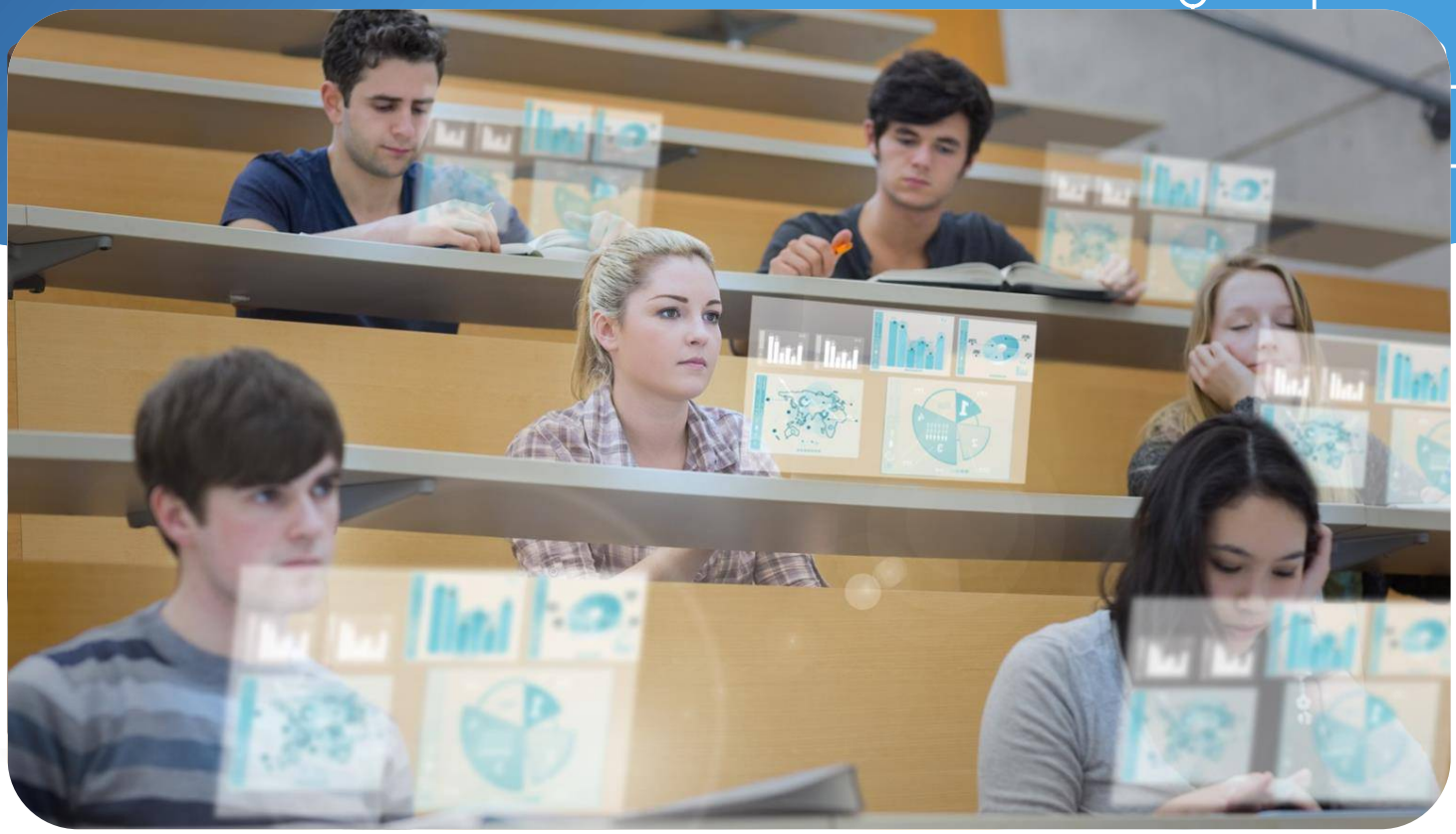
The Hague **Security Delta**



Human Capital Actieagenda Cyber Security

2016-2018

Human Capital Programmateam | 20 december 2016 | Versie 1.0

The Hague **Security Delta**

info@thehaguesecuritydelta.com | thehaguesecuritydelta.com | @HSD_NL

Human Capital Actieagenda Cyber Security

Inhoudsopgave

1 Inleiding

The Hague Security Delta (HSD) is het leidende veiligheidscluster van Europa. In dit Nederlandse cluster werken bedrijven, overheden en kennisinstellingen samen aan innovaties en kennisontwikkeling onder andere op het gebied van cyber security. Met als gezamenlijke ambitie: meer bedrijvigheid, meer banen en een veilige wereld. Alleen al in de regio Den Haag realiseren 400 veiligheidsbedrijven meer dan 25% van de landelijke omzet in veiligheid en bieden werk aan 13.400 mensen. Landelijk wordt 6 miljard euro omgezet en zijn er inmiddels 3.100 bedrijven en 61.500 mensen werkzaam in het veiligheidsdomein. Naast Den Haag leveren in het bijzonder de regio's Twente en Brabant hier een bijdrage aan met hun innovatieve living labs en universiteiten.

Een van de speerpunten van HSD is het organiseren van toegang tot talent, omdat organisaties voor hun groei en succes afhankelijk zijn van de beschikbaarheid van gekwalificeerde werknemers. Verschillende studies, beleidsstukken en het dagelijkse nieuws laten zien dat cyber security een belangrijke en groeiende maatschappelijke uitdaging is en dat het een kansrijke sector vormt voor Nederlandse bedrijvigheid. Om deze redenen is samen met HSD-partners deze Human Capital Actieagenda (HCA) opgesteld. Het uiteindelijke doel van de HCA Cyber Security luidt:

> *"Nederland heeft internationaal een koppositie op het gebied van cyber security, benut de kansen van digitalisering volledig en is weerbaar tegen geavanceerde dreigingen. Er is voldoende gekwalificeerd personeel dat deze koppositie, innovatie en uitwisseling van kennis mogelijk maakt. De cyber security community is aantrekkelijk om in te werken en talent "stroomt" tussen organisaties voor optimale kennisuitwisseling. De veiligheidssector biedt talent een duurzaam carrièreperspectief en het aanbod van cybertalent sluit aan bij de behoeften. Werken in de cyber security sector staat synoniem voor uitdaging, content-driven, flexibel, leven-lang-leren, ondernemen en eigen initiatief."*

Dit is een uitdagend doel, maar het cluster heeft veel leden die hier al een rol in gepakt hebben of in kunnen vervullen. Deze agenda leunt sterk op het benutten van die expertise, uitvoeringsmacht en ambities van de partners en andere relaties. De rol van de HSD-office is primair geen uitvoerende maar verbindend, faciliterend, organiserend, uitdragend en soms is zij agenderend, aanjagend en initiatief nemend of ondersteunend. Het bereik van de activiteiten die benoemd worden in deze agenda is voor een belangrijk deel bepaald door al geplande en gestarte activiteiten die in samenhang en verbinding meer resultaat kunnen boeken.

2 Analyse knelpunten

2.1 Definitie en afbakening

Voor deze actieagenda wordt gebruik gemaakt van de definitie van cyber security die in het rapport 'Arbeidsmarkt voor Cyber Security Professionals' wordt gehanteerd (PLATO & Ockham IPS, 2014). Deze definitie is een licht aangepaste versie van de definitie zoals gebruikt in de Nationale Cyber Security Strategy 2 (NCSS 2) en luidt:

> *"Cyber security betreft het reduceren van gevaar of schade veroorzaakt door introductie van nieuwe technologie, storing of uitval van ICT of misbruik van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie."*

Zoals terecht wordt aangegeven in het PLATO rapport, plaatst deze definitie cyber security nog iets te nadrukkelijk in de context van ICT en reductie van gevaar in plaats van bewustzijn en weerbaarheid. Het is van belang te beseffen dat cyber security betrekking heeft op alle activiteiten in cyberspace. In de praktijk van organisaties reikt dit verder dan informatiebeveiliging en rollen die voorheen exclusief waren voorbehouden aan ICT-afdelingen. Jan van den Berg (TU Delft) maakt het nuttige onderscheid tussen de technische laag (IT diensten), de sociaal-technische laag (brede activiteiten in cyberspace) en de bestuurlijke laag (governance & management). Deze agenda voor cyber security gaat over alle drie de lagen. Per activiteit moet duidelijk zijn of worden op welk van de lagen het gericht is.

Onder 'Human Capital' of 'menselijk kapitaal' verstaan we de competenties, kennis, sociale en persoonlijke vaardigheden, die mensen in staat stelt om waarde te creëren. Deze Human Capital Agenda schetst een nationale analyse en aanpak om het menselijk kapitaal voor cyber security te vergroten, maar heeft de acties vooral beschreven voor het regionale cluster en in samenwerking met bestaande HSD-partners. Het blikveld in opleidingsniveaus is van middelbaar tot en met hoger niveau. Daar waar opportuun verbindt de HSD-office activiteiten met nationale[1]- en andere regionale initiatieven en moedigen wij opschaling en verbinding aan.

2.2 Landelijke arbeidsmarkt

Uit onderzoek in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (Ministerie van Veiligheid & Justitie) blijkt dat er in Nederland ongeveer 7.000 personen werkzaam zijn in cyber security[2] in 2014. In hetzelfde onderzoek worden 1.158 cybersecurity-vacatures gemeten in 2014. Het werkelijke aantal openstaande vacatures ligt volgens de onderzoekers waarschijnlijk minimaal 10% hoger. De verwachte groei bedraagt 10% per jaar. Rekenen we door met deze cijfers dan geeft dit een aantal van 1.541 openstaande vacatures in 2016. Van de openstaande vacatures is het merendeel op HBO niveau (77%). Een studie in opdracht van het Ministerie van Economische Zaken[3] uit 2016 schat in dat er in 2014 in de ICT sector alleen al 16.400 personen zijn die zich bezig houden met cyberactiviteiten met een gemiddelde groei tussen 2010 en 2014 van 7%. Wanneer deze lijn doorgetrokken wordt is het aan personen in 2016 rond de 18.776. Of daarmee het aantal vacatures ook 2,3 keer zo hoog zou moeten zijn is niet te achterhalen vanuit de studies, dit heeft naast de analysemethode ook met het gehanteerde criterium te maken. In de studie voor het Ministerie van EZ wordt het gebrek aan beschikbaarheid van goed gekwalificeerde mensen zowel als grootste zwakte van Nederland en als grootste bedreiging van de marktontwikkeling genoemd.

Er is een mismatch van niveaus tussen vraag en aanbod: 77% van de vraag zich richt op HBO terwijl het maar 51% van het aanbod vormt. Zelfs wanneer het overschot aan WO geschoolden (3% van de vraag tegen 10% aanbod maakt een overschot van 7%, in de praktijk van de HSD partners wordt dit overschot niet herkend) in zou stromen op HBO functies is er nog altijd 19% tekort aan

[1] Zoals dcypher voor hoger onderwijs en ECP/DDD voor Human Capital Agenda ICT
[2] PLATO & Ockham IPS (2014). Arbeidsmarkt voor Cyber Security Professionals.
[3] SEO/VKA (2016). Economische kansen Nederlandse Cybersecurity-sector.

aanbod van kandidaten op HBO niveau[4]. De HBO/WO ICT Security specialist is door het UWV geïdentificeerd als moeilijk vervulbare vacature[5]. Tijdens een meting in oktober 2016 zien we dat 15% van de 585 IT Security vacatures op Monsterboard langer dan 60 dagen open staat (dit is een deelverzameling van alle functies in cyber security). Uit een internationale studie van ISACA[6] blijkt dat posities in cyber security zelfs voor 63% langer dan twee maanden open staan. Daarbij gaven cybersecurity-experts in meerderheid aan dat de helft van het aangenomen personeel niet over de juiste kwalificaties beschikt. De vraag om talent is niet uniek voor Nederland. Er is wereldwijd een grote vraag naar cybersecurity talent. Beschikbaarheid van goed geschoold talent is vaak een voorwaarde voor werkgevers om zich in een regio of land te vestigen. Ook door Nederlandse organisaties wordt talent uit het buitenland geworven om te voorzien in de behoefte.

Er is een grote diversiteit aan functies in cyber security. Wanneer we spreken over tekorten in cyber security dan is dat niet één profiel. Sommige zijn dominant technisch van aard (penetratietesters en systeembeheerders bijvoorbeeld), andere meer mens of beleid gericht (zoals security officer of beleidsmedewerker). De mate waarin cyber security een onderdeel van de functie vormt verschilt per functie en per werkgever. Door de groeiende vraag ontstaat er ook een nieuwe groep waar de vraag aanhoudend stijgt: onderzoekers en opleiders, deze zijn niet apart onderscheiden. In onderstaande tabel staat een typering van de functies en een duiding van het tekort.

	Functiegroepen	Denk aan	Tekort
1	Technisch dominante specialistische cybersecurityfuncties	Ethical hackers, penetratietesters, software testers en technical security-engineers)	Vraag stijgt aanhoudend
2	Niet technisch dominante specialistische cybersecurity functies	IT security officers, IT security specialists, security officers, Information security officers, informatiebeveiligers	Vraag stijgt komende 5 jaar
3	Technisch dominante functies waarbij cybersecurity een onderdeel is	Systeembeheerders, softwareontwikkelaars en architects	Grootste groei
4	Niet technisch dominante functies waarbij cybersecurity een onderdeel is	Jurist in privacy-issues, beleidsmedewerker op het gebied van cybersecurity	Vraag naar competenties

Bron: PLATO rapport en inventarisatie onder HSD-leden uit 2014.

2.3 Scholing

Vanwege het tekort aan cybersecurity-specialisten is er ook een druk op de beschikbaarheid van docenten. Er zijn onvoldoende mensen die er voor kiezen om voor de klas te staan. Docenten in cyber security stappen in een overspannen arbeidsmarkt regelmatig over naar andere functies waardoor er nog minder docenten beschikbaar zijn. Het aantal opleidingen is wel toegenomen vanwege de toegenomen vraag, maar het is voor opleiders vaak moeilijk geschikte docenten te vinden en vast te houden. Hiermee wordt de basis voor goed en voldoende omvangrijk scholingsaanbod ondermijnd. Voor bijvoorbeeld de hogescholen in de regio Leiden-Den Haag-Rotterdam-Zoetermeer gaat het tekort soms wel om 5 docenten per instelling[7].

[4] HSD (2015), Nulmeting Securitytalent
[5] UWV (2015). 'Technische en ICT-beroepen arbeidsmarktbeschrijving'
[6] ISACA & RSA (2016). 'State of cybersecurity. Implications for 2016.'
[7] Uit een gesprek met de directeur IT & Design van de Haagse Hogeschool.

Door digitalisering van de samenleving is er groeiende aandacht voor cyber security en verwachten we een verdere toename in de scholingsvraag, veelal in kortere cursussen en opleidingen met certificering (zoals bevestigt door ISACA, Security Academy en EXIN)[8]. Steeds meer functies krijgen een cyber security component. Dit komt waarschijnlijk niet in het aanbod van vacatures naar boven. De groeiende vraag naar professionaliseringsmodules blijkt uit de ervaring van de Security Academy (toenemende interesse in Post-HBO trajecten en korte 'nieuwsgierigheidscursussen' zoals Ethical Hacking Foundation) en onderzoek van PvIB/QIS[9] waarin wordt geconstateerd dat initiële opleidingen maar een deel van de benodigde competenties en ervaring voor cybersecurity-profielen op strategisch-tactisch niveau leveren. Door werkervaring en/of extra cursussen verwerft men aanvullende competenties of specialiseert men zich. Dit is ook merkbaar aan de aanwas van nieuwe certificeringen, cursussen en opleidingen in Nederland die is ontstaan op dit gebied, zoals van het Sans Institute, (ISC)², EC-Council, EXIN, ISACA en SECO als certificerende instellingen en de Security Academy, ISACA en de FoxAcademy als opleiders.

Door de HSD-partners TU Delft, De Haagse Hogeschool en de Universiteit Leiden is met steun van de Gemeente Den Haag de Cyber Security Academy opgericht. Zij draagt bij aan het opleiden van professionals door het aanbieden van een geaccrediteerde MSc Cyber Security (al twee maal ruim 20 deelnemers) en binnenkort een 'professionele master cyber security', gericht op HBO+'ers. Deze opleidingen verminderen de kwalitatieve mismatch, maar de kwantitatieve tekorten lost het niet of zeer beperkt op. Iets vergelijkbaars geldt voor de 'Cyber Security Summerschool' die door NCI Agency, Europol, HSD en HCSS al twee keer is georganiseerd. De inschrijvingen in 2016 (140) zijn groter dan de beschikbare plaatsen (61), maar met 24 deelnemende nationaliteiten is de beschikbaarheid van talent in Nederland waarschijnlijk beperkt toegenomen. De aantrekkingskracht en bekendheid van Nederland in dit domein neemt wel toe en zal op termijn de instroom van buitenlands talent kunnen vergroten. Private opleiders rapporteren soms wel honderden cursisten die jaarlijks uitstromen en wellicht voorzien in een deel van de vraag, maar het is niet bekend of dit nieuwe toetreders tot het domein zijn of mensen die hun competenties blijven ontwikkelen. Naast het al beschikbare aanbod van vaak breder georiënteerde ICT-opleidingen met een minor of specialisatie security ontstaan uit samenwerkingen tussen universiteiten meer specialistische opleidingen tot Master in Cyber Security (TRU/e Master in Cyber Security van de TU Eindhoven en de Radboud Universiteit, en het 4TU.CybSec master specialisatie programma dat gegeven wordt door de TU Delft en Universiteit Twente). Een overzicht in opleidingsaanbod relevant voor cyber security is onder andere te vinden op securitytalent.nl.

2.4 Behouden voor het vak

Meer studenten in het reguliere onderwijs met een relevante achtergrond moeten kiezen voor een carrière in cyber security om tekorten op te heffen. Onderzoekers van PLATO en Ockham IPS trekken in twijfel of deelnemers aan cyber security-gerelateerde opleidingen het vakgebied wel als loopbaanoptie zien, bijvoorbeeld vanwege de beperkte verbinding met de 'business continuity' kant of omdat ze er te beperkt of te laat mee in aanraking komen. Factoren die van belang zijn in het keuzeproces zijn[10]: opleidingsvoorlichting (over de opleiding, over de school, proefstuderen), beïnvloeders (ouders en docenten), intrinsieke- (ontwikkelkansen, interesses/capaciteiten) en excentrieke (goed betaalde baan, kans op diploma) factoren.
Nu vindt nog veel uitval in het eerste jaar plaats. Het imago of beeldvorming van het beroep is hiervoor van belang (zowel voor de studie als tijdens) evenals toekomstperspectief en transparant opleidingsaanbod. Ander knelpunt is de beperkte differentiatie in beroeps- en opleidingsbeeld: er bestaat niet één profiel van de cyber security medewerker, er zijn diverse profielen waar mensen met verschillende vaardigheden en belangstelling voor worden gevraagd. Mannen én vrouwen, maatschappelijk én commercieel, sociaal én technisch.

[8] Gabberty, James W. (2013). Educating The Next Generation Of Computer Security Professionals: The Rise And Relevancy Of Professional Certifications. Review of Business Information Systems . In: Vol. 17 Issue 3, p85-98.
[9] Spruit & van Noord (2014). ' Beroepsprofielen informatiebeveiliging. PVIB (Platform voor Informatiebeveiliging)
[10] http://www.hboaansluitingsmonitor.nl/factoren-van-invloed-op-het-keuzeproces/

Generieke ontwikkelingen op de arbeidsmarkt hebben ook hun weerslag op talent voor de veiligheidssector. Zo stelt “generatie Y” andere eisen aan werk en kenmerkt zij zich door andere competenties:

- Inhoud lijkt de sleutel voor boeien en binden van talent.
- Aantrekkelijk en flexibel werken, vaker wisselen van werkgever.
- Ondernemend en initiatiefrijk.

Vanwege de snelle wijzigingen in de behoefte is het noodzakelijk talent zelf verantwoordelijkheid te laten nemen over hun loopbaan en ontwikkeling en ze daarvoor de middelen te geven. Zowel voordat de carrière is begonnen als een leven lang (duurzaam inzetbaar).

2.5 Observaties HSD Partners

Eerder genoemde cijfers zijn gebaseerd op de nationale situatie en -verwachtingen. Dit beeld wordt door verschillende HSD-partners onderschreven: de vraag naar cybersecurity-experts in de markt is groter dan het huidige aanbod. De Haagse Hogeschool geeft bijvoorbeeld aan dat studenten van de relevante HBO-studies vrijwel allemaal direct na hun afstuderen (en vaak al daarvóór) een baan hebben. Wat onder meer naar voren wordt gebracht is dat er gezocht wordt naar cybersecurity-specialisten op HBO niveau die ook consultancy of commerciële vaardigheden bezitten. Verwachte groei van behoefte aan cybersecurity-experts wordt breed gedeeld. Ondanks het inzetten van diverse kanalen voor de werving van cybersecurity-experts zijn de inspanningen vaak niet succesvol. Dit leidt ertoe dat bedrijven ervoor kiezen om zelf intern op te gaan leiden, ondanks de kosten die dit met zich meebrengt. Voorbeelden hiervan zijn KPN, Thales en Defensie die intern werven en selecteren voor een (intern verzorgd) cybersecurity-specifiek opleidingstraject.

Uit beschikbare data van de HSD-website securitytalent.nl blijkt dat de vacatures voor meer dan 60% zich in het cybersecurity-domein bevinden (302 van de 486 over een periode van twee jaar). Ten opzichte van bijvoorbeeld de ICT sector in bredere zin heeft HSD een sterke concentratie cybersecurity-vacatures (cijfers van nationalevacaturebank.nl tijdens een steekproef in oktober 2016: minder dan 10% ICT vacatures bevat de term “security”). Vanuit contact met partners wordt meermaals duidelijk dat zij tegen problemen aanlopen bij het werven van cybersecurity-talent.

2.6 Omvang tekort

Een deel van de vacatures die er zijn betreft reguliere mobiliteit op de arbeidsmarkt. Waar het vacatures betreft die lang vacant blijven (langer dan twee maanden) is het aannemelijk dat er een tekort is. Wanneer we de geprognotiseerde omvang van vacatures in 2016 nemen (1.541) en daar het eerder genoemde percentage van 15% langdurig vacant van nemen, is er een structureel tekort van ruim 230 cybersecurity-professionals met diverse profielen in Nederland. Dit is een zeer voorzichtige schatting omdat we van verschillende grote werkgevers hebben gehoord dat soms tientallen vacatures nooit verschijnen omdat men verwacht ze niet te kunnen invullen. We zijn hierbij ook uitgegaan van de omvang van de arbeidsmarkt van 7.000[11] in 2014 (waar 1.158 vacatures 17% van de banen betreft, wat in arbeidsmobiliteit geen vreemd cijfer is) en niet 16.400[12] (bij 1.158 vacatures zou dat 7% zijn, wat een laag aantal is). Met andere woorden: het tekort van 230 mensen in cyber security zou goed 2 á 3 keer hoger kunnen zijn, zeker wanneer functies waar cyber security slechts een onderdeel van de functie vormt en in andere dan ICT- of veiligheidsdomein wordt uitgevoerd. Om tot 600 extra cybersecurity-professionals te komen (bovenop het huidige aanbod dat onder meer van onderwijsinstellingen vandaan komt) is een grote impuls nodig.

Gezien de verwachte groei van de behoefte aan professionals van 10% per jaar neemt dit tekort de komende twee jaar eerder toe dan af. Er wordt door verschillende onderwijsinstellingen wel groei in studentenaantallen beoogd maar daarin zit een afhankelijkheid van jongeren die moeten willen kiezen voor het vak. Daarnaast is er nog sprake van een ‘slapende olifant’ bij het Midden- en Kleinbedrijf zoals De Haagse Hogeschool treffend zegt. Wanneer de groeiende bewustwording bij het MKB omslaat in actiebereidheid of noodzaak, nemen de tekorten verder toe. Ook de toename

[11] PLATO & Ockham IPS (2014)
[12] SEO/VKA (2016). Economische kansen Nederlandse Cybersecurity-sector.

van bijvoorbeeld cybercrime ten opzichte van reguliere misdaad[13] zal vragen om een forse groei van de vraag om professionals. Dit is nu al zichtbaar bij grote organisaties als Politie[14] en Defensie[15].

Het type professionals dat men zoekt is divers, maar het zwaartepunt van het tekort is op dit moment mensen met een technische achtergrond op HBO niveau. Voor andere typen cybersecurity-profielen is er een groeiende behoefte, de opleidingsmarkt daarvoor is zeer divers en de eisen aan kandidaten ook. Hierdoor is dit segment beperkt transparant en de omvang is op basis van de beschikbare gegevens niet in te schatten.

Gezien de focus op cyber security in de regio Den Haag en het zwaartepunt van het nationale security cluster verwachten we dat het tekort voor 25-30% zijn weerslag vindt in deze regio wanneer we naar specialistische cyber security functies kijken.

[13] https://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk/
[14] High Tech Crime zoekt digitale rechercheurs via crimediggers.nl en https://www.kombijdepolitie.nl/htc
[15] https://www.defensie.nl/onderwerpen/cyber-security/inhoud/defensie-cyber-strategie en de kamerbrief https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/02/23/kamerbrief-over-actualisering-defensie-cyber-strategie/kamerbrief-over-actualisering-defensie-cyber-strategie.pdf

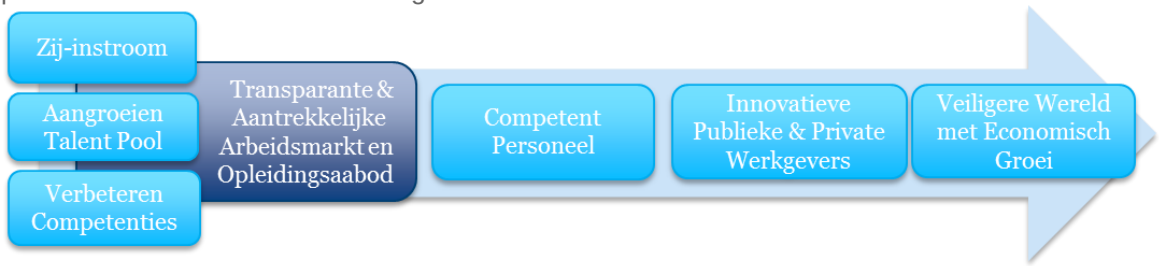
3 Actieplan

3.1 Aanpak HCA Cyber Security

Om tot een oplossing van de diverse knelpunten uit voorgaand hoofdstuk te komen stellen we twee programmalijnen voor:

1. Verbeteren van de aansluiting tussen onderwijs en werkgevers (primair gericht op organisaties).
2. Aantrekken en ontwikkelen van talent (primair gericht op talenten).

Vanuit onderstaand denkraam werken we hieronder deze twee lijnen uit in acties en bijbehorende activiteiten. Hierbij geldt dat de rol van de HSD-office primair geen uitvoerende maar een verbindende, faciliterende, organiserende, uitdragende en soms agenderende, aanjagende en initiatief nemende of ondersteunende is zoals in hoofdstuk 1 beschreven. De genoemde acties en activiteiten zijn op basis van lopende initiatieven, kansrijke ontwikkelingen en dialoog met partners/behoeftestellers tot stand gekomen.



3.2 Programmalijn 1: Verbeteren van de aansluiting tussen onderwijs en werkgevers

3.2.1 Opleidingsaanbod en docentenaantal gericht vergroten

Er is een behoefte aan docenten, zowel gastdocenten als vaste docenten, met inhoudelijke expertise en domeinkennis. Via de netwerken van HSD wordt deze behoefte naar buiten gebracht en wordt via securitytalent.nl de kans gegeven aan aangesloten opleidingsinstituten om hun docentenbehoefte naar buiten te brengen. Op sommige niveaus en inhoudelijke gebieden is er nog een tekort aan opleidingen, reguliere onderwijsinstellingen en trainingsorganisaties spelen hier zelfstandig, soms ondersteund door HSD, op in. Activiteiten zijn:

- Partners van HSD worden individueel benaderd voor het invullen van het tekort aan docenten om tot minimaal vijf extra (deeltijd) docenten te komen in het eerste jaar. Indien noodzakelijk wordt met partners naar innovatieve oplossingen gezocht om barrières weg te nemen. Voorbeelden zijn het bieden van baanzekerheid door een aanstelling bij een detacheerder of gerichte scholing in didactische vaardigheid. Na succes in het eerste jaar en aanhoudende behoefte herhaalt HSD-office deze activiteit in jaar twee. In het kader van P@CT (zie bijlage 3) wordt momenteel het concept ‘De Hybride docent’ uitgewerkt met onderwijs en bedrijfsleven. Docenten zullen naast hun werk in het bedrijfsleven, actief zijn in het onderwijs. Er wordt een nieuwe functie ontwikkeld: de Cyber Security Ambassador.
- Er wordt additioneel scholingsaanbod ontwikkeld door partners van HSD, vaak ondersteund door de Gemeente Den Haag. Via onder anderen de tweede master aan de Cyber Security Academy (HBO+ niveau), de RIF-aanvraag P@CT ROC Mondriaan (keuzemodulen en awareness trainingen, zie bijlage 3), nieuw lectoraat aan de Haagse Hogeschool (Cyber-MKB) en de Hogeschool Leiden (ontwikkeling vakgebied Digital Forensics en e-Discovery) wordt hierin voorzien. Verkend wordt de samenwerking met de Defensie cyber opleidingen. Het aanbod wordt gedeeld en verbonden aan partners waar nodig voor inhoudelijke invulling.
- Een verkenning van samenwerking tussen HBO-instellingen op cyber security onderwijs in de regio. Door specialisatie (in toepassingsgebied of op beroepsprofielen) en samenwerking op de gemeenschappelijke basis kunnen studenten een specifieker opleidingsaanbod krijgen dat meer bij hun interesses aansluit waardoor er minder uitval ontstaat. Ook de meerwaarde van samenwerking met private opleiders (zoals Security Academy, FOX-IT) en gebruik van internationaal erkende certificeringen en beroepsprofielen in het reguliere onderwijs wordt hierin verkend.

3.2.2 Inhoudelijke aansluiting onderwijs met werkgeversbehoefte versterken

Het onderwijs worstelt met de invulling van de opleidingen voor IT en cyber security. De vraag uit de markt groeit onstuimig en vernieuwt snel. De koninklijke route van een opleiding ontwikkelen, formaliseren en accrediteren kost veel tijd. Tussen het moment van ideeën ontwikkelen en studenten afleveren zit als snel 6 – 8 jaar. Dat is voor de snel veranderende cyber security-wereld niet toereikend. Het is voor publieke opleidingen moeilijk de markt en trends in ICT en cyber security goed te volgen en daar flexibel op in te spelen. Tegelijkertijd zijn er tekorten aan specialisten, zowel voor het bedrijfsleven als voor de opleidingen zelf. Samenwerking tussen onderwijs en bedrijfsleven is cruciaal voor het slagen van de inspanningen om het tekort op te lossen. Goede praktijkgerichte docenten zijn moeilijk voor het docentschap te interesseren. Positieve ontwikkelingen in de Haagse regio zijn recent gestarte lectoraten zoals ingevuld door Tracks Inspector bij de Hogeschool Leiden (digital forensics & e-discovery) en door Thales bij de Haagse Hogeschool (cyber security).
Zowel voor kennisoverdracht (trends in cyber security en arbeidsmarkt), het vaststellen van vereisten van werkgevers en samen innovatieve oplossingen voor flexibilisering van het onderwijs te bedenken is praktische afstemming en samenwerking noodzakelijk. Ondersteunende activiteiten zijn:

- Onderwijstafel MBO-HBO voor doorlopende leerlijnen organiseren voor faciliteren van concrete initiatieven. Omdat de algemene trend is dat de behoefte aan hoger geschoold personeel toeneemt ten koste van lager geschoold, is het van belang om de verbinding tussen MBO en HBO te optimaliseren. Hierdoor wordt het gemakkelijker en daarmee aantrekkelijker om door te stromen. Er zal kennis worden genomen van de doorlopende leerlijnen voor cyber security zoals die bij Defensie worden opgezet. HSD zet een netwerk van mensen uit het onderwijsveld in de regio op om de behoefte aan talent en kennisontwikkeling vast te stellen, accentverschillen tussen de opleidingen expliciet te maken en te kunnen werken aan doorlopende leerlijnen. Er wordt gebruik gemaakt van de kennis van dcypher[16] die net een cyber security onderzoek- en onderwijsberaad is gestart voor het HBO en de samenwerking tussen MBO-HBO in P@CT. Dit loopt na opstart gedurende de rest van de periode van deze HCA.
- Actieve aansluiting van meer partners. De Human Capital vraagstukken en activiteiten zoals in deze actieagenda staan blijven zo afgestemd op de actuele behoefte in de sector. Jaarlijks organiseert HSD-office een Human Capital tafel voor HR directieleden van HSD-partners én de directieleden van de bij HSD aangesloten opleidingsinstituten waarin de plannen van de Human Capital Programmeerraad worden besproken, resultaten worden gedeeld en nieuwe input wordt gevraagd. Hiervoor worden ook recente ontwikkelingen in de arbeidsmarkt geïnventariseerd en gepubliceerd in een te ontwikkelen monitor. Waar mogelijk stimuleren we ‘partnerships in education’ tussen werkgevers, publieke en private onderwijsinstellingen. Via ‘cyber challenges’ van werkgevers aan studenten wordt vraag en aanbod bij elkaar gebracht.
- Verkenning taakdifferentiatie MBO-niveau functies en HBO-niveau functies. Er is een duidelijk tekort van cyber security professionals op HBO niveau, maar er lijkt een overschot van ICT-ers op MBO niveau. Dit wordt door partners maar gedeeltelijk herkend. Naast doorstroming stimuleren van MBO naar HBO onderzoeken we met opleiders en werkgevers of taken uit HBO-niveau functieprofielen meer te verdelen zijn over een MBO- en een HBO-niveau profiel. Hiermee kunnen meer MBO’ers in dit veld aan de slag en kunnen HBO’ers effectiever worden ingezet. Deze verkenning wordt in het eerste jaar opgeleverd zodat eventuele vervolgacties kunnen doorlopen in het tweede jaar.

[16] https://www.dcypher.nl/

3.3 Programmalijn 2: Aantrekken en ontwikkelen van talent

3.3.1 Nieuwe instroom van onderop vergroten

Er is op zich een potentieel van studenten met relevante achtergrond, ze kiezen echter niet voldoende voor cyber security. Dit ligt mede aan het beeld van het beroep, de aantrekkingskracht van het onderwijsaanbod en de arbeidsmarkt, en het ontwikkelperspectief. Om de talentpool te laten aangroeien vanuit het reguliere onderwijs zijn de volgende activiteiten noodzakelijk:

- Carrièreperspectieven/loopbaanpaden schetsen. Vanuit het Voortgezet Onderwijs naar het MBO en daarna MBO'ers laten doorstromen naar HBO via het P@CT-project (zie bijlage 3). In overleg met het onderwijsveld en private opleiders in de regio Den Haag gaan we de doorlopende leerlijnen identificeren en delen met studenten. Bij opleidingen in cyber security vragen we opleiders wat een logische vervolgopleiding kan zijn waar dat nog niet aangegeven is. Beroepsprofielen worden in relatie tot elkaar beschreven zodat loopbaanpaden inzichtelijker worden voor studiekeuze. Dit wordt in een notitie gedeeld in jaar 2. Met een aantal werkgevers, opleiders en ondersteunende partijen die regelmatig talent uit het buitenland (helpen te) halen wordt verkend of acties onder de vlag van HSD van toegevoegde waarde zijn.
- Aantrekkelijk en transparant onderwijsaanbod realiseren. We maken het onderwijs/scholingsaanbod van partners relevant voor cyber security overzichtelijk en gemakkelijk doorzoekbaar. Binnen het eerste jaar is dat volledig, zolang ook de partners daaraan meewerken. Samen met dcypher[17] doet HSD-office dat ook breder voor het relevante HBO/WO opleidingsaanbod van onderwijsinstellingen die geen partner zijn en met onder meer het Paars Partnerschap voor het landelijke MBO met als ambitie 95% compleet binnen twee jaar. Dit wordt ontsloten via securitytalent.nl.
- Beeldvorming beroep verrijken om meer talent aan te trekken en te behouden. Via landelijke en regionale programma's wordt de vijver van technici vergroot (zoals Techniekpact[18] en Wetenschapsknooppunten[19]). We maken testimonia voor beroepsprofielen die relevant zijn voor cyber security en aansprekend voor een brede doelgroep. Dit verspreiden we landelijk naar het Primair- en Voortgezet Onderwijs via VHTO en Platform Bèta Techniek en werken samen met ECP/Dutch Digital Delta. In de regio Den Haag bieden we het als voorlichtingsmateriaal aan bij MBO, HBO en WO binnen passende opleidingen. Ook voor de om- en bijscholers alsook zij-instromers komt dit beschikbaar. Door de testimonia te laten inbedden in de onderwijsprogramma's (ook van Primair- en Voortgezet Onderwijs) via de actieagenda HA!-Tech wordt de impact vergroot. Voor de realisatie is input nodig van beroepsverenigingen (zoals het Platform voor InformatieBeveiliging), professionals om te portretteren via de partners en samenwerking met de andere genoemde partijen. De materialen worden in het eerste jaar ontwikkeld en de verbindingen met de bestaande infrastructuur worden geborgd. Deze activiteit is er een van de lange adem waar we direct mee starten maar die zijn invloed pas op langere termijn zal hebben.

3.3.2 Competenties verbeteren

Mede door de toenemende digitalisering is security een dynamisch vakgebied dat zich in rap tempo ontwikkelt en voortdurend verandert. Dit vraagt van professionals, zeker op het gebied van cyber security, dat zij hun kennis en competenties actueel houden. Kortom, security professionals moeten in staat zijn om een leven lang te leren. Daarvoor is het noodzakelijk om a) te weten welke competenties door werkgevers worden gevraagd (beroepsprofielen) en b) het aanbod van (contract)onderwijs en bijscholing te ontsluiten voor werkgevers. Hiervoor worden de volgende activiteiten gerealiseerd:

- Ontsluiten van het aanbod (contract)onderwijs en bijscholing in relatie tot beroepen en vacatures. Op securitytalent.nl zal een actueel overzicht worden gegeven van de opleidingen in Nederland met betrekking tot bijscholing en competentieontwikkeling op het gebied van IT en cyber security. Securitytalent.nl zal (geaccrediteerde) opleidingen weergeven die worden verzorgd door publieke onderwijsinstellingen en die verbinden met beroepsprofielen en vacatures van partners waar die bekend zijn. Voor private- en commerciële opleidingen geldt

[17] Een initiatief van NWO en de Ministeries V&J, EZ en OCW
[18] http://www.techniekpact.nl/
[19] Wetenschap & Technologie in het basisonderwijs http://www.wetenschapsknooppunten.nl/

dat aanbieders lid moeten zijn van HSD. Met deze activiteit is al gestart en dit groeit de komende twee jaar door.

- Beschikbaar stellen van actuele beroepsprofielen met heldere eisen aan kennis en competenties. HSD inventariseert 8 beschikbare beroepsprofielen voor IT en cyber security die via securitytalent.nl worden ontsloten. Hiervoor wordt o.a. samengewerkt met het Platform voor Informatie Beveiliging en de onderwijsinstellingen en certificeerders. De beroepsprofielen sluiten waar mogelijk aan bij standaarden zoals het e-Competence Framework[20] van de Europese Commissie. Waar nog niet gebeurd worden de gehanteerde profielen getoetst bij partners. We starten met delen en gebruiken in jaar 1 en passen daarna waar nodig aan (bijvoorbeeld vanwege actuele ontwikkelingen).
- Drempel tot het ontwikkelen van competenties verlagen. Door het cursusaanbod overzichtelijk en doorzoekbaar te presenteren in combinatie met de mogelijkheden tot financiering van (bij)scholing te ontsluiten via een scholingssubsisiewijzer verlagen we met onze partners de drempels tot het volgen van een cursus of opleiding. Onderzocht wordt of het concept van ‘train de trainer’ binnen bestaande opleidingen en cursussen kan worden meegenomen, door mensen met kennis van cyber security dit actiever te laten uitdragen wordt de cyber awareness van de massa vergroot. We laten online (zoals Massive Online Open Courses, MOOCs), on-site en maatwerk scholing van partners nadrukkelijker zien zodat diversiteit in onderwijsvormen inzichtelijk wordt voor het einde van het eerste jaar.

3.3.3 Zij-instroom en omscholing stimuleren

In de huidige markt is er een tekort aan IT en cybersecurity-talent. Daarom is de wens van HSD-partners om de pool met talent ook te vergroten met zogenaamde ‘hidden treasures’; talenten met een ICT achtergrond die niet in de security sector werken, maar die na beperkte bij- en/of omscholing geschikt kunnen zijn om dat wel te doen. Het realiseren van een transparante en attractieve arbeidsmarkt is hiervoor één middel om talent te interesseren in de security sector. Meer gericht is het identificeren van potentieel talent dat nu al beschikbaar is en door middel van bijscholing (beperkt, maximaal 1 jaar) aan de slag kan als cybersecurity-professional. Dit gebeurt door:

- Werkzoekenden met ICT ervaring om te scholen/certificeren naar cybersecurity-specialist. Door de digitale transitie komen op dit moment veel werkzoekenden beschikbaar die geschikt kunnen zijn, bijvoorbeeld uit de bankensector. Denk aan projectmanagers ICT, ICT help- en servicedesk medewerkers, service engineers, etc. Samen met partners van HSD en aanbieders van beschikbaar talent (zoals UWV, gemeenten) wordt 1 pilot geïnitieerd om een pool van 10 tot 20 werkzoekenden te selecteren, op te leiden en te plaatsen als cybersecurity-deskundigen bij de partners van HSD aan het einde van het eerste jaar. Op dit moment vinden al gesprekken plaats met de Haagse Hogeschool en het UWV om een dergelijke pilot op te starten (zie bijlage 4). Bij een succesvolle pilot onderzoeken we of dit uit te breiden is naar een grotere pool en hogere frequentie.
- We maken andere initiatieven tot omscholing succesvol door bij te dragen in kennis, netwerk van werkgevers of publiciteit. Voorbeelden zijn de New York Coding + Design Academy die samen met Fortress werkzoekenden willen omscholen naar cybersecurity-professional en de Hogeschool van Amsterdam die dit verkent binnen het programma Make-IT-Work voor cyber security. Dit doen we gedurende de looptijd van de HCA waar het zich aandient.

[20] http://www.ecompetences.eu/

3.4 Uitvoering

Deze Human Capital Actieagenda Cyber Security beschrijft de activiteiten op hoofdlijnen die gaandeweg verder ingevuld of geoperationaliseerd moeten worden, het is een rollende agenda. Per programmalijn volgt een uitvoeringsplan met betrokken partijen, hun activiteiten en bijdragen. De HSD-office levert 0,4 FTE van een programmamanager met Human Capital in portefeuille en 0,8 FTE ondersteuning door een projectcoördinator per jaar. Bij hen ligt als belangrijkste taak het activeren van partners voor de programmalijnen waar nodig, initiëren/organiseren van nieuwe concrete projecten en het informeren van het bestuur en de partners over de voortgang. Daarnaast realiseren en onderhouden zij de ondersteunende infrastructuur van securitytalent.nl. Van de uitvoeringsplannen bewaken zij de deadlines en oplevering. Belangrijk element bij de meeste activiteiten is een sterke, intensieve en structurele samenwerking tussen onderwijs, bedrijfsleven en overheid. Vanuit HSD is daar een sterke basis voor.

Voor sommige van de beschreven activiteiten is al projectfinanciering of subsidie beschikbaar (bijvoorbeeld P@CT, zie bijlage 3), voor anderen ligt die in ieder geval gedeeltelijk in het verschiet via bestaande regelingen (zoals voor bijscholing werklozen, zie bijlage 4). Er zullen directe kosten zijn voor het verzorgen van materiaal, onderhoud en doorontwikkeling van securitytalent.nl en organisatie van bijeenkomsten (zoals een Human Capital- en onderwijstafel). Een deel van activiteiten is nog niet ver genoeg geoperationaliseerd om een kosteninschatting te maken (bijvoorbeeld het ontwikkelen van een monitor). De begroting en partnering worden na inhoudelijke vaststelling verder geconcretiseerd in het uitvoeringsplan met de betrokken partners. Daarbij wordt goed gebruik gemaakt van de diverse expertises van de partners, zoals die ook is gebruikt in de ontwikkeling van deze Actieagenda.

Bijlagen

Bijlage 1: Geraadpleegde organisaties

HSD heeft veel partijen gesproken die daarmee van invloed zijn geweest op de inhoud van deze agenda. In het bijzonder hebben de volgende organisaties bijgedragen aan het huidige document:

- Cyber Security Academy
- dcypher
- ECP/Dutch Digital Delta
- Fortress
- Fox-IT
- Gemeente Den Haag
- Haagse Hogeschool
- KPN
- ROC Mondriaan
- Security Academy
- Security & Continuity Institute (SECO)
- TU Delft

Bijlage 2: Brondocumenten

- Arbeidsmarkt voor Cyber Security Professionals, PLATO & Ockham IPS i.o.v. WODC.
- Economische kansen Nederlandse CyberSecurity-Sector, SEO/VKA i.o.v. minEZ.
- Plan van Aanpak P@CT, ROC Mondriaan.
- Human Capital Agenda ICT, Dutch Digital Delta/ECP.
- State of cybersecurity, ISACA/RSA.
- Beroepsprofielen InformatieBeveiliging, Platvorm voor InformatieBeveiliging.
- HSD 0-meting 2015, The Hague Security Delta.

Bijlage 3: Project 'Partners in @ction for Cyber Talent' (P@CT)

P@CT, Partners in @ction for Cyber Talent, het nieuwe samenwerkingsverband op het terrein van cybersecurity in de regio Den Haag, gaat voor goed geschoolde cyber-professionals: studenten, werkenden en docenten. P@CT zet in op cyber-awareness in alle beroepen en voor up-to-date cyber-onderwijs in doorlopende leerlijnen die we gezamenlijk met onderwijs, bedrijven en overheden ontwikkelen en uitvoeren.

Deelnemende organisaties

Partners P@CT				
Arbeidsorganisaties	**Gemeenten**	**Onderwijs**	**Samenwerking met**	**Steunbetuigingen**
the Hague Security Delta	Gemeente Den Haag	ROC Mondriaan	MRA ROC Amsterdam	PvIB - Platform voor informatiebeveiliging
Leids Universitair medisch centrum (LUMC)	Gemeenten in Haaglanden*	Haagse Hogeschool	Cyber Securitiy Reseach and Education platform (NWO)	Topsector dutch digital delta
Deloitte		Centre of Expertise Cybersecurity		
Siemens		Hofstad mavo havo		
Fortress Group		Corbulo College		
UNO2Cloud		Scholen Combinatie Delfland		
Institute For Financial Crime				
Menskracht 7				
TNO				
Abn Amro				
Gemeente Den Haag afd. ICT				
* Geslaagd in het vak 2.0*: is ondertekend door door de gemeenten in de regio Haaglanden. Daarmee wordt speerpunt 8 van Geslaagd in het vak 2.0: Aantrekkelijker maken van en Leren en Ontwikkelen in de ICT, onderschreven door de aangesloten gemeenten.*				

Partners variëren van ICT-bedrijven, een instelling in de zorg, tot bedrijven in de industrie, adviesorganisaties en overheden. De impact van cybersecurity wordt door allen gevoeld. Met elke partner is in de samenwerkingsovereenkomst afspraken gemaakt wat de specifieke inbreng in de gezamenlijke ontwikkeling en uitvoering is. Deze inbreng varieert van het leveren van faciliteiten, gastdocenten tot cyberstages voor studenten en hybride arbeidsplaatsen voor docenten.

Omvang (2016-2020)

Dekking begroting 2016-2020		Totaal
Gemeente Den Haag (subsidie)		€ 380.000
Arbeidsorganisaties		€ 475.668
Hbo		€ 71.467
Vo		€ 21.900
Subsidie RIF		€ 474.500
SUBTOTAAL		**€ 1.423.535**
Eigen inzet ROC Mondriaan		€ 85.223
Gemeente Den Haag (in kind)		€ 58.400
TOTAAL		**€ 1.567.158**

Doelstellingen

Voor de realisatie van onze ambities maakt P@CT werk van de volgende doelstellingen:

1. Inrichten en organiseren van het kennisuitwisselingsplatform ten behoeve van innovatie van het cybersecurity onderwijs met de focus op het mbo.
2. Een op de arbeidsmarkt afgestemde uitstroom én een vergrote, kansrijkere doorstroom naar het hbo. Door middel van het versterken van kennis en vaardigheden van mbo ICT studenten op het gebied van Cybersecurity, niveau 4 en het ontwikkelen van een doorlopende leerlijn cybersecurity (de Cyberroute) vo-mbo-hbo.
3. Het vergroten van awareness cybersecurity in andere mbo-beroepsopleidingen die toe geleiden naar de arbeidsmarkt, waar cybersecurity om aandacht vraagt.
4. Het realiseren van voldoende en kwalitatief goede praktijkopdrachten en stages voor studenten waar studenten in een combinatie van leren en werken praktijkervaring opdoen.
5. Kwaliteit voor de klas: Docenten professionaliseren met input en inzet van het bedrijfsleven.

6. Leven lang leren: Werkenden op mbo-niveau en werkzoekenden houden hun kennis en vaardigheden continue op actueel niveau.

Bereik & Planning

Het bereik en de planning hieronder is afkomstig van het ingediende plan voor de RIF-aanvraag van januari 2016.

	Aantallen leerlingen	**Bereik**
Cybersecurity voor ICT professional	- ROC Mondriaan heeft binnen de ICT-opleidingen 260 leerlingen op niveau 4. - Het totaal van ICT-opleidingen niveau 2, 3 en 4 bedraagt 452. - Jaarlijks stromen daarvan op dit moment 28 studenten met een niveau 4 diploma door naar het hbo en 22 studenten niveau 4 direct naar de arbeidsmarkt om als ITC professional werkzaam te zijn. Dat betekent dat 56% doorstroomt en 44% gaat werken. - Binnen de gehele regio gaat het om totaal ca 700 niveau 4 studenten verdeeld over de 3 ROC's: Mondriaan, ID College en ROC Leiden.	- Op termijn wil P@CT alle leerlingen in de ICT-opleidingen op niveau 4 binnen ROC-Mondriaan de keuzedelen voor cybersecurity professionalisering bieden. - Daarnaast kunnen ook de andere ROC's een beroep doen op de keuzemodulen.
Cybersecurity voor andere sectoren	ROC Mondriaan heeft naast de ICT-opleidingen ook nog ca 15.000 leerlingen in de andere sectoren als economisch administratief, zorg, metaal, elektronica/installatie, bouw, orde en veiligheid.	Tijdens de projectperiode van 4 jaar wil P@CT 700 studenten opleiden met awareness modules. Uiteraard kan dit bereik op termijn worden vergroot, zeker als de inzet wordt opgenomen in het reguliere programma van deze opleidingen.

Producten en bereik	**Fase 0**	**Fase 1**	**Fase 2**	**Fase 3**	**Fase 4**	**Fase 5**
	t/m 1 febr 2016	**feb 2016 Sep 2016**	**Sep 2016 Sep 2017**	**Sep 2017 Sep 2018**	**Sep 2018 Sep 2019**	**2019 - 2024**
3 keuzedelen MBO niveau 4: 2 keuzedelen in ICT Beheer 1 keuzedeel in ICT Applicatie Ontwikkeling	Aanvraag en ontwikkelen	Ontwikkelen	ICT Beheer: Pilot met 1 keuzedeel voor 25 studenten	ICT Beheer: Keuzedeel 1 voor 45 studenten; Pilot ICT Beheer Keuzedeel 2 voor 25 studenten; Pilot ICT Applicatie keuzedeel voor 25 studenten	ICT Beheer: Keuzedeel 1 voor 60 studenten; ICT Beheer Keuzedeel 2 voor 60 studenten ICT Applicatie Keuzedeel voor 45 studenten	Professionele organisatie
Awarenessmodule voor VO ihkv doorlopende leerlijn cyber startend in VO	Behoefte onderzoek	Ontwikkelen	Pilot in 3 VO-scholen: 10 leerlingen/school; Doorontwikkeling	3 VO scholen: 15 leerlingen per school	4 VO scholen: 60 leerlingen totaal	Professionele organisatie
Awareness-modules andere niet ICT gerelateerde MBO opleidingen	Behoefte onderzoek	Plaats in curriculum bepalen en ontwikkelen	Pilot MBO niveau 2 ICT beheer voor 25 studenten; Niet-ICT gerelateerde	MBO niveau 2/3 ICT beheer voor 50 studenten Uitbreiding naar 6 MBO opleidingen: 200 studenten	MBO niveau 2/3 ICT beheer voor 100 studenten Inzet niet ICT gerelateerde opleidingen: 400 studenten	Professionele organisatie

			opleidingen: Pilot in 4 opleidingen: 100 studenten			
Awareness module voor bedrijven	Behoefte onderzoek	Ontwikkelen	Ontwikkelen	Pilot van module in 3 bedrijven	5 bedrijven	Professionele organisatie
Opscholing van werkenden en werkzoekenden met ICT gerelateerde keuzedelen op maat	Onderzoek	Onderzoek en start ontwikkelen	Ontwikkelen	Pilot voor 3 bedrijven	Open zetten naar de markt	Professionele organisatie
Docenten scholing	Voorbereiding gedifferentieerd aanbod	Scholing ontwikkelen en uitvoeren voor 5 docenten	10 docenten	15 docenten	Alle betrokken docenten	
Hybride werknemer		Onderzoek	Ontwikkeling en pilot	Inzet	Verdere inzet	
Docenten stages		Voorbereiding en Ontwikkelen	3 MBO en 3 VO docent-stages	5 MBO en 3 VO docentstages	Alle betrokken docenten	
Studenten stages Naast reguliere ICT-stages	Voorbereiding	Ontwikkelen	15 MBO studentstages	30 MBO studentstages	50 MBO studentstages	
Cyber@ctionlab	Voorbereiding	Ontwikkelen en invulling	Doorontwikkeling	Cyber@ctionlab vol In gebruik	Cyber@ctionlab vol In gebruik	Professionele organisatie
Platform voor kennisuitwisseling en innovatie		Voorbereiding en eerste activiteiten	Activiteiten op basis van plan	Activiteiten op basis van plan	Activiteiten op basis van plan	Activiteiten op basis van plan
@ccess2Talent		Onderzoek	Ontwikkeling op basis van onderzoek	Verdere uitrol	Verdere uitrol	

Bereik	**Fase 0**	**Fase 1**	**Fase 2**	**Fase 3**	**Fase 4**	**Fase 5**
	t/m 1 febr 2016	**feb 2016 Sep 2016**	**Sep 2016 Sep 2017**	**Sep 2017 Sep 2018**	**Sep 2018 Sep 2019**	**2019 - 2024**
Succesvollere doorstroom naar hbo		Onderzoek en plan	Activiteiten op basis van plan	Activiteiten op basis van plan	Activiteiten op basis van plan	Activiteiten op basis van plan
Partners: Bedrijven en Overheden		20	25	35	40	
Gastcolleges, workshops, masterclasses	Voorbereiden	Totaal 18	Totaal 30	Totaal 40	Totaal 50	
Digitale leeromgeving	Onderzoek	Ontwerp	Ontwikkeling	Pilot	Uitrol	

Bijlage 4: Initiatief zij-instroom Cyber Security

Aanleiding

Er is een tekort aan cybersecurity professionals op de arbeidsmarkt. Hier tegenover staat dat er een groot aantal ICT'ers momenteel werkloos thuis zit (bijna 7.000 in de WW, cijfers april 2016). De ervaring op het werkterrein van ICT maakt dat er in potentie een aanzienlijke groep werklozen via een bij- of omscholingstraject kan worden ingezet als cybersecurity professional. Er zijn succesvolle voorbeelden waarin werklozen worden omgeschoold tot ICT-er, zoals PION in het verleden en op dit moment Make IT Work voor JAVA-programmeurs in de metropoolregio Amsterdam. Redenen voor HSD om dit voor cyber security in de regio Den Haag met partners te initiëren. HSD, de Haagse Hogeschool en het UWV zijn al gestart om een pilot op te zetten. Andere partners, zoals de CSA en de Gemeente Den Haag hebben al aangegeven bij te willen dragen.

Aanpak

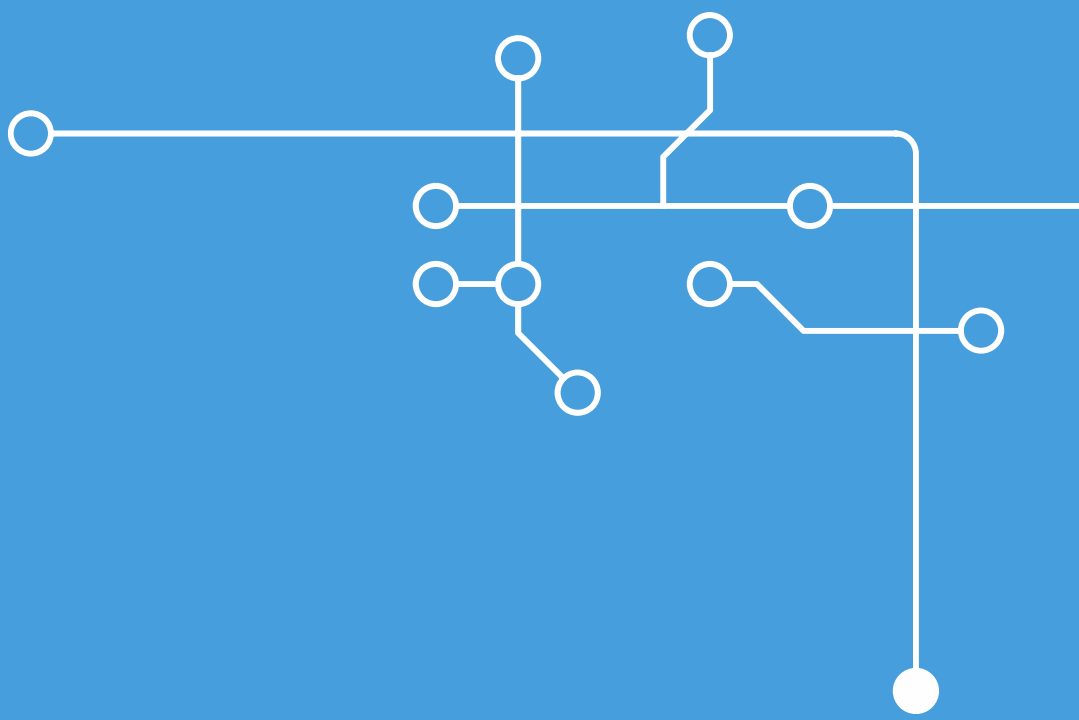
Het UWV selecteert werklozen van 45 jaar en ouder met (relevante) ICT-ervaring die in aanmerking komen voor omscholing tot cybersecurity professional en werkeloze HBO/WO opgeleiden die omgeschoold willen worden. Het opleidingsprogramma dat de geselecteerden zullen volgen wordt samengesteld na overleg met werkgevers (De Haagse Hogeschool is hiermee al gestart). Na een aantal maanden 'werkend leren' bij de Hogeschool en een aantal maanden 'lerend werken' bij een beoogd werkgever kunnen deze werklozen straks aan het werk als cybersecurity experts.
De financiering wordt waarschijnlijk verzorgd door verschillende partijen (in cash en in kind). Het UWV zal een overzicht maken van subsidiegelden die gebruikt kunnen worden voor het inzetten voor opleidingskosten en de projectorganisatie.

Planning

Overleg tussen HSD, UWV en Haagse Hogeschool is dusdanig gevorderd dat er begin 2017 een selectie van bedrijven zal worden uitgenodigd bij de HSD waaraan het omscholingsproject Cyber Security Professionals zal worden gepresenteerd. Hier zullen ook een aantal kandidaten uit de doelgroep werkloze ICT medewerkers van 45+ en werkloze HBO/WO'ers uitgenodigd worden. In afstemming met de bedrijven die worden uitgenodigd zal ook het profiel waar de toekomstige cybersecurity professionals aan moeten voldoen worden vastgesteld. In de loop van 2017 moet het opleidingstraject starten voor een pilotgroep van 10 á 20 personen die dan binnen een jaar aan het werk kunnen.

Beoogd rendement

Er zijn verschillende HSD partners gebaat bij dit project. Ten eerste de directe betrokken organisaties. Het UWV omdat zij langdurig werklozen een kans kan bieden om weer te participeren in de arbeidsmarkt. De gemeente Den Haag zal eveneens een groep werklozen weer kunnen introduceren op de arbeidsmarkt. Naast de sociale meerwaarde van het herintroduceren van werklozen op de arbeidsmarkt is er voor het UWV en de gemeente ook een financieel gewin doordat zij minder uitkeringen hoeven uit te keren. Voor de Haagse Hogeschool zit er naast het maatschappelijk verantwoord ondernemen ook een verdienmodel achter het verzorgen voor de opleidingen. Daarnaast is voor alle partners van HSD die actief zijn op het gebied van cyber security sprake van een toename van geschoold personeel op de nu krappe arbeidsmarkt.



The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
070 204 51 80

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL