Auteurs: Rik van Dijk en Nicole van Deursen zijn onderzoekers bij het NCSC en zijn bereikbaar via research@ncsc.nl.

Tekort op de arbeidsmarkt: vele oplossingen voor een onduidelijk probleem

Je hoort vaak dat er een tekort is aan goede securityspecialisten. Zo meldt het (ISC)² in de 2021 Workforce Study dat er alleen al in Nederland 22.000 vacatures zijn. De oplossing wordt vaak gezocht in het opstellen van beroepsprofielen en het ontwikkelen van opleidingen en trainingen. Hoe helpen competentieprofielen om vacatures te vervullen? Moeten werkgevers en opleiders zich vastpinnen op die profielen? Is het verstandig dat werkgevers zoeken naar werknemers met een lijst certificaten op hun LinkedInprofiel? En waaraan precies hebben we eigenlijk een tekort?

De Cyber Security Skills Shortage is een onderwerp waar de afgelopen jaren over is gesproken en geschreven. Het overheersende idee is dat het ontbreekt aan bekwame specialisten die Nederland kunnen verdedigen tegen het snel toenemende aantal digitale aanvallen. Ook over de grens wordt het ontbreken van geschikte specialisten gezien als een groot probleem. Uit onderzoek van het International Information System Security Certification Consortium (ISC)² een bekend opleidingsinstituut dat onder andere de populaire CISSP training aanbiedt, ziet 63% van hun respondenten dat er een personeelstekort is (1).

Opleidingen

Onderwijsinstellingen spreken vaak met werkgevers over de inhoud van opleidingen en bieden zo wellicht aanknopingspunten om te reflecteren welke behoeftes er zijn op de arbeidsmarkt. Zo dacht ook ENISA die in november 2021 een rapport publiceerde over de kloof in de Europese Unie tussen de vraag naar revelante cybersecurityvaardigheden en het huidige aanbod van deze vaardigheden (2). Daarin laat ENISA zien dat de huidige studies ruimschoots technische vaardigheden aan studenten aanbieden. Gemiddeld gaat bijna 50% van de studiepunten naar technische vakken, gevolgd door een categorie overig, waar onder andere onderzoeksvaardigheden onder vallen. Op de derde plek staat de categorie organizational, risk management, business compliance met 12% van het aanbod. Daarmee zou je zeggen dat het huidige aanbod van studies en met een focus op technische vaardigheden, we hard op weg zijn het gat te dichten? Alleen wat ook weer ontbreekt in het rapport is een duidelijke omschrijving waar precies de vaardighedenkloof in de EU uit bestaat.
De jaarlijkse (ISC)² Workforce Study biedt meer houvast. Volgens dit onderzoek zijn de meest gevraagde kennisgebieden:

- Cloud Security (40%);
- Risk assessment, analysis and management (26%);
- Artificial intelligence/machine learning (25%);
- Governance, risk management and compliance (GRC) (24%);
- Threat intelligence analysis (22%).

Kijken we naar het aanbod van de cybersecuritystudies dan zien we hier dus een mismatch ontstaan. Het meest gevraagde kennisgebied, cloudsecurity, is pas sinds een aantal jaar sterk in opkomst. De kennisgebieden risicomanagement en governance raken sterk aan economische en bestuurskundige studies, niet aan technische opleidingen. Zelfs threat analysis bestaat voor grote delen uit niet-technisch gerelateerde onderwerpen, zoals internationale betrekkingen en militaire studies. De meest gevraagde kennisgebieden uit de (ISC)² studie en uit analyses van vacatures (3) genereren het beeld dat een cybersecurity expert dus een soort alleskunner moet zijn.

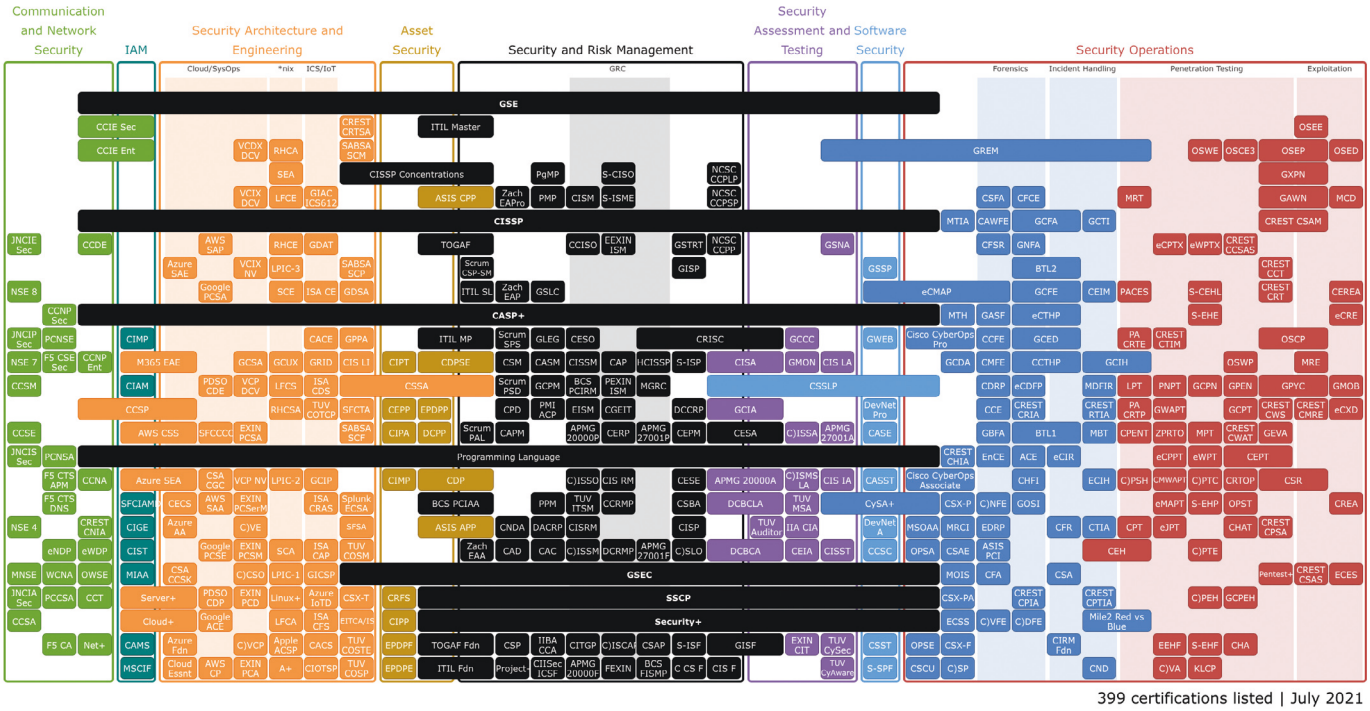
Certificeringen

Hoe moeten we dat soort diamanten dan vinden? Veel organisaties grijpen naar certificering als een proeve van bekwaamheid. Om een CISSP of CISM certificering te dragen moet je vijf jaar ervaring hebben. De certificeringen behandelen onderwerpen uiteenlopend van het Lapadula-Bell model (Don't Read Up!) tot aan Kernel Security. Alleen, het hoofdstuk Cloud Security, volgens (ISC)² het meest gevraagde kennisdeel door werkgevers, is net drie pagina's lang. Onderwerpen als Threat Intelligence Analysis of AI worden omschreven maar het hoe en wat blijft achterwege. Toch geldt CISSP vaak als harde eis om een baan in het vakgebied te vinden. De focus van werkgevers op CISSP is opmerkelijk: er zijn honderden mogelijke certificeringen, waardoor er voor iedereen wel mogelijkheden zijn om relevante kennis op te bouwen. Voor verzamelaars van certificaten hebben we het overzicht van Paul Jerimy bijgevoegd, hij heeft inmiddels 399 mogelijke certificeringen in kaart gebracht, zie afbeelding 1 op pagina 10.

Toch gaan er veel stemmen op voor certificeringen van professionals. Iedereen kan zich informatiebeveiligings- of cybersecurityprofessional noemen, dus een erkende vorm van bewijs kan wel helpen om charlatans in je organisatie te vermijden. In het Verenigd Koninkrijk is recentelijk een publieke consultatie gestart (4) over de behoefte aan helderheid van professionele standaarden en carrièrepaden, zoals we die kennen voor accounting of juridische beroepen. Met de antwoorden hopen ze meer inzicht te krijgen in de beroepsgroep.

Competentieprofielen

Certificeringen, opleidingen en competentieprofielen gaan hand in hand. Omdat er van alles en nog wat lijkt te vallen onder de noemer 'cybersecurity' kunnen we tientallen uiteenlopende profielen vinden. Alleen al het NICE framework van de US National Institute of Standards and Technology (NIST) telt 52 functies over 33 specialistische werkvelden (5). Het vakgebied is breed en een multidisciplinair samenspel van diverse beroepen. Dit zie je bijvoorbeeld ook terug in de mogelijke carrièrepaden, waar een IT-opleiding al lang geen vereiste meer is om aan de slag te gaan. Carrièrepaden zijn hierdoor



Afbeelding 1 - Een overzicht van certificeringen. Bron: https://pauljerimy.com/security-certification-roadmap/.

geen vaste routes en het van tevoren kiezen van de 'juiste' opleiding voor je carrière is een lastige opgave. We vragen ons af of we niet te veel proberen om allerlei taken en rollen in hokjes te stoppen? Of is het juist een teken van groeiende volwassenheid van het vak?

Het QIS framework van het PvIB (6) is een goede start voor organisaties om voor zichzelf in kaart te brengen wat ze echt nodig hebben. Het is echter niet helemaal toereikend voor een multidisciplinair team waarin je bijvoorbeeld ook incident response doet of OT-beveiliging. De profielen beschrijven bijvoorbeeld wel functies die plannen maken voor incident management, maar er staat geen profiel in voor de mensen die daadwerkelijk de incidenten onderzoeken en oplossen. Kaders beschreven door andere organisaties kunnen dat aanvullen, hoewel die soms weer naar heel veel detail doorslaan. De beschrijvingen verschillen sterk in aantal functies per werkveld en diepte waarin functies worden uitgeschreven. Het NICE framework is bijzonder uitgebreid en gedetailleerd en geeft ook carrièrepaden weer. Commerciële partijen zoals SANS bieden ook diensten aan om te helpen bij het beschrijven van gewenste teamrollen en (uiteraard) de bijbehorende (dure) GIAC certificeringen (7).

Vaardigheden versus inhoudelijke kennis

Recruiteren op wat mensen al inhoudelijk weten kan helpen om enkele plekken te vullen op korte termijn. Voor de lange termijn moeten werkgevers ook inzetten op het om- en bijscholen van mensen en het werven op vaardigheden in plaats van kennis. Dit is een aanpak van lange adem, maar wel op termijn een duurzame: je houdt de mensen enthousiaster, up-to-date en hopelijk langer in dienst. Dit heeft ook gevolgen voor hoe opleidingen in elkaar zitten: het ontwikkelen van analytisch denken, problemen oplossen en hoe je zelfmanagement doet, vraagt om specifieke lesmethoden. Reflecterend op de huidige staat van opleidingen en certificeringen zien we een enorme focus op (technische) kennisopbouw, waarbij we proberen te komen tot een soort holistische cybersecurity expert die zowel kan pentesten, de pentestresultaten duidelijk aan het management kan uitleggen, geopolitieke dreigingen kan duiden, verschillende risicomanagementmethoden kan toepassen en ook de organisatiestructuur goed neerlegt. Het is toch of je aan een Europees Recht expert vraagt de verdediging van je moordzaak op zich te nemen: hoogstwaarschijnlijk een slecht idee.

Naam	Werkveld	Aantal beschreven profielen	Bron
PvIB QIS	Informatiebeveiliging	6	(6)
Security Delta	Safety & Security	48	(10)
CSA Singapore	OT security	15	(9)
NICCS – CISA (NICE)	Cybersecurity	52	(11)
SANS GIAS certificeringen	Cybersecurity	43	(12)
EN16234-1:2019 e-Competence Framework (e-CF).	ICT	42 ICT profielen, waarvan 2 informatiebeveiliging	(13)

Tabel 1 - Overzicht van enkele bronnen voor competentieprofielen.

Bijkomend probleem is dat ons vak niet is losgezongen van de sectoren, domeinen en organisaties die digitale beveiliging nodig hebben. De noodzaak tot domeinkennis is misschien het meest evident in het Operational Technology (OT) Security gebied. Een onderzoek uitgevoerd door Secura in opdracht van het NCSC (9) toont aan organisaties met OT-netwerken het meest waarde hechten aan domeinkennis, bijvoorbeeld het begrijpen van de processen en risico's rondom sluizen in de watersectoren, de werking van chemische processen in de olie en chemie sector. Uit het onderzoek blijkt dat het begrijpen van operationele risico's en deze kunnen vertalen naar bedrijfsafwegingen waardevoller is dan pure technische kennis.

Ook een uitgebreid onderzoek van de Cyber Security Agency (CSA) van Singapore (10) naar OT-securityrollen laat zien dat technische kennis over bijvoorbeeld cryptografie en netwerk security wenselijk is. Echter, net zo belangrijk is dat de medewerker probleemoplossend kan denken, goed kan communiceren, buiten zijn of haar comfortzone moeten kunnen stappen en over analytisch vermogen beschikt. Kortgezegd blijkt uit zowel het Secura onderzoek als die van CSA dat een focus op puur technische verworvenheden niet leidt tot de meest geschikte expert.
Een focus op certificeringen en technische vaardigheden verhoogt daarnaast de drempel voor mogelijk nieuwe medewerkers uit andere vakgebieden. Hiermee krijgt gemotiveerd talent moeilijk voet aan de grond omdat ze een certificering missen, terwijl ze deze kennis on the job net zo goed opdoen. Het omgekeerde is ook waar. Zwaar overgekwalificeerde specialisten met meerdere certificeringen en een studie op zak, worden aan het werk gezet als generalisten. Iemand die malware analyse heeft gestudeerd, meerdere certificeringen over het onderwerp heeft gehaald, wordt hoogstwaarschijnlijk niet gemotiveerd om aan een bestuur zonder enige cybersecurity kennis te moeten pleiten voor een hoger securitybudget.

Hoe moet het verder?

Het gebrek aan duiding van het uiteenlopende probleem 'tekort aan cybersecurity mensen' heeft ook tot gevolg dat voorgestelde oplossingen veelsoortig zijn. De verschillende bronnen voor dit artikel geven een aantal richtingen. Bijvoorbeeld ENISA suggereert drie type algemene acties die een overheid kan nemen om de tekorten aan te pakken:

- Kennis en awareness verbeteren in de samenleving, zowel in basis onderwijs als in voortgezet onderwijs;
- Verbeteren van opleidingen in hoger onderwijs en studenten stimuleren om in cybersecurity te gaan werken;
- Organiseren van cybersecurity oefeningen en challenges om jong talent te laten oefenen.

Competentieprofielen kunnen hierbij een houvast geven, maar gebruik ze vooral ter inspiratie voor je eigen functiehuis binnen je specifieke domein.

(ISC)² stelde de vraag aan professionals, die zeggen:

- Leg de nadruk op ontwikkelen en behoud van de mensen die je al hebt;
- Neem initiatieven voor recruitment en aanmoedigen van toekomstige medewerkers;
- Investeer in AI/ML en overige automatisering van processen.

Wij dragen graag bij aan de hoeveelheid mogelijke oplossingen en voegen er nog drie toe voor organisaties:

- Organiseer je organisatie. Inventariseer concreet wat je nu echt nodig hebt en stapel niet verschillende behoeftes op. Werf dus niet voor één persoon die eigenlijk acht vacatures tegelijk moet kunnen vullen, maar wees redelijk en splits zware functies op. Zo creëer je ook plek voor MBO'ers. Competentieprofielen kunnen hierbij een houvast geven, maar gebruik ze vooral ter inspiratie voor je eigen functiehuis binnen je specifieke domein. Blijf ruimte houden voor mensen om hun eigen ontwikkelpad te volgen. Kijk ook eens over de grenzen van je eigen afdeling. Misschien zijn er mensen met talent die gemotiveerd zijn om voor een paar uur per week security taken op te pakken.
- Straal uit dat het leuk is! Werken in dit vak is belangrijk, uitdagend, dynamisch, spannend en maatschappelijk relevant. Vertel het dus door. Ga regelmatig in gesprek met studenten en docenten in MBO en hoger onderwijs om een realistische kijk in de keuken te geven. Denk daarbij ook aan andere opleidingen dan ICT. Communicatie, data science, rechten, accountancy, economie, psychologie en zelfs geschiedenis zijn allemaal richtingen die waardevol kunnen blijken bij het opstellen van beleid, risicoscenario's, awareness programma's, threat intelligence, of het analyseren van oorzaken van incidenten.
- Train je recruiters. Voor specialistische vacatures is het verstandig dat recruiters enigszins bekend zijn met terminologie en specifieke opleidingen. Een goed geschreven vacaturetekst nodigt uit te solliciteren. Zorg ook dat de eisen redelijk zijn. Zoek je een azure cloud security specialist? Vraag dan niet om een generieke certificering. Zoek je een junior? Vraag dan niet om een dure certificering die je pas mag voeren na vijf jaar werkervaring. Zoek je een senior? Dan is vijf jaar ervaring misschien echt nog niet genoeg.

Referenties

(1) https://www.isc2.org/Research/Workforce-Study
(2) https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education
(3 N. van Deursen. Wie is de meest gezochte informatiebeveiliger? iB-Magazine 4, 2018
(4) https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025/embedding-standards-and-pathways-across-the-cyber-profession-by-2025#introduction
(5) https://niccs.cisa.gov/workforce-development/cyber-career-pathways
(6) https://www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging
(7) https://www.giac.org/workforce-development/job-descriptions/
(8) https://www.ncsc.nl/onderzoek/onderzoeksresultaten/iacs-competenties
(9) https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)
(10) https://securitytalent.nl/career/career-navigator-in-safety-security
(11 https://niccs.cisa.gov/workforce-development/cyber-career-pathways?community=cybersecurity
(12) https://www.giac.org/certifications/
(13) https://ecfexplorer.itprofessionalism.org/