegevens uit de monitoring en testen, het doen van voorstellen en implementeren van beveiligingsaanpassingen. In het studiejaar 2022-2023 wordt dit keuzedeel door 13 mbo's, bij 20 opleidingen aan 321 studenten gegeven.

3.3.3 Hoe vullen mbo's het ICT-onderwijs in?

De kwalificatiedossiers zorgen voor uniformiteit in eindtermen van de mbo-opleidingen. Daarbinnen hebben de mbo-opleidingen de nodige ruimte om het onderwijsprogramma in te vullen.
Om meer zicht te krijgen op hoe binnen de ICT-opleidingen vorm wordt gegeven aan het onderwijs op het gebied van cybersecurity is een enquête uitgezet onder alle 40 ICT opleidingsdirecteuren.
Dit heeft een respons van 17 deelnemers opgeleverd.

Een aantal inzichten uit deze enquête kort samengevat (supplementaire tabellen in Bijlage 2):

- Gevraagd naar welk rapportcijfer voor de eigen inzet op cybersecurity geeft ruim de helft van de respondenten zichzelf een 7 of hoger. Tegelijk valt de spreiding van de scores op: er is dus het nodige verschil tussen de mbo ICT-opleidingen in hoeverre ze zelf vinden dat ze voldoende aandacht besteden aan cybersecurity (supplementaire tabel 4).
- Uitgesplitst naar opleiding is binnen drie van de vier opleidingen aandacht voor cybersecurity (supplementaire tabellen 5.1 t/m 5.4). Alleen bij de niveau 2-opleiding Medewerker ICT Support niveau 2 besteedt 50 % van de opleidingen aandacht aan cybersecurity.
- Bij de opleiding Expert IT system & devices niveau 4 (supplementaire tabel 5.4) is er vooral binnen de individuele praktijkopdrachten en specifieke vakken en modules aandacht voor cybersecurity. Bij de opleiding tot software developer (supplementaire tabel 5.2) is er regelmatig aandacht bij individuele praktijkopdrachten en tijd de beroepspraktijkvorming

Voorts is deskresearch gedaan om ROC's in beeld te brengen die zich tot nu toe specifiek op cybersecurity profileren. Momenteel zijn dit:

- ROC van Amsterdam: cybersecurity maakt standaard onderdeel uit van ICT-opleidingen. De student kan in het 2e en 3e jaar kiezen voor het keuzedeel Cyber Security. Als deze succesvol wordt afgerond, mag de student zich officieel Cyber Security Specialist noemen. ROC van Amsterdam werkt intensief samen met grote organisaties zoals SLTN, KPN en Hewlett Packard Enterprise. Deze bedrijven brengen kennis, deskundigheid en docenten in;
- ROC Mondriaan: cybersecurity vormt een standaard onderdeel van de opleidingen van de School voor ICT. De student kan na de opleiding een bedrijf met praktische oplossingen meer bestand maken tegen cyberdreigingen of goed doorstromen naar een vervolgopleiding op hbo- niveau. Alle studenten krijgen in het eerste jaar les in het vak COPS van Cisco en in het tweede jaar een praktijkopdracht, waarbij binnen een mkb-bedrijf een cybersecurityopdracht wordt uitgevoerd;
- ROC Noorderpoort is verbonden met het Practoraat Digitaal Vakmanschap. Het Practoraat richt zich zowel op de digitale weerbaarheid als persoon als op de digitale weerbaarheid in het beroep. Het Practoraat is een vervolg op Cyber@Work, een project waarbij docenten ICT cybersecurity inbedden in het mbo ICT-onderwijs en studenten inzetten voor het versterken van de digitale veiligheid van burgers, verenigingen, stichtingen en mkb-bedrijven. Cyber@Work is nu als kenniskring een onderdeel van het Practoraat;
- ROC Aventus participeert in het Centrum voor Veiligheid en Digitalisering in de programma's Onderwijs en Leven Lang Ontwikkelen. Zo wordt de mogelijkheid van een nieuwe inhoudelijke niveau 4 opleiding Veiligheid & Digitalisering verkend.

Op dit moment zijn er voor het mbo drie opleidingen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn:

- Mbo Rijnland : Cyber education
- ROC Aventus : Safety & Security
- ROC Mondriaan : Cyber education

3.3.4 Voor welke expertise wordt in het mbo opgeleid?

Geredeneerd vanuit een indeling in competenties die de arbeidsmarkt vraagt is een expert-inschatting op basis van de kwalificatiedossiers gemaakt van de typen competenties per opleiding (tabel 5).
Hieruit ontstaat het beeld dat ICT-opleidingen in het mbo vooral aansluiten bij de technische functies binnen cybersecurity.

Actuele opleidingsnaam	Aandeel cybersecurity	Technisch	M&O	Legal	Onderzoek	Onderwijs
Software developer	Deels	3	0	0	0	0
Expert IT systems and devices	Deels	3	2	0	0	0
Allround medewerker IT systems and devices	Deels	3	1	0	0	0
Medewerker ICT support	Deels	3	0	0	0	0

Tabel 5: expert-inschatting mate van aanwezigheid typen competenties per opleiding op basis van de kwalificatiedossiers. Van 0 geen/nauwelijks een rol voor de desbetreffende competentie tot 3 de primaire focus ligt op deze competentie.

3.3.5 Knelpunten

Aan de opleidingsdirecteuren ICT is de vraag voorgelegd wat er nog nodig is om actueel onderwijs op het gebied van cybersecurity te bieden (supplementaire tabel 6). In volgorde van het meest genoemd zijn dit professionalisering van docenten (70 %), medewerking van het werkveld (70 %), onderwijs & examenmateriaal (bijna 65 %), voldoende docenten (50 %) en hybride leerwerkplekken (ruim 40 %).

Ook is gevraagd naar welke cybersecuritythema's meer aandacht behoeven. Dit hoeft natuurlijk niet per se een knelpunt te zijn maar wijst mogelijk wel in de richting van waar een knelpunt in het onderwijs kan ontstaan. Het vaakst genoemd worden AI (bijna 80 %), Data-awareness (bijna 60 %) en Samenwerkingstooling (50%) (supplementaire tabel 7).

3.4 Hoger onderwijs

3.4.1 Opleidingsaanbod

Hogescholen en universiteiten bieden opleidingen aan op respectievelijk hbo- en wo- niveau. Elke onderwijsinstelling bepaalt zelf de inhoud van de studies die ze aanbiedt. Wel moet de instelling een opleidingsplan schrijven, dat gekeurd wordt door een panel van onafhankelijke deskundigen van de NVAO.

Tabel 6 geeft een overzicht van de aantallen relevante Nederlandse opleidingen op het gebied van cybersecurity op hbo en wo-niveau. Binnen de NVAO-geaccrediteerde opleidingen, zijn er 10 studies geïdentificeerd die volledig in het teken staan van cybersecurity, 29 studies die een specialisatie-/keuzerichting cybersecurity aanbieden, en 13 studies die een verplicht onderdeel cybersecurity in hun programma hebben geïntegreerd, groter dan 6 ECTS. Details over welke studies van welke onderwijsinstellingen dit exact betreffen is terug te lezen in bijlage (supplementaire tabel 8 t/m 10). Tijdens het in kaart brengen van de relevante Nederlandse opleidingen op het gebied van cybersecurity op hbo- en wo-niveau, zijn tevens enkele studies (waaronder drie mbo-initiatieven) aan het licht gekomen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn. Voor de volledigheid zijn deze studies toegevoegd onder aan tabel 6. Details over welke studies van welke onderwijsinstellingen dit exact betreffen is opgenomen in supplementaire tabel 11 in Bijlage 2.

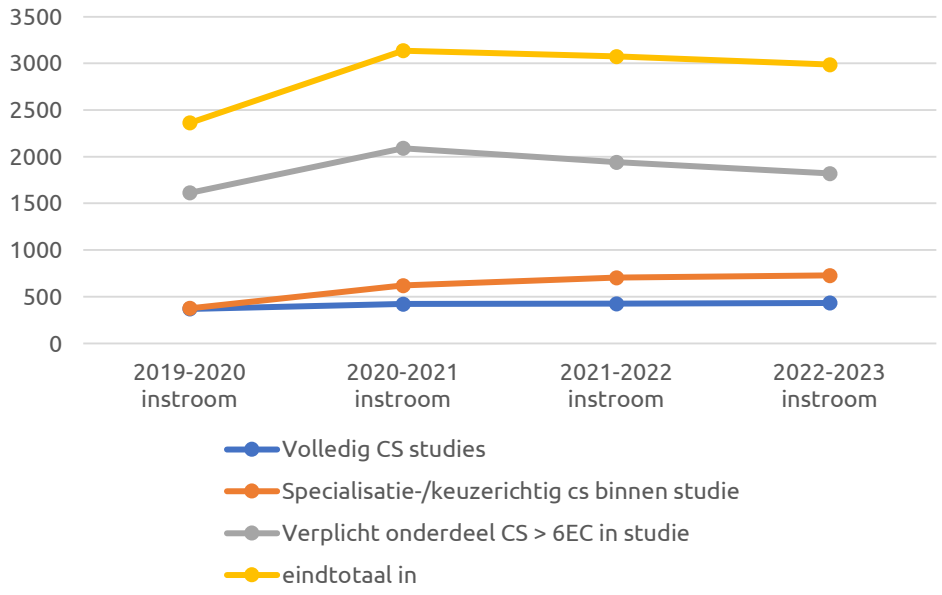
Volledig cybersecurity studies	Aantal
Hbo	5
Wo	5
Totaal	**10**
Specialisatie-/keuzerichtig cybersecurity binnen studie	**Aantal**
Hbo	18
Wo	11
Totaal	**29**
Verplicht onderdeel cybersecurity > 6ECTS in studie	**Aantal**
Hbo	6
Wo	7
Totaal	**13**
Aankomende cybersecurity opleidingen	**Aantal**
Hbo	8
Wo	1
Totaal	**9**

Tabel 6: overzicht van de aantallen relevante Nederlandse opleidingen op het gebied van cybersecurity op hbo-en wo-niveau

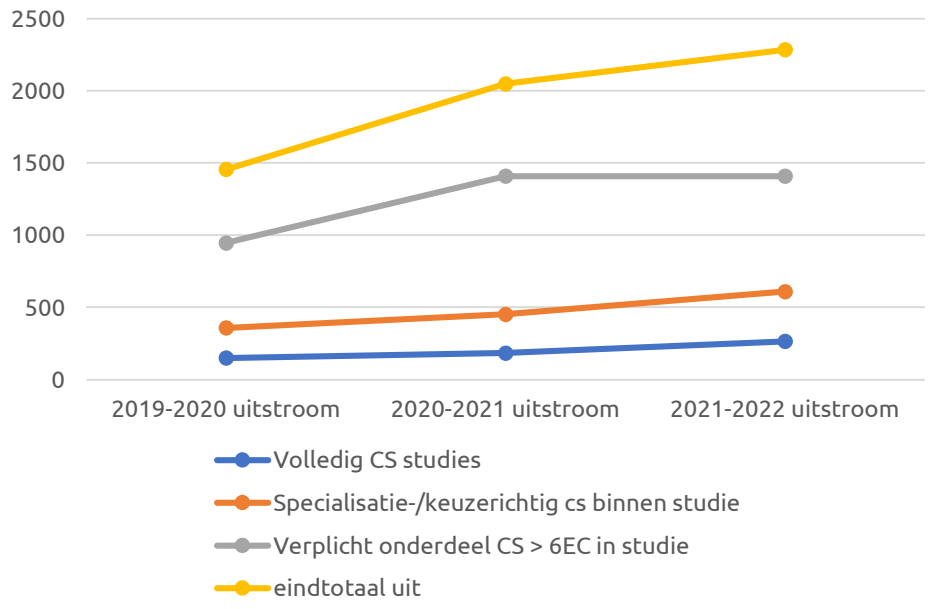
3.4.2 In- en uitstroom

Ook voor het hoger onderwijs is gekeken naar het aantal bekostigde studenten in de afgelopen jaren. Om een gevoel te krijgen van de omvang vanuit het hoger onderwijs van de potentiële HCA pool voor cybersecurity, zijn de in- en uitstroomcijfers van studenten opgehaald in de schooljaren 2019/2020 t/m 2022/2023, per studie. Waar beschikbaar, zijn deze gegevens opgehaald vanuit de open Dienst Uitvoering Onderwijs (DUO)-data. Cijfers die niet voor DUO beschikbaar gesteld zijn, zijn opgevraagd bij de desbetreffende programma directors. De cijfers per opleiding zijn terug te vinden in Bijlage 2 (supplementaire tabel 8 t/m 10). Onderstaande figuren geven de in- en uitstroom gegevens weer voor het volledige hoger onderwijs. Gegevens uitgesplitst voor hbo en wo, zijn terug te vinden in de bijlage (supplementaire figuur 2 t/m 7 en 8 t/m 13, respectievelijk).

Figuur 6 en 7 geven respectievelijk de in- en uitstroom qua studenten weer voor alle studies met een relevant onderdeel cybersecurity. Dit zijn zowel de studies die volledig in het teken staan van cybersecurity, als ook de studies die een specialisatie-/keuzerichting cybersecurity aanbieden en de studies die een verplicht onderdeel cybersecurity in hun programma hebben geïntegreerd (> 6 ECTS). Aangezien de open DUO uitstroomdata van het leerjaar 2022/2023 en de instroomdata van het leerjaar 2023/2024 nog niet beschikbaar zijn, zijn deze schooljaren voor de visuele weergave weggelaten in de grafieken. Voor enkele cybersecurity specifieke opleidingen zijn deze data wel door de programma directors beschikbaar gesteld. Deze data zijn terug te vinden in bijlage 2 (supplementaire tabel 8 t/m 10).

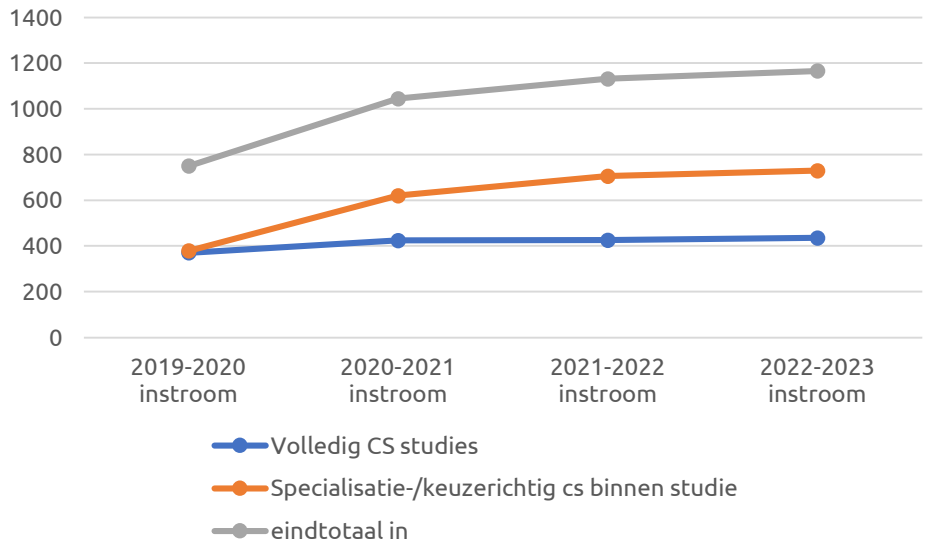


Figuur 6: Verloop instroom studenten over de tijd, alle studies met relevant onderdeel cybersecurity

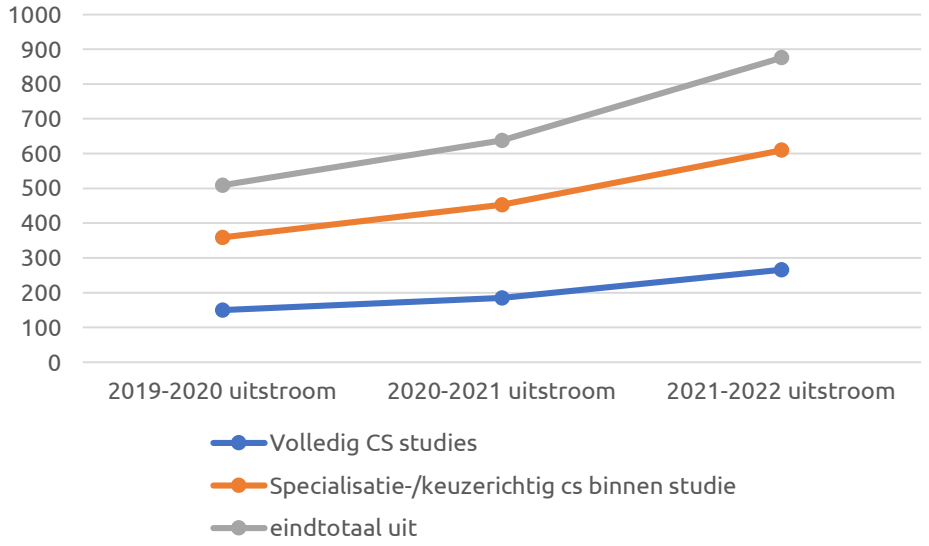


Figuur 7: Verloop uitstroom studenten over de tijd, alle studies met relevant onderdeel cybersecurity

Figuur 8 en 9 geven respectievelijk de in- en uitstroom van studenten weer met een specialistische cybersecurity focus. Dit zijn studenten vanuit studies die volledig in het teken staan van cybersecurity en studenten die binnen hun studie een specialisatie-/keuzerichting cybersecurity gekozen hebben. Ook hier geldt dat de uitstroomdata van schooljaar 2022/2023 en de instroomdata van leerjaar 2023/2024 visueel weggelaten zijn in de grafieken, omdat de open DUO data van deze schooljaren nog niet beschikbaar zijn. Waar wel beschikbaar zijn deze cijfers terug te vinden in bijlage 2 (supplementaire tabel 8 t/m 10).



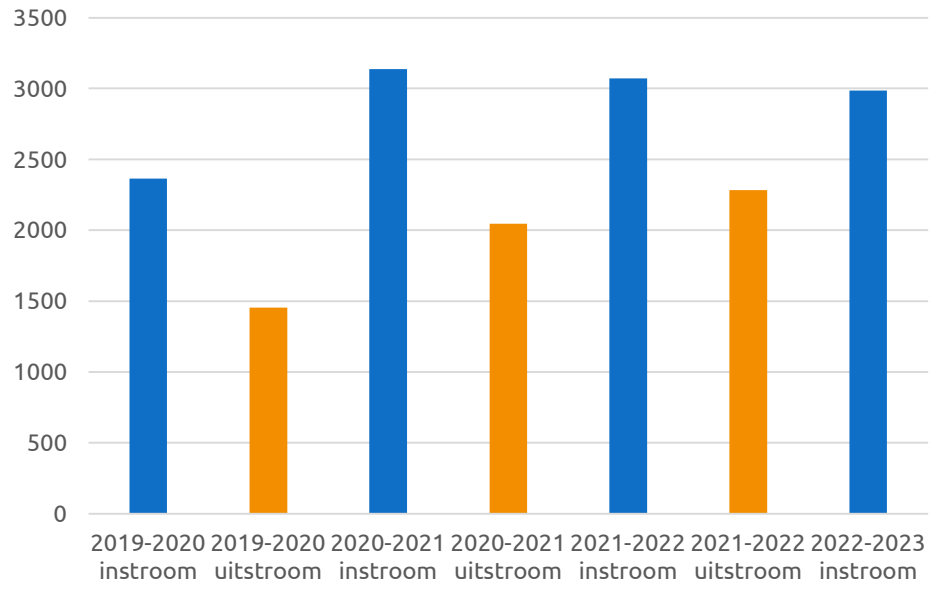
Figuur 8: Verloop instroom studenten over de tijd, studenten vanuit studies die volledig in het teken staan van cybersecurity en studenten die binnen hun studie een specialisatie-/keuzerichting cybersecurity gekozen hebben



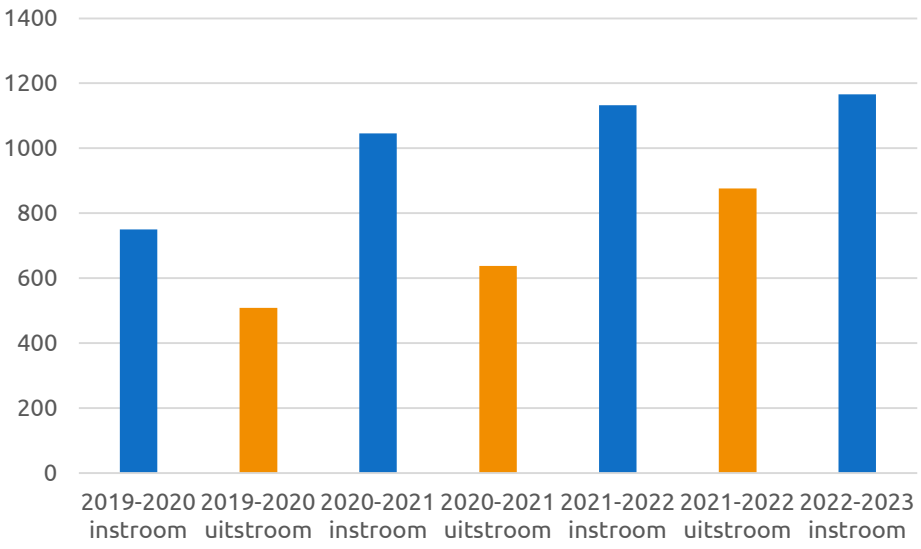
Figuur 9: Verloop uitstroom studenten over de tijd, studenten vanuit studies die volledig in het teken staan van cybersecurity en studenten die binnen hun studie een specialisatie-/keuzerichting cybersecurity gekozen hebben

Wat opvalt in figuur 6 en 7 is dat de instroom aan studenten met een relevant onderdeel cybersecurity in hun studie primair initieel stijgt, maar de laatste jaren redelijk gelijk blijft rond de 3000 studenten jaarlijks. De uitstroom aan studenten neemt jaarlijks echter duidelijk geleidelijk toe. Deze toename lijkt hem met name te zitten in het aantal studenten vanuit studies die volledig in het teken staan van cybersecurity danwel studenten die binnen hun studie een specialisatie-/keuzerichting cybersecurity gekozen hebben. Figuur 8 en 9 bevestigen dat zowel de in- als uitstroom van deze categorie studenten toeneemt over de tijd. Gezien de in- en uitstroomcijfers van circa 70% van deze opleidingen met cyberfocus beschikbaar gesteld zijn, zullen de absolute aantallen studenten circa 40% hoger liggen dan weergegeven in de grafieken. Naar verwachting beïnvloedt dit de relatieve stijging over de jaren niet tot nauwelijks.

Om inzichtelijk te maken wat de trend in de verhouding instroom/uitstroom door de jaren is, wordt in figuren 10 en 11 de in- en uitstroom per leerjaar naast elkaar weergeven.



Figuur 10: instroom versus uitstroom voor alle studies met relevant onderdeel cybersecurity



Figuur 11: instroom versus uitstroom van studenten die een specifieke cybersecurity opleiding danwel een specifieke cybersecurity gerichte specialisatie-/keuzerichting gevolgd hebben.

Voor alle leerjaren geldt dat de instroom aan studenten groter is dan de uitstroom aan studenten. Deze verschillen worden over de tijd echter wel geleidelijk kleiner. Meest waarschijnlijk is deze afname van de instroom/uitstroom verhouding te verklaren doordat de meeste cybersecurity specifieke opleidingen danwel specialisatie-/keuzerichtingen pas enkele jaren bestaan. Er zijn bijvoorbeeld drie specialisatie-/keuzerichtingen die pas de eerste studenteninstroom ná het schooljaar 2019-2020 hebben. Daarnaast heeft de Ad Cybersecurity van de Hogeschool van Amsterdam bijvoorbeeld in 2019-2020 voor het eerst instroom, en nog geen uitstroom (supplementaire tabel 8 t/m 9). In de eerste jaren zal een studie en/of specialisatie-/keuzerichting meer instroom dan uitstroom hebben. Dit haalt zich dan in de loop der tijd in tot er een evenwicht ontstaat.

3.4.3 Resultaten enquête: ontwikkelingen en knelpunten binnen het cybersecurity onderwijs en reeds genomen acties om de aansluiting op de arbeidsmarkt te optimaliseren

Om inzicht te verkrijgen in de huidige ontwikkelingen/trends binnen het cybersecurity onderwijs, de aansluiting/ samenwerking met de arbeidsmarkt en de ervaren knelpunten is een enquête uitgezet bij een selectie aan programma directors van specifieke cybersecurity opleidingen en cybersecurity gerichte specialisatie- en keuzerichtingen. Twintig programma directors vanuit dertien verschillende opleidingen hebben gehoor gegeven aan deze enquête. Hieronder zijn de belangrijkste resultaten uit deze enquête samengevat:

Ontwikkelingen/trends binnen cybersecurity onderwijs

- Multidisciplinaire benadering van cybersecurity met zowel aandacht voor de technische kant als ook de organisatorische kant/beleid, wet- en regelgeving, ethiek en communicatie (specialistisch niveau en lekentaal);
- Introduceren van een circulair beleid (Adaptive Security Framework van Gartner, CSF2.0 van NIST, etc.);
- Voldoen aan wet- en regelgeving (AVG, GDPR, NIS2, etc.);
- IT of security-gerelateerde certificaten (ISO27001, ISO7510, BIO etc.);
- Continu updaten van het onderwijs gezien snel ontwikkelende aandachtsgebieden: informatiebeheer, cloud security, automatisering door AI waardoor rollen mens en technologie drastisch zullen veranderen, internet of things, pentesting, vulnerability reporting, SecDevOps, cyberspace, quantum technologie, verdediging tegen geavanceerde geautomatiseerde cyberaanvallen, thread intelligence, etc.);
- Lectoraten en experts uit publieke en private organisaties, waarmee een hoge kwaliteitsstandaard gegarandeerd kan worden;
- In het algemeen is er een toename in het aantal cyberincidenten.

Actuele acties ten behoeve van optimale aansluiting/samenwerking met de arbeidsmarkt

- Gebruik van gastsprekers en freelance docenten vanuit bedrijfsleven;
- Stages en/of afstudeerprojecten in het werkveld;
- Stimuleren aansluiting onderwijs op vraag arbeidsmarkt door vertegenwoordiging van zowel onderwijs als arbeidsmarkt in o.a. opleidingsadviesraad, bedrijfsadviesraad, andere adviesorganen, vertegenwoordigerscommissie, beroepenveldcommissie;
- Organisaties en stichtingen zoals Cyber Veilig Nederland, Security Delta, Platform voor Informatie Beveiliging, Nationaal Cyber Security Centrum, HBO-i, Intersct, ACademic Cyber Security Society, dcypher, NEXIS;
- Cybersecurity evenementen voor zowel onderwijs als bedrijfswereld;
- Netwerk van docenten, alumni en hun werkgevers;
- Stakeholders events (bijvoorbeeld een jaarlijks stakeholder diner)

Knelpunten binnen het onderwijs

- Docenten:
  - Tekort aan docenten met voldoende kennis, schaarse pool van experts;
  - Vasthouden van gekwalificeerd onderwijzend personeel uitdagend door o.a. discrepantie tussen beloning bedrijfsleven en onderwijs;
  - Aanleren van cybersecurity skills vereist technische hands-on cursussen. Deze zijn relatief zwaar voor docenten en moeten in relatief kleine groepjes gegeven worden voor optimaal leren;
- Ontwikkelen van materiaal en samenstelling van een curriculum waarin de kwaliteit over een breed profiel met het aanleren van zeer diverse skills geborgd wordt, en waarin tegelijkertijd ook scherpe en specialistische profilering binnen het cyberdomein geboden wordt;
- Snelheid waarmee de securitywereld zich ontwikkelt in combinatie met het gebrek aan vermogen om hier flexibel op te reageren. Dit gezien onderwijseenheden al ruim een jaar voor de uitvoering vast moeten staan;
- Cybersecurity onderwijs wordt nog vaak gezien als technische studie. Daarmee wordt onvoldoende erkend dat cybersecurity onderwijs een onderdeel is van alle aspecten van onze leefwereld. Dit is belangrijk in de werving en het verwachtingsmanagement van (potentiële) studenten;
- Gebrek aan middelen (lab met apparatuur).

3.5 Vergelijking inhoud opleidingen mbo en ho

Om een inschatting te maken voor welke typen competenties een student opgeleid wordt, is de vertegenwoordiging van de volgende competenties binnen de mbo- en hb-opleidingen onderzocht: technisch, management & organisatie (M&O), legal, onderzoek en onderwijs. De vertegenwoordiging van de desbetreffende competentie zijn gescoord op een schaal van 0 (geen/nauwelijks een rol voor de desbetreffende competentie) tot 3 (de primaire focus ligt op deze competentie) (tabel 7).

Onderwijstype	Technisch	M&O	Legal	Onderzoek	Onderwijs	Totaal
Wo	2,4	1,1	0,9	2,7	0,0	7,0
Hbo	2,3	1,8	0,9	0,9	0,0	6,0
Mbo	3,0	0,8	0,0	0,0	0,0	3,8
Totaal	2,4	1,4	0,9	1,6	0,0	6,3

Tabel 7: vertegenwoordiging van typen competenties binnen mbo- en hb-opleidingen

Over de opleidingen heen lijken de hbo- en wo-opleidingen meer multidisciplinair ingestoken. De vier mbo-opleidingen (kwalificatiedossiers) zijn sterk technisch ingericht. De competentie onderwijs is in alle studies sterk ondervertegenwoordigd tot afwezig. Een overzicht van de individuele mbo-, hbo- en wo-opleidingen, gescoord naar mate van aansluiting bij arbeidsmarktcompetenties, is terug te vinden in bijlage 2 (supplementaire tabel 12).

3.6 Leven Lang Ontwikkelen Aanbod

3.6.1 Opleidingsaanbod

Bij het aanbod voor Leven Lang Ontwikkelen (LLO) zijn in deze inventarisatie zowel niet-bekostigd onderwijs als publieke of publiek-private initiatieven in ogenschouw genomen die zich richten op bij-/ na- en omscholing in alle soorten en maten en doelgroepen. Ook initiatieven die beogen extra (zij-)instroom te generen zijn meegenomen.

Niet-bekostigd onderwijs

Niet-bekostigd onderwijs wordt niet gesubsidieerd door de ministeries van OCW en EZK. De kosten van de opleiding komen voor rekening van degene die de opleiding volgt, van de werkgever of van de uitkeringsinstantie. Dit particuliere opleidingsaanbod is breed en divers.

De volgende bronnen zijn geraadpleegd:

- www.leeroverzicht.nl

Deze website is met een uitputtende lijst van cybersecurity gerelateerde termen gescrapet. Dit heeft 2.409 hits opgeleverd die vervolgens zijn ingedeeld naar volledig cybersecurity, deels cybersecurity en geen cybersecurity (tabel 8).

	Volledig cybersecurity	Deels cybersecurity	Geen cybersecurity	Totale gescreende hits
Aantal opleidingen niet-bekostigd onderwijs	1136	824	449	2409

Tabel 8: resultaten www.leeroverzicht.nl ingedeeld naar volledig, deels en geen cybersecurity

De lijst uit leeroverzicht geeft inzicht in de belangrijkste aanbieders, wanneer zij gerangschikt worden naar het aantal opleidingen/cursussen etc dat wordt aangeboden (tabel 9):

#	Opleider	Aantal
1	Global Knowledge Network Netherlands bv	543
2	Icttrainingen.nl	155
3	Startel	132
4	Fast Lane Benelux B.V.	120
5	Master it Training	107
6	NCOI	104
7	Vijfhart IT-Opleidingen	92
8	@The Academy	89
9	Eduvision Opleiding & Training	69
10	CLS-trainingen	63
11	Computrain	63
12	Security Academy Opleidingen B.V.	57
13	SpiralTrain BV	30
14	Capgemini Academy	26
15	TSTC BV	23
16	LOI	16
17	IT Management Group	9
18	Xebia Academy	9
19	BTR Trainingen	7
20	Cibit Academy BV	7

Tabel 9: top 20 aanbieders opleidingen op www.leeroverzicht.nl

Ook is het aantal opleidingen geteld dat in de vorm van contractonderwijs door mbo, hbo en universiteiten wordt geboden (tabel 10):

	Mbo- en ho- aanbod in leeroverzicht.nl	
	Volledig cybersecurity	Deels cybersecurity
Mbo	10	12
Hbo	21	33
Wo	10	3

Tabel 10: aantal opleidingen aangeboden door mbo, hbo en universiteiten

Het merendeel van deze opleidingen vragen een substantiële tijdsinvestering want leiden op tot een regulier diploma (supplementaire tabel 13 en 14).

Ongeveer 20% van alle onbekostigde cybersecurity opleidingen is gericht op de meest gevraagde cybersecurity certificaten op de arbeidsmarkt. Bijlage 2 bevat de supplementaire tabel 15 net het aantal opleidingen uit leeroverzicht.nl dat opleidt voor een certificaat. Tevens zijn de certificaten gescoord op de mate waarin zij aansluiten bij de gevraagde arbeidsmarktcompetenties.

- *overzicht van opleidingen van de NRTO*

Niet alle opleiders zetten hun aanbod op leeroverzicht.nl. Volledigheidshalve is daarom een quick scan gedaan van de website met trainingen, cursussen en opleidingen met het NRTO-keurmerk. Dit leverde slechts een handjevol opleidingen op die niet via leeroverzicht in beeld zijn gekomen. Voor de analyse lijkt dit een te verwaarlozen aantal.

Publiek private initiatieven

- *Regioscan digitalisering mkb*

In elke provincie in Nederland is eind 2022, begin 2023 de Regioscan digitalisering mkb uitgevoerd, een systematische inventarisatie van regionale publiek-private initiatieven en activiteiten gericht op digitalisering van het mkb. De Regioscan is ontwikkeld op initiatief van het Ministerie van Economische Zaken en Klimaat in nauwe samenwerking met provincies en grote gemeentes, met als doel om:

- Meer inzicht te verkrijgen in de ecosystemen van publieke of publiek-private initiatieven die digitalisering bij mkb stimuleren;
- Best practices te identificeren en het lerend vermogen over regiogrenzen heen te vergroten;
- Meer samenhang, samenwerking en doorverwijzing tussen initiatieven te stimuleren.

De initiatieven zijn voorzien van een aantal labels, waaronder het label cybersecurity. Deze selectie op basis van dit label is nog aangevuld met initiatieven bekend bij de regiocontactpersonen van de HCA-ICT en levert het overzicht op zoals gepresenteerd in tabel 11.

Type activiteit	Aantal	Voorbeelden
Workshops & kennisevents	39	Online kennissessies om digitalisering onder de aandacht te brengen Openbaar kenniscafé
Advisering/consultancy	28	Digitaal hulpteam Eerstelijns advies
Netwerk & coördineren	26	Leren van elkaar kringen MIEC Data
Subsidies & financiering	21	Algemene Innovatie - innovatieprojecten Digitaliseringsvouchers
Scans & assessments	22	AVG Scan Basisscan Cyberweerbaarheid
Werken met studenten	19	Vouchers blockchain projecten Adviestrajecten studenten
Onderwijs voor professionals	16	Leven Lang Leren & Ontwikkelen - branches mkb Online trainingen
Onderwijs voor studenten	15	Cyber Serious game Hacklab.frl
Kennisplatform	12	MIEC Data Platform ICT- aanbieders
Gezamenlijke faciliteiten	10	Digitaliseringsscan vanuit ik ben Drenths Ondernemer R&D Labs
Onderzoek & ontwikkeling	12	Onderzoek - cyberweerbaarheid Practoraat Veilige Apparatuur
Signaleren	5	Communicatie richting mkb belanghebbenden over acute cyberdreigingen. In kaart brengen scholingsbehoefte (o.a. via scan)
Totaal	**225**	

Tabel 11: Activiteiten voor mkb-ers en regio's, specifiek cybersecurity.

In Bijlage 2 is supplementaire tabel 16 opgenomen met de lijst met alle regionale initiatieven.

- *Publiek-private (om)scholingsinitiatieven*

Op internet en binnen het Katapult-netwerk is gezocht naar publiek-private (om)scholingsinitiatieven, gericht op het vergroten van de instroom in cybersecurityonderwijs en functies. Een overzicht van deze initiatieven is weergegeven in tabel 12. De initiatieven Hacklab, Cloud IT Academy en Make IT Work staan vermeld op de HCA-ICT - netwerkkaart, waarbij Make IT Work bovendien als werkend model/voorbeeldinitiatief wordt gezien.

	Naam	Regio	Omschrijving
1	Hacklab	Friesland	Het Hacklab is een veilige plek waar jonge getalenteerde internetgebruikers naar toe kunnen komen om kennis en kunde binnen het cyberdomein op eigen niveau en tempo te ontwikkelen. De werkplaats staat open voor digitale hangjongeren, gamers, schoolverlaters, jongeren binnen het autisme spectrum en jongeren die uitdaging in hun huidige opleiding missen. Een vooropleiding is niet noodzakelijk; motivatie en nieuwsgierigheid wel. In het Hacklab wordt door verschillende gastdocenten aandacht besteed aan 21e-eeuwse vaardigheden op het gebied van IT/internet. Hierbij worden de leerlingen met verschillende individuele en groepsopdrachten uitgedaagd op het gebied van hacken, programmeren, lockpicking, pentesting etc. Omdat iedere leerling anders is, wordt met een mentor gekeken naar een passend ontwikkeltraject binnen de werkplaats. De mentoren binnen het Hacklab maken, indien gewenst, matches tussen de leerlingen en mogelijke werkgevers. Zo kunnen leerlingen praktijkervaring op doen, leren wat “werken” is, en, indien er sprake is van een wederzijdse klik en fijne samenwerking, een volwaardige stageplek, traineeship of zelfs baan krijgen. https://hacklab.frl/
2	Cybersecurity werkt	Landelijk	Met het platform cybersecuritywerkt.nl wil HSD helpen de mismatch tussen vraag en aanbod van cybersecurity talent op te lossen. De website biedt volop mogelijkheden voor omscholing en zij-instromers die hun carrière willen voortzetten in cybersecurity. Zo helpen we mensen met een interesse in cybersecurity -maar die een andere achtergrond hebben- op weg in de cybersecurity arbeidsmarkt. Op de website vinden ze: kennis over cybersecurity, een overzicht van de verschillende werkvelden, een keuzetest gebaseerd op hun werk- en opleidingsachtergrond en een overzicht van relevante vacatures voor starters in het cybersecurity domein https://cybersecuritywerkt.nl/
3	Cyber Security & Cloud	Utrecht	CITA-bedrijven bieden directe werkgelegenheid en de mogelijkheid om je kennis te verdiepen en uit te breiden via de duale hbo-opleiding Cyber Security & Cloud van Hogeschool Utrecht. https://cita.academy/studenten/cyber-security-cloud/
4	Make IT Work	Landelijk	Omscholingstraject op hbo-niveau mét baangarantie in de IT. Een van de drie omscholingsprogramma’s is cybersecurity. Gedurende deze cybersecurity opleiding wordt in de basisfase de basis gelegd voor programmeren, databases en SQL, operating systems en netwerken. In de verdiepingsfase verwerft de cursist in werkcolleges en met praktijkopdrachten, fundamentele kennis en -vaardigheden over een diversiteit van cybersecurity onderwerpen. https://it-omscholing.nl/programmas/cybersecurity/

5	re_B00TCMP	Landelijk	Een event speciaal voor jongeren met interesse én skills op het gebied van IT. Tijdens de re_B00TCMP krijgen zij meer inzicht in het werken binnen de IT-industrie. Dit door verschillende sessies met de cyber securitybranche, de politie en de gaming sector. Daarnaast leren zij meer over online grenzen en de impact van cybercrime. Jongeren met IT-interesse in de leeftijd tussen 12 en 25 krijgen op deze dag middels interactieve workshops inzicht in de kansen en risico's van hun uitzonderlijke cybertalenten. https://re-b00tcmp.nl/
6	International Cyber Security Summer School	Landelijk	Elk jaar in augustus organiseert HSD in samenwerking met de NCI Agency, Europol, Universiteit Leiden, en verschillende HSD partners, de International Cyber Security Summer School (ICSSS). Een meerdaags evenement met één belangrijk doel: aanstormend talent voor cybersecurity voorbereiden op een mooie carrière. Deelnemers zijn studenten (PhD, Master) en starters/young professionals. Het programma biedt uiteenlopende zaken zoals interessante colleges van topexperts, perspectieven van professionals uit het werkveld, groepsopdrachten en leuke sociale activiteiten zoals het bezoeken van bedrijven en het doen van excursies. www.summerschoolcybersecurity.org

Tabel 12: (Om)scholings- en (zij)instroom initiatieven specifiek gericht op cybersecurity

3.6.2 In- en uitstroom

Er zijn geen kwantitatieve gegevens over bereik/aantal deelnemers beschikbaar die particulier onderwijs volgen.
Enkele kwalitatieve beelden van de opleiders:

- Deelnemers: veelal 35 jaar en ouder;
- Veel vraag naar scholing gericht op het behalen van specifieke cybersecurity–certificaten;
- Afname in vraag naar scholing op gebied van privacy, toename in de vraag naar simulaties (met een groep iets hacken);
- Hybride leervormen worden steeds gewilder;
- Klanten: met name overheid, banken, telecom.

Om verder een beeld bij de belangstelling voor (om)scholen te krijgen is het UWV benaderd met de vraag hoeveel mensen een STAP-budget hebben aangevraagd voor scholing op het gebied van cybersecurity. Helaas beschikt het UWV nog niet over de functionaliteit om dit soort selecties uit het databestand van deelnemers en gevolgde scholingen te maken. Dit was wel een wens, maar gezien het stopzetten van de STAP regeling gaat de ontwikkeling hiervan niet door.

Het aantal deelnemers aan de regionale (mkb)-initiatieven is bij de onderzoekers niet bekend en lastig te achterhalen.

3.6.3 Welke expertise?

Waar wordt vooral voor opgeleid binnen het niet-bekostigd onderwijs?
Omdat certificaten een belangrijke rol spelen binnen het LLO op het gebied van cybersecurity is hierop ingezoomd. Wat zijn de certificaten waar de meeste vraag naar is vanuit de arbeidsmarkt en hoe wordt hierop ingespeeld door de opleidingsmarkt?

We hebben deze vraag op twee manieren benaderd:

- Ten eerste is via Chat GPT-zoekopdrachten en de vraag- en antwoordfunctie van website Tweakers vastgesteld welke certificaten het meest gevraagd worden. Dit heeft een lijst van 22 certificaten opgeleverd. Vervolgens is gekeken naar hoe vaak opleidingen voorkomen in leeroverzicht.nl die voor deze op cybersecurity certificaten opleiden. Om deze informatie enigszins op dezelfde noemer te brengen als die van het bekostigde onderwijs zijn ook de certificaten gescoord op de typen competenties die vanuit de arbeidsmarkt worden gevraagd. In totaal zijn er 240 opleidingen binnen leeroverzicht.nl die aangeven op te leiden voor een van de meest gevraagde cybersecurity certificaten. Kijkend naar het aanbod in opleidingen voor certificaten gaat het bij 111 opleidingen om certificaten die een bredere scope hebben dan techniek/technologie, dus ook management èn organisatie èn legal (supplementaire tabel 15).
- Ten tweede is bij de vacatureanalyse gekeken naar welke certificaten hoe vaak worden gevraagd in vacatures.

De top drie blijkt dan CISSP, CISM en CISA te zijn. Ook als je kijkt naar de meest voorkomende functies en welke certificaten in de vacatures daarvoor worden gevraagd blijft deze top drie hetzelfde. En aanvullend is uitgezocht bij de meest voorkomende functies hoe vaak naar certificaten wordt gevraagd. Bijvoorbeeld blijkt voor de IT Security Officer en de Information Security Consultant bij 70 % van de vacatures naar certificaten gevraagd te worden. Andere functies zoals (cybersecurity-) consultant lijken juist minder certificaat-afhankelijk (supplementaire tabel 25).

3.6.4 Knelpunten in het LLO-domein

Vanuit de leden van de NRTO wordt het volgende signaal afgegeven: omscholen is nog te doen als je een welwillende werkgever achter je hebt maar is onbetaalbaar voor de individuele werknemer die dat niet heeft. Structurele voorzieningen zoals een systeem van individuele leerrechten ontbreken immers. Dit raakt met name private IT-opleiders die kansen bieden aan iedereen; vrouwen, werkeloze jongeren of mensen uit sociaal zwakkere milieus. Het stimuleren van private IT-opleiders die ook een maatschappelijke bijdrage leveren heeft als voordeel dat er een win-win situatie ontstaat en de diversiteit in de beroepsgroep van cybersecurity-specialisten toeneemt.

Daarnaast spelen ook hier de bekende knelpunten bij leven lang ontwikkelen als het combineren van een opleiding met privé-situatie en de voortdurende kosten voor levensonderhoud enerzijds en het vasthouden aan zekerheden en korte termijn denken anderzijds. Opleiders zien bovendien dat het volkrijgen van groepen voor een cybersecuritytraining en de deelname aan training na aanmelding problematisch is, omdat werknemers niet vrijgespeeld worden door hun werkgevers.
Deze knelpunten zijn natuurlijk niet uniek voor cybersecurity -opleidingen, maar speelt daar – ondanks de urgentie van het onderwerp – net zo goed. Cyber-security-opleidingen rondom certificaten zouden volgens private opleiders daarom goed kunnen dienen als pilot voor het stimuleren van leercultuur of toekennen van leerrechten. Daarmee verbind je immers maatschappelijk nut aan kansen voor mensen om zich verder te ontwikkelen.

3.7 Conclusies en knelpunten onderwijsaanbod

Concluderend zien we per type onderwijs het volgende:

Mbo

- Binnen het mbo is er steeds meer specifieke aandacht voor cybersecurity in ICT-opleidingen afgaande op de aanvullingen in de kwalificatiedossiers;
- De mbo ICT-opleidingen focussen vooral op de technische aspecten van cybersecurity;
- Het aantal ICT –studenten blijft de afgelopen jaren ongeveer op hetzelfde niveau, met een lichte daling van studenten in de opleiding ICT system engineer niveau 4 die juist van alle mbo-opleidingen het meest aansluit bij de cybersecurity loopbaan;
- Bij een aantal mbo-instellingen is duidelijk ambitie en visie aanwezig om hun ICT -studenten voor te bereiden op cybersecurity functies;
- Binnen het domein Zakelijke Dienstverlening vinden momenteel pilots plaats met cybersecurity in de vorm van een keuzedeel en een kopopleiding voor de opleiding beveiliging; de vraag is natuurlijk of deze toekomstige beroepsbeoefenaren als cybersecurity specialisten beschouwd kunnen worden;
- ICT-opleidingen melden als knelpunten bij het realiseren van actueel onderwijs op het gebied van cybersecurity een tekort aan docenten, het up-to-date krijgen van zittende docenten en ontoereikende faciliteiten. Een uitdaging is ook hoe nieuwe thema's (waaronder o.a. AI) te laten landen in het onderwijs.

Hoger onderwijs

- Binnen de NVAO-geaccrediteerde opleidingen zijn 10 studies geïdentificeerd die volledig in het teken staan van cybersecurity, 29 studies die een specialisatie-/keuzerichting cybersecurity aanbieden en 13 studies die een verplicht onderdeel cybersecurity in hun programma hebben geïntegreerd (groter dan 6 ECTS).
- De uitstroom aan studenten neemt jaarlijks geleidelijk toe, met name bij studies die volledig in het teken staan van cybersecurity danwel een specialisatie-/keuzerichting cybersecurity.
- De hoger onderwijs-opleidingen lijken meer multidisciplinair ingestoken. De competentie onderwijs is in alle studies echter sterk ondervertegenwoordigd tot afwezig.
- Belangrijke knelpunten binnen het hoger onderwijs zijn een tekort aan docenten met voldoende kennis, de inhoud van het curriculum waarin zowel een breed profiel als specialistische profilering binnen het cyberdomein dienen te worden aangeboden, de snelheid waarin de security wereld zich ontwikkelt in combinatie met het gebrek aan vermogen om hier flexibel op te reageren, en de beeldvorming rondom cybersecurity onderwijs als technische studie die invloed heeft op de werving en het verwachtingsmanagement van (potentiële) studenten en het gebrek aan middelen.
- Er zijn 12 studies (waaronder drie mbo-initiatieven) aan het licht gekomen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn.

LLO

- Er is veel particulier aanbod, veruit de grootste speler met opleidingen met cybersecurityelementen is Global Network Netherlands.
- Een substantieel deel van de opleidingen leidt op voor het behalen van relevante certificaten voor cybersecurity.
- Particuliere opleiders zien bij werving en deelname nog veel belemmeringen voor mensen die zich willen laten om-bij en nascholen in cybersecurity.
- Veel en diverse initiatieven (publiek-privaat) zijn gericht op mkb en burgers. Dit illustreert wellicht het punt uit de HCA HSD 2030: er is een gebrek aan structuur en overzicht wat het aanbod voor formeel en non-formeel leren op het gebied van (cyber) security betreft;
- De opleidingen die door ho- en mbo-instellingen als niet-initieel onderwijs worden aangeboden leiden veelal voor de reguliere diploma's op. Hier valt mogelijk nog wat te winnen door in te spelen op een andere aanbeveling uit de HCA HSD: zorg voor kortere modules en trainingen die geschikt zijn voor mensen die werken; zij vormen immers de grootste talentenpool voor cybersecurity. De vraag is danwel hoe deze kwalificaties aansluiten bij de vraag vanuit de arbeidsmarkt waar in veel vacatures naar specifieke certificaten wordt gevraagd.

4. Resultaten arbeidsmarkt

Onderzoeksvraag 5.
Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) hoe groot de vraag naar cybersecurity experts is, en welke expertise gevraagd wordt. Doe dit op basis van:

- *Een overzicht van de openstaande vacatures bij Nederlandse organisaties waar cybersecurity professionals in dienst (gaan) zijn*
- *Een overzicht van het soort cybersecurity expertise dat gevraagd wordt;*
- *Inzicht in de sectorale en regionale verdeling van de vraag naar cybersecurity expertise binnen Nederland: waar komt de vraag vandaan?*

De vraag naar cybersecurity expertise groeit, zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt. We schatten in dat er circa 60.000-110.000 cybersecurity professionals op de arbeidsmarkt actief zijn, waarvan 17.000-33.000 professionals met een specialistisch cybersecurityprofiel. De vraag naar cybersecurity expertise is geconcentreerd in de provincies Noord-Holland, Zuid-Holland, Utrecht, en het zwaartepunt in de vraag ligt bij medior- en senior-functies waarvoor een hbo- of wo-opleidingsniveau gevraagd wordt. De overheid en de IT-sector zijn de twee sectoren met de meeste vraag naar cybersecurity expertise. Daarnaast hebben organisaties die relatief meer doen met cybersecurity ook meer vraag naar specialistische profielen. De vraag naar cybersecurity professionals is onder andere afhankelijk van de rol die partijen hebben in de 'cybersecurity waardeketen'. Zo heeft de cybersecuritysector zelf (de productie van cybersecuritygoederen en -diensten) een grote vraag naar specialistische cybersecurity profielen, wordt er in de Cyber R&D logischerwijs veel naar Cyber Researchers gevraagd.
Over de linie is er relatief veel technische kennis vereist om actief te zijn binnen de cybersecurity, maar de benodigde vaardigheden en uit te voeren taken zijn daarentegen voor een groot deel niet-technisch van aard. De samenstelling van kennis/vaardigheden/taken blijkt vrij stabiel naarmate de functies meer werkervaring vereisen. Dit impliceert dat met name de concrete invulling van deze bouwstenen en de mate waarin personen in staat zijn deze kwalitatief invulling te geven groeit naarmate men zich verder ontwikkelt. Afsluitend zien we dat er in 15% van de vacatures expliciet wordt gevraagd naar een cybersecurity certificaat. De meest gevraagde certificaten zijn de CISSP, CISM, en CISA.

Onderzoeksvraag 8.
Maak inzichtelijk (waar mogelijk cijfermatig onderbouwd) wat de uitstroom is van cybersecurity expertise uit de Nederlandse arbeidsmarkt en waar dit door komt.

De populatie cybersecurity professionals is relatief jong, met circa driekwart van de populatie jonger dan 50 jaar. In 2021 verliet een kwart van de cybersecurity professionals de cybersecuritysector, waarvan driekwart een baan vond bij een bedrijf buiten de onderzoekspopulatie. Pensioen en emigratie zijn slechts voor 4% van de uitstromers de reden van uitstromen. Naar verwachting zal er komende jaren relatief weinig vervangingsvraag vanwege pensioen zijn.

4.1 Inleiding

Cybersecurity is een multidisciplinair vakgebied en kent vele facetten. Het is dan ook niet triviaal om de 'cybersecurity arbeidsmarkt' goed in beeld te brengen. Verschillende partijen hebben de afgelopen jaren inspanningen geleverd om grip op deze arbeidsmarkt te krijgen.

Volgens de publicatie 'ICT in beeld' van het UWV[10] werden er 4.100 cybersecurity vacatures in 2022 uitgezet (security specialist ICT / adviseur ICT-beveiliging). Op pr-eDICT.nl wordt voor het jaar 2022 gesproken over 4.738 cybersecurity vacatures en 11.071 ICT-vacatures waarin gevraagd wordt om minimaal één cybersecurity vaardigheid.

In termen van het aantal werkzame cybersecurity professionals komt het UWV o.b.v. cijfers van CBS op 13.000 securityspecialisten ICT / adviseurs ICT-beveiliging. In de Human Capital Agenda van de HSD schat men in dat in 2021 0,4% van de beroepsbevolking cybersecurity professional is, wat overeenkomt met ~39.000 professionals.

Zoals al snel duidelijk wordt is het bij dergelijke cijfers cruciaal welke afbakening en definitie van 'cybersecurity professional' gehanteerd wordt. In veel onderzoeken lijkt cybersecurity in een redelijk nauwe (en veelal technische) zin benaderd te worden, terwijl gesprekspartners in het veld juist wijzen op de breedte en multidisciplinariteit van het thema.

In dit onderzoek wordt verdiepend inzicht verkregen over de vraag naar cybersecurity expertise op de arbeidsmarkt. Wat wordt er precies gevraagd en door wie? De onderzoeksbasis hiervoor is een uitgebreide vacature-analyse, een online enquête onder leden van Cyberveilig Nederland, en georganiseerde workshops.

Dit hoofdstuk is als volgt opgebouwd:

- In 4.2 zal het conceptueel kader gepresenteerd worden waarmee er binnen dit onderzoek naar de begrippen 'cybersecurity professional' en 'cybersecurity expertise' gekeken wordt.
- In 4.3 wordt de vraag naar cybersecurity professionals in algemene zin besproken. Om hoeveel vacatures gaat het en hoe zijn deze onderverdeeld naar zaken als gevraagd opleidingsniveau, werkervaring, regio, sector en doelgroep.
- In 4.4 wordt de vraag naar specifieke functieprofielen besproken. Daarbij wordt er onderscheid gemaakt naar functieprofielen met een grote en kleine component 'cyber'.
- In 4.5 wordt de vraag naar specifieke kennis en vaardigheden besproken. Hier wordt een niveau dieper dan 'functieprofiel' gekeken door te kijken naar welke individuele 'bouwstenen' ten aanzien van taken, kennis en vaardigheden gevraagd worden binnen vacatures op de arbeidsmarkt.
- In 4.6 worden de 'uitstroom' en 'instroom' van cybersecurity professionals besproken. Hier wordt onder andere gekeken naar de uitstroom vanwege pensioen en emigratie en de instroom vanwege immigratie.
- In 4.7 worden relevante ontwikkelingen voor de toekomstige vraag naar cybersecurity professionals besproken. Hier komen onder andere zaken zoals de NIS2, CRA en de inzet van AI aan bod.
- In 4.8 wordt afgesloten met de voornaamste conclusies die we kunnen verbinden aan de resultaten binnen dit onderzoek.

4.2 Conceptueel kader

4.2.1 Cybersecurity expertise

Cybersecurity is een breed concept. Het gaat om digitale veiligheid in de brede zin van het woord, waar onderwerpen als techniek, wet- en regelgeving, bestuur en organisatie allemaal een rol spelen. De breedte van het concept 'cybersecurity' wordt logischerwijs ook weerspiegeld in de expertise die professionals (moeten) hebben om werkzaam te zijn op dit gebied. Wanneer we naar cybersecurity expertise op de arbeidsmarkt kijken, kunnen we het op verschillende 'aggregatieniveaus' benaderen. Het meest directe en duidelijke aggregatieniveau is het niveau van functietitels- en profielen. Binnen dit onderzoek is het ECSF van ENISA als basis genomen voor twaalf relevante (doch illustratieve) cybersecurity profielen.

Cyberexpertise laat zich niet vangen in enkele functies, maar kan onderdeel zijn van een grote variëteit aan beroepen op de arbeidsmarkt. Het is derhalve ook relevant om niet enkel naar functieprofielen te kijken, maar op een aggregatieniveau 'lager' ook te kijken naar individuele taken, kennis en vaardigheden. Relevante taken, kennis en vaardigheden op het gebied van cybersecurity zijn in dit onderzoek geïdentificeerd aan de hand van hetzelfde ECSF. De twaalf genoemde functies zijn gedetailleerd beschreven en opgebouwd aan de hand van 'Deliverables', 'Main task(s)', 'Key skills' en 'Key knowledge'. Zie ook 4.2.1 voor meer toelichting.

Hoewel de twaalf profielen op zichzelf geenszins dekkend zijn voor de cybersecurity arbeidsmarkt in brede zin, verwachten wij als onderzoekers wel dat de onderliggende 384 bouwstenen (deliverables, taken, kennis en vaardigheden) wel een vrij compleet beeld schetsen van wat er onder cybersecurity expertise verstaan kan worden. In dit onderzoek kijken we

10. Bron: UWV, augustus 2023, op basis van cijfers van het CBS. https://www.werk.nl/imagesdxa/factsheet_ict_tcm95-451428.pdf

dus naar cyberexpertise op het niveau van profielen, maar onderzoeken we ook de vraag naar individuele bouwstenen. Deze individuele bouwstenen kunnen we vervolgens aantreffen in de 12 (illustratieve) ECSF-profielen, maar we kunnen hen ook aantreffen in andere functieprofielen. In dit onderzoek is er dus aandacht voor beroepen waarin cybersecurity expertise de hoofdmoot vertegenwoordigt, maar wordt er ook gekeken naar beroepen waarin cybersecurity expertise wel degelijk een rol speelt en tegelijkertijd niet per se de hoofdmoot vertegenwoordigt.

4.2.2. Doelgroepen

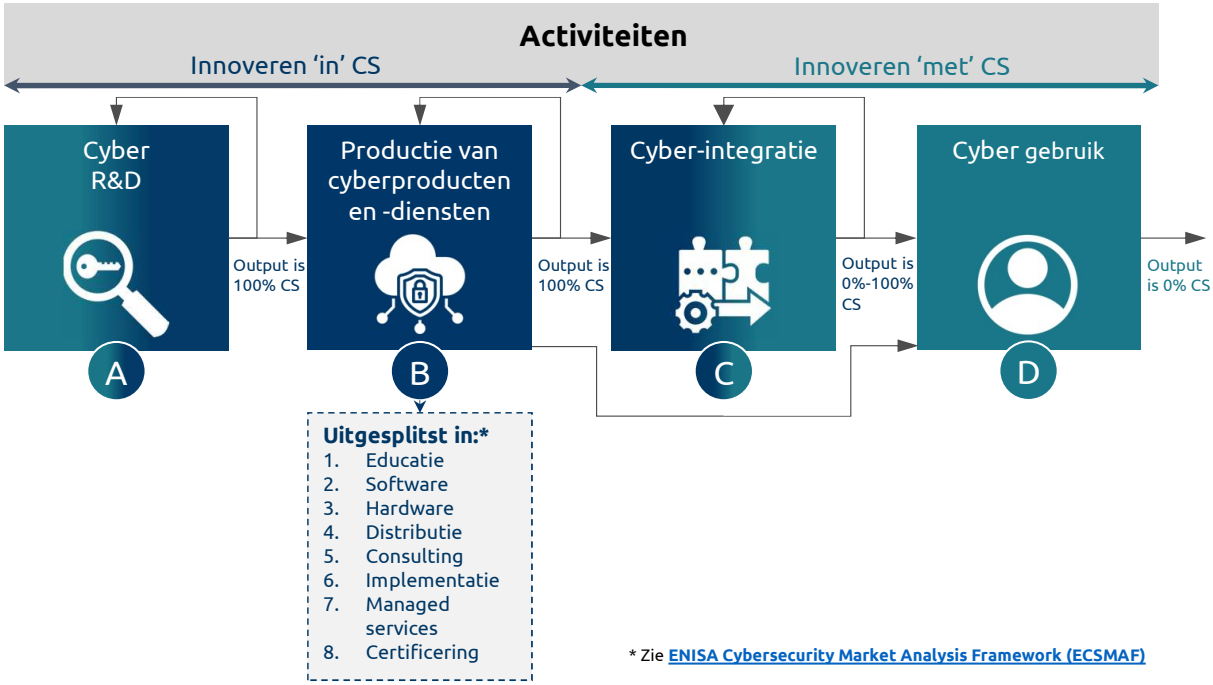
In dit onderzoek zijn we niet enkel geïnteresseerd in wat voor typen expertise gevraagd worden in wat voor functieprofielen, maar zijn we ook geïnteresseerd in **wie welke behoefte aan cybersecurity expertise** heeft. Er zijn immers grote verschillen tussen organisaties in termen van doel- en taakstelling, activiteiten en de rol die cybersecurity speelt. Allereerst wordt gekeken naar de driedeling bedrijfsleven, overheid en kennis-/onderwijsinstellingen. Dit geeft meer inzicht in welke context er gevraagd wordt om cybersecurity expertise. Daarnaast wordt er ook gekeken naar de rollen die partijen vertegenwoordigen in de 'waardeketen' van cybersecurity. Hiervoor wordt gebruik gemaakt van het eerdere onderzoek voor het ministerie van Economische Zaken en Klimaat aangaande 'De economische kansen van de cybersecuritysector'.[11] Hierin is een kader gepresenteerd waarin vier categorieën onderscheiden worden (figuur 12):

A. **Cyber R&D**. Dit zijn de R&D-activiteiten specifiek op het gebied van cybersecurity. Deze resultaten kunnen doorgaans door de cybersecuritysector gebruikt worden om producten (goederen/diensten) te ontwikkelen en/ of te verbeteren.

B. **Productie van cyberproducten en –diensten**. Hier gaat het om de (economische) activiteiten waarbij cyberproducten/-diensten ontwikkeld worden, waarbij te stellen is dat de output 100% cybersecurity gerelateerd is. Binnen deze categorie heeft ENISA acht subcategorieën onderscheiden, o.a. hardware, consulting en managed services.

C. **Cyber-integratie**. Hier gaat het om (economische) activiteiten waarbij cybersecurity geïntegreerd wordt in 'breder' product. Voorbeelden zijn betaaldiensten die cybersecure moeten werken, remsystemen van voertuigen die niet gehackt moeten kunnen worden, of huishoudelijke apparaten die digitaal beschermd moeten worden. De output in deze categorie is daarmee deels cybersecurity gerelateerd en deels niet.

D. **Cyber-eindgebruik**. Tot slot geeft de categorie cyber-eindgebruik alle (economische) activiteiten weer waarbij 'cybersecurity producten' (100% cyber of geïntegreerd in andere producten) wel gebruikt worden, maar waarbij de output geen cyberelement meer bevat. Denk bijvoorbeeld aan een bakker die wel een veilig betaalsysteem inkoopt en gebruikt, maar zelf brood produceert.



Figuur 12: De cybersecuritysector en haar waardeketen. Bron: Dialogic (2023), De economische kansen van de cybersecuritysector

11. Dialogic (2023), De economische kansen van de cybersecuritysector. Te vinden op: https://www.rijksoverheid.nl/documenten/rapporten/2023/04/06/de-economische-kansen-van-de-cybersecuritysector

Merk op dat individuele organisaties meerdere rollen kunnen vervullen. Zo kan een bedrijf bijvoorbeeld cyberproducten maken en tegelijkertijd ook als eindgebruiker optreden. In feite kunnen vrijwel alle organisaties vandaag de dag als eindgebruikers gezien worden, omdat cybersecurity voor vrijwel iedere organisatie van belang is. De rollen rondom cyber R&D, productie en integratie zijn echter bij een selectievere groep organisaties belegd. Bij aanvang van dit onderzoek was de inschatting dat de rollen die partijen vervullen ook samenhangen met het type cybersecurity expertise waar zij naar op zoek zijn.
Tot slot is er ook expliciet aandacht voor partijen die relatief veel cybersecurity expertise vragen op de arbeidsmarkt (i.e. veel vacatures uitzetten waarin cybersecurity expertise een rol speelt) versus partijen die relatief weinig cybersecurity expertise vragen. De dynamiek rondom dit thema is naar verwachting verschillend tussen deze organisaties, en de verwachting vooraf was dat organisaties die enkel als 'cybersecurity eindgebruiker' optreden ook minder vraag en een andere vraag hebben.

4.3 Vraag naar cybersecurity professionals – algemeen

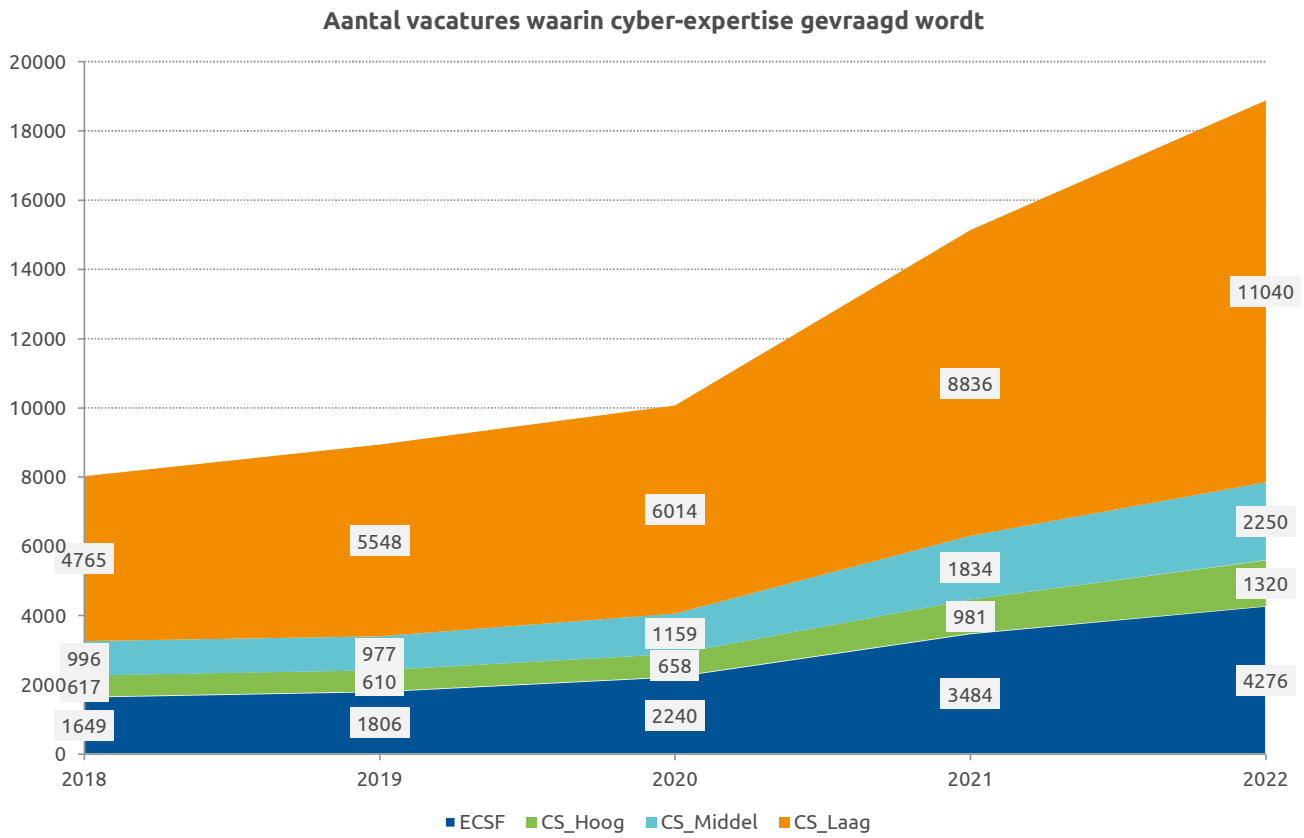
4.3.1 Totaal

In 4.2 is benoemd dat cybersecurity expertise op verschillende manieren terug kan komen op de arbeidsmarkt. Er zijn functies die men als 'cybersecurity functie' zou kunnen bestempelen, maar er zijn ook velerlei functies waarin cybersecurity in meer of mindere mate een onderdeel is van een breder takenpakket. Voor de analyses die hier gepresenteerd worden is dan ook operationeel onderscheid gemaakt tussen deze verschillende manifestatievormen. De in de vacatures gevonden functies zijn gekoppeld aan één van de volgende vier categorieën[12]:

- **ECSF**: dit zijn functieprofielen die (grotendeels) overeenkomen met de functieprofielen zoals benoemd in het ECSF. Personen die een dergelijke functie bekleden worden gezien als cybersecurity professional.
- **Cybersecurity – hoog**: dit zijn functieprofielen die primair op cybersecurity gericht zijn, maar die niet direct aan een ECSF-profiel gekoppeld zijn. Personen die een dergelijke functie bekleden worden ook gezien als cybersecurity professional.
- **Cybersecurity – middel**: dit zijn functieprofielen die een bredere scope hebben dan enkel cybersecurity, maar die wel een substantiële component cybersecurity bevatten. Personen die een dergelijke functie bekleden zien we in dit onderzoek niet als (pure) cybersecurity professional, maar dienen wel (substantiële) kennis over cybersecurity te hebben.
- **Cybersecurity – laag**: dit zijn functieprofielen waarbij cybersecurity weliswaar een rol speelt, maar enkel op een marginale wijze. De personen die een dergelijke functie bekleden worden niet gezien als cybersecurity professional, maar hebben wel op enige wijze te maken met het thema.

Het aantal vacatures waarin gevraagd wordt om cybersecurity expertise is in de laatste jaren flink gestegen van circa 8.000 in 2018 tot circa 19.000 in 2022. Alle vier beschreven categorieën kennen een forse groei in de vraag, zie figuur 13.

12. Zie bijlage voor meer toelichting op de methodologische keuzes en verantwoording



Figuur 13: Aantal vacatures waarin gevraagd om cybersecurity expertise. Bron: Jobdigger, bewerking Dialogic

Door het onderscheid naar verschillende typen profielen te maken wordt ook snel duidelijk wat de impact is van het hanteren van verschillende definities. Zo hebben het CBS en pr-eDICT bij de meeste cijfers een vrij nauwe benadering van het begrip cybersecurity professional genomen, waardoor zij op circa 4.000 vacatures uitkomen in 2022. Binnen dit onderzoek is er een bredere operationalisering van cybersecurity gebruikt, en komen we tot 4.200 – 18.900 vacatures afhankelijk van de gekozen benadering. Wij zouden niet aanraden om de categorie 'Cybersecurity – laag' mee te tellen als cybersecurity professionals, maar de categorie geeft wel goed aan hoe cybersecurity een brede weerslag vindt op de arbeidsmarkt. Het zijn immers niet enkel de pure cybersecurity professionals die ermee te maken hebben.
Er zijn volgens deze cijfers in 2022 dus ~5.600 vacatures voor cybersecurity professionals en nog eens ~2.250 vacatures waarin cybersecurity een substantiële rol speelt (~7.850 in totaal).
Bij de cijfers van 'ICT in beeld' van het UWV zijn er 3,17 keer meer professionals actief dan het aantal vacatures dat gerapporteerd wordt; op pr-eDICT zijn er in het geval van ICT-professionals 5,81 keer meer professionals actief op de arbeidsmarkt dan het aantal vacatures. Zouden we voor cybersecurity professionals met deze kentallen werken, dan komen we op basis van deze vacatureanalyse tot een schatting van een totaal aantal cybersecurityprofessionals op de arbeidsmarkt van 60.000-110.000 mensen (figuur 14).

	Laag	**Hoog**
	3,17	5,81

		CS-professionals	
Type CS-profiel	Vacatures	Laag	Hoog
ECSF	4276	13555	24844
CS - Hoog	1320	4184	7669
CS - Middel	2250	7133	13073
CS - Laag	11040	34997	64142
Totaal	**18886**	**59869**	**109728**

Figuur 14: Schatting totaal aantal cybersecurity professionals op de arbeidsmarkt. Bron: Jobdigger, bewerking Dialogic

4.3.2 Regio

De vraag is niet homogeen verdeeld over de verschillende provincies in Nederland. Het gros van de vacatures (71%) richt zich op de Randstad: Noord-Holland, Zuid-Holland en Utrecht, zie figuur 15. Dit geldt voor zowel de vacatures in generieke zin als voor de vier afzonderlijke categorieën.

	ECSF	CS_Hoog	CS_Middel	CS_Laag	Totaal
Noord-Holland	3683	1271	2095	9752	16801
Zuid-Holland	3357	1189	1790	9148	15484
Utrecht	2372	811	1549	6392	11124
Noord-Brabant	1510	337	685	3550	6082
Gelderland	1001	208	413	2313	3935
Overijssel	615	91	195	1921	2822
Limburg	334	104	163	1021	1622
Groningen	230	47	132	727	1136
Flevoland	123	30	66	392	611
Friesland	70	42	50	449	611
Drenthe	77	40	58	294	469
Zeeland	80	14	18	209	321
Onbekend	3	3	2	35	43
Totaal	13455	4187	7216	36203	61061

Figuur 15: Aantal vacatures naar regio[13]. Bron: Jobdigger, bewerking Dialogic

4.3.3 Opleidingsniveau en werkervaring

In de cybervacatures wordt grotendeels gevraagd naar een hbo- of wo-opleidingsniveau. Over alle vacatures gaat het om 91% waarin hbo of wo gevraagd wordt, tot zelfs 98% in de categorie 'Cybersecurity – hoog'. Dit komt overeen met het in de gesprekken geschetste beeld dat het met name gaat om functies waar een hoog opleidingsniveau voor vereist is. Daarnaast wordt er vaak gevraagd om meerdere jaren werkervaring. Voor zover het binnen de data bekend is, lijkt er een zwaartepunt bij 3+ jaar werkervaring te zijn, zie ook figuur 16.

Totaal				
	WO	HBO	MBO	Totaal
onbekend	6665	25017	3918	**35600**
starter	260	955	191	**1406**
1-3	1048	4276	813	**6137**
3-5	1382	6466	543	**8391**
5-10	1682	6127	283	**8092**
>10	370	902	38	**1310**
Totaal	**11407**	**43743**	**5786**	**60936**
	19%	72%	9%	100%

ECSF				
	WO	HBO	MBO	Totaal
onbekend	1132	5813	422	**7367**
starter	31	191	14	**236**
1-3	198	906	73	**1177**
3-5	253	1895	99	**2247**
5-10	333	1803	46	**2182**
>10	46	196	2	**244**
Totaal	**1993**	**10804**	**656**	**13453**
	15%	80%	5%	100%

CS_Hoog				
	WO	HBO	MBO	Totaal
onbekend	536	1794	49	**2379**
starter	22	92	2	**116**
1-3	118	300	13	**431**
3-5	158	473	8	**639**
5-10	143	357	8	**508**
>10	40	65	1	**106**
Totaal	**1017**	**3081**	**81**	**4179**
	24%	74%	2%	100%

13. De provincie waarin de vacature wordt uitgezet is automatisch gededuceerd. Voor enkele vacatures kon de provincie niet gededuceerd worden, deze zijn daarom als onbekend weergegeven.

CS_Middel				
	WO	HBO	MBO	Totaal
onbekend	853	3067	237	**4157**
starter	47	120	12	**179**
1-3	117	565	63	**745**
3-5	183	678	38	**899**
5-10	262	812	17	**1091**
>10	45	87	2	**134**
Totaal	**1507**	**5329**	**369**	**7205**
	21%	74%	5%	100%

CS_Laag				
	WO	HBO	MBO	Totaal
onbekend	4144	14343	3210	**21697**
starter	160	552	163	**875**
1-3	615	2505	664	**3784**
3-5	788	3420	398	**4606**
5-10	944	3155	212	**4311**
>10	239	554	33	**826**
Totaal	**6890**	**24529**	**4680**	**36099**
	19%	68%	13%	100%

Figuur 16: Aantal vacatures naar opleidingsniveau en werkervaring. Bron: Jobdigger, bewerking Dialogic

Op basis van de vacaturedata is ook een inschatting gemaakt van het type functie in termen van junior, medior of senior.[14] Hieruit blijkt dat, voor zover bekend, circa driekwart van de vacatures betrekking heeft op medior- en seniorfuncties. Slechts een kwart heeft betrekking op juniorfuncties, waarbij vaak ook al enige werkervaring gevraagd wordt (figuur 17).

Totaal				
	WO	HBO	MBO	Totaal
onbekend	1847	8633	1793	**12273**
junior	2511	9244	1644	**13399**
medior	4446	17811	1533	**23790**
senior	2603	8055	816	**11474**
Totaal	**11407**	**43743**	**5786**	**60936**
	19%	72%	9%	100%

Figuur 17: Vacatures naar junior-, medior- en seniorniveau. Bron: Jobdigger, bewerking Dialogic

Er wordt vaak gesproken over 'de mismatch tussen onderwijs en arbeidsmarkt'. Als we eerlijk kijken naar de dynamiek op de arbeidsmarkt, dan zouden we moeten spreken over de eventuele mismatch tussen het onderwijs en de arbeidsmarkt voor juniorfuncties. Het is, uitzonderingen daargelaten, immers niet realistisch om vanuit de collegebanken rechtstreeks een medior- of seniorfunctie in te stromen. Het is wel realistisch om vanuit de collegebanken een juniorpositie in te stromen.

Aanvullend zijn de bovenstaande cijfers uitgesplitst naar jaar. Deze zijn opgenomen in supplementaire tabel 17 in Bijlage 3. In 2022 zijn er 4.364 vacatures die op junioren gericht zijn. Daarvan zijn er 1.256 gekoppeld aan specialistisch cybersecurityprofiel (ECSF en 'CS – Hoog'), 537 aan profielen met een substantiële cybersecurity component ('CS – middel') en 2.571 aan profielen met een kleine cybersecurity component ('CS – Laag'). Voor het bestuderen van de koppeling tussen regulier onderwijs en arbeidsmarkt is het wellicht logischer om naar deze vraag vanuit de arbeidsmarkt te kijken. Gaat het om doorstroom en ontwikkeling op de arbeidsmarkt, na- en bijscholing, en Leven Lang Ontwikkelen (LLO), dan is het met name zinvol om ook naar de medior- en seniorposities te kijken. Merk op dat de aantallen voor junior-, medior- en senior-functies onderschattingen zullen zijn, omdat er nog een groep 'onbekend' is die in de praktijk wel in één van deze categorieën zal moeten vallen.

14. Dit is een label dat dataleverancier Jobdigger toekent op basis van de beschikbare informatie.

4.3.4 Sector

De meeste vacatures zien we terug in de sectoren overheid, IT en zakelijke dienstverlening en advies. In figuur 18 is de top 10 weergegeven.

#	SBI-2	Sector_naam	2018	2019	2020	2021	2022	Totaal
1	84	Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	857	1152	1503	1743	2570	7825
2	62	Dienstverlenende activiteiten op het gebied van informatietechnologie	927	1054	1409	1541	2196	7127
3	69	Rechtskundige dienstverlening, accountancy, belastingadvisering en administratie	550	621	544	1240	1658	4613
4	70	Holdings (geen financiële), concerndiensten binnen eigen concern en managementadvisering	795	792	593	973	1079	4232
5	46	Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	425	490	732	1337	805	3789
6	64	Financiële instellingen (geen verzekeringen en pensioenfondsen)	489	628	513	776	1040	3446
7	85	Onderwijs	344	351	385	572	716	2368
8	80	Beveiliging en opsporing	197	327	372	524	463	1883
9	86	Gezondheidszorg	312	318	285	461	475	1851
10	78	Arbeidsbemiddeling, uitzendbureaus en personeelsbeheer	95	121	211	613	603	1643

Figuur 18: top 10 sectoren met cybervacatures. Bron: Jobdigger, bewerking Dialogic

Wanneer we onderscheid maken naar het aandeel van cybersecurity in het profiel en de bijbehorende vier categorieën, dan valt op dat de IT-sector eruit springt als het gaat om specifiek de vraag naar ECSF-profielen (figuur 19).

#	SBI-2	Sector_naam	ECSF	CS_Hoog	CS_Middel	CS_Laag	Totaal
1	84	Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen	1178	845	1082	4720	7825
2	62	Dienstverlenende activiteiten op het gebied van informatietechnologie	1895	308	788	4136	7127
3	69	Rechtskundige dienstverlening, accountancy, belastingadvisering en administratie	792	645	797	2379	4613
4	70	Holdings (geen financiële), concerndiensten binnen eigen concern en managementadvisering	776	412	583	2461	4232
5	46	Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)	717	208	352	2512	3789
6	64	Financiële instellingen (geen verzekeringen en pensioenfondsen)	913	163	419	1951	3446
7	85	Onderwijs	493	201	234	1440	2368
8	80	Beveiliging en opsporing	354	168	312	1049	1883
9	86	Gezondheidszorg	371	133	199	1148	1851
10	78	Arbeidsbemiddeling, uitzendbureaus en personeelsbeheer	204	70	125	1244	1643

Figuur 19: Top 10 sectoren met cybervacatures, uitgesplitst naar categorie. Bron: Jobdigger, bewerking Dialogic

4.3.5 Organisaties

In de vacaturedata zijn circa 6.200 organisaties in Nederland aangetroffen die minimaal één cybervacature hebben uitgezet in de periode 2018-2022. De top 100 organisaties zijn daarbij goed voor 42% van de vacatures, wat betekent dat de arbeidsmarkt voor cybersecurity professionals afgelopen jaren vrij geconcentreerd was. Figuur 20[15] geeft de top 50 weer.

15. Bij het maken van dit figuur is geaggregeerd naar de naam van de organisatie die de vacature uit heeft gezet. Daardoor komen zowel Ministerie van Defensie en Rijksoverheid voor in de tabel.

#	Organisatie	2018	2019	2020	2021	2022	Totaal CS vacatures	Δ 2019-2022
1	Politie	119	425	484	314	717	2059	48%
2	PWC	105	88	87	355	623	1258	616%
3	CGI	9	146	250	267	530	1202	112%
4	EY	63	125	99	329	476	1092	381%
5	Belastingdienst	47	134	197	238	319	935	62%
6	ING	119	174	126	195	244	858	94%
7	ABN AMRO	141	113	120	164	232	770	93%
8	Capgemini	77	62	49	223	166	577	239%
9	KPMG	77	94	56	115	234	576	318%
10	Ministerie van Defensie	91	28	158	103	182	562	15%
11	Philips	11	13	149	149	143	465	-4%
12	Rohde & Schwarz Benelux			50	396		446	-100%
13	Rabobank	52	99	70	79	134	434	91%
14	Fox-IT	74	112	57	141	12	396	-79%
15	UWV	37	46	55	97	151	386	175%
16	Atos			24	47	314	385	1208%
17	Alliander	85	41	47	85	113	371	140%
18	ASML	43	44	81	81	105	354	30%
19	Stichting Cyber Security Academy The Hague	152	89	38	32	37	348	-3%
20	Thales Group	80	37	107	88	35	347	-67%
21	Macee	63	184	68	21	1	337	-99%
22	Rijkswaterstaat	39	45	55	81	105	325	91%
23	Irdeto	11	15	47	127	119	319	153%
24	Sogeti Nederland	49	123	56	15	52	295	-7%
25	De Nederlandsche Bank	44	58	45	71	76	294	69%
26	Thales Nederland	116	30	108	17	15	286	-86%
27	Accenture	39	11	17	99	119	285	600%
28	Rijksoverheid	48	45	1	62	125	281	12400%
29	TNO	55	25	25	82	91	278	264%
30	PwC Accountants	89	152	15			256	-100%
31	Deloitte Legal	48		103	103	1	255	-99%
32	Secura	31	19	72	83	46	251	-36%
33	NS	15	22	39	48	123	247	215%
34	Kader Group			1	62	170	233	16900%
35	Levy				75	151	226	
36	Gemeente Amsterdam	29	28	61	55	46	219	-25%
37	Openbaar Ministerie	36	33	25	47	72	213	188%
38	Modis		1	30	173	9	213	-70%
39	Deloitte	72	16	30	66	25	209	-17%
40	de Volksbank	26	29	39	57	53	204	36%
41	Witteveen+Bos Raadgevende ingenieurs	52	45	40	29	34	200	-15%
42	SAP Nederland	7		29	153	3	192	-90%
43	PLUSIT			7	91	93	191	1229%
44	DHL		29	33	41	81	184	145%
45	Mazars	5	33	18	31	94	181	422%
46	KPN	22	96	26	15	18	177	-31%
47	TM Software Europe	57	21	35	32	17	162	-51%
48	Orange Cyberdefense			51	56	50	157	-2%
49	Northwave	6	12	35	64	36	153	3%
50	Centric	32	17	41	37	25	152	-39%

Figuur 20: Top 50 organisaties - aantal cybervacatures. Bron: Jobdigger, bewerking Dialogic

In deze top 50 zijn zowel overheidspartijen te vinden (bijv. de Politie, de Belastingdienst, het Ministerie van Defensie als Rijksoverheid), partijen uit het bedrijfsleven (bijv. PWC, CGI, Fox-IT, ING en ASML) als een kennisinstelling (TNO). Hoewel al deze partijen veel vraag hebben naar cybersecurity expertise, kan het type profiel dat gezocht wordt verschillen, zie figuur 21.

#	Organisatie	ECSF	CS_Hoog	CS_Middel	CS_Laag	Totaal CS vacatures
1	Politie	291	228	369	1171	2059
2	PWC	190	208	266	594	1258
3	CGI	359	50	26	767	1202
4	EY	152	160	181	599	1092
5	Belastingdienst	149	52	118	616	935
6	ING	221	45	115	477	858
7	ABN AMRO	219	21	89	441	770
8	Capgemini	116	102	91	268	577
9	KPMG	93	90	70	323	576
10	Ministerie van Defensie	55	86	72	349	562
11	Philips	135	50	71	209	465
12	Rohde & Schwarz Benelux	24	1	34	387	446
13	Rabobank	105	22	62	245	434
14	Fox-IT	88	74	73	161	396
15	UWV	53	11	32	290	386
16	Atos	46	5	25	309	385
17	Alliander	132	15	44	180	371
18	ASML	171	9	32	142	354
19	Stichting Cyber Security Academy The Hague	123	43	55	127	348
20	Thales Group	87	5	21	234	347
21	Macee	80	16	29	212	337
22	Rijkswaterstaat	34	22	50	219	325
23	Irdeto	37	6	37	239	319
24	Sogeti Nederland	51	30	29	185	295
25	De Nederlandsche Bank	76	11	26	181	294
26	Thales Nederland	73	11	27	175	286
27	Accenture	95	41	45	104	285
28	Rijksoverheid	58	70	48	105	281
29	TNO	98	20	67	93	278
30	PwC Accountants	30	26	31	169	256
31	Deloitte Legal	26	49	38	142	255
32	Secura	114	8	45	84	251
33	NS	88	13	11	135	247
34	Kader Group	10	6	5	212	233
35	Levy	39	2	9	176	226
36	Gemeente Amsterdam	46	4	27	142	219
37	Openbaar Ministerie	7	15	24	167	213
38	Modis	2		2	209	213
39	Deloitte	39	30	43	97	209
40	de Volksbank	54	13	34	103	204
41	Witteveen+Bos Raadgevende ingenieurs	9	18	3	170	200
42	SAP Nederland	67	7	27	91	192
43	PLUSIT	46	15	16	114	191
44	DHL	10		2	172	184
45	Mazars	135		2	44	181
46	KPN	65	6	17	89	177
47	TM Software Europe	59	17	33	53	162
48	Orange Cyberdefense	46	47	31	33	157
49	Northwave	40	8	49	56	153
50	Centric	52	16	41	43	152

Figuur 21: Top 50 organisaties - aantal cybervacatures naar categorie. Bron: Jobdigger, bewerking Dialogic

Uit deze resultaten is op te maken dat de accenten sterk verschillen tussen organisaties. Zo hebben bijvoorbeeld CGI en ASML betrekkelijk veel vraag naar ECSF-profielen, terwijl partijen als het UWV en Atos cybersecurity meer in de periferie van bredere functies meenemen.

4.3.6 Doelgroepen

Zoals beschreven in 4.2.2 zijn we ook geïnteresseerd in wie vraag heeft naar cybersecurity expertise. Daarvoor kijken we naar de rollen van partijen in de waardeketen van cybersecurity, en kijken we of de partij toebehoort aan de overheid, het bedrijfsleven of onderwijs-/kennisinstellingen. Voor de top 100 organisaties is ingeschat tot welke categorie zij (primair) behoren. Dit geeft grofweg het volgende beeld (figuur 22):

Op basis van top 100 organisaties

Categorie	ECSF	CS_Hoog	CS_Middel	CS_Laag	Totaal
Cyber R&D (n=4)	198	32	83	252	565
Cyberproductie (n=31)	1833	1074	1384	4535	8826
Cyberintegratie (n=50)	2954	635	1299	7246	12134
Bedrijfsleven (n=71)	4199	1438	2259	10063	17959
Overheid (n=22)	1229	612	926	4134	6901
Onderwijs/KI (n=5)	229	33	94	302	658
Overig (n=2)	156	45	55	171	427
Cybereindgebruik (iedereen)	6174	2206	3462	15325	27167

Figuur 22: Aantal vacatures naar doelgroep o.b.v. de top 100 organisaties. Bron: Jobdigger, bewerking Dialogic

Op basis van primaire focus lijkt de cyber-R&D-categorie verreweg het kleinst te zijn. Dit is ook in lijn met het eerdere onderzoek 'de economische kansen van de cybersecuritysector'. Deze aantallen kunnen weliswaar een onderschatting zijn, omdat er diverse organisaties kunnen zijn die voor een (klein) deel wel wat met cyber-R&D doen, maar hoe dan ook lijkt dit de kleinste categorie te zijn. In de top 100 zien we veel partijen die (ook) actief zijn als cyberproducent of cyberintegrator. Daarbij wordt in deze populatie bijna 80% van de ECSF-profielen gevraagd door partijen die (ook) actief zijn als producent of integrator. Dit komt overeen met het beeld dat uit de gesprekken binnen dit onderzoek naar voren komt: de meeste vraag naar pure cybersecurityprofielen zit beperkt bij de sec eindgebruikers (m.u.v. de CISO-functie).
Een andere manier om de organisaties binnen de data te vergelijken is door te kijken naar hoeveel cybersecurity vacatures organisaties hebben geplaatst, zie figuur 23. Ook hier blijkt uit dat organisaties die relatief meer doen met cybersecurity ook meer vraag hebben naar specialistische profielen. En andersom: organisaties die weinig cybersecurity vacatures plaatsen vragen relatief vaker om mensen met een breder/ander profiel waar cybersecurity slechts een aandeel van is. Slechts 22% van de vacatures van organisaties met <=3 cybersecurity vacatures hebben betrekking op ECSF-profielen of functieprofielen met een groot aandeel cybersecurity.

Aantal vacatures dat organisatie heeft	Totaal	ECSF	CS_Hoog	CS_Middel	CS_Laag
>50	30751	6817	2491	3952	17491
11-50	14727	3279	940	1732	8776
4-10	8146	1883	407	804	5052
<=3	6209	1115	270	600	4224
Onbekend	1228	361	79	128	660
Totaal	**61061**	**13455**	**4187**	**7216**	**36203**

Aantal vacatures dat organisatie heeft	Totaal	ECSF	CS_Hoog	CS_Middel	CS_Laag
>50	100%	22%	8%	13%	57%
11-50	100%	22%	6%	12%	60%
4-10	100%	23%	5%	10%	62%
<=3	100%	18%	4%	10%	68%
Onbekend	100%	29%	6%	10%	54%
Totaal	**100%**	**22%**	**7%**	**12%**	**59%**

Figuur 23: Vraag naar typen cybersecurity profielen naar het aantal cybersecurity vacatures dat organisaties plaatsen. Bron: Jobdigger, bewerking Dialogic

4.4 Vraag naar specifieke functieprofielen

In 4.3 is de algemene vraag naar cybersecurity expertise beschreven. In deze sectie wordt één niveau verder ingezoomd en wordt gekeken naar specifieke functieprofielen die gevraagd worden.

4.4.1 Totaal

Binnen de vacatures is onderzocht waar gevraagd wordt om cyberexpertise. Functietitels, zoals gebruikt door Jobdigger, zijn vervolgens aan de vier typen categorieën (ECSF, hoog, middel, laag) gekoppeld. De koppeling met ECSF-profielen is gebeurd door de genoemde functietitels in de vacaturedata te koppelen aan een ECSF-profiel, indien van toepassing. Voor de labels van de functietitels behorend aan de categorieën 'CS – hoog', 'CS – middel' en 'CS – laag' zijn de labels zoals Jobdigger ze hanteert intact gelaten. Dit leidt tot de meest gevraagde functieprofielen/-titels, zoals in figuur 24 weergegeven.

Op basis van deze resultaten zien we het volgende:

- Binnen de ECSF-profielen zijn de (C)ISO en de Cybersecurity Implementer verreweg de meest gevraagde profielen.
- Binnen de categorie 'CS – hoog' zien we met name veel cybersecurity consultants/adviseurs, experts op het gebied van privacy en managers op het gebied van cybersecurity.
- Binnen de categorie 'CS – middel' zien we met name veel consultants/adviseurs en managers die naast cybersecurity een breder vakgebied bestrijken (veelal IT in de brede zin).
- Binnen de categorie 'CS – laag' zien we met name technische ICT-georiënteerde beroepen waarvan cybersecurity een (klein) aandeel vertegenwoordigt.

#	ECSF-profiel	Aantal vacatures
1	ECSF - CISO	3649
2	ECSF - Cybersecurity Implementer	3619
3	ECSF - Cyber Threat Intelligence Specialist	1626
4	ECSF - Cybersecurity Architect	1382
5	ECSF - Cybersecurity Risk Manager	823
6	ECSF - Cybersecurity Auditor	557
7	ECSF - Penetration Tester	520
8	ECSF - Cybersecurity Researcher	489
9	ECSF - Cyber Legal, Policy & Compliance Officer	275
10	ECSF - Cyber Incident Responder	246
11	ECSF - Digital Forensics Investigator	154
12	ECSF - Cybersecurity Educator	115
	Totaal	13455

#	Functietitel - CS-hoog	Aantal vacatures
1	Cyber Security Consultant	301
2	Functionaris (gegevensbescherming)	296
3	Adviseur Informatiebeveiliging	254
4	Cybersecurity Consultant	99
5	Informatiebeveiliging Consultant	58
6	Business Consultant Security	55
7	Onderzoeker	47
8	Adviseur Informatiebeveiliging & Privacy	39
9	Manager Cyber Security	37
10	Adviseur Cybersecurity	36
11	Privacy Manager	34
12	Adviseur Privacy & Informatiebeveiliging	34
13	Security Adviseur	32
14	Cyber Security	31
15	Cyber Security Expert	30
16	Traineeship Cyber Security	29
17	Coördinator Informatiebeveiliging	28
18	Architect Identity & Management	27
19	Accountmanager Publiek Private Samenwerking	26
20	Cyber Security Project Manager	24
	Overig	2670
	Totaal	4187

#	Functietitel - CS-middel	Aantal vacatures
1	Privacy Officer	467
2	Security Consultant	329
3	Consultant	298
4	Adviseur	216
5	Manager	160
6	Analist	131
7	Privacy Consultant	124
8	Digitaal Specialist	119
9	Security Manager	103
10	Security Talent	89
11	Business Development Manager	75
12	Risk Manager	72
13	Traineeship	69
14	Webdeveloper	69
15	IT Security Manager	69
16	Privacy Adviseur	67
17	IT Risk Manager	67
18	Cloud Security Consultant	67
19	Sales Manager	66
20	Jurist Privacy	62
	Overig	4497
	Totaal	7216

#	Functietitel - CS-laag	Aantal vacatures
1	Systeembeheerder	449
2	Auditor	358
3	Functioneel Beheerder	248
4	Accountmanager	226
5	Projectmanager	213
6	Koerier	198
7	Software Engineer	190
8	Informatiemanager	188
9	Netwerkbeheerder	167
10	Engineer	166
11	Developer	158
12	Architect	149
13	Data Engineer	147
14	Traineeship Informatiemanagement Overheid	146
15	Product Owner	142
16	Business Analist	135
17	Compliance Officer	127
18	Projectleider	123
19	Software Developer	113
20	Technisch Applicatiebeheerder	108
	Overig	32452
	Totaal	36203

Figuur 24: Meest gevraagde functietitels per categorie. Bron: Jobdigger, bewerking Dialogic

4.4.2 Regio

In 4.3.2 is de regionale spreiding van cybersecurity vacatures weergegeven: een groot deel van de vacatures wordt in de Randstad geplaatst. De drie provincies Noord-Holland, Zuid-Holland en Utrecht lijken daarmee ook relatief meer gespecialiseerd te zijn op het gebied van cybersecurity. Dit beeld komt terug in de functieprofielen waar naar gevraagd wordt in de regio. De top 20 functieprofielen van de top provincies bevatten ook meer cybersecurity specialistische functies (ECSF en 'Cybersecurity – Hoog') dan de provincies waar minder cybersecurity vacatures zijn uitgezet, zie supplementaire tabel 18 in Bijlage 3.

4.4.3 Opleidingsniveau en werkervaring

Op het niveau van functieprofielen is ook gekeken naar de vraag gekoppeld aan werkervaring en opleidingsniveau. Voor iedere combinatie van enerzijds mbo, hbo en wo en anderzijds junior, medior en senior zijn de top 20 gevraagde functieprofielen uitgedraaid. Dat komt dus overeen met 3x3=9 combinaties/tabellen. Details over de functieprofielen per combinatie van het gevraagde opleidingsniveau en de werkervaring is opgenomen in supplementaire tabel 19 in Bijlage 3.

Uit de tabellen blijkt duidelijk dat er over het algemeen verschillende typen professionals gevraagd worden aan de hand van de opleidingsniveaus. Op mbo-niveau zien we relatief veel functieprofielen met een laag cybersecurity gehalte, en zijn er veel functieprofielen met een IT-karakter waar cybersecurity een onderdeel van uitmaakt. Daarnaast zijn de ECSF-profielen waar soms een mbo-opleidingsniveau voor gevraagd wordt met name technisch van aard. Dit beeld is ook in lijn met de algehele bevindingen; mbo-opgeleiden hebben vaak een gerichte technische focus.

De functies op hbo- en wo-niveau zijn relatief vergelijkbaar. Er zijn wel verschillen aan te treffen. Zo is het profiel van researcher iets waarvoor (logischerwijs) met name een wo-opleiding gevraagd wordt.

Een belangrijke bevinding is dat de ECSF-profielen voldoende mogelijkheden bieden om wel als junior te kunnen starten. Zo zal een junior niet direct als hoofdleidinggevende aan de slag gaan, maar kan het wel onderdelen van het CISO-pakket oppakken, waarna je als een ISO (met een gericht takenpakket) door kunt ontwikkelen naar een 'volledige' CISO. Ook bij profielen zoals Implementer lijken er doorgroeimogelijkheden te zijn, waarbij men bij de start een gericht stukje kan oppakken en tijdens het werken meer en meer bij kan leren.

4.4.4 Sector

De cybersecurity profielen die gevraagd worden op de arbeidsmarkt houden ook verband met de sectoren waarin organisaties werkzaam zijn. De doelen, taken en activiteiten van organisaties creëren immers de behoefte aan bepaalde kennis en expertise bij mensen om de benodigde taken goed uit te kunnen voeren. Om te illustreren hoe verschillende sectoren om verschillende profielen vragen zijn hieronder de top 20 functieprofielen weergegeven voor de vier sectoren waarin de vraag naar cybersecurity expertise het grootste is (figuur 25).

Bepaalde profielen worden in al deze sectoren veel gevraagd, zoals de ECSF-profielen CISO, Cyber Threat Intelligence Specialist, Cybersecurity Implementer, Cybersecurity Risk Manager en Cybersecurity Architect. Andere profielen worden met name in bepaalde sectoren gevraagd; een Pentester wordt met name in de IT en zakelijke dienstverlening gevraagd, en de Privacy Officer wordt met name binnen de overheid gevraagd.

#1. 84 - Openbaar bestuur, overheidsdiensten en verpl. soc. verz.

#	Functieprofiel	Type	Aantal vacatures
1	ECSF - CISO	ECSF	460
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	222
3	ECSF - Cybersecurity Implementer	ECSF	142
4	ECSF - Cybersecurity Risk Manager	ECSF	127
5	Privacy Officer	CS_Middel	125
6	Digitaal Specialist	CS_Middel	119
7	ECSF - Cybersecurity Architect	ECSF	108
8	Functionaris	CS_Hoog	85
9	Functioneel Beheerder	CS_Laag	71
10	ECSF - Cybersecurity Auditor	ECSF	66
11	Adviseur Informatiebeveiliging	CS_Hoog	62
12	Informatiemanager	CS_Laag	55
13	Adviseur	CS_Middel	55
14	Auditor	CS_Laag	40
15	Systeembeheerder	CS_Laag	35
16	Privacy Adviseur	CS_Middel	34
17	Officier	CS_Laag	32
18	Jurist	CS_Laag	32
19	Informatieadviseur	CS_Laag	32
20	ICT Beheerder	CS_Laag	32

#2. 62 - Dienstverlenende activiteiten op het gebied van IT

#	Functieprofiel	Type	Aantal vacatures
1	ECSF - Cybersecurity Implementer	ECSF	682
2	ECSF - CISO	ECSF	425
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	242
4	ECSF - Cybersecurity Architect	ECSF	174
5	ECSF - Penetration Tester	ECSF	174
6	Security Consultant	CS_Middel	132
7	ECSF - Cybersecurity Risk Manager	ECSF	110
8	Cyber Security Consultant	CS_Hoog	74
9	Accountmanager	CS_Laag	67
10	Consultant	CS_Middel	58
11	Systeembeheerder	CS_Laag	52
12	Technisch Applicatiebeheerder	CS_Laag	45
13	PHP Developer	CS_Laag	35
14	Servicedesk Medewerker	CS_Laag	33
15	Access Management Consultant	CS_Laag	33
16	Projectmanager	CS_Laag	32
17	Engineer	CS_Laag	32
18	Developer	CS_Laag	31
19	Cloud Consultant	CS_Laag	30
20	Backend Developer	CS_Laag	30

#3. 69 - Rechtskundige dienstverl., accountancy, belastingadv. en admin.

#	Functieprofiel	Type	Aantal vacatures
1	ECSF - Cybersecurity Auditor	ECSF	199
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	128
3	ECSF - Cybersecurity Implementer	ECSF	88
4	ECSF - CISO	ECSF	87
5	ECSF - Penetration Tester	ECSF	78
6	Auditor	CS_Laag	76
7	ECSF - Cybersecurity Architect	ECSF	70
8	Cyber Security Consultant	CS_Hoog	69
9	ECSF - Digital Forensics Investigator	ECSF	65
10	Consultant	CS_Middel	59
11	Sales & Marketing Intern	CS_Laag	52
12	Manager	CS_Middel	43
13	Cybersecurity Consultant	CS_Hoog	38
14	ECSF - Cyber Incident Responder	ECSF	37
15	Business Management Consultant	CS_Middel	37
16	Actuarial & Quantitative Consultant	CS_Laag	31
17	Associate	CS_Laag	31
18	Werkstudent & Quantitative Consulting	CS_Laag	30
19	Advisor	CS_Middel	29
20	Werkstudent Actuarieel & Consulting	CS_Laag	27

#4. 70 - Holdings (geen fin.), concerndiensten intern en mgt.-adv.

#	Functieprofiel	Type	Aantal vacatures
1	ECSF - Cybersecurity Implementer	ECSF	184
2	ECSF - CISO	ECSF	150
3	ECSF - Cybersecurity Architect	ECSF	133
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	105
5	Adviseur Informatiebeveiliging	CS_Hoog	58
6	Webdeveloper	CS_Middel	55
7	Adviseur	CS_Middel	55
8	ECSF - Cybersecurity Risk Manager	ECSF	54
9	Cyber Security Consultant	CS_Hoog	52
10	ECSF - Cybersecurity Auditor	ECSF	44
11	Systeembeheerder	CS_Laag	39
12	Consultant	CS_Middel	39
13	Privacy Consultant	CS_Middel	37
14	Consultant IT & Assurance	CS_Laag	36
15	Consultant IT Assurance	CS_Laag	35
16	Cloud Security Consultant	CS_Middel	32
17	Cybersecurity Consultant	CS_Hoog	31
18	ECSF - Cyber LPC Officer	ECSF	29
19	ECSF - Cyber Incident Responder	ECSF	29
20	Security Consultant	CS_Middel	28

Figuur 25: Top 20 functieprofielen per sector. Bron: Jobdigger, bewerking Dialogic

4.4.5 Organisaties

De geaggregeerde cijfers over de cybersecurity arbeidsmarkt zijn in zekere zin abstract; het gaat onder meer over 'totalen', volledige sectoren, en vacatures op een bepaald opleidingsniveau. In werkelijkheid zijn dit aggregaten van allemaal individuele manifestaties van behoefte aan cybersecurity expertise. Het zijn individuele organisaties die in individuele casussen behoefte hebben aan mensen die bepaalde taken kunnen uitvoeren en bepaalde kennis en vaardigheden met zich meebrengen. Deze onderliggende concrete casuïstiek in de praktijk wordt duidelijker wanneer we inzoomen op individuele organisaties.

In figuur 26 is voor vier organisaties met veel vraag naar cybersecurity expertise, de Politie, CGI, de Belastingdienst en de ABN AMRO getoond welke functieprofielen (met een cybercomponent) zij vragen op de arbeidsmarkt. Hoewel een aantal generieke ECSF-profielen door allen gevraagd worden, wordt snel zichtbaar dat het bij verschillende organisaties om verschillende functieprofielen gaat. Bij de Politie wordt o.a. om rechercheurs, teamchefs en generalisten tactische opsporing gevraagd. Bij CGI is (ook) de vraag naar IT-professionals met enige expertise op het gebied van cybersecurity zichtbaar. Voor een organisatie zoals de Belastingdienst komen ook profielen zoals financieel rechercheur en fiscaal rechercheur naar voren. Bij ABN AMRO komen bedrijfsspecifieke profielen zoals het ABN IT Talent Programme en Global IT Talent programma naar voren, alsmede functies zoals de Transaction Monitoring Specialist.

Politie

#	Functieprofiel	Type	Aantal
1	Digitaal Specialist	CS_Middel	119
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	112
3	ECSF - Cybersecurity Implementer	ECSF	59
4	ECSF - Cybersecurity Architect	ECSF	54
5	ECSF - Cybersecurity Risk Manager	ECSF	40
6	Accountmanager Publiek Private Samenwerking	CS_Hoog	26
7	Rechercheur	CS_Laag	20
8	Developer	CS_Laag	19
9	Teamchef	CS_Laag	17
10	Analist	CS_Middel	17
11	Generalist Tactische Opsporing	CS_Middel	17
12	Operationeel Specialist	CS_Laag	16
13	Delivery Manager Oracle Linux	CS_Laag	15
14	Medewerker Intake & Service	CS_Laag	14
15	Gebruikersondersteuner	CS_Laag	14
16	Specialist Open Source Intelligence	CS_Laag	13
17	Tester	CS_Laag	13
18	Financieel Rechercheur	CS_Middel	13
19	Adviseur Privacy	CS_Middel	13
20	Digitaal Coördinator Cybercrime	CS_Hoog	13

CGI

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	163
2	ECSF - Cybersecurity Architect	ECSF	59
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	44
4	ECSF - CISO	ECSF	42
5	Technisch Applicatiebeheerder	CS_Laag	38
6	ECSF - Cybersecurity Risk Manager	ECSF	37
7	Cyber Security Consultant	CS_Hoog	27
8	Testautomatiseerder	CS_Laag	26
9	Outsystems Ontwikkelaar	CS_Laag	24
10	Java Software Engineer	CS_Laag	22
11	Business Information Analyst	CS_Laag	21
12	Director Consulting Service	CS_Laag	19
13	Experienced Java Software Engineer	CS_Laag	18
14	Filenet Consultant	CS_Laag	16
15	Oracle Database Administrator DBA	CS_Laag	15
16	Digital Workplace Engineer	CS_Laag	13
17	Engineer	CS_Laag	12
18	Projectmanager	CS_Laag	12
19	MES Service Engineer	CS_Laag	12
20	MES Business Consultant	CS_Laag	12

Belastingdienst

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Auditor	ECSF	46
2	ECSF - Cybersecurity Implementer	ECSF	35
3	ECSF - CISO	ECSF	22
4	Adviseur Informatiebeveiliging	CS_Hoog	19
5	ECSF - Cyber Threat Intelligence Specialist	ECSF	17
6	ECSF - Cybersecurity Risk Manager	ECSF	17
7	Analist	CS_Middel	12
8	Financieel Rechercheur	CS_Middel	12
9	Forensisch IT Rechercheur	CS_Laag	11
10	Fiscaal Rechercheur	CS_Laag	11
11	Tactisch Rechercheur	CS_Middel	10
12	Teamleider	CS_Laag	9
13	Rechercheur	CS_Laag	9
14	Adviseur Bedrijfsvoering AO/IC	CS_Laag	9
15	Adviseur Informatiehuishouding	CS_Laag	8
16	Adviseur Bedrijfsvoering	CS_Middel	8
17	Adviseur Integrale Beveiliging	CS_Middel	8
18	Adviseur	CS_Middel	8
19	Audit Traineeship	CS_Laag	8
20	Privacy & Data Coördinator	CS_Middel	7

ABN AMRO

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	82
2	ECSF - CISO	ECSF	68
3	ECSF - Cybersecurity Auditor	ECSF	31
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	22
5	ABN IT Talent Programme	CS_Laag	17
6	Compliance Advisor	CS_Laag	16
7	Global IT Talent Programme	CS_Laag	10
8	ECSF - Cybersecurity Architect	ECSF	10
9	Artificial Intelligence Translator	CS_Laag	10
10	Analist	CS_Middel	10
11	IT Projectmanager	CS_Laag	9
12	Business Architect	CS_Laag	9
13	Model Innovation & Project	CS_Laag	9
14	Transaction Monitoring Specialist	CS_Laag	8
15	Security Case Developer Application	CS_Laag	8
16	Careerguide	CS_Middel	7
17	Administratief Medewerker	CS_Laag	7
18	ABN Amro	CS_Middel	7
19	Business Proces Expert Security	CS_Hoog	7
20	Innovation&projects Model Validator	CS_Laag	7

Figuur 26: Vier organisaties en hun top 20 profielen. Bron: Jobdigger, bewerking Dialogic

4.4.6 Doelgroepen

De verschillende doelgroepen zoals besproken in 4.2.2. kennen een verschillende dynamiek, wat zich ook uit in de vraag naar verschillende functieprofielen. Voor de top 100 organisaties is een (ruwe) inschatting gemaakt van in welke doelgroep zij (primair) vallen. Deze is opgenomen in supplementaire tabel 20 in Bijlage 3.

Niet verrassend wordt er binnen 'cyber R&D' relatief veel naar researchers gevraagd. Bij de cybersecuritysector zelf (producenten van cybersecuritygoederen/-diensten) en de integrators lijkt er een grote vraag aan specialistische cybersecurity profielen te zijn, waaronder ook de sterk technische profielen.

Zoals eerder genoemd zijn de partijen die relatief veel met cybersecurity doen en veel vraag naar cybersecurity professionals hebben, ook de partijen die relatief vaak specialistische profielen vragen. Deze resultaten ondersteunen dat beeld.

4.5 Vraag naar specifieke taken, kennis en vaardigheden

In deze sectie wordt er verder ingezoomd op het concept cybersecurity expertise. Van het niveau van functieprofielen wordt hier de stap gemaakt naar individuele taken, kennis en vaardigheden. Deze 'bouwstenen' vormen de basis voor wat de cybersecurity professional moet weten, kunnen en doen. Zie ook 4.2.1 voor meer toelichting. Voor een methodologische verantwoording, zie Bijlage 1.

4.5.1 Totaal

De uitwerking van de ECSF-profielen kent een aantal onderdelen, waaronder deliverables, main tasks, key skills en key knowledge. In veel vacatures kunnen we expliciet bepaalde bouwstenen terugvinden. Uiteraard is niet iedere vacature even uitgebreid beschreven, en soms kan men taalgebruik hanteren dat niet (eenvoudig) geautomatiseerd te herkennen is, maar over het algemeen is het mogelijk om te analyseren hoe vaak bepaalde bouwstenen voorkomen. In 79-85% van de vacatures kunnen we individuele bouwstenen terugvinden m.b.t. cybersecurity kennis en cybersecurity vaardigheden (figuur 27).

Type bouwsteen	Aantal vacatures	% vacatures
Deliverable	33006	54%
Key knowledge	51966	85%
Key skills	48279	79%
Main tasks	40783	67%

Figuur 27: Overzicht gevonden bouwstenen. Bron: Jobdigger, bewerking Dialogic

Op basis van de analyse kunnen we de top 20 laten zien per type bouwsteen. Figuur 28 laat de top 20 **taken** zien die teruggevonden zijn binnen de vacatures. Direct valt het op dat de top 3 bestaat uit taken die betrekking hebben op de categorie 'Management & Organisatie'. Het gaat daarbij om het ontwikkelen en onderhouden van samenwerkingsrelaties met zowel externe stakeholders als interne stakeholders. Andere taken die vaak expliciet geïdentificeerd worden liggen in het domein van het werken binnen juridische kaders, het voorstellen van nieuwe processen en procedures op het gebied van cybersecurity, en het beoordelen en omgaan met cybersecurity risico's.
De resultaten laten daarnaast (wederom) zien dat cybersecurity allesbehalve een puur 'technisch' domein is, een opvatting die soms leeft binnen Nederland. Er is zonder meer behoefte aan de uitvoering van technisch georiënteerde taken, maar een groot deel van de bijbehorende taken hebben het karakter van management en organisatie, wet- en regelgeving en onderzoek/analyse.

#	Main task(s)	Categorie	% vacatures	Aantal vacatures
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	40,7%	24860
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36,7%	22439
3	Collaborate with other teams and colleagues	Man. & Org.	31,4%	19178
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25,1%	15331
5	Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions	Onderzoek	3,2%	1933
6	Enforce and advocate organisation's data privacy and protection program	Legal	3,1%	1870
7	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technisch	1,8%	1112
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Onderwijs	1,6%	997
9	Deploy penetration testing tools and penetration test programs	Technisch	1,6%	952
10	Design and propose a secure architecture to implement the organisation's strategy	Technisch	1,4%	863
11	Manage legal aspects of information security responsibilities and third-party relations	Legal	1,3%	776
12	Develop organisation's cybersecurity architecture to address security and privacy requirements	Technisch	1,3%	776
13	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1,1%	700
14	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technisch	1,1%	657
15	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance	Man. & Org.	0,7%	439
16	Conduct research, innovation and development work in cybersecurity-related topics	Onderzoek	0,6%	357
17	Identify, analyse and assess technical and organisational cybersecurity vulnerabilities	Onderzoek	0,5%	333
18	Identify and document compliance gaps	Onderzoek	0,5%	309
19	Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations	Legal	0,5%	294
20	Contribute to the development of the organisation's cybersecurity strategy, policy and procedures	Man. & Org.	0,5%	285

Figuur 28: Top 20 gevonden 'Main tasks'. Bron: Jobdigger, bewerking Dialogic

Wanneer we kijken naar de gevraagde vaardigheden, zien we voor een groot deel een vergelijkbaar beeld. Er worden veel niet-technische vaardigheden gevraagd op het gebied van communicatie, management en organisatie. Tegelijkertijd zien we relatief veel technische vaardigheden terug in de top 20 (figuur 29). Het feit dat taken en vaardigheden geen 1-op-1-relatie hebben is ook niet vreemd; er kunnen immers meerdere vaardigheden nodig zijn om een bepaalde taak uit te voeren, en er kunnen meerdere taken uitgevoerd worden op basis van dezelfde vaardigheid. In technische termen kan men spreken van een 'many-to-many-relatie (m:m').

#	Key skill(s)	Categorie	% vacature	Aantal vacature
1	Motivate and encourage people	Man. & Org.	44,0%	26863
2	Identify, analyse and correlate cybersecurity events	Onderzoek	41,9%	25562
3	Collaborate with other team members and colleagues	Man. & Org.	31,4%	19182
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	31,2%	19074
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9,9%	6016
6	Develop codes, scripts and programmes	Technisch	5,9%	3619
7	Develop code, scripts and programmes	Technisch	5,9%	3619
8	Think creatively and outside the box	Onderzoek	4,1%	2484
9	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	2,6%	1577
10	Work under pressure	Man. & Org.	2,3%	1383
11	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	2,0%	1240
12	Conduct ethical hacking	Technisch	2,0%	1225
13	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technisch	1,9%	1132
14	Identify and exploit vulnerabilities	Technisch	1,8%	1100
15	Assess the security and performance of solutions	Technisch	1,6%	984
16	Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Technisch	1,4%	861
17	Perform social engineering	Technisch	1,3%	818
18	Review codes assess their security	Technisch	1,3%	788
19	Conduct technical analysis and reporting	Technisch	1,2%	731
20	Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Legal	0,7%	456

Figuur 29: Top 20 gevonden 'key skills'. Bron: Jobdigger, bewerking Dialogic

Tot slot zien we in de top 20 **kennisonderwerpen** veel technische kenniselementen terugkomen (figuur 30). Er zijn ook andere kennisonderwerpen, zoals kennis over managementpraktijken en bepaalde procedures, maar in termen van kennis lijkt de technische component wel de bovenhand te voeren. Deze bevindingen tezamen suggereren op hoofdlijnen dat men, om werkzaam te zijn op het gebied van cybersecurity, een substantiële kennisbasis nodig heeft, maar dat veel taken die cybersecurity professionals uitvoeren niet per se (enkel) technisch van aard zijn. Het onderstreept het multidisciplinaire karakter van het domein cybersecurity, en toont daarnaast ook het belang van 'technische' kennis binnen het domein. Verderop in deze paragraaf zal deze bevinding verder uitgediept worden in relatie tot verschillende typen cybersecurity profielen.

#	Key knowledge	Categorie	% vacatures	Aantal vacatures
1	Cybersecurity standards, methodologies and frameworks	Technisch	45,8%	27983
2	Cybersecurity controls and solutions	Technisch	43,1%	26336
3	Cyber threats	Technisch	35,9%	21906
4	Cybersecurity related laws, regulations and legislations	Legal	34,7%	21199
5	Management practices	Man. & Org.	30,3%	18481
6	Cybersecurity procedures	Man. & Org.	30,0%	18296
7	Cybersecurity risks	Technisch	28,2%	17243
8	Cybersecurity recommendations and best practices	Man. & Org.	26,5%	16151
9	Cybersecurity policies	Man. & Org.	21,6%	13167
10	Cybersecurity-related technologies	Technisch	13,9%	8458
11	Multidiscipline aspect of cybersecurity	Man. & Org.	10,4%	6356
12	Secure Operation Centres (SOCs) operation	Technisch	6,8%	4134
13	Cybersecurity-related research, development and innovation (RDI)	Onderzoek	5,8%	3554
14	Auditing-related certification	Technisch	5,7%	3476
15	Risk management standards, methodologies and frameworks	Man. & Org.	4,7%	2859
16	Penetration testing procedures	Technisch	4,1%	2478
17	Cybersecurity attack procedures	Technisch	3,5%	2122
18	Computer networks security	Technisch	2,8%	1699
19	Operating networks security	Technisch	2,7%	1658
20	Computer programming	Technisch	2,7%	1658

Figuur 30: Top 20 gevonden 'Key knowledge'. Bron: Jobdigger, bewerking Dialogic

Wanneer we kijken naar de vraag naar verschillende 'typen bouwstenen' over de tijd, dan zien we dat de vraag naar deze bouwstenen in de breedte in absolute zin stijgt, maar dat de relatieve verhouding over tijd nagenoeg gelijk blijft (figuur 31). Het vakgebied 'lijkt dus niet te veranderen in termen van samenstelling'. Ongeveer een derde van de bouwstenen heeft betrekking op de categorie 'management & Organisatie', circa 30% op techniek, circa 20% op wet- en regelgeving en circa 20% op onderzoek.

Aantal vacatures met type bouwsteen	2018	2019	2020	2021	2022	Totaal
Legal	4.151	4.472	4.976	7.677	10.328	**31.604**
Management & Organisatie	6.891	7.702	8.631	13.506	16.728	**53.458**
Onderwijs	304	261	344	624	807	**2.340**
Onderzoek	3.986	4.380	5.021	8.068	9.746	**31.201**
Technisch	6.054	6.840	7.558	11.752	14.758	**46.962**
Totaal	**21.386**	**23.655**	**26.530**	**41.627**	**52.367**	**165.565**

Aantal vacatures met type bouwsteen	2018	2019	2020	2021	2022	Totaal
Legal	19%	19%	19%	18%	20%	**19%**
Management & Organisatie	32%	33%	33%	32%	32%	**32%**
Onderwijs	1%	1%	1%	1%	2%	**1%**
Onderzoek	19%	19%	19%	19%	19%	**19%**
Technisch	28%	29%	28%	28%	28%	**28%**

Figuur 31: Ontwikkeling vraag naar 'typen bouwstenen' over de tijd. Bron: Jobdigger, bewerking Dialogic

De diverse taken, vaardigheden en kennis zijn ook uitgesplitst naar typen cybersecurity professional, zie onderstaande figuren. Daarbij is het belangrijk om op te merken dat het hier gaat om de meest voorkomende bouwstenen met betrekking tot cybersecurity (o.b.v. het ECSF-raamwerk). Ter illustratie: een developer zal mogelijk gevraagd worden om ook kundig te zijn in de omgang met JavaScript of PHP, een financieel analist zal ook kennis moeten hebben over financiële stromen, maar die bouwstenen zijn niet onderzocht in dit onderzoek. Het gaat dus expliciet om het identificeren van cybersecurity relevante bouwstenen in de verschillende functies.
Op basis van de uitsplitsing naar de vier categorieën cybersecurity functies (ECSF, CS – Hoog, CS – Middel, CS – Laag) kunnen we constateren dat er een flink aantal overeenkomsten zijn. In termen van taken en vaardigheden is onder

andere de samenwerking met interne en externe stakeholders, en het (kunnen) identificeren en beoordelen van cyberrisico's een gemeenschappelijke deler. Op het gebied van kennis is de vraag naar technische know- how over risico's en bedreigingen, standaarden, methodologieën en raamwerken veelal aanwezig. Binnen de ECSF-profielen lijkt relatief vaker naar cybersecurity technische vaardigheden gevraagd te worden, bijvoorbeeld op het gebied van ethisch hacken en het ontleden van technische systemen. Binnen de profielen met een laag cybersecurity gehalte lijkt daarentegen meer vraag te zijn naar meer 'generieke' IT-skills op het gebied van bijvoorbeeld programmeren en de omgang met OS en servers. Dit is ook in lijn met de verschillende typen functies die aangetroffen zijn in de verschillende categorieën (Supplementaire tabel 21 t/m 24).

Certificaten

Een specifieke bouwsteen waar veel interesse voor is getoond in de gesprekken en workshops binnen dit onderzoek zijn de certificaten die gevraagd worden op de arbeidsmarkt. Onder andere vanuit de NRTO is opgemerkt dat certificaten relatief belangrijk zijn op de arbeidsmarkt voor cybersecurity professionals.
Binnen 9.387 vacatures (15%) worden expliciet één of meerdere certificaten gevraagd of genoemd. De meest gevraagde certificaten zijn de 'Certified Information Systems Security Professional' (CISSP), de 'Certified Information Security Manager' (CISM) en de 'Certified Information Systems Auditor' (CISA), zie Figuur 32.

#	Certificaat	% vacatures	Aantal vacatures
1	CISSP	11,2%	6821
2	CISM	8,1%	4925
3	CISA	5,6%	3417
4	CIPP	2,8%	1713
5	CEH	2,1%	1301
6	CCSP	1,6%	999
7	OSCP	1,6%	950
8	CRISC	1,3%	785
9	CIPM	1,2%	762
10	GIAC	0,6%	342

#	Certificaat	% vacatures	Aantal vacatures
11	GCIH	0,4%	253
12	CSSLP	0,4%	230
13	OSCE	0,3%	204
14	SSCP	0,2%	150
15	GSEC	0,2%	141
16	GCIA	0,2%	105
17	GCFA	0,2%	103
18	CFE	0,2%	97
19	ECSA	0,1%	52
20	GWAPT	0,1%	45

Figuur 32: Top 20 meest gevraagde certificaten. Bron: Jobdigger, bewerking Dialogic

Deze relatieve ranking houdt op hoofdlijnen stand bij de vacatures voor de verschillende typen cybersecurity professionals. Wel is het zo dat, in lijn der verwachtingen, de meeste certificaten gevraagd worden voor cybersecurity functies met een ECSF-profiel, zie Figuur 33.

#	Functietitel - ECSF	% vacatures	Aantal vacatures
1	CISSP	25,6%	3440
2	CISM	17,0%	2290
3	CISA	10,6%	1422
4	CEH	5,4%	729
5	OSCP	4,2%	568
6	CCSP	3,6%	491
7	CRISC	2,9%	385
8	CIPP	2,8%	376
9	GIAC	1,8%	238
10	GCIH	1,7%	235

#	Functietitel - CS-hoog	% vacatures	Aantal vacatures
1	CISSP	27,3%	1145
2	CISM	22,9%	960
3	CISA	14,4%	603
4	CIPP	9,0%	377
5	CEH	6,1%	256
6	CRISC	3,6%	149
7	OSCP	3,2%	136
8	CIPM	3,2%	132
9	CCSP	2,1%	89
10	OSCE	1,0%	42

#	Functietitel - CS-laag	% vacatures	Aantal vacatures
1	CISSP	2,9%	1065
2	CISM	2,1%	751
3	CISA	2,0%	708
4	CIPP	0,8%	286
5	CCSP	0,5%	199
6	CIPM	0,4%	160
7	CRISC	0,4%	144
8	CEH	0,3%	106
9	OSCP	0,3%	106
10	SSCP	0,1%	41

#	Functietitel - CS-middel	% vacatures	Aantal vacatures
1	CISSP	15,5%	1121
2	CISM	12,1%	873
3	CIPP	9,0%	649
4	CISA	8,4%	606
5	CIPM	4,7%	340
6	CEH	2,7%	198
7	CCSP	2,6%	190
8	OSCP	2,0%	143
9	CRISC	1,3%	92
10	GIAC	0,6%	44

Figuur 33: Certificaten per categorie cybersecurity vacatures. Bron: Jobdigger, bewerking Dialogic

Voor sommige functies wordt in het merendeel van de tijd expliciet gevraagd om een cybersecurity certificaat. In andere functies gebeurt dat minder vaak. Voor de top 25 functies waarin expliciet gevraagd wordt om een cybersecurity certificaat, zien we dat de Access Management Consultant, de CISO en de Security Advisor relatief vaak een certificaat wordt gevraagd, zie figuur 34. Aanvullend is voor de 10 functies waarin de meeste certificaten gevraagd zijn uitgesplitst welke specifieke certificaten gevraagd worden, zie supplementaire tabel 25. Een aantal certificaten zoals de CISSP wordt overal veel gevraagd. Andere certificaten zijn specifieker, zoals de CISSP-ISSAP voor de Cybersecurity Architect of de Offensive Security Certified Professional (OSCP) voor de Penetration Tester.

#	Functie	Aantal vacatures	Totaal aantal vacatures	% vacatures in deze functie
1	ECSF - CISO	2051	2649	77%
2	ECSF - Cyber Threat Intelligence Specialist	609	1627	37%
3	ECSF - Cybersecurity Implementer	428	3619	12%
4	ECSF - Cybersecurity Architect	375	1382	27%
5	ECSF - Penetration Tester	302	520	58%
6	ECSF - Cybersecurity Risk Manager	272	823	33%
7	Privacy Officer	198	467	42%
8	ECSF - Cybersecurity Auditor	173	557	31%
9	Security Consultant	172	329	52%
10	Cyber Security Consultant	161	301	53%
11	Auditor	125	358	35%
12	Adviseur Informatiebeveiliging	111	254	44%
13	ECSF - Cyber Incident Responder	91	246	37%
14	Consultant	73	298	24%
15	ECSF - Cyber Legal, Policy & Compliance Officer	71	275	26%
16	Cybersecurity Consultant	67	99	68%
17	Functionaris	66	296	22%
18	Privacy Consultant	63	124	51%
19	Manager	48	160	30%
20	IT Security Manager	45	69	65%
21	Jurist Privacy	43	62	69%
22	Informatiebeveiliging Consultant	40	58	69%
23	Security Advisor	34	44	77%
24	Access Management Consultant	32	34	94%
25	Analist	30	131	23%

Figuur 34: Top 25 functieprofielen waarin expliciet gevraagd wordt om een cybersecurity certificaat. Bron: Jobdigger, bewerking Dialogic

4.5.2 Regio

De verschillende bouwstenen zijn ook naar regio uitgesplitst, zie figuur 35. De verdeling over bouwstenen volgt op hoofdlijnen dezelfde verdeling die de vacatures op hoofdlijnen hebben. Er zitten enkele afwijkingen in, zoals dat er in Noord-Brabant en Zuid-Holland relatief veel onderwijsbouwstenen gevonden worden. De individuele taken, kennis en vaardigheden die gevraagd worden volgen de algemene vraag van de regio's. Voor een overzicht, zie hiervoor supplementaire tabel 26.

Absoluut

Provincie	Legal	Man. & Org.	Onderwijs	Onderzoek	Technisch	Totaal
Drenthe	279	433	25	235	354	**1326**
Flevoland	331	554	35	297	482	**1699**
Friesland	353	521	31	266	416	**1587**
Gelderland	2181	3451	99	1970	3042	**10743**
Groningen	607	1007	30	553	886	**3083**
Limburg	863	1358	57	801	1274	**4353**
Noord-Brabant	3113	5365	345	2990	4784	**16597**
Noord-Holland	7769	14544	576	8727	12589	**44205**
Overijssel	1408	2475	56	1340	2368	**7647**
Utrecht	5731	9780	390	5892	8443	**30236**
Zeeland	161	248	20	159	234	**822**
Zuid-Holland	8786	13687	671	7954	12063	**43161**
Onbekend	22	35	5	17	27	**106**
Totaal	**31325**	**53025**	**2315**	**30966**	**46608**	**164239**

Relatief

Provincie	Legal	Man. & Org.	Onderwijs	Onderzoek	Technisch	Totaal
Drenthe	1%	1%	1%	1%	1%	**1%**
Flevoland	1%	1%	2%	1%	1%	**1%**
Friesland	1%	1%	1%	1%	1%	**1%**
Gelderland	7%	7%	4%	6%	7%	**7%**
Groningen	2%	2%	1%	2%	2%	**2%**
Limburg	3%	3%	2%	3%	3%	**3%**
Noord-Braban	10%	10%	15%	10%	10%	**10%**
Noord-Hollanc	25%	27%	25%	28%	27%	**27%**
Overijssel	4%	5%	2%	4%	5%	**5%**
Utrecht	18%	18%	17%	19%	18%	**18%**
Zeeland	1%	0%	1%	1%	1%	**1%**
Zuid-Holland	28%	26%	29%	26%	26%	**26%**
Onbekend	0%	0%	0%	0%	0%	**0%**

Figuur 35: Typen bouwstenen per provincie. Bron: Jobdigger, bewerking Dialogic

4.5.3 Opleidingsniveau en werkervaring

De bouwstenen zijn ook uitgesplitst naar vacatures op basis van het gevraagde opleidingsniveau en werkervaring en opgenomen in supplementaire tabel 27. Hierin is te zien per categorie functies welke bouwstenen veel gevraagd worden. Door de verschillende mate van werkervaring heen zijn de gevraagde bouwstenen redelijk vergelijkbaar. Ook tussen de opleidingsniveaus zijn er veel overeenkomsten, afgezien van een aantal nuanceverschillen. Dit suggereert dat de gevraagde kennis en vaardigheden op een bepaald conceptueel niveau vergelijkbaar zijn tussen verschillende opleidingsniveaus en mate van werkervaring, maar dat het met name zit in de invulling daarvan. Ter illustratie: het goed kunnen samenwerken speelt vanaf het begin een rol, maar de manier waarop zich dat manifesteert en de mensen met wie je moet (kunnen) samenwerken veranderen wel naarmate een persoon zich in een meer seniore functie bevindt. Het niveau binnen een bouwsteen lijkt dus te variëren, terwijl het belang van de bouwstenen vrij stabiel lijkt te zijn.[16]

16. Deels kan dit ook een methodologische verklaring hebben. Sommige bouwstenen worden sneller expliciet benoemd in een vacature dan andere bouwstenen.

4.5.4 Sector

Voor de 5 sectoren waarin de meeste cybersecurity vacatures zijn gevonden zijn de meest gevonden bouwstenen getoond in supplementaire tabel 28. Op hoofdlijnen zijn er veel overeenkomsten, maar ook hier zijn verschillen in nuance. Zo lijkt er binnen de overheid relatief meer nadruk te liggen op bouwstenen met betrekking tot Management & Organisatie en Legal. Binnen de IT-sector ligt er niet onverwacht wat meer nadruk op technische vaardigheden.

4.5.5 Organisaties

De gevraagde bouwstenen kunnen ook op het niveau van individuele organisaties bekeken worden. Hieronder zijn drie voorbeelden gegeven: TNO, Secura en de ABN AMRO (figuur 36). Binnen de functies van TNO treffen we relatief veel bouwstenen m.b.t. Management & Organisatie aan in de top 10, terwijl we voor Secura relatief veel bouwstenen m.b.t. Techniek in de top 10 aantreffen.

Naam organisatie
TNO

Categorie
Kennisinstelling
Cyber R&D

#	Top 10 CS-functieprofielen	Vacatures 2018-2022
1	Crypto Specialist	22
2	Cyber Security Specialist	18
3	Onderzoeker Cyber Security	17
4	Scientist Cyber Security	14
5	Security Talent	12
6	Onderzoeker Crypto	12
7	Startfunctie	10
8	Onderzoeker	6
9	System Simulation Engineer	5
10	Researcher Cyber Security	5
	Overig	*157*
	Totaal	**278**

	starter	onbekend	1-3	3-5	5-10	>10	Totaal
WO	6	171	12	11	7	3	**210**
HBO		45	1	10	3		**59**
MBO	3	6					**9**
Totaal	**9**	**222**	**13**	**21**	**10**	**3**	**278**

	2018	2019	2020	2021	2022	Totaal
Totaal	55	25	25	82	91	**278**

	Fulltime	Fulltime,Parttime	onbekend	Parttime	Totaal
Totaal	134	6	68	70	**278**

#	Top 10 CS-competenties	Type	Categorie	Vacatures 2018-2022
1	Develop relationships with cybersecurity-related authorities and communiti	Main task(s)	Man. & Org.	151
	Motivate and encourage people	Key skill(s)	Man. & Org.	151
3	Cybersecurity controls and solutions	Key knowledge	Technisch	142
4	Cooperate and share information with authorities and professional groups	Main task(s)	Man. & Org.	139
5	Management practices	Key knowledge	Man. & Org.	132
6	Collaborate with other team members and colleagues	Key skill(s)	Man. & Org.	117
	Collaborate with other teams and colleagues	Main task(s)	Man. & Org.	117
8	Cybersecurity recommendations and best practices	Key knowledge	Man. & Org.	98
9	Cyber threats	Key knowledge	Technisch	94
10	Cybersecurity procedures	Key knowledge	Man. & Org.	90
	Totaal			**278**

Naam organisatie
Secura

Categorie
Bedrijf
Cyberproductie

#	Top 10 CS-functieprofielen	Vacatures 2018-2022
1	Information Security Consultant	19
2	IOT Security Expert	18
3	Auditor	14
4	Technical Security Specialist	13
5	Penetration Tester	12
6	Cloud Security Specialist	11
7	Consultant Security Awareness	10
8	Principal Security Expert	9
9	Information and Security Consultant	7
10	Ethical Hacker	7
	Overig	*131*
	Totaal	**251**

	starter	onbekend	1-3	3-5	5-10	Totaal
WO		28	3	7	1	**39**
HBO	12	94	5	41	54	**206**
MBO		4	2			**6**
Totaal	**12**	**126**	**10**	**48**	**55**	**251**

	2018	2019	2020	2021	2022	Totaal
Totaal	31	19	72	83	46	**251**

	Fulltime	Fulltime,Parttime	onbekend	Parttime	Totaal
Totaal	12	5	175	59	**251**

#	Top 10 CS-competenties	Type	Categorie	Vacatures 2018-2022
1	Motivate and encourage people	Key skill(s)	Man. & Org.	141
2	Cybersecurity risks	Key knowledge	Technisch	113
3	Identify, analyse and correlate cybersecurity events	Key skill(s)	Onderzoek	104
4	Cybersecurity standards, methodologies and frameworks	Key knowledge	Technisch	103
	Cyber threats	Key knowledge	Technisch	103
6	Cybersecurity-related technologies	Key knowledge	Technisch	89
7	Multidiscipline aspect of cybersecurity	Key knowledge	Man. & Org.	84
	Work on operating systems, servers, clouds and relevant infrastructures	Key skill(s)	Technisch	84
9	Cybersecurity controls and solutions	Key knowledge	Technisch	77
10	Cyber threat actors	Key knowledge	Technisch	69
	Totaal			**251**

Naam organisatie
ABN AMRO

Categorie
Bedrijf
Cyberintegratie

#	Top 10 CS-functieprofielen	Vacatures 2018-2022
1	IT Development Engineer	22
2	Technical IT-Auditor	20
3	Business Information Security Office	17
4	ABN IT Talent Programme	17
5	Information Security Officer	17
6	Compliance Advisor	16
7	Information Security Expert	11
8	Artificial Intelligence Translator	10
9	Analist	10
10	Global IT Talent Programme	10
	Overig	*620*
	Totaal	**770**

	starter	onbekend	5-10	3-5	1-3	>10	Totaal
WO	12	83	123	11	17	20	**266**
HBO	38	230	136	54	11	6	**475**
MBO	7	20				1	**28**
VWO		1					**1**
Totaal	**57**	**334**	**259**	**65**	**28**	**27**	**770**

	2018	2019	2020	2021	2022	Totaal
Totaal	141	113	120	164	232	**770**

	Fulltime	Fulltime,Parttime	onbekend	Parttime	Totaal
Totaal	230	23	239	278	**770**

#	Top 10 CS-competenties	Type	Categorie	Vacatures 2018-2022
1	Cybersecurity controls and solutions	Key knowledge	Technisch	263
2	Cyber threats	Key knowledge	Technisch	257
3	Develop relationships with cybersecurity-related authorities and communiti	Main task(s)	Man. & Org.	256
4	Identify, analyse and correlate cybersecurity events	Key skill(s)	Onderzoek	244
5	Cybersecurity risks	Key knowledge	Technisch	227
6	Work on operating systems, servers, clouds and relevant infrastructures	Key skill(s)	Technisch	224
7	Cybersecurity standards, methodologies and frameworks	Key knowledge	Technisch	210
8	Motivate and encourage people	Key skill(s)	Man. & Org.	179
9	Cooperate and share information with authorities and professional groups	Main task(s)	Man. & Org.	162
	Develop relationships with cybersecurity-related authorities and communiti	Main task(s)	Man. & Org.	162
	Totaal			**770**

Figuur 36: Voorbeelden van bouwstenen bij individuele organisaties. Bron: Jobdigger, bewerking Dialogic

4.5.6 Doelgroepen

Tot slot zijn de bouwstenen ook over de genoemde doelgroepen gesplitst, in dit geval gebaseerd op de top 100 organisaties die handmatig gelabeld zijn (zie supplementaire tabel 29). (Hierin vinden we binnen de 'cybersecurity waardeketen' relatief veel technische bouwstenen terug in de cyberproductie-en integratie. De technische bouwstenen vinden we relatief ook meer terug in het bedrijfsleven dan bij de overheid. Over de gehele linie zijn niet-technische vaardigheden, waaronder ook echte soft skills, belangrijk voor het uitoefenen van deze beroepen.

4.6 Uitstroom en instroom

Binnen dit onderzoekstraject hebben wij als onderzoekers opgemerkt dat men bij de groeiende vraag op de cybersecurity arbeidsmarkt met name de associatie heeft met de zogenaamde 'uitbreidingsvraag': de vraag die het resultaat is van additioneel uit te voeren werkzaamheden op de arbeidsmarkt in relatie tot cybersecurity. Hoewel deze uitbreidingsvraag ook uiterst relevant is voor de cybersecurity arbeidsmarkt, bestaat er tegelijkertijd ook een zogenaamde 'vervangingsvraag': de vraag die het resultaat is van uitstromende arbeidskrachten. Die uitstroom kan allerlei redenen hebben; denk bijvoorbeeld aan het switchen naar een ander (type) beroep, met pensioen gaan, emigreren naar het buitenland of het onverhoopt ziek of arbeidsongeschikt worden. Bij de aanvang van dit onderzoekstraject was er met name een interesse om te weten hoeveel cybersecurity professionals met pensioen gaan en/of emigreren naar het buitenland, om daarmee een beeld te krijgen van welke cybersecurity expertise we als Nederland 'verliezen'.

Het onderzoeken hiervan is niet triviaal en kent een aantal uitdagingen. De meest belangrijke uitdaging is dat er in Nederland niet wordt geregistreerd wie een 'cybersecurity professional' is. Bestaande beroepenindelingen zijn daarbij niet geschikt om goed zicht te krijgen op deze professionals[17]. Dat betekent dat we op een indirecte manier moeten inschatten welke mensen met een relatief hoge waarschijnlijkheid actief zijn als cybersecurity professional.

In eerder onderzoek naar de 'economische kansen van de cybersecuritysector' is een lijst van bedrijven opgesteld die onderdeel uitmaken van de cybersecuritysector. Het gaat dan specifiek om bedrijven die (ook) actief zijn als producenten van cybersecurityproducten (goederen/diensten), zie categorie B in figuur 12. De mensen die binnen deze bedrijven werken hebben een relatief hogere waarschijnlijkheid om cybersecurity professional te zijn. Daarbij weten we op basis van de vacature-analyse dat er bij het gros van de cybersecurity functies om een hbo- of wo-opleidingsniveau gevraagd wordt. **Van de analyses die we in deze sectie zullen presenteren vormen derhalve personen de basis die [1] een hbo- of wo-opleiding afgerond hebben en die [2] werkzaam zijn binnen bedrijven die (ook) als producent van cybersecurity goederen-en diensten actief zijn**. Hierbij dient dus opgemerkt te worden dat [i] veel van deze bedrijven ook niet- cybersecurity activiteiten ontplooien en dat [ii] er ook niet-cybersecurity professionals actief zijn binnen cybersecurity bedrijven. Hoewel dit dus geen waterdichte benadering is, is het gegeven de huidige informatie een pragmatische manier om enig inzicht in de dynamiek op de arbeidsmarkt voor cybersecurity professionals te krijgen. Op basis van gegevens beschikbaar binnen de CBS-microdata-omgeving zijn uitstroom-en instroomcijfers in kaart gebracht. De hier gepresenteerde uitkomsten hebben betrekking op 2021, omdat er voor het jaar 2022 minder gedetailleerde gegevens beschikbaar zijn. De cijfers kunnen dienen om de verwachte ordegroottes van in-en uitstroom van cybersecurity professionals te schatten in relatieve termen. *De absolute aantallen die hier genoemd worden staan niet gelijk aan het aantal cybersecurity professionals.*

17. In de publicatie ICT in beeld van het UWV (augustus 2023) lijkt een maatwerkopdracht gegeven te zijn aan het CBS, waarbij het CBS vermoedelijk de brondata van de Enquête Beroepsbevolking (EBB) specifiek heeft bewerkt. Deze informatie is voor de onderzoekers in dit traject niet beschikbaar. Voor de toekomst zou het interessant kunnen zijn om te verkennen of de ruwe data van de EBB gebruikt kan worden om meer zicht op cyberprofessionals te krijgen. Daarbij zou ook een bredere scope gebruikt kunnen/moeten worden als nu gedaan is om meer recht te doen aan de volledige bandbreedte van manifestaties van het begrip 'cybersecurity professional'.

Resultaten

De resultaten van de analyse zijn in twee infographics samengevat, zie figuur 37.
Op basis hiervan kunnen de volgende conclusies getrokken worden:

Huidige populatie

- De populatie cybersecurity professionals is relatief jong. Circa driekwart van de populatie is jonger dan 50 jaar. Naar verwachting zal er komende jaren relatief weinig vervangingsvraag vanwege pensioen zijn.
- Mannen zijn relatief 'oververtegenwoordigd'. Twee op de drie professionals in deze populatie is man. Een derde is vrouw.

Uitstroom

- In 2021 was er een uitstroom van bijna 25% van de populatie.
- Een klein deel van de populatie (0,4%) ging met pensioen (~2% van de uitstromers).
- Een klein deel van de populatie (0,4%) emigreerde (~2% van de uitstromers).
- Ongeveer driekwart van de uitstromers gaat werken bij een organisatie buiten de onderzoekspopulatie[18]. Dat wil niet zeggen dat ze een ander beroep gaan uitoefenen; ze kunnen ook hetzelfde beroep of een vergelijkbaar beroep uitoefenen bij een andere werkgever.
- Ongeveer 2,5% van de populatie maakte een switch naar een ander bedrijf binnen de populatie.

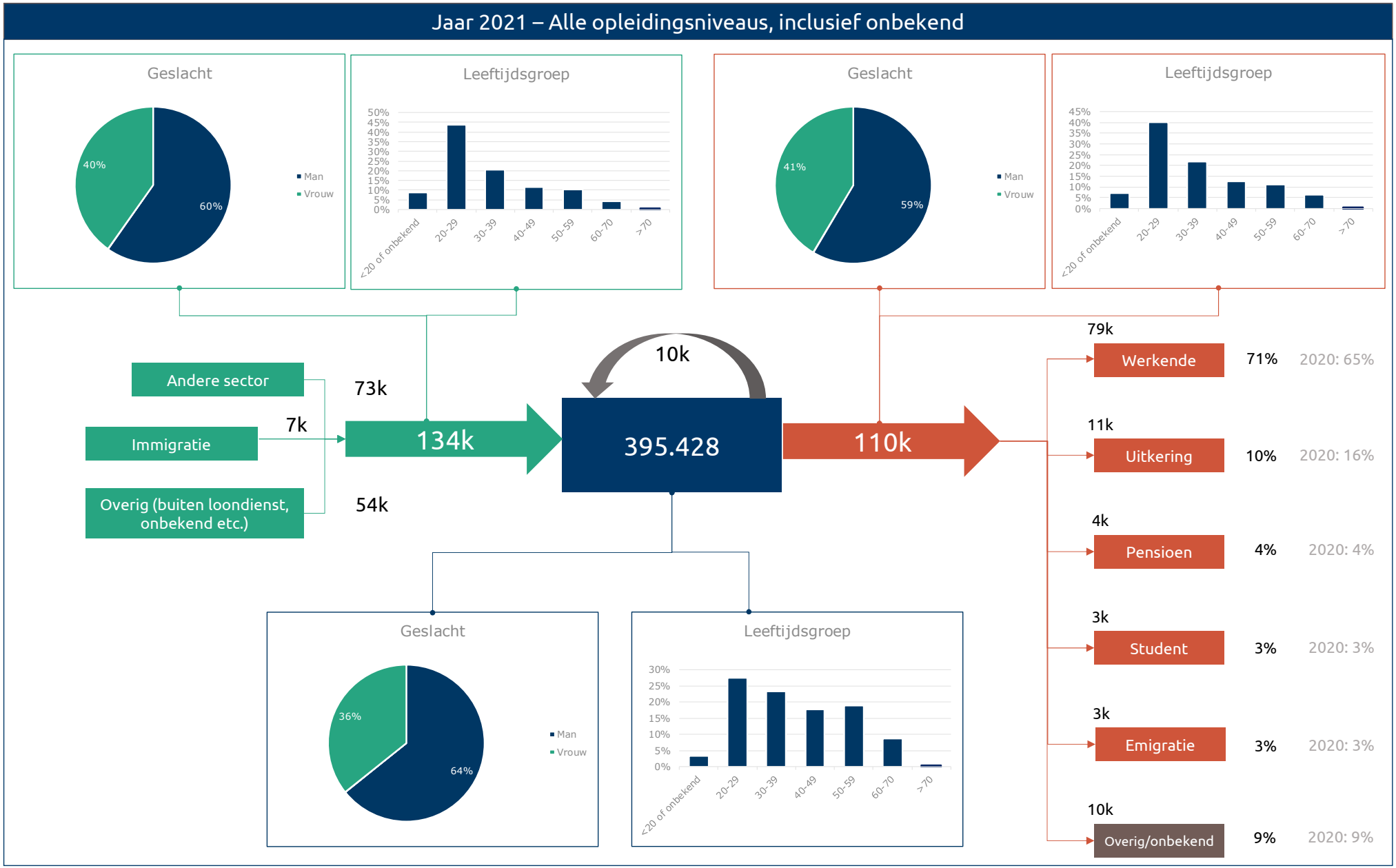
Instroom

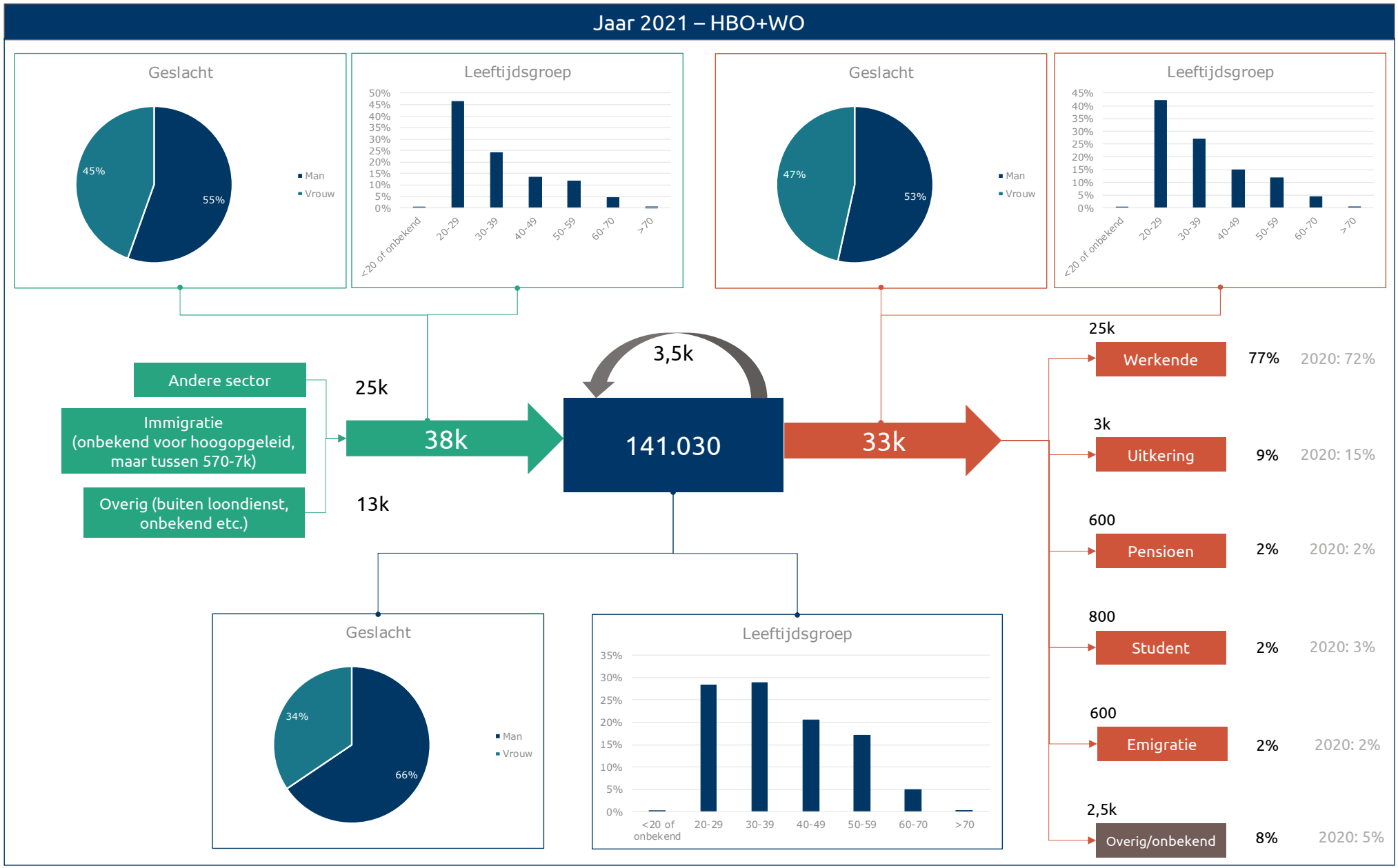
- Immigratie en arbeidsmigranten lijken belangrijk te zijn voor de sector. Ongeveer 5-10% van de instroom is toe te schrijven aan immigratie. Dit is in lijn met wat we bij de topsector ICT zien. Daar komt zelfs ~15% van de instroom uit immigratie. Ook daar is ~3% van de totale stock toe te schrijven aan immigratie in het desbetreffende jaar.
    - Bij immigranten is het doorgaans het geval dat het opleidingsniveau niet in Nederlandse registraties is opgenomen. Daardoor kunnen we voor deze doelgroep moeilijk aangeven wat het opleidingsniveau is. We weten wel dat er in 2021 ~7.000 immigranten deze populatie binnenkwamen, waarvan we voor 570 mensen wel weten dat ze hoogopgeleid zijn. Voor de andere ~6.500 is het onbekend.

Algemeen

- De instroom-en uitstroomcijfers fluctueren door de jaren heen. Dit kan verschillende oorzaken hebben. Hoewel dit niet direct uit de cijfers is op te maken, en dit niet nader onderzocht is in het huidige onderzoek, is het denkbaar dat de situatie m.b.t. COVID-19 hier een impact op heeft gehad.

18. De huidige onderzoekspopulatie betreft enkel organisaties in de categorieën cyber R&D, cyberproducenten en cyber integratie zoals beschreven in figuur 12: De cybersecuritysector en haar waardeketen. Bron: Dialogic (2023), De economische kansen van de cybersecuritysector. Voor meer informatie over de totstandkoming van deze onderzoekspopulatie: https://www.rijksoverheid.nl/documenten/rapporten/2023/04/06/de-economische-kansen-van-de-cybersecuritysector


Jaar 2021 – Alle opleidingsniveaus, inclusief onbekend
Geslacht
40%
60%
Man
Vrouw
Leeftijdsgroep
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
<20 of onbekend
20-29
30-39
40-49
50-59
60-70
>70
Geslacht
41%
59%
Man
Vrouw
Leeftijdsgroep
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
<20 of onbekend
20-29
30-39
40-49
50-59
60-70
>70
Andere sector
73k
Immigratie
7k
Overig (buiten loondienst, onbekend etc.)
54k
134k
10k
395.428
110k
79k
Werkende
71%
2020: 65%
11k
Uitkering
10%
2020: 16%
4k
Pensioen
4%
2020: 4%
3k
Student
3%
2020: 3%
3k
Emigratie
3%
2020: 3%
10k
Overig/onbekend
9%
2020: 9%
Geslacht
36%
64%
Man
Vrouw
Leeftijdsgroep
30%
25%
20%
15%
10%
5%
0%
<20 of onbekend
20-29
30-39
40-49
50-59
60-70
>70



Figuur 37: Uitstroom en instroom op basis van een populatie bedrijven die (ook) actief is in de cybersecuritysector. Bron: CBS-microdata, bewerking Dialogic

4.7 Relevante ontwikkelingen

Binnen dit onderzoek is aan betrokkenen gevraagd welke ontwikkelingen zij van belang achten voor de ontwikkeling in de vraag naar cybersecurity expertise. De meest genoemde ontwikkelingen zijn:

1. De intrede van de NIS2;
2. De intrede van de CRA;
3. Inzet van AI;
4. De wijze waarop organisaties hun benodigde cybersecurity expertise gaan organiseren (in-house en/of extern).

In deze sectie beschrijven we deze ontwikkelingen en lichten we toe hoe deze impact hebben op de vraag naar cybersecurity expertise, voor zover wij daar op basis van opgehaalde input, empirie en onderbouwing toe in staat zijn.

4.7.1 NIS2

De NIS2, de Network and Information Security directive, is de opvolger van de NIS-richtlijn.[19] De Europese versie hiervan is bekend, en wordt momenteel vertaald naar Nederlandse wetgeving. Het doel van de richtlijn is om "de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te vergroten". Binnen deze nieuwe richtlijn wordt de reikwijdte vergroot door meer sectoren te omvatten en worden strengere beveiligingsnormen en meldingsvereisten verplicht. De richtlijn heeft betrekking op organisaties die [1] in bepaalde sectoren actief zijn en [2] geclassificeerd kunnen worden als 'essentiële' of 'belangrijke' entiteit, zie ook de toelichting op de website van de NCTV.[20] Partijen die binnen deze nieuwe richtlijn vallen hebben een zorgplicht en een meldplicht en vallen onder toezicht.

In generieke zin wordt opgemerkt dat er met deze nieuwe wetgeving een impuls wordt gegeven aan 'wat men moet doen aan cybersecurity'. De verwachting is dat de impact van de NIS2 op de vraag naar cybersecurity expertise van organisaties verschilt tussen organisaties. Enerzijds is er een deel van de organisaties dat al veel doet op het gebied van cybersecurity en derhalve door de intrede van de NIS2 niet of beperkt extra inspanningen binnen de eigen organisatie moet plegen. Wel wordt opgemerkt dat grote partijen ook zorg moeten dragen voor cybersecurity binnen de keten. Ter illustratie: als een groot maakbedrijf een grote hoeveelheid mkb-toeleveranciers heeft, moeten die ook op niveau komen. Indien die toeleveranciers dat niet volledig zelf kunnen organiseren, kan er ondersteuning nodig zijn van grote partijen binnen de waardeketen c.q. het ecosysteem. Dus het feit dat een partij intern bezien zaken goed op orde zou hebben, wil nog niet zeggen dat deze partij geen gevolgen gaat ondervinden van de NIS2.

Anderzijds zullen er naar verwachting ook organisaties zijn die ook voor de interne aangelegenheden een tandje moeten bijzetten. De verwachting is dat met name organisaties die vooralsnog enkel de rol van 'cyber-eindgebruiker' innemen, en niet de rol van cyber R&D, cyberproductie of cyberintegrator, voor een relatief nieuwe uitdaging kunnen komen te staan. De partijen die op een meer specialistische manier met het onderwerp cybersecurity bezig zijn hebben een hoger maturiteitsniveau op het gebied van cybersecurity en begrijpen in de regel goed wat er speelt en wat er nodig is. Dat neemt niet weg dat ook zij het een uitdaging kunnen vinden, maar gezien de relatief grotere onervarenheid met cybersecurity van 'pure cybersecurity eindgebruikers' kan de transitie die zij moeten maken (vanwege de NIS2) ook relatief groter zijn.

Het werken aan cybersecurity lijkt volgens gesprekspartners vaak het proces te volgen dat er eerst één of enkele mensen aangesteld worden die het overzicht hebben en snappen wat er moet gebeuren. Dit kunnen bijvoorbeeld informatiemanagers, cybersecuritymanagers of CISO's zijn. Wanneer men scherp heeft wat er moet gebeuren, moet dat natuurlijk ook nog uitgevoerd worden. De vraag naar 'het plan uitvoeren' volgt daarmee op een natuurlijke manier de vraag naar 'het plan opstellen'. Men verwacht dat de NIS2 voor organisaties een impuls zal geven aan het (beter) opstellen van een strategie en plan, en dat zich dat ook zal vertalen naar een grotere vraag aan professionals die in de uitvoering actief zijn. Die uitvoering kan ook verschillende functieprofielen aannemen, van de Pentester tot de Cybersecurity Implementer, Cyber Incident Responder en de systeembeheerder.
Ook wordt genoemd dat nieuwe wetgeving ook vraagt om activiteiten op het gebied van compliance, toezicht en handhaving. In dat kader zullen er naar verwachting ook meer professionals benodigd zijn die zich bezighouden met bijvoorbeeld auditing-taken.

Men verwacht dus dat de NIS2 met haar zorgplicht, meldplicht en toezicht de vraag naar cybersecurity professionals in de breedte zal doen toenemen. De vervolgvraag is hoe die gevraagde expertise georganiseerd gaat worden binnen de economie. In welke mate gaan organisaties cybersecurity expertise in huis halen of organiseren ze dat extern via inhuur en inkoop en/of via samenwerkingsverbanden? Dit punt komt nader aan bod in 4.7.4.

19. Voor meer informatie, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/
20. https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen/wat-zijn-de-sectoren-en-criteria-die-bepalen-of-een-organisatie-onder-de-nis2-richtlijn-valt

4.7.2 CRA

Naast de NIS2 is ook de komst van de Cyber Resilience Act (CRA) een relevante ontwikkeling voor de vraag naar cybersecurity expertise. De CRA zorgt ervoor dat digitale producten die op de (Europese) markt komen voldoen aan strenge cybersecurity eisen. De belangrijkste punten van de CRA zoals beschreven op digitaleoverheid.nl[21]:

- "Er komen alleen digitale producten op de markt die voldoen aan de strengste beveiligingseisen.
- Fabrikanten worden verplicht gedurende de hele levensduur van de producten gratis veiligheidsupdates te leveren en digitale kwetsbaarheden en incidenten te melden.
- Niet-commerciële open source software is vrijgesteld.
- Fabrikanten krijgen voldoende tijd om de regels te implementeren."

De Europese Unie vermeldt hierbij dat de wetgeving in het begin van 2024 zijn intrede moet vinden. Daarbij: "manufacturers will have to apply the rules 36 months after their entry into force".[22] De wet zal de komende jaren dus een rol gaan spelen. In termen van het in dit rapport gebruikte conceptueel model van de cybersecurity waardeketen zal deze wet met name toezien op de 'integrators'. Enerzijds zullen er strengere eisen kunnen zijn voor partijen die zich nu al als cyberintegrator opstellen. Anderzijds zullen er ook partijen gedwongen worden om als cyberintegrator op te gaan treden, terwijl ze dat nu nog niet (voldoende) doen.

De verplichtingen die door de CRA worden opgelegd kunnen impact hebben op de gehele cybersecurity waardeketen. Partijen die sec als cyber-eindgebruiker functioneren zullen naar verwachting weinig impact van de CRA ondervinden op hun eigen vraag naar cybersecurity professionals. Partijen die echter in de integratie, maar ook productie en R&D zitten, zullen over de linie meer moeten gaan investeren in cybersecurity om alles op orde te krijgen en te houden.
Door de verplichtingen die door de CRA worden opgelegd zullen fabrikanten op een meer strategisch niveau moeten gaan voldoen aan de wet, en hun strategieën en plannen daarop moeten aanpassen. Dat vraagt onder meer om cybersecurity professionals met een integraal beeld op de bedrijfsvoering en de inpassing van cybersecurity daarbinnen. Op een meer tactisch en operationeel niveau zullen fabrikanten ook hun producten moeten gaan aanpassen om te voldoen aan de eisen. Dit vraagt op zijn beurt onder meer om meer mensen die cybersecurity ook technisch kunnen vormgeven en implementeren. Dat mondt uit in een grotere vraag naar cybersecurity professionals in de breedste zin van het woord, maar denk onder andere aan cybersecurity architecten en implementers.
Ook voor deze wetgeving geldt dat het de vraag naar professionals vergroot die bezig zijn met compliance, toezicht en handhaving. Dan is o.a. te denken aan meer auditors en legal & compliancy officers.

4.7.3 Inzet van AI

Eén van de meest genoemde relevante ontwikkelingen is de opkomst en inzet van kunstmatige/artificiële intelligentie, ook wel 'AI' genoemd. De term AI wordt door verschillende mensen op een andere manier geïnterpreteerd, maar in de basis verwijzen we hier naar (computer)systemen die in zekere zin een vorm van (menselijke) intelligentie vertonen. Met andere woorden: de computer kan [1] bestaande taken uitvoeren die wij nu als mensen uitvoeren en/of kan [2] nieuwe taken uitvoeren die wij als mens niet (kunnen) uitvoeren.

Drie belangrijke redenen voor de snelle ontwikkeling van AI zijn:

1. **Informatieverzameling**. Er worden meer data, de 'input' voor AI, gecreëerd op basis waarvan de AI moet leren en werken. Meer (bruikbare) data gaat ook gepaard met meer mogelijkheden om waarde uit die data te halen.
2. **Informatieverwerking**. De informatieverwerking wordt steeds krachtiger, zowel in termen van hardware (krachtigere computers, snellere processoren, beter werkgeheugen, …) als in software (betere algoritmen die in staat zijn om complexere taken uit te voeren).
3. **Toegankelijkheid**. Krachtige AI-modellen worden in toenemende mate toegankelijk voor een breder publiek. Centraal gehoste modellen (denk aan GPT-4 of DALL-E op dit moment) kunnen bijvoorbeeld eenvoudig aangeroepen worden en kunnen doorgaans middels een API relatief eenvoudig geïntegreerd worden in bredere werkprocessen.

De kansen én risico's van AI beperken zich niet tot een enkele sector; ook het cybersecuritydomein wordt geconfronteerd met kansen en risico's. Wanneer we kijken naar de kansen m.b.t. het arbeidsmarktvraagstuk lijken er een aantal cybersecurity taken te zijn waarbij AI een rol kan spelen. **In de basis gaat AI altijd over informatieverwerking**; het moeten dus taken zijn waarbij informatieverwerking centraal staat en de informatieverwerkingsvaardigheden zonder AI in principe bij mensen belegd zouden worden (of helemaal niet belegd zouden worden).
Voor de verschillende taken en vaardigheden is door de onderzoekers gelabeld of het gaat om informatieverwerking waarbij AI dus (vooralsnog wellicht enkel in theorie) een rol zou kunnen spelen. De resultaten zijn weergegeven in figuur 38. Uit de analyse komt naar voren dat er met name bij de relatief technisch georiënteerde ECSF-profielen veel potentie

21. https://www.digitaleoverheid.nl/nieuws/overeenstemming-eu-landen-over-cyber-resilience-act/
22. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

lijkt te zitten voor de inzet van AI. Het gaat dan om de Penetration Tester, Cyber Threat Intelligence Specialist, Digital Forensics Investigator en de Cyber Incident Responder.

		Key skills - potentie AI			Main tasks - potentie AI			Skills + tasks - potentie AI		
#	ECSF-profiel	Geen/weinig	Substantieel	% substantieel	Geen/weinig	Substantieel	% substantieel	Geen/weinig	Substantieel	% substantieel
1	Penetration Tester	3	8	73%	3	5	63%	6	13	68%
2	Cyber Threat Intelligence Specialist	3	7	70%	7	5	42%	10	12	55%
3	Digital Forensics Investigator	3	2	40%	3	3	50%	6	5	45%
4	Cyber Incident Responder	4	2	33%	6	5	45%	10	7	41%
5	Cybersecurity Implementer	5	2	29%	7	3	30%	12	5	29%
6	Cybersecurity Risk Manager	6		0%	4	4	50%	10	4	29%
7	Cybersecurity Architect	9	1	10%	8	4	33%	17	5	23%
8	Cybersecurity Auditor	5	3	38%	11	1	8%	16	4	20%
9	Cybersecurity Researcher	4	3	43%	12	0	0%	16	3	16%
10	Cyber Legal, Policy & Compliance Officer	8		0%	11	1	8%	19	1	5%
11	Chief Information Security Officer (CISO)	15	1	6%	14	0	0%	29	1	3%
12	Cybersecurity Educator	9		0%	8	0	0%	17	0	0%
	Totaal ECSF	**74**	**29**	**28%**	**94**	**31**	**25%**	**168**	**60**	**26%**

Figuur 38: Potentie van AI voor de verschillende ECSF-profielen. Bron: Dialogic

Het is dus goed denkbaar dat in de toekomst delen van het werk van deze functieprofielen door of samen met de AI uitgevoerd worden. Deels betekent dit dat bepaalde taken kunnen verdwijnen, maar ook dat nieuwe taken zullen ontstaan (bijv. het ontwikkelen en beheren van de AI) en nieuwe competenties benodigd zijn (bijv. kunnen omgaan met software waarin AI op een slimme manier is geïntegreerd). Op de arbeidsmarkt in brede zin hebben we gezien dat wanneer er voldoende nieuwe taken en specialismes gevraagd worden, dit vaak in een nieuw functieprofiel gegoten wordt. Zo worden er tegenwoordig bijv. AI engineers in de hoek van de hightech-industrie gevraagd en zijn privacy-officers (mede door de intrede van de AVG) een gemeengoed geworden; functies die een aantal jaren geleden nog niet op die manier bestonden. De (verdere) opkomst van 'AI Cyber Experts' is dan ook niet ondenkbaar, nog los van hoe deze groep professionals genoemd zal worden.

AI zal daarmee aan de ene kant ongetwijfeld de vraag naar bepaalde taken, kennis en vaardigheden reduceren (opdat we meer met minder mensen kunnen doen), maar zal tegelijkertijd ook tot nieuwe taken leiden en vragen om nieuwe kennis en vaardigheden.

De taken en vaardigheden binnen het ECSF die zich naar onze inschatting relatief goed lenen voor ondersteuning of invulling door AI worden in vacatures ook regelmatig expliciet gevraagd. In figuur 39 wordt hiervan een overzicht gegeven.

#	Bouwsteen	Aantal vacatures	% vacatures
	Main tasks		
1	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	1112	1,8%
2	Design and propose a secure architecture to implement the organisation's strategy	863	1,4%
3	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	657	1,1%
4	Identify, analyse and assess technical and organisational cybersecurity vulnerabilities	333	0,5%
5	Identify and document compliance gaps	309	0,5%
6	Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems	136	0,2%
7	Identify, recover, extract, document and analyse digital evidence	82	0,1%
8	Identify, analyse, mitigate and communicate cybersecurity incidents	67	0,1%
9	Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence	43	0,1%
10	Identification of threat landscape including attackers' profiles and estimation of attacks' potential	42	0,1%
	Key skill(s)		
1	Identify, analyse and correlate cybersecurity events	25562	41,9%
2	Develop codes, scripts and programmes	3619	5,9%
3	Develop code, scripts and programmes	3619	5,9%
4	Conduct ethical hacking	1225	2,0%
5	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	1131	1,9%
6	Identify and exploit vulnerabilities	1100	1,8%
7	Assess the security and performance of solutions	984	1,6%
8	Perform social engineering	818	1,3%
9	Review codes assess their security	788	1,3%
10	Conduct technical analysis and reporting	731	1,2%

Figuur 39: Vraag naar taken en vaardigheden waarin AI een rol zou kunnen spelen. Bron: Jobdigger, bewerking Dialogic

AI zal niet enkel via een 'interne' route impact gaan hebben op de manier waarop cybersecurity professionals hun werk kunnen uitvoeren, maar het zal ook via een 'externe' route impact hebben op hetgeen waartegen de cybersecurity professionals ons moeten of willen beschermen. Een bekend voorbeeld is AI en de opkomst van deep fakes, waardoor misdaden als laster en identiteitsfraude op nieuwe manieren mogelijk zijn geworden. Ook kan AI ertoe leiden dat meer digitale systemen verbonden zijn en slim samenwerken, waardoor de risico's van bijv. uitval groter worden, bepaalde systemen een groter doelwit worden en de roep om cybersecurity ook groter kan worden. Dit zijn slechts enkele voorbeelden, maar het illustreert wel dat AI zowel de wereld in brede zin beïnvloedt als specifiek het werk dat cybersecurity professionals uitvoeren.

4.7.4 'Make or buy'

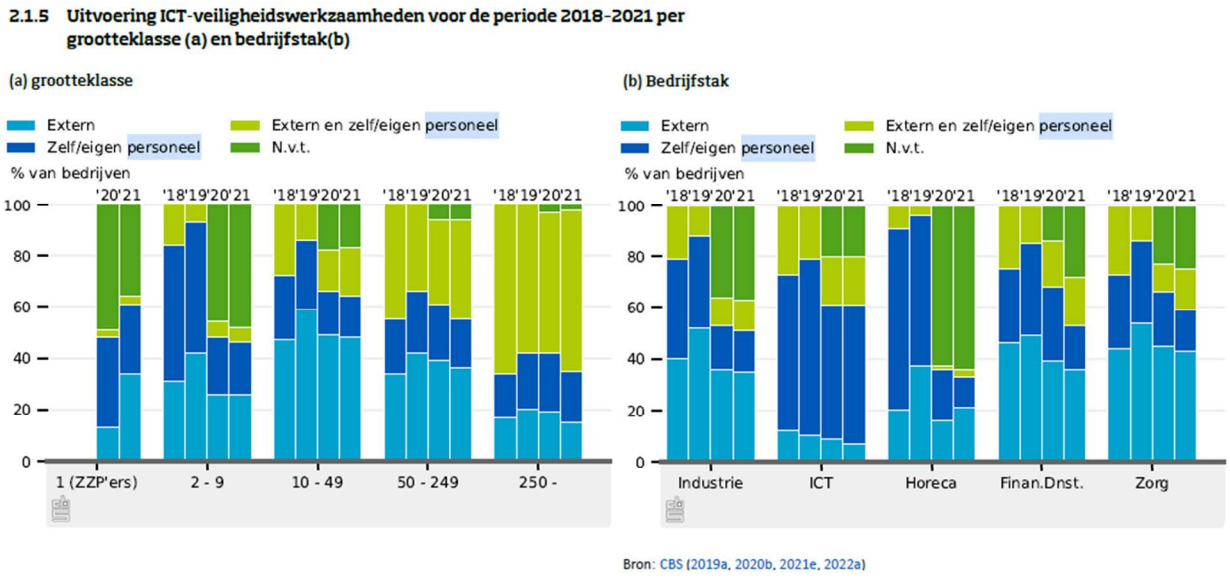
Een relevante ontwikkeling die binnen dit onderzoek meermaals is genoemd is de afweging die organisaties zullen gaan maken om benodigde cybersecurity expertise [1] in-house te organiseren of dit [2] extern te organiseren door bijv. inkoop of middels samenwerkingsverbanden. Men zou dit kunnen beschouwen als een 'make-or-buy' beslissing.
We zien veel situaties waarin bijvoorbeeld één FG of CISO voor meerdere organisaties actief is of waar via gezamenlijke regelingen bij gemeenten zorggedragen wordt voor de invulling van specialistische functies die de maturiteit en behoeften van individuele organisaties soms nog overstijgt. In andere woorden: aangenomen dat er sprake is van een groeiende toekomstige vraag naar cybersecurity expertise, is de vervolgvraag bij welke organisaties deze vraag zich op welke manier gaat manifesteren. Moet iedere organisatie zelf cybersecurity expertise in huis hebben en zo ja, welke expertise dan precies?

Het CBS heeft in de Cybersecuritymonitor (2022) aan bedrijven gevraagd hoe zij hun ICT-veiligheidswerkzaamheden uitvoeren. De resultaten zijn terug te vinden in figuur 40. Uit de resultaten blijkt dat kleine organisaties t/m negen personen relatief veel zelf doen of aangeven dat het voor hen niet relevant is. Voor grotere organisaties geldt op hoofdlijnen dat circa 20% het echt helemaal zelf regelt, en de overige 80% het óf volledig extern belegt of in samenwerking met externen oppakt. Daarbij geldt nog eens dat hoe groter de organisatie is, hoe vaker het in samenwerking met externe

partijen uitgevoerd wordt. Een belangrijke verklaring is dat de complexiteit en de risico's voor grote organisaties toenemen, en (nog) meer specialistische kennis, kunde en producten benodigd zijn om digitaal veilig te opereren.
In de vacaturedata zien we ook dat veel partijen die weinig bezig zijn met de ontwikkeling van cyber (R&D, productie, integratie) en veelal als cybereindgebruiker te maken hebben met het onderwerp, cybersecurity veelal beleggen bij professionals met een breder profiel. Dat kunnen bijvoorbeeld meer 'generieke' IT-professionals zijn die óók de cybersecurity regelen. De vraag is of toekomstige ontwikkelingen ertoe leiden dat deze groep organisaties meer specialistische cybersecurity profielen in huis gaat halen, of dat zij blijven werken met eigen 'hybride' professionals en/of het met externe partijen regelen. In generieke zin is binnen dit onderzoek naar voren gekomen dat deze organisaties allereerst wel bewust moeten zijn van wat de rol van cybersecurity is voor de organisatie in kwestie, en dat het aannemen van iemand die het overzicht heeft wel stap 1 is. Deze persoon kan vervolgens ook inschatten wat er extern ingehuurd/ingekocht moet worden en/of wat er intern moet gebeuren om aan de cybersecuritydoelen van de organisatie te voldoen.

Hoewel we als onderzoekers geen glazen bol hebben, verwachten wij op basis van de opgehaalde informatie dat:

- organisaties die marginaal met het onderwerp bezig zijn, waar cybersecurity een relatief kleine rol speelt, en die niet onder de NIS2 en/of CRA vallen vermoedelijk blijven kiezen voor de 'hybride' functies in combinatie met externe inhuur/inkoop.
- organisaties die marginaal met het onderwerp bezig zijn, maar die wel onder de NIS2 en/of CRA gaan vallen in ieder geval minimaal één specialistisch(er) cybersecurity profiel in dienst zullen hebben. Daarbij merken we dus op dat veel partijen die onder de wetgeving gaan vallen dergelijke professionals al in dienst hebben, en dat we geen goed zicht hebben op welke groep organisaties nu nog geen/weinig cybersecurity expertise in huis heeft maar dat straks wel moet hebben.



Figuur 40: Wijzen waarop bedrijven hun ICT-veiligheidswerkzaamheden uitvoeren. Bron: CBS, Cybersecuritymonitor 2022.

4.8 Conclusies

Op basis van de bevindingen ten aanzien van de arbeidsmarkt komen we tot de volgende conclusies:

Vraag naar cybersecurity professionals - algemeen

1. [4.3.1] **De vraag naar cybersecurity expertise groeit**, zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt.
2. [4.3.1] We schatten in dat er **circa 60.000-110.000 cybersecurity professionals op de arbeidsmarkt** actief zijn, waarvan 17.000-33.000 professionals met een specialistisch cybersecurityprofiel.
3. [4.3.2] **De vraag naar cybersecurity expertise is geconcentreerd in de Randstad** (Noord-Holland, Zuid-Holland, Utrecht)
4. [4.3.3] Het zwaartepunt in de vraag ligt bij **medior- en senior-functies waarvoor een hbo- of wo-opleidingsniveau** gevraagd wordt.
5. [4.3.4] De **overheid en de IT-sector** zijn de twee sectoren met de meeste vraag naar cybersecurity expertise.
6. [4.3.5] De **tien organisaties** met de meeste cybervacatures zijn de Politie, PWC, CGI, EY, Belastingdienst, ING, ABN AMRO, Capgemini, KPMG en het Ministerie van Defensie.
7. [4.3.6] **Organisaties die relatief meer doen met cybersecurity hebben ook meer vraag naar specialistische profielen**. Een groot deel van de vraag naar specialistische cybersecurity professionals ligt daarbij bij partijen die, naast de rol van cybereindgebruiker, ook de rol van producent en/of integrator hebben.

Vraag naar cybersecurity professionals - functieprofielen

8. [4.4.1] **De meest gevraagde functieprofielen** per type cybersecurityprofiel zijn:
   a. **ECSF**. [1] CISO, [2] Cybersecurity Implementer en [3] Cyber Threat Intelligence Specialist
   b. **'Cybersecurity – Hoog'**. [1] Cyber Security Consultant, [2] Functionaris (gegevensbescherming) en [3] Adviseur informatiebeveiliging
   c. **'Cybersecurity – Middel'**. [1] Privacy Officer, [2] Security Consultant en [3] Consultant
   d. **'Cybersecurity – Laag'**. [1] Systeembeheerder, [2] Auditor, [3] Functioneel Beheerder
9. [4.4.2] **De top provincies hebben meer specialistische cybersecurityprofielen** in de top 20 functieprofielen dan de provincies waar minder cybervacatures uitgezet zijn.
10. [4.4.3] **Voor veel cybersecurity profielen zijn er mogelijkheden om op juniorpositie aan de slag** te kunnen gaan, zij het met een gerichter takenpakket en minder verantwoordelijkheden.
11. [4.4.4] **Verschillende sectoren kennen verschillende manieren waarop cybersecurity expertise zich manifesteert.** Zo zien we bijvoorbeeld in de IT-sector ook veel vraag naar bredere IT-functies waar cybersecurity een onderdeel van uitmaakt, terwijl we binnen de overheid relatief veel adviseurs zien met een breder profiel waar cybersecurity onderdeel van uitmaakt.
12. [4.4.5] **Op organisatieniveau wordt pas echt duidelijk welke concrete vraag er is in specifieke contexten**. Uiteindelijk is de arbeidsmarkt een optelsom van individuele functies bij individuele organisaties. Om de vraag op detailniveau echt goed te begrijpen moet verder ingezoomd worden.
13. [4.4.6] **De vraag naar cybersecurity professionals verschilt tussen partijen die een andere rol hebben in de 'cybersecurity waardeketen'**. Zo heeft de cybersecuritysector zelf (de productie van cybersecuritygoederen en -diensten) een grote vraag naar specialistische cybersecurity profielen, wordt er in de Cyber R&D logischerwijs veel naar Cyber Researchers gevraagd.

Vraag naar cybersecurityprofessionals – taken, kennis en vaardigheden

14. [4.5.1] Over de linie is er relatief **veel technische kennis** vereist om actief te zijn binnen de cybersecurity, maar de benodigde **vaardigheden en uit te voeren taken** zijn daarentegen voor een groot deel **niet-technisch** van aard. De technische component weegt bij ECSF-profielen zwaarder dan bij de andere typen cybersecurity profielen.
15. [4.5.1] De vraag naar cybersecurity expertise en onderliggende bouwstenen kent een **sterke groei in absolute zin**, maar in relatieve zin is de **verhouding tussen verschillende typen kennis en vaardigheden stabiel**.
16. [4.5.1] **In 15% van de vacatures wordt expliciet gevraagd naar een cybersecurity certificaat**. De meest gevraagde certificaten zijn de CISSP, CISM, en CISA.
17. [4.5.1] **Binnen de specialistische cybersecurity profielen wordt vaak een certificaat gevraagd**; zo treffen we voor het CISO-profiel in 77% van de vacatures de vraag naar een certificaat aan en voor de Pentester is dat in 58% het geval.
18. [4.5.3] **De samenstelling van bouwstenen blijkt vrij stabiel** naarmate de functies meer werkervaring vereisen. Dit impliceert dat met name de concrete invulling van deze bouwstenen en de mate waarin personen in staat zijn deze kwalitatief invulling te geven groeit naarmate men zich verder ontwikkelt.

Uitstroom en instroom

19. [4.6] De **populatie cybersecurity professionals is relatief jong**. Circa driekwart van de populatie is jonger dan 50 jaar. Naar verwachting zal er komende jaren relatief weinig vervangingsvraag vanwege pensioen zijn.
20. [4.6] **Mannen zijn relatief 'oververtegenwoordigd'**. Twee op de drie professionals is man. Een derde is vrouw.
21. [4.6] **0,4% van de populatie ging met pensioen** (~2% van de uitstromers).
22. [4.6] **0,4% van de populatie emigreerde** (~2% van de uitstromers).
23. [4.6] **Immigratie / arbeidsmigranten lijken belangrijk te zijn voor de sector.** ~ 5-10% Van de instroom is toe te schrijven aan immigratie.

Relevante ontwikkelingen

24. [4.7.1] De verwachting is dat de **NIS2 met haar zorgplicht, meldplicht en toezicht de vraag naar cybersecurity professionals in de breedte zal doen toenemen**, van CISO's tot aan Implementers, Analisten, Auditors en Pentesters.
25. [4.7.2] De verwachting is dat de **CRA de vraag naar cybersecurity professionals in de breedte zal doen toenemen, met vermoedelijk de grootste impact voor de cyberintegrators**.
26. [4.7.3] Met de verdere **ontwikkeling en inzet van AI zal de vraag naar de uitvoering van bepaalde taken door mensen afnemen**, maar tegelijkertijd zullen er ook **nieuwe taken ontstaan** en zullen **nieuwe competenties** benodigd zijn. Binnen de ECSF-profielen zit de grootste potentie voor AI om delen van het werk te kunnen uitvoeren/ ondersteunen bij de Penetration Tester, Cyber Threat Intelligence Specialist en de Digital Forensics Investigator.
27. [4.7.4] **Organisaties die marginaal met cybersecurity bezig zijn, waar cybersecurity een relatief kleine rol speelt**, en die niet onder de NIS2 en/of CRA vallen zullen vermoedelijk blijven kiezen voor de **'hybride' functies in combinatie met externe inhuur/inkoop/organisatie** van cybersecurity expertise.

5. Aansluiting onderwijs- arbeidsmarkt

Onderzoeksvraag 6.
Maak inzichtelijk (kwantitatief en kwalitatief) welke discrepantie er zit tussen de vraag naar en het aanbod van cybersecurity expertise. Analyseer welke factoren deze discrepantie veroorzaken. Sta onder andere stil bij (ervaren) kwaliteitsverschillen tussen verschillende opleidingen en certificering.

Het idee dat onderwijs en (alle) concrete vacatures op de arbeidsmarkt perfect zouden kunnen matchen is een misconceptie, omdat er meerdere jaren en in verschillende contexten (werkomgeving, trainingen e.d.) bijgeleerd moet worden. In dit onderzoek is derhalve gekeken naar de vraag op de arbeidsmarkt naar junior functies en de aansluiting met de opleidingen.
Bij het hoger onderwijs zien we relatief te weinig hbo en wo-gediplomeerden met een specialistisch cybersecurity profiel afstuderen ten opzichte van de vraag op de arbeidsmarkt. Het aantal hbo en wo gediplomeerden dat een 'substantiële' component cybersecurity in de opleiding heeft gehad is echter op peil met de vraag. Net als de kwantitatieve vraag naar mbo cybersecurity junior personeel: deze is op peil met de uitstroom in de twee betreffende mbo-4-opleidingen.
Inhoudelijk gezien wordt er op de arbeidsmarkt veel gevraagd naar de competenties van het type 'Technisch' en 'Management & Organisatie'. Deze bouwstenen zien we ook terug bij de opleidingen met een specialisatierichting cybersecurity. De focus op 'legal' competenties vinden we met name terug bij de opleidingen waar cybersecurity geen specialisatierichting is. De competenties op het gebied van 'onderwijs' (bijv. lesgeven) zien we echter nergens terugkomen - niet bij de opleidingen en niet in de vacatures op juniorniveau.

Een grote opgave voor de cybersecurity arbeidsmarkt lijkt dus met name te liggen in het Leven Lang Ontwikkelen, bij zowel het aantrekken als het behouden van de (huidige) cybersecurity professionals.

Hierbij dient rekening gehouden te worden met het verschil tussen de functie waar iemand vandaan komt en de functie waar iemand bij in moet stromen. Dit verschil kan niet te groot zijn; er moet een 'overbrugbare stap' zijn. Het is zaak om secuur te kijken naar welke achtergronden voldoende basis hebben om de stap te overbruggen.
Hierbij kunnen certificaten een rol spelen: het belang van certificaten op de cybersecurity arbeidsmarkt is groot, met name bij de meer specialistische cybersecurity profielen. Deze certificaten en bijbehorende trainingen zijn een manier om de stap te overbruggen.
Daarnaast is het van belang de genoemde knelpunten in het onderwijs aan te pakken; de instroom van de reguliere opleidingen wordt hiermee kwantitatief en kwalitatief verbeterd om zo beter aan te sluiten op de vraag van de arbeidsmarkt.

5.1 Verbinding onderwijs en arbeidsmarkt

Er wordt vaak gesproken over 'de mismatch tussen onderwijs en arbeidsmarkt'. Als we kijken naar wat er in de praktijk gebeurt zouden we de twee concepten 'onderwijs' en 'arbeidsmarkt' nader moeten specificeren om zinnige uitspraken te doen over de aansluiting tussen de twee. Wanneer we naar het **regulier** onderwijs kijken, zouden we aan de kant van de arbeidsmarkt vooral moeten kijken naar de **juniorfuncties**; het is immers niet reëel om als net gediplomeerde een medior- of seniorfunctie te bekleden, uitzonderingen daargelaten. En als we wél kijken naar **medior- en seniorfuncties**, is het reëler om niet naar het regulier onderwijs te kijken, maar naar **Leven Lang Ontwikkelen** (bijscholing, learning on the job, private opleiders, etc.).

Hieronder zullen we eerst de relatie leggen tussen het regulier onderwijs enerzijds en de vacatures op de arbeidsmarkt anderzijds. Hierbij willen we vooraf een aantal kanttekeningen meegeven:

- Vacatures
  - **Vacatures zijn een proxy voor de vraag op de arbeidsmarkt, maar vacatures zijn niet gelijk aan de vraag.** Vacatures zijn één, weliswaar gangbare, manifestatievorm van de vraag. Organisaties kunnen ook mensen aannemen zonder ooit een vacature te hebben uitgezet (denk bijv. aan stagiaires die direct een arbeidscontract aangeboden krijgen na afronding van de stage).
  - **De vacaturedata die hier gebruikt worden zijn omvangrijk, maar niet 100% dekkend.** De data-aanbieder Jobdigger verzamelt vacatures van veel bronnen (vacatureplatforms, individuele websites van organisaties), er zullen echter ook vacatures in Nederland zijn die niet door hen geïdentificeerd zijn (bijv. offline vacatures op prikborden).
  - **Vacaturecijfers houden op zichzelf geen rekening met 'doorloop'**. In theorie zouden twee professionals iedere week elkaars functie kunnen overnemen. Als daar iedere week twee vacatures voor uitgezet zouden worden, zouden op jaarbasis twee professionals 104 vacatures invullen. Hoewel dit voorbeeld onrealistisch is, illustreert het wel dat een vacature niet zomaar gelijkgesteld kan worden aan de (permanente) vraag naar één professional.
- Onderwijs

  Het aantal behaalde diploma's is niet gelijk aan het aantal mensen dat een diploma behaald heeft, omdat één persoon meer dan één diploma kan behalen. De cijfers voor gediplomeerden worden opgeteld voor de geïdentificeerde opleidingen. Hierbij wordt geen rekening gehouden met het feit dat één persoon meerdere opleidingen kan volgen. Iemand met een bachelor-opleiding kan bijvoorbeeld nog een masteropleiding volgen, of een persoon met een mbo4-opleiding kan nog een hbo-opleiding volgen. Omdat voor gediplomeerden geldt dat het aantal behaalde opleidingen minimaal 1 is, en het aantal behaalde diploma's niet gelijk staat aan het aantal gediplomeerden, kan er een overschatting plaatsvinden van het aantal personen met minimaal één relevante behaalde cyberopleiding.
- Relatie onderwijs en arbeidsmarkt

  In de hieronder gepresenteerde analyses kijken we niet naar [1] de (zij-)instroom vanuit de arbeidsmarkt en de [2] instroom via arbeidsmigratie. Wanneer er dus een 'gap' zit tussen wat het reguliere onderwijs 'aflevert' en waar de arbeidsmarkt om vraagt, kan het zo zijn dat het verschil wordt ingevuld door deze twee bronnen.

5.2 Regulier onderwijs & juniorfuncties

Hieronder wordt eerst een kwantitatief beeld van de relatie tussen de vraag vanuit de arbeidsmarkt en het aanbod vanuit het regulier onderwijs gegeven. Daarna volgen nog enkele kwalitatieve reflecties.

Kwantitatief beeld

Uitgangspunten

Om de aansluiting tussen (regulier) onderwijs en arbeidsmarkt (juniorfuncties) in kaart te brengen hanteren we de volgende uitgangspunten:

- Vacatures
  - We kijken naar alle cybersecurity vacatures die in het jaar 2022 als 'juniorpositie' zijn aangemerkt.
  - Wanneer we naar juniorposities kijken, dan zijn dat naar verwachting functies waar je redelijkerwijs op kunt solliciteren als (net) gediplomeerde. Wel is het zo dat de 'junior-fase' zich doorgaans over meer dan één jaar strekt. Vaak wordt drie jaar genoemd als 'juniorfase'. In dat geval zou het eerlijker kunnen zijn om de totale vraag naar juniorfuncties te delen door 3 wanneer het gematcht zou worden met de jaarlijkse uitstroom uit het onderwijs.

- We houden daarbij rekening met opleidingsniveau, waarbij we ons focussen op hbo en wo, omdat het gros van de vraag naar cybersecurity expertise zich hier concentreert.
- We houden daarbij rekening met het type cybersecurity profiel (ECSF, CS – Hoog, CS – Middel, CS – Laag)

- Onderwijs
  - We kijken naar alle cybersecurity opleidingen die zich [1] volledig op cybersecurity focussen, [2] deels focussen op cybersecurity middels een specialisatierichting, of [3] deels focussen op cybersecurity middels een verplicht onderdeel van >6 EC.
  - We kijken daarbij naar de uitstroom (en instroom) in 2022, wat overeenkomt met het collegejaar 2021-2022.

Aansluiting regulier onderwijs en juniorfuncties op de arbeidsmarkt – hbo en wo

De relatie tussen onderwijs en arbeidsmarkt op hbo en wo-niveau laat zich op hoofdlijnen samenvatten door de volgende figuur 41:

Arbeidsmarkt en onderwijs hbo & wo - 2022

Vacatures		Uitstroom onderwijs		Instroom onderwijs	
Volledig CS		**Volledig CS**		**Volledig CS**	
Vacatures ECSF	845				
Vacatures CS - Hoog	295				
Vacatures volledig CS	1140	Gediplomeerden volledig CS	266	Instroom volledig CS	426
Deels CS		**Deels CS**		**Deels CS**	
Vacatures CS - Middel	481	Gediplomeerden deels CS (spcialisatie)	610	Instroom deels CS (spcialisatie)	706
Vacatures CS - Laag	2116	Gediplomeerden deels CS (onderdeel)	1409	Instroom deels CS (onderdeel)	1940
Vacatures deels CS	2597	Gediplomeerden totaal	2019	Instroom totaal	2646

Figuur 41: arbeidsmarkt en onderwijs hbo en wo 2022

We zien een vraag van 1.140 vacatures naar **specialistische cybersecurity profielen**, waarvan 845 gekoppeld zijn aan een ECSF-profiel. Kijken we naar de uitstroom uit het onderwijs dat zich volledig specialiseert in cybersecurity, dan waren dat er in 2022 slechts 266, waarbij zelfs aangenomen wordt dat ieder behaald diploma overeenkomt met een uniek persoon. Indien de vraag ~3 jaar aan juniorposities zou bestrijken en een deel van de vacatures dus ook van toepassing is op professionals die al (1 of 2 jaar) op de arbeidsmarkt actief zijn, zou dat overeenkomen met ~380 (1/3 van 1140) op jaarbasis. Ook in dat geval is er meer vraag vanuit de arbeidsmarkt dan wat het onderwijs momenteel aflevert. Wel zien we dat de instroom in 2022 op 426 ligt, en dat de instroom in het onderwijs de groei op de arbeidsmarkt wel volgt. **Op basis van deze cijfers lijkt het er echter wel op dat het onderwijs enigszins achterloopt, en dat meer aandacht voor instroom in en afronding van deze opleidingen gewenst is**. Zoals eerder benoemd kan de arbeidsmarkt via instroom vanuit de arbeidsmarkt en arbeidsmigratie ook aan de vraag voldoen, dus de hierboven **ingeschatte 'mismatch' wil niet direct zeggen dat er niet aan de vraag voldaan wordt**.

Voor de vacatures die betrekking hebben op **'deels cybersecurity'**, zien we in 2022 een vraag van 481 (CS – Middel) en 2.116 (CS – Laag) op de arbeidsmarkt. Dat zijn 2.597 vacatures in totaal. Ook hier geldt dat als deze vacatures betrekking zouden hebben op een tijdsperiode van drie jaar, dit overeenkomt met ~865 vacatures per jaar. Het onderwijs leverde in 2022 2.019 gediplomeerden af (610 met een specialisatierichting cybersecurity en 1.409 met een verplicht onderdeel cybersecurity > 6 EC). Hier **lijkt dus op hoofdlijnen te gelden dat het onderwijs in de pas loopt met de vraag op de arbeidsmarkt**. Ook voor deze opleidingen zien we een toename in instroom; een groei die we ook op de arbeidsmarkt terugzien.

Hoewel de bovenstaande cijfers met enige onzekerheid omgeven zijn, lijken we te kunnen stellen dat er **relatief te weinig gediplomeerden worden afgeleverd met een specialistisch cybersecurity profiel, maar dat het aantal gediplomeerden dat een 'substantiële' component cybersecurity in de opleiding heeft gehad op peil ligt**. Indien de gediplomeerden met een 'deels-cybersecurity opleiding' ook zouden solliciteren op de specialistische cybersecurity profielen, zou er vervolgens wel weer een tekort aan gediplomeerden in die categorie kunnen ontstaan. Om naar de verwachte (grotere) vraag in de toekomst te voldoen lijkt meer uitstroom bij zowel de specialistische opleidingen als de 'hybride' opleidingen gewenst.

Mbo

Per jaar studeren ongeveer 6000 mbo studenten af aan de betreffende 4 mbo opleidingen. De opleidingen software developer en expert IT systems & devices, hebben het grootste aandeel cybersecurity in hun opleiding. Derhalve hebben zij de meeste kans om de vacature-eisen te matchen. Aangezien we niet de uitstroomcijfers per opleiding hebben, maar wel de verhouding in 2022 van deze opleidingen ten opzichte van de andere 2 kwalificatiedossiers is het onze inschatting dat ongeveer 75% van de uitstroom vanuit deze opleidingen komt.
Hierbij lijkt het aannemelijk dat de **kwantitatieve vraag naar mbo cybersecurity junior personeel (733) kan worden beantwoord door de uitstroom in het mbo (75% van de totale uitstroom= 4500)**.

Kwalitatief beeld: heterogeniteit in de specialistische profielen

Om het overzicht te bewaren is hierboven het onderscheid gemaakt tussen specialistische cybersecurity profielen en de deels-cybersecurity profielen. Er is echter nog sprake van heterogeniteit in de specialistische profielen. Hieronder hebben we de vraag in 2022 uiteengezet naar 'typen' competenties die gekoppeld zijn aan de verschillende specialistische ECSF-profielen. Alle bouwstenen (taken, kennis en vaardigheden) binnen de beschreven ECSF-profielen zijn voorzien van een 'type', waarbij een inschatting is gemaakt van het primaire type waartoe een bouwsteen behoort (figuur 42). Dit is geen exacte wiskunde, en de percentages moeten niet tot op de komma gelezen worden, maar de inschatting geeft wel een grof beeld van een verschillende focus binnen de verschillende profielen.

	2022 - Junior - vacatures				Bouwstenen					
ECSF-profiel	WO	HBO	MBO	Totaal	Legal	M&O	Onderwijs	Onderzoek	Technisch	Totaal
Cybersecurity Researcher	33	6	0	39	8%	20%	4%	56%	12%	100%
Digital Forensics Investigator	9	7	0	16	4%	12%	0%	15%	69%	100%
Cyber Threat Intelligence Specialist	6	83	15	104	3%	30%	0%	11%	57%	100%
Penetration Tester	4	71	1	76	0%	15%	0%	9%	76%	100%
Cybersecurity Risk Manager	1	61	11	73	0%	38%	0%	8%	54%	100%
Cybersecurity Educator	0	2	0	2	4%	15%	63%	7%	11%	100%
Cyber Incident Responder	0	13	1	14	6%	25%	0%	3%	66%	100%
Cyber Legal, Policy & Compliance Officer	2	15	0	17	56%	33%	4%	4%	4%	100%
CISO	28	167	9	204	5%	86%	2%	2%	5%	100%
Cybersecurity Architect	4	51	2	57	5%	24%	0%	0%	71%	100%
Cybersecurity Implementer	22	225	66	313	0%	17%	0%	0%	83%	100%
Cybersecurity Auditor	9	26	1	36	7%	23%	0%	0%	70%	100%
Totaal	118	727	106	951	8%	30%	5%	9%	48%	100%

CS - Hoog	52	243	10	305	-	-	-	-	-	-
CS - Middel	93	388	56	537	-	-	-	-	-	-
CS - Laag	388	1728	455	2571	-	-	-	-	-	-
Totaal	651	3086	627	4364						

Figuur 42: bouwstenen binnen de junior vacatures 2022

Zo zien we dat sommige profielen meer leunen op technische kennis en kunde, zoals de Cybersecurity Implementer en de Penetration Tester. Andere functies leunen meer op kennis en kunde op het gebied van Management & Organisatie, zoals de CISO en de Cyber Risk Manager.

De mate waarin deze bouwstenen in diverse opleidingen naar voren komen verschilt. Voor de volledige cybersecurity opleidingen is voor het gemak aangenomen dat zij redelijkerwijs op de juniorpositie van alle ECSF-profielen zouden moeten kunnen solliciteren en dat de ontbrekende kennis binnen de functie opgedaan kan worden. We zijn ons er van bewust dat dit niet in alle gevallen op zal gaan.

Alle ‘deels-cybersecurity opleidingen’ zijn gelabeld aan de hand van hoeveel aandacht er is voor de vijf typen competenties: 0 (geen aandacht), 1 (enige aandacht), 2 (substantieel aandacht) of 3 (primaire focus). Hieronder is een overzicht gegeven van het aantal gediplomeerden dat binnen de opleiding minimaal substantiële aandacht (dus score 2 of 3) voor het type competentie heeft gehad (figuur 43):

	2021-2022					
	Totaal		Hbo		Wo	
	Uitstroom	Instroom	Uitstroom	Instroom	Uitstroom	Instroom
1. Volledig CS	266	426	43	94	223	332
2. Deels CS - specialisatierichting	610	706	389	387	221	319
- waarvan substantiële aandacht voor 'Technisch' (>=2)	421	443	354	352	67	91
- waarvan substantiële aandacht voor 'M&O' (>=2)	240	312	86	84	154	228
- waarvan substantiële aandacht voor 'Legal' (>=2)	35	35	35	35	0	0
- waarvan substantiële aandacht voor 'Onderzoek' (>=2)	221	319	0	0	221	319
- waarvan substantiële aandacht voor 'Onderwijs' (>=2)	0	0	0	0	0	0
3. Deels CS - Verplicht onderdeel > 6EC	1409	1940	785	1079	624	861
- waarvan substantiële aandacht voor 'Technisch' (>=2)	514	742	140	164	374	578
- waarvan substantiële aandacht voor 'M&O' (>=2)	924	1206	730	983	194	223
- waarvan substantiële aandacht voor 'Legal' (>=2)	619	784	369	501	250	283
- waarvan substantiële aandacht voor 'Onderzoek' (>=2)	541	704	0	0	541	704
- waarvan substantiële aandacht voor 'Onderwijs' (>=2)	0	0	0	0	0	0

Figuur 43: in en uitstroom per categorie cybersecurity opleiding (volledig- specialisatie- verplicht onderdeel)

Op de arbeidsmarkt wordt veel gevraagd naar de competenties van het type ‘Technisch’ en ‘Management & Organisatie’. Dit is ook het geval bij de opleidingen met een specialisatierichting cybersecurity. De focus op ‘legal’ vinden we met name terug bij de opleidingen waar cybersecurity geen specialisatierichting is, en de focus op competenties op het gebied van ‘onderwijzen’ zien we nergens terug. Op de arbeidsmarkt zien we in principe ook geen vraag naar ‘Cyber Educators’ op juniorniveau terug, dus dit lijkt geen enkel probleem te zijn. Het opleiden en trainen van andere mensen op het gebied van cybersecurity is daarmee wel een competentie die mensen pas eenmaal op de arbeidsmarkt lijken te ontwikkelen.
Een algemeen aandachtspunt is de mate waarin men na het afronden van een opleiding nog betrekkelijk eenvoudig bijgeschoold kan worden in de juniorfunctie. Als het gat te groot is, kan de organisatie in kwestie de gediplomeerde niet meer aannemen. Deze kwalitatieve mismatch is lastig te vangen in vacature-aantallen en cijfers over gediplomeerden.

5.3 Medior-/ senior functies

Voor medior- en seniorfuncties kunnen we niet simpelweg meer kijken naar de uitstroom uit het regulier onderwijs. Voor deze categorie moeten we met name kijken naar facetten als learning-on-the-job, autonoom leren, en private bij- en omscholing.

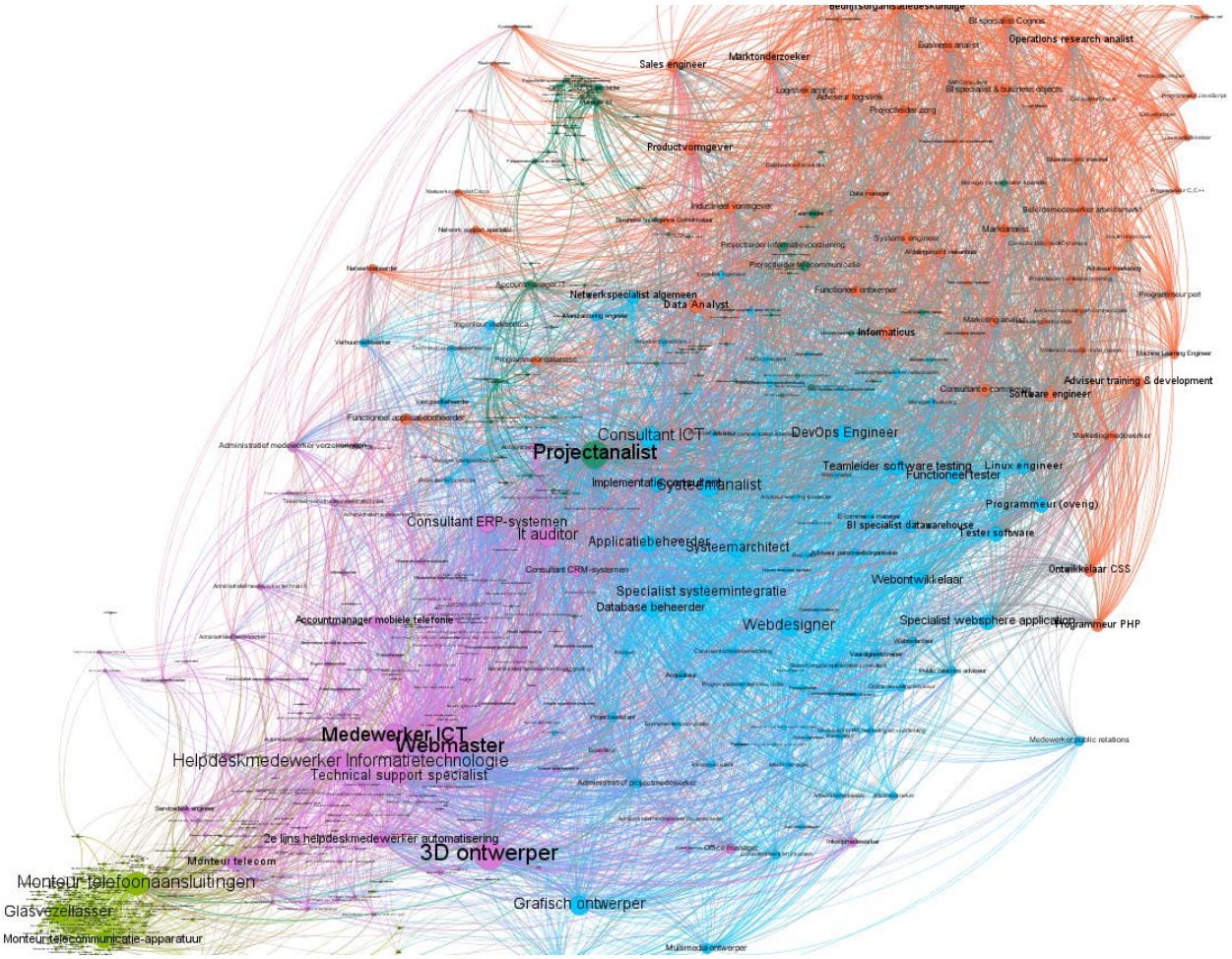
Voor deze functies dienen we derhalve met name te kijken naar de professionals die al op de arbeidsmarkt actief zijn en die voldoende basis hebben om in te stromen in de desbetreffende medior- of seniorfunctie. Voor medioren zullen dit vaak junioren zijn ‘binnen hetzelfde profiel’ (verticale ontwikkeling) of zij-instromers die op een deel van de benodigde competenties zich al goed ontwikkeld hebben. Voor seniorfuncties geldt in algemene zin hetzelfde, waarbij er instroom/ doorstroom is vanuit mediorfuncties met een vergelijkbaar profile of zij-instromers (bijv. goede managers die hun focus verleggen naar het cybersecurity domein).

Voor de cybersecurity arbeidsmarkt op medior- en seniorniveau is het met name belangrijk om aandacht te hebben voor de ontwikkelpaden. Vanuit welke positie kan iemand bij de medior-of seniorpositie in kwestie instromen? Het verschil tussen de functie waar iemand vandaan komt en de functie waar iemand in moet stromen kan niet te groot zijn; er moet een ‘overbrugbare gap’ zijn. De ‘gap’ tussen twee functies hangt af van de kennis en kunde (en benodigde persoonlijkheid) in de volle breedte.

Ter illustratie kunnen we kijken naar een gesimplificeerd voorbeeld m.b.t. het CISO-profiel waar het gaat om twee componenten: [1] managementvaardigheden én [2] (technische) kennis over cybersecurity. De volgende scenario's kunnen zich in dit gesimplificeerde voorbeeld voordoen:

- Als iemand beide componenten beheerst, komt de persoon direct in aanmerking.
- Als iemand beide componenten mist, zal de gap te groot zijn.
- Als iemand wél de kennis over cybersecurity heeft, maar geen/onvoldoende managementvaardigheden is de vraag of iemand de managementvaardigheden kan aanleren/ontwikkelen. Voor sommige mensen zal dit op natuurlijke wijze al aanwezig zijn, voor sommigen is het te ontwikkelen, en voor anderen zal dit nooit een competentie zijn waar ze voldoende goed in worden.
- Als iemand niet de kennis over cybersecurity heeft, maar wel voldoende managementvaardigheden heeft, is de vraag of die persoon binnen afzienbare tijd voldoende kennis over cybersecurity kan opdoen om de functie te vervullen. Zoals we in Hoofdstuk 4 hebben gezien is een groot deel van het taken- en vaardighedenpakket van een CISO niet technisch van aard. Wie geschikt kan zijn voor de overstap zal vermoedelijk afhangen van hoe groot de 'gap' is voor deze persoon.

Dit principe van overbrugbare afstanden kan men ook projecteren op cybersecurity beroepen. Voor ICT-beroepen in generieke zin is onderstaande visualisatie gemaakt, waarin twee beroepen zijn verbonden met een lijntje wanneer de gap overbrugbaar is (figuur 44). Wanneer ingezoomd wordt op profielen, wordt snel duidelijk dat men niet van alle beroepen A kan doorstromen naar beroepen B. Wanneer de instroom voor een bepaald cybersecurity profiel op medior- of seniorniveau vergroot moet worden, is het zaak om secuur te kijken naar welke achtergronden voldoende basis hebben om de gap te overbruggen.



Figuur 44: Overstapberoepen, geredeneerd vanuit het beroep van bestemming (een ICT-beroep). Bron: pr-eDICT, data aangeleverd door CentERdata. Bewerking door Dialogic

Zoals in Hoofdstuk 3 beschreven is er veel LLO-aanbod. Daarbij is het belang van certificaten op de cybersecurity arbeidsmarkt groot, met name bij de meer specialistische cybersecurity profielen. Deze certificaten en bijbehorende trainingen zijn een manier om de gap te overbruggen.

5.4 Conclusie

Ter afsluiting van dit onderzoek en dit hoofdstuk beschrijven we de volgende conclusies:

Startersfuncties:

- Er zit voor veel functies een gap tussen wat gevraagd wordt en hoe mensen de 'opleidingsbanken' uitkomen. Er zijn veel niet-startersfuncties. Die gap moet overbrugd worden. **Het idee dat onderwijs en (alle) concrete vacatures op de arbeidsmarkt perfect zouden kunnen matchen is een misconceptie**, omdat er meerdere jaren en in andere contexten bijgeleerd moet worden.
- Er zijn **relatief te weinig hbo en wo-gediplomeerden met een specialistisch cybersecurity profiel**.
- Het aantal gediplomeerden dat een **'substantiële' component cybersecurity in de opleiding heeft gehad is op peil** met de vraag.
- De kwantitatieve vraag naar **mbo cybersecurity junior personeel is op peil met de uitstroom** in de twee betreffende mbo 4-opleidingen.
- Op de arbeidsmarkt wordt veel gevraagd naar de **competenties van het type 'Technisch' en 'Management & Organisatie'**. Deze bouwstenen zien we ook terug bij de opleidingen met een specialisatierichting cybersecurity.
- **De focus op 'legal'** vinden we met name terug bij de opleidingen waar cybersecurity geen specialisatierichting is.
- De focus op **competenties op het gebied van 'onderwijzen' zien we nergens terug** – niet bij de opleidingen en niet in de vacatures op juniorniveau.

Medior-/ seniorfuncties:

- Het is relevant om mensen met een goede basis de arbeidsmarkt op te sturen, maar **een groot vraagstuk voor cybersecurity lijkt dus met name te liggen in LLO**.
- Het verschil tussen de functie waar iemand vandaan komt en de functie waar iemand in moet stromen kan niet te groot zijn; er moet een 'overbrugbare gap' zijn. Het is zaak om secuur te kijken naar **welke achtergronden voldoende basis hebben om de gap te overbruggen**.
- Het belang van certificaten op cybersecurity arbeidsmarkt is groot, met name bij de meer specialistische cybersecurity profielen. Deze **certificaten en bijbehorende trainingen zijn een manier om de gap te overbruggen**.

5.5 Aandachtspunten voor vervolg

Met de afronding van het beantwoorden van de onderzoeksvragen 1 tot en met 8 hebben we een beeld gekregen van de vraag- en aanbod kant van de cybersecurity arbeidsmarkt. Richting het advies spelen o.a. de volgende zaken mee:

Onderwijs:

- De regionale verschillen t.a.v. de arbeidsmarktvraag zijn groot: op welke manier is dit van invloed op het opleidingsaanbod? Wordt dit meegenomen, en zo ja hoe?
- We zien een behoefte aan verschillende typen profielen: van het hybride/ multidisciplinaire profiel tot het cyberspecialistische profiel. Hoe verhoudt deze behoefte zich tot het huidige en toekomstige aanbod van de opleidingen? Hoe ga je als opleidingen hiermee om?

Arbeidsmarkt:

- Bedrijven die zich niet bewust zijn van de (toekomstige) risico's, hebben momenteel nog geen vraag. Dit kan een grote latente vraag betekenen. Hierbij is er sprake van een verschil tussen need and demand.
- Er is sprake van een ketenafhankelijkheid door toeleveranciers; grote bedrijven hebben daarmee ook een verantwoordelijkheid om de kleinere bedrijven mee te krijgen.
- Veel vacatures komen van de grote bedrijven - de kleine(re) bedrijven lijken het zich nog niet helemaal bewust te zijn, hebben minder nodig en een andere vraag. Hierbij zal het relatief vaak gaan om hybride functies. Hoe zorgen we voor veel mensen op de arbeidsmarkt met een bredere scope?
- De regionale verschillen op de arbeidsmarkt zorgen voor een geconcentreerde vraag: wat betekenen de regionale verschillen voor de in te zetten beleidsinstrumenten?

Internationaal:

- Arbeidsmigratie: 5-15% van de instroom bestaan uit arbeidsmigranten. Wat kunnen we aan beleidsinstrumenten inzetten in een scenario met veel/weinig arbeidsmigratie?
- Deze vraag geldt ook voor de cybersecurity opleidingen: wat kunnen we aan beleidsinstrumenten inzetten in een scenario met veel/weinig arbeidsmigratie?

Toekomstige ontwikkelingen:

- De verwachte gevolgen van de komst van bijv. NIS2 op de arbeidsmarkt zijn besproken in Hoofdstuk 4. De implicaties van deze nieuwe wetgeving zijn nog onbekend op organisatieniveau. De omvang van deze verwachte groei is lastig in te schatten: hoe gaan we hiermee om?

Aansluiting onderwijs - juniorfunctie:

- Hoe bereiden we studenten voor op een juniorfunctie binnen de cybersecurity, bijv.:
  a. door na de opleiding mee te lopen met bepaalde taakverantwoordelijkheid, zoals een implementer;
  b. Inrichten van traineeships;
  c. In het onderwijs meer werkplekleren opnemen, zodat studenten die extra vaardigheden kunnen ontwikkelen die niet per se technisch van aard zijn, maar meer te maken hebben met kunnen samenwerken, de link kunnen leggen tussen inhoud en de organisatie-context etc.;
  d. In het reguliere onderwijs al de meest gevraagde certificaten op te nemen.

6. Tot slot: hoe komen we tot een advies?

6.1 Inleiding

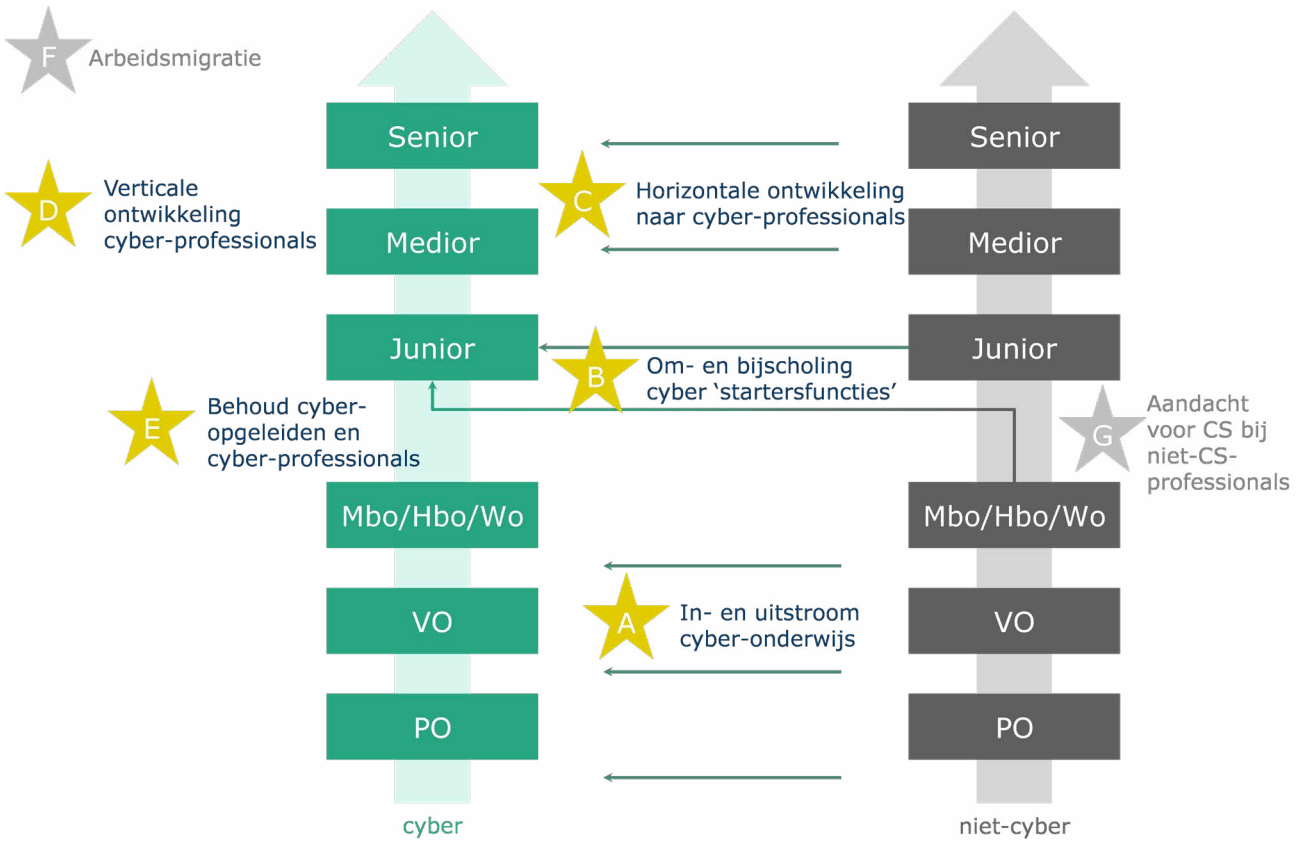
Bovenstaande rapportage levert veel en rijke input op waarmee weer een dieper inzicht is verkregen in de mate waarin onderwijs en arbeidsmarkt op het gebied van cybersecurity op elkaar aansluiten en welke bewegingen we zien op de arbeidsmarkt. Deze informatie biedt een goed overzicht van de afgelopen 5 jaren en de huidige situatie en is daarmee een belangrijk vertrekpunt voor verdere beleidsadviezen. In dit hoofdstuk wordt alvast een vooruitblik gegeven op de totstandkoming van het advies met bijbehorend implementatieplan.

6.2 Aanpak en conceptueel kader voor advies

Tijdens meerdere bijeenkomsten in januari 2024 wordt er met diverse stakeholders vanuit onderwijs, bedrijfsleven en partijen betrokken bij Human Capital-activiteiten besproken welke (beleids-) instrumenten er op basis van deze uitkomsten ingezet kunnen worden en op welke manier en door wie deze uitgevoerd dienen te worden.

Hiervoor maken we gebruik van onderstaand conceptueel kader (figuur 45) dat een beeld geeft van de totale onderwijs-arbeidsmarkt keten. De meest cruciale punten om aandacht aan te besteden zijn:

A. In- en uitstroom in het cybersecurity onderwijs: wat kunnen we doen om meer leerlingen te interesseren voor een opleiding op het gebied van cybersecurity en ze de juiste skills en kennis mee te geven zodat ze worden opgeleid passend bij de vraag naar juniorfuncties op de arbeidsmarkt?
B. Om- en bijscholing voor cybersecurity ‘startersfuncties’: wat kunnen we doen om net afgestudeerden van een niet-cyber-gerelateerde opleiding om en bij te scholen zodat ze beschikbaar zijn voor een cyberfunctie? Met welke opleidingsachtergrond is dit het meest kansrijk?
C. Horizontale ontwikkeling naar cybersecurity professionals: hoe kunnen we medior en senior professionals in een niet-cyberfunctie om- en bijscholen naar een cyberfunctie? Bij welke functies is dit het meest kansrijk en wat is hier voor nodig?
D. Verticale ontwikkeling cybersecurity professionals: hoe kunnen we de keten van junior naar medior naar senior functies zo goed mogelijk laten doorstromen zodat professionals doorgroeien?
E. Behouden cybersecurity opgeleiden en cybersecurity professionals: wat is er nodig om de uitstroom zo klein mogelijk te houden en professionals te behouden voor de cybersecurity arbeidsmarkt?
F. Arbeidsmigratie: hoeveel cyberprofessionals komen vanuit het buitenland in NL werken? Maar ook hoeveel cyberprofessionals uit Nederland verlaten NL om in het buitenland te gaan werken? Wat kunnen en willen we met de relatief grote internationale instroom op de cybersecurity arbeidsmarkt?
G. Aandacht voor cybersecurity bij niet-cybersecurity professional: hoeveel aandacht voor cybersecurity is er bij niet-cybersecurity professionals? Kunnen we dit vergroten en wat betekent dat voor de totale arbeidsmarktketen?



Figuur 45: Conceptueel kader dat een beeld geeft van de totale onderwijs-arbeidsmarktketen

Tijdens de volgende fase van dit onderzoek gaan we met diverse stakeholders bovenstaande cruciale punten bespreken en op basis van de output van de onderzoeksvragen 1 t/m 8 de in te zetten (beleids-) instrumenten bepalen.
Voor een gedetailleerde aanpak en uitwerking van het advies, incl. implementatie verwijzen we naar het tweede deel van dit onderzoek: het adviesrapport.

Contactinformatie

Sonja Kleter, Dialogic
Wazir Sahebali, Dialogic
Manon Schrijnemaekers, PTvT
Marion Sieh, PTvT
Arthur Vankan, Dialogic
Jasper Veldman, Dialogic
Loes Willems, PTvT

Contactpersoon Platform Talent voor Technologie:
Marion Sieh
m.sieh@ptvt.nl

Contactpersoon Dialogic:
Arthur Vankan
vankan@dialogic.nl

Postadres:
Platform Talent voor Technologie
Postbus 76
2501 CB Den Haag

Bezoekadres:
Oranjebuitensingel 6 (4e etage)
2511 VE Den Haag

©PTvT, januari 2024

Bijlagen

Bijlage 1.
Methodologische verantwoording arbeidsmarkt

In deze bijlage worden de methodologische keuzes voor het in kaart brengen van de 'cybersecurity arbeidsmarkt' sector toegelicht.

Identificatie van cybersecurity vacatures

De vacatures, die zijn doorzocht zijn ingekocht bij Jobdigger. De analyse van de 'cybersecurity arbeidsmarkt' is gebaseerd op zowel vacatures in de ICT-sector, zoals gedefinieerd op pr-edict, als vacatures buiten de ICT-sector. Het is noodzakelijk om ook buiten de ICT-sector te kijken omdat de cybersecurity sector een sterk multidisciplinair karakter heeft. Het is daarom aannemelijk dat cybersecurity functies ook in andere sectoren worden gevraagd.
Deze vacatures zijn doorzocht op de aanwezigheid van de cybersecurity gerelateerde termen weergegeven in supplementaire tabel 1. De vacatures zijn daarna steekproefsgewijs bekeken om te bepalen hoeveel cybersecurity gerelateerde termen in een vacature moeten voorkomen voordat wij deze als cybersecurity vacature beschouwen. Tijdens deze inspectie bleek dat relevante cybersecurity vacatures soms slechts één cybersecurity gerelateerde term bevatten. Een vacature is daarom meegenomen in de analyse wanneer deze minimaal één van de cybersecurity gerelateerde termen bevat. Het verhogen van de threshold leidt ons inziens tot meer verwijderde true positive-vacatures dan verwijderde false positive-vacatures, waardoor de kwaliteit van het sample enkel zal afnemen. Daarmee hebben wij er dus voor gekozen om een (lichte) overschatting op te nemen van het aantal cybersecurity vacatures.

Cybersecurity gerelateerde termen
Cyber
Informatiebeveiliging
Information security
Netwerkbeveiliging
Netwerk security
Network security
Cloud security
Cloudbeveiliging
IT-security
IT security
Databeveiliging
Data security
Digitale veiligheid
Digitale beveiliging
Digitale crime

Supplementaire tabel 1: Cybersecurity gerelateerde termen voor de identificatie van cybersecurity vacatures

Identificatie van functieprofielen

De (lichte) overschatting in het aantal cybersecurity vacatures gaan wij tegen door de vacatures te classificeren op de mate van cybersecurity relevantie per functieprofiel. Hiervoor zijn de functietitels opgeschoond en opnieuw geaggregeerd naar (waar mogelijk) een ECSF-profiel. We hebben daartoe de operationalisering gebruikt zoals beschreven in supplementaire tabel 2. Een functietitel die de termen bevat in de rechterkolom is opgewerkt naar het ECSF-profiel in de linker kolom.

ECSF-profiel	Mapping van functietitels
Chief Information Security Officer (CISO)	security & officer or functionaris & informat or informat & security or functionaris & beveiliging or ciso or chief information security
Penetration Tester	security & tester or pentester or penetration or ethical hacker
Cybersecurity Implementer	security & implement or security & engineer or cyber & engineer or IT & engineer or system & engineer or devops & engineer or cloud & engineer or network & engineer or netwerk & engineer or solution & engineer
Cybersecurity Researcher	onderzoeker & security or onderzoeker & cyber or research & security or phd or postdoc or post doc
Cybersecurity Risk Manager	risk manager & security or risk manager & informat or security & analist or informat & analist or security & assessor
Cybersecurity Architect	solution & architect or data & architect or security & architect or infra & architect or IT & architect
Cyber Legal, Policy & Compliance Officer	compliance & risk or compliance & security or compliance & analist or GRC or protection & officer or policy & officer or IT & beleid or beveiliging & beleid or functionaris & bescherming
Digital Forensics Investigator	forensic
Cyber Incident Responder	incident & respon or cyber & defen or crisis & manage or siem & engineer or incident & security
Cybersecurity Auditor	audit & security or audit & IT
Cybersecurity Educator	security & trainer or docent & security or security & awareness
Cyber Threat Intelligence Specialist	cyber & threat or threat & analist or cyber & intelligence or cyber & dreiging or cyber & specialist or security & sepcialist

Supplementaire tabel 2: Mapping van functietitels naar ECSF-profielen

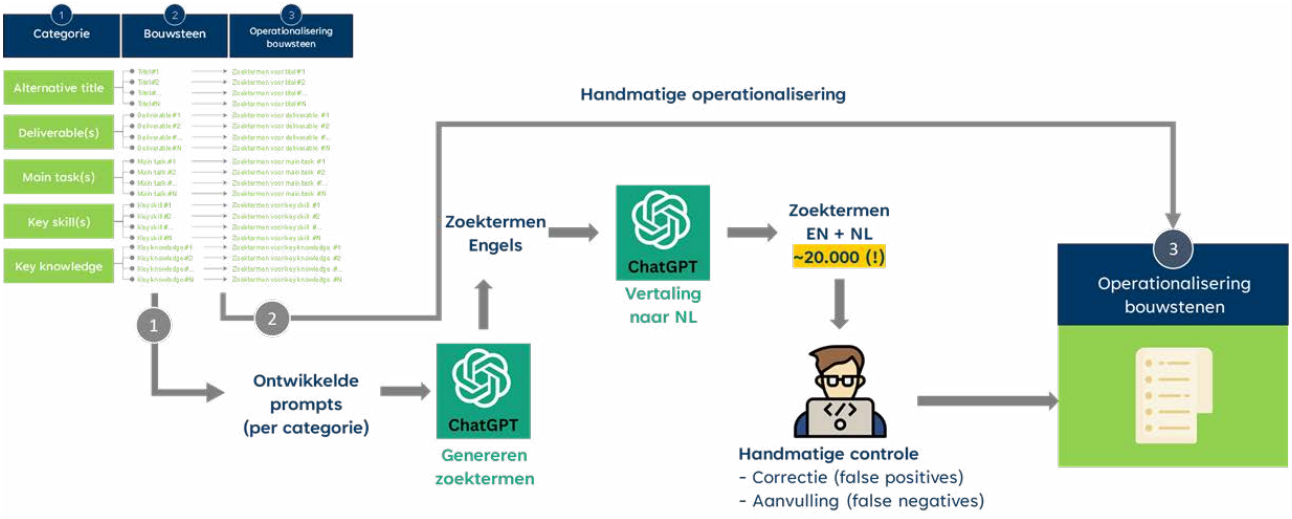
Per functietitel die niet aan een ECSF-profiel is gekoppeld is de mate van cybersecurity relevantie bepaald door te kijken naar het aantal cybersecurity gerelateerde termen per vacature. Door middel van een handmatige inspectie hebben wij de volgende categorisering ontwikkeld:

- Hoge cybersecurity relevantie: Functietitels met gemiddeld 6 of meer cybersecurity gerelateerde termen per vacature.
- Middelmatige cybersecurity relevantie: Functietitels met gemiddeld tussen de 3 en 5.9 cybersecurity gerelateerde termen per vacature.
- Lage cybersecurity relevantie: Functietitels met gemiddeld minder dan 3 cybersecurity gerelateerde termen per vacature.

Deze categorisering is gebruikt bij de uitsplitsingen om zo een eerlijke weergave te bieden van ons vacature sample.

Identificatie van specifieke kennis en vaardigheden

Na het identificeren van de cybersecurity vacatures en het categoriseren van functietitels zijn de vacatures doorzocht op de aanwezigheid van specifieke taken, vaardigheden en kennis binnen het cybersecurity domein. Deze 'bouwstenen' zijn per profiel gedefinieerd in het ECSF. Aan de hand van zoektermen per bouwsteen is gekwantificeerd in welke mate en bij welke functies de bouwstenen relevant zijn. Het definiëren van deze zoektermen is via twee routes geoperationaliseerd, zie supplementaire figuur 1.



Supplementaire figuur 1: Operationalisering taken, vaardigheden en kennis

Bij route 1 zijn zoektermen opgesteld door ChatGPT slim te bevragen. Per categorie bouwstenen (Deliverables, Main task(s), Key skill(s) en Key knowledge) zijn vragen opgesteld waar ChatGPT zoektermen als suggesties op geeft. Bij deze vragen is geautomatiseerd de informatie over de bouwsteen meegegeven en heeft ChatGPT per bouwsteen relevante zoektermen gegenereerd. Deze zoektermen zijn automatisch door ChatGPT vertaald naar het Nederlands. Omdat het sample zowel Engelstalige als Nederlandstalige vacatures bevat is het van belang om de zoektermen in beide talen te operationaliseren. Dit heeft geleid tot een set van ongeveer 20.000 zoektermen. Deze termen zijn handmatig beoordeeld op de precisie. De precisie geeft een mate van zekerheid aan. Wanneer een zoekterm met een hoge precisie voor een bouwsteen wordt gevonden in een vacature, zijn we er zeker van dat deze bouwsteen daadwerkelijk aanwezig is in de vacature. Het geeft dus aan hoe specifiek een zoekterm is. Voor de analyse zijn enkel zoektermen gebruikt met een hoge precisie. Door zoektermen te gebruiken met een hoge precisie minimaliseren we het aantal false positives.
Bij route 2 zijn zoektermen handmatig opgesteld in de vorm van queries. Een query is een combinatie van termen die onderling samenhangen. De achterliggende gedachte daarbij is dat een combinatie van termen de aanwezigheid van een bouwsteen kan signaleren. Doordat het hierbij om een combinatie van termen gaat, kunnen we gebruik maken van minder specifieke termen dan bij route 1. Tabel 3 toont de operationalisering van de queries in het huidige onderzoek. Voor elke bouwsteen is minimaal één term ingevuld in de eerste set zoektermen (set A), de andere sets zijn optioneel. De zoektermen binnen een set hebben onderling een OF-relatie, de sets hebben onderling een EN-relatie. Aan de hand van Tabel 3 kunnen we een voorbeeld uitwerken. Volgens de huidige methode is bouwsteen A aanwezig in een vacature wanneer term 2, term 3 en term 4 aanwezig zijn in een vacature. Maar, deze bouwsteen is ook aanwezig wanneer term 1, term 3 en term 5 aanwezig zijn in een vacature. Het gaat er dus om dat minimaal één term per (ingevulde) set aanwezig is in de vacature.

Tabel 3 Operationalisering handmatige queries	Set A	Set B	Set C	Set D	Cybersecurity specifieke term
Bouwsteen A	term 1, term 2	Term 3	term 4, term 5		
Bouwsteen B	term 6				term 7

Supplementaire tabel 3: Operationalisering handmatige queries

De resultaten van beide routes zijn tenslotte gecombineerd. Wanneer een bouwsteen volgens minimaal één van de twee routes aanwezig is in de vacature is deze als zodanig meegenomen in de analyse.

Bijlage 2. Tabellen behorende bij onderwijs

Tabellen mbo bij paragraaf 3.3

Tabellen m.b.t. de uitkomsten van de enquête onder de ICT-opleidingsmanagers

rapport cijfer	aantal respondenten
1	
2	
3	2
4	
5	3
6	1
7	2
8	
9	3
10	3

(N= 14)

Supplementaire tabel 4: Welk rapportcijfer geeft u zelf voor de inzet op cybersecurity binnen uw eigen ICT-opleidingen?

	Nooit		Incidenteel		Regelmatig		Vaak		Altijd		Totaal	Gewogen gemiddelde
Gastlessen	20,00%	2	50,00%	5	20,00%	2	0,00%	0	10,00%	1	10	2,3
Groepsopdrachten	30,00%	3	30,00%	3	20,00%	2	10,00%	1	10,00%	1	10	2,4
Praktijkopdrachten individueel	20,00%	2	0,00%	0	40,00%	4	10,00%	1	30,00%	3	10	3,3
Specifieke vakken/ modules	30,00%	3	20,00%	2	10,00%	1	20,00%	2	20,00%	2	10	2,8
BPV	20,00%	2	30,00%	3	30,00%	3	10,00%	1	10,00%	1	10	2,6
Overige	33,33%	3	33,33%	3	33,33%	3	0,00%	0	0,00%	0	9	2

Supplementaire tabel 5.1 : Mdw ICT-support niveau 2: In welke mate is of kan cybersecurity een onderwerp zijn?

	Nooit		Incidenteel		Regelmatig		Vaak		Altijd		Totaal	Gewogen gemiddelde
Gastlessen	20,00%	3	46,67%	7	26,67%	4	0,00%	0	6,67%	1	15	2,27
Groepsopdrachten	20,00%	3	26,67%	4	20,00%	3	20,00%	3	13,33%	2	15	2,8
Praktijkopdrachten individueel	13,33%	2	20,00%	3	6,67%	1	40,00%	6	20,00%	3	15	3,33
Specifieke vakken/ modules	13,33%	2	20,00%	3	26,67%	4	13,33%	2	26,67%	4	15	3,2
BPV	6,67%	1	33,33%	5	40,00%	6	0,00%	0	20,00%	3	15	2,93
Overige	46,67%	7	20,00%	3	13,33%	2	6,67%	1	13,33%	2	15	2,2

Supplementaire tabel 5.2: Software developer niveau 4: In welke mate is of kan cybersecurity een onderwerp zijn?

	Nooit		Incidenteel		Regelmatig		Vaak		Altijd		Totaal	Gewogen gemiddelde
Gastlessen	8,33%	1	58,33%	7	16,67%	2	8,33%	1	8,33%	1	12	2,5
Groepsopdrachten	0,00%	0	41,67%	5	25,00%	3	8,33%	1	25,00%	3	12	3,17
Praktijkopdrachten individueel	0,00%	0	25,00%	3	16,67%	2	25,00%	3	33,33%	4	12	3,67
Specifieke vakken/ modules	8,33%	1	16,67%	2	33,33%	4	0,00%	0	41,67%	5	12	3,5
BPV	8,33%	1	33,33%	4	25,00%	3	0,00%	0	33,33%	4	12	3,17
Overige	50,00%	5	30,00%	3	0,00%	0	0,00%	0	20,00%	2	10	2,1

Supplementaire tabel 5.3: Allround IT system & device niveau 4: In welke mate is of kan cybersecurity een onderwerp zijn?

	Nooit		Incidenteel		Regelmatig		Vaak		Altijd		Totaal	Gewogen gemiddelde
Gastlessen	7,14%	1	64,29%	9	14,29%	2	7,14%	1	7,14%	1	14	2,43
Groepsopdrachten	0,00%	0	28,57%	4	28,57%	4	21,43%	3	21,43%	3	14	3,36
Praktijkopdrachten individueel	0,00%	0	14,29%	2	7,14%	1	50,00%	7	28,57%	4	14	3,93
Specifieke vakken/ modules	0,00%	0	14,29%	2	21,43%	3	14,29%	2	50,00%	7	14	4
BPV	0,00%	0	35,71%	5	28,57%	4	7,14%	1	28,57%	4	14	3,29
Overige	22,22%	2	44,44%	4	11,11%	1	0,00%	0	22,22%	2	9	2,56

Supplementaire tabel 5.4: Expert IT system & device niveau 4: In welke mate is of kan cybersecurity een onderwerp zijn?

Antwoordkeuzen	Reacties	
Voldoende docenten	50,00%	7
Professionalisering van docenten	71,43%	10
Onderwijs-en examenmateriaal	64,29%	9
Hybride leerwerkplekken	42,86%	6
Medewerking van het werkveld, bijv. middels gastlessen, bedrijfsbezoeken, praktijkopdrachten	71,43%	10
Overige (geef nadere toelichting)	14,29%	2
Totaal aantal respondenten: 14		

Supplementaire tabel 6: Wat heeft u (nog) nodig om actueel onderwijs te bieden op het gebied van cybersecurity? (meerdere antwoorden mogelijk)

	Vraagt zeker meer aandacht		Krijgt nu al voldoende aandacht		N.v.t.		Totaal	Gewogen gemiddelde
Beveiliging van netwerken en systemen, gebruikers, software en devices	28,57%	4	64,29%	9	7,14%	1	14	1,69
Datawareness	57,14%	8	35,71%	5	7,14%	1	14	1,38
AI	78,57%	11	7,14%	1	14,29%	2	14	1,08
Cloud	28,57%	4	64,29%	9	7,14%	1	14	1,69
Samenwerkingstooling	50,00%	7	35,71%	5	14,29%	2	14	1,42
Privacy	35,71%	5	57,14%	8	7,14%	1	14	1,62
Soft skills (samenwerken, ethisch en integer handelen, met druk omgaan etc)	28,57%	4	64,29%	9	7,14%	1	14	1,69
Totaal aantal respondenten: 14								

Supplementaire tabel 7: Kunt u bij de onderstaande cybersecurity thema's aangeven of daar de komende periode meer aandacht in uw opleidingen moet worden gegeven?

Tabellen ho bij paragraaf 3.4

	2019-2020 instroom	2019-2020 uitstroom	2020-2021 instroom	2020-2021 uitstroom	2021-2022 instroom	2021-2022 uitstroom	2022-2023 instroom	2022-2023 uitstroom	2023-2024 instroom
De Haagse Hogeschool	**10**	**10**	**10**	**10**	**12**	**7**	**11**		**14**
m Cyber Security Engineering (post-initiele master)	10	10	10	10	12	7	11		14
Hogeschool INHOLLAND									**40**
Ad Cybersecurity deeltijd									16
Ad Cybersecurity voltijd									24
Hogeschool Utrecht									
Ad Cybersecurity									
Hogeschool van Amsterdam	**51**	**0**	**80**	**19**	**82**	**36**	**90**		
Ad Cybersecurity	51	0	80	19	82	36	90		
NHL Stenden Hogeschool									
Ad Cyber Safety & Security									
Universiteit Leiden	**261**	**83**	**298**	**123**	**280**	**193**	**284**	**217**	**257**
b Security Studies	237	65	281	107	265	174	269	207	249
m Cyber Security (post-initiele master)	24	18	17	16	15	19	15	10	8
Universiteit Maastricht									
m Advanced Master in Privacy, Cybersecurity, Data Management and Leadership (post-initiele master)									
Universiteit van Amsterdam	**44**	**47**	**26**	**26**	**34**	**25**	**38**		
m Security and Network Engineering deeltijd	13	18	5	7	14	5	10		
m Security and Network Engineering voltijd	31	29	21	19	20	20	28		
Vrije Universiteit Amsterdam	**5**	**10**	**10**	**7**	**18**	**5**	**13**		
m Computer Security	5	10	10	7	18	5	13		
Totaal	**371**	**150**	**424**	**185**	**426**	**266**	**436**	**217**	**311**

Supplementaire tabel 8: overzicht van volledige cybersecurity studies binnen het hoger onderwijs

	2019-2020 instroom	2019-2020 uitstroom	2020-2021 instroom	2020-2021 uitstroom	2021-2022 instroom	2021-2022 uitstroom	2022-2023 instroom	2022-2023 uitstroom	2023-2024 instroom
Chr. Hogeschool Windesheim	**59**	**59**	**76**	**76**	**68**	**68**	**60**	**60**	
Infrastructure Design and Security (b HBO-ict)	59	59	76	76	68	68	60	60	
De Haagse Hogeschool									
Information Security Management (b HBO-ict)									
Erasmus Universiteit Rotterdam					**49**	**49**	**49**	**49**	
Data Privacy and Cybersecurity (m business information management)					49	49	49	49	
Fontys Hogescholen	**58**	**58**	**57**	**57**	**66**	**66**	**177**	**72**	**78**
ICT & Infrastructure (ad ad-ict)	0	0	0	0	0	0	64	0	14
ICT & Cybersecurity (b HBO-ict)	58	58	57	57	66	66	113	72	64
Hanzehogeschool Groningen									
Software Engineering (b HBO-ict)									
Hogeschool INHOLLAND	**25**	**25**	**29**	**29**	**20**	**20**	**24**	**18**	**6**
Security (b informatica)	25	25	29	29	20	20	9	9	
Information Security Officer (b Integrale Veiligheidskunde)							15	9	6
Hogeschool Rotterdam	**35**	**35**	**35**	**35**	**35**	**35**	**35**	**35**	**35**
Privacy, Security, Risk (b business it & management)	35	35	35	35	35	35	35	35	35
Hogeschool Utrecht	**39**	**39**	**40**	**40**	**47**	**47**	**9**	**9**	
Cyber Security & Cloud (b HBO-ict)	39	39	40	40	47	47	9	9	
Informatieveiligheid (b Integrale Veiligheidskunde)									
Hogeschool van Amsterdam	**26**	**26**	**50**	**50**	**47**	**47**	**66**	**66**	
Cybersecurity (b HBO-ict)	26	26	50	50	47	47	66	66	
Hogeschool van Arnhem en Nijmegen	**47**	**32**	**58**	**40**	**49**	**51**	**49**	**32**	

Infrastructure & Security Management (b HBO-ict)	47	32	58	40	49	51	49	32	
NHL Stenden Hogeschool									
Certified Ethical Hacking (b (technische) informatica)									
Secure Programming (b (technische) informatica)									
Hack@Sea (b (technische) informatica)									
Radboud Universiteit Nijmegen									
Cyber security (b computing science)									
Cyber Security (m computing science)									
Cyber Security and AI (m computing science)									
Security or Privacy Office (m information sciences)									
Saxion Hogeschool									
Infrastructuur (b HBO-ict)									
Cyber Security (not related to one specific program)									
Techn. Universiteit Eindhoven	**83**	**64**	**87**	**65**	**88**	**64**	**69**	**22**	
Information Security Technology (m computer science and engineering)	23	10	29	12	27	20	25	22	
Cyber-Physical systems (m embedded systems)	60	54	58	53	61	44	44		
Technische Universiteit Delft									
Cyber Security (m computer science)									
Universiteit Leiden	**0**	**0**	**184**	**54**	**179**	**105**	**171**	**89**	
Cybersecurity (m Crisis and Security Management)	0	0	184	54	179	105	171	89	
Universiteit Twente									
Cybersecurity (m computer science)									

Vrije Universiteit Amsterdam	**7**	**21**	**5**	**7**	**3**	**3**			
Security (m computer science (joint degree))	7	21	5	7	3	3			
Zuyd Hogeschool					**55**	**55**	**21**	21	45
Cybersecurity (b HBO-ict)					55	55	21	21	45
Totaal	**379**	**359**	**621**	**453**	**706**	**610**	**730**	**473**	**164**

Supplementaire tabel 9: overzicht van studies met een specialisatie- of keuzerichting cybersecurity binnen het hoger onderwijs

	2019-2020 instroom	2019-2020 uitstroom	2020-2021 instroom	2020-2021 uitstroom	2021-2022 instroom	2021-2022 uitstroom	2022-2023 instroom	2022-2023 uitstroom	2023-2024 instroom
Avans Hogeschool	**89**	**60**	**97**	**82**	**68**	**85**	**82**		
b business it & management deeltijd	22	13	21	31	18	20	19		
b business it & management voltijd	67	47	76	51	50	65	63		
De Haagse Hogeschool	**298**	**119**	**284**	**146**	**282**	**136**	**248**		
b Integrale Veiligheidskunde deeltijd	24	13	24	26	32	11	25		
b Integrale Veiligheidskunde duaal	141	64	142	71	112	76	103		
b Integrale Veiligheidskunde voltijd	133	42	118	49	138	49	120		
Hogeschool INHOLLAND			**405**	**330**	**350**	**290**	**310**	**230**	**250**
b Integrale Veiligheidskunde			405	330	350	290	310	230	250
NHL Stenden Hogeschool	**273**	**162**	**307**	**161**	**247**	**134**	**251**		
b HBO-ict deeltijd	26	10	13	5	18	5	12		
b HBO-ict voltijd	98	44	112	61	78	50	81		
b Integrale Veiligheidskunde deeltijd	0	10	13	0	12	5	23		
b Integrale Veiligheidskunde voltijd	149	98	169	95	139	74	135		
Radboud Universiteit Nijmegen	**164**	**62**	**141**	**52**	**134**	**69**	**183**		
b computing science	164	62	141	52	134	69	183		
Rijksuniversiteit Groningen	**90**	**78**	**112**	**106**	**88**	**98**	**54**		
m it-recht deeltijd	20	20	10	20	10	20	0		
m it-recht voltijd	70	58	102	86	78	78	54		
Saxion Hogeschool	**181**	**98**	**203**	**128**	**132**	**140**	**120**		
b Integrale Veiligheidskunde deeltijd	21	14	20	18	19	10	14		
b Integrale Veiligheidskunde voltijd	160	84	183	110	113	130	106		
Technische Universiteit Delft	**192**	**149**	**225**	**165**	**259**	**180**	**263**		
m computer science	192	149	225	165	259	180	263		
Tilburg University	**108**	**92**	**100**	**102**	**137**	**97**	**140**		
m Law and Technology	108	92	100	102	137	97	140		

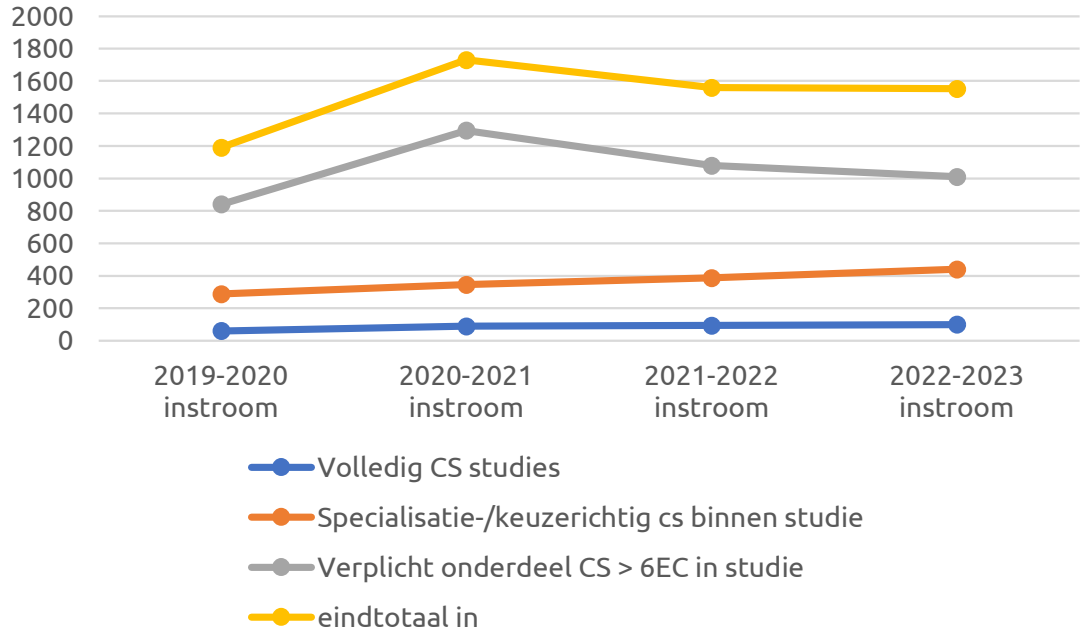
Universiteit Leiden	**219**	**127**	**218**	**137**	**243**	**180**	**168**	**38**	**56**
b informatica voltijd	141	68	149	70	157	83	108		
Law and Digital Technologies (Advanced Master Programme)	38	33	34	31	58	55	40	38	56
m ict in business and the public sector	40	26	35	36	28	42	20		
Totaal	**1576**	**914**	**2058**	**1378**	**1882**	**1354**	**1779**	**230**	**250**

Supplementaire tabel 10: overzicht van studies met een verplicht onderdeel cybersecurity (>6 ECTS) binnen het hoger onderwijs

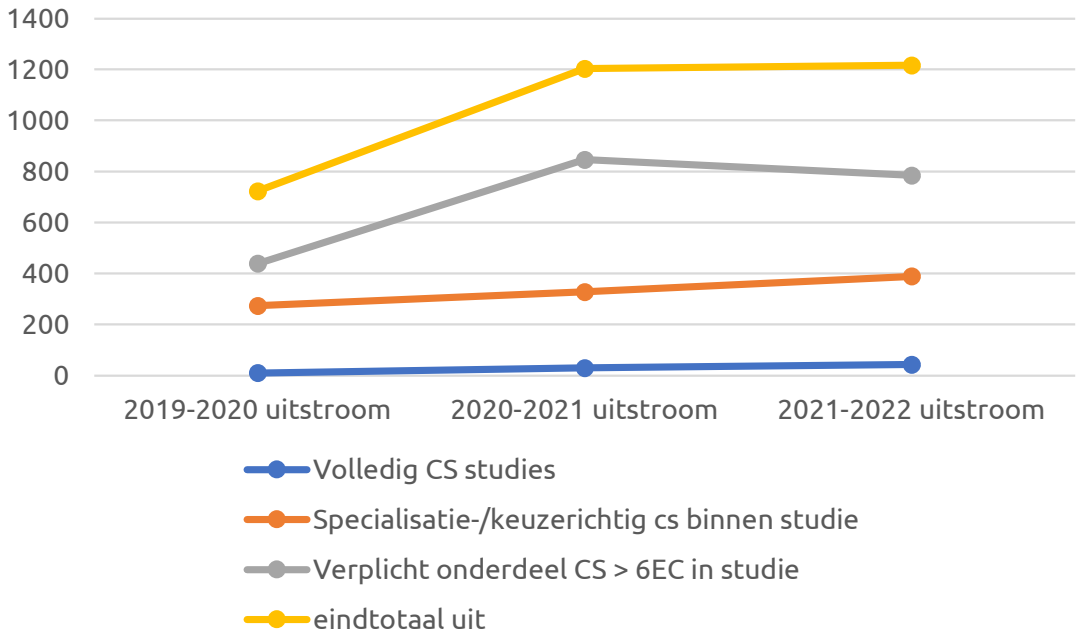
Aankomende opleidingen
Avans Hogeschool
AI & Security learning community
De Haagse Hogeschool
Ad Cybersecurity
B cyber engineering
Hogeschool Leiden
M Digital Forensics
Hogeschool Utrecht
Ad Cybersecurity
B Digital Security
M Digital Security
Mbo Rijnland
Cyber education
NHL Stenden Hogeschool
Ad Cyber Safety & Security
ROC Aventus
Safety & Security
ROC Mondriaan
Cyber education
Universiteit Leiden
B Cyber Security and Cyber Governance / Cybercrime & Cybersecurity

Supplementaire tabel 11: overzicht van geïdentificeerde opleidingen die nog in ontwikkelingsfase, accreditatiefase, of opstartfase zijn.

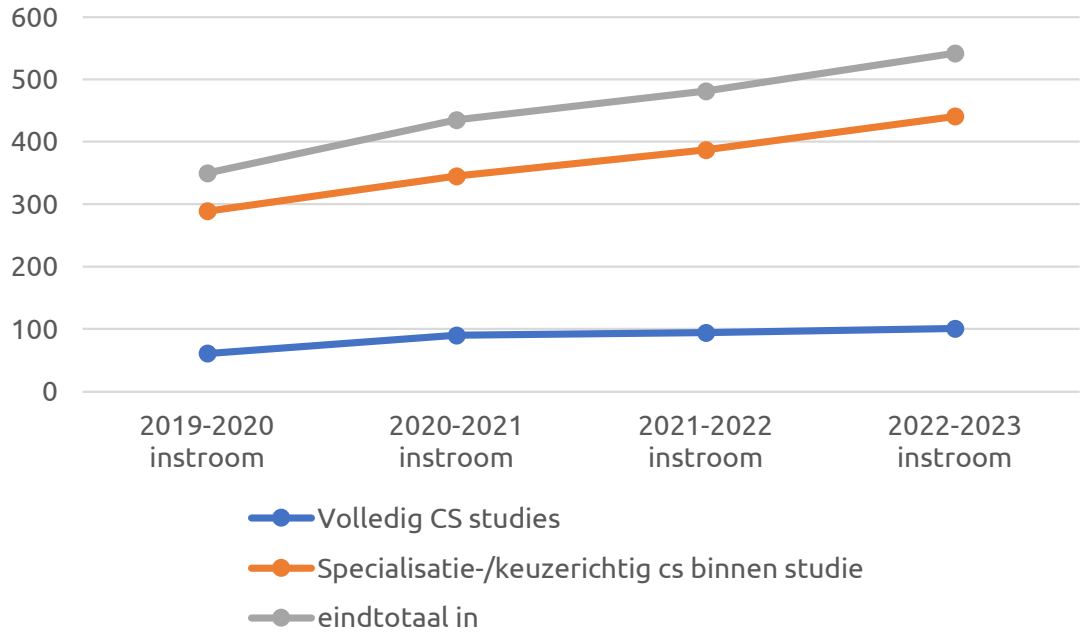
In- en uitstroom gegevens bekostigd hbo-onderwijs



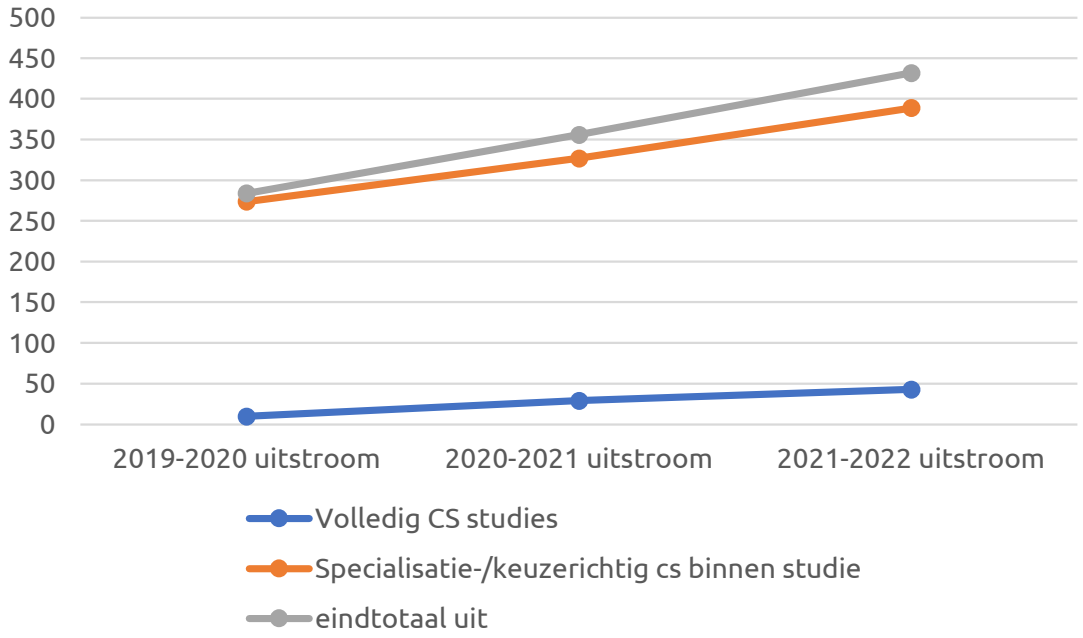
Supplementaire figuur 2: Verloop instroom studenten over de tijd, alle hbo-studies met relevant onderdeel cybersecurity



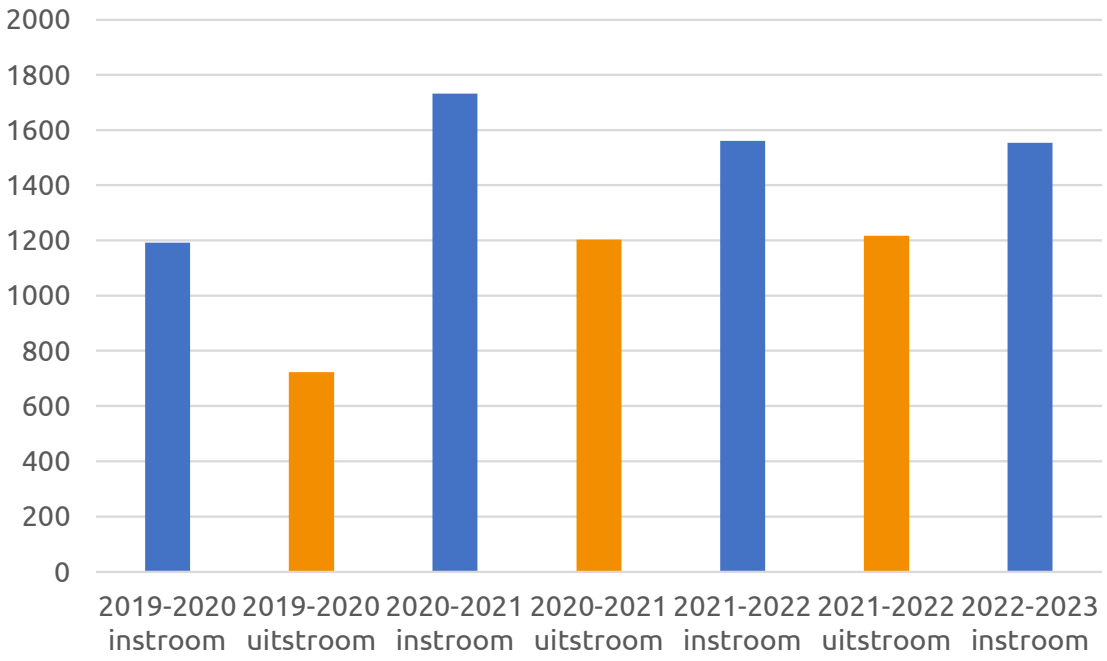
Supplementaire figuur 3: Verloop uitstroom studenten over de tijd, alle hbo-studies met relevant onderdeel cybersecurity



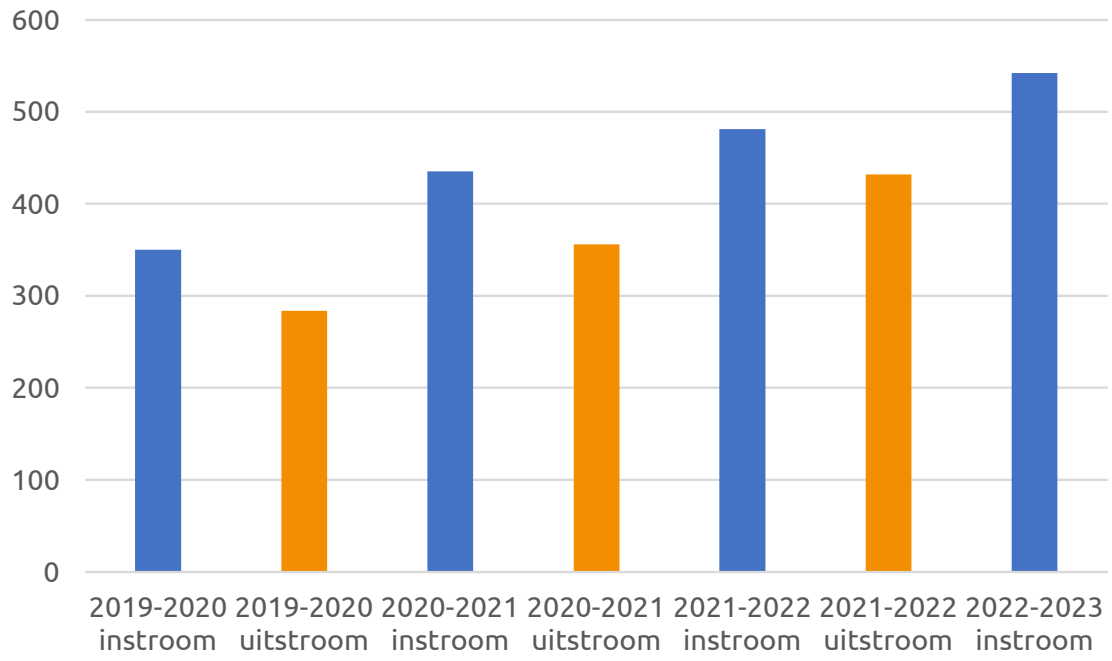
Supplementaire figuur 4: Verloop instroom studenten over de tijd, studenten vanuit hbo-studies die volledig in het teken staan van cybersecurity en studenten die binnen hun hbo-studie een specialisatie-/keuzerichting cybersecurity gekozen hebben



Supplementaire figuur 5: Verloop uitstroom studenten over de tijd, studenten vanuit hbo-studies die volledig in het teken staan van cybersecurity en studenten die binnen hun hbo-studie een specialisatie-/keuzerichting cybersecurity gekozen hebben

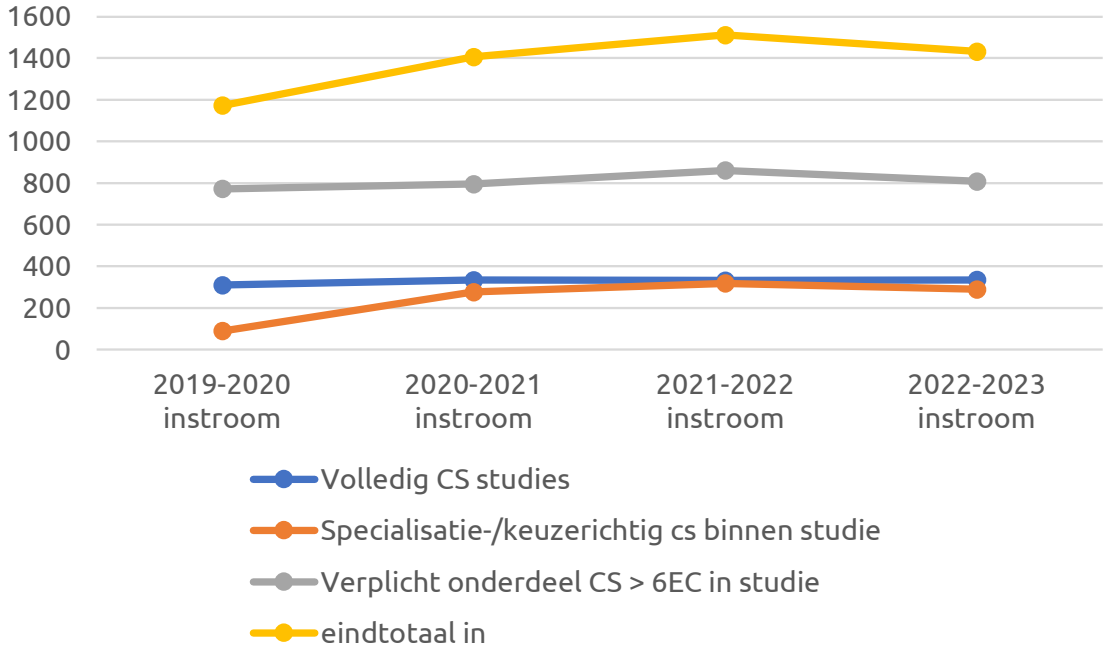


Supplementaire figuur 6: instroom versus uitstroom voor alle hbo-studies met relevant onderdeel cybersecurity

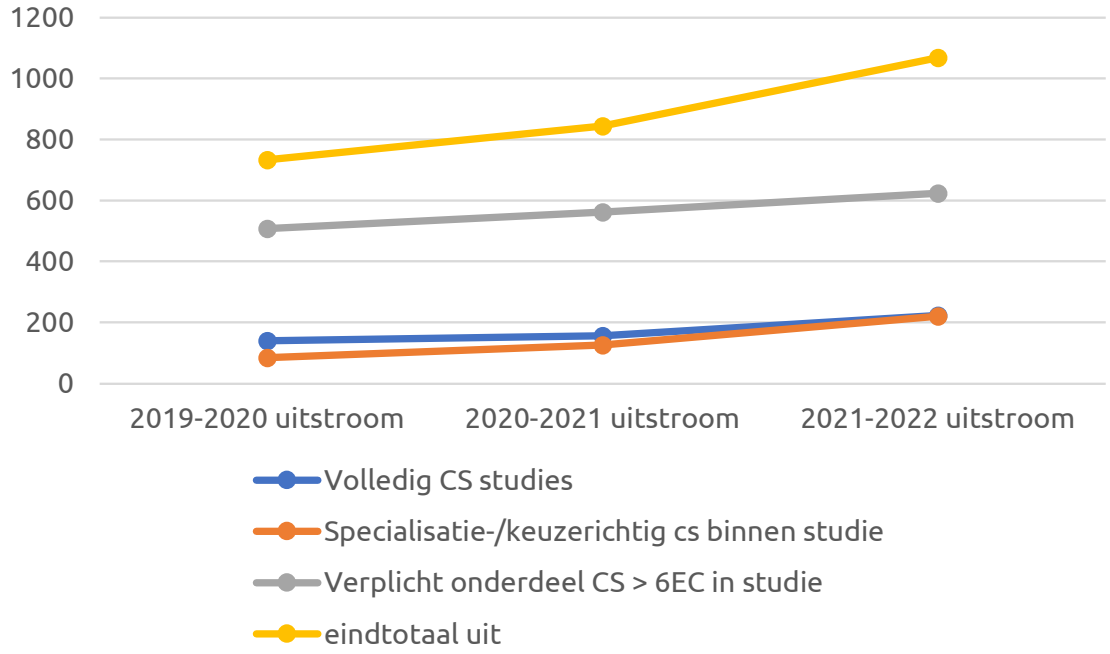


Supplementaire figuur 7: instroom versus uitstroom van hbo-studenten die een specifieke cybersecurity opleiding danwel een specifieke cybersecurity gerichte specialisatie-/keuzerichting gevolgd hebben.

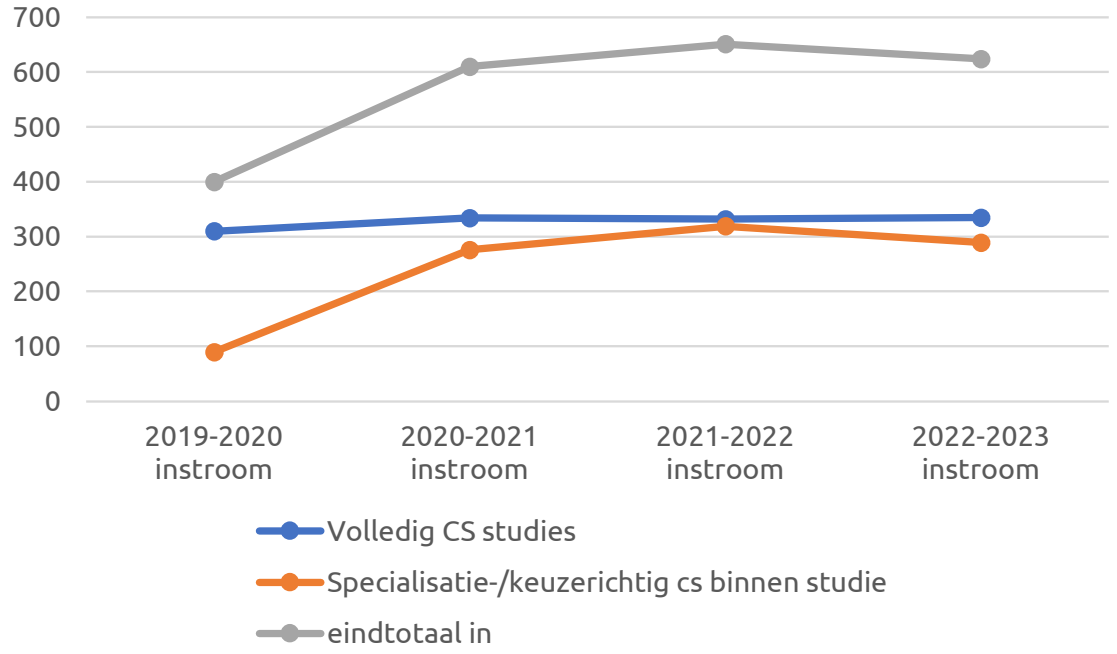
In- en uitstroom gegeven bekostigd wo-onderwijs



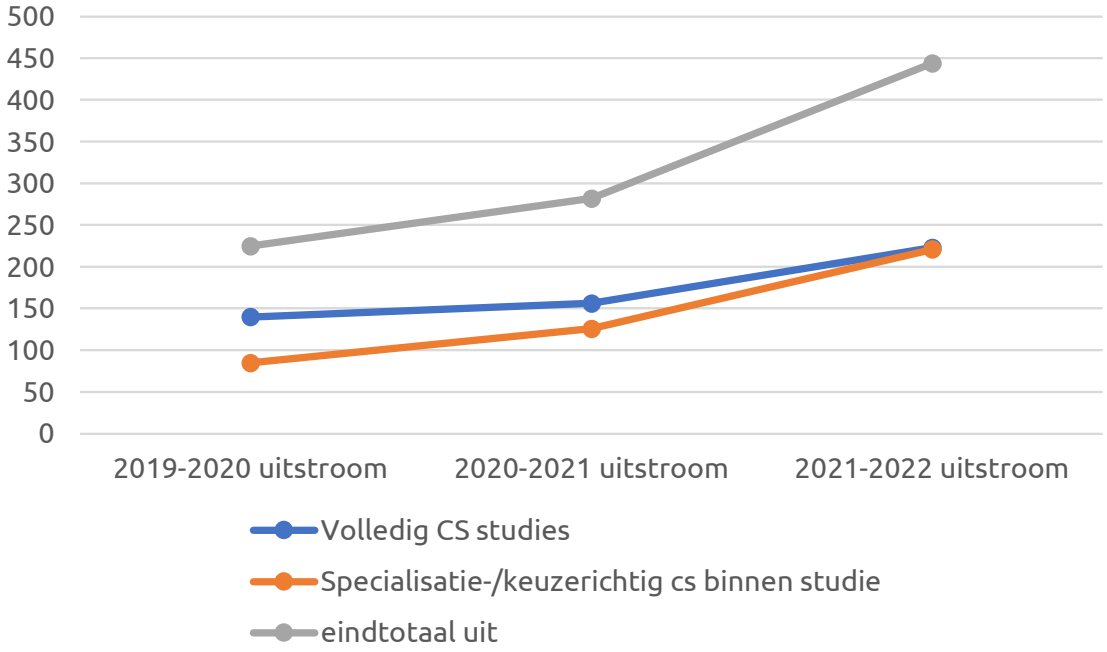
Supplementaire figuur 8: Verloop instroom studenten over de tijd, alle wo-studies met relevant onderdeel cybersecurity



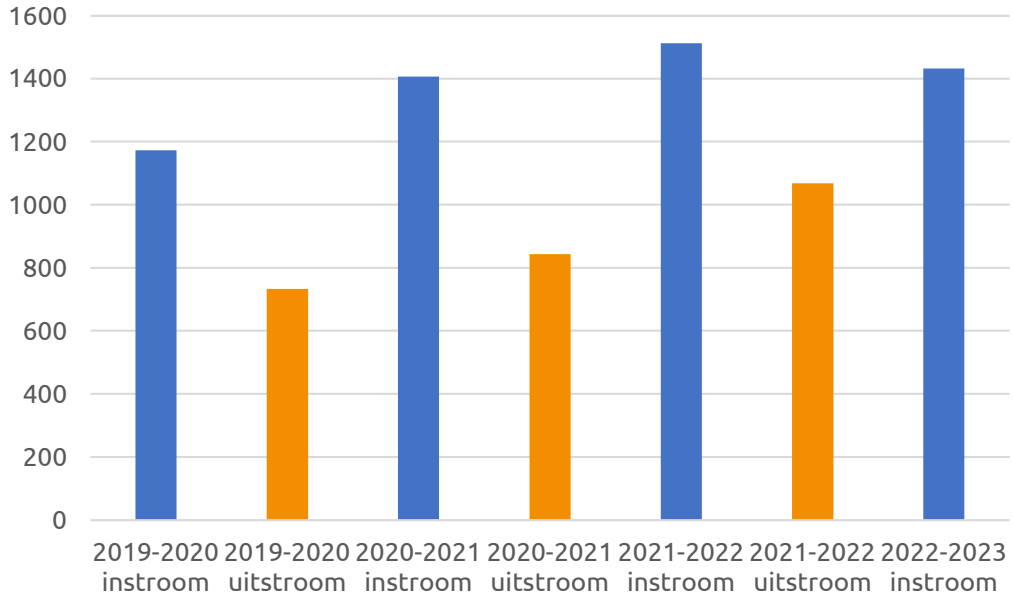
Supplementaire figuur 9: Verloop uitstroom studenten over de tijd, alle wo-studies met relevant onderdeel cybersecurity



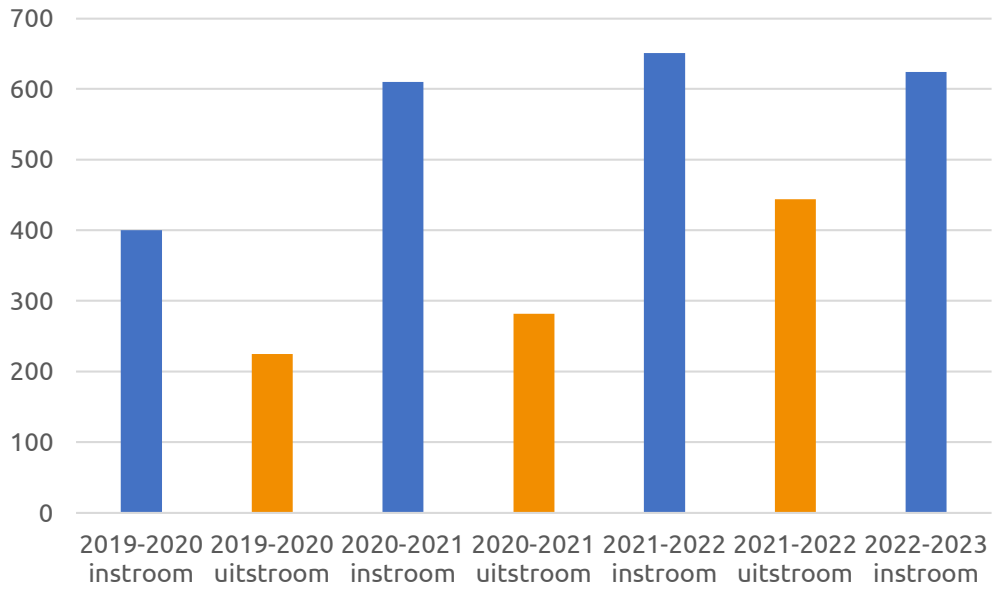
Supplementaire figuur 10: Verloop instroom studenten over de tijd, studenten vanuit wo-studies die volledig in het teken staan van cybersecurity en studenten die binnen hun wo-studie een specialisatie-/keuzerichting cybersecurity gekozen hebben



Supplementaire figuur 11: Verloop uitstroom studenten over de tijd, studenten vanuit wo-studies die volledig in het teken staan van cybersecurity en studenten die binnen hun wo-studie een specialisatie-/keuzerichting cybersecurity gekozen hebben



Supplementaire figuur 12: instroom versus uitstroom voor alle wo-studies met relevant onderdeel cybersecurity



Supplementaire figuur 13: instroom versus uitstroom van wo-studenten die een specifieke cybersecurity opleiding danwel een specifieke cybersecurity gerichte specialisatie-/keuzerichting gevolgd hebben.

Tabellen vergelijking inhoud opleidingen mbo en ho bij paragraaf 3.5

Onderwijs-type	Instelling	Actuele opleidings-code	Actuele opleidingsnaam	Aandeel cyber-security	Tech-nisch	M&O	Legal	Onder-zoek	Onder-wijs
Mbo	Mbo - generiek	25604	Software developer	Deels	3	0	0	0	0
Mbo	Mbo - generiek	25606	Expert IT systems and devices	Deels	3	2	0	0	0
Mbo	Mbo - generiek	25605	Allround medewerker IT systems and devices	Deels	3	1	0	0	0
Mbo	Mbo - generiek	25607	Medewerker ICT support	Deels	3	0	0	0	0
Wo	Universiteit Leiden	75120	M Cyber Security (post-initiele master)	Volledig	3	3	3	2	0
Wo	Universiteit Maastricht	75150	M Advanced Master in Privacy, Cybersecurity, Data Management and Leadership (post-initiele master)	Volledig	3	3	3	2	0
Hbo	De Haagse Hogeschool	70207	M Cyber Security Engineering (post-initiele master)	Volledig	3	1	1	1	0
Hbo	Hogeschool van Amsterdam	80156	Ad Cybersecurity	Volledig	3	1	0	1	0
Wo	Universiteit Leiden	59320	B Security Studies	Volledig	1	3	1	2	0
Wo	Universiteit Leiden	60417	M Crisis and Security Management	Deels	1	3	1	2	0
Wo	Universiteit van Amsterdam	60227	M Security and Network Engineering voltijd	Volledig	3	0	0	2	0
Wo	Universiteit van Amsterdam	60227	M Security and Network Engineering deeltijd	Volledig	3	0	0	2	0
Wo	Vrije Universiteit Amsterdam	60802	M Computer Security	Volledig	3	0	0	2	0
Hbo	Saxion Hogeschool	39268	B Integrale Veiligheidskunde voltijd	Deels	1	3	1	1	0

Hbo	Saxion Hogeschool	39268	B Integrale Veiligheidskunde deeltijd	Deels	1	3	1	1	0
Hbo	Hogeschool Utrecht	39268	B Integrale Veiligheidskunde	Deels	1	3	2	1	0
Hbo	Hogeschool INHOLLAND	39268	B Integrale Veiligheidskunde	Deels	1	3	2	1	0
Hbo	Hogeschool INHOLLAND	39268	B Integrale Veiligheidskunde	Deels	1	3	2	1	0
Hbo	De Haagse Hogeschool	39268	B Integrale Veiligheidskunde voltijd	Deels	1	3	1	1	0
Hbo	De Haagse Hogeschool	39268	B Integrale Veiligheidskunde deeltijd	Deels	1	3	1	1	0
Hbo	De Haagse Hogeschool	39268	B Integrale Veiligheidskunde duaal	Deels	1	3	1	1	0
Hbo	NHL Stenden Hogeschool	39268	B Integrale Veiligheidskunde voltijd	Deels	1	3	2	1	0
Hbo	NHL Stenden Hogeschool	39268	B Integrale Veiligheidskunde deeltijd	Deels	1	3	2	1	0
Hbo	NHL Stenden Hogeschool	80185	Ad Cyber Safety & Security	Volledig	3	3	1	1	0
Hbo	Hogeschool INHOLLAND	80156	Ad Cybersecurity voltijd	Volledig	3	2	3	1	0
Hbo	Hogeschool INHOLLAND	80156	Ad Cybersecurity deeltijd	Volledig	3	2	3	1	0
Hbo	Hogeschool Utrecht		Ad Cybersecurity	Volledig	3	2	1	1	0
Hbo	Chr. Hogeschool Windesheim	30020	b HBO-ict	Deels	3	0	0	1	0
Hbo	Avans Hogeschool	39118	b business it & management voltijd	Deels	2	3	0	1	0
Hbo	Hogeschool Rotterdam	39118	b business it & management	Deels	1	3	3	1	0
Hbo	Saxion Hogeschool	30020	b HBO-ict	Deels	3	0	0	1	0
Hbo	Hanzehogeschool Groningen	30020	b HBO-ict	Deels	3	2	1	1	1
Hbo	Hogeschool Utrecht	30020	b HBO-ict	Deels	3	1	0	1	0
Hbo	Zuyd Hogeschool	30020	b HBO-ict	Deels	3	1	0	0	0
Hbo	Hs van Arnhem en Nijmegen	30020	b HBO-ict	Deels	3	2	1	1	0

Hbo	Hs van Arnhem en Nijmegen	34131	b embedded systems engineering voltijd	Deels	3	0	0	0	0
Hbo	Hogeschool INHOLLAND	34479	b informatica	Deels	3	1	1	1	0
Hbo	De Haagse Hogeschool	30020	b HBO-ict	Deels	3	2	1	1	0
Hbo	Hogeschool van Amsterdam	30020	b HBO-ict	Deels	3	1	0	1	0
Hbo	Fontys Hogescholen	30020	b HBO-ict	Deels	3	1	1	1	0
Hbo	Fontys Hogescholen	34479	b informatica	Deels	3	1	0	1	0
Hbo	Fontys Hogescholen	80083	ad ad-ict	Deels	3	0	0	1	0
Hbo	NHL Stenden Hogeschool	30020	b HBO-ict voltijd	Deels	3	1	0	1	0
Hbo	NHL Stenden Hogeschool	34475	b technische informatica	Deels	3	0	0	1	0
Hbo	NHL Stenden Hogeschool	34479	b informatica	Deels	3	0	0	1	0
Wo	Universiteit Leiden	56978	b informatica voltijd	Deels	3	0	0	1	0
Wo	Universiteit Leiden	60205	m ict in business and the public sector	Deels	2	3	1	3	0
Wo	Rijksuniversiteit Groningen	60620	m it-recht voltijd	Deels	1	1	3	3	0
Wo	Erasmus Universiteit Rotterdam	60453	m business information management	Deels	1	3	1	3	0
Wo	Technische Universiteit Delft	60300	m computer science	Deels	3	1	0	3	0
Wo	Techn. Universiteit Eindhoven	60331	m embedded systems	Deels	3	0	0	3	0
Wo	Techn. Universiteit Eindhoven	60438	m computer science and engineering	Deels	3	0	0	3	0
Wo	Universiteit Twente	60300	m computer science	Deels	3	0	0	3	0
Wo	Universiteit Twente	60331	m embedded systems	Deels	3	0	0	3	0
Wo	Maastricht University	50300	b data science and artificial intelligence	Deels	3	1	0	3	0
Wo	Vrije Universiteit Amsterdam	65014	m computer science (joint degree)	Deels	3	0	0	3	0

Wo	Radboud Universiteit Nijmegen	59326	b computing science	Deels	3	0	0	3	0
Wo	Radboud Universiteit Nijmegen	59326	b computing science	Deels	3	0	0	3	0
Wo	Radboud Universiteit Nijmegen	60255	m information sciences	Deels	3	1	1	3	0
Wo	Radboud Universiteit Nijmegen	60364	m computing science	Deels	3	0	0	3	0
Wo	Radboud Universiteit Nijmegen	60364	m computing science	Deels	3	0	0	3	0
Wo	Tilburg University	60069	M Law and Technology	Deels	1	3	3	3	0
Wo	Universiteit Leiden	?	Law and Digital Technologies (Advanced Master Programme)	Deels	1	2	3	3	0
Wo	Rijksuniversiteit Groningen	60620	M IT-recht	Deels	1	1	3	3	0

Supplementaire tabel 12: Opleidingen mbo en ho, gescoord naar mate van aansluiting bij arbeidsmarktcompetenties

Tabellen LLO bij paragraaf 3.6

Naam opleiding	Instituut	Duur/ omvang
Business IT & Management	Avans Hogeschool	240 EC
Computer Science	Universiteit Twente	120 EC
Computer Science and Engineering	Technische Universiteit Eindhoven	120 EC
Computing Science	Radboud Universiteit	180 EC
Computing Science	Radboud Universiteit	120 EC
Criminologie	Universiteit Leiden	180 EC
Crisis and Security Management	Universiteit Leiden	60 EC
Engineering Systems	HAN University of Applied Sciences	90 EC
Engineering Systems	HAN_ University of Applied Sciences	36 maanden
Engineering Systems	HAN_ University of Applied Sciences	18 maanden
Engineering Systems - Cyber-Physical Systems	HAN_ University of Applied Sciences	18 maanden
Engineering Systems - Cyber-Physical Systems	HAN_ University of Applied Sciences	18 maanden
HBO-ICT	Fontys Hogeschool	240 EC
HBO-ICT	Hanzehogeschool Groningen	240 EC
HBO-ICT	Hogeschool Utrecht	240 EC
HBO-ICT	Hogeschool van Amsterdam	240 EC
HBO-ICT	HZ University of Applied Sciences	240 EC
HBO-ICT	Windesheim	240 EC
Industrial and Applied Mathematics	Technische Universiteit Eindhoven	120 EC
Informatica	Hogeschool Leiden	240 EC
Informatica	NHL Stenden	240 EC
Informatica	NHL Stenden Hogeschool	48 maanden
Informatica	NHL Stenden Hogeschool	48 maanden
Integrale Veiligheidskunde	Avans Hogeschool	240 EC
Integrale Veiligheidskunde	Avans Hogeschool	240 EC
Integrale Veiligheidskunde	NHL Stenden	240 EC
Integrale Veiligheidskunde	NHL Stenden Hogeschool	48 maanden
Integrale Veiligheidskunde	Saxion	240 EC
Integrale Veiligheidskunde	Saxion	240 EC
Integrale Veiligheidskunde (IVK)	Hogeschool Utrecht	240 EC
International Trends and Threats in Safety and Security	Saxion Hogeschool	10 weken
Introductie ICT	Deltion College	1 dag
IT Audit Compliance & Advisory (ITACA)	VU Vrije universiteit Amsterdam	129 dagen
IT-recht	Rijksuniversiteit Groningen	60 EC
Master Computer Science	Open Universiteit	Geen studieduur bekend
Master Digital Forensics	Hogeschool Leiden	60 EC
Master Military Strategic Studies	Faculteit Militaire Wetenschappen	Geen studieduur bekend
Master Software Engineering	Open Universiteit	Geen studieduur bekend

Privacy, Law & Security	Hogeschool Utrecht*	0 uur
Safety & Security Management (Engelstalige variant van Integrale Veiligheidskunde)	De Haagse Hogeschool	240 EC
Security Management	Hogeschool Utrecht	Geen studieduur bekend
Security Management	Hogeschool Utrecht*	0 uur
Security Management	Saxion	240 EC
Security Studies	Universiteit Leiden	180 EC
Software developer mbo 4 BBL	ROC Friese Poort Volwassenenonderwijs	4 jaar
Software developer mbo 4 BOL	ROC Friese Poort Volwassenenonderwijs	4 jaar
Strategische Kijk op Data Analytics	Erasmus Universiteit Rotterdam	4 maanden
Technische Informatica	NHL Stenden	240 EC
Technische Informatica	NHL Stenden Hogeschool	48 maanden

Supplementaire tabel 13: LLO-onderwijs mbo en ho - deels cybersecurity

Naam opleiding	Instituut	Duur/ omvang
Advanced Business Analytics & (Big) Data Governance	VU - Vrije Universiteit Amsterdam	6 weken
Advanced Master in Privacy, Cybersecurity and Data Management	Maastricht University	Geen studieduur bekend
Bachelor cyber security	Avans+	2 jaar
Basistraining Security in Systemen en Netwerken	Koning Willem I College	21 uur
Be Cyber Secure	Saxion Hogeschool	10 weken
Computer Security	Vrije Universiteit Amsterdam	120 EC
Cyber Safety & Security	NHL Stenden	120 EC
Cyber Safety & Security	NHL Stenden	120 EC
Cyber Safety and Security	NHL Stenden Hogeschool	24 maanden
Cyber Security	Hogeschool van Amsterdam	120 EC
Cyber Security	Technische Universiteit Delft	0 dagen
Cyber Security	Universiteit Leiden	Geen studieduur bekend
Cyber Security & Ethics	Hogeschool Utrecht	Geen studieduur bekend
Cyber Security & Ethics	Hogeschool Utrecht*	0 uur
Cyber Security Awareness	Deltion College	2 weken
Cyber Security Engineering	De Haagse Hogeschool	Geen studieduur bekend
Cyber Security Engineering	De Haagse Hogeschool	Geen studieduur bekend
Cyber Security Engineering	De Haagse Hogeschool	Geen studieduur bekend
Cyber Security Fundamentals	Hbo Drechtsteden (Da Vinci hbo Drechtsteden)	5 maanden
Cybersecurity	Hogeschool Inholland	120 EC
Cybersecurity for Managers and Executives: Taking the Lead	Technische Universiteit Delft	6 weken
Cybersecurity specialist	ICT College (ROC Midden Nederland)	36 maanden
Cybersecurity specialist	ICT College (ROC Midden Nederland)	36 maanden
Cybersecurity specialist	Tech Campus (ROC Midden Nederland)	36 maanden

Cybersecurity specialist	Tech Campus (ROC Midden Nederland)	36 maanden
Ethical Hacking	Hanzehogeschool Groningen (Hanzehs van Groningen)	Geen studieduur bekend
Expert IT systems and devices, Security	Mbo Rijnland mbo College Techniek & ICT (mbo Rijnland)	3 jaar
Expert IT systems and security	ICT College (ROC Midden Nederland)	36 maanden
Expert IT systems and security	Media, ICT & Design College (ROC Midden Nederland)	36 maanden
Expert IT systems and security	Tech Campus (ROC Midden Nederland)	36 maanden
Hardware Security: Physical Attacks	Universiteit van Amsterdam	2 dagen
Informatiebeveiliging	Hanzehogeschool Groningen (Hanzehs van Groningen)	Geen studieduur bekend
Informatiebeveiliging	Saxion Hogeschool	10 weken
Informatiebeveiliging en Privacywetgeving in de Praktijk (DPO) - Dag	Bestuursacademie Nederland	2 dagen
Information Security Management	De Haagse Hogeschool	240 EC
Master Course Cybercrime, Cybersecurity & Risk Management	Universiteit Twente	6 maanden
Masterclass Risks of Digitisation, Cybercrime, Prevention & Security	Universiteit Twente	4 dagen
Post-hbo Cyber Security Management	De Haagse Hogeschool	240 uur
Security and Network Engineering	Universiteit van Amsterdam	Geen studieduur bekend
Security and Safety Standardisation	HAN_ University of Applied Sciences	4 uur
The fundamentals of information security	Saxion Hogeschool	10 weken

Supplementaire tabel 14: LLO-onderwijs mbo en ho: volledig cybersecurity

Index	Volledige naam certificaat	Afkorting	Aantal	Beschrijving	Tech-nisch	M&O	Legal	Onder-zoek	Onder-wijs
1	Certified Information Systems Security Professional	CISSP	47	Dit certificaat wordt aangeboden door (ISC)² en is bedoeld voor ervaren informatiebeveiligingsprofessionals. Het behandelt een breed scala aan beveiligingstopics en is zeer gewaardeerd in de branche. Certificaten die hier nog onder vallen zijn: CISSP-ISSMP, CISSP-ISSAP.	3	2	2	0	0
2	Certified Ethical Hacker	CEH	31	De CEH-certificering, aangeboden door EC-Council, richt zich op ethisch hacken en penetratietesten. Het leert professionals hoe ze kwetsbaarheden kunnen identificeren en beveiliging kunnen verbeteren.	3	0	0	0	0
3	Certified Information Security Manager	CISM	33	Dit certificaat is ook van (ISC)² en is gericht op informatiebeveiligingsbeheer. Het richt zich op beveiligingsstrategie en governance.	2	3	2	0	0
4	Certified Information Systems Auditor	CISA	14	Ook aangeboden door ISACA, is CISA gericht op audit, controle en zekerheid van informatiesystemen. Het is waardevol voor professionals die betrokken zijn bij auditwerkzaamheden.	2	3	2	1	0
5	CompTIA Security+	CompTIA Security+	23	Dit is een toegankelijk certificaat dat de basisbeginselen van cybersecurity behandelt. Het is geschikt voor beginners en is vaak de eerste stap voor mensen die een carrière in cybersecurity willen beginnen.	3	0	0	0	0
6	Certified Cloud Security Professional	CCSP	21	Deze certificering is gericht op cloud-beveiliging en wordt aangeboden door (ISC)². Het is geschikt voor professionals die werken met cloudtechnologieën.	3	0	1	0	0
7	Certified Information Security Technician	CIST	0	Dit is een certificering die wordt aangeboden door CompTIA en is bedoeld voor technische professionals die werken aan de uitvoering van beveiligingsmaatregelen en technologieën.	2	3	0	0	0
8	Certified Information Privacy Professional	CIPP	10	Aangeboden door de International Association of Privacy Professionals (IAPP), zijn er verschillende CIPP-certificeringen beschikbaar, zoals CIPP/E (Europese privacy), CIPP/US (Amerikaanse privacy), en anderen, gericht op privacywetgeving en -beleid.	1	0	3	0	0
9	Certified Secure Software Lifecycle Professional	CSSLP	4	Ook van (ISC)², is deze certificering gericht op beveiliging gedurende de volledige levenscyclus van softwareontwikkeling en is geschikt voor beveiligingsprofessionals die betrokken zijn bij softwareontwikkeling.	3	0	1	0	0
10	Certified in Risk and Information Systems Control	CRISC	11	Aangeboden door ISACA, is CRISC gericht op beveiligingsrisicobeheer en -controle, en is bedoeld voor professionals die betrokken zijn bij risicobeheer op het gebied van in-formatiebeveiliging.	3	2	1	0	0
11	Certified Information Forensics Investigator	CIFI	9	Dit certificaat richt zich op forensische onderzoeken en wordt aangeboden door het International Association of Forensic and Security Metrology (IAFSM).	3	0	3	0	0

12	Certified Wireless Security Professional	CWSP	3	Dit certificaat richt zich op draadloze netwerkbeveiliging en wordt aangeboden door CWNP. Het is ideaal voor professionals die betrokken zijn bij het beveiligen van draadloze netwerken.	3	0	0	0	0
13	Certified Blockchain Security Professional	CBSP	4	Dit certificaat is gericht op blockchain-beveiliging en wordt aangeboden door Blockchain Training Alliance. Het is geschikt voor professionals die werken met blockchain-technologieën.	3	0	0	0	0
14	Certified IoT Security Practitioner	CIoTSP	0	Dit certificaat is gericht op beveiliging van het Internet of Things (IoT) en wordt aangeboden door CertNexus. Het behandelt de beveiligingsuitdagingen in verband met IoT-apparaten en -netwerken.	3	0	0	0	0
15	Certified Cloud Professional	CCP	5	Dit certificaat wordt aangeboden door Cloud Security Alliance en is gericht op verschillende aspecten van cloudbeveiliging, waaronder cloudarchitectuur en -beheer.	3	0	0	0	0
16	Certified Network Defender	CND	9	Gericht op netwerkbeveiliging en -verdediging.	3	0	0	0	0
17	Certified Cloud Security Specialist	CCSS	0	Voor beveiligingsspecialisten die werken met de cloud.	3	0	0	0	0
18	Offensive Security Certified Professional	OSCP	5	Concentreert zich op praktische penetratietestvaardigheden.	3	0	0	0	0
19	Certified Wireless Analysis Professional	CWAP	0	Gericht op diepgaande analyse van draadloze netwerken.	3	0	0	0	0
20	Certified Incident Response Handler	CIRH	0	Voor gespecialiseerde incidentresponsvaardigheden.	3	0	0	0	0
21	Certified Information Systems Security Officer	CISSO	5	Gericht op beveiligingsbeheer en -beleid.	3	0	0	0	0
22	Certified Cloud Security Knowledge	CCSK	6	Gericht op cloudbeveiligingskennis en -praktijken.	3	1	1	0	0

Supplementaire tabel 15: cybersecurity certificaten: aantal opleidingen uit leeroverzicht.nl dat opleidt voor dit certificaat en gescoord op de mate waarin certificaat aansluit bij arbeidsmarktcompetenties

Provincie	Initiatief	Activiteit ID	Activiteit naam	Activiteit type	Startdatum activiteit	Eind-datum	Vestigingsplaats / geografie
Zuid-Holland	Cybernetwerk Drechtsteden	25	IT security manager	Advisering/consultancy	1-1-2020		Regio Drechtsteden
Zuid-Holland	Mkb Deal Leiden	162	Coaching	Advisering/consultancy	1-9-2021		Leiden
Noord-Holland	SPOT035	538	Vaste vraagbaak voor alle stappen die je op het terrein van digitalisering wil maken	Advisering/consultancy	1-1-2021		Hilversum/Regio Gooi & Vechtstreek
Noord-Holland	Cupola XS	568	Advies door expert	Advisering/consultancy	3-1-2022		Haarlem
Landelijk	Smart Industry	605	Programma Data Delen	Advisering/consultancy	5-2-2018		Zoetermeer
Noord-Holland	Data Science Alkmaar	521	Data Science Alkmaar is een platform voor innovatie waar de triple helix goed zicht krijgt op de ontwikkelingen rond big data en kunstmatige intelligentie om deze te benutten ten behoeve van regionale economische groei en ontwikkeling.	Kennisplatform	1-1-2013		Alkmaar/ Werkgebebied Provincie NH
Noord-Holland	SPOT035	536	Workshops, webinars, cursussen en kennissessies, persoonlijk adviesgesprek, plan van aanpak, coaching en begeleiding.	Kennisplatform	1-1-2021		Hilversum/Regio Gooi & Vechtstreek
Noord-Holland	Purmervalley	545	Inspireren, informeren en verbinden. Ambitie om jongeren te inspireren en te interesseren voor een opleiding en een baan in de ICT en technologie. Optimale connectie tussen bedrijfsleven en onderwijs.	Kennisplatform	1-1-2017		Purmerend/ regio Zaanstreek waterland/West Friesland
Landelijk	Mijn Digitale Zaak	587	Platform ICT-aanbieders	Kennisplatform			Utrecht
Landelijk	Digital Trust Center	589	Kennis, informatie en advies via de website	Kennisplatform	8-6-2018		Den Haag
Landelijk	Nederland Digitaal	593	Website Nederland Digitaal	Kennisplatform	1-7-2018		Den Haag
Landelijk	Dutch Blockchain Coalition	595	Kennisbank DBC	Kennisplatform	1-3-2017		n.t.b.
Zuid-Holland	EDIH	7	Toegang tot financiering	Netwerken & coördineren	1-6-2023		MRDH
Zuid-Holland	EDIH	9	Innovatie ecosysteem en netwerken	Netwerken & coördineren	1-6-2023		MRDH
Zuid-Holland	The Hague Security Delta	51	Partijen samenbrengen voor projecten	Netwerken & coördineren	1-1-2013		Den Haag
Zuid-Holland	The Hague Security Delta	52	Ondersteuning bij het vinden van financiering	Netwerken & coördineren	1-1-2013		Den Haag

Zuid-Holland	The Hague Security Delta	53	Helpen de mismatch tussen vraag en aanbod van securitytalent op te lossen.	Netwerken & coördineren	1-1-2013		Den Haag
Zuid-Holland	Cyberweerbaarheids-centrum Greenport	75	Samenbrengen van partijen voor onderling overleg	Netwerken & coördineren	1-10-2022		Zuid-holland
Zuid-Holland	FERM Rotterdam	79	Netwerk app	Netwerken & coördineren	1-1-2017		Haven van Rotterdam
Zuid-Holland	Human Capital Cyber Security (werktitel)	151	Interactieve tool voor mkb op het gebied van Cyber Security	Netwerken & coördineren	nog te starten		Zuid-Holland
Noord-Holland	TechConnect	519	Doel is om de de kansengelijkheid op de tech-arbeidsmarkt te vergroten en tech-opleidingen en -banen toegankelijk te maken voor iedereen. Vrouwen, mensen uit sociaal kansarmere wijken en mkb'ers van eigen bodem worden tot programmeur, data-analist, 'growth hacker', UX ontwerper of tech-beheerder worden opgeleid.	Onderwijs voor professionals	1-1-2019		Amsterdam/ Werkgebied MRA
Noord-Holland	Cupola XS	571	Ontwikkeltraject & trainingen	Onderwijs voor professionals	3-1-2022		Haarlem
Noord-Holland	Smart Makers Academy	573	Skillsgerichte trainingen (metrolijn)	Onderwijs voor professionals	1-1-2021		Haarlem
Noord-Holland	3D Makers Zone	501	Skills programma	Onderwijs voor studenten	17-4-2014		Haarlem
Noord-Holland	Digital Society School	520	Bedrijf/stichting die studenten, professionals en organisaties ondersteunt dirigent en leider te worden op het gebied van digitale transformatie.	Onderwijs voor studenten	1-1-2018		Amsterdam/ werkgebied groot amsterdam. Trainees/studenten komen van heel de wereld.
Noord-Holland	House of Digital	533	Ontstaan vanuit RIF aanvraag	Onderwijs voor studenten	1-6-2018		Amsterdam/mra
Noord-Holland	De Digitale Accountant	542	Onderzoeken hoe mkb-accountantskantoren hun weg kunnen vinden in het woud van software tools, om digitalisering en data-analyse efficiënt in te kunnen zetten voor de klanten en de eigen bedrijfsvoering.	Onderwijs voor studenten	1-4-2020	1-10-2022	Amsterdam

Noord-Holland	Purmervalley	543	Inspireren, informeren en verbinden. Ambitie om jongeren te inspireren en te interesseren voor een opleiding en een baan in de ICT en technologie. Optimale connectie tussen bedrijfsleven en onderwijs.	Onderwijs voor studenten	1-1-2017		Purmerend/ regio Zaanstreek waterland/West Friesland
Noord-Holland	De Digitale Accountant	541	Onderzoeken hoe mkb-accountantskantoren hun weg kunnen vinden in het woud van software tools, om digitalisering en data-analyse efficiënt in te kunnen zetten voor de klanten en de eigen bedrijfsvoering.	Onderzoek & ontwikkeling	1-4-2020	1-10-2022	Amsterdam
Zuid-Holland	Cybernetwerk Drechtsteden	24	Doe-het-zelf-scans	Scans & assessments	1-1-2020		Regio Drechtsteden
Zuid-Holland	Cybernetwerk Drechtsteden	26	Cyberscan	Scans & assessments	1-1-2020		Regio Drechtsteden
Zuid-Holland	Cybernetwerk ZHE	57	Veiligheidsscans	Scans & assessments	1-1-2020		Oud-Beijerland
Zuid-Holland	Cyberweerbaarheids-centrum Greenport	73	Nulmeting & toolbox	Scans & assessments	1-10-2022		Zuid-holland
Zuid-Holland	FERM Rotterdam	81	Betaalde scan	Scans & assessments	1-1-2017		Haven van Rotterdam
Noord-Holland	ROMInwest	535	Innoveren: ROM InWest helpt om proposities sneller naar de markt te brengen.	Scans & assessments	1-10-2021		Haarlem/Noord Holland
Landelijk	Mijn Digitale Zaak	585	Digitaliseringsscan van KVK	Scans & assessments			Utrecht
Landelijk	Digital Trust Center	588	Basisscan Cyberweerbaarheid	Scans & assessments	14-11-2019		Den Haag
Zuid-Holland	FERM Rotterdam	80	Vouchers	Subsidies & financiering	1-1-2017		Haven van Rotterdam
Zuid-Holland	MKB010NEXT	176	Vouchers (corona)	Subsidies & financiering	1-1-2020		Rotterdam
Noord-Holland	Mkb Innovatie Topsectoren (MIT) Haalbaarheid	524	Het bevorderen van duurzame innovaties in het mkb om op deze manier een bijdrage te leveren aan een duurzame, vernieuwende en ondernemende economie. subsidie voor het uitvoeren van een haalbaarheidsproject. Dit project bestaat uit het verrichten van een haalbaarheidsstudie of uit een combinatie van een haalbaarheidsstudie met industrieel onderzoek en/of experimentele ontwikkeling.	Subsidies & financiering	1-1-2015		Provincie NH

Noord-Holland	Mkb Innovatie Topsectoren (MIT) R&D	525	Het bevorderen van duurzame innovaties in het mkb om op deze manier een bijdrage te leveren aan een duurzame, vernieuwende en ondernemende economie. Subsidie voor het uitvoeren van een Research & Development-samenwerkingsproject dat bestaat uit industrieel onderzoek of experimentele ontwikkeling of een combinatie hiervan.	Subsidies & financiering	1-1-2015		Provincie NH
Noord-Holland	Innovatiefonds NH	527	Het Fonds stelt converteerbare leningen beschikbaar voor het bewijzen van nieuwe concepten en ideeën: Proof-of-Concept.	Subsidies & financiering	1-8-2018		Provincie NH
Noord-Holland	ROMInwest	534	Investeren: ROM InWest stimuleert technologie en innovatie en laat deze via investeringen verder groeien. Hiervoor beheert ROM InWest twee fondsen: het mkb-fonds van 60 miljoen euro en het Transitiefonds met een doelkapitaal van 100 miljoen euro	Subsidies & financiering	1-10-2021		Haarlem/Noord Holland
Landelijk	Mijn Digitale Zaak	586	Digitaliseringssubsidie	Subsidies & financiering	21-6-2022		Den Haag
Landelijk	Subsidie cyberweerbaarheid	591	Subsidie cyberweerbaarheid	Subsidies & financiering	21-2-2019		Den Haag
Europees	Digital Europe Programme	619	Digitale Europe Programme	Subsidies & financiering	29-4-2021		Brussel
Zuid-Holland	Mkb Digiwerkplaats Haaglanden	153	Adviestrajecten studenten voor ondernemers	Werken met studenten	1-2-2020		Haaglanden
Zuid-Holland	Dutch Innovation Factory	155	TechTalent: studenten werken aan (innovatieve) vraagstukken van ondernemers via challenges	Werken met studenten	1-9-2019		Zoetermeer
Zuid-Holland	Digiwerkplaats Rijnmond	165	adviestrajecten studenten	Werken met studenten	1-9-2021		Rotterdam
Noord-Holland	Mkb Digital Workspace	518	Studenten lossen de digitaliseringsvraag op van bedrijven.	Werken met studenten	1-10-2019		Amsterdam/ Werkgebied MRA
Noord-Holland	Cupola XS	569	Opdrachten door studenten	Werken met studenten	3-1-2022		Haarlem
Zuid-Holland	EDIH	5	Informatie services	Workshops & kennisevents	1-6-2023		MRDH
Zuid-Holland	EDIH	6	Test before invest	Workshops & kennisevents	1-6-2023		MRDH

Zuid-Holland	Cybernetwerk Drechtsteden	23	Informatie sessies	Workshops & kennisevents	1-1-2020		Regio Drechtsteden
Zuid-Holland	The Hague Security Delta	50	Kennis vergroten	Workshops & kennisevents	1-1-2013		Den Haag
Zuid-Holland	Cybernetwerk ZHE	54	Kennisbijeenkomsten	Workshops & kennisevents	1-1-2020		Oud-Beijerland
Zuid-Holland	Cybernetwerk ZHE	55	Webinars	Workshops & kennisevents	1-1-2020		Oud-Beijerland
Zuid-Holland	Cyberweerbaarheids-centrum Greenport	74	Q&As, cybercafé, awareness sessies en informatie verspreiding	Workshops & kennisevents	1-10-2022		Zuid-holland
Zuid-Holland	FERM Rotterdam	82	Openbaar kenniscafé	Workshops & kennisevents	1-1-2017		Haven van Rotterdam
Zuid-Holland	FERM Rotterdam	83	besloten kennissessies	Workshops & kennisevents	1-1-2017		Haven van Rotterdam
Zuid-Holland	Mkb Digicafe	152	Online kennissessies om digitalisering onder de aandacht te brengen	Workshops & kennisevents	1-4-2021		Zuid-Holland
Zuid-Holland	Mkb Digiwerkplaats Haaglanden	154	Kennissessies/roadmaps voor mkb-ers	Workshops & kennisevents	1-2-2020		Haaglanden
Zuid-Holland	Mijn digitale werkplaats Drechtsteden	167	Kennissessies (thematafel met expertbedrijven, gemeentes & Provincie)	Workshops & kennisevents	1-9-2020		Dordrecht
Zuid-Holland	MKB010NEXT	175	Webinars, Sessies, Workshops	Workshops & kennisevents	1-1-2020		Rotterdam
Noord-Holland	3D Makers Zone	498	Inspiratiesessie	Workshops & kennisevents	17-4-2014		Haarlem
Noord-Holland	SPOT035	537	Vaste vraagbaak voor alle stappen die je op het terrein van digitalisering wil maken	Workshops & kennisevents	1-1-2021		Hilversum/Regio Gooi & Vechtstreek
Noord-Holland	Purmervalley	544	Inspireren, informeren en verbinden. Ambitie om jongeren te inspireren en te interesseren voor een opleiding en een baan in de ICT en technologie. Optimale connectie tussen bedrijfsleven en onderwijs.	Workshops & kennisevents	1-1-2017		Purmerend/ regio Zaanstreek waterland/West Friesland
Noord-Holland	Cupola XS	570	masterclasses	Workshops & kennisevents	1-11-2021		Haarlem

Utrecht	Cybernetwerk Utrecht		Website voor met doorverwijzingen voor ondernemers. Evenementen samen met partners (bijvoorbeeld PVO) worden ook vanuit deze website georganiseerd: https://www.cybernetwerkutrecht.nl/				
Workshop & kennisevents			Gemeente Utrecht				
Utrecht	Ondernemer centraal		Ondernemerspunt waar ondernemers terecht kunnen o.a met vragen over digitalisering	Subsidies & financiering			Gemeente Utrecht
Utrecht	Lectoraat Cybersecurity HU		Doet praktijkonderzoek naar cybersecurity op verzoek van bedrijven/brancheorganisaties	Onderzoek & ontwikkeling			Hogeschool Utrecht
Utrecht	Weerbaarheidstrainingen voor ondernemers		PVO organiseert kostenloos op verzoek van een ondernemersveniging, bedrijventerrein of andere vereniging van ondernemers workshops gericht op cyberweerbaarheid.	Workshop & kennisevents			Regio Midden Nederland
Utrecht	Cyberchef Amersfoort		Studenten van ROC Midden Nederland maken een digitale scan van een bedrijf en geven advies op maat. Dit gebeurt gratis en onder professionele begeleiding van cybersecurity professionals.	Werken met studenten			Amersfoort
Flevoland	Cyberchef Dronten		Studenten van ROC Friese Poort maken een digitale scan van een bedrijf en geven advies op maat. Dit gebeurt gratis en onder professionele begeleiding van cybersecurity professionals.	Werken met studenten			Dronten
Overijssel	WinSecure - You win, we secure!		Leveren van IT-security diensten en het opzetten van een security community om de online veiligheid in de Regio Zwolle te vergroten. Wordt uitgevoerd door studenten van Hogeschool Windesheim	Werken met studenten			Regio Zwolle
Overijssel	Cursus Cyber Security Awareness door Deltion		Cursus voor mkb-ondernemer of werknemer.om de risico's voor de cruciale digitale infrastructuur te verkleinen. Bijvoorbeeld hoe de veiligheid van de website en devices te verbeteren.				
	Workshops & kennisevents			Overijssel			
Overijssel	Cursus Cyber Aware voor beinners door ITPH Academy		Training is bedoeld voor iedereen, zowel zakelijk als privé, om digitale weerbaarheid te vergroten	Workshops & kennisevents			Overijssel

Utrecht	Bedrijvenkring Ondernemend Veenendaal		Cybermonitor	Scans & assessments			Veenendaal
Flevoland	Veilig Ondernemen Flevoland		Organiseren ook kennissessies rondom cybersecurity.	Workshops & kennisevents			Flevoland
Flevoland	Mkb Schakelteam Flevoland		De adviseurs van het mkb Schakelteam ondersteunen en adviseren mkb-bedrijven op zes thema's : strategie, organisatie, financiering, marketing, personeel en uitvoering. Kunnen doorverwijzen bij cybersecurity vraagstukken.	Scans & assessments			Flevoland
Flevoland	EDIH Digital Hub Noordwest		Ondernemers krijgen via hun regionale EDIH snel toegang tot testfaciliteiten, kennisinstellingen, experts uit het partnernetwerk en financierings- en internationaliseringsmogelijkheden. Met als doel de digitaliseringstransitie in de industrie-, zorg- en agri-en foodsectoren te versnellen.	Netwerken & coördineren			Flevoland

Supplementaire tabel 16: Regioscan digitalisering mkb - alle regionale initiatieven.

Bijlage 3. Tabellen behorende bij arbeidsmarkt

Junior						
	2018	2019	2020	2021	2022	Totaal
ECSF	271	394	419	618	951	2653
WO	66	63	67	136	118	450
HBO	188	305	334	454	727	2008
MBO	17	26	18	28	106	195
CS_Hoog	146	138	159	208	305	956
WO	34	40	41	67	52	234
HBO	112	96	115	137	243	703
MBO		2	3	4	10	19
CS_Middel	193	241	278	373	537	1622
WO	59	38	39	84	93	313
HBO	129	187	214	259	388	1177
MBO	5	16	25	30	56	132
CS_Laag	977	1465	1296	1859	2571	8168
WO	209	272	269	376	388	1514
HBO	589	933	850	1256	1728	5356
MBO	179	260	177	227	455	1298
Totaal	**1587**	**2238**	**2152**	**3058**	**4364**	**13399**

Medior						
	2018	2019	2020	2021	2022	Totaal
ECSF	721	715	1009	1534	1857	5836
WO	126	108	127	214	197	772
HBO	553	577	838	1289	1568	4825
MBO	42	30	44	31	92	239
CS_Hoog	217	212	258	386	545	1618
WO	69	60	69	94	115	407
HBO	145	150	184	287	417	1183
MBO	3	2	5	5	13	28
CS_Middel	375	342	496	773	887	2873
WO	106	66	102	176	188	638
HBO	258	259	375	577	675	2144
MBO	11	17	19	20	24	91
CS_Laag	1681	2019	2345	3361	4057	13463
WO	373	453	426	695	682	2629
HBO	1110	1401	1691	2412	3045	9659
MBO	198	165	228	254	330	1175
Totaal	**2994**	**3288**	**4108**	**6054**	**7346**	**23790**

Senior						
	2018	2019	2020	2021	2022	Totaal
ECSF	297	341	376	712	880	2606
WO	65	74	64	124	116	443
HBO	229	253	300	568	698	2048
MBO	3	14	12	20	66	115
CS_Hoog	133	132	122	221	275	883
WO	43	33	46	69	55	246
HBO	87	99	70	149	215	620
MBO	3		6	3	5	17
CS_Middel	224	227	166	398	468	1483
WO	65	41	34	97	107	344
HBO	155	181	129	291	327	1083
MBO	4	5	3	10	34	56
CS_Laag	968	813	909	1666	2146	6502
WO	268	206	238	433	425	1570
HBO	615	538	574	1114	1463	4304
MBO	85	69	97	119	258	628
Totaal	**1622**	**1513**	**1573**	**2997**	**3769**	**11474**

Onbekend						
	2018	2019	2020	2021	2022	Totaal
ECSF	359	355	436	620	588	2358
WO	65	46	50	91	76	328
HBO	280	288	363	518	474	1923
MBO	14	21	23	11	38	107
CS_Hoog	120	128	118	166	190	722
WO	30	19	19	34	28	130
HBO	89	105	94	131	156	575
MBO	1	4	5	1	6	17
CS_Middel	203	165	218	285	356	1227
WO	40	39	37	47	49	212
HBO	147	117	170	219	272	925
MBO	16	9	11	19	35	90
CS_Laag	1122	1235	1449	1929	2231	7966
WO	188	172	218	323	276	1177
HBO	721	764	927	1282	1516	5210
MBO	213	299	304	324	439	1579
Totaal	**1804**	**1883**	**2221**	**3000**	**3365**	**12273**

Supplementaire tabel 17: Vacatures naar opleidingsniveau, werkervaring en jaar. Bron: Jobdigger, bewerking Dialogic

1. Noord-Holland

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	1035
2	ECSF - CISO	ECSF	885
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	502
4	ECSF - Cybersecurity Architect	ECSF	430
5	ECSF - Cybersecurity Auditor	ECSF	198
6	ECSF - Cybersecurity Risk Manager	ECSF	187
7	Cyber Security Consultant	CS_Hoog	160
8	ECSF - Penetration Tester	ECSF	130
9	Consultant	CS_Middel	115
10	Auditor	CS_Laag	108
11	Systeembeheerder	CS_Laag	93
12	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	89
13	Privacy Officer	CS_Middel	83
14	Security Consultant	CS_Middel	79
15	Manager	CS_Middel	78
16	ECSF - Digital Forensics Investigator	ECSF	73
17	ECSF - Cyber Incident Responder	ECSF	71
18	Software Engineer	CS_Laag	65
19	Functionaris (gegevensbescherming)	CS_Hoog	60
20	ECSF - Cybersecurity Researcher	#VERW!	59

2. Zuid-Holland

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	950
2	ECSF - CISO	ECSF	893
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	296
4	ECSF - Cybersecurity Architect	ECSF	289
5	ECSF - Cybersecurity Risk Manager	ECSF	252
6	ECSF - Cybersecurity Researcher	ECSF	188
7	ECSF - Penetration Tester	ECSF	152
8	ECSF - Cybersecurity Auditor	ECSF	136
9	Privacy Officer	CS_Middel	107
10	Functioneel Beheerder	CS_Laag	97
11	Systeembeheerder	CS_Laag	90
12	Security Consultant	CS_Middel	78
13	Adviseur Informatiebeveiliging	CS_Hoog	76
14	Projectmanager	CS_Laag	69
15	Functionaris	CS_Hoog	67
16	Auditor	CS_Laag	67
17	Consultant	CS_Middel	63
18	Adviseur	CS_Middel	59
19	ECSF - Digital Forensics Investigator	ECSF	57
20	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	56

3. Utrecht

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	723
2	ECSF - Cybersecurity Implementer	ECSF	566
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	331
4	ECSF - Cybersecurity Architect	ECSF	238
5	ECSF - Cybersecurity Risk Manager	ECSF	188
6	ECSF - Penetration Tester	ECSF	112
7	Privacy Officer	CS_Middel	103
8	Traineeship Programma	CS_Laag	86
9	ECSF - Cybersecurity Auditor	ECSF	74
10	Security Consultant	CS_Middel	71
11	Auditor	CS_Laag	66
12	Cyber Security Consultant	CS_Hoog	62
13	Systeembeheerder	CS_Laag	60
14	ECSF - Cyber Incident Responder	ECSF	60
15	Webdeveloper	CS_Middel	59
16	Adviseur Informatiebeveiliging	CS_Hoog	59
17	Accountmanager	CS_Laag	55
18	Informatiemanager	CS_Laag	48
19	Projectmanager	CS_Laag	45
20	Consultant	CS_Middel	45

4. Noord-Brabant

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	404
2	ECSF - Cybersecurity Implementer	ECSF	324
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	239
4	ECSF - Cybersecurity Architect	ECSF	139
5	ECSF - Cybersecurity Researcher	ECSF	114
6	Systeembeheerder	CS_Laag	96
7	ECSF - Cybersecurity Risk Manager	ECSF	65
8	ECSF - Cybersecurity Auditor	ECSF	65
9	ECSF - Penetration Tester	ECSF	62
10	Privacy Officer	CS_Middel	56
11	Security Consultant	CS_Middel	49
12	Auditor	CS_Laag	45
13	Adviseur	CS_Middel	44
14	Koerier	CS_Laag	43
15	ECSF - Cyber Incident Responder	ECSF	43
16	Adviseur Informatiebeveiliging	CS_Hoog	43
17	Functionaris	CS_Hoog	36
18	Consultant	CS_Middel	35
19	Netwerkbeheerder	CS_Laag	30
20	ECSF - Cybersecurity Educator	ECSF	29

5. Gelderland

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	304
2	ECSF - Cybersecurity Implementer	ECSF	224
3	ECSF - Cybersecurity Architect	ECSF	171
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	113
5	ECSF - Cybersecurity Risk Manager	ECSF	63
6	ECSF - Cybersecurity Auditor	ECSF	49
7	Systeembeheerder	CS_Laag	48
8	Auditor	CS_Laag	41
9	Privacy Officer	CS_Middel	37
10	Security Consultant	CS_Middel	32
11	Functionaris	CS_Hoog	30
12	ECSF - Penetration Tester	ECSF	27
13	Informatiemanager	CS_Laag	23
14	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	23
15	Traineeship Informatiemanagement Overheid	CS_Laag	21
16	Consultant	CS_Middel	21
17	Architect	CS_Laag	21
18	Adviseur Informatiebeveiliging	CS_Hoog	19
19	Koerier	CS_Laag	17
20	Accountmanager	CS_Laag	17

6. Overijssel

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	288
2	ECSF - CISO	ECSF	144
3	ECSF - Cybersecurity Researcher	ECSF	42
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	42
5	ECSF - Cybersecurity Architect	ECSF	37
6	Technicus IndustriÃ¥le Automatisering	CS_Laag	33
7	Software Engineer	CS_Laag	27
8	ECSF - Cybersecurity Risk Manager	ECSF	27
9	Systeembeheerder	CS_Laag	26
10	Functionaris	CS_Hoog	26
11	Adviseur Smart Industriële Automatisering	CS_Laag	24
12	Privacy Officer	CS_Middel	23
13	Adviseur Informatiebeveiliging	CS_Hoog	21
14	Adviseur Machineveiligheid	CS_Laag	20
15	Cloud Architect	CS_Laag	20
16	Informatiemanager	CS_Laag	18
17	Aankomend Specialist Technisch Installatie	CS_Laag	18
18	Middelbaar Veiligheidskundige	CS_Laag	16
19	Adviseur Digitaal Vertrouwen	CS_Laag	16
20	System Architect	CS_Laag	15

7. Limburg

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	114
2	ECSF - CISO	ECSF	103
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	29
4	ECSF - Cybersecurity Architect	ECSF	28
5	Koerier	CS_Laag	27
6	Privacy Officer	CS_Middel	24
7	Auditor	CS_Laag	18
8	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	18
9	ECSF - Cybersecurity Risk Manager	ECSF	17
10	Functionaris	CS_Hoog	17
11	Traineeship Informatiemanagement Overheid	CS_Laag	16
12	Systeembeheerder	CS_Laag	13
13	Projectleider	CS_Laag	13
14	ECSF - Digital Forensics Investigator	ECSF	13
15	Projectleider Software	CS_Laag	12
16	Functioneel Beheerder	CS_Laag	12
17	Beleidsmedewerker	CS_Laag	12
18	Integratie Specialist	CS_Laag	12
19	Sales Manager	CS_Middel	11
20	Technisch Medewerker Secundair	CS_Laag	10

8. Groningen

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	62
2	ECSF - Cybersecurity Implementer	ECSF	51
3	ECSF - Cybersecurity Researcher	ECSF	38
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	36
5	Crypto Specialist	CS_Middel	16
6	Software Developer	CS_Laag	16
7	ECSF - Cybersecurity Auditor	ECSF	13
8	Traineeship Informatiemanagement Overheid	CS_Laag	12
9	Functioneel Beheerder	CS_Laag	12
10	ECSF - Cybersecurity Architect	ECSF	10
11	Microsoft Server Specialist	CS_Laag	10
12	ECSF - Penetration Tester	ECSF	10
13	Adviseur Compliancy	CS_Middel	9
14	ECSF - Cybersecurity Risk Manager	ECSF	8
15	Jurist	CS_Laag	8
16	Adviseur Informatiebeveiliging	CS_Hoog	8
17	Adviseur	CS_Middel	8
18	Onderzoeker Crypto	CS_Laag	7
19	Privacy Officer	CS_Middel	7
20	Integraal Beveiligingscoördinator	CS_Hoog	7

9. Flevoland

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	33
2	ECSF - Cybersecurity Implementer	ECSF	23
3	ECSF - Penetration Tester	ECSF	20
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	19
5	Engineer Protection Automation Control	CS_Laag	10
6	ECSF - Cyber Incident Responder	ECSF	9
7	Sales Manager	CS_Middel	8
8	Privacy Officer	CS_Middel	7
9	Cloud Infrastructure Specialist	CS_Laag	7
10	ECSF - Cybersecurity Educator	ECSF	7
11	Adviseur	CS_Middel	6
12	Product Owner	CS_Laag	6
13	Systeembeheerder	CS_Laag	6
14	Consultant	CS_Middel	5
15	Projectleider ICT	CS_Laag	5
16	Audio & Video Engineer	CS_Laag	5
17	Software Engineer	CS_Laag	5
18	Adviseur Informatiemanagement	CS_Laag	5
19	Inspire Programmeur	CS_Laag	5
20	Account Manager High	CS_Laag	5

10. Friesland

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	42
2	Functionaris	CS_Hoog	13
3	Privacy Officer	CS_Middel	13
4	Docent Integrale Veiligheidskunde	CS_Laag	11
5	Netwerkbeheerder	CS_Laag	10
6	ECSF - Cybersecurity Implementer	ECSF	10
7	Technicus a Energietechniek	CS_Laag	9
8	Software Engineer	CS_Laag	7
9	Product Manager	CS_Middel	7
10	Systeembeheerder	CS_Laag	7
11	C# Delphi Software Engineer	CS_Laag	7
12	Professor IT Security	CS_Hoog	6
13	Beleidsmedewerker Openbare Orde Veiligheid	CS_Laag	6
14	Data Analist	CS_Laag	6
15	.NET Software Developer	CS_Laag	6
16	Projectcoördinator	CS_Laag	5
17	Data Engineer	CS_Laag	5
18	Manager ICT	CS_Laag	5
19	Technicus a Operationele Technologie	CS_Laag	5
20	R&D Engineer	CS_Laag	4

11. Drenthe

#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	33
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	13
3	Chauffeur	CS_Laag	13
4	ECSF - Cybersecurity Implementer	ECSF	10
5	Security Manager	CS_Middel	9
6	ECSF - Cybersecurity Architect	ECSF	8
7	Technisch Cmdb Beheerder	CS_Laag	7
8	Technisch Medewerker Secundair	CS_Laag	7
9	Adviseur Informatiebeveiliging	CS_Hoog	6
10	Systeembeheerder	CS_Laag	6
11	Privacy Officer	CS_Middel	6
12	ECSF - Cybersecurity Risk Manager	ECSF	6
13	Informatiemanager	CS_Laag	5
14	Call Center Agent Dutch	CS_Laag	5
15	Projectmanager	CS_Laag	5
16	Functionaris	CS_Hoog	5
17	ICT Coördinator	CS_Laag	5
18	Java Ontwikkelaar	CS_Laag	5
19	Adviseur	CS_Middel	4
20	Business Manager	CS_Laag	4

12. Zeeland

#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	24
2	ECSF - Cybersecurity Architect	ECSF	23
3	ECSF - CISO	ECSF	21
4	ICT Technicus Specialisatie IT	CS_Laag	20
5	Functioneel Beheerder	CS_Laag	9
6	Traineeship Informatiemanagement Overheid	CS_Laag	9
7	Netwerkbeheerder	CS_Laag	8
8	Project Engineer Simulation Based	CS_Laag	7
9	ECSF - Cyber Threat Intelligence Specialist	ECSF	6
10	Process Automation Engineer	CS_Laag	5
11	Functionaris	CS_Hoog	5
12	ICT Systeemspecialist Cloud	CS_Laag	4
13	Beleidsmedewerker	CS_Laag	4
14	Adviseur Informatiebeveiliging & Privacy	CS_Hoog	4
15	Adviseur	CS_Middel	4
16	Systeem/Applicatie Beheerder	CS_Laag	4
17	ECSF - Cybersecurity Risk Manager	ECSF	4
18	Engineer / Specialist Telecom	CS_Laag	4
19	Planner	CS_Laag	3
20	Beleidsmedewerker Informatievoorziening ICT	CS_Laag	3

Supplementaire tabel 18: De top 20 functieprofielen per regio. Bron: Jobdigger, bewerking Dialogic

Junior - WO			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Researcher	ECSF	97
2	ECSF - CISO	ECSF	84
3	ECSF - Cybersecurity Implementer	ECSF	69
4	ECSF - Cybersecurity Auditor	ECSF	64
5	ECSF - Cyber Threat Intelligence Specialist	ECSF	50
6	Sales & Marketing Intern	CS_Laag	32
7	Consultant	CS_Middel	32
8	ECSF - Penetration Tester	ECSF	23
9	Traineeship	CS_Middel	21
10	Crypto Specialist	CS_Middel	21
11	ECSF - Cybersecurity Architect	ECSF	21
12	Trainee	CS_Laag	20
13	Jurist	CS_Laag	20
14	ECSF - Digital Forensics Investigator	ECSF	20
15	Officier	CS_Laag	19
16	Consultant IT Assurance	CS_Laag	18
17	Privacy Officer	CS_Middel	17
18	Manager IT Risk Mitigation	CS_Hoog	17
19	Associate	CS_Laag	17
20	Digital Assurance Traineeship	CS_Laag	16

Junior - HBO			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	572
2	ECSF - CISO	ECSF	456
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	262
4	ECSF - Cybersecurity Risk Manager	ECSF	175
5	ECSF - Penetration Tester	ECSF	174
6	ECSF - Cybersecurity Architect	ECSF	112
7	Consultant	CS_Middel	91
8	ECSF - Cybersecurity Auditor	ECSF	90
9	Traineeship Informatiemanagement Overheid	CS_Laag	86
10	Traineeship Programma	CS_Laag	84
11	Auditor	CS_Laag	78
12	Privacy Officer	CS_Middel	72
13	Cyber Security Consultant	CS_Hoog	70
14	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	58
15	Accountmanager	CS_Laag	53
16	Systeembeheerder	CS_Laag	49
17	Digitaal Specialist	CS_Middel	46
18	Adviseur Informatiebeveiliging	CS_Hoog	46
19	Traineeship	CS_Middel	44
20	Engineer	CS_Laag	44

Junior - MBO			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	115
2	Systeembeheerder	CS_Laag	52
3	Koerier	CS_Laag	43
4	Medewerker operations	CS_Laag	31
5	ECSF - Cyber Threat Intelligence Specialist	ECSF	30
6	Support Engineer	CS_Laag	27
7	Servicedesk Medewerker	CS_Laag	21
8	Administratief Medewerker	CS_Laag	21
9	ECSF - CISO	ECSF	21
10	ECSF - Cybersecurity Risk Manager	ECSF	20
11	Netwerkbeheerder	CS_Laag	17
12	Accountmanager	CS_Laag	17
13	Medewerker Operations	CS_Laag	16
14	IT Support Medewerker	CS_Laag	16
15	Commercieel Medewerker	CS_Laag	16
16	Chauffeur	CS_Laag	15
17	Managementondersteuner	CS_Laag	13
18	Medewerker ICT	CS_Laag	12
19	ICT Specialist	CS_Laag	12
20	Informatiespecialist Verandermanager	CS_Laag	12

Medior - WO			
#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	292
2	ECSF - Cybersecurity Implementer	ECSF	123
3	ECSF - Cybersecurity Architect	ECSF	119
4	Functionaris	CS_Hoog	64
5	ECSF - Cyber Threat Intelligence Specialist	ECSF	60
6	ECSF - Cybersecurity Auditor	ECSF	58
7	ECSF - Cybersecurity Researcher	ECSF	51
8	Auditor	CS_Laag	49
9	Cyber Security Consultant	CS_Hoog	46
10	Privacy Officer	CS_Middel	41
11	Manager	CS_Middel	35
12	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	31
13	Compliance Officer	CS_Laag	31
14	IT Risk Manager	CS_Middel	30
15	Informatiemanager	CS_Laag	28
16	Product Consultant	CS_Laag	27
17	Consultant	CS_Middel	22
18	Enterprise Architect	CS_Laag	21
19	Engineer	CS_Laag	21
20	Data Scientist	CS_Laag	18

Medior - HBO			
#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	1377
2	ECSF - Cybersecurity Implementer	ECSF	1299
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	615
4	ECSF - Cybersecurity Architect	ECSF	594
5	ECSF - Cybersecurity Risk Manager	ECSF	330
6	ECSF - Penetration Tester	ECSF	178
7	ECSF - Cybersecurity Auditor	ECSF	148
8	Security Consultant	CS_Middel	137
9	Functioneel Beheerder	CS_Laag	115
10	Privacy Officer	CS_Middel	108
11	ECSF - Cyber Incident Responder	ECSF	104
12	Systeembeheerder	CS_Laag	99
13	Auditor	CS_Laag	98
14	Cyber Security Consultant	CS_Hoog	89
15	Adviseur Informatiebeveiliging	CS_Hoog	87
16	Accountmanager	CS_Laag	83
17	Projectmanager	CS_Laag	77
18	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	76
19	Architect	CS_Laag	71
20	Informatiemanager	CS_Laag	70

Medior - MBO			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	146
2	Systeembeheerder	CS_Laag	99
3	ECSF - CISO	ECSF	40
4	Netwerkbeheerder	CS_Laag	39
5	ECSF - Cyber Threat Intelligence Specialist	ECSF	29
6	Technicus a Energietechniek	CS_Laag	22
7	ICT Technicus Specialisatie IT	CS_Laag	18
8	Middelbaar Veiligheidskundige	CS_Laag	17
9	Support Engineer	CS_Laag	17
10	Servicedesk Medewerker ICT	CS_Laag	14
11	ICT Specialist	CS_Laag	14
12	ECSF - Cybersecurity Risk Manager	ECSF	14
13	Technicus Energietechniek	CS_Laag	13
14	Medewerker ICT	CS_Laag	13
15	Security Consultant	CS_Middel	12
16	Support Medewerker	CS_Laag	12
17	Technisch Applicatiebeheerder	CS_Laag	11
18	Servicedesk Medewerker	CS_Laag	11
19	Werkplekbeheerder	CS_Laag	11
20	Office Manager	CS_Laag	10

Senior - WO			
#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	130
2	ECSF - Cybersecurity Researcher	ECSF	89
3	ECSF - Cybersecurity Architect	ECSF	62
4	ECSF - Cybersecurity Implementer	ECSF	55
5	ECSF - Cybersecurity Auditor	ECSF	45
6	Auditor	CS_Laag	44
7	Jurist Privacy	CS_Middel	41
8	Manager Justitie & Veiligheid	CS_Laag	22
9	ECSF - Cyber Threat Intelligence Specialist	ECSF	22
10	Privacy Officer	CS_Middel	21
11	Functionaris	CS_Hoog	21
12	Consultant Financial Risk Management	CS_Laag	20
13	Associate & Financial Consulting	CS_Laag	20
14	Werkstudent & Quantitative Consulting	CS_Laag	19
15	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	18
16	Projectmanager	CS_Laag	17
17	Consultant / Manager	CS_Laag	17
18	Sales & Marketing Intern	CS_Laag	16
19	Consultant Operational & Value	CS_Laag	16
20	Cyber Security Consultant	CS_Hoog	15

Senior- HBO			
#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	550
2	ECSF - Cybersecurity Implementer	ECSF	496
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	296
4	ECSF - Cybersecurity Architect	ECSF	273
5	ECSF - Cybersecurity Risk Manager	ECSF	136
6	Privacy Officer	CS_Middel	96
7	ECSF - Cybersecurity Auditor	ECSF	86
8	ECSF - Penetration Tester	ECSF	67
9	Security Consultant	CS_Middel	64
10	Traineeship Informatiemanagement Overheid	CS_Laag	60
11	ECSF - Cyber Incident Responder	ECSF	51
12	Consultant	CS_Middel	48
13	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	43
14	Systeembeheerder	CS_Laag	41
15	Accountmanager	CS_Laag	41
16	Functionaris	CS_Hoog	38
17	Product Owner	CS_Laag	37
18	Projectmanager	CS_Laag	35
19	Cyber Security Consultant	CS_Hoog	35
20	Adviseur	CS_Middel	32

Senior - MBO			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	65
2	Technisch Medewerker Secundair	CS_Laag	25
3	ECSF - CISO	ECSF	20
4	Support Engineer	CS_Laag	18
5	Systeembeheerder	CS_Laag	17
6	Netwerkbeheerder	CS_Laag	13
7	ECSF - Cybersecurity Auditor	ECSF	11
8	Rechercheur	CS_Laag	8
9	ECSF - Cyber Threat Intelligence Specialist	ECSF	8
10	Administratief Medewerker	CS_Laag	8
11	Generalist Tactische Opsporing	CS_Middel	8
12	Werkplekbeheerder	CS_Laag	8
13	Hosting Engineer Paas	CS_Laag	7
14	Planner	CS_Laag	7
15	Specialist BRP	CS_Laag	7
16	Medewerker ICT	CS_Laag	6
17	Tactisch Rechercheur	CS_Middel	6
18	Infrastructure Platform Specialist	CS_Laag	6
19	IT Service Desk Medewerker	CS_Laag	6
20	Technicus	CS_Laag	5

Supplementaire tabel 19: De top 20 functieprofielen per ervaringscategorie en opleidingsniveau. Bron: Jobdigger, bewerking Dialogic

Op basis van de top 100 organisaties

Cyber R&D			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Researcher	ECSF	100
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	33
3	ECSF - Cybersecurity Implementer	ECSF	26
4	Crypto Specialist	CS_Middel	22
5	ECSF - Cybersecurity Educator	ECSF	20
6	Onderzoeker Crypto	CS_Laag	12
7	Security Talent	CS_Middel	12
8	Candidates	CS_Laag	10
9	Startfunctie	CS_Middel	10
10	Docent Software Engineering	CS_Laag	7
11	ECSF - CISO	ECSF	7
12	Coach Hogeschooldocent ICT	CS_Laag	6
13	Onderzoeker	CS_Hoog	6
14	Outstanding Pdeng Candidate	CS_Laag	6
15	ECSF - Cybersecurity Risk Manager	ECSF	6
16	Research	CS_Laag	6
17	Cyber Workforce Developer	CS_Middel	4
18	Projectleider Cyber Security	CS_Hoog	4
19	Projectleider Veilige Maatschappij	CS_Laag	4
20	Lector Cyber Security	CS_Middel	4

Cyberproductie			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	464
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	317
3	ECSF - Cybersecurity Architect	ECSF	254
4	ECSF - CISO	ECSF	233
5	ECSF - Penetration Tester	ECSF	181
6	Cyber Security Consultant	CS_Hoog	170
7	ECSF - Cybersecurity Risk Manager	ECSF	152
8	ECSF - Cyber Incident Responder	ECSF	100
9	ECSF - Digital Forensics Investigator	ECSF	93
10	Consultant	CS_Middel	90
11	ECSF - Cybersecurity Auditor	ECSF	73
12	Cybersecurity Consultant	CS_Hoog	73
13	Projectmanager	CS_Laag	60
14	Webdeveloper	CS_Middel	55
15	Cloud Security Consultant	CS_Middel	54
16	Privacy Consultant	CS_Middel	51
17	Manager	CS_Middel	51
18	Accountmanager	CS_Laag	44
19	Technisch Applicatiebeheerder	CS_Laag	43
20	Security Consultant	CS_Middel	43

Cyberintegratie			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	904
2	ECSF - CISO	ECSF	646
3	ECSF - Cybersecurity Architect	ECSF	447
4	ECSF - Cyber Threat Intelligence Specialist	ECSF	440
5	ECSF - Cybersecurity Auditor	ECSF	258
6	ECSF - Cybersecurity Risk Manager	ECSF	172
7	Koerier	CS_Laag	132
8	Auditor	CS_Laag	106
9	ECSF - Penetration Tester	ECSF	91
10	Traineeship Programma	CS_Laag	85
11	Privacy Officer	CS_Middel	82
12	Software Engineer	CS_Laag	72
13	ECSF - Cyber Incident Responder	ECSF	69
14	Product Owner	CS_Laag	51
15	Engineer	CS_Laag	51
16	Analist	CS_Middel	48
17	Business Analist	CS_Laag	45
18	Adviseur Informatiebeveiliging	CS_Hoog	44
19	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	43
20	Security Manager	CS_Middel	36

Onderwijs-/kennisinstellingen			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Researcher	ECSF	100
2	ECSF - Cybersecurity Educator	ECSF	35
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	34
4	ECSF - Cybersecurity Implementer	ECSF	26
5	Crypto Specialist	CS_Middel	22
6	ECSF - CISO	ECSF	18
7	Onderzoeker Crypto	CS_Laag	12
8	Security Talent	CS_Middel	12
9	Informatiemanager	CS_Laag	11
10	Startfunctie	CS_Middel	10
11	Candidates	CS_Laag	10
12	Functioneel Beheerder	CS_Laag	9
13	Software Engineer	CS_Laag	7
14	Docent Software Engineering	CS_Laag	7
15	ECSF - Cybersecurity Risk Manager	ECSF	7
16	Privacy Officer	CS_Middel	6
17	Outstanding Pdeng Candidate	CS_Laag	6
18	Research	CS_Laag	6
19	Coach Hogeschooldocent ICT	CS_Laag	6
20	Onderzoeker	CS_Hoog	6

Bedrijfsleven			
#	Functieprofiel	Type	Aantal
1	ECSF - Cybersecurity Implementer	ECSF	1379
2	ECSF - CISO	ECSF	690
3	ECSF - Cyber Threat Intelligence Specialist	ECSF	658
4	ECSF - Cybersecurity Architect	ECSF	572
5	ECSF - Cybersecurity Auditor	ECSF	285
6	ECSF - Penetration Tester	ECSF	269
7	ECSF - Cybersecurity Risk Manager	ECSF	256
8	Cyber Security Consultant	CS_Hoog	217
9	ECSF - Cyber Incident Responder	ECSF	158
10	Traineeship Informatiemanagement Overheid	CS_Laag	146
11	Auditor	CS_Laag	139
12	Koerier	CS_Laag	132
13	Consultant	CS_Middel	125
14	ECSF - Digital Forensics Investigator	ECSF	95
15	Projectmanager	CS_Laag	90
16	Traineeship Programma	CS_Laag	85
17	ECSF - Cyber Legal, Policy & Compliance Officer	ECSF	78
18	Security Consultant	CS_Middel	77
19	Software Engineer	CS_Laag	74
20	Cybersecurity Consultant	CS_Hoog	74

Overheid			
#	Functieprofiel	Type	Aantal
1	ECSF - CISO	ECSF	282
2	ECSF - Cyber Threat Intelligence Specialist	ECSF	269
3	ECSF - Cybersecurity Architect	ECSF	260
4	ECSF - Cybersecurity Implementer	ECSF	199
5	ECSF - Cybersecurity Risk Manager	ECSF	131
6	Digitaal Specialist	CS_Middel	119
7	ECSF - Cybersecurity Auditor	ECSF	107
8	Privacy Officer	CS_Middel	43
9	Adviseur Informatiebeveiliging	CS_Hoog	41
10	Analist	CS_Middel	40
11	Adviseur	CS_Middel	38
12	Auditor	CS_Laag	35
13	Security Manager	CS_Middel	31
14	Rechercheur	CS_Laag	29
15	Officier	CS_Laag	29
16	ICT Beheerder	CS_Laag	28
17	Functioneel Beheerder	CS_Laag	27
18	Accountmanager Publiek Private Samenwerking	CS_Hoog	26
19	Luchtmacht Officier ICT	CS_Laag	25
20	Financieel Rechercheur	CS_Middel	25

Supplementaire tabel 20: Vraag naar functieprofielen (op basis van de top 100 organisaties). Bron: Jobdigger, bewerking Dialogic

#	ECSF-profiel	Categorie	% vacatures
	Key knowledge		
1	Cybersecurity standards, methodologies and frameworks	Technisch	57,6%
2	Cyber threats	Technisch	52,1%
3	Cybersecurity controls and solutions	Technisch	51,4%
4	Cybersecurity risks	Technisch	43,6%
5	Cybersecurity related laws, regulations and legislations	Legal	40,3%
6	Cybersecurity procedures	Man. & Org.	33,3%
7	Cybersecurity recommendations and best practices	Man. & Org.	30,2%
8	Management practices	Man. & Org.	27,8%
9	Cybersecurity-related technologies	Technisch	26,8%
10	Cybersecurity policies	Man. & Org.	24,3%
	Key skill(s)		
1	Identify, analyse and correlate cybersecurity events	Onderzoek	51,6%
2	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	45,5%
3	Motivate and encourage people	Man. & Org.	44,3%
4	Collaborate with other team members and colleagues	Man. & Org.	28,1%
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9,7%
6	Develop codes, scripts and programmes	Technisch	7,2%
7	Develop code, scripts and programmes	Technisch	7,2%
8	Identify and exploit vulnerabilities	Technisch	4,7%
9	Conduct ethical hacking	Technisch	4,4%
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technisch	3,9%
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	41,4%
2	Cooperate and share information with authorities and professional groups	Man. & Org.	31,7%
3	Collaborate with other teams and colleagues	Man. & Org.	28,1%
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	21,2%
5	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technisch	4,4%
6	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Onderwijs	3,9%
7	Design and propose a secure architecture to implement the organisation's strategy	Technisch	3,2%
8	Enforce and advocate organisation's data privacy and protection program	Legal	2,9%
9	Deploy penetration testing tools and penetration test programs	Technisch	2,9%
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technisch	2,4%

Supplementaire tabel 21: Top 10 taken, vaardigheden en kennis voor ECSF-profielen. Bron: Jobdigger, bewerking Dialogic

#	Functietitel - CS-hoog	Categorie	% vacatures
	Key knowledge		
1	Cybersecurity standards, methodologies and frameworks	Technisch	66,0%
2	Cyber threats	Technisch	62,1%
3	Cybersecurity risks	Technisch	51,8%
4	Cybersecurity related laws, regulations and legislations	Legal	49,2%
5	Cybersecurity controls and solutions	Technisch	45,0%
6	Cybersecurity recommendations and best practices	Man. & Org.	42,6%
7	Cybersecurity procedures	Man. & Org.	40,7%
8	Management practices	Man. & Org.	36,8%
9	Cybersecurity policies	Man. & Org.	35,5%
10	Cybersecurity-related technologies	Technisch	17,6%
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	57,1%
2	Identify, analyse and correlate cybersecurity events	Onderzoek	56,0%
3	Collaborate with other team members and colleagues	Man. & Org.	38,0%
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	27,2%
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7,9%
6	Think creatively and outside the box	Onderzoek	4,2%
7	Conduct ethical hacking	Technisch	4,2%
8	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	3,5%
9	Identify and exploit vulnerabilities	Technisch	3,5%
10	Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Technisch	3,4%
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	53,7%
2	Cooperate and share information with authorities and professional groups	Man. & Org.	39,4%
3	Collaborate with other teams and colleagues	Man. & Org.	38,0%
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	27,8%
5	Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions	Onderzoek	5,1%
6	Enforce and advocate organisation's data privacy and protection program	Legal	5,0%
7	Manage legal aspects of information security responsibilities and third-party relations	Legal	3,3%
8	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	3,2%
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Onderwijs	3,0%
10	Design and propose a secure architecture to implement the organisation's strategy	Technisch	3,0%

Supplementaire tabel 22: Top 10 taken, vaardigheden en kennis voor profielen met een hoog cybersecurity gehalte. Bron: Jobdigger, bewerking Dialogic

#	Functietitel - CS-middel	Categorie	% vacatures
	Key knowledge		
1	Cybersecurity standards, methodologies and frameworks	Technisch	53,5%
2	Cyber threats	Technisch	48,1%
3	Cybersecurity controls and solutions	Technisch	44,6%
4	Cybersecurity related laws, regulations and legislations	Legal	44,4%
5	Cybersecurity risks	Technisch	41,8%
6	Cybersecurity recommendations and best practices	Man. & Org.	33,7%
7	Cybersecurity procedures	Man. & Org.	33,7%
8	Management practices	Man. & Org.	30,0%
9	Cybersecurity policies	Man. & Org.	25,2%
10	Cybersecurity-related technologies	Technisch	16,9%
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	49,5%
2	Identify, analyse and correlate cybersecurity events	Onderzoek	48,3%
3	Collaborate with other team members and colleagues	Man. & Org.	34,7%
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	29,3%
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10,0%
6	Develop code, scripts and programmes	Technisch	5,0%
7	Develop codes, scripts and programmes	Technisch	5,0%
8	Think creatively and outside the box	Onderzoek	4,2%
9	Conduct ethical hacking	Technisch	3,6%
10	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	3,3%
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	48,0%
2	Cooperate and share information with authorities and professional groups	Man. & Org.	37,8%
3	Collaborate with other teams and colleagues	Man. & Org.	34,7%
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25,2%
5	Enforce and advocate organisation's data privacy and protection program	Legal	5,2%
6	Manage legal aspects of information security responsibilities and third-party relations	Legal	4,4%
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	4,4%
8	Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions	Onderzoek	4,0%
9	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technisch	2,7%
10	Develop organisation's cybersecurity architecture to address security and privacy requirements	Technisch	2,6%

Supplementaire tabel 23: Top 10 taken, vaardigheden en kennis voor profielen met een substantieel cybersecurity gehalte. Bron: Jobdigger, bewerking Dialogic

#	Functietitel - CS-laag	Categorie	% vacatures
	Key knowledge		
1	Cybersecurity controls and solutions	Technisch	39,6%
2	Cybersecurity standards, methodologies and frameworks	Technisch	37,6%
3	Management practices	Man. & Org.	30,5%
4	Cybersecurity related laws, regulations and legislations	Legal	29,0%
5	Cybersecurity procedures	Man. & Org.	26,7%
6	Cyber threats	Technisch	24,4%
7	Cybersecurity recommendations and best practices	Man. & Org.	21,8%
8	Cybersecurity policies	Man. & Org.	18,2%
9	Cybersecurity risks	Technisch	17,1%
10	Multidiscipline aspect of cybersecurity	Man. & Org.	8,3%
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	41,3%
2	Identify, analyse and correlate cybersecurity events	Onderzoek	35,3%
3	Collaborate with other team members and colleagues	Man. & Org.	31,2%
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	26,8%
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10,1%
6	Develop codes, scripts and programmes	Technisch	6,0%
7	Develop code, scripts and programmes	Technisch	6,0%
8	Think creatively and outside the box	Onderzoek	4,3%
9	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	2,7%
10	Work under pressure	Man. & Org.	2,3%
	Main task(s)		
1	Cooperate and share information with authorities and professional groups	Man. & Org.	38,1%
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	37,5%
3	Collaborate with other teams and colleagues	Man. & Org.	31,2%
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26,2%
5	Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions	Onderzoek	3,1%
6	Enforce and advocate organisation's data privacy and protection program	Legal	2,5%
7	Deploy penetration testing tools and penetration test programs	Technisch	1,2%
8	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technisch	0,7%
9	Develop organisation's cybersecurity architecture to address security and privacy requirements	Technisch	0,6%
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Onderwijs	0,5%

Supplementaire tabel 24: Top 10 taken, vaardigheden en kennis voor profielen met een laag cybersecurity gehalte. Bron: Jobdigger

1. ECSF - CISO

#	Certificaat	Aantal vacatures
1	CISSP	1799
2	CISM	1537
3	CISA	875
4	CIPP	290
5	CRISC	253
6	CCSP	201
7	CEH	144
8	CIPM	111
9	GIAC	48
10	OSCP	47

Manager

#	Certificaat	Aantal vacatures
1	CISSP	217
2	CEH	128
3	CISM	87
4	CISA	60
5	GCIH	82
6	OSCP	50
7	GSEC	33
8	GIAC	28
9	GCIA	21
10	CCSP	20

2. ECSF - Cyber Threat Intelligence

#	Certificaat	Aantal vacatures
1	CISSP	454
2	CISM	246
3	CEH	166
4	CISA	157
5	OSCP	80
6	CCSP	78
7	GIAC	69
8	GCIH	63
9	CRISC	27
10	SSCP	27

7. Privacy Officer

#	Certificaat	Aantal vacatures
1	CIPP	199
2	CIPM	119
3	CISSP	14
4	CISM	6
5	CDPSE	5
6	CISA	5

3. ECSF - Cybersecurity

#	Certificaat	Aantal vacatures
1	CISSP	334
2	CISM	126
3	CEH	113
4	OSCP	65
5	CSSLP	52
6	CISA	44
7	CCSP	35
8	SSCP	35
9	GIAC	28
10	GCIH	24

8. ECSF - Cybersecurity Auditor

#	Certificaat	Aantal vacatures
1	CISA	132
2	CISSP	110
3	CISM	39
4	CCSP	34
5	CEH	20
6	CRISC	18
7	CSSLP	11
8	OSCP	4

4. ECSF - Cybersecurity Architect

#	Certificaat	Aantal vacatures
1	CISSP	366
2	CISM	145
3	CCSP	99
4	CISA	75
5	CEH	42
6	CRISC	35
7	OSCP	24
8	GIAC	15
9	CISSP-ISSAP	15
10	CHFI	12

9. Security Consultant

#	Certificaat	Aantal vacatures
1	CISSP	154
2	CISM	111
3	CISA	62
4	CEH	35
5	CCSP	23
6	CIPP	18
7	OSCP	18
8	SSCP	4
9	CRISC	4
10	CSSLP	4

5. ECSF - Penetration Tester

#	Certificaat	Aantal vacatures
1	OSCP	278
2	CISSP	81
3	OSCE	81
4	CEH	62
5	CISA	30
6	GIAC	21
7	GWAPT	15
8	CISM	12
9	CSSLP	10
10	ECSA	9

10. Cyber Security Consultant

#	Certificaat	Aantal vacatures
1	CISSP	150
2	CISM	128
3	CISA	88
4	CIPP	48
5	CRISC	30
6	CEH	22
7	OSCP	20
8	CCSP	13
9	CIPM	6
10	OSCE	4

Supplementaire tabel 25: Top 10 gevraagde certificaten voor de 10 functies waarin de meeste certificaten worden gevraagd. Bron: Jobdigger, bewerking Dialogic.

1. Noord-Holland

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	40%	6803
2	Cooperate and share information with authorities and professional groups	Man. & Org.	32%	5369
3	Collaborate with other teams and colleagues	Man. & Org.	26%	4291
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	21%	3585
5	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	5%	809
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	551
7	Design and propose a secure architecture to implement the organisation's strategy	Technisch	3%	459
8	Assess cybersecurity risks and propose most appropriate risk treatment options, inc	Technisch	3%	458
9	Deploy penetration testing tools and penetration test programs	Technisch	2%	414
10	Implement threat intelligence collection, analysis and production of actionable inte	Technisch	2%	288
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	7356
2	Identify, analyse and correlate cybersecurity events	Onderzoek	41%	6894
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	32%	5447
4	Collaborate with other team members and colleagues	Man. & Org.	26%	4291
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	2167
6	Develop code, scripts and programmes	Technisch	7%	1187
7	Develop codes, scripts and programmes	Technisch	7%	1187
8	Anticipate required changes to the organisation's information security strategy and	Man. & Org.	4%	694
9	Think creatively and outside the box	Onderzoek	3%	532
10	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	3%	431
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	43%	7285
2	Cybersecurity standards, methodologies and frameworks	Technisch	41%	6812
3	Cyber threats	Technisch	37%	6197
4	Management practices	Man. & Org.	37%	6152
5	Cybersecurity risks	Technisch	30%	5100
6	Cybersecurity related laws, regulations and legislations	Legal	30%	4975
7	Cybersecurity procedures	Man. & Org.	25%	4224
8	Cybersecurity recommendations and best practices	Man. & Org.	23%	3891
9	Cybersecurity-related technologies	Technisch	18%	3016
10	Cybersecurity policies	Man. & Org.	16%	2658

2. Zuid-Holland

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	43%	6707
2	Cooperate and share information with authorities and professional groups	Man. & Org.	39%	6104
3	Collaborate with other teams and colleagues	Man. & Org.	34%	5293
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	28%	4379
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	422
6	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	2%	367
7	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	256
8	Deploy penetration testing tools and penetration test programs	Technisch	1%	218
9	Assess cybersecurity risks and propose most appropriate risk treatment options, inc	Technisch	1%	190
10	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	181
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	6775
2	Identify, analyse and correlate cybersecurity events	Onderzoek	44%	6736
3	Collaborate with other team members and colleagues	Man. & Org.	34%	5296
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30%	4622
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	1198
6	Develop code, scripts and programmes	Technisch	5%	801
7	Develop codes, scripts and programmes	Technisch	5%	801
8	Think creatively and outside the box	Onderzoek	5%	789
9	Work under pressure	Man. & Org.	3%	424
10	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	2%	336
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	48%	7395
2	Cybersecurity controls and solutions	Technisch	42%	6511
3	Cybersecurity related laws, regulations and legislations	Legal	39%	6029
4	Cyber threats	Technisch	36%	5622
5	Cybersecurity procedures	Man. & Org.	34%	5226
6	Management practices	Man. & Org.	29%	4415
7	Cybersecurity risks	Technisch	28%	4371
8	Cybersecurity recommendations and best practices	Man. & Org.	27%	4242
9	Cybersecurity policies	Man. & Org.	25%	3861
10	Cybersecurity-related technologies	Technisch	13%	1965

3. Utrecht

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	40%	4500
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	39%	4317
3	Collaborate with other teams and colleagues	Man. & Org.	36%	3963
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	26%	2883
5	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	3%	281
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	259
7	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	186
8	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	2%	177
9	Conduct privacy impact assessments and develop, maintain, communicate and train	Legal	2%	177
10	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	154
	Key skill(s)			
1	Identify, analyse and correlate cybersecurity events	Onderzoek	43%	4765
2	Motivate and encourage people	Man. & Org.	43%	4734
3	Collaborate with other team members and colleagues	Man. & Org.	36%	3963
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30%	3383
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	1131
6	Think creatively and outside the box	Onderzoek	6%	696
7	Develop codes, scripts and programmes	Technisch	6%	630
8	Develop code, scripts and programmes	Technisch	6%	630
9	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	3%	340
10	Conduct ethical hacking	Man. & Org.	3%	284
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	49%	5428
2	Cybersecurity controls and solutions	Technisch	41%	4547
3	Cyber threats	Technisch	39%	4306
4	Cybersecurity related laws, regulations and legislations	Legal	35%	3922
5	Cybersecurity risks	Technisch	30%	3373
6	Cybersecurity procedures	Man. & Org.	30%	3372
7	Cybersecurity recommendations and best practices	Man. & Org.	28%	3159
8	Management practices	Man. & Org.	26%	2889
9	Cybersecurity policies	Man. & Org.	22%	2400
10	Cybersecurity-related technologies	Technisch	12%	1371

4. Noord-Brabant

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	41%	2472
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	2173
3	Collaborate with other teams and colleagues	Man. & Org.	28%	1690
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	24%	1470
5	Enforce and advocate organisation's data privacy and protection program	Legal	5%	288
6	Assess cybersecurity risks and propose most appropriate risk treatment options, inc	Technisch	4%	243
7	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	4%	226
8	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	141
9	Conduct research, innovation and development work in cybersecurity-related topics	Onderzoek	2%	141
10	Deploy penetration testing tools and penetration test programs	Technisch	2%	114
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	46%	2788
2	Identify, analyse and correlate cybersecurity events	Onderzoek	38%	2336
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	33%	2035
4	Collaborate with other team members and colleagues	Man. & Org.	28%	1690
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	11%	695
6	Develop codes, scripts and programmes	Technisch	7%	409
7	Develop code, scripts and programmes	Technisch	7%	409
8	Decompose and analyse systems to develop security and privacy requirements and	Technisch	4%	258
9	Identify and exploit vulnerabilities	Technisch	3%	177
10	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	2%	141
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	49%	2951
2	Cybersecurity standards, methodologies and frameworks	Technisch	44%	2687
3	Cybersecurity related laws, regulations and legislations	Legal	33%	2025
4	Cyber threats	Technisch	32%	1919
5	Management practices	Man. & Org.	30%	1809
6	Cybersecurity procedures	Man. & Org.	29%	1779
7	Cybersecurity recommendations and best practices	Man. & Org.	26%	1604

5. Gelderland

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	42%	1666
2	Cooperate and share information with authorities and professional groups	Man. & Org.	35%	1390
3	Collaborate with other teams and colleagues	Man. & Org.	32%	1253
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	25%	980
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	114
6	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	2%	85
7	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	58
8	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	1%	46
9	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	1%	43
10	Implement threat intelligence collection, analysis and production of actionable inte	Technisch	1%	39
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	45%	1783
2	Identify, analyse and correlate cybersecurity events	Onderzoek	44%	1746
3	Collaborate with other team members and colleagues	Man. & Org.	32%	1253
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30%	1182
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	209
6	Develop code, scripts and programmes	Technisch	5%	181
7	Develop codes, scripts and programmes	Technisch	5%	181
8	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	4%	150
9	Think creatively and outside the box	Onderzoek	2%	82
10	Work under pressure	Man. & Org.	2%	78
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	50%	1962
2	Cybersecurity controls and solutions	Technisch	42%	1650
3	Cybersecurity related laws, regulations and legislations	Legal	40%	1585
4	Cyber threats	Technisch	39%	1522
5	Cybersecurity procedures	Man. & Org.	35%	1367
6	Cybersecurity risks	Technisch	31%	1237
7	Cybersecurity recommendations and best practices	Man. & Org.	29%	1138

6. Overijssel

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	40%	1139
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	1015
3	Collaborate with other teams and colleagues	Man. & Org.	34%	969
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	26%	721
5	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	3%	72
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	52
7	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	1%	30
8	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	26
9	Assess cybersecurity risks and propose most appropriate risk treatment options, inc	Technisch	1%	20
10	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	1%	20
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47%	1322
2	Identify, analyse and correlate cybersecurity events	Onderzoek	42%	1183
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	37%	1036
4	Collaborate with other team members and colleagues	Man. & Org.	34%	969
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	270
6	Develop codes, scripts and programmes	Technisch	6%	169
7	Develop code, scripts and programmes	Technisch	6%	169
8	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	2%	61
9	Conduct ethical hacking	Technisch	1%	42
10	Think creatively and outside the box	Onderzoek	1%	40
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	56%	1575
2	Cybersecurity standards, methodologies and frameworks	Technisch	47%	1340
3	Cybersecurity related laws, regulations and legislations	Legal	31%	864
4	Cyber threats	Technisch	30%	834
5	Cybersecurity recommendations and best practices	Man. & Org.	27%	773
6	Management practices	Man. & Org.	27%	763
7	Cybersecurity risks	Technisch	24%	664

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	37%	598
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	582
3	Collaborate with other teams and colleagues	Man. & Org.	34%	550
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	27%	431
5	Enforce and advocate organisation's data privacy and protection program	Legal	6%	95
6	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Legal	4%	57
7	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	2%	40
8	Manage legal aspects of information security responsibilities and third-party relatio	Legal	2%	36
9	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	32
10	Deploy penetration testing tools and penetration test programs	Technisch	2%	27
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	42%	678
2	Identify, analyse and correlate cybersecurity events	Onderzoek	37%	607
3	Collaborate with other team members and colleagues	Man. & Org.	34%	550
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	29%	472
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7%	116
6	Think creatively and outside the box	Onderzoek	7%	108
7	Develop codes, scripts and programmes	Technisch	5%	85
8	Develop code, scripts and programmes	Technisch	5%	85
9	Work under pressure	Man. & Org.	3%	55
10	Decompose and analyse systems to develop security and privacy requirements and i	Technisch	2%	37
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	49%	801
2	Cybersecurity controls and solutions	Technisch	41%	672
3	Cybersecurity related laws, regulations and legislations	Legal	34%	549
4	Cybersecurity procedures	Man. & Org.	33%	542
5	Cyber threats	Technisch	30%	483
6	Cybersecurity recommendations and best practices	Man. & Org.	28%	454
7	Management practices	Man. & Org.	27%	445
8	Cybersecurity policies	Man. & Org.	26%	420
9	Cybersecurity risks	Technisch	21%	345
10	Multidiscipline aspect of cybersecurity	Man. & Org.	9%	148

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	41%	469
2	Collaborate with other teams and colleagues	Man. & Org.	37%	416
3	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	37%	415
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	26%	298
5	Manage legal aspects of information security responsibilities and third-party relatio	Legal	2%	19
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	19
7	Conduct privacy impact assessments and develop, maintain, communicate and train	Legal	1%	14
8	Deploy penetration testing tools and penetration test programs	Technisch	1%	13
9	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	1%	12
10	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	1%	11
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47%	535
2	Identify, analyse and correlate cybersecurity events	Onderzoek	44%	496
3	Collaborate with other team members and colleagues	Man. & Org.	37%	417
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	31%	353
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	62
6	Develop codes, scripts and programmes	Technisch	4%	51
7	Develop code, scripts and programmes	Technisch	4%	51
8	Think creatively and outside the box	Onderzoek	4%	42
9	Design systems and architectures based on security and privacy by design and by de	Technisch	3%	32
10	Decompose and analyse systems to develop security and privacy requirements and i	Technisch	2%	20
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	53%	598
2	Cybersecurity related laws, regulations and legislations	Legal	39%	442
3	Cybersecurity controls and solutions	Technisch	37%	420
4	Cyber threats	Technisch	34%	390
5	Cybersecurity procedures	Man. & Org.	33%	375
6	Cybersecurity policies	Man. & Org.	33%	370
7	Cybersecurity recommendations and best practices	Man. & Org.	30%	339
8	Management practices	Man. & Org.	28%	317
9	Cybersecurity risks	Technisch	25%	286
10	Multidiscipline aspect of cybersecurity	Man. & Org.	8%	87

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	39%	239
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	36%	221
3	Collaborate with other teams and colleagues	Man. & Org.	35%	211
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	27%	166
5	Manage legal aspects of information security responsibilities and third-party relatio	Legal	3%	19
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	16
7	Conduct privacy impact assessments and develop, maintain, communicate and train	Legal	2%	14
8	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	10
9	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	2%	10
10	Implement threat intelligence collection, analysis and production of actionable intel	Technisch	1%	9
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	45%	277
2	Identify, analyse and correlate cybersecurity events	Onderzoek	40%	242
3	Collaborate with other team members and colleagues	Man. & Org.	35%	211
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	33%	200
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	12%	74
6	Develop codes, scripts and programmes	Technisch	7%	41
7	Develop code, scripts and programmes	Technisch	7%	41
8	Think creatively and outside the box	Onderzoek	6%	35
9	Conduct ethical hacking	Technisch	4%	26
10	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	4%	23
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	46%	284
2	Cybersecurity procedures	Man. & Org.	42%	256
3	Cybersecurity controls and solutions	Technisch	42%	255
4	Cybersecurity related laws, regulations and legislations	Legal	38%	233
5	Cyber threats	Technisch	38%	230
6	Management practices	Man. & Org.	35%	211
7	Cybersecurity risks	Technisch	30%	181
8	Cybersecurity recommendations and best practices	Man. & Org.	27%	165
9	Cybersecurity policies	Man. & Org.	25%	155
10	Cybersecurity-related technologies	Technisch	10%	62

10. Friesland

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	42%	259
2	Collaborate with other teams and colleagues	Man. & Org.	39%	236
3	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	36%	217
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	31%	191
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	21
6	Identify cross-sectoral cybersecurity achievements and apply them in a different cor	Onderzoek	2%	15
7	Design and propose a secure architecture to implement the organisation's strategy	Technisch	2%	12
8	Assist in designing, implementing, auditing and compliance testing activities in orde	Man. & Org.	2%	10
9	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	9
10	Conduct privacy impact assessments and develop, maintain, communicate and train	Legal	1%	7
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	42%	259
2	Collaborate with other team members and colleagues	Man. & Org.	39%	236
3	Identify, analyse and correlate cybersecurity events	Onderzoek	35%	216
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	19%	118
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	47
6	Develop codes, scripts and programmes	Technisch	4%	22
7	Develop code, scripts and programmes	Technisch	4%	22
8	Think creatively and outside the box	Onderzoek	3%	18
9	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	3%	18
10	Work under pressure	Man. & Org.	3%	16
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	45%	272
2	Cybersecurity related laws, regulations and legislations	Legal	40%	245
3	Cybersecurity procedures	Man. & Org.	33%	200
4	Cybersecurity controls and solutions	Technisch	32%	198
5	Management practices	Man. & Org.	32%	194
6	Cybersecurity policies	Man. & Org.	29%	179
7	Cybersecurity recommendations and best practices	Man. & Org.	26%	159
8	Cyber threats	Technisch	25%	150

11. Drenthe

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	43%	202
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	43%	202
3	Collaborate with other teams and colleagues	Man. & Org.	37%	173
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	29%	136
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	13
6	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	1%	7
7	Conduct privacy impact assessments and develop, maintain, communicate and train	Legal	1%	5
8	Ensure the senior management approves the cybersecurity risks of the organisation	Man. & Org.	1%	4
9	Assist in cybersecurity-related capacity building including awareness, theoretical tra	Onderwijs	1%	4
10	Manage legal aspects of information security responsibilities and third-party relatio	Legal	1%	4
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	48%	224
2	Identify, analyse and correlate cybersecurity events	Onderzoek	44%	208
3	Collaborate with other team members and colleagues	Man. & Org.	37%	173
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	28%	133
5	Identify and select appropriate pedagogical approaches for the intended audience	Onderzoek	6%	27
6	Develop codes, scripts and programmes	Technisch	4%	21
7	Develop code, scripts and programmes	Technisch	4%	21
8	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	4%	21
9	Design systems and architectures based on security and privacy by design and by de	Technisch	3%	14
10	Work under pressure	Man. & Org.	3%	12
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	56%	261
2	Cybersecurity related laws, regulations and legislations	Legal	45%	211
3	Cybersecurity procedures	Man. & Org.	39%	183
4	Cybersecurity controls and solutions	Technisch	39%	182
5	Cybersecurity policies	Man. & Org.	38%	178
6	Cyber threats	Technisch	35%	163
7	Cybersecurity recommendations and best practices	Man. & Org.	33%	156
8	Management practices	Man. & Org.	32%	150

12. Zeeland

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	116
2	Collaborate with other teams and colleagues	Man. & Org.	36%	115
3	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	27%	88
4	Cooperate with key personnel for reporting of security incidents according to applic	Legal	25%	80
5	Enforce and advocate organisation's data privacy and protection program	Legal	5%	17
6	Manage legal aspects of information security responsibilities and third-party relatio	Legal	4%	12
7	Assess cybersecurity risks and propose most appropriate risk treatment options, ind	Technisch	2%	8
8	Develop and propose staff awareness training to achieve compliance and foster a cu	Onderwijs	2%	7
9	Deploy penetration testing tools and penetration test programs	Technisch	1%	4
10	Develop organisation's cybersecurity architecture to address security and privacy re	Technisch	1%	2
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	38%	122
2	Identify, analyse and correlate cybersecurity events	Onderzoek	38%	121
3	Collaborate with other team members and colleagues	Man. & Org.	36%	115
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	27%	87
5	Think creatively and outside the box	Onderzoek	9%	28
6	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	17
7	Develop code, scripts and programmes	Technisch	4%	13
8	Develop codes, scripts and programmes	Technisch	4%	13
9	Anticipate required changes to the organisation's information security strategy and	Man. & Org.	3%	10
10	Decompose and analyse systems to develop security and privacy requirements and i	Technisch	3%	9
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	42%	135
2	Cybersecurity procedures	Man. & Org.	33%	107
3	Cybersecurity related laws, regulations and legislations	Legal	33%	106
4	Cybersecurity policies	Man. & Org.	29%	93
5	Cyber threats	Technisch	26%	83
6	Cybersecurity controls and solutions	Technisch	25%	80
7	Management practices	Man. & Org.	23%	73
8	Cybersecurity risks	Technisch	21%	69

Supplementaire tabel 26: individuele taken, kennis en vaardigheden die gevraagd worden in de regio's

Junior - MBO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	30%	490
2	Collaborate with other teams and colleagues	Man. & Org.	26%	429
3	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	26%	425
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	19%	309
5	Enforce and advocate organisation's data privacy and protection program	Legal	2%	25
6	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	1%	10
7	Deploy penetration testing tools and penetration test programs	Technisch	1%	10
8	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	1%	9
9	Implement threat intelligence collection, analysis and production of actionable in	Technisch	1%	9
10	Identify and assess cybersecurity-related threats and vulnerabilities of ICT system	Onderzoek	0%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	41%	677
2	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	31%	503
3	Identify, analyse and correlate cybersecurity events	Onderzoek	29%	472
4	Collaborate with other team members and colleagues	Man. & Org.	26%	429
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	88
6	Think creatively and outside the box	Onderzoek	5%	76
7	Work under pressure	Man. & Org.	4%	69
8	Develop code, scripts and programmes	Technisch	4%	61
9	Develop codes, scripts and programmes	Technisch	4%	61
10	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	2%	36
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	38%	622
2	Management practices	Man. & Org.	31%	505
3	Cybersecurity standards, methodologies and frameworks	Technisch	29%	482
4	Cyber threats	Technisch	29%	475
5	Cybersecurity related laws, regulations and legislations	Legal	24%	389
6	Cybersecurity procedures	Man. & Org.	23%	378
7	Cybersecurity risks	Technisch	17%	280
8	Cybersecurity recommendations and best practices	Man. & Org.	15%	246
9	Cybersecurity policies	Man. & Org.	11%	183
10	Cybersecurity-related technologies	Technisch	10%	163

Junior - HBO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	35%	3257
2	Cooperate and share information with authorities and professional groups	Man. & Org.	34%	3188
3	Collaborate with other teams and colleagues	Man. & Org.	30%	2782
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	24%	2194
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	234
6	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	2%	206
7	Develop organisation's cybersecurity architecture to address security and privacy	Technisch	2%	167
8	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	1%	123
9	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	1%	119
10	Manage legal aspects of information security responsibilities and third-party relat	Legal	1%	114
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	4086
2	Identify, analyse and correlate cybersecurity events	Onderzoek	43%	3929
3	Collaborate with other team members and colleagues	Man. & Org.	30%	2782
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30%	2745
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	757
6	Develop code, scripts and programmes	Technisch	8%	715
7	Develop codes, scripts and programmes	Technisch	8%	715
8	Think creatively and outside the box	Onderzoek	4%	362
9	Conduct ethical hacking	Technisch	3%	271
10	Work under pressure	Man. & Org.	3%	241
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	44%	4085
2	Cybersecurity controls and solutions	Technisch	43%	3940
3	Cyber threats	Technisch	36%	3299
4	Cybersecurity related laws, regulations and legislations	Legal	33%	3062
5	Management practices	Man. & Org.	29%	2690
6	Cybersecurity risks	Technisch	28%	2574
7	Cybersecurity procedures	Man. & Org.	28%	2563
8	Cybersecurity recommendations and best practices	Man. & Org.	26%	2435
9	Cybersecurity policies	Man. & Org.	20%	1806
10	Cybersecurity-related technologies	Technisch	14%	1253

Junior - WO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	48%	1200
2	Cooperate and share information with authorities and professional groups	Man. & Org.	45%	1141
3	Collaborate with other teams and colleagues	Man. & Org.	39%	991
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	30%	750
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	2%	54
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	49
7	Develop organisation's cybersecurity architecture to address security and privacy	Technisch	2%	42
8	Conduct privacy impact assessments and develop, maintain, communicate and tra	Legal	2%	39
9	Deploy penetration testing tools and penetration test programs	Technisch	1%	35
10	Manage legal aspects of information security responsibilities and third-party relat	Legal	1%	29
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	54%	1365
2	Identify, analyse and correlate cybersecurity events	Onderzoek	48%	1200
3	Collaborate with other team members and colleagues	Man. & Org.	39%	991
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	25%	635
5	Develop code, scripts and programmes	Technisch	10%	242
6	Develop codes, scripts and programmes	Technisch	10%	242
7	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9%	223
8	Think creatively and outside the box	Onderzoek	3%	87
9	Work under pressure	Man. & Org.	3%	64
10	Conduct ethical hacking	Technisch	2%	61
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	44%	1116
2	Cybersecurity controls and solutions	Technisch	40%	1014
3	Management practices	Man. & Org.	37%	928
4	Cybersecurity related laws, regulations and legislations	Legal	36%	895
5	Cybersecurity recommendations and best practices	Man. & Org.	35%	890
6	Cyber threats	Technisch	35%	875
7	Cybersecurity procedures	Man. & Org.	31%	772
8	Cybersecurity risks	Technisch	28%	713
9	Cybersecurity policies	Man. & Org.	24%	593
10	Multidiscipline aspect of cybersecurity	Man. & Org.	15%	385

Medior - MBO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	28%	429
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	26%	392
3	Collaborate with other teams and colleagues	Man. & Org.	24%	373
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	20%	308
5	Enforce and advocate organisation's data privacy and protection program	Legal	2%	25
6	Deploy penetration testing tools and penetration test programs	Technisch	1%	20
7	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	1%	18
8	Contribute to the development of the organisation's cybersecurity strategy, polic	Man. & Org.	1%	9
9	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	1%	9
10	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	1%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	40%	617
2	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	37%	561
3	Identify, analyse and correlate cybersecurity events	Onderzoek	26%	400
4	Collaborate with other team members and colleagues	Man. & Org.	24%	373
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	79
6	Think creatively and outside the box	Onderzoek	3%	48
7	Develop codes, scripts and programmes	Technisch	3%	40
8	Develop code, scripts and programmes	Technisch	3%	40
9	Work under pressure	Man. & Org.	2%	36
10	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	2%	36
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	40%	608
2	Cybersecurity standards, methodologies and frameworks	Technisch	36%	552
3	Cyber threats	Technisch	30%	465
4	Management practices	Man. & Org.	30%	464
5	Cybersecurity procedures	Man. & Org.	29%	443
6	Cybersecurity related laws, regulations and legislations	Legal	26%	398
7	Cybersecurity recommendations and best practices	Man. & Org.	18%	270
8	Cybersecurity risks	Technisch	16%	245
9	Cybersecurity policies	Man. & Org.	16%	241
10	Cybersecurity-related technologies	Technisch	13%	195

Medior - HBO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	43%	7637
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	6348
3	Collaborate with other teams and colleagues	Man. & Org.	30%	5342
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	24%	4349
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	4%	672
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	590
7	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	3%	551
8	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	2%	368
9	Design and propose a secure architecture to implement the organisation's strateg	Technisch	2%	353
10	Deploy penetration testing tools and penetration test programs	Technisch	2%	321
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	43%	7656
2	Identify, analyse and correlate cybersecurity events	Onderzoek	43%	7586
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	36%	6491
4	Collaborate with other team members and colleagues	Man. & Org.	30%	5343
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	1726
6	Develop code, scripts and programmes	Technisch	6%	1152
7	Develop codes, scripts and programmes	Technisch	6%	1152
8	Think creatively and outside the box	Onderzoek	4%	701
9	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	3%	507
10	Decompose and analyse systems to develop security and privacy requirements an	Technisch	3%	489
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	51%	9084
2	Cybersecurity controls and solutions	Technisch	48%	8605
3	Cyber threats	Technisch	39%	6979
4	Cybersecurity related laws, regulations and legislations	Legal	36%	6375
5	Cybersecurity procedures	Man. & Org.	32%	5637
6	Cybersecurity risks	Technisch	31%	5608
7	Management practices	Man. & Org.	31%	5457
8	Cybersecurity recommendations and best practices	Man. & Org.	27%	4797
9	Cybersecurity policies	Man. & Org.	21%	3764
10	Cybersecurity-related technologies	Technisch	17%	3048

Medior - WO

#	Bouwsteen	Categorie	% vacatures	Aantal vacatures
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	52%	2301
2	Cooperate and share information with authorities and professional groups	Man. & Org.	47%	2081
3	Collaborate with other teams and colleagues	Man. & Org.	41%	1818
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	34%	1505
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	5%	218
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	152
7	Conduct privacy impact assessments and develop, maintain, communicate and tra	Legal	2%	96
8	Deploy penetration testing tools and penetration test programs	Technisch	2%	89
9	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	2%	88
10	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	2%	86
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	52%	2314
2	Identify, analyse and correlate cybersecurity events	Onderzoek	49%	2161
3	Collaborate with other team members and colleagues	Man. & Org.	41%	1818
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	28%	1234
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	14%	617
6	Develop code, scripts and programmes	Technisch	6%	245
7	Develop codes, scripts and programmes	Technisch	6%	245
8	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	3%	155
9	Think creatively and outside the box	Onderzoek	3%	149
10	Work under pressure	Man. & Org.	3%	128
	Key knowledge			
1	Cybersecurity standards, methodologies and frameworks	Technisch	56%	2471
2	Cybersecurity related laws, regulations and legislations	Legal	44%	1976
3	Cybersecurity controls and solutions	Technisch	44%	1952
4	Cyber threats	Technisch	40%	1767
5	Cybersecurity recommendations and best practices	Man. & Org.	37%	1644
6	Management practices	Man. & Org.	36%	1597
7	Cybersecurity procedures	Man. & Org.	36%	1585
8	Cybersecurity risks	Technisch	36%	1581
9	Cybersecurity policies	Man. & Org.	32%	1430
10	Multidiscipline aspect of cybersecurity	Man. & Org.	12%	539

Senior - MBO					
#	Bouwsteen	Categorie	% vacatures	Aantal vacatures	
	Main task(s)				
1	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	295	
2	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	35%	288	
3	Collaborate with other teams and colleagues	Man. & Org.	35%	282	
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	23%	191	
5	Deploy penetration testing tools and penetration test programs	Technisch	4%	29	
6	Enforce and advocate organisation's data privacy and protection program	Legal	1%	11	
7	Identify and assess cybersecurity-related threats and vulnerabilities of ICT system	Onderzoek	1%	10	
8	Assess cybersecurity risks and propose most appropriate risk treatment options,	Technisch	1%	10	
9	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	1%	7	
10	Develop organisation's cybersecurity architecture to address security and privacy	Technisch	0%	4	
	Key skill(s)				
1	Motivate and encourage people	Man. & Org.	46%	377	
2	Identify, analyse and correlate cybersecurity events	Onderzoek	37%	302	
3	Collaborate with other team members and colleagues	Man. & Org.	35%	282	
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	33%	266	
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7%	54	
6	Work under pressure	Man. & Org.	6%	47	
7	Think creatively and outside the box	Onderzoek	4%	30	
8	Assess the security and performance of solutions	Technisch	4%	29	
9	Develop codes, scripts and programmes	Technisch	3%	22	
10	Develop code, scripts and programmes	Technisch	3%	22	
	Key knowledge				
1	Cybersecurity controls and solutions	Technisch	43%	351	
2	Cybersecurity standards, methodologies and frameworks	Technisch	34%	279	
3	Cybersecurity related laws, regulations and legislations	Legal	33%	270	
4	Cyber threats	Technisch	32%	258	
5	Management practices	Man. & Org.	31%	256	
6	Cybersecurity procedures	Man. & Org.	30%	245	
7	Cybersecurity risks	Technisch	16%	132	
8	Cybersecurity recommendations and best practices	Man. & Org.	15%	121	
9	Cybersecurity-related technologies	Technisch	10%	83	
10	Cybersecurity policies	Man. & Org.	10%	78	

Senior - HBO					
#	Bouwsteen	Categorie	% vacatures	Aantal vacatures	
	Main task(s)				
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	44%	3568	
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	2867	
3	Collaborate with other teams and colleagues	Man. & Org.	30%	2399	
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	25%	1988	
5	Identify cross-sectoral cybersecurity achievements and apply them in a different	Onderzoek	5%	420	
6	Enforce and advocate organisation's data privacy and protection program	Legal	4%	344	
7	Design and propose a secure architecture to implement the organisation's strate	Technisch	2%	196	
8	Assess cybersecurity risks and propose most appropriate risk treatment options,	Technisch	2%	169	
9	Deploy penetration testing tools and penetration test programs	Technisch	2%	168	
10	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	2%	167	
	Key skill(s)				
1	Identify, analyse and correlate cybersecurity events	Onderzoek	45%	3600	
2	Motivate and encourage people	Man. & Org.	44%	3536	
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	33%	2645	
4	Collaborate with other team members and colleagues	Man. & Org.	30%	2399	
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	1045	
6	Think creatively and outside the box	Onderzoek	5%	381	
7	Develop codes, scripts and programmes	Technisch	4%	348	
8	Develop code, scripts and programmes	Technisch	4%	348	
9	Anticipate required changes to the organisation's information security strategy a	Man. & Org.	4%	286	
10	Conduct ethical hacking	Technisch	3%	221	
	Key knowledge				
1	Cybersecurity standards, methodologies and frameworks	Technisch	46%	3717	
2	Cybersecurity controls and solutions	Technisch	46%	3681	
3	Cyber threats	Technisch	39%	3179	
4	Cybersecurity related laws, regulations and legislations	Legal	35%	2847	
5	Cybersecurity risks	Technisch	32%	2583	
6	Management practices	Man. & Org.	32%	2544	
7	Cybersecurity procedures	Man. & Org.	29%	2316	
8	Cybersecurity recommendations and best practices	Man. & Org.	28%	2231	
9	Cybersecurity policies	Man. & Org.	21%	1681	
10	Cybersecurity-related technologies	Technisch	17%	1378	

Senior - WO					
#	Bouwsteen	Categorie	% vacatures	Aantal vacatures	
	Main task(s)				
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	54%	1398	
2	Cooperate and share information with authorities and professional groups	Man. & Org.	46%	1197	
3	Collaborate with other teams and colleagues	Man. & Org.	39%	1006	
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	33%	846	
5	Identify cross-sectoral cybersecurity achievements and apply them in a different	Onderzoek	4%	109	
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	77	
7	Design and propose a secure architecture to implement the organisation's strate	Technisch	2%	49	
8	Deploy penetration testing tools and penetration test programs	Technisch	2%	47	
9	Manage legal aspects of information security responsibilities and third-party rela	Legal	2%	46	
10	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	2%	44	
	Key skill(s)				
1	Identify, analyse and correlate cybersecurity events	Onderzoek	51%	1326	
2	Motivate and encourage people	Man. & Org.	51%	1320	
3	Collaborate with other team members and colleagues	Man. & Org.	39%	1009	
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	22%	572	
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	334	
6	Develop code, scripts and programmes	Technisch	4%	116	
7	Develop codes, scripts and programmes	Technisch	4%	116	
8	Think creatively and outside the box	Onderzoek	3%	86	
9	Design systems and architectures based on security and privacy by design and by	Technisch	3%	78	
10	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	3%	75	
	Key knowledge				
1	Cybersecurity standards, methodologies and frameworks	Technisch	48%	1254	
2	Cybersecurity related laws, regulations and legislations	Legal	43%	1127	
3	Management practices	Man. & Org.	40%	1042	
4	Cyber threats	Technisch	38%	984	
5	Cybersecurity controls and solutions	Technisch	36%	944	
6	Cybersecurity risks	Technisch	34%	888	
7	Cybersecurity procedures	Man. & Org.	33%	854	
8	Cybersecurity recommendations and best practices	Man. & Org.	31%	804	
9	Cybersecurity policies	Man. & Org.	30%	782	
10	Multidiscipline aspect of cybersecurity	Man. & Org.	16%	415	

Supplementaire tabel 27: individuele taken, kennis en vaardigheden uitgesplitst naar vacatures op basis van het gevraagde opleidingsniveau en werkervaring

SBI 46 - Groothandel en handelsbemiddeling (niet in auto's en motorfietsen)

#	Bouwsteen	Categorie	Aantal
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	1422
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1220
3	Collaborate with other teams and colleagues	Man. & Org.	1022
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	588
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	205
6	Enforce and advocate organisation's data privacy and protection program	Legal	199
7	Conduct research, innovation and development work in cybersecurity-related top	Onderzoek	113
8	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	81
9	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	73
10	Deploy penetration testing tools and penetration test programs	Technisch	68
	Key skill(s)		
1	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	1406
2	Motivate and encourage people	Man. & Org.	1378
3	Identify, analyse and correlate cybersecurity events	Onderzoek	1255
4	Collaborate with other team members and colleagues	Man. & Org.	1022
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	883
6	Think creatively and outside the box	Onderzoek	508
7	Develop codes, scripts and programmes	Technisch	224
8	Develop code, scripts and programmes	Technisch	224
9	Decompose and analyse systems to develop security and privacy requirements an	Technisch	164
10	Identify and exploit vulnerabilities	Technisch	105
	Key knowledge		
1	Cybersecurity controls and solutions	Technisch	2164
2	Cybersecurity standards, methodologies and frameworks	Technisch	1388
3	Management practices	Man. & Org.	1035
4	Cybersecurity related laws, regulations and legislations	Legal	1031
5	Cyber threats	Technisch	912
6	Cybersecurity-related research, development and innovation (RDI)	Onderzoek	766
7	Cybersecurity recommendations and best practices	Man. & Org.	748
8	Cybersecurity procedures	Man. & Org.	715
9	Cybersecurity risks	Technisch	643
10	Cybersecurity-related technologies	Technisch	590

SBI 62 - Dienstverlenende activiteiten op het gebied van informatietechnologie

#	Bouwsteen	Categorie	Aantal
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	2589
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1607
3	Collaborate with other teams and colleagues	Man. & Org.	1424
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	1089
5	Enforce and advocate organisation's data privacy and protection program	Legal	181
6	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	151
7	Deploy penetration testing tools and penetration test programs	Technisch	124
8	Assist in designing, implementing, auditing and compliance testing activities in or	Man. & Org.	110
9	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	101
10	Design and propose a secure architecture to implement the organisation's strateg	Technisch	72
	Key skill(s)		
1	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	2933
2	Motivate and encourage people	Man. & Org.	2486
3	Identify, analyse and correlate cybersecurity events	Onderzoek	2418
4	Collaborate with other team members and colleagues	Man. & Org.	1424
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	561
6	Develop codes, scripts and programmes	Technisch	479
7	Develop code, scripts and programmes	Technisch	479
8	Think creatively and outside the box	Onderzoek	331
9	Conduct ethical hacking	Technisch	312
10	Identify and exploit vulnerabilities	Technisch	177
	Key knowledge		
1	Cybersecurity controls and solutions	Technisch	3502
2	Cybersecurity standards, methodologies and frameworks	Technisch	3154
3	Cyber threats	Technisch	2412
4	Cybersecurity procedures	Man. & Org.	1937
5	Management practices	Man. & Org.	1906
6	Cybersecurity related laws, regulations and legislations	Legal	1890
7	Cybersecurity risks	Technisch	1852
8	Cybersecurity recommendations and best practices	Man. & Org.	1393
9	Cybersecurity-related technologies	Technisch	1355
10	Multidiscipline aspect of cybersecurity	Man. & Org.	775

SBI 84 - Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen

#	Bouwsteen	Categorie	Aantal
	Main task(s)		
1	Cooperate and share information with authorities and professional groups	Man. & Org.	4581
2	Collaborate with other teams and colleagues	Man. & Org.	4401
3	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	3998
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	3486
5	Enforce and advocate organisation's data privacy and protection program	Legal	266
6	Develop organisation's cybersecurity architecture to address security and privacy	Technisch	169
7	Manage legal aspects of information security responsibilities and third-party relat	Legal	167
8	Conduct privacy impact assessments and develop, maintain, communicate and tra	Legal	121
9	Develop and propose staff awareness training to achieve compliance and foster a	Onderwijs	31
10	Ensure the organisation's resiliency to cyber incidents	Man. & Org.	24
	Key skill(s)		
1	Collaborate with other team members and colleagues	Man. & Org.	4401
2	Identify, analyse and correlate cybersecurity events	Onderzoek	4400
3	Motivate and encourage people	Man. & Org.	4233
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	2222
5	Work under pressure	Man. & Org.	447
6	Identify and select appropriate pedagogical approaches for the intended audienc	Onderzoek	374
7	Develop code, scripts and programmes	Technisch	263
8	Develop codes, scripts and programmes	Technisch	263
9	Think creatively and outside the box	Onderzoek	159
10	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	150
	Key knowledge		
1	Cybersecurity standards, methodologies and frameworks	Technisch	4858
2	Cybersecurity procedures	Man. & Org.	4445
3	Cybersecurity related laws, regulations and legislations	Legal	3944
4	Cyber threats	Technisch	3641
5	Cybersecurity policies	Man. & Org.	3376
6	Cybersecurity recommendations and best practices	Man. & Org.	3077
7	Cybersecurity controls and solutions	Technisch	2781
8	Cybersecurity risks	Technisch	2652
9	Management practices	Man. & Org.	1973
10	Multidiscipline aspect of cybersecurity	Man. & Org.	787

SBI 69 - Rechtskundige dienstverlening, accountancy, belastingadvisering en administratie

#	Bouwsteen	Categorie	Aantal
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	1752
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1189
3	Collaborate with other teams and colleagues	Man. & Org.	894
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	739
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	454
6	Design and propose a secure architecture to implement the organisation's strateg	Technisch	259
7	Enforce and advocate organisation's data privacy and protection program	Legal	164
8	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	98
9	Implement threat intelligence collection, analysis and production of actionable int	Technisch	86
10	Assist in designing, implementing, auditing and compliance testing activities in or	Man. & Org.	86
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	2654
2	Identify, analyse and correlate cybersecurity events	Onderzoek	2162
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	1085
4	Collaborate with other team members and colleagues	Man. & Org.	894
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	512
6	Develop code, scripts and programmes	Technisch	359
7	Develop codes, scripts and programmes	Technisch	359
8	Anticipate required changes to the organisation's information security strategy ar	Man. & Org.	343
9	Conduct ethical hacking	Technisch	205
10	Think creatively and outside the box	Onderzoek	151
	Key knowledge		
1	Management practices	Man. & Org.	2709
2	Cybersecurity controls and solutions	Technisch	1864
3	Cyber threats	Technisch	1813
4	Cybersecurity standards, methodologies and frameworks	Technisch	1734
5	Cybersecurity risks	Technisch	1630
6	Cybersecurity related laws, regulations and legislations	Legal	1435
7	Cybersecurity recommendations and best practices	Man. & Org.	1288
8	Cybersecurity procedures	Man. & Org.	1119
9	Multidiscipline aspect of cybersecurity	Man. & Org.	902
10	Cybersecurity-related technologies	Technisch	876

SBI 70 - Holdings (geen financiële), concerndiensten binnen eigen concern en managementadvisering

#	Bouwsteen	Categorie	Aantal
	Main task(s)		
1	Develop relationships with cybersecurity-related authorities and communities	Man. & Org.	1538
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1190
3	Collaborate with other teams and colleagues	Man. & Org.	913
4	Cooperate with key personnel for reporting of security incidents according to app	Legal	787
5	Identify cross-sectoral cybersecurity achievements and apply them in a different c	Onderzoek	164
6	Enforce and advocate organisation's data privacy and protection program	Legal	127
7	Conduct privacy impact assessments and develop, maintain, communicate and tra	Legal	70
8	Assess cybersecurity risks and propose most appropriate risk treatment options, i	Technisch	67
9	Design and propose a secure architecture to implement the organisation's strateg	Technisch	66
10	Develop organisation's cybersecurity architecture to address security and privacy	Technisch	57
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	1762
2	Identify, analyse and correlate cybersecurity events	Onderzoek	1392
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	1300
4	Collaborate with other team members and colleagues	Man. & Org.	913
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	315
6	Develop code, scripts and programmes	Technisch	285
7	Develop codes, scripts and programmes	Technisch	285
8	Conduct ethical hacking	Technisch	130
9	Anticipate required changes to the organisation's information security strategy ar	Man. & Org.	94
10	Think creatively and outside the box	Onderzoek	87
	Key knowledge		
1	Cybersecurity controls and solutions	Technisch	1735
2	Cybersecurity standards, methodologies and frameworks	Technisch	1725
3	Cybersecurity related laws, regulations and legislations	Legal	1341
4	Management practices	Man. & Org.	1287
5	Cyber threats	Technisch	1223
6	Cybersecurity recommendations and best practices	Man. & Org.	1152
7	Cybersecurity risks	Technisch	976
8	Cybersecurity procedures	Man. & Org.	840
9	Cybersecurity policies	Man. & Org.	646
10	Cybersecurity-related technologies	Technisch	534

Supplementaire tabel 28: Top bouwstenen per sector. Bron: Jobdigger, bewerking Dialogic

Cyber R&D

#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	59,6%	337
2	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	45,0%	254
3	Collaborate with other teams and colleagues	Man. & Org.	40,9%	231
4	Cooperate with key personnel for reporting of security incidents according t	Legal	30,6%	173
5	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	2,5%	14
6	Secure resources to implement the cybersecurity strategy	Man. & Org.	1,9%	11
7	Review, plan and allocate appropriate cybersecurity resources	Man. & Org.	1,9%	11
8	Deploy penetration testing tools and penetration test programs	Technisch	1,4%	8
9	Implement threat intelligence collection, analysis and production of actionat	Technisch	1,4%	8
10	Produce architectural documentation and specifications	Technisch	1,1%	6
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	56,5%	319
2	Collaborate with other team members and colleagues	Man. & Org.	40,9%	231
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	36,6%	207
4	Identify, analyse and correlate cybersecurity events	Onderzoek	31,5%	178
5	Develop codes, scripts and programmes	Technisch	19,1%	108
6	Develop code, scripts and programmes	Technisch	19,1%	108
7	Identify and select appropriate pedagogical approaches for the intended aud	Onderzoek	9,2%	52
8	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	8,7%	49
9	Manage and analyse log files	Technisch	3,5%	20
10	Think creatively and outside the box	Onderzoek	2,5%	14
	Key knowledge			
1	Management practices	Man. & Org.	0,2%	1
2	Cybersecurity controls and solutions	Technisch	0,4%	2
3	Cybersecurity procedures	Man. & Org.	0,5%	3
4	Cyber threats	Technisch	0,7%	4
5	Cybersecurity recommendations and best practices	Man. & Org.	0,9%	5
6	Cybersecurity standards, methodologies and frameworks	Technisch	1,1%	6
7	Cybersecurity related laws, regulations and legislations	Legal	1,2%	7
8	Pedagogical standards, methodologies and frameworks	Onderwijs	1,4%	8
9	Cybersecurity risks	Technisch	1,6%	9
10	Cybersecurity policies	Man. & Org.	1,8%	10

Cyberintegratie

#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	41,8%	5053
2	Cooperate and share information with authorities and professional groups	Man. & Org.	41,2%	4982
3	Collaborate with other teams and colleagues	Man. & Org.	34,5%	4169
4	Cooperate with key personnel for reporting of security incidents according t	Legal	26,0%	3151
5	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	3,8%	461
6	Assess cybersecurity risks and propose most appropriate risk treatment optic	Technisch	3,4%	407
7	Enforce and advocate organisation's data privacy and protection program	Legal	2,8%	333
8	Deploy penetration testing tools and penetration test programs	Technisch	2,3%	274
9	Develop and propose staff awareness training to achieve compliance and fos	Onderwijs	1,9%	232
10	Implement threat intelligence collection, analysis and production of actionat	Technisch	1,8%	216
	Key skill(s)			
1	Identify, analyse and correlate cybersecurity events	Onderzoek	43,6%	5273
2	Motivate and encourage people	Man. & Org.	38,8%	4690
3	Collaborate with other team members and colleagues	Man. & Org.	34,5%	4169
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30,4%	3680
5	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	17,3%	2098
6	Develop codes, scripts and programmes	Technisch	7,1%	864
7	Develop code, scripts and programmes	Technisch	7,1%	864
8	Think creatively and outside the box	Onderzoek	6,4%	777
9	Decompose and analyse systems to develop security and privacy requiremer	Technisch	3,1%	373
10	Anticipate required changes to the organisation's information security strate	Man. & Org.	2,6%	319
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	43,7%	5288
2	Cybersecurity standards, methodologies and frameworks	Technisch	42,5%	5143
3	Cyber threats	Technisch	34,7%	4199
4	Cybersecurity related laws, regulations and legislations	Legal	31,5%	3811
5	Cybersecurity procedures	Man. & Org.	29,5%	3566
6	Management practices	Man. & Org.	28,4%	3432
7	Cybersecurity risks	Technisch	28,3%	3427
8	Cybersecurity recommendations and best practices	Man. & Org.	23,9%	2885
9	Cybersecurity policies	Man. & Org.	16,6%	2007
10	Cybersecurity-related technologies	Technisch	15,7%	1905

Cyberproductie

#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	41,5%	3580
2	Cooperate and share information with authorities and professional groups	Man. & Org.	24,9%	2147
3	Collaborate with other teams and colleagues	Man. & Org.	19,4%	1669
4	Cooperate with key personnel for reporting of security incidents according t	Legal	16,3%	1401
5	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	6,1%	525
6	Design and propose a secure architecture to implement the organisation's st	Technisch	3,7%	323
7	Enforce and advocate organisation's data privacy and protection program	Legal	2,8%	238
8	Assess cybersecurity risks and propose most appropriate risk treatment optic	Technisch	1,6%	140
9	Deploy penetration testing tools and penetration test programs	Technisch	1,6%	139
10	Implement threat intelligence collection, analysis and production of actionat	Technisch	1,6%	135
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47,4%	4084
2	Identify, analyse and correlate cybersecurity events	Onderzoek	41,4%	3567
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	35,5%	3056
4	Collaborate with other team members and colleagues	Man. & Org.	19,4%	1669
5	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	9,1%	784
6	Think creatively and outside the box	Onderzoek	7,7%	666
7	Develop codes, scripts and programmes	Technisch	6,9%	596
8	Develop code, scripts and programmes	Technisch	6,9%	596
9	Anticipate required changes to the organisation's information security strate	Man. & Org.	4,9%	420
10	Conduct ethical hacking	Technisch	4,8%	415
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	50,4%	4345
2	Management practices	Man. & Org.	42,6%	3672
3	Cyber threats	Technisch	41,1%	3541
4	Cybersecurity standards, methodologies and frameworks	Technisch	38,2%	3291
5	Cybersecurity risks	Technisch	34,2%	2947
6	Cybersecurity related laws, regulations and legislations	Legal	29,1%	2509
7	Cybersecurity procedures	Man. & Org.	27,9%	2409
8	Cybersecurity recommendations and best practices	Man. & Org.	23,4%	2018
9	Cybersecurity-related technologies	Technisch	19,0%	1642
10	Multidiscipline aspect of cybersecurity	Man. & Org.	19,0%	1639

Bedrijfsleven

#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	41,0%	7251
2	Cooperate and share information with authorities and professional groups	Man. & Org.	29,0%	5128
3	Collaborate with other teams and colleagues	Man. & Org.	23,5%	4163
4	Cooperate with key personnel for reporting of security incidents according t	Legal	18,1%	3206
5	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	5,5%	967
6	Assess cybersecurity risks and propose most appropriate risk treatment optic	Technisch	3,3%	585
7	Enforce and advocate organisation's data privacy and protection program	Legal	3,0%	528
8	Deploy penetration testing tools and penetration test programs	Technisch	2,7%	481
9	Design and propose a secure architecture to implement the organisation's st	Technisch	2,6%	466
10	Implement threat intelligence collection, analysis and production of actionat	Technisch	1,8%	326
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	41,2%	7300
2	Identify, analyse and correlate cybersecurity events	Onderzoek	40,2%	7111
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	33,6%	5953
4	Collaborate with other team members and colleagues	Man. & Org.	23,5%	4163
5	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	16,3%	2885
6	Think creatively and outside the box	Onderzoek	7,6%	1337
7	Develop codes, scripts and programmes	Technisch	7,5%	1336
8	Develop code, scripts and programmes	Technisch	7,5%	1336
9	Anticipate required changes to the organisation's information security strate	Man. & Org.	4,1%	730
10	Conduct ethical hacking	Technisch	3,1%	557
	Key knowledge			
1	Cybersecurity controls and solutions	Technisch	49,9%	8839
2	Cybersecurity standards, methodologies and frameworks	Technisch	39,3%	6950
3	Cyber threats	Technisch	35,9%	6360
4	Management practices	Man. & Org.	35,5%	6282
5	Cybersecurity risks	Technisch	29,6%	5235
6	Cybersecurity related laws, regulations and legislations	Legal	26,1%	4615
7	Cybersecurity procedures	Man. & Org.	23,4%	4151
8	Cybersecurity recommendations and best practices	Man. & Org.	22,6%	4001
9	Cybersecurity-related technologies	Technisch	19,5%	3447
10	Multidiscipline aspect of cybersecurity	Man. & Org.	15,5%	2751

Overheid

#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	57,8%	3981
2	Collaborate with other teams and colleagues	Man. & Org.	53,2%	3666
3	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	46,3%	3188
4	Cooperate with key personnel for reporting of security incidents according t	Legal	42,4%	2918
5	Develop organisation's cybersecurity architecture to address security and pri	Technisch	1,5%	104
6	Conduct privacy impact assessments and develop, maintain, communicate ar	Legal	1,1%	75
7	Enforce and advocate organisation's data privacy and protection program	Legal	1,0%	68
8	Manage legal aspects of information security responsibilities and third-party	Legal	0,8%	55
9	Develop and propose staff awareness training to achieve compliance and fos	Onderwijs	0,5%	36
10	Implement threat intelligence collection, analysis and production of actionat	Technisch	0,4%	30
	Key skill(s)			
1	Identify, analyse and correlate cybersecurity events	Onderzoek	58,1%	4004
2	Collaborate with other team members and colleagues	Man. & Org.	53,2%	3666
3	Motivate and encourage people	Man. & Org.	52,1%	3586
4	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	30,6%	2110
5	Work under pressure	Man. & Org.	5,7%	391
6	Develop code, scripts and programmes	Technisch	5,2%	356
7	Develop codes, scripts and programmes	Technisch	5,2%	356
8	Identify and select appropriate pedagogical approaches for the intended aud	Onderzoek	4,4%	306
9	Think creatively and outside the box	Onderzoek	3,6%	246
10	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	2,1%	147
	Key knowledge			
1	Cybersecurity procedures	Man. & Org.	57,3%	3947
2	Cybersecurity standards, methodologies and frameworks	Technisch	55,3%	3810
3	Cyber threats	Technisch	46,0%	3166
4	Cybersecurity related laws, regulations and legislations	Legal	42,0%	2893
5	Cybersecurity controls and solutions	Technisch	35,5%	2446
6	Cybersecurity risks	Technisch	34,3%	2360
7	Cybersecurity policies	Man. & Org.	32,9%	2264
8	Cybersecurity recommendations and best practices	Man. & Org.	32,5%	2239
9	Management practices	Man. & Org.	22,8%	1571
10	Multidiscipline aspect of cybersecurity	Man. & Org.	12,0%	824

Onderwijs-/kennisinstellingen				
#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	62,3%	410
2	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	46,5%	306
3	Collaborate with other teams and colleagues	Man. & Org.	43,2%	284
4	Cooperate with key personnel for reporting of security incidents according t	Legal	36,6%	241
5	Develop organisation's cybersecurity architecture to address security and pri	Technisch	2,9%	19
6	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	2,1%	14
7	Review, plan and allocate appropriate cybersecurity resources	Man. & Org.	1,7%	11
8	Secure resources to implement the cybersecurity strategy	Man. & Org.	1,7%	11
9	Deploy penetration testing tools and penetration test programs	Technisch	1,2%	8
10	Implement threat intelligence collection, analysis and production of actional	Technisch	1,2%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	54,1%	356
2	Collaborate with other team members and colleagues	Man. & Org.	43,2%	284
3	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	32,7%	215
4	Identify, analyse and correlate cybersecurity events	Onderzoek	31,9%	210
5	Develop codes, scripts and programmes	Technisch	17,3%	114
6	Develop code, scripts and programmes	Technisch	17,3%	114
7	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	8,1%	53
8	Identify and select appropriate pedagogical approaches for the intended aud	Onderzoek	7,9%	52
9	Think creatively and outside the box	Onderzoek	3,3%	22
10	Manage and analyse log files	Technisch	3,0%	20
	Key knowledge			
1	Management practices	Man. & Org.	40,4%	266
2	Cybersecurity controls and solutions	Technisch	38,8%	255
3	Cybersecurity procedures	Man. & Org.	33,0%	217
4	Cyber threats	Technisch	31,5%	207
5	Cybersecurity recommendations and best practices	Man. & Org.	28,3%	186
6	Cybersecurity standards, methodologies and frameworks	Technisch	26,3%	173
7	Cybersecurity related laws, regulations and legislations	Legal	25,1%	165
8	Pedagogical standards, methodologies and frameworks	Onderwijs	21,4%	141
9	Cybersecurity risks	Technisch	19,6%	129
10	Cybersecurity policies	Man. & Org.	18,5%	122

Overig				
#	Bouwsteen	Categorie	% vacatur	Aantal vaca
	Main task(s)			
1	Develop relationships with cybersecurity-related authorities and communitie	Man. & Org.	34,0%	145
2	Cooperate and share information with authorities and professional groups	Man. & Org.	29,3%	125
3	Collaborate with other teams and colleagues	Man. & Org.	26,5%	113
4	Cooperate with key personnel for reporting of security incidents according to	Legal	17,8%	76
5	Assist in designing, implementing, auditing and compliance testing activities	Man. & Org.	5,6%	24
6	Implement threat intelligence collection, analysis and production of actionat	Technisch	1,9%	8
7	Design and propose a secure architecture to implement the organisation's st	Technisch	1,2%	5
8	Conduct privacy impact assessments and develop, maintain, communicate an	Legal	0,9%	4
9	Develop an organisation's cybersecurity risk management strategy	Man. & Org.	0,7%	3
10	Identify cross-sectoral cybersecurity achievements and apply them in a differ	Onderzoek	0,7%	3
	Key skill(s)			
1	Work on operating systems, servers, clouds and relevant infrastructures	Technisch	34,0%	145
2	Identify, analyse and correlate cybersecurity events	Onderzoek	33,5%	143
3	Motivate and encourage people	Man. & Org.	28,6%	122
4	Collaborate with other team members and colleagues	Man. & Org.	26,5%	113
5	Develop code, scripts and programmes	Technisch	14,1%	60
6	Develop codes, scripts and programmes	Technisch	14,1%	60
7	Conduct ethical hacking	Technisch	11,9%	51
8	Work under pressure	Man. & Org.	6,8%	29
9	Communicate, coordinate and cooperate with internal and external stakehol	Man. & Org.	6,1%	26
10	Conduct technical analysis and reporting	Technisch	5,6%	24
	Key knowledge			
1	Cyber threats	Technisch	42,6%	182
2	Cybersecurity standards, methodologies and frameworks	Technisch	39,8%	170
3	Cybersecurity controls and solutions	Technisch	37,5%	160
4	Cybersecurity risks	Technisch	33,0%	141
5	Cybersecurity related laws, regulations and legislations	Legal	27,9%	119
6	Management practices	Man. & Org.	24,1%	103
7	Cybersecurity procedures	Man. & Org.	23,0%	98
8	Cybersecurity recommendations and best practices	Man. & Org.	21,5%	92
9	Cybersecurity-related technologies	Technisch	17,6%	75
10	Cybersecurity policies	Man. & Org.	16,4%	70

Supplementaire tabel 29: Bouwstenen per doelgroep, gebaseerd op de top 100 organisaties. Bron: Jobdigger, bewerking Dialogic

Adviesrapport Onderwijs en Arbeidsmarkt Cybersecurity

Platform **Talent** voor **Technologie**

dialogic
innovatie • interactie

In opdracht van Ministerie van Economische Zaken en Klimaat

Managementsamenvatting

'Onze maatschappij is tot in de haarvaten afhankelijk van het internet en andere digitale netwerken, diensten en producten. Ontwikkelingen op het gebied van digitalisering gaan razendsnel en bieden veel kansen, maar brengen ook essentiële vraagstukken op het gebied van cyberweerbaarheid met zich mee. Adequate cybersecurity hoort voor organisaties bij een gezonde bedrijfsvoering, net als grip op hun financiële huishouding; het is een dragende factor die overal aanwezig én noodzakelijk is, anders komt de veiligheid en continuïteit in gevaar en stokt onze economie."[1]

Om te zorgen voor adequate cybersecurity in Nederland is de aanwezigheid van voldoende goed geschoolde cybersecurityprofessionals een essentiële voorwaarde.

Onderzoek

Het Ministerie van Economische Zaken en Klimaat heeft graag een goed beeld van de **huidige kwantitatieve en kwalitatieve tekorten** op de Nederlandse cybersecurity arbeidsmarkt, **de verwachte groei** en de mogelijkheden om onderwijs en arbeidsmarkt **beter op elkaar aan te sluiten** (ook beschreven als actie in het Actieplan Nederlandse Cybersecuritystrategie 2022 -2028).

Platform Talent voor Technologie (PTvT) en Dialogic hebben van september 2023 tot februari 2024 antwoord gegeven op een negen- tal onderzoeksvragen die zich richtten op het in kaart brengen van vraag en aanbod (arbeidsmarkt en opleidingsmogelijkheden). Dit moet leiden tot een **onderbouwd advies**, inclusief implementatieplan, over welke (beleids-)instrumenten op de korte en op de lange termijn ingezet kunnen worden om de cybersecurity arbeidsmarkt te versterken. De resultaten van dit onderzoek worden middels **twee rapporten** kenbaar gemaakt:

1. De onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity[2].
2. Een adviesrapport.

Dit voorliggende adviesrapport beschrijft **12 aanbevelingen** om de vraag naar cybersecurityprofessionals en cybersecurity-opleidingsaanbod (privaat en particulier) beter op elkaar aan te laten sluiten.

De cybersecurity onderwijs- arbeidsmarkt

De cybersecurity-arbeidsmarkt kenmerkt zich door een veelheid aan profielen waarin verschillende (cybersecurity) expertise benodigd is. Het is een multidisciplinair werkveld; naast technische kennis en vaardigheden zijn o.a. ook juridische en management en organisatie competenties nodig.

Toekomstige ontwikkelingen zoals de Network and Information Security Directive (NIS2), Cyber Resilience Act (CRA) en de ontwikkeling en inzet van artificiële intelligentie (AI) zullen de komende jaren voor een grotere en andere vraag naar expertise op de cybersecurity-arbeidsmarkt zorgen.
Tegelijkertijd zien we binnen de cybersecurity-opleidingen een veelheid aan opleidingen met een eigen (specifieke) focus.
Door de grote diversiteit van cybersecurity-expertise, de grote diversiteit aan doelgroepen en snel opvolgende veranderingen, is er gecoördineerde inzet van veel partijen nodig om aan de cybersecurity arbeidsmarktvraag te kunnen voldoen, over de gehele breedte.

Van onderzoek naar aanbevelingen

Het totale systeem van onderwijs en arbeidsmarkt is omvangrijk en divers. Zoals in het onderzoeksrapport staat beschreven gaat het ***op de arbeidsmarkt*** om verschillende typen expertise, een groot aantal verschillende (typen) organisaties en velerlei functieprofielen waar cybersecurity-expertise een rol speelt. ***In het onderwijs*** gaat het om verschillende onderwijstypen (PO, VO, MBO, HBO, WO, LLO) en een grote variëteit aan opleidingen die zich volledig of deels richten op cybersecurity. ***De mensen*** die zich door het systeem van onderwijs en arbeidsmarkt bewegen worden op hun beurt ook gekenmerkt door eigen beweegredenen, een eigen context en dynamiek. Alle betrokken partijen en schakels tussen hen vormen het gehele systeem van onderwijs en arbeidsmarkt. Zij ervaren allen hun eigen uitdagingen en knelpunten.

Hoewel we in dit adviesrapport de behoefte aan voldoende cybersecurityprofessionals als 'één uitdaging' brengen, willen we benadrukken dat het in de werkelijkheid gaat om een verzameling van een groot aantal kleinere deelproblemen, verspreid over de gehele keten van onderwijs en arbeidsmarkt. Er zal dan ook geen one-size-fits-all-oplossing zijn die alle deelproblemen in de gehele keten gaat oplossen. Het beeld dat we met één of enkele inspanningen of initiatieven het gehele vraagstuk kunnen oplossen is wat ons betreft niet reëel.

1. https://www.cybersecurityraad.nl/documenten/brieven/2024/02/05/brief-aan-de-informateur
2. Onderzoeksrapportage Onderwijs en Arbeidsmarkt cybersecurity, PTvT en Dialogic, 2024

In dit adviesrapport is er bewust voor gekozen om een twaalftal aanbevelingen te formuleren ten aanzien van wat er zou moeten gebeuren, aangevuld met concrete voorbeelden ten aanzien van hoe hier invulling aan gegeven zou kunnen worden. Er is bewust niet voor gekozen om op detailniveau aan te geven wie wat moet gaan doen vanwege twee belangrijke argumenten:

1. **Praktische haalbaarheid:**
   Er zijn veel inspanningen op veel plekken in de onderwijs-arbeidsmarktketen nodig, en het uitwerken van al deze inspanningen op microniveau is praktisch niet haalbaar. Andersom geredeneerd heeft het geen zin om slechts één of enkele aanbevelingen te noemen, omdat het vraagstuk daarmee te plat wordt geslagen. Om deze reden is ervoor gekozen om de aanbevelingen te formuleren op een aggregatieniveau dat concreet genoeg en niet te gedetailleerd is. De aanbevelingen zijn nader uitgewerkt in dit adviesrapport (Hoofdstuk 3 t/m 5) en zijn aangevuld met concrete voorbeeldinitiatieven uit de praktijk (Bijlagen 5 t/m 8).

2. **Draagvlak:**
   De aanbevelingen moeten geoperationaliseerd worden door de betrokken partijen. Afhankelijk van bepaalde waarden, overtuigingen en uitgangsposities zullen verschillende betrokkenen op een andere manier willen omgaan met de aanbevelingen. Gedurende dit proces dienen inhoudelijke en procesmatige keuzes gemaakt te worden, die o.i. juist door de betrokken partijen genomen moeten worden. Dit zal het eigenaarschap en draagvlak vergroten.

Aanbevelingen

In de onderzoeksrapportage zijn 7 **kernpunten in de totale onderwijs- en arbeidsmarkt keten** gesignaleerd, waarop de aanbevelingen gericht moeten worden. Tijdens een bijeenkomst op 17 januari met ruim 40 stakeholders (uit het onderwijs, bedrijfsleven, de betrokken Ministeries en het Human Capital ecosysteem) zijn deze 7 punten besproken om vervolgens **adviezen, acties en instrumenten** op te halen. Aangevuld met activiteiten uit internationaal Human Capital cybersecuritybeleid, is vervolgens de input getoetst, aangescherpt en gecategoriseerd. Dit heeft geleid tot de volgende 12 aanbevelingen, uitgesplitst in aanbevelingen gericht op **het gehele ecosysteem (1-4), de arbeidsmarkt (5-8)** en **het onderwijs (9-12)**:

#	Aanbeveling	Toelichting
1	Ontwikkel een gezamenlijke taal en gezamenlijk beeld m.b.t. 'cybersecurity-expertise'.	Ontwikkel de gezamenlijke taal die cruciaal is voor het creëren van een collectief begrip van 'de vraag' naar en 'het aanbod' van cybersecurity-expertise. Versterk vervolgens het gezamenlijke beeld over hoe het staat met 'de vraag' en 'het aanbod' door te werken aan de gezamenlijke informatiepositie m.b.t. dataverzameling, het verwerken en het ontsluiten van data.
2	Breng gerichte coördinatie aan op de aansluiting onderwijs-arbeidsmarkt.	Om de vraag op de arbeidsmarkt en het aanbod vanuit onderwijs over de volledige breedte van cybersecurity goed aan te laten sluiten is gecoördineerde actie nodig om de volledige vraag af te dekken én niet onnodig dubbel werk uit te voeren. Hierbij dient rekening gehouden te worden met de algehele krapte op de arbeidsmarkt en de mogelijke (beleids)concurrentie.
3	Spreek het volledige potentiële talent aan	Meer aandacht voor diversiteit en inclusie door o.a. te werken aan het aantrekken van ondervertegenwoordigde (gender-) groepen. Benut het bestaande (cybersecurity-) talent met een mbo-opleidingsachtergrond beter voor de sector.
4	Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.	Regio's verschillen in termen van vraag én aanbod van cybersecurity-professionals. Binnen de regio's verdient het dan ook aandacht om goed te kijken naar de regionale context en het verbinden van vraag en aanbod. Ook binnen en tussen sectoren en (waarde)ketens kunnen de handen ineengeslagen worden.
5	Vergroot de zichtbaarheid en aantrekkelijkheid van 'het beroep'	De aantrekkingskracht kan vergroot worden door de grote variëteit in functies en expertise (niet enkel technisch van aard), de breedte van het werkveld en het belang van werken binnen deze sector zichtbaar te benadrukken.
6	Stimuleer om-, bij- en nascholing ten behoeve van horizontale en verticale ontwikkeling	Ontwikkelpaden bieden carrièreperspectief waardoor professionals weten welke mogelijkheden er zijn en welk aanbod hierbij passend is. De samenwerking tussen onderwijs (publiek en privaat) en werkgevers dient voor een actueel en gevarieerd aanbod te zorgen dat alle medewerkers stimuleert verder te ontwikkelen.

7	Werk aan behoud van professionals m.b.v. arbeidsmobiliteit binnen de sector	In een regionale en lokale samenwerking tussen werkgevers kunnen o.a. aantrekkelijke voorwaarden gecreëerd worden, waardoor cybersecurityprofessionals beter behouden kunnen worden binnen de cybersecuritysector.
8	Verbeter de startpositie van net afgestudeerden	Door de overstap van onderwijs naar bedrijfsleven te begeleiden, en als werkgever bewust in te zetten op de training en ontwikkeling van startende medewerkers kunnen de junior professionals sneller op het gewenste niveau gebracht worden.
9	Vergroot de interesse voor studeren en werken in cybersecurity	In het po en vo kan meer aandacht komen voor digitale technologie en digitale vaardigheden in generieke zin, maar ook voor cybersecurity specifiek. Onderwijsinstellingen kunnen cybersecurity duidelijker en aantrekkelijker neerzetten binnen de diverse vervolgopleidingen in het mbo en ho.
10	Versterk de kaders en het materiaal voor cybersecurity-onderwijs	Er is behoefte aan meer uitgewerkte kerndoelen en doorlopende leerlijnen/curricula en onderwijsmateriaal voor en vanaf het funderend onderwijs. Binnen het hoger onderwijs is het uitdagend om samenwerking op te tuigen tussen opleidingen en instellingen, terwijl dat nodig is wanneer het multidisciplinaire karakter van cybersecurity in een onderwijsprogramma gecombineerd dient te worden. Gezamenlijke kaders en inspanningen kunnen hier een oplossing bieden.
11	Betrek de arbeidsmarkt sterker in het onderwijs	Wegens de razend snelle cybersecurity-arbeidsmarkt is het voor het onderwijs van belang om goed verbonden te blijven met de arbeidsmarkt. Samen met de arbeidsmarkt kan gewerkt worden aan actuele vaardigheden voor studenten, het docententekort, contextrijke leeromgevingen, flexibeler opleiden, en gezamenlijke promotie van het werkveld.
12	Versterken vergroot de aantrekkelijkheid van het docentschap	Het docentschap in cybersecurity moet zowel voor zittende als nog te werven docenten aantrekkelijk gemaakt. Hybride functies, het investeringen in bij- en nascholing, en het toegankelijker maken van omscholing kunnen hierbij helpen.

Opvolging van de aanbevelingen

Op het gebied van Human Capital cybersecurity zijn veel diverse initiatieven betrokken. Uit de vele gesprekken blijkt dat het vooral ontbreekt aan de verbinding van deze initiatieven en de coördinatie ervan waardoor het aan slagkracht ontbreekt. Om beleidscoördinatiefalen te voorkomen, is het belangrijk om **een duidelijke partij** (bijv. een van de betrokken Ministeries) te benoemen met voldoende mandaat, positie en middelen, die verantwoordelijk is voor de **coördinatie en verdere opvolging van deze adviezen**. Een **coördinatiegroep**, waarin Rijksoverheid, onderwijs en bedrijfsleven vertegenwoordigd zijn, kan vervolgens het totaal aan adviezen overzien en de samenhang bewaken.

Vanuit **ieder betrokken Ministerie** kan vervolgens besproken worden welke aanbevelingen passend zijn om op te nemen in de **huidige infrastructuur, programma's en regelingen**. De aanbevelingen binnen de deelgebieden onderwijs, arbeidsmarkt en ecosysteem zouden vervolgens het best besproken kunnen worden in **heterogene werkgroepen** waarin Rijksoverheid (incl. het coördinerende Ministerie), onderwijs, bedrijfsleven en de betreffende overige partijen plaatsnemen. Binnen deze werkgroepen worden de adviezen besproken en wordt de verdere aanpak bepaald. Een goede verbinding tussen de landelijke, regionale en lokale aanpak is essentieel.

Bovenstaande aanbevelingen hebben specifiek betrekking op de cybersecurity-arbeidsmarkt. Bij het opvolgen van de aanbevelingen en verdere uitvoer dient rekening gehouden te worden met de inspanningen die door allerlei sectoren worden ondernomen, de **algehele arbeidsmarktkrapte** en specifiek op **ICT-breed gebied**. Het risico op **beleidsconcurrentie** is in deze tijden van schaarste aan menselijk kapitaal dan ook groot: vanuit verschillende hoeken wordt getrokken aan dezelfde groep mensen.

Wanneer meerdere domeinen ongecoördineerd inspanningen plegen om dezelfde personen aan zich te binden gaat dit gepaard met aanzienlijke kosten en geen of nauwelijks netto resultaat voor Nederland. **Aansluiten bij bestaand beleid en maatregelen**, met een **specifieke focus op cybersecurity**, kan deze risico's beperken en leiden tot doelmatiger beleid.

Inhoudsopgave

Leeswijzer

Dit rapport is onderdeel van een tweedelige rapportage waarin de onderzoeksvragen beantwoord worden die het Ministerie van Economische Zaken en Klimaat heeft gesteld om de kwantitatieve en kwalitatieve tekorten op de Nederlandse cybersecurity-arbeidsmarkt en de verwachte groeiende vraag naar cybersecuritypersoneel in kaart te brengen.

In deze rapportage worden aanbevelingen gegeven voor mogelijke (beleids-)instrumenten die op de korte en op de lange termijn ingezet kunnen worden om het geconstateerde tekort aan professionals op de cybersecurity- arbeidsmarkt te verkleinen. **Hoofdstuk 1** geeft als inleiding: de probleemstelling van het bijbehorende onderzoek, de belangrijkste bevindingen van de voorgaande onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity[3] en er wordt een korte beschrijving van de totstandkoming van de aanbevelingen. **Hoofdstuk 2** beschrijft de 12 aanbevelingen voor mogelijke (beleids-)instrumenten. In **Hoofdstuk 3, 4 en 5** worden deze aanbevelingen toegelicht voor respectievelijk ecosysteem (3), arbeidsmarkt (4) en het onderwijs (5). **Hoofdstuk 6** schetst een beeld hoe opvolging en prioritering kan worden gegeven aan deze aanbevelingen. Het rapport sluit af met een **Dankwoord** aan alle betrokken partijen en deelnemers die een bijdrage hebben geleverd aan de beantwoording van alle onderzoeksvragen en de aanbevelingen. In de **Bijlagen** is achtergrondinformatie te vinden over de totstandkoming van de aanbevelingen, de rationale voor overheidsinterventie, de benutte internationale voorbeelden en de contextbeschrijving behorende bij de aanbevelingen.

3. Onderzoeksrapportage Onderwijs en Arbeidsmarkt cybersecurity, PTvT en Dialogic, 2024

1. Probleemstelling en korte terugblik naar het onderzoeksrapport

1.1. Probleemstelling

In Nederland en de EU wordt hard gewerkt aan een digitaal veilige samenleving. De aanwezigheid van voldoende goed geschoolde cybersecurity-professionals is hiervoor een essentiële voorwaarde. Het Ministerie van Economische Zaken en Klimaat (EZK) krijgt graag een goed beeld van de huidige kwantitatieve en kwalitatieve tekorten op de Nederlandse cybersecurity-arbeidsmarkt en de verwachte ontwikkelingen. EZK heeft Platform Talent voor Technologie en Dialogic gevraagd dit in kaart te brengen.

In het Actieplan Nederlandse Cybersecuritystrategie 2022 -2028 zijn de volgende acties op het gebied van Human Capital opgenomen:

- De kwalitatieve en kwantitatieve tekorten op de cybersecurity-arbeidsmarkt worden onderzocht, met aanbevelingen over hoe deze tekorten aan te pakken;
- Verkend wordt of de initiatieven voor inzicht in ICT- brede tekorten en de ontwikkeling van een onderwijs en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity-specialisten.

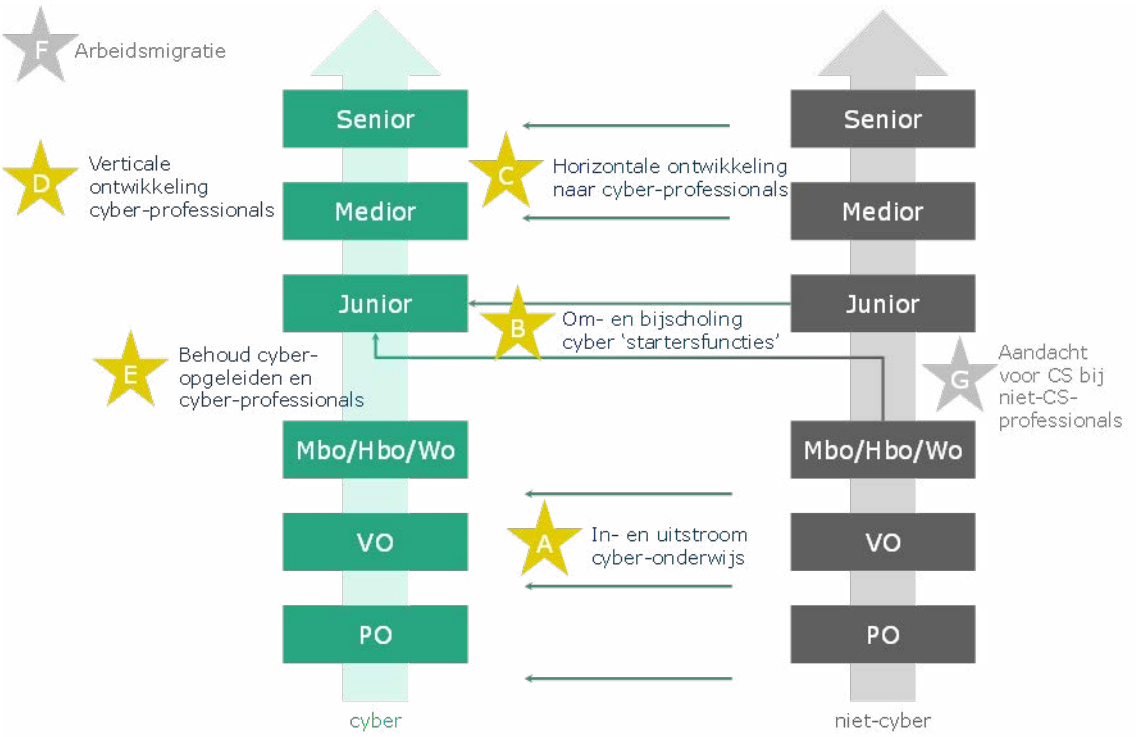
Om uitvoering te geven aan bovengenoemde acties heeft het Ministerie van Economische Zaken en Klimaat een onderzoeksvoorstel geschreven. De onderzoeksvragen daarin richten zich op vraag en aanbod (arbeidsmarkt en opleidingsmogelijkheden) en moeten leiden tot een onderbouwd advies, inclusief implementatieplan, over welke (beleids-)instrumenten op de korte en op de lange termijn ingezet kunnen worden om het geconstateerde tekort op de cybersecurity-arbeidsmarkt te verkleinen.

De resultaten van dit onderzoek worden middels twee rapporten kenbaar gemaakt:

1. De onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity.
2. Een adviesrapport.

1.2. Totstandkoming adviesrapport

In de onderzoeksrapportage is de totale onderwijs- arbeidsmarkt keten beschreven met daarin 7 kernpunten, waarop de aanbevelingen gericht moeten worden (zie Figuur 1). Tijdens een bijeenkomst op 17 januari met ruim 40 stakeholders (uit het onderwijs, bedrijfsleven, de betrokken Ministeries en het Human Capital ecosysteem) zijn deze 7 punten besproken om vervolgens adviezen, acties en instrumenten op te halen. Deze input is vervolgens getoetst en aangescherpt door gesprekken te voeren met vertegenwoordigers uit de verschillende groepen die niet op 17 januari aanwezig waren. De aangescherpte opbrengst is daarna gecategoriseerd en vergeleken met de Human Capital aanpak zoals deze in het Verenigd Koninkrijk, de Verenigde Staten van Amerika en in Europees beleid uitgevoerd wordt. Een uitgebreide beschrijving van de methodologische aanpak is terug te lezen in Bijlage 1. De Internationale voorbeelden zijn beschreven in Bijlage 2.



Figuur 1: Conceptueel kader dat een beeld geeft van de totale onderwijs- arbeidsmarkt keten

1.3. Korte terugblik onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity

In de onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity wordt een overzicht geboden van de huidige en toekomstige cybersecurity opleidingen, op mbo, hbo en wo niveau en binnen het Leven Lang Ontwikkelen (LLO) aanbod. De huidige vraag op de arbeidsmarkt is geanalyseerd aan de hand van een uitgebreide vacature analyse.

De belangrijkste inzichten van dit onderzoek zijn als volgt:

Op het gebied van onderwijs:

- is er groeiende aandacht voor cybersecurity in de mbo-, hbo-, en wo-opleidingen,
- waarbij een verschil in focus te zien is op de technische en management & organisatie competenties bij het mbo-onderwijs en een meer multidisciplinaire focus bij de hbo- en wo-opleidingen.
- De in ontwikkeling zijnde opleidingen kenmerken zich door een multidisciplinaire insteek.
- Over het algemeen zien we bij de huidige mbo-, hbo- en wo-opleidingen een redelijk gelijk blijvende instroom over de afgelopen jaren (aantallen studenten). Het aantal mbo afgestudeerden blijft redelijk gelijk en groeit bij de hbo- en wo-opleidingen. Wegens de relatief korte bestaansduur van een aantal opleidingen, zien we het aantal afgestudeerden stijgen in de afgelopen jaren; na de eerste vier jaar studeren de eerste studenten af, met een uitloop in de jaren erna.

Op het gebied van de vraag op de arbeidsmarkt:

- Er is een groeiende vraag naar cybersecurity-specialisten te zien in de vacature-analyses vooral medior- en senior posities. Er zijn provinciale en regionale verschillen te zien in de vraag, zowel kwantitatief als functie-inhoudelijk.
- In de vacatures wordt vooral gevraagd naar technische, management en organisatie competenties op hbo- en wo-niveau.
- Er studeren relatief te weinig hbo- en wo-gediplomeerden met een specialistisch cybersecurity profiel af om te kunnen voorzien in de vraag op de arbeidsmarkt.
- In de vacatures is een variëteit te zien binnen de cybersecurity-expertise, met vraag naar technische, juridische en/ of meer op management en organisatie gerichte kennis en vaardigheden.
- De mate van specialisatie binnen de functies varieert van een duidelijk ECSF (European Cyber Security Framework) profiel met een 'hoog' cybersecuritygehalte, tot een brede schil van functies met een 'laag' cybersecuritygehalte (bijv. netwerkbeheerder en huisartsassistente).

- Typen functies lijken erg gerelateerd te zijn aan typen organisaties, waarbij de specialistische producenten en integrators een heel andere dynamiek en vraag kennen. Daarbij lijken veel van die partijen in de Randstad te zitten. Differentiatie tussen doelgroepen is dus een must.
- Technische kennis is een grote vereiste, maar veel van de vaardigheden en taken binnen het brede veld van CS zijn niet technisch.
- Toekomstige ontwikkelingen zullen de vraag in de breedte doen toenemen; van de ECSF profielen Chief Information Security Officers (CISO) tot aan Implementers, Analisten, Auditors en Pentesters voor de Network and Information Security Directive (NIS2). Door de Cyber Resilience Act (CRA) zal de vraag naar cybersecurity-professionals naar verwachting in de breedte toenemen, met vermoedelijk de grootste impact voor de cyberintegrators.

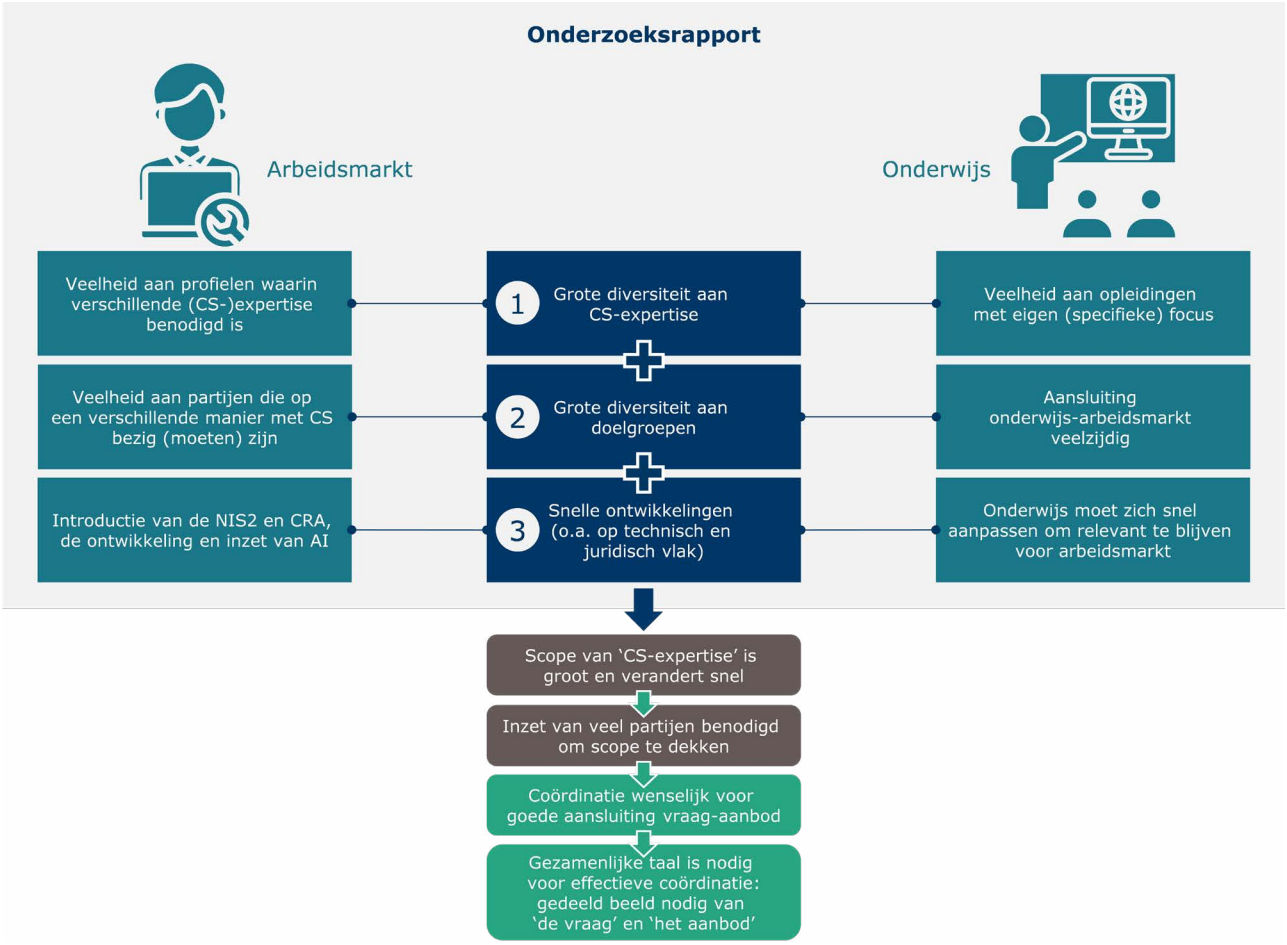
Op het gebied van de aansluiting onderwijs en arbeidsmarkt:
- De collectieve afstemming van hoe alle opleidingen gezamenlijk opleiden tot alle gezamenlijke functies op de arbeidsmarkt lijkt beperkt aanwezig. Hierbij gaat het om de afstemming van alle opleidingen in een doorlopende lijn (mbo, hbo en wo) en de afstemming van de opleidingen per onderwijsniveau. We zien een hele grote variëteit aan cybersecurity professionals: als iedereen voor een deel van deze professionals opleidt, is de vraag of we als gezamenlijke opleidingen voldoende opleiden voor de gehele vraag.
- Er ontbreekt een gezamenlijke taal om over het onderwerp te spreken; waardoor vraag en aanbod moeilijk af te stemmen valt aangezien het niet duidelijk kan zijn over welke vraag en aanbod men spreekt.

De kracht van de term ‘cybersecurity’ is dat het veel mensen verbindt, dat iedereen zich er iets bij kan voorstellen en dat het gezamenlijkheid creëert in termen van waar we naartoe willen: een cyberveilige samenleving. De keerzijde hiervan is echter dat een dergelijke term een dusdanige hoge mate van abstractie en een hoog aggregatieniveau kent dat de term daarmee tegelijkertijd een **containerbegrip** is. Er gaat veel schuil achter deze ene term, en uit het onderzoek is gebleken dat dat niet anders is als het gaat om cybersecurity-expertise. Er is sprake van een grote rijkheid aan verschillende functieprofielen, verschillende typen cybersecurity-expertise, verschillende doelgroepen en verschillende plekken in waardeketens. Deze variëteit zien we ook terug bij de associaties die mensen met het vakgebied hebben. Sommige mensen denken bij cybersecurity-expertise bijvoorbeeld allereerst aan de technische kennis en kunde en beroepsprofielen als ‘ethical hackers’, terwijl andere mensen denken aan multidisciplinaire functies zoals de CISO. Daarbij verschillen mensen in hun kennis en opvattingen over cybersecurity-expertise in de **breedte** (“wat voor typen expertise zijn er en wat voor beroepsprofielen vragen om cybersecurity-expertise?”) en de **diepte** (“wat houdt het precies in om een penetration tester, een CISO, of een netwerkbeheerder te zijn?”). Hier komt nog eens bij dat het domein relatief jong is en er verschillende ontwikkelingen zijn die vraag en aanbod beïnvloeden, zoals de NIS2, CRA en de inzet van AI.

Doordat cybersecurity-expertise een dusdanig brede scope kent is er geen enkele organisatie, laat staan een enkel individu, die de volledige breedte én diepte van de vraag (arbeidsmarkt) en het aanbod (cybersecurity-professionals, onderwijs en opleiding) kan doorgronden. Het is een groot vraagstuk dat om gezamenlijke inspanningen vraagt. We willen aan de volledige maatschappelijke en economische vraag op het gebied van cybersecurity voldoen, en willen het aanbod zo inrichten en faciliteren dat er een goede aansluiting van vraag en aanbod gerealiseerd kan worden. Dat betekent dat we enerzijds hiaten in de cybersecurity-expertise moeten voorkomen, en anderzijds dat we niet (onnodig) dubbel werk leveren om voldoende cybersecurity-expertise te realiseren. Dit vraagt in een omvangrijk domein zoals cybersecurity om een goede coördinatie van inspanningen van alle betrokken stakeholders in het onderwijs, bedrijfsleven en overheid. De rationale voor overheidsinterventie naast de inspanningen van alle betrokken stakeholders is beschreven in Bijlage 3.

Om deze coördinatie te bewerkstelligen en vraag en aanbod goed op elkaar af te stemmen, is het allereerst essentieel dat er een goed gezamenlijk begrip is van wat ‘de vraag’ en ‘het aanbod’ nu eigenlijk is. Uit het onderzoek is naar voren gekomen dat er, mede vanwege het relatief jonge karakter van het domein, geen gezamenlijke (geaccepteerde) taal bestaat om hierover van gedachten te wisselen. Het gevolg hiervan is dat (logischerwijs) iedereen vanuit een eigen perspectief en zienswijze spreekt en opereert. Vaak hebben deze perspectieven betrekking op een (klein) onderdeel van het totale human capital vraagstuk, waardoor een gezamenlijk totaalbeeld ontbreekt en er regelmatig gestreden wordt voor specifieke deelbelangen. Het gevaar van het ontbreken van een gezamenlijke taal is dat mensen, ondanks alle goede intenties, langs elkaar heen praten en het daarmee ook vrijwel onmogelijk wordt om effectieve coördinatie in te richten. Wij benadrukken dan ook het belang van **een gezamenlijke taal als cruciaal ingrediënt** bij het beschrijven van ‘de vraag’ en ‘het aanbod’, het verbinden van deze twee, en het coördineren van alle inspanningen die nodig zijn om dit succesvol te doen. De resultaten uit het onderzoeksrapport kunnen een basis vormen om deze gezamenlijke taal verder te gaan ontwikkelen.

De bovenbeschreven bevindingen zijn hieronder schematisch weergegeven:



Figuur 2 Conclusies uit onderzoeksrapport en de relatie met het advies

2. Het advies in het kort

2.1 Van onderzoek naar aanbevelingen

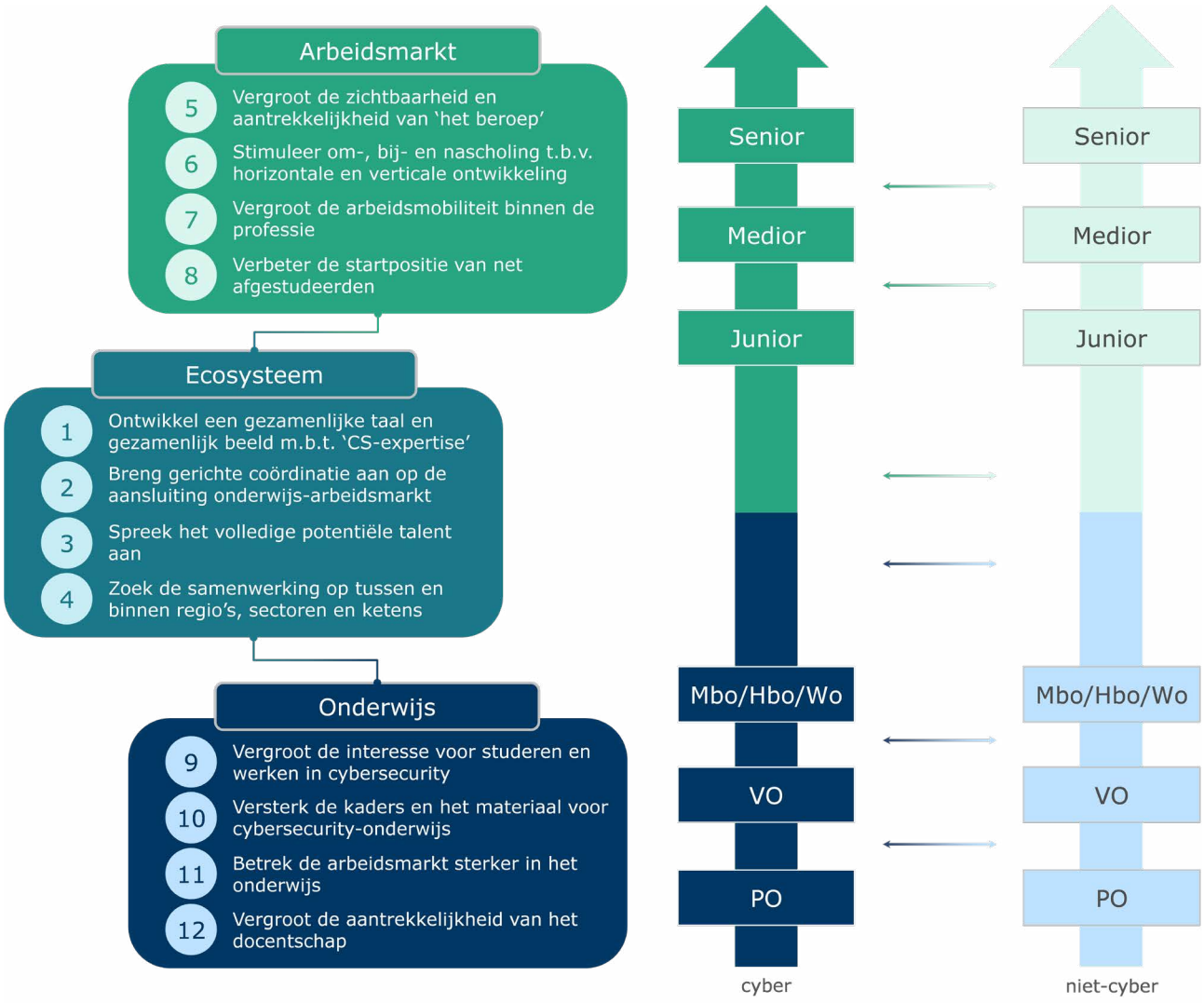
Het totale systeem van onderwijs en arbeidsmarkt is omvangrijk en divers. Zoals in het onderzoeksrapport staat beschreven gaat het ***op de arbeidsmarkt*** om verschillende typen expertise, een groot aantal verschillende (typen) organisaties en velerlei functieprofielen waar cybersecurity-expertise een rol speelt. ***In het onderwijs*** gaat het om verschillende onderwijstypen (PO, VO, MBO, HBO, WO, LLO) en een grote variëteit aan opleidingen die zich volledig of deels richten op cybersecurity. ***De mensen*** die zich door het systeem van onderwijs en arbeidsmarkt bewegen worden op hun beurt ook gekenmerkt door eigen beweegredenen, een eigen context en dynamiek. Alle betrokken partijen en schakels tussen hen vormen het gehele systeem van onderwijs en arbeidsmarkt. Zij ervaren allen hun eigen uitdagingen en knelpunten.

Hoewel we in dit adviesrapport de behoefte aan voldoende cybersecurityprofessionals als 'één uitdaging' brengen, willen we benadrukken dat het in de werkelijkheid gaat om een verzameling van een groot aantal kleinere deelproblemen, verspreid over de gehele keten van onderwijs en arbeidsmarkt. Er zal dan ook geen one-size-fits-all-oplossing zijn die alle deelproblemen in de gehele keten gaat oplossen. Het beeld dat we met één of enkele inspanningen of initiatieven het gehele vraagstuk kunnen oplossen is wat ons betreft niet reëel.
In dit adviesrapport is er bewust voor gekozen om een twaalftal aanbevelingen te formuleren ten aanzien van wat er zou moeten gebeuren, aangevuld met concrete voorbeelden ten aanzien van hoe hier invulling aan gegeven zou kunnen worden. Er is bewust niet voor gekozen om op detailniveau aan te geven wie wat moet gaan doen vanwege twee belangrijke argumenten:

1. **Praktische haalbaarheid:**
   Er zijn veel inspanningen op veel plekken in de onderwijs-arbeidsmarktketen nodig, en het uitwerken van al deze inspanningen op microniveau is praktisch niet haalbaar. Andersom geredeneerd heeft het geen zin om slechts één of enkele aanbevelingen te noemen, omdat het vraagstuk daarmee te plat wordt geslagen. Om deze reden is ervoor gekozen om de aanbevelingen te formuleren op een aggregatieniveau dat concreet genoeg en niet te gedetailleerd is. De aanbevelingen zijn nader uitgewerkt in dit adviesrapport (Hoofdstuk 3 t/m 5) en zijn aangevuld met concrete voorbeeldinitiatieven uit de praktijk (Bijlagen 5 t/m 8).

2. **Draagvlak:**
   De aanbevelingen moeten geoperationaliseerd worden door de betrokken partijen. Afhankelijk van bepaalde waarden, overtuigingen en uitgangsposities zullen verschillende betrokkenen op een andere manier willen omgaan met de aanbevelingen. Gedurende dit proces dienen inhoudelijke en procesmatige keuzes gemaakt te worden, die o.i. juist door de betrokken partijen genomen moeten worden. Dit zal het eigenaarschap en draagvlak vergroten.

We komen tot de volgende 12 aanbevelingen voor [A] het gehele ecosysteem van onderwijs en arbeidsmarkt, [B] stakeholders met betrekking tot de arbeidsmarkt in het bijzonder en [C] stakeholders met betrekking tot het (initieel en bekostigd) onderwijs in het bijzonder, zie figuur 3. Onder de figuur worden de adviezen kort toegelicht (tabel 1), waarna deze in hoofdstukken 3, 4 en 5 in meer detail uitgewerkt worden en van voorbeelden worden voorzien.



Figuur 3 Overzicht aanbevelingen

#	Aanbeveling	Toelichting
1	Ontwikkel een gezamenlijke taal en gezamenlijk beeld m.b.t. 'cybersecurity-expertise'.	Het is essentieel dat er een goed gezamenlijk begrip is van wat 'de vraag' en 'het aanbod' nu eigenlijk is. Zonder gezamenlijke taal is de kans groot dat men over verschillende facetten van cybersecurity-expertise spreekt. Hierdoor is het ook moeilijk is om gezamenlijke en gecoördineerde actie te ondernemen. Op basis van een gezamenlijke taal kan ook het gezamenlijke beeld over hoe het staat met 'de vraag' en 'het aanbod' versterkt worden. Er kan gewerkt worden aan de gezamenlijke informatiepositie m.b.t. dataverzameling (bijv. enquêtes van het CBS), het verwerken van data (bijv. gedeelde en gedragen classificaties van beroepen) en het ontsluiten van data (bijv. middels een gezamenlijk dashboard).
2	Breng gerichte coördinatie aan op de aansluiting onderwijs-arbeidsmarkt.	Cybersecurity-professionals en cybersecurity-expertise kennen een grote rijkheid aan verschillende typen beroepen, typen expertise en typen opleidingen. De reikwijdte is dusdanig groot dat geen enkele partij alleen de gevraagde expertise kan realiseren. Om de vraag op de arbeidsmarkt en het aanbod vanuit onderwijs over de volledige breedte van cybersecurity goed aan te laten sluiten is gecoördineerde actie nodig om de volledige vraag af te dekken én niet onnodig dubbel werk uit te voeren.
3	Spreek het volledige potentiële talent aan	Gezien de toenemende vraag naar talent is het van belang om zo min mogelijk potentieel talent onbenut te laten. Dit betekent dat er meer aandacht dient te komen voor diversiteit en inclusie in algemene zin. Daarbij kan er concreet gewerkt worden aan het aantrekken van (vooralsnog) ondervertegenwoordigde gender-groepen. Ook kan verkend worden hoe we het bestaande (cybersecurity-)talent met een mbo-opleidingsachtergrond beter kunnen benutten voor de sector.
4	Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.	Regio's verschillen in termen van vraag én aanbod van cybersecurity-professionals. Binnen de regio's verdient het dan ook aandacht om goed te kijken naar de regionale context en het verbinden van vraag en aanbod. Ook binnen sectoren en (waarde)ketens kunnen de handen ineengeslagen worden, omdat er binnen sectoren vaak sprake is van een sectorspecifieke kennisbasis voor cybersecurity-professionals. Tot slot kan ook tussen sectoren en (waarde)ketens samengewerkt worden, bijvoorbeeld als het gaat om het vergroten van de cybersecurity van mkb-toeleveranciers in complexe waardeketens.
5	Vergroot de zichtbaarheid en aantrekkelijkheid van 'het beroep'	Werkgevers in de cybersecurity kunnen de beeldvorming over de werkzaamheden en de professionals bijstellen. De aantrekkingskracht kan vergroot worden door de grote variëteit in functies en expertise (niet enkel technisch van aard), de breedte van het werkveld en het belang van werken binnen deze sector zichtbaar te benadrukken.
6	Stimuleer om-, bij- en nascholing ten behoeve van horizontale en verticale ontwikkeling	Om cybersecurity professionals te stimuleren zich verder te ontwikkelen dient de vraag vanuit de werkgevers gestimuleerd te worden. Ontwikkelpaden bieden carrièreperspectief waardoor professionals weten welke mogelijkheden er zijn en welk aanbod hierbij passend is. De samenwerking tussen onderwijs (publiek en privaat) en werkgevers dient voor een actueel en gevarieerd aanbod te zorgen dat alle medewerkers stimuleert verder te ontwikkelen. Deze ontwikkelpaden met bijbehorende aanbod is ook in te zetten ter bevordering van de horizontale ontwikkeling, waardoor de overstap naar een cybersecurity loopbaan aantrekkelijk wordt gemaakt.
7	Werk aan behoud van professionals m.b.v. arbeidsmobiliteit binnen de sector	In een regionale en lokale samenwerking tussen werkgevers kunnen aantrekkelijke voorwaarden gecreëerd worden, waardoor cybersecurity professionals beter behouden kunnen worden binnen de cybersecurity sector. Door bijvoorbeeld in gezamenlijkheid 1 baan te creëren, binnen het netwerk de mogelijkheid bieden om verschillende werkgevers te verkennen en samen op zoek te gaan naar de juiste match.

8	Verbeter de startpositie van net afgestudeerden	Door de overstap van onderwijs naar bedrijfsleven te begeleiden, en als werkgever bewust in te zetten op de training en ontwikkeling van startende medewerkers kunnen de junior professionals sneller op het gewenste niveau gebracht worden. Hierdoor vergroot je de kans op het behouden van junior professionals voor de cybersecurity sector en kan een junior sneller medior taken uitvoeren.
9	Vergroot de interesse voor studeren en werken in cybersecurity	Het ontwikkelen van interesse voor een bepaald vakgebied begint al op jonge leeftijd. In het po en vo kan meer aandacht komen voor digitale technologie en digitale vaardigheden in generieke zin, maar ook voor cybersecurity specifiek. De beeldvorming over deze onderwerpen en het studeren en werken in het vakgebied is een belangrijke determinant voor de keuze voor studie en werk. Onderwijsinstellingen kunnen cybersecurity duidelijker en aantrekkelijker neerzetten binnen de diverse vervolgopleidingen in het mbo en ho. Het gaat dan niet enkel om de 'cyber-specialistische' opleidingen, maar bijv. ook om juridisch of economisch georiënteerde opleidingen die relevant zijn voor het cybersecuritydomein.
10	Versterk de kaders en het materiaal voor cybersecurity-onderwijs	Om cybersecurity beter in te bedden in de gehele onderwijsketen zijn goede kaders en materiaal een vereiste. Er is behoefte aan meer uitgewerkte kerndoelen en doorlopende leerlijnen/curricula en onderwijsmateriaal voor en vanaf het funderend onderwijs. In het mbo is voor de ICT-opleidingen in de kwalificatiedossiers vastgelegd wat mbo-studenten aan het eind van hun opleiding moeten kennen en kunnen. Cybersecurity krijgt hierbinnen al in toenemende aandacht. Voor het hoger onderwijs kan gedacht worden aan het gezamenlijk opstellen van content en curricula voor zowel cyber-specialistische als aanpalende opleidingen. Binnen het hbo kan cybersecurity eventueel verplicht gesteld worden binnen HBO-ICT-opleidingen. Voor het wo kan een pool van hoogleraren aangesteld worden die voor een dekkend onderwijsaanbod zorgen.
11	Betrek de arbeidsmarkt sterker in het onderwijs	De cybersecurity-arbeidsmarkt verandert razend snel. Voor het onderwijs is het daarom van belang om goed verbonden te blijven met de arbeidsmarkt om te weten wat er gevraagd wordt. De arbeidsmarkt kan daarbij ook een belangrijke rol spelen in het bieden van de expertise die binnen de opleidingen benodigd is om de studenten adequaat op te leiden. Samen met de arbeidsmarkt kan gewerkt worden aan actuele vaardigheden voor studenten, het docententekort, contextrijke leeromgevingen, flexibeler opleiden, en gezamenlijke promotie van het werkveld.
12	Versterk en vergroot de aantrekkelijkheid van het docentschap	Het docentschap in cybersecurity moet zowel voor zittende als nog te werven docenten aantrekkelijk gemaakt. Om te beginnen moeten we bestaande docenten in cybersecurity behouden en optimaal benutten. Hybride functies, zoals docentenaanstellingen gecombineerd met dienstverbanden bij bedrijven, kunnen hierbij helpen. Daarnaast vraagt het investeringen in bij- en nascholing voor docenten om hun kennis over cybersecurity actueel te houden. Maak dit laagdrempeliger door subsidies voor ICT-docenten en docentstages bij bedrijven en landelijke masterclasses . En ook moet gezien de tekorten aan docenten omscholing naar docent cybersecurity toegankelijker worden. Voorbeelden zoals Make IT Work bieden aantrekkelijke omscholingsmogelijkheden naar IT en cybersecurity met baangarantie en beperkte kosten voor de deelnemer.

Tabel 1 Toelichting aanbevelingen

3. Advies Ecosysteem

Onderstaande aanbevelingen gaan in op acties die door het ecosysteem als geheel genomen kunnen worden. Met de term 'ecosysteem' doelen we hier op alle actoren die van belang (kunnen) zijn voor het versterken van het onderwijs en de arbeidsmarkt ten aanzien van cybersecurityprofessionals. Het gaat dus om stakeholders vanuit de overheid, het bedrijfsleven, het onderwijs, en overige stakeholders die hierbij een rol (kunnen) spelen. We hanteren hier de term ecosysteem, omdat de aanbevelingen door alle betrokken (typen) stakeholders gezamenlijk opgepakt zouden moeten worden. De impact van de aanbevolen acties is direct afhankelijk van de mate waarin alle betrokkenen zich committeren aan de acties.

De volgende vier aanbevelingen worden verder toegelicht:
1. Ontwikkel een gezamenlijke taal en gezamenlijk beeld m.b.t. 'cybersecurity-expertise'.
2. Breng gerichte coördinatie aan op de aansluiting onderwijs-arbeidsmarkt.
3. Spreek het volledige potentiële talent aan
4. Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.

3.1. Ontwikkel een gezamenlijke taal en gezamenlijk beeld m.b.t. 'cybersecurity-expertise'.

Zoals in Hoofdstuk 1 is beschreven zijn de termen 'cybersecurity' en 'cybersecurity-expertise' in zekere zin containerbegrippen. Het gaat over een grote rijkheid aan typen professionals, typen expertise en typen organisaties die op hun eigen manier te maken hebben met het thema cybersecurity. Het is essentieel dat we een goed gezamenlijk begrip hebben van wat we verstaan onder 'cybersecurity-expertise'. Dit is immers ook de basis om te beschrijven wat 'de vraag' en 'het aanbod' nu eigenlijk is. Zonder gezamenlijke taal is de kans groot dat men over verschillende facetten van cybersecurity-expertise spreekt. Hierdoor is het ook moeilijk om gezamenlijke en gecoördineerde actie te ondernemen. Op basis van een gezamenlijke taal kan ook het gezamenlijke beeld over hoe het staat met 'de vraag' en 'het aanbod' versterkt worden. Er kan gewerkt worden aan de gezamenlijke informatiepositie m.b.t. dataverzameling (bijv. enquêtes van het CBS), het verwerken van data (bijv. gedeelde en gedragen classificaties van beroepen) en het ontsluiten van data (bijv. middels een gezamenlijk dashboard). Hieronder werken we een aantal concrete suggesties nader uit.

1) Gezamenlijke taal

Om een gezamenlijke taal te spreken kan het waardevol zijn om aan te sluiten bij bestaande conceptuele kaders over cybersecurity-professionals en -expertise. Door gebruik te maken van gezamenlijke conceptuele kaders kan men borgen dat mensen over dezelfde concepten spreekt. Eén bron is het ECSF, welke ook in het voorgaande onderzoek is gebruikt. Een beperking is echter dat er veel meer functieprofielen op de arbeidsmarkt bestaan waar cybersecurity-expertise gevraagd wordt dan de functies die door het ECSF beschreven worden. In het onderzoeksrapport wordt getoond hoe verschillende functieprofielen een 'hoog', 'middel' of 'laag' cybersecuritygehalte hebben. Sommige functies bevatten slechts één of enkele cybersecuritytaken of benodigde cybersecuritycompetenties. Om toch met een gezamenlijke taal te spreken over alle relevante functies kan gebruik gemaakt worden van gezamenlijke taal op het niveau van onderliggende bouwstenen (taken, deliverables, kennis, vaardigheden) in plaats van enkel gezamenlijke taal op het niveau van functies. In het onderzoeksrapport is daarbij gepoogd om de grote variëteit aan deze bouwstenen te groeperen aan de hand van een 'categorie' waar ze toe behoren (technisch, management en organisatie, juridisch, onderzoek/ analyse, onderwijs).

Een dergelijke benadering kan helpen om de grote variëteit en complexiteit in cybersecurity-expertise terug te brengen naar [1] een behapbaar niveau dat tegelijkertijd [2] voldoende fijnmazigheid biedt om recht te doen aan de verschillende facetten van cybersecurity-expertise.

Wij bevelen de betrokken stakeholders in het ecosysteem aan om gezamenlijk te bespreken hoe de gehanteerde taal op het onderwerp verder ontwikkeld en gestandaardiseerd kan worden. Welke conceptuele kaders zouden bruikbaar kunnen zijn, en welke afspraken willen we maken over het spreken over cybersecurity-expertise? Idealiter wordt deze gezamenlijke taal gesproken in zowel het onderwijs als de arbeidsmarkt. Dit stelt het onderwijs beter in staat haar opleidingsaanbod beter te richten op de behoeften op de arbeidsmarkt. De arbeidsmarkt kan eenvoudiger aangeven waar haar behoeften liggen en kan makkelijker een rol pakken in het vormgeven van gezamenlijk onderwijs tussen onderwijsinstellingen en arbeidsmarkt.

2) Gezamenlijk beeld: informatiepositie vergroten

Met een gezamenlijke taal wordt het vervolgens eenvoudiger om een gezamenlijk beeld te creëren van de stand van zaken rondom human capital op het gebied van cybersecurity. Om goed te kunnen sturen op actuele ontwikkelingen op de onderwijs- en arbeidsmarkt is het van belang om een goede informatiepositie te hebben: wat gebeurt er, waar zit de vraag, waar zit het aanbod, en hoe kunnen we vraag en aanbod goed op elkaar laten aansluiten? Op een eenduidige wijze data verzamelen en ontsluiten kan hierbij behulpzaam zijn. Veel arbeidsmarktdata op het gebied van cybersecurity wordt momenteel op verschillende manieren door verschillende partijen opgehaald, en gekoppeld aan de individuele vraag. Deze manier van dataverzameling maakt het niet altijd mogelijk om informatie te bundelen om bijv. op landelijk niveau data te vergelijken. De volgende adviezen hebben allen als doel het vergroten van de informatiepositie waardoor ook op landelijk niveau gestuurd kan worden.

- Beroepenclassificatie cybersecurity verbeteren
  Het CBS gebruikt verschillende beroepenclassificaties in statistieken over de arbeidsmarkt om beroepen te kunnen indelen naar niveau en richting. In de beroepenclassificatie is momenteel cybersecurity niet gespecificeerd terug te vinden in de beschrijving. Dit maakt dat het verder onderzoeken en monitoren van de ontwikkelingen binnen deze beroepsgroep niet eenduidig gebeurt. Het advies is dan ook om de mogelijkheden te verkennen de beroepenclassificatie voor cybersecurity te verbeteren door verdere specificatie mogelijk te maken.

- Dashboard
  De data en manier van dataverzameling van het onderwijs- en arbeidsmarktonderzoek kan breed ontsloten worden. Hierdoor kunnen alle betrokken partijen werken met dezelfde data. Dit heeft als voordeel dat data systematisch verzameld kunnen worden en dat ze efficiënter en effectiever ingezet kunnen worden. Het aanbieden van een netwerkkaart in een visueel overzicht biedt bijv. de mogelijkheid om alle onderwijsmogelijkheden voor cybersecurity terug te vinden, en bijv. ook de partijen die werken aan het Human Capital beleid voor cybersecurity. Dit dashboard kan ook ingericht worden om de effecten van alle acties zichtbaar te maken en om data op verschillende manieren te onttrekken voor regionale/ lokale toepassingen.

- Standpuntbepalingen + uitdragen
  Naast het aanbieden van eenduidige informatie en het monitoren van effecten, kan het gecoördineerd nationaal verzamelen van data belangrijke input geven om bijv. effecten zichtbaar te maken van interventies en besluiten. Bijvoorbeeld ten aanzien van arbeidsmigratie wordt meermaals als advies genoemd om gezamenlijk de impact te onderzoeken van arbeidsmigratiebeleid op de cybersecurity arbeidsmarkt.
  De sector kenmerkt zich door een relatief hoge instroom van arbeidsmigranten: welk effect hebben mogelijke toekomstige maatregelen? Denk hierbij ook aan bijvoorbeeld de effecten van de verandering van Engelstalig onderwijs naar Nederlandstalig onderwijs op de instroom van cybersecurity studenten en PhD's. Deze impactmeting dient als input genomen te worden om vervolgens standpunt te bepalen en dit op nationaal niveau uit te dragen.

- Zicht krijgen op mbo- vacatures cybersecurity.
  Het onderzoeksrapport is gebaseerd op vacatureanalyses. Arbeidsposities die ingevuld worden op een andere manier zijn hierdoor buiten de scope van het onderzoek gevallen. Tijdens de reeks van gesprekken en bijeenkomsten is naar voren gekomen dat mogelijk voor mbo-vacatures de vervulling wellicht op een andere manier verloopt. Via stages en door gebruik te maken van het bestaande netwerk van bedrijven, vinden mbo-professionals mogelijkerwijs eerder een baan dan bij het stellen van een vacature. Hierdoor kan de arbeidsmarktanalyse een onvolledig beeld geven. Dat er geen tekort is aan mbo-opgeleiden wordt namelijk niet herkend. Wel moet hierbij opgemerkt worden dat een (relatief) laag aantal vacatures niet betekent dat er geen tekort is; het gaat bij een tekort immers om onvervulde vraag (hier is aanbod dus ook relevant voor).

  Het advies zal dan ook zijn om bij beleidsmaatregelen voor het mbo en mbo-afgestudeerden verdiepend onderzoek te verrichten als de huidige informatiepositie als onvoldoende bestempeld wordt.

3) Gezamenlijk beeld: curricula

Zoals eerder beschreven in hoofdstuk 5 worden er op landelijk niveau afspraken gemaakt over de inhoud van de mbo-kwalificatiedossiers en werken de hbo-ICT opleidingen aan een gezamenlijk addendum voor cybersecurity van het landelijke beroepsprofiel. Daarnaast werkt iedere opleiding aan de verbinding met de arbeidsmarkt door in bijv. werkveldadviescommissies de actuele ontwikkelingen te bespreken. De diversiteit in het cybersecurity onderwijs is erg hoog, en niet altijd passend bij de actuele en toekomstige ontwikkelingen. Een gezamenlijke taal en een gezamenlijk beeld van vraag en aanbod kunnen helpen bij het effectief vormgeven van curricula binnen Nederland.

Een manier om dit vorm te geven is door het nationaal ontwikkelen van een **frame en profielen met kaders over de inhoud van het curriculum van de cyberopleidingen op mbo- en hoger onderwijsniveau**. Dit zal bijdragen aan een kwalitatieve en eenduidige inhoud van de cybersecurity-opleidingen die ook kan zorgen voor een kwalitatief goede aansluiting in de doorstroom van opleidingen. Een **landelijke commissie met vertegenwoordigers van kennisinstellingen en bedrijfswereld** heeft in dat geval de opdracht om een dekkend curriculum te ontwikkelen en kan dit tevens ook jaarlijks updaten, gezien de hoge innovatiesnelheid. Daarnaast kan het **landelijk ontwikkelen en beschikbaar stellen van onderwijsmateriaal** ervoor zorgen dat op een efficiënte manier kwalitatief goede modules ingezet kunnen worden in de verschillende curricula. Dit voorkomt zowel dubbel werk als hiaten in het opleidingsaanbod.

4) Gezamenlijk beeld: visie op migratie

Immigratie en arbeidsmigranten lijken belangrijk te zijn voor de sector: circa 5-10% van de instroom is toe te schrijven aan werknemers uit het buitenland die in Nederland komen werken. In de eerdere adviezen rondom het vergroten van de informatiepositie is al gesproken over de impact die beleid en maatregelen kunnen hebben op de cybersecurity-arbeidsmarkt en haar instroom. Als advies geldt dan ook om de implicatie van politieke keuzes scherp te krijgen en de impact voor de cybersecurity-arbeidsmarkt inzichtelijk te maken. Zonder een politiek standpunt in te nemen is het wel waardevol als we binnen Nederland zicht hebben op de gevolgen van bepaalde politieke keuzes. De rol die professionals vanuit het buitenland vervullen dient in ieder geval meegenomen te worden in de overwegingen met betrekking tot migratiebeleid.

Indien men voor deze groep arbeidsmigranten/kennismigranten zou besluiten hen juist wel aan te willen trekken, worden door gesprekspartners stimulerende maatregelen genoemd in de hoek van community building en het faciliteren van een soepele en veilige instroom vanuit het buitenland. Specifiek gaat het bijvoorbeeld om het erkennen van buitenlandse diploma's en het gebruik van het EU skills & jobs platform. Voor internationale studenten geldt uiteraard dat het wijzigen van de Engelse voertaal naar het Nederlands een sterk beperkend effect zal hebben voor de instroom.

3.2. Breng gerichte coördinatie aan op de aansluiting onderwijs-arbeidsmarkt

Cybersecurity-professionals en cybersecurity-expertise kennen een grote rijkheid aan verschillende typen beroepen, typen expertise en typen opleidingen. De reikwijdte is dusdanig groot dat geen enkele partij alleen de gevraagde expertise kan realiseren. Om de vraag op de arbeidsmarkt en het aanbod vanuit onderwijs over de volledige breedte van cybersecurity goed aan te laten sluiten is gecoördineerde actie nodig om de volledige vraag af te dekken én niet onnodig dubbel werk uit te voeren. Zoals hiervoor beschreven is een gezamenlijke taal en een gezamenlijk beeld een belangrijk ingrediënt voor effectieve coördinatie.

De benodigde coördinatie dient zich in ieder geval te richten op het volgende:

1. Het in kaart brengen van de diverse en omvangrijke vraag op de arbeidsmarkt. Welke partijen hebben welke professionals en expertise nodig?
2. Het in kaart brengen van de diverse opleidingen (bekostigd en onbekostigd). Welke partijen bieden welk scholingsaanbod aan?
3. Het coördineren van inspanningen om vraag en aanbod beter op elkaar aan te laten sluiten.

Voor het coördineren van de activiteiten om vraag en aanbod beter op elkaar aan te laten sluiten valt te denken aan gezamenlijk portfoliomanagement op alle curricula binnen onderwijsinstellingen, om ervoor te zorgen dat er niet

te weinig en niet te veel in- en uitstroom van bepaalde profielen ontstaat. Ook kan gericht gekeken worden welke spelers op de arbeidsmarkt een gerichte bijdrage kunnen leveren aan het vormgeven en versterken van bestaande opleidingen. Een derde voorbeeld is het creëren van deeltijdaanstellingen voor professionals die graag ook actief zijn in het onderwijs, maar waarvoor het ontbreken van een duidelijke match met een opleiding/onderwijsinstelling nu een te grote drempel opwerpt.

Voor het coördineren van vraag en aanbod op het gebied van cybersecurity is het van belang om aan te geven dat **cybersecurity slechts een klein deel van het gehele Human Capital vraagstuk in Nederland is** en dat we bij het bepalen en uitvoeren van beleidsinstrumenten rekening moeten houden met het overkoepelende geheel. Veel sectoren en beroepsgroepen kennen immers tekorten; denk bijvoorbeeld aan de zorg, het onderwijs of 'groene professionals'. Het risico op beleidsconcurrentie is in deze tijden van schaarste aan menselijk kapitaal dan ook groot: vanuit verschillende hoeken wordt getrokken aan dezelfde groep mensen. Ter illustratie: wanneer iemand vanuit de softwareontwikkeling naar cybersecurity wordt omgeschoold heeft het cybersecuritydomein er weliswaar een professional bij, maar heeft het softwaredomein (waar ook schaarste is) iemand verloren. Wanneer meerdere domeinen ongecoördineerd inspanningen plegen om dezelfde personen aan zich te binden gaat dit gepaard met aanzienlijke kosten en geen of nauwelijks netto resultaat voor Nederland. Aansluiten bij bestaand beleid en maatregelen, zoals bijvoorbeeld bij de Human Capital Agenda ICT, kan deze risico's beperken en leiden tot doelmatiger beleid. Vanuit de specifieke situatie voor cybersecurity dient een duidelijke focus en keuze in aanpak en uitvoer gekozen te worden.

De adviezen die in dit rapport genoemd worden dienen door de verschillende betrokken partijen besproken te worden en vertaald te worden in concrete programma's en acties. De afstemming hiervan bij de verschillende betrokken ministeries, het gericht inzetten van acties en investeringen, al dan niet in samenwerking met bestaande regelingen heeft landelijke coördinatie en monitoring nodig. In hoofdstuk 6 geven we enkele suggesties over wie er aan zet kan zijn en hoe dit ingericht zou kunnen worden.

3.3. Spreek het volledige potentiële talent aan

In tijden van schaarste aan menselijk kapitaal is het vanuit het perspectief van het cybersecuritydomein van belang om het volledige potentiële talent aan te spreken. Om dit te bewerkstelligen zijn drie concrete richtingen naar voren gekomen: [1] het versterken van het imago, [2] het potentieel van mbo-opgeleiden beter benutten en [3] versterken diversiteit & inclusie.

1) Versterken van het imago

Uit de verschillende workshops en gesprekken is meerdere malen naar voren gekomen dat het imago rondom leren en werken in de cybersecurity-sector voornamelijk een technische en ICT-achtige insteek kent. Studenten en werkenden hebben het beeld dat dit voornamelijk een (ICT) technisch vakgebied is. Het werkveld geeft aan dat deze sector veel diverser en breder is dan dat. Het advies is dan ook om middels een landelijk uitgevoerd programma te werken aan een juiste beeldvorming van wat leren en werken binnen deze sector inhoudt. Het gebruik van rolmodellen wordt hierbij van verschillende kanten aangeraden. Deze beeldvorming dient ingezet te worden in de gehele keten, van het basisonderwijs tot en met de huidige werknemers. Er kan gebruik gemaakt worden van bestaande en nieuwe middelen. Denk hierbij aan gastlessen, challenges, voorlichtingen, maar ook in actuele opdrachten op mbo-, hbo- en wo-niveau.

2) Potentieel mbo-opgeleiden beter benutten

Binnen de mbo-opleidingen heerst het beeld dat de kennis en met name de vaardigheden van mbo-ICT-ers op de arbeidsmarkt onderschat worden. In de vacature-analyses beschreven in het onderwijs en arbeidsmarkt onderzoek is ook te zien dat de vraag naar medior- en seniorfuncties op hbo- en wo-niveau groeiende is en niet voldoende gematcht wordt met de vraag. Door de huidige kennis en vaardigheden van mbo-opgeleiden beter voor het voetlicht brengen, kunnen mbo-afgestudeerden beter ingezet worden en wellicht een deel van de werkzaamheden verrichten die nu als hbo-werkzaamheden gekwalificeerd worden.

Op landelijk niveau kan dit meegenomen worden in bijv. het nationaal op te stellen framework en kaders rondom de curricula. Op regionaal en lokaal niveau kunnen in samenwerking met het onderwijs en bedrijfsleven kennis en vaardigheden van mbo afgestudeerden gematcht worden met de vraag vanuit het bedrijfsleven. Op deze manier kan op basis van de actuele kennis en vaardigheden van afgestudeerden gekeken worden naar de vacaturevraag.

3) Diversiteit & inclusie

Als algehele kans voor de cybersecurity-arbeidsmarkt wordt het vergroten van de diversiteit gezien. "Op de ICT-arbeidsmarkt is slechts 20% van de werkenden een vrouw. Dit grote verschil in verhouding man versus vrouw is ook zichtbaar in het hoger beroepsonderwijs. De instroom in de bachelor hbo-ICT opleiding bestaat voor 89% uit mannen."[4] Tijdens het onderwijs- en arbeidsmarktonderzoek vonden we dat de huidige populatie cybersecurity-professionals voor ongeveer een derde bestaat uit vrouwen.

In de gesprekken gevoerd voorafgaand aan het opstellen van het advies is meermaals het vergroten van de gehele diversiteit in de sector genoemd. Hierbij dient een programma met activiteiten in de gehele keten ervoor te zorgen dat de diversiteit vergroot wordt. Ter inspiratie kan ook naar buitenlandse voorbeelden gekeken worden zoals dit voorbeeld van 'Empowering you' in de UK.

3.4. Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.

In veel van de gevoerde gesprekken is het belang van samenwerking tussen en binnen regio's, sectoren en ketens benoemd. Wij bevelen aan om hier verder gehoor aan te geven. Hieronder werken we een aantal richtingen uit waarin samenwerking versterkt kan worden.

1) Regionale samenwerking

Iedere regionale arbeidsmarkt kenmerkt zich op een eigen manier, zo ook voor cybersecurity. De aanwezigheid van bepaalde bedrijven, sectoren en onderwijsinstellingen maakt dat regionaal vraag en aanbod afgestemd dienen te worden. Op het gebied van kennisdisseminatie en het matchen van vraag en aanbod worden de volgende adviezen gegeven:

- Kennisdisseminatie
  Regionaal (opleidings-/ ontwikkel-)aanbod kan heel goed via regionale partijen ontsloten worden. Middels publiek private samenwerkingen, en regionaal arbeidsmarktbeleid kan aanbod bekend worden gemaakt, aangeboden worden en (financieel) aantrekkelijk worden gemaakt.

- Match vraag en aanbod
  De cybersecurity-arbeidsmarktvraagstukken dienen ook regionaal gesignaleerd en opgepakt te worden. Bestaande netwerken, arbeidsmarktregio's, PPS-en en/of learning communities kunnen hierin een grote rol spelen. Bedrijven kunnen samenwerken door bijv. traineeships te gaan aanbieden en mogelijkheden in gezamenlijkheid te creëren zodat het voor cybersecurity-professionals aantrekkelijk wordt om in de regio en binnen de sector te (blijven) werken. Een voorbeeld hiervan is het regionaal werkgeverschap: **'Regionaal werkgeverschap biedt kansen om het arbeidspotentieel beter benutten, professionals te behouden en beter inzetbaar te maken. Doordat professionals (tegelijkertijd) voor meerdere organisaties in de keten kunnen werken, zijn zij breder inzetbaar, ontwikkelen zij hun talent en vergroten zij hun werkzekerheid.**'[5] Vanuit werkgeversperspectief is dit bovendien interessant om zelfs bij een klein dienstverband een gespecialiseerde medewerker in dienst te kunnen nemen. In de zorg zijn al voorbeelden van dit soort constructies bekend waarbij een consortium van werkgevers en werknemers binnen dit besloten netwerk onderling werk, opdrachten en bijvoorbeeld stages uitwisselen (De Werkgeverij).

  Het advies is dan ook om de bestaande regionale netwerken te benutten en de samenwerking en afstemming tussen deze netwerken en landelijk beleid te stimuleren.

2) Samenwerking tussen sectoren en ketens

Eén van de observaties in het onderzoek is dat, mede met de introductie van de NIS2 en CRA, cybersecurity een fenomeen is dat in de gehele waardeketen geborgd moet worden. Partijen zijn immers afhankelijk van elkaar en elkaars (deel)producten, waardoor beperkte borging van cybersecurity bij de ene partij invloed heeft op andere partijen in de keten.

4. https://hcaict.nl/thema/diversiteit-en-inclusie/
5. https://wzw.nl/goed-werkgeverschap/regionaal-werkgeverschap-en-flexibilisering-arbeidsmarkt/

Met name grote bedrijven zien ook een verantwoordelijkheid om de toeleveranciers, wat veelal uit mkb bestaat, op een voldoende niveau van cybersecurity te krijgen. Deze ontwikkeling beperkt zich niet tot één sector, omdat cybersecurity immers sector-overstijgend is. Het borgen van cybersecurity is echter niet enkel een verantwoordelijkheid van de grote stuwende bedrijven, maar is een verantwoordelijkheid van alle ketenspelers (en de overheid).

Wij adviseren daarom om kennisuitwisseling te faciliteren m.b.t. het cyberveilig krijgen van de gehele waardeketen tussen/over sectoren heen. Gezien de prominente positie van grote bedrijven in deze ketens, kan bijvoorbeeld gedacht worden aan een samenwerkingsvorm die door/binnen de Topsectoren in Nederland ingericht wordt. Hier bestaan immers al de nodige organisaties, netwerken en ervaring om dit in te richten. Door de samenwerking tussen sectoren op te zoeken kunnen partijen vanuit bijv. de hightechsector en de energiesector de handen ineenslaan om de gedeelde uitdagingen m.b.t. samenwerking in de keten op dit thema aan te pakken.

4. Advies Arbeidsmarkt

Onderstaande aanbevelingen gaan in op het **aantrekken en behouden van cybersecurity-professionals**. Hierbij maken we onderscheid in het behouden en doorontwikkelen van de huidige professionals (de verticale ontwikkeling van cybersecurity professionals) alsook het aantrekken van zij-instromers (de horizontale ontwikkeling van cybersecurity professionals). De volgende vier aanbevelingen worden verder toegelicht:

- Vergroot de zichtbaarheid en aantrekkelijkheid van 'het beroep'.
- Stimuleer om-, bij- en nascholing ten behoeve van horizontale (overstap vanuit een andere sector) en verticale ontwikkeling (binnen de cybersecurity sector verder ontwikkelen).
- Werk aan behoud van professionals met behulp van arbeidsmobiliteit binnen de sector.
- Verbeter de startpositie van net afgestudeerden.

4.1. Vergroot de zichtbaarheid en aantrekkelijkheid van 'het beroep'

Uit de vragenlijst die tijdens dit onderzoek gehouden is onder cybersecurity werkgevers wordt benoemd dat er door niet- cybersecurity professionals heel anders naar het werk gekeken wordt. Vaak betreft dit een onrealistisch beeld over de complexiteit en de inhoud van het werk dat met name technisch van aard zou zijn. Werkgevers in de cybersecurity kunnen de beeldvorming over de werkzaamheden en de professionals bijstellen. Deze constatering wordt beaamd in de verschillende gesprekken die verder gevoerd zijn.

De aantrekkingskracht kan vergroot worden door de grote variëteit in functies en expertise (niet enkel technisch van aard), de breedte van het werkveld en het belang van werken binnen deze sector zichtbaar te benadrukken. Via aanbeveling 9 (vergroot de interesse voor studeren en werken in cybersecurity) en 11 (betrek de arbeidsmarkt sterker in het onderwijs) kunnen de juiste beelden overgebracht worden op leerlingen, studenten en potentiële zij- instromers.

4.2. Stimuleer om-, bij- en nascholing ten behoeve van horizontale en verticale ontwikkeling

Om de verticale en horizontale ontwikkeling van cybersecurity professionals te stimuleren worden 8 verschillende acties benoemd die te maken hebben met stimuleren van scholing, het inzichtelijk maken van verschillende ontwikkelmogelijkheden en de manier van aanbieden van het om, bij en nascholingsaanbod.

1) Bewustwording vergroten over Leven Lang Ontwikkelen

Vooral vanwege de groter wordende vraag naar cybersecurityspecialisten met multidisciplinaire (achtergrond) kennis die het thema breed kunnen aanvliegen, is er een dringende oproep om huidige en toekomstige cybersecuritymedewerkers bij, om en na te scholen.

In de verschillende gesprekken die gevoerd zijn in de aanloop naar dit advies geven meerdere partijen aan dat het bestaande aanbod aan scholing niet voldoende wordt afgenomen. Het vrijmaken van medewerkers voor scholing is lastig in verband met (onder andere) de huidige hoeveelheid werk en orderportefeuille van bedrijven. Het is van belang om de bewustwording voor het volgen van scholing te vergroten, op landelijke, regionale en lokale schaal en vervolgens te faciliteren. Gezien de impact die cybersecurity heeft op onze samenleving, dienen we het Leven Lang Ontwikkelen op het gebied van cybersecurity extra aan te jagen.

2) Generiek stimuleringsbeleid

Het al dan niet volgen van cursussen, modules, opleidingen etc. is voor een medewerker afhankelijk van meerdere factoren. De zogeheten kosten-batenanalyse maakt dat een leidinggevende en/of de medewerker zelf besluit of de inzet (tijd, financieel etc.) het waard is ten opzichte van de te verwachte opbrengst.

Het landelijk aanbieden van een financieel aantrekkelijke regeling om Leven Lang Ontwikkelen te stimuleren binnen cybersecurity wordt gezien als een maatregel die veel impact kan hebben. Hiermee kan het om-, bij- en nascholen van cyberspecialisten extra aandacht krijgen en medewerkers en bedrijven sneller, makkelijker in staat stellen om de keuze te maken aangezien de financiële eigen bijdrage verkleind wordt. In de National Cyber Workforce and Education Strategy van de Verenigde Staten (start 2023) maken ze gebruik van een soortgelijke

regeling om goedkope/ gratis bijscholingsmogelijkheden aan te bieden voor kleine bedrijven (zie Bijlage 2).
Er zijn drie belangrijke voordelen van het inrichten van een dergelijk generiek instrument:

a. We zetten de markt, individuele organisaties en individuele personen in hun kracht doordat zij zelf kunnen besluiten [1] aan welke (private) opleidingen, trainingen en cursussen behoefte is en deze in de markt kunnen zetten, en [2] welke opleidingen, trainingen en cursussen men wil volgen. Het is een illusie dat vanuit de Rijksoverheid geformuleerd kan worden waar alle individuele ondernemingen behoefte aan hebben en wat zij zouden moeten doen. Ondernemers kennen hun eigen bedrijf als geen ander, en het is juist essentieel om hen te faciliteren in wat nodig is voor hén. Met een generiek instrument kunnen wel criteria gesteld worden waar de gesubsidieerde opleidingen aan moeten voldoen (bijv. relevant voor cybersecuritydomein), zonder specifiek te bepalen wat de inhoud van de opleiding moet zijn; daar kan de markt zelf vorm aan geven.
b. Het instrument hoeft zich niet te beperken tot cybersecurity. Ook andere relevante maatschappelijke thema's zoals AI, duurzaamheid, zorg of onderwijs kunnen opgenomen worden in een dergelijk generiek instrument. De criteria om ondersteuning voor om-, bij- of nascholing (deels) gesubsidieerd te krijgen kunnen periodiek aangepast worden. Wel is het essentieel dat er sprake is van goede 'gate-keeping': een scherpe controle of het opleidingsaanbod aan de vastgestelde kwaliteitscriteria voldoet. Het instrument kan vanwege het generieke karakter meebewegen met de toekomstige (maatschappelijke) vraag.
c. Doordat het instrument generiek is kunnen de uitvoeringskosten relatief laag gehouden worden. Middels één instrument kan de nodige ondersteuning op het gebied van Human Capital geboden worden voor allerhande onderwerpen en domeinen.

Kortom: de uitvoeringskosten kunnen relatief laag gehouden worden, ook andere maatschappelijke (transitie)thema's kunnen ervan profiteren, wordt de markt in zijn kracht gezet, en kan het instrument ook in de toekomst continu meebewegen met de (maatschappelijke) vraag.

3) Vraagstimulering

Het stimuleren van het Leven Lang Ontwikkelen van de huidige medewerkers ligt voor een groot deel bij de werkgevers. Bovenstaande adviezen stimuleren dit. In de gesprekken met stakeholders is ook het belang van verdere vraagstimulering vaker aan bod gekomen.

Concrete ideeën om de vraag verder te stimuleren is door te verkennen of het invoeren van een landelijke PE (permanente educatie)-systematiek mogelijk meerwaarde kan bieden om continue bij- en nascholing voor cybersecurity professionals te stimuleren Ook kan via de route van normering en standaarden (bijv. ISO) verkend worden of dergelijke kaders de vraag kunnen stimuleren om mensen verder op te leiden op het gebied van cybersecurity.

Wij raden aan te verkennen of het invoeren van een PE- systematiek en verdere normering standaardisatie (bijv. ISO, PE, etc.) mogelijke meerwaarde heeft. Zo ja, op welke wijze dit dan het beste uitgevoerd kan worden.

4) Ontwikkelpaden en carrièreperspectief

Naast het vergroten van de deelname aan bij-, na- en omscholingsaanbod, kan het inzichtelijk maken en ontsluiten van ontwikkelpaden en het bieden van carrièreperspectief op landelijk, regionaal en lokaal niveau een bijdrage leveren. Voor afgestudeerden van het mbo en hoger onderwijs biedt dit de mogelijkheid om middels een helder pad door te groeien en verder te ontwikkelen (incl. softskills) binnen cybersecurity. Hierdoor kan meer perspectief zichtbaar geboden worden en de verticale doorstroom vergroot worden.

Het inzichtelijk maken van ontwikkelpaden kan tevens de horizontale doorstroom stimuleren door de relatie en doorstroom tussen beroepen in kaart te brengen. Belangrijk hierbij is het redeneren vanuit een startberoep ("wat doet iemand nu?") en het beroep van bestemming ("waar ga ik heen?"). Vanuit beide startpunten kan vertrokken worden. Vanuit het startberoep worden logische paden naar de plek van bestemming beschreven. Vanuit het bestemmingsberoep kan bekeken worden vanuit welke groepen mensen aangetrokken kunnen worden, ook met het oog op het vergroten van de diversiteit.

De ontwikkelpaden kunnen starten met een competentiescan: het (door)ontwikkelen en uitrollen van vaardigheidsscans om (snel) inzichtelijk te krijgen welke kennis en vaardigheden men al heeft en wat nog nodig is om de overstap naar een bepaald cybersecurity profiel te maken. Hierdoor komt er meer focus op competenties en competentieontwikkeling te liggen, dan sec op specifieke diploma's. Door minder te focussen op de traditionele diplomaniveaus vergroot je tevens de pool van mensen die zich tot cybersecurityspecialist kunnen ontwikkelen, waaronder mogelijk ook meer mbo-gediplomeerden.

5) Learning communities

Bij- en nascholingsaanbod kan op verschillende manieren aangeboden worden. De vele nieuwe ontwikkelingen in het vakgebied vragen echter om regelmatige actualisatie van kennis en vaardigheden. Middels leergemeenschappen (learning communities) kunnen bedrijven, kennisinstellingen en onderzoekers samen leren. Deze learning communities worden momenteel bijvoorbeeld via het Centrum voor Veiligheid en Digitalisering (CVD) uitgevoerd voor het mkb[6]. Advies is dan ook om ook bij Leven Lang Ontwikkelen op regionaal en lokaal niveau een zo gevarieerd mogelijk aanbod te hebben, op basis van good practices zoals de learning communities voor het mkb.

Hierbij willen we adviseren om voldoende oog te houden voor verschillende doelgroepen, omdat verschillende typen organisaties op een andere manier te maken hebben met cybersecurity. Zo variëren uitdagingen onder meer tussen de rollen die partijen hebben in de 'cybersecurity-waardeketen' (R&D, productie, integratie, eindgebruik), de sector waar de organisatie in actief is en de omvang van de organisatie. Alle partijen op één hoop gooien brengt het risico met zich mee dat er te weinig gemene delers zijn om effectief van elkaar te kunnen leren en elkaar gericht op weg te helpen.

6) Opschaling instrumentarium

Bovenstaande advies gaat in op het vergroten van de diversiteit van het Leven Lang Ontwikkelen aanbod, op basis van good practices en passend bij de vraag. Het huidige instrumentarium aan aanbod dient, waar relevant voor cybersecurity, verder opgeschaald en regionaal/ lokaal ontsloten te worden.

Verken welke good practices op welke manier opgeschaald kunnen worden en zet (indien opschaalbaar) regionale ecosystemen, zoals bijvoorbeeld publiek-private samenwerkingen (zoals bijv. HSD en CVD), het ecosysteem van het HCA- ICT netwerk, etc. in zodat goed werkende mechanismen zo optimaal mogelijk ingezet worden.

7) Traineeships

Om de verticale ontwikkeling tot cyberspecialist te stimuleren en net afgestudeerden aan te trekken of te behouden voor de cybersecuritysector kan regionaal ingezet worden op traineeships. In samenwerking tussen onderwijs en bedrijfsleven krijgen net afgestudeerden de mogelijkheid om zich verder te ontwikkelen en de mogelijkheden binnen de arbeidsmarkt te verkennen. Door regionaal de mogelijkheid te ontsluiten om ervaring op te doen bij verschillende bedrijven is de verwachting dat junior cybersecurity medewerkers beter behouden blijven voor de sector en de regio.

8) Niet- werkenden

Naast het stimuleren van horizontale en verticale ontwikkeling voor werkenden, is er ook een groep niet- werkenden die mogelijk als cybersecurityprofessional aan de slag kan gaan. Regionaal dienen de mogelijkheden verkend te worden, in samenwerking met bedrijfsleven, onderwijs en maatschappelijke partners (UWV, gemeenten, regionale tafels, sociaal domein, etc.), van omscholingstrajecten specifiek voor het cybersecuritydomein. Maatschappelijke partners kunnen kandidaten identificeren, aanbod ontsluiten en begeleiden. Het onderwijs kan deze trajecten aanbieden en samen met bedrijven en maatschappelijke partners de medewerkers begeleiden. Hierbij dient wel rekening gehouden te worden met de eisen en wensen die de arbeidsmarkt stelt aan desbetreffende functies (zie ook het onderzoeksrapport).

6. https://www.cvdnederland.nl/

4.3. Werk aan behoud van professionals met behulp van arbeidsmobiliteit binnen de sector

In het onderzoeksrapport is beschreven hoe er in 2021 er een uitstroom van bijna 25% van de populatie te zien is. Ongeveer 2% van de uitstromers ging dat jaar met pensioen en nog eens ongeveer 2% emigreerde.
Om de uitstroom te verminderen en meer mensen te behouden voor de cybersecurity-sector is het belangrijk om de arbeidsmobiliteit binnen de sector te stimuleren. Een regionale en lokale infrastructuur en het benutten van dit netwerk, behoudt professionals meer voor de sector èn de regio. Binnen deze samenwerking kan bijvoorbeeld gewerkt worden met deelcontracten, of het inzetten van 1 CISO voor meerdere organisaties. Voor cybersecurityprofessionals kan het dan aantrekkelijker zijn om te blijven binnen de sector, gezien de diversiteit en afwisseling van verschillende werkplekken.

4.4. Verbeter de startpositie van net afgestudeerden

In het onderzoeksrapport is gekeken naar de vraag op de arbeidsmarkt naar juniorfuncties en de aansluiting met de opleidingen. Hierbij is zowel de kwalitatieve als de kwantitatieve aansluiting van de instroom van afgestudeerden op de arbeidsmarkt onderzocht. Met het huidige tekort aan arbeidskrachten is het van belang om het potentieel van alle afgestudeerde studenten te benutten.

Om de startpositie van net afgestudeerden te verbeteren is dan ook raadzaam om de overstap van onderwijs naar arbeidsmarkt te begeleiden. Middels regionale en lokale programma's die in samenwerking met onderwijs en arbeidsmarkt worden ontwikkeld en uitgevoerd, krijgen starters op de arbeidsmarkt een stevige start.

In een 10-jarig onderzoek[7] uitgevoerd via Tech Your Future komt naar voren dat jongeren van werkgevers in de technische sector onder andere verwachten dat er 1) samen een concreet plan opgesteld wordt voor 2-3 jaar met interne loopbaan- en ontwikkelkansen, uitdaging en afwisseling en; 2) goede begeleiding door een mentor gegeven wordt. Talentontwikkelingsprogramma's, het aanbieden van leerwerkplekken, de eerder genoemde traineeships, maar ook het Dienjaar van Defensie zijn voorbeelden van programma's die ingezet kunnen worden om de startpositie van net afgestudeerden te vergroten.

7. https://wp.kennisbanksocialeinnovatie.nl/wp-content/uploads/2022/04/Technischtalent.pdf

5. Advies Onderwijs

In dit hoofdstuk worden de aanbevelingen 8 t/m 12 uit hoofdstuk 2 uitgewerkt. Daarmee zijn nog lang niet alle tekorten opgelost, het krapteprobleem overstijgt immers de reikwijdte van het initieel onderwijs. De aanbevolen acties in dit hoofdstuk leveren met name een bijdrage aan het verbeteren van de aansluiting tussen de vraag en aanbod naar juniorfuncties op de arbeidsmarkt.

5.1. Vergroot de interesse voor studeren en werken in cybersecurity

Om de aandacht voor digitale geletterdheid in het basis- en voortgezet onderwijs te versterken, is het wenselijk dat cybersecurity een vanzelfsprekend onderdeel wordt van het onderwijs in digitale vaardigheden. De uitdaging is om dit in een onderwijssysteem voor elkaar te krijgen waar onderwijsinstellingen veel autonomie hebben en er tegelijkertijd qua maatschappelijke vraagstukken veel op het bordje van het onderwijs wordt gelegd. In het Primair Onderwijs bijvoorbeeld wordt de afgelopen jaren meer de focus gelegd op basisvaardigheden als taal en rekenen.

De HCA ICT echter blijft aandacht vragen voor digitale vaardigheden in het primair onderwijs al inzet is op het versterken van digitale vaardigheden. En voor het voortgezet onderwijs bepleit de HCA ICT om de keuze voor het vak informatica te stimuleren. Het ligt voor de hand om deze inspanningen van de HCA ICT te ondersteunen om ook cybersecurity op de kaart te zetten.

Interesse bij jonge mensen wordt ook vergroot door het werkveld van cybersecurity al vroeg zichtbaar te maken. Hiervoor kunnen cybersecuritybedrijven en scholen aansluiten bij Jet-Net. Binnen regionale netwerken werken bedrijven en scholen nauw samen om leerlingen de eindeloze mogelijkheden binnen de wereld van technologie, techniek en ICT te laten zien. Ook een mooi voorbeeld is het leerplatform Cyberexplorers in het Verenigd Koninkrijk dat inmiddels 2. 000 scholen, 2 500 leraren en 41.000 leerlingen (11- 14 jaar) heeft bereikt[8].

Als de studiekeuze voor het mbo en het ho in beeld komt is het van belang om de breedte van cybersecurity en de grote variatie in functies en expertise te laten zien. Het gaat niet enkel om de technische cybersecurityspecialisten en bijbehorende opleidingen, maar juist ook om bijvoorbeeld de juridisch-, management-, bedrijfskunde en bestuurskunde georiënteerde functies en opleidingen waar cyber een rol kan spelen. Cybersecurity moet van het stigma af dat het een '(extreem) technisch vakgebied' (verder) is. Juist de multidisciplinariteit moet zichtbaar gemaakt worden. Zo worden (toekomstige) studenten geënthousiasmeerd in plaats van dat zij cybersecurity als (onderdeel van hun) vakgebied onterecht naast zich neerleggen vanwege incomplete en/of onjuiste informatie. Loopbaanoriëntatie op cybersecurity wordt idealiter een logisch onderdeel van het studietraject. Door tijdens de opleidingen en met name aan het eind van de opleidingen (stage-) opdrachten te laten uitvoeren neemt de kans toe dat studenten als cybersecurity-professional aan de slag zullen gaan. Ook kan via nieuwe onderwijsconcepten mogelijk een extra doelgroep aan studenten worden geënthousiasmeerd voor cybersecurity. Zo blijken de principes (nadruk op ontwikkelen van leermindset, moeilijke projecten krijgen en die in stukjes ophakken, peer-to-peer learning) die bij CODAM worden gehanteerd heel goed te werken voor studenten die in het reguliere onderwijs hun draai niet goed vonden.

(In bijlage 7 en 8 worden nog meer voorbeelden gegeven van innovatieve onderwijstrajecten zowel specifiek voor cybersecurity als voor de ICT. Kernelement is veelal het bieden van levensechte opdrachten aan studenten).

De Nationale Cyber Workforce and Education Strategy van de Verenigde Staten bevat op bladzijde 19 een indeling van leerfasen specifiek voor cybersecurity die richting kan geven bij het bepalen wat op welk moment op welke manier aan leerlingen en studenten kan worden aangereikt.

Het breed tonen van cybersecurity in al haar facetten wordt versterkt door landelijke/gezamenlijke afstemming tussen onderwijsinstellingen. Door als één blok cybersecurity (nog verder) op de kaart te zetten kunnen scholieren en studenten beïnvloed worden in hun keuze, bijvoorbeeld wanneer ze bij open dagen van verschillende instellingen cybersecurity (op een eenduidige en herkenbare manier) geëtaleerd zien staan als belangrijk maatschappelijk en economisch thema. En daarbij tegelijk ook kennismaken met de breedte van cybersecurity, van de technologische innovaties door AI tot en met het maatschappelijk belang.

8. National Cyber_Strategy Progress Report 2022 -2023

Wij raden aan deze gezamenlijke cybersecurity-communicatie- en voorlichtingsaanpak in eerste instantie op te pakken met onderwijsinstellingen die hier open voor staan. Daarbij is het zaak de verbinding te zoeken met al lopende initiatieven die de aandacht voor techniek, technologie en ICT in het onderwijs versterken zoals Jet-Net, Sterk techniek Onderwijs, Nationale Cybersecurity Summer School van dycpher en de HCA ICT. Door het gezamenlijk op te pakken kunnen [1] schaalvoordelen gerealiseerd worden in termen van kosten, doordat bepaalde inspanningen maar één keer gedaan hoeven te worden (bijv. het opstellen van brochures, video's en ander materiaal), en kan [2] cybersecurity krachtiger als 'aantrekkelijk domein' op de kaart gezet worden aangezien zoveel partijen in gezamenlijkheid zich hier hard voor maken. Voor het effectief communiceren met jongeren kan ook gedacht worden aan het ontwikkelen van een tool zoals het mentalitymodel voor de techniek. Dit is een hulpmiddel om verschillende typen jongeren aan te spreken voor een opleiding of een loopbaan in de techniek.

5.2. Versterk de kaders en het materiaal voor cybersecurity-onderwijs

Momenteel is het helaas nog zo dat bijna alle middelbare scholieren hun schoolperiode afronden zonder een substantieel onderdeel digitale geletterdheid te hebben gehad. Voor het **primair onderwijs** zijn sinds vorig jaar inhoudslijnen voor digitale geletterdheid beschikbaar. Dit zijn handreikingen voor scholen over hoe hun curriculum in te richten. Voor het voorgezet onderwijs zijn er inhoudslijnen met aanbodsdoelen. Ook zijn er bij de SLO leermaterialen voor digitale geletterdheid in het voortgezet onderwijs te verkrijgen.

De vraag is of deze richtlijnen en handreikingen voldoende zijn om cybersecurity in de hoofden en harten van onze leerlingen te krijgen. Binnen deze inhoudslijnen is immers maar beperkt aandacht voor specifiek cybersecurity. Vandaar dat tijdens de stakeholder-workshop de roep klonk naar meer uitgewerkte kerndoelen en doorlopende leerlijnen/ curricula en onderwijsmateriaal voor **het funderend onderwijs**. Het ontwikkelen hiervan op landelijk niveau is zeker laaghangend fruit; een meer complex vraagstuk is wie dit gaat onderwijzen binnen de scholen. Er zal dus tegelijk nagedacht moeten worden over de vorm van het onderwijs en het professionaliseren van docenten zonder een ICT-achtergrond. Gelukkig is cybersecurity wel een thema dat heel geschikt is om in digitale vorm aan te bieden. Er kan gedacht worden aan online-leergangen zoals Elements of AI, een MOOC voor po- en vo leerlingen over kunstmatige intelligentie. Daarnaast kunnen landelijke of regionale challenges en hackathons georganiseerd worden.

In het **mbo** is voor de ICT-opleidingen in de kwalificatiedossiers vastgelegd wat mbo-studenten aan het eind van hun opleiding moeten kennen en kunnen. Dit wordt in samenwerking met het werkveld omschreven. Op basis van deze eisen stelt de mbo-opleiding onderwijsprogramma's en examens op.
Deze kwalificaties zijn recentelijk vernieuwd, waarbij cybersecurity een explicietere uitwerking heeft gekregen.
Wat meteen opvalt en ook in de lijn der verwachtingen ligt is dat er veel meer aandacht is voor cybersecurity. Zo is er een apart profieldeel binnen de opleiding ICT-system engineer.

Voor het hoger onderwijs is er een nationaal framework voor kennis en vaardigheden op het gebied van cybersecurity voor het hbo in ontwikkeling. Momenteel wordt door HBO-i (het samenwerkingsverband van ICT-opleidingen in het hoger beroepsonderwijs) gewerkt aan een IT security framework binnen de domeinbeschrijving of als addendum bij de domeinbeschrijving om de link tussen opleiding en bedrijfsleven te versterken.

In de Nationale Cyber Educatie Agenda van dcypher wordt aangeraden om een gids met de hoofdlijnen voor een cybersecurity curriculum aan onderwijsinstellingen beschikbaar te stellen (naar het voorbeeld van het Canadian Centre for Cyber Security). Dit bevordert het ontwikkelen en het afstemmen van curricula (mbo, hbo en wo).

Binnen het **hoger onderwijs** is het uitdagend om samenwerking op te tuigen tussen opleidingen en instellingen, terwijl dat nodig is wanneer het multidisciplinaire karakter van cybersecurity in een onderwijsprogramma gecombineerd dient te worden. Gezamenlijke kaders en inspanningen kunnen hier een oplossing bieden.

Tijdens de implementatieworkshop zijn de volgende suggesties verder ter sprake gekomen:

- Maak cybersecurity een verplicht onderdeel in alle HBO-ICT opleidingen. Een dergelijke eis is wel een uitdaging voor het onderwijs, aangezien de inhoud van cybersecurity razendsnel verandert. Betrokkenheid van het werkveld bij het onderwijs is daarom onontbeerlijk.

- Stel voor het wetenschappelijk onderwijs een pool van hoogleraren aan. Deze hoogleraren krijgen gezamenlijk de opdracht om voor een dekkend onderwijsaanbod te zorgen. Dit zorgt voor het doorbreken van silo's tussen universiteiten.
- Ontwikkel gezamenlijk/ landelijk beter en tegen minder kosten curriculummateriaal. ICT-studies lenen zich daarbij goed voor zelfstudie, zo zijn minder docenten nodig. Docenten kunnen dan vooral ingezet worden voor het coachen en begeleiden. Een optie is om Cyber Security Special Interest Group (SIG CS) te vragen om een nationaal bachelor curriculum cybersecurity in te richten met natuurlijk nog de nodige ruimte voor regionale accenten. Dit netwerk omvat alle Nederlandse academische instellingen waar cybersecurity vanuit een computerwetenschappelijk perspectief wordt uitgevoerd.
- Ook voor mbo- en hbo zijn landelijke/regionale challenges en hackathons (net als voor leerlingen in het funderend onderwijs) een aantrekkelijke en goed op te schalen onderwijsvorm.
- Het verder uitrollen van cybersecurity-opleidingsaanbod in aanpalende opleidingen. Cybersecurity kan bij een bredere groep studenten, waarbij cybersecurity niet de kern van de opleiding is maar wel relevant voor het vakgebied (in de toekomst), onderwezen worden. Op deze manier kan cybersecurity bijvoorbeeld ook meer aandacht krijgen bij managementopleidingen, juridische opleidingen, e.d. Dit zijn ook opleidingen waarvan afgestudeerden als cybersecurity-professional aan de slag zouden kunnen gaan, al dan niet met extra bijscholing en ontwikkeling.
- Creëer doorlopende leerlijnen mbo- hbo, zodat de mbo- ICT-opleidingen als vooropleiding voor cybersecurity-specialist kunnen fungeren. Er zijn al een aantal Associate degree opleidingen, maar dit zou breder navolging kunnen krijgen. Eerste stap hierin is dat er een overzicht is van deze voorbeelden en dit gericht verspreid wordt onder de ICT-opleidingen van mbo en hbo.

5.3. Betrek de arbeidsmarkt sterker in het onderwijs

Het bouwen van een community rondom cybersecurity in de regio biedt de beste uitvalsbasis om een aantal vraagstukken tegelijk te tackelen. Onderwijsinstellingen, bedrijven en ook regionale overheden kunnen daar gezamenlijk:

- Het docententekort aanpakken (samen docenten werven, opleiden en delen).
- De aansluiting tussen onderwijs en bedrijven versterken (zorgen dat studenten met actuele vaardigheden van de opleiding komen).
- Contextrijke leeromgevingen voor het onderwijs inrichten (bijvoorbeeld door opdrachten van bedrijven te integreren in het onderwijs, leren op de werkplek).
- Flexibeler opleiden in het mbo en het ho (door deeltijdopleidingen, hybride opleidingen, modulair opleiden, microcredentials) en daarmee grotere groep studenten te bereiken.
- Aan promotie doen van het leren en werken in cybersecurity.

Voor het mbo kan bijvoorbeeld een aanvraag worden gedaan bij het Regionaal Investeringsfonds mbo om bovenstaande doelstellingen te realiseren.

Zo'n regionale community kan uiteraard tegelijk allerlei arbeidsmarkt-en innovatie-vraagstukken oppakken, bijvoorbeeld werken aan zij-instroomarrangementen, learning communities inrichten en ondersteunen van het mkb. Wat daarbij helpt is om een geografisch overzicht samen te stellen van waar welke opleidingen, initiatieven, kennisbronnen etc. zitten zodat men elkaar in de regio maar ook bovenregionaal weet te vinden (naar voorbeeld van de netwerkkaart van de HCA ICT). Voorbeelden van (boven-)regionale communities in Nederland zijn de HSD en de CVD.

En ter inspiratie: op bladzijde 16 van de National Cyber Workforce and Education Strategy van de Verenigde Staten worden 10 ecosystemen op het gebied van Educatie en Human Capital ontwikkeling gepresenteerd.

5.4. Versterk en vergroot de aantrekkelijkheid van het docentschap

Ten eerste moet **behoud en het zo optimaal mogelijk inzetten** van degenen die al als docent cybersecurity werkzaam zijn worden nagestreefd. Binnen een regionaal ecosysteem dienen onderwijs, bedrijven en Rijksoverheid de handen ineen te slaan om voor voldoende docenten te zorgen. Dit kan in de vorm van het aanbieden van hybride functies: een pakket van een docentaanstelling én een dienstverband bij een bedrijf of ruimte om zelfstandig ondernemer te zijn of te blijven in de cybersecurity. Hierbij kan voortgebouwd worden op eerdere ervaringen met hybride docentschap. Ook kan dit in de vorm van PhD-kandidaten die door een universiteit en een bedrijf gezamenlijk aangesteld worden en die naast onderzoek ook onderwijstaken heeft.

Ten tweede ligt grote inzet op bij- en nascholing voor de hand. Denk hierbij aan maatregelen als:

- Subsidie voor bij- en nascholing van docenten op gebieden met raakvlakken met cybersecurity om de kwaliteit van het onderwijs te verbeteren. Uiteraard gaat dit om ICT-docenten, maar ook om docenten in andere domeinen zoals bijvoorbeeld security, management en organisatie, rechten en bestuurskunde.
- Docentstages, waarbij docenten een tijdje bij een bedrijf meelopen, zijn ook een heel effectief middel om docenten bij te scholen. Stimuleer daarom in het regionale ecosysteem samenwerking tussen onderwijs en bedrijven bij het inrichten van deze stages.
- Daarnaast is het op landelijk niveau ontwikkelen van masterclasses voor docenten in cybersecurity laaghangend fruit. Voor de ICT-docenten in het mbo was dit in het recente verleden al gangbaar en kan dit voor cybersecurity weer opgepakt worden.
- Vanwege de nijpende tekorten moet omscholing naar docent cybersecurity zo laagdrempelig mogelijk worden ingericht. Make IT Work is een voorbeeld van een omscholingspropositie die vanwege baangarantie, een versneld traject en een beperkte bijdrage aan de opleidingskosten voor de omscholer aantrekkelijk is. Gekeken zou kunnen worden naar of deze elementen meegenomen kunnen worden in specifieke arrangementen voor cybersecurity -docenten bij de lerarenopleiding Informatica (voor docenten in het voortgezet onderwijs), een pdg-traject (voor docenten in het mbo) of BDB-traject (voor docenten in het hbo).

6. Wie is er aan zet?

6.1. Hoe ziet de ontwikkeling, uitvoering en het toezicht op deze adviezen op landelijk, regionaal en lokaal niveau eruit?

In voorgaande hoofdstukken zijn de verschillende aanbevelingen beschreven op het gebied van en op het gehele ecosysteem, arbeidsmarkt en onderwijs. Om te komen tot een samenhangende aanpak van de adviezen dienen we per niveau te bekijken wie op welk niveau opereert. Tabel 2 geeft een beeld van de verschillende partijen die op de betreffende niveaus betrokken kunnen worden bij de uitvoer van de adviezen. Deze lijst biedt een indicatie om de verschillende niveaus en de partijen te duiden en is niet volledig.

	Overheid	Onderwijs	Bedrijfsleven	Overig
Landelijk	Ministeries: EZK, OCW, SZW, J&V Interdepartementale overleggen (DOCS, IOCS) Anders: CBS, UWV, NWO, NEXIS	PO- raad, VO- raad, mbo- raad, Vereniging Hogescholen, UNL, ACCSS	VNO_NCW, MKB- Nederland, brancheverenigingen, Cyberveilig Nederland, CCoT	CSR, dcypher, NCTV, NCSC, PTvT
Regionaal	Provincies, ROM's, RMT's	Onderwijsinstellingen mbo, hbo, wo	Ondernemingsverenigingen	Initiatieven rondom cyber, zie regioscan digitalisering mkb, HSD, CVD, DTC
Lokaal	Gemeenten	Onderwijsinstellingen po, vo	Individuele bedrijven	

Tabel 2: overzicht van betrokken partijen op landelijk, regionaal en lokaal niveau.

In de beschrijving per aanbeveling staat vermeld op welk niveau en met welke typen partijen deze uitgevoerd zou kunnen worden. Een totaaloverzicht van de aanbevelingen, gekoppeld aan de typen partijen die logischerwijs bij de uitvoer betrokken moeten/kunnen zijn, is te vinden in Bijlage 1.

Op het gebied van Human Capital cybersecurity zijn veel initiatieven (deels) betrokken. De afgelopen maanden blijkt uit de vele gesprekken, dat het vooral ontbreekt aan de verbinding van deze initiatieven en de coördinatie ervan waardoor het aan slagkracht ontbreekt. Bij het vertalen van de adviezen uit dit rapport benadrukken we dat het startpunt eerst de huidige relevante beleids- en actieplannen, regelingen, programma's en samenwerkingen moet zijn. In Bijlage 5 is een overzicht opgenomen van de relevante beleids- en actieplannen en agenda's. Bijlage 6 laat een aantal regelingen en programma's zien waarbij aangesloten kan worden in de uitvoering. Gedurende het onderzoek zijn ook kansrijke concepten voor cybersecurity (Bijlage 7) en kansrijke voorbeelden in de IT sector (Bijlage 8) verzameld.

6.2. Wanneer moet dit aangepakt worden? Een beschrijving van de eerste stappen en volgordelijkheid

In de voorgaande hoofdstukken beschreven we het belang van de samenwerking tussen alle betrokken partijen en de coördinatie van alle acties, gezien de breedte en complexiteit van het cybersecurityveld. Om beleidscoördinatiefalen te voorkomen, is er in onze optiek ook specifiek aandacht nodig voor beleidscoördinatie op dit deelthema 'Human Capital' om daadwerkelijk het aantal professionals en de benodigde expertise te vergroten. Voor gewenste uit te voeren acties en interventies is het onder meer van belang dat [1] deze acties uitgevoerd worden ('voorkomen hiaten'), [2] deze acties niet dubbel uitgevoerd worden ('overlap en beleidsconcurrentie') en [3] dat deze acties waar mogelijk door partijen uitgevoerd worden die hier doeltreffend en doelmatig invulling aan kunnen geven. Hieronder volgt een beschrijven van hoe de opvolging van de adviezen vormgegeven zou kunnen worden. Dit is schematisch weergegeven in Figuur 3.

De opvolging van de genoemde adviezen uit dit rapport starten ons inziens bij de Rijksoverheid, als start van de algemene coördinatie. Zowel het onderzoeks- als het adviesrapport dienen ingediend en besproken te worden bij de betreffende ministeries in de verschillende inter- en departementale overleggen. Om beleidscoördinatiefalen te voorkomen, is het belangrijk om een duidelijke partij te benoemen met voldoende mandaat, positie en middelen, die verantwoordelijk is voor de coördinatie en verdere opvolging van deze adviezen. Gezien het inhoudelijke karakter van de adviezen kan dit bijvoorbeeld bij het Ministerie van Economische Zaken en Klimaat of het Ministerie van Onderwijs, Cultuur en Wetenschap komen te liggen.

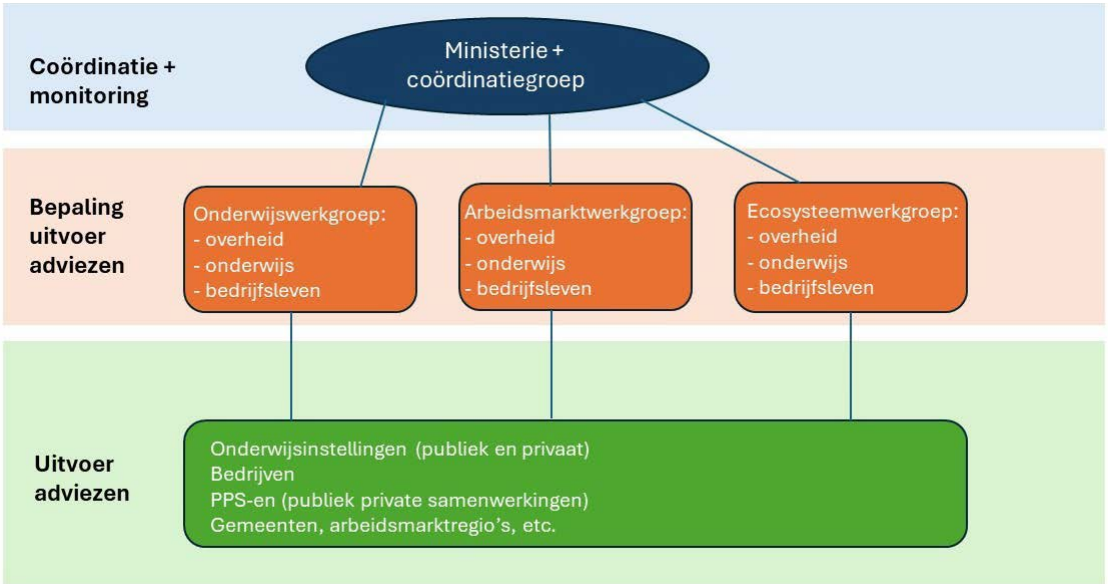
Het Ministerie dat de opvolging van de adviezen op zich neemt zal een coördinatiegroep aanwijzen, waarin Rijksoverheid, onderwijs en bedrijfsleven vertegenwoordigd zijn. Deze coördinatiegroep dient het totaal aan adviezen te overzien en de samenhang te bewaken.

Vanuit ieder betrokken Ministerie kan vervolgens besproken worden welke adviezen passend zijn om in uitvoering te nemen via de huidige infrastructuur, programma's en regelingen (Bijlage 6) en/of middels opschaling/ uitbreiding van bestaande programma's en initiatieven (Bijlage 7 en 8).

De adviezen binnen de deelgebieden onderwijs, arbeidsmarkt en ecosysteem zouden vervolgens het best besproken kunnen worden in heterogene werkgroepen waarin Rijksoverheid (incl. het betrokken Ministerie), onderwijs, bedrijfsleven en de betreffende overige partijen (zie Tabel 2) plaatsnemen. Binnen deze werkgroepen worden de adviezen besproken en wordt de verdere aanpak bepaald. Hierbij is het van belang het juiste aggregatieniveau te kiezen: zo diep als nodig, maar zo hoog als mogelijk en altijd zoveel mogelijk aansluitend bij de bestaande gremia, rollen en verantwoordelijkheden.

Een goede verbinding tussen de landelijke, regionale en lokale aanpak is essentieel. De werkgroepen rapporteren o.a. de aanpak, uitvoering, knelpunten en resultaten aan de coördinatiegroep. Deze bewaakt de voortgang en onderlinge samenhang en adviseert de werkgroepen met betrekking tot de opvolging en uitvoering van de adviezen.

Naast deze algemene opzet van de coördinatie kan/moet voor specifieke individuele adviezen de aansluiting gezocht worden met andere bestaande gremia. Zo ligt het voor de hand om ten aanzien van de sectoroverstijgende samenwerking m.b.t. het borgen van cybersecurity in waardeketens de samenwerking (en uitvoering) te zoeken bij de Topsectoren.
Bovenstaande opzet en structuur zal vooral daadkrachtig zijn door meer centrale overheidsregie met de benodigde mandaat om de opvolging van de adviezen daadwerkelijk te realiseren.



Figuur 4: Mogelijke structuur opvolging adviezen

Dankwoord

Gedurende dit onderzoekstraject zijn in de periode van september 2023 tot en met februari 2024 de aanpak en inzichten met regelmaat getoetst middels gesprekken en workshops. Partners in het onderwijs, bedrijfsleven en partners die huidige activiteiten en inspanningen verrichten ten behoeve van Human Capital beleid voor cybersecurity hebben hieraan bijgedragen.
De adviezen zoals beschreven in dit Adviesrapport zijn opgehaald bij deze partners in verschillende bijeenkomsten.

Eenieder die hieraan bijgedragen heeft willen wij hartelijk danken. Jullie input en inspanningen hebben bijgedragen aan een overzicht van de huidige stand van zaken, aan een methodiekontwikkeling om de onderwijs- en arbeidsmarkt voor cybersecurity verder te volgen in de toekomst en aan een veelheid van adviezen die op nationaal, regionaal en lokaal niveau besproken en uitgevoerd kunnen worden. We hopen dat de concrete uitvoering op net zoveel bijdrage mag rekenen, zodat er samengewerkt wordt aan een toekomstbestendig Human Capital-beleid voor cybersecurity.

Met als resultaat: voldoende goed geschoolde cybersecurity professionals met de juiste expertise die in Nederland en de EU werken aan een digitaal veilige samenleving.

Contactinformatie

Sonja Kleter, Dialogic
Manon Schrijnemaekers, PTvT
Marion Sieh, PTvT
Arthur Vankan, Dialogic
Loes Willems, PTvT

Contactpersonen:
Contactpersoon Platform Talent voor Technologie:
Marion Sieh
m.sieh@ptvt.nl

Contactpersoon Dialogic:
Arthur Vankan
vankan@dialogic.nl

Postadres:
Platform Talent voor Technologie
Postbus 76
2501 CB Den Haag

Bezoekadres:
Oranjebuitensingel 6 (4e etage)
2511 VE Den Haag

©PTvT, januari 2024

Bijlage 1. Methodologie adviesrapport

1.1. Inleiding

De separaat opgeleverde onderzoeksrapportage biedt een rijk beeld van de inzichten over de mate waarin cybersecurity onderwijs en arbeidsmarkt op elkaar aansluiten en welke bewegingen te zien zijn op de arbeidsmarkt. Deze informatie biedt een goed overzicht van de afgelopen vijf jaren en de huidige situatie en is daarmee een belangrijk vertrekpunt voor verdere beleidsadviezen. In deze bijlage wordt beschreven hoe het advies gestructureerd is (het gebruikte kader) en hoe de adviezen tot stand zijn gekomen.

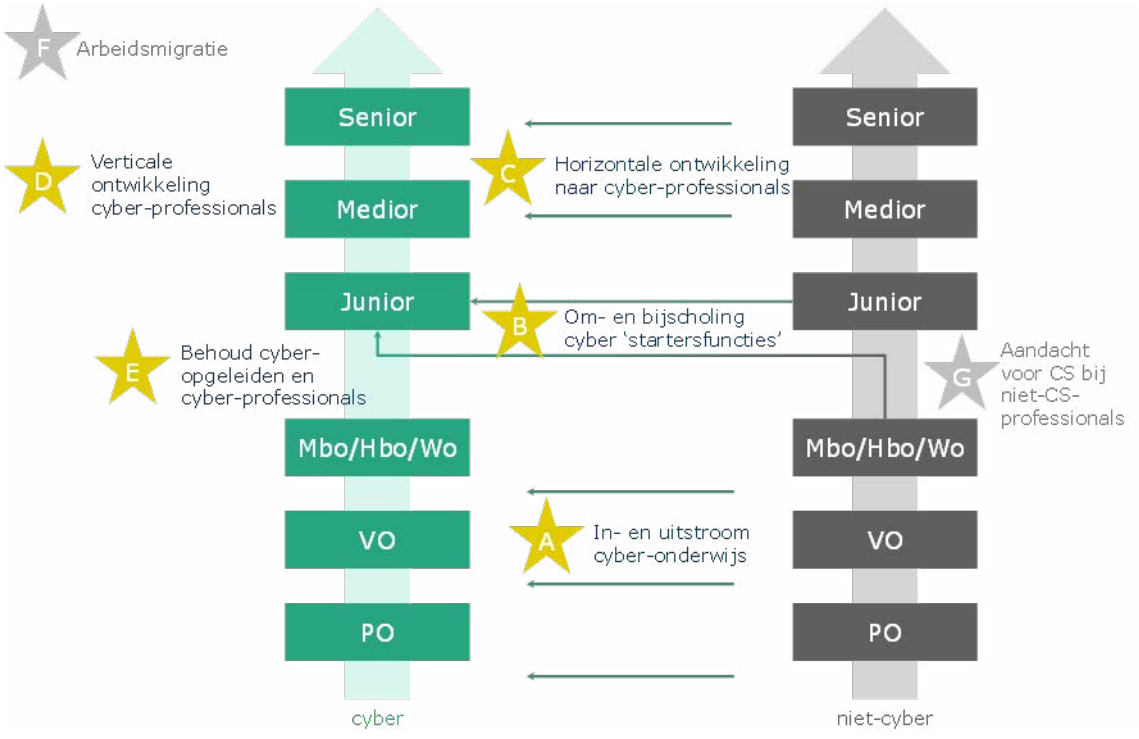
1.2. Aanpak en conceptueel kader voor advies

1.2.1. Bijeenkomsten en gesprekken

Tijdens bijeenkomsten in januari en februari 2024 is er met stakeholders vanuit onderwijs, bedrijfsleven en het Human Capital ecosysteem, besproken welke (beleids-) instrumenten er op basis van het onderzoek ingezet kunnen worden en op welke manier en op welk niveau deze uitgevoerd dienen te worden. Op 17 januari 2024 is er gestart met een bijeenkomst waarbij meer dan 40 genodigden met diverse expertise en achtergronden hebben meegedacht aan de vertaling van de bevindingen richting adviezen. Hierbij is getracht zoveel mogelijk diverse perspectieven mee te nemen door 1) medewerkers van de diverse betrokken Ministeries uit te nodigen, 2) (vertegenwoordigers van) groot, midden en klein bedrijf, 3) medewerkers (o.a. hoogleraren, lectoren, docenten) van mbo, hbo en wo onderwijsinstellingen, 4) publiek private samenwerkingen en 5) uitvoeringsorganisaties van (Human Capital) beleid.
Door de adviezen die tijdens deze bijeenkomst zijn opgehaald, vervolgens te toetsen en aan te scherpen tijdens diverse andere bijeenkomsten en gesprekken met medewerkers van onderwijsinstellingen, bedrijfsleven en (regionale) samenwerkingsverbanden, is getracht een zo volledig mogelijk advies op te stellen dat gedragen wordt door diverse partijen.

1.2.2. Conceptueel kader voor advies

Om alle opgehaalde input te structureren maken we, zoals toegelicht in de onderzoeksrapportage, gebruik van onderstaand conceptueel kader (Figuur 2) dat een beeld geeft van de totale onderwijs- arbeidsmarkt keten. Hoewel het kader een versimpelde weergave van de complexe werkelijkheid is, biedt het de mogelijkheid om gestructureerd te kijken naar de drie typen stromen (instroom, doorstroom, en uitstroom) die aan de basis liggen van het aantal cybersecurity-professionals binnen Nederland.



Figuur 2: Conceptueel kader dat een beeld geeft van de totale onderwijs- arbeidsmarkt keten

De belangrijkste onderdelen in dit kader om aandacht aan te besteden zijn:

A. **In- en uitstroom in het cyber-onderwijs:** wat kunnen we doen om meer leerlingen te interesseren voor een opleiding op het gebied van cybersecurity en studenten de juiste skills en kennis mee te geven zodat ze worden opgeleid passend bij de vraag naar (junior)functies op de arbeidsmarkt?
B. **Om- en bijscholing cyber 'startersfuncties':** wat kunnen we doen om net afgestudeerden van een niet-cyber gerelateerde opleiding om en bij te scholen zodat ze beschikbaar zijn voor een cyberfunctie? Met welke opleidingsachtergrond is dit het meest kansrijk? En kunnen we mensen in een starters-/juniorfunctie op de arbeidsmarkt interesseren om een overstap naar cybersecurity te maken?
C. **Horizontale ontwikkeling naar cyber-professionals:** hoe kunnen we medior- en senior professionals in een niet cyberfunctie om- en bijscholen naar een cyberfunctie? Bij welke functies is dit het meest kansrijk en wat is hiervoor nodig?
D. **Verticale ontwikkeling cyber-professionals:** hoe kunnen we de keten van junior-, naar medior- naar seniorfuncties zo goed mogelijk laten doorstromen zodat professionals doorgroeien en ruimte ontstaat in het begin van de keten?
E. **Behouden cyber-opgeleiden en cyber-professionals:** wat is er nodig om de uitstroom van cyberprofessionals uit de sector zo klein mogelijk te houden en professionals te behouden voor de cybersecurity-arbeidsmarkt?
F. **Arbeidsmigratie:** hoeveel cyberprofessionals komen vanuit het buitenland in NL werken? Maar ook hoeveel cyberprofessionals uit Nederland verlaten NL om in het buitenland te gaan werken? Wat kunnen en willen we met de relatief grote internationale instroom op de cybersecurity-arbeidsmarkt?
G. **Aandacht voor cybersecurity bij niet-cybersecurity-professionals:** hoeveel aandacht voor cybersecurity is er bij niet-cybersecurity-professionals? Kunnen we dit vergroten en wat betekent dat voor de totale arbeidsmarktketen?

1.3. Methode verwerking suggesties en ideeën tot advies

We hebben bovenstaande onderdelen met diverse stakeholders besproken tijdens gemeenschappelijke en individuele bijeenkomsten. Samen met de onderzoeksresultaten uit de eerste fase zijn er op deze onderdelen concrete ideeën en suggesties geformuleerd die moeten bijdragen aan [1] de instroom van cybersecurity-professionals, [2] de doorstroom van cybersecurity-professionals en [3] het beperken van (ongewenste) uitstroom van cybersecurity-professionals.

Deze suggesties en ideeën hebben we vertaald naar concrete acties. Deze acties zijn gestructureerd aan de hand van een viertal dimensies:

1. Op welke onderdelen van figuur 1 heeft het advies betrekking? (A t/m G)
2. Op welke schaalniveaus van beleid moet het advies opgepakt worden? (landelijk, regionaal, lokaal)
3. Welke typen partijen zijn primair aan zet voor het opvolgen van het advies? (Rijksoverheid, onderwijs, bedrijfsleven, overig).
4. Een cluster en subcluster waar de actie toe behoort, om de variëteit aan acties te kunnen voorzien van structuur.

Deze acties met bovenstaande dimensies zijn verwerkt in een Excel bestand. Door te categoriseren langs de dimensies zijn de acties vertaald naar 12 aanbevelingen, zoals beschreven in Hoofdstuk 2. Hoofdstuk 3, 4 en beschrijft per aanbeveling de bijbehorende acties voor het gehele ecosysteem, de arbeidsmarkt en het onderwijs.

Bijlage 2. Internationale voorbeelden

In dit hoofdstuk lichten we ter illustratie drie voorbeelden uit van het Human Capital beleid voor cybersecurity. De planvorming van het Verenigd Koninkrijk focust zich op het Verenigd Koninkrijk als leidende kracht op het gebied van cybersecurity in de toekomstige wereld, terwijl het plan van de Verenigde Staten van Amerika zich specifiek richt op Human Capital en het onderwijs rondom cybersecurity. De beleidsadviezen op EU niveau bieden mogelijkheden om de Nederlandse adviezen aan te verbinden. De voorbeelden worden hieronder toegelicht ter inspiratie voor de aanpak en de inhoud van Human Capital beleidsinstrumenten.

2.1. Beleidsstrategieën cybersecurity in het Verenigd Koninkrijk

De afgelopen jaren heeft het Verenigd Koninkrijk twee uitgebreide plannen uitgebracht rondom hun cybersecurity doelstellingen: National Cyber Security Strategy over de periode 2016- 2021 en de periode 2022-2025. Gezien de nauwe verwantschap tussen de twee plannen, beschrijven we beide met de focus op Human Capital beleid.

1. NATIONAL CYBERSECURITY STRATEGY 2016 – 2021

De National Cyber Security Strategy 2016-2021 focust zich op drie primaire doelstellingen: verdedigen, afschrikken en ontwikkelen. Ontwikkelen gaat over een duurzame aanvoer van Human Capital met cybersecurity talent van eigen bodem. Dit pakt het Verenigd Koninkrijk aan door:

a) Opzetten van een skills adviesgroep met leden vanuit Rijksoverheid, industrie en kennisinstelling die zich richt op het specificeren van cyber security skills, integreren van deze skills in het onderwijssysteem, waarbij minimaal in de opleidingen Computer Science, Computer Technology, en Digital Skills de fundamenten van cybersecurity onderwezen worden.

b) Investeren in initiatieven die tot directe verbetering van de Human Capital leiden, danwel tot het ontwikkelen van een lange termijn strategie. Voorbeelden hiervan zijn:
   (1) opzetten van een educatie programma om stapsgewijs verandering teweeg te brengen in gespecialiseerd cybersecurity onderwijs;
   (2) extra training voor 14-18 jarigen met talent;
   (3) cybersecurity opleidingsplaatsen creëren in energie/financiën/transport sectoren;
   (4) opzetten van een fonds om omscholingsinitiatieven naar cybersecurity te identificeren en op te schalen;
   (5) subsidiëren van accreditatie en professionele ontwikkeling van docenten;
   (6) opzetten van de Defence Cyber Academy waar hoogstaand cybersecuritytraining gegeven wordt voor defensie en Rijksoverheid
   (7) cybersecurity en digitale vaardigheden integraal onderdeel maken van de volledige leerlijn primair tot postacademisch onderwijs.

2. NATIONAL CYBERSECURITY STRATEGY 2022 - 2025

De National Cyber Security Strategy 2022-2025 focust zich meer op het Verenigd Koninkrijk als leidende kracht op het gebied van cybersecurity in de toekomstige wereld. Zij beogen dit te bereiken op basis van vijf pijlers waarvan met name de eerste, Versterken van het cyber-ecosysteem, gericht is op het kwalitatief en kwantitatief verbeteren van de Human Capital.

Specifieke acties om de Human Capital te verbeteren zijn:

- Opschalen en subsidiëren van 16+ training programma's, cybersecurity skills bootcamps, CyberFirst beurzen voor studenten.
- Nationale uitwerking van het curriculum van technologie-instituten.
- Bewerkstelligen van professionele standaarden en (om)scholingstrajecten tot een cybercarrière.
- Opschalen van diversiteit stimulerende initiatieven zoals de CyberFirst Girls competitie.
- National Centre for Computing Education faciliteert bijscholing van docenten.
- Investeren cybersecurity opleidingsplaatsen en skills programma voor de Rijksoverheid

2.2. Beleidsstrategie cybersecurity in de Verenigde Staten van Amerika

In 2023 hebben de Verenigde staten de National Cyber Workforce and Education Strategy uitgebracht. Dit is een plan om de Human Capital ontwikkeling en het cybersecurity onderwijs in de Verenigde Staten te verbeteren aan de hand van vier pilaren:

1. **Elke Amerikaan uitrusten met een cyber fundament**
   Cyber skills-onderwijs wordt toegankelijk gemaakt voor iedereen door het uitbreiden van aanbod, opschalen van bestaande initiatieven en tools, opzetten van open kennisnetwerken en integreren van cyber skills-onderwijs in de volledige leerlijn vanaf primair onderwijs. Daarnaast worden Amerikanen geïnspireerd hun cyber skills te vergroten of een cyber carrière te starten door awareness campagnes, uitvergroten van economische en maatschappelijke voordelen en het opzetten van Cyber Awards voor studenten met cyber skills.

2. **Veranderen van cybersecurity onderwijs**
   Ecosystemen rondom cybersecurity- onderwijs worden opgezet en opgeschaald, de betrokkenheid van bedrijven en organisaties (door o.a. bootcamps en hackatons) wordt vergroot en cyber-veilige leeromgevingen voor studenten worden gecreëerd. Er wordt geïnvesteerd in het uitbreiden van competentiegericht cybersecurity-onderwijs, cyber-lesmateriaal in interdisciplinaire opleidingsprogramma's, mogelijkheden voor behalen van certificaten en een systeem waarbij credits behaald kunnen worden die ook overdraagbaar zijn in verschillende leerfases (zoals highschool, universiteit, en extracurriculair verdiende credits). Ook wordt geïnvesteerd in het algemeen verbeteren van het cybercurriculum en docenten door faciliteren van flexibelere contract opties (zoals deeltijd of deelaanstelling), subsidiëren van cyberfaculteiten om curricula op te zetten, opzetten van fellowship programma's binnen publiek-private samenwerkingen, uitbreiden aantal inschrijvingen voor masteropleidingen verhogen door subsidies en scholarship programma's, en het opzetten en subsidiëren van cyber-award programma's voor scholen en docenten. Als laatste is er aandacht voor het opzetten van carrière programma's binnen ondervertegenwoordigde groepen.

3. **Kwantitatieve en kwalitatieve groei van Amerikaanse Human Capital**
   Er word onder andere gewerkt aan: 1) beter zicht krijgen op huidige Human Capital en beroepsclassificaties door ecosystemen; 2) opschalen van bijscholingsinitiatieven; 3) uitbreiden van goedkope of gratis bijscholingsmogelijkheden voor kleine bedrijven; 4) bijscholen en selecteren van personeel op basis van skills waaronder scholen van HR professionals om hierop te kunnen selecteren; 5) meer hands-on les binnen kennisinstellingen; 6) diversiteit stimuleren door subsidies gericht op ondervertegenwoordigde groepen, samenwerken met organisaties in regio's met veel ondervertegenwoordigde groepen, stimuleren van omscholing van veteranen tot cyberprofessionals en
   regels rondom immigratie opstellen om internationaal talent te kunnen rekruteren, en; 7) identificeren van internationale best practices voor toepassing binnen de Verenigde Staten.

4. **Versterken van Human Capital voor cybersecurity voor de Rijksoverheid**
   De Feder Cyber Workforce Working Group (FCWWG wordt opgezet. Deze coördineert verschillende acties om duurzame verbetering van cybersecurity Human Capital te bewerkstelligen, zoals: 1) definiëren van cyber rollen en verantwoordelijkheden en carrièrepaden; 2) opzetten van op skills gebaseerde selectie procedures inclusief trainen van HR professionals hierop; 3) opzetten van het scholarship programma CyberCorps Scholarship For Service; 4) opschalen van stages en leerwerkplekken; 5) switch tussen privaat en publieke organisaties makkelijker maken; 6) flexibele contracten zoals deeltijd en flexibele uren mogelijk maken.

2.3. Beleidsinitiatieven op EU niveau

In het onderzoek is gezocht naar EU programma's en regelingen die een link hebben met het Human Capital-vraagstuk cybersecurity. Hieruit kwamen de volgende EU platformen en initiatieven naar voren.

1. Cyber Skills Academy

De Cyber Skills Academy[9] is een Europees beleidsinitiatief dat onderdeel is van het Digital skills & jobs Europe[10] programma. De Cyber Skills Academy heeft tot doel bestaande initiatieven op het gebied van cybervaardigheden samen te brengen en hun coördinatie te verbeteren, met het oog op het dichten van het gat in het cybersecurity-talent en het stimuleren van de concurrentiekracht, groei en veerkracht van de EU.
Langs de volgende lijnen wordt hieraan gewerkt:

- Deskundigheidsbevordering en training: door middel van onderwijs en training, door een gemeenschappelijk EU-kader voor cybersecurity-rollen en bijbehorende vaardigheden vast te stellen. Dit omvat het verbeteren van het Europese onderwijs- en trainingsaanbod om aan de behoeften te voldoen, het ontwikkelen van loopbaanpaden en bieden van inzicht in en overzicht van cybersecurity-trainingen en certificeringen.
- Financiering en projecten: bieden van inzicht in en overzicht van beschikbare financieringsmogelijkheden en bestaande projecten voor vaardigheden-gerelateerde activiteiten om hun impact te maximaliseren.
- Stakeholderbetrokkenheid: mobilisatie van relevante partijen om de genderbalans in cybersecurity te verbeteren en specifieke maatregelen te nemen om het gat in cybersecurity-vaardigheden in nationale cybersecurity-strategieën aan te pakken.
- Voortgang meten: ontwikkelen van een methodologie om voortgang te meten in het dichten van het gat in cybersecurity-vaardigheden. Organisaties of personen die actief zijn op het gebied van cybervaardigheden worden aangemoedigd om hun eigen input te leveren.

2. Digital Europe Programme

Dit programma is een nieuw financieringsprogramma van de EU dat gericht is op het aanreiken van digitale technologie aan bedrijven, burgers en Rijksoverheidsdiensten om daarmee het economisch herstel en de digitale transitie te versnellen.
Er wordt subsidie verstrekt om vijf belangrijke capaciteitsgebieden te ondersteunen: op het gebied van supercomputing, kunstmatige intelligentie, cyberbeveiliging, geavanceerde digitale vaardigheden en het waarborgen van een breed gebruik van digitale technologieën in de hele economie en samenleving, onder meer via digitale-innovatiehubs.

Bovenstaande voorbeelden bieden inspiratie en binnen de EU concrete instrumenten om op aan te haken. Bijvoorbeeld is de Cyber Skills Academy niet alleen een platform om goede praktijken uit Nederland op het podium te zetten of om financiering voor doorontwikkeling te krijgen maar ook een vindplaats voor materiaal en goede voorbeelden uit andere landen. In Hoofdstuk 2 worden de aanbevelingen beschreven die, naar aanleiding van de uitkomsten van het onderwijs en arbeidsmarkt onderzoek, voor Nederland gelden.

9. https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy
10. https://digital-skills-jobs.europa.eu/en/about

3. ECSO (European Cybersecurity Organisation)

ECSO brengt Europese publieke en private cybersecurity partijen samen, vertegenwoordigt hen en bevordert hun samenwerking. De leden van ECSO zijn grote bedrijven, mkb, start-ups, onderzoekscentra, universiteiten, eindgebruikers en exploitanten van essentiële diensten, clusters en verenigingen, evenals lokale, regionale en nationale Rijksoverheidsinstanties in de lidstaten van de Europese Unie.
Binnen ECSO is de werkgroep Skills & Human Factors- Road2Cyber[11] actief op het gebied van Human Capital voor cybersecurity. Zo wordt gewerkt aan:

- Onderwijs: richtlijnen voor minimale curricula voor cybersecurity-cursussen voor universiteiten, hoger onderwijs en professionele opleidingsaanbieders, en samenwerking tussen industrie en academische wereld.
- Vaardigheden / HR: Ondersteuning voor HR, vaardigheidsverificatie en koppeling aan opleidingstrajecten, bijdrage aan het Europese Cybersecurityvaardighedenkader (ECSF) van ENISA, ontwikkeling van de Europese HR-gemeenschap, lancering van een toegewijd Europees platform voor cybersecuritybanen.
- Bewustwording / cyberhygiëne / genderdiversiteit / menselijke factoren: Initiatieven zoals Youth4Cyber en Women4Cyber, bewustwordingskalender, samenwerking met EU-instellingen en -agentschappen, en betrokkenheid van burgers.

Zo is er een Call Advanced Digital Skills[12] uitgezet voor consortia van ho- instellingen, beroepsopleidingen en trainingsinstellingen, onderzoeksorganisaties en bedrijven die geavanceerde digitale technologieprogramma's en multidisciplinaire cursussen aanbieden voor gebruikers van geavanceerde digitale technologieën om in onderlinge samenwerking onderwijsaanbod, faciliteiten, beurzen etc. te realiseren. Deze call sluit in maart 2024.

ESCO is een alliance partner van de The Hague Security Delta.

11. https://ecs-org.eu/activities/education-training-awareness-and-cyber-ranges/
12. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2023-skills-05-specialedu?tenders=false&callIdentifier=DIGITAL-2023-SKILLS-05

Bijlage 3. Rationale voor overheidsinterventie

Cyberveiligheid is een cruciaal element in het opbouwen en behouden van een veilige digitale samenleving. Het creëren van cyberveiligheid is weliswaar een gezamenlijke verantwoordelijkheid van private en publieke partijen, maar zonder overheidsinterventie zullen de doelen op het gebied van cyberveiligheid niet behaald worden.

Een belangrijke uitdaging binnen de transitie naar een cyberveilige samenleving is het ontwikkelen en behouden van voldoende cybersecurity-expertise. Hoewel we als Nederland veelvuldig inspanningen leveren om aan het Human Capital vraagstuk te werken, is de consensus bij de gesprekspartners dat aanvullende inspanningen nodig zijn om de gewenste cybersecurity-expertise nu en in de toekomst te realiseren. Het maatschappelijk-economische systeem is nog onvoldoende geëquipeerd op dit gebied wat in beleidsjargon beschreven kan worden met het zogenaamde systeemfalen 'capability failure'.[13]

Dit systeemfalen kent in de context van het voorliggende Human Capital vraagstuk een aantal meer specifieke en prominente marktfalen die gewenste ontwikkelingen in de weg kunnen staan. Hieronder beschrijven we een aantal belangrijke marktfalen binnen deze context:

- **Publiek goed**. De waarde van cyberveiligheid voor de maatschappij (en daarmee ook professionals die hier aan werken) kan niet altijd door bedrijven in de prijs van goederen en diensten verdisconteerd worden, waardoor deze waarde dus niet altijd door bedrijven toegeëigend kan worden. Dit fenomeen legitimeert Rijksoverheidsinterventie, o.a. in de vorm van het (deels) publiek bekostigen van benodigde inspanningen en het formuleren van wet-en regelgeving, kaders en richtlijnen.
- **Informatieasymmetrie en informatiegebreken**. Niet alle partijen hebben voldoende/volledig zicht op cybersecurity inclusief de bijbehorende kansen en risico's, waardoor gewenste (trans)acties op het gebied van cybersecurity niet tot stand komen. Dit onderliggende probleem legitimeert Rijksoverheidsinterventie, o.a. in de vorm van het faciliteren van activiteiten om de awareness te vergroten.
- **Positieve externaliteiten (spillovers)**. Organisaties kunnen niet altijd de volledige waarde van hun investeringen toe-eigenen. Dit speelt regelmatig op het gebied van innovatie en opleiding. Specifiek op het gebied van investeringen in na-, om- of bijscholing m.b.t. cybersecurity kan het zo zijn dat een werkgever investeert in opleiding, maar dat de persoon in kwestie vervolgens naar een andere organisatie vertrekt. Maatschappelijk gezien kan deze opleiding in deze persoon zichzelf wel degelijk terugbetalen, maar voor de oorspronkelijke werkgever is er geen sprake van een directe positieve business case. Dergelijke dynamiek kan leiden tot onder-investering in de (maatschappelijk) gewenste opleiding m.b.t. cybersecurity. Dit onderliggende marktfalen kan Rijksoverheidsinterventie legitimeren, o.a. in de vorm van het subsidiëren van na-, om- of bijscholing en het (semi)publiek aanbieden van gratis/goedkoop opleidingsaanbod.
- **Negatieve externaliteiten**. Er kan ook sprake zijn van zogenaamde negatieve externaliteiten wanneer de kosten voor bepaald (uitblijven van) handelen niet volledig neerslaan bij de organisatie die het (uitblijven van) handelen vertoont. Wanneer een organisatie niet cyberveilig opereert kan dit bijvoorbeeld ook de veiligheid van andere spelers binnen de keten negatief beïnvloeden vanwege onderlinge afhankelijkheden en relaties. Zo kunnen de resulterende kosten van een cyberaanval vele malen groter zijn dan de kosten die deze individuele partij maakt. Dit marktfalen legitimeert Rijksoverheidsinterventie, o.a. in de vorm van financiële compensatie voor collectief optimaal gedrag en wet- en regelgeving (bijv. verplichtingen).
- **Coördinatiefalen**. Om bepaalde doelen te bereiken moeten vaak meerdere partijen gezamenlijk de handen ineen slaan en dienen hun inspanningen gecoördineerd worden. Denk bijvoorbeeld aan het afstemmen van opleidingsaanbod tussen onderwijsinstellingen voor een optimale dekking en 'taakverdeling' op het gebied van cybersecurity-onderwijs, of het coördineren van cyber-inspanningen binnen een waardeketen waardoor alle bedrijven in gezamenlijkheid cyberveilig opereren. Alle betrokkenen hebben weliswaar baat bij dergelijke collectieve inspanningen, maar voor iedere individuele partij zijn de baten niet dusdanig hoog om de volledige coördinatie(kosten) op zich te nemen. Dit kan resulteren in een ongecoördineerd collectief dat niet in het teken staat van het collectief belang. Dit falen legitimeert Rijksoverheidsinterventie, o.a. in de vorm van het financieren, faciliteren en/of zorgdragen voor coördinatie en regie.

Dergelijke uitdagingen in het systeem (deze zogenoemde 'falen') kunnen dus overheidsinterventie legitimeren. Het hier opgestelde advies, zeker voor zover het zich richt op de betrokkenheid van de publieke sector, vloeit dan ook voort uit deze fundamentele onderliggende problemen. Het (reguliere) onderwijssysteem is daarbij één van de routes die de overheid neemt om de uitdagingen trachten aan te pakken. Het onderwijssysteem raakt in de voorliggende context aan

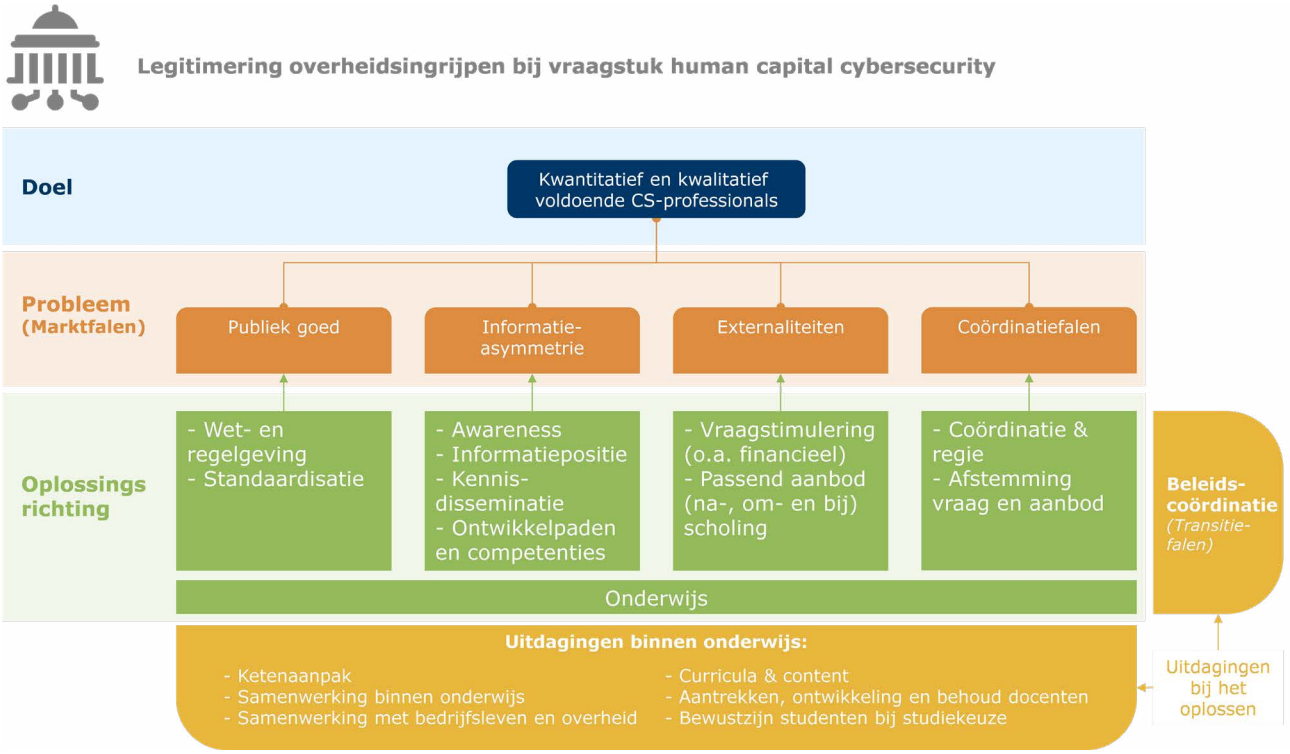
13. Zie bijvoorbeeld: 'Onderzoeks- en innovatie-ecosystemen in Nederland. Achtergrondstudie bij de kabinetsstrategie: Versterken van onderzoeks- en innovatie-ecosystemen'. Dialogic (2020)

alle beschreven falen, en kan op meerdere punten een deel van de oplossing bieden. Het onderwijs heeft derhalve ook een relatief belangrijke positie binnen dit advies.

Tot slot constateren we dat er op het gebied van Human Capital m.b.t. cybersecurity sprake is van nog een extra uitdaging. In het paradigma van 'transitiefalen' wordt gerefereerd aan het concept 'beleidscoördinatiefalen', waar de auteurs van het rapport "Durf te leren, ga door met meten" het volgende over schrijven[14]:
"Hoewel het begrip coördinatiefalen in het onderzoeks- en innovatiebeleid is gebruikt als een voorbeeld van systeemfalen, verwijst het alleen naar coördinatieproblemen van innovatieactoren, niet naar coördinatieproblemen bij beleid. Het organiseren van activiteiten op bijvoorbeeld nationaal, regionaal en sectoraal niveau en tussen verschillende partijen is van belang tijdens transities."

Gezien de breedte en complexiteit van het cybersecurityveld is het van belang dat alle betrokkenen hun beleidsinspanningen goed coördineren. De diversiteit aan typen professionals, in een relatief snel veranderende arbeidsmarkt en een beperkte gezamenlijke taal om dat te duiden, maken dat er in onze optiek ook specifiek aandacht nodig is voor beleidscoördinatie op dit deelthema Human Capital, aanvullend op de generieke coördinatie die reeds bestaat (middels o.a. de NLCS).
Voor gewenste uit te voeren acties en interventies is het onder meer van belang dat [1] deze acties uitgevoerd worden ('voorkomen hiaten'), [2] deze acties niet dubbel uitgevoerd worden ('overlap en beleidsconcurrentie') en [3] dat deze acties waar mogelijk door partijen uitgevoerd worden die hier doeltreffend en doelmatig invulling aan kunnen geven.

De genoemde (voorbeelden van) falen, de oplossingsrichtingen en de uitdagingen daarbij die in dit advies centraal zullen staan, kunnen als volgt schematisch samengevat worden:



Figuur 3: Legitimering Rijksoverheidsingrijpen bij vraagstuk Human Capital cybersecurity

14. Zie: Ministerie van Economische Zaken en Klimaat (2022), "Durf te leren, ga door met meten Op zoek naar kaders en methoden voor de evaluatie van systeem- en transitiebeleid"

Bijlage 4. Overzicht adviezen en niveau actie

Advies	Nationaal	Regionaal	Lokaal	(Rijks) overheid	Onderwijs	Bedrijfs-leven	Overig
1: Ontwikkel een gezamenlijke taal en gezamenlijk beeld m.b.t. 'cybersecurity-expertise'							
• Gezamenlijke taal: Ontwikkelen en standaardiseren van de gehanteerde taal op het onderwerp. Inclusief welke conceptuele kaders bruikbaar kunnen zijn, en welke afspraken er gemaakt worden over het spreken over cybersecurity-expertise.	x			x	x	x	X

• Gezamenlijk beeld:
informatiepositie vergroten door:
  • Verbeteren beroepenclassificatie cybersecurity
  • Dashboard met uitkomsten van onderwijs- en arbeidsmarkt onderzoek en een netwerkkaart van opleidingen en initiatieven
  • Impactmeting van maatregelen zoals bijvoorbeeld arbeidsmigratiebeleid
  • Meer zicht krijgen op vraag en aanbod wat mbo-vacatures betreft
	x			x	x	x	X

• Gezamenlijk beeld: curricula
  • Landelijk programma over leren en werken in de cybersecurity (bijv. met rolmodellen, gastlessen etc)
  • Instellen landelijke commissie met vertegenwoordigers van kennisinstellingen en bedrijfsleven die een dekkend curriculum ontwikkelt en actueel houdt.
  • Landelijke ontwikkelen en beschikbaar stellen van onderwijsmateriaal
	x			x	x	x	x

• Gezamenlijk beeld: visie op migratie De implicatie van politieke keuzes scherpkrijgen en de impact voor de cybersecurity-arbeidsmarkt inzichtelijk te maken. (zie ook gezamenlijk beeld- informatiepositie vergroten door)	x			x	x	x	X
2: Breng gerichte coördinatie aan op de aansluiting onderwijs- arbeidsmarkt.	x			x	x	x	
• Het in kaart brengen van de diverse en omvangrijke vraag op de arbeidsmarkt. Welke partijen hebben welke professionals en expertise nodig?	X			X	X	X	X
• Het in kaart brengen van de diverse opleidingen (bekostigd en onbekostigd). Welke partijen bieden welk scholingsaanbod aan?	X			X	X	X	x
• Het coördineren van inspanningen om vraag en aanbod beter op elkaar aan te laten sluiten.	x			X	x	x	x

3: Spreek het volledige potentiële talent aan.	x			x	x		
• het versterken van het imago: middels een landelijk uitgevoerd programma te werken aan een juiste beeldvorming van wat leren en werken binnen deze sector inhoudt	x				x	x	x
• het potentieel van mbo-opgeleiden beter benutten: kennis en vaardigheden van mbo-ers beter over voetlicht brengen en matchen met de vraag vanuit bedrijven		x			x	x	
• Het versterken van diversiteit & inclusie: landelijke programma met activiteiten in de gehele keten om de diversiteit in de sector te vergroten.	x				x	x	
4: Zoek de samenwerking op tussen en binnen regio's, sectoren en ketens.							

• Regionale samenwerking op het gebied van:
  • Kennisdisseminatie
  • Betere matching van vraag en aanbod door traineeships, gezamenlijk werkgeverschap
		x			x	x	

• Samenwerking tussen sectoren en ketens	x	x			x	x	x
5: Vergroot de zichtbaarheid en aantrekkelijkheid van 'het beroep'.							
• de grote variëteit in functies en expertise (niet enkel technisch van aard) zichtbaar maken • de breedte van het werkveld en het belang van werken binnen deze sector zichtbaar te benadrukken.	x	x	x			x	x
6: Stimuleer om-, bij- en nascholing ten behoeve van horizontale en verticale ontwikkeling.							
• Bewustwording vergroten over Leven Lang Ontwikkelen	x	x				x	
• Generiek stimuleringsbeleid	x			x			
• Vraagstimulering	x			x		x	
• Ontwikkelpaden en carrièreperspectief	x	x			x	x	
• Learning Communities		x			x	x	Regionale overheid
• Opschaling instrumentarium	x	x			x	x	
• Traineeships		x			x	x	
• Niet-werkenden		x			x	x	Gemeenten, UWV

7: Werk aan behoud van professionals m.b.v. arbeidsmobiliteit binnen de sector.							
• Regionale infrastructuur opzetten om mensen cybersecurity-professionals voor de sector re behouden		x				x	Regionale overheid
8: Verbeter de startpositie van net afgestudeerden.							
• Goede onboarding en talentontwikkeling voor startende cybersecurity werknemers organiseren		x	x		x	x	
9: Vergroot de interesse voor studeren en werken in cybersecurity.							
• Primair en voorgezet onderwijs: meer aandacht voor cybersecurity in de curricula	x			x	x		
• Primair en voorgezet onderwijs: onderwijsmateriaal laagdrempelig beschikbaar maken	x			x	x		
• Primair en voorgezet onderwijs: tools ontwikkelen voor loopbaan oriëntatie	x				x		
• Primair en voorgezet onderwijs: activiteiten organiseren om leerlingen bekend te maken met de wereld cybersecurity		x	x		x	x	
10: Verstrek de kaders en het materiaal voor cybersecurity-onderwijs.							
• Specifiek mbo: Vroegtijdig maar ook op doorslaggevende momenten aandacht aan cybersecurity in de ICT-opleidingen (tijdig starten met loopbaanorientatie en tegelijk stages en projecten in cybersecurity aan het eind van de opleiding programmeren)			x		x		
• Specifiek ho: aanreiken nationaal framework voor kennis en vaardigheden op het gebied van cybersecurity	x			x	x	x	
• Specifiek wo: zorgen voor een landelijke dekkend onderwijsaanbod	x				x		
• Nieuwe onderwijsconcepten om een bredere doelgroep van studenten te bereiken					x	x	
• Op landelijk niveau curriculummateriaal ontwikkelen	x				x		
• Uitrollen cybersecurity opleidingsaanbod in aanpalende opleidingen			x		x		
• Organiseren challenges en hackathons	x	x			x	x	
• Zorgen voor goede aansluiting mbo- hbo, zodat mbo ICT-opleidingen als vooropleiding voor cybersecurity-specialist kunnen fungeren	x				x		
11: Betrek de arbeidsmarkt sterker in het onderwijs.		x		x	x		

• Gezamenlijk werven, opleiden en delen van docenten							
• Afstemming welke actuele vaardigheden studenten nodig hebben en welke flexibiliteit in het onderwijs nodig is			x		x	x	
• Contextrijke leeromgevingen voor het onderwijs inrichten		x			x	x	
• Flexibeler opleiden in het mbo en het ho (door deeltijdopleidingen, hybride opleidingen, modulair opleiden, microcredentials) en daarmee grotere groep studenten te bereiken.		x			x	x	
• Promotie van cybersecurity richting leerlingen en studenten		x	x	x	x	x	
12: Versterk en vergroot de aantrekkelijkheid van het docentschap.							
• Mogelijkheden hybride docentschap en/ of gezamenlijk aanstelling door universiteit en bedrijven van Phd-kandidaat onderzoeken		x	x		x	x	
• Subsidie voor bij- en nascholing van docenten zowel ICT-docenten als docenten in andere domeinen	x			x			
• Aanbieden docent-stages bij bedrijven		x			x	x	
• Landelijk masterclasses ontwikkelen en organiseren	x				x	x	
• Laagdrempelige omscholingstrajecten aanbieden voor mensen die zich willen omscholen naar Informatica/ICT/cybersecurity -docent	x	x			x	x	

Bijlage 5. Relevante beleidsplannen, actieplannen en agenda's

	Naam	Omschrijving
1	Actieplan Groene en digitale banen	Het Actieplan groene en digitale banen van het ministerie van EZK bevat maatregelen om de krapte op de arbeidsmarkt aan te pakken in sectoren die van groot belang zijn voor de klimaat- en digitale transitie. Dit plan richt zich op banen die cruciaal zijn voor duurzame groei en de energietransitie. Specifiek de vraag naar cybersecurity beroepen wordt in het actieplan niet expliciet vermeld, maar het algemene doel is om tekorten aan technisch en digitaal geschoold personeel aan te pakken. Dit omvat ook de behoefte aan gekwalificeerde professionals in het cybersecuritydomein. Het plan benadrukt de noodzaak van een gecoördineerde aanpak waarbij werkgevers, werknemers, onderwijsinstellingen en Rijksoverheidsinstanties samenwerken om deze tekorten te verminderen.
2	Human Capital Agenda (HCA) ICT	De Human Capital Agenda (HCA) ICT is het actieplan om aan de groeiende vraag naar ICT-professionals te voldoen en werk te maken van de noodzaak voor een 'leven lang ontwikkelen' die door digitalisering ontstaat12. Het bundelt de krachten van onderwijs, bedrijfsleven en Rijksoverheid in Nederland om deze uitdaging aan te pakken. Hier zijn enkele belangrijke aspecten van de Human Capital Agenda ICT: • 1 miljoen ICT'ers in 2030: Het doel is om tegen 2030 maar liefst 1 miljoen ICT-professionals in Nederland te hebben. • Sterke binding van ICT'ers met beroep en sector: Het plan richt zich op het creëren van een sterke verbinding tussen ICT-professionals en hun vakgebied en sector. • Thema's: De HCA ICT behandelt thema's zoals behoud van talent, digitale geletterdheid, en diversiteit en inclusie. • Regionale aanpak: Samenwerking op regionaal niveau is essentieel om het tekort aan ICT'ers aan te pakken.
3	Het Aanvalsplan Chronisch Tekort ICT'ers	Het Aanvalsplan Chronisch Tekort ICT'ers is een gezamenlijk initiatief van branchevereniging in Nederland om het chronische tekort aan ICT-professionals aan te pakken. Dit plan sluit nauw aan bij de Human Capital Agenda ICT (HCA ICT) en heeft als ambitie om 1 miljoen ICT'ers in Nederland te krijgen. Hier zijn de belangrijkste pijlers uit het aanvalsplan: • Promotie van keuze voor ICT en technische beroepen: Het plan richt zich op het stimuleren van jongeren om te kiezen voor een carrière in de ICT en techniek. • Scholing van PO tot beroepsonderwijs en WO: Het bevordert onderwijs en opleidingen op alle niveaus om meer ICT-professionals op te leiden. • Noodzakelijke cultuurverandering: Het aanvalsplan benadrukt het belang van een veranderde mindset en cultuur om meer mensen naar de ICT-sector te trekken. • Zij-instroom uit andere sectoren en landen: Het plan moedigt zij-instroom aan vanuit andere vakgebieden en landen. • Regionale aanpak: Samenwerking op regionaal niveau is essentieel om het tekort aan ICT'ers aan te pakken.

4	Human Capital Agenda Security 2023 – 2026	Deze agenda van de The Hague Security Delta en CVD bevat een gedeelde ambitie van 70 organisaties en reikt een basis aan voor verdere samenwerking op lokaal, regionaal en nationaal niveau. De belangrijkste bevindingen en knelpunten vormen de basis voor 25 interventies gericht op de arbeidsmarkt van digitale veiligheid. Deze omvatten: • het versterken en monitoren van arbeidsmarktinzichten • de ontwikkeling van specifieke trainingsmodules • programma's voor professionals en carrièreswitchers, • flexibilisering van de werkverdeling • het aantrekken van ondervertegenwoordigde groepen • het promoten van werk in de beveiliging • ondersteuning van HR • effectieve leergemeenschappen • competentieontwikkeling op het gebied van beveiliging.
5	Nationale Cyber Security Educatie Agenda	In 2020 opgesteld door dcypher. Voor de volgende thema worden interventies aangereikt: • voorbereiden: leerlingen in het primair en voortgezet onderwijs moeten les krijgen in digitale veiligheid en privacy, van docenten met cybersecuritykennis. • interesseren: een positief imago en een duidelijk beeld van het vakgebied en de loopbaanmogelijkheden, trekken meer studenten aan. • professionaliseren: werkgevers, opleiders, studenten en experts hebben profijt van onafhankelijk opgestelde, uniforme, transparante eisen aan vakbekwaamheid. • doceren: er zijn meer gekwalificeerde docenten met cybersecuritykennis en -vaardigheden nodig. • samenwerken: er is regie op vraag en aanbod; periodiek monitoren onderwijsinstellingen en de arbeidsmarkt gezamenlijk de kwalitatieve en kwantitatieve behoefte en spelen daar actief op in. • verbreden: verbreding heeft betrekking op niet-specifieke cybersecurityberoepen. Elke beroepsgroep stelt eisen op met betrekking tot het noodzakelijke cybersecurity-kennisniveau dat aansluit bij de beroepsuitoefening

Bijlage 6. Huidige regelingen en programma's

Huidige regelingen en programma's PTvT	Wat is het?	Kansen voor cybersecurity
Regionaal Investeringsfonds mbo	Subsidieregeling waarbij mbo's als penvoerder samen met het werkveld middelen kunnen aanvragen om de aansluiting tussen opleidingen en werkveld te verbeteren.	Samenwerking tussen onderwijs en werkveld cybersecurity te versterken. Nog meer aandacht voor cybersecurity in ICT- en andere mbo-opleidingen. Beter/ actueler cybersecurity onderwijs. Pool van cybersecurity opgeleiden vergroten.
NGF-aanvraag ICT	Stimuleringsregeling voor regionale programmatische ketenaanpak van publieke –, private- en publiek/private initiatieven om meer mensen (1 miljoen ICT- ers in 2030) voor de ICT op te leiden. O.a. door opleidingen te laten aansluiten bij wat het werkveld nodig heeft systeembeheerders, software- en applicatieontwikkelaars, data-analisten, netwerk-specialisten en cybersecurity experts.	Specifiek aandacht vragen voor cybersecurity, pool van cybersecurity -opgeleiden vergroten.
NGF-aanvraag po-vo "Investeren in het talent van de toekomst"	Subsidieregeling voor regionale netwerken om via een impuls de samenhang en de impact van lopende initiatieven en activiteiten op het gebied van technologieonderwijs te vergroten.	Promotie van cybersecurity in po- en vo
Sterk Techniek Onderwijs	Regeling met als doel is om – in regionale samenwerking met po, mbo en bedrijfsleven- tot een duurzaam, dekkend en kwalitatief hoogstaand technisch onderwijsaanbod in de regio te komen.	Meer aandacht voor cybersecurity in het vmbo-mbo curriculum. Doorlopende leerlijnen. Promotie voor cybersecurity in het vmbo en vanuit de regionale STO-samenwerkingsverbanden promotie voor cybersecurity in het po.
Jet-Net	Jet-Net deelt data en ontwikkelt kennis en tools om techniek en technologie in het funderend onderwijs beter vorm te geven en goed aan te laten sluiten bij de belevingswereld van jongeren. Doet dit samen met regionale samenwerkingen van scholen, bedrijven en andere organisaties.	Promotie van cybersecurity in po- en vo
MKB-route HBO	Programma dat beoogt studenten vroegtijdig te koppelen aan het midden-en kleinbedrijf (mkb) in werkend leren trajecten. Het landelijk programma biedt onder andere ondersteuning bij het opzetten of doorontwikkelen van de opleiding en verbinding met relevante partners zoals branches en mkb-bedrijven.	Vergroten uitstroom hbo-gediplomeerden die meteen in de cybersecurity aan de slag kunnen. Formule die deels in speelt op de vraag vanuit bedrijven naar mensen die al werkervaring hebben. Beter/actueler cybersecurity onderwijs door directe verbinding met werkveld.

Digitale werkplaatsen MKB	Digitale Werkplaatsen zijn publiek-private samenwerkingen waarbij studenten in het mbo, hbo en wo mkb-ondernemers helpen te digitaliseren. (Er zijn momenteel 20 digitale werkplaatsen in Nederland)	Schakelpunt om interessante levensechte opdrachten op het gebied van cybersecurity bij studenten uit te zetten. Kan eraan bijdragen dat studenten geïnteresseerd raken in een cybersecuritycarrière en tegelijkertijd relevante kennis en ervaring opdoen bij het uitvoeren van een cybersecurity-opdracht.

Bijlage 7. Kansrijke concepten specifiek voor cybersecurity

	Naam	Regio	Omschrijving
1	Hacklab	Friesland	Deze werkplaats staat open voor digitale hangjongeren, gamers, schoolverlaters, jongeren binnen het autisme spectrum en jongeren die uitdaging in hun huidige opleiding missen. De mentoren binnen het Hacklab maken, indien gewenst, matches tussen de leerlingen en mogelijke werkgevers https://hacklab.frl/
2	Cybersecurity werkt	Landelijk	Met het platform cybersecuritywerkt.nl wil HSD helpen de mismatch tussen vraag en aanbod van cybersecurity talent op te lossen. De website biedt volop mogelijkheden voor omscholing en zij-instromers die hun carrière willen voortzetten in cybersecurity. https://cybersecuritywerkt.nl/
3	Cyber Security & Cloud Cloud IT Academy	Utrecht	CITA-bedrijven bieden directe werkgelegenheid en de mogelijkheid om je kennis te verdiepen en uit te breiden via de duale hbo-opleiding Cyber Security & Cloud van Hogeschool Utrecht. https://cita.academy/studenten/cyber-security-cloud/
4	Make IT Work	Landelijk	Omscholingstraject op hbo-niveau mét baangarantie in de IT. Een van de drie omscholingsprogramma's is cybersecurity. Gedurende deze cybersecurity opleiding wordt in de basisfase de basis gelegd voor programmeren, databases en SQL, operating systems en netwerken. In de verdiepingsfase verwerft de cursist in werkcolleges en met praktijkopdrachten, fundamentele kennis en -vaardigheden over een diversiteit van cybersecurity onderwerpen. https://it-omscholing.nl/programmas/cybersecurity/
5	re_B00TCMP	Landelijk	Jongeren met IT-interesse in de leeftijd tussen 12 en 25 krijgen op deze dag middels interactieve workshops inzicht in de kansen en risico's van hun uitzonderlijke cybertalenten. https://re-b00tcmp.nl/
6	Nationale en Internationale summerschool	Landelijk	Zie website dcypher https://dcypher.nl/ en HSD https://securitydelta.nl/nl/
7	Challenge the Cyber	Landelijk	https://challengethecyber.nl/

Bijlage 8. Kansrijke voorbeelden IT

	Naam	Regio	Omschrijving
1	Bit Academy	Amsterdam Purmerend Groningen	In de Bit Academy volgt de theorie de praktijk en volgen studenten een MBO4 opleiding Software Developer via een niet-schoolse aanpak. Deelnemers bepalen hun eigen leerroute en tempo, worden ondersteund door (hybride) coaches en medestudenten en werken veel met praktijkopdrachten. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20Model%20BIT.pdf
2	TalentIT	Twente	Verzorgt de matching tussen de vraag van ICT-bedrijven in Twente en studenten die op zoek zijn naar een passende bijbaan of opdracht. Op deze manier kunnen potentiële toekomstige werknemers kennismaken met bedrijven in hun regio. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20Talent%20IT%20Twente.pdf
3	The Young Digitals	Den Haag Rotterdam Utrecht	Stichting die jongeren met een afstand tot de arbeidsmarkt begeleidt naar werk als digitale markerteer. Dit doen zij door een kosteloos traject van 24 maanden aan te bieden waar de jongeren (18-27 jaar) worden opgeleid en intern en extern werkervaring opdoen. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20YD.pdf
4	Scalda		In de bedrijfsmatig ingerichte leeromgeving van Scalda gaan mbo-studenten aan de slag met praktijkopdrachten van opdrachtgevers uit de regio. Op deze manier leren de studenten zowel de inhoudelijke kennis als de soft skills. De studenten worden begeleid door coaches van Scalda. Bovendien kunnen ze ook nog inhoudelijk geholpen worden door experts uit het bedrijfsleven. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20Scalda.pdf
5	DAATLAB		Trekt in meerdere steden actief op voor werkzoekenden met een afstand tot de arbeidsmarkt samen met werkgevers die sociaal ondernemen. Om eenieders potentieel te benutten biedt DAATLAB een werk-leertraject op passend niveau aan om te groeien naar een betaalde functie in de richting van data. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20Daatlab.pdf
6	Technasium en Codasium		Naast het reguliere onderwijsprogramma, wordt Technasium en Codasium zoveel mogelijk als extra programma aangeboden, waarbij vo-leerlingen respectievelijk de vakken Onderzoek & Ontwerpen en Modelleren & Programmeren gedurende 3 uur in de week volgen tot het eindexamen. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20Lyceum%20Rotterdam.pdf
7	KE@Work		2-jarig honours programma van de bachelor opleiding Data Science & Artificial Intelligence, Maastricht University. Het programma biedt ambitieuze studenten de kans om een complex probleem uit de praktijk op te lossen. Studenten werken gedurende 2 jaar in een 50/50 constructie aan een uitdaging bij een regionaal bedrijf of organisatie, inclusief salaris. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20Ke%40Work.pdf

8	SPARC		Vereniging van zelfstandige (ICT-)bedrijven die hun innovatiekracht gebundeld hebben. Daarvoor werkt SPARC samen met lectoren, docenten en studenten van Fontys Hogeschool ICT aan onderzoeken en experimenten in het Fontys ICT InnovationLab. Leden van SPARC brengen onderzoeksvoorstellen in die binnen onderwijscontext als toegepast onderzoek worden uitgevoerd. Zo werken leden van SPARC samen met jong technisch talent en professionals van Fontys Hogeschool ICT aan nieuwe technologie en vooruitstrevende ICT-innovaties. In ruil daarvoor dragen de leden van SPARC bij aan het door SPARC beheerde Innovatiefonds, van waaruit onderzoeksprojecten gefinancieerd worden. https://www.wijzijnkatapult.nl/files/downloads/Werkende%20modellen/Werkend%20model%20SPARC.pdf