cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

O1. Gezamenlijk curriculum beroepsonderwijs en -opleiding op het gebied van cyberbeveiliging

Een instrument om cyberbeveiligingscompetenties voor verschillende leerprofielen te identificeren

Dit project is gefinancierd met steun van de Europese Commissie. Deze publicatie [mededeling] weerspiegelt alleen de standpunten van de auteur en de Commissie kan niet verantwoordelijk worden gehouden voor enig gebruik dat kan worden gemaakt van de daarin vervatte informatie.

INHOUDSOPGAVE

1. Introductie

Volgens een recent rapport vrijgegeven door Intel Security, genaamd "Hacking the Skills Shortage" (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf), zullen er 1 miljoen tot 2 miljoen onvervulde cyber-security banen wereldwijd in 2019. Het rapport bevat de resultaten van een enquête onder 775 IT-beslissers die betrokken zijn bij beveiliging, van wie 82% een gebrek aan cyber-security vaardigheden binnen hun bedrijf meldde.

Uit het onderzoek van ESG (Enterprise Strategy Group) blijkt dat 45% van de organisatiesin 2017 een problematisch tekort aan cybersecurityvaardigheden heeft(https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse). Natuurlijk geldt dit voor alle gebieden van cyberbeveiliging, maar recent ESG-onderzoek toont aan dat het tekort aan vaardigheden een directe impact heeft op security analytics en operations.

Met het oog op een dynamisch evoluerend dreigingslandschap en voortbouwend op de herziening van de EU-cyberbeveiligingsstrategie van 2013, was het samen aanpakken van de cyberbeveiligingsgevaar een van de drie uitdagingen die bij de tussentijdse herziening van de digitale eengemaakte markt aan de orde kwamen. Zo heeft de Commissie op 13 september 2017 een pakket cyberbeveiliging aangenomen.

Het pakket bouwt voort op bestaande instrumenten en presenteert nieuwe initiatieven om de cyberweerbaarheid en respons in de EU verder te verbeteren. Het is in het strategisch belang van de EU ervoor te zorgen dat de technologische instrumenten van cyberbeveiliging worden ontwikkeld op een manier die de digitale economie tot bloei laat komen en tegelijkertijd onze veiligheid, samenleving en democratie beschermt. Dit omvat de bescherming van kritieke hardware en software. Om de cyberbeveiligingscapaciteit van de EU te versterken, stellen de Commissie en de hoge vertegenwoordiger onder andere prioriteiten en acties voor om de lacune in vaardigheden op het gebied van cyberdefensie aan te pakken. Met deze doelstelling zal de EU in 2018 een platform voor cyberdefensieopleiding en -onderwijs creëren.

Dit zijn slechts enkele gegevens en initiatieven die de realiteit van de IT-wereld vertegenwoordigen als het gaat om cyberbeveiliging en het CyVETsecurity-project voedt zich met dit momentum dat cybersecurity op de Europese en mondiale agenda staat door twee intellectuele resultaten te produceren die pretenderen bij te dragen aan het verkleinen van de kloof tussen bestaande cyberbeveiligingscompetenties (en bewustzijn) en de reële behoeften (niet alleen van bedrijven, maar van de samenleving zelf).

De eerste van de2 intellectuele outputs is dit "gezamenlijke beroepsonderwijs en -opleiding in cyberbeveiliging", een selectie van de belangrijkste kennis, vaardigheden en competenties met betrekking tot cyberbeveiliging uit een uitgebreid onderzoek uitgevoerd door het projectteam, dat de volgende bronnen heeft opgenomen:

- Het **SANS Institute** (Escal Institute of Advanced Technologies), een Amerikaans bedrijf gespecialiseerd in security en cybersecurity training en certificering.
- Het **National Institute of Standards and Technology (NIST),** een niet-regelgevend agentschap uit de VS dat de certificering NIST 800-53 cybersecurity framework heeft ontwikkeld.
- De **International Organisation for Standardization (ISO),**die een reeks normen biedt met betrekking totinformatiebeveiliging in het kader van de ISO/IEC 27000 .
- Het **DigiComp Framework** (Europees kader voor digitalecompetentie voor burgers),dat een uitgebreide beschrijving biedt van de kennis, vaardigheden en attitudes die mensen op 5 belangrijke gebieden nodig hebben, is veiligheid een van hen.

Tijdens het onderzoek hebben we vastgesteld dat kennis, vaardigheden en competenties op het gebied van cybersecurity als volgt kunnen worden gegroepeerd (volgens het SANS Institute) op deze vakgebieden:

- **Inbraakdetectie.** Het gaat om het ontdekken van potentieel schadelijke activiteiten die de vertrouwelijkheid, integriteit of beschikbaarheid van informatie in gevaar kunnen brengen. Er zijn een paar veel voorkomende vormen van inbraakdetectie. Netwerkgebaseerde detectiepogingen om

ongeoorloofd gedrag te detecteren op basis van netwerkverkeer. Host-based detectie probeert illegale activiteiten op een specifiek apparaat te vinden. Fysieke detectie omvat het vinden van bedreigingen op fysieke systemen.

- **Veilige softwareontwikkeling.** De meeste datalekken zijn succesvol als gevolg van kwetsbaarheden of gebreken in software code, en commerciële software moet worden gepatcht op een regelmatige basis.
- **Risicobeperking.** Het gaat om het bijhouden van geïdentificeerde risico's, het ontdekken van nieuwe risico's en het bijhouden van risico's in een project. Ten eerste is het noodzakelijk om te begrijpen dat gegevens moeten worden beschermd en waarom. Bedrijven moeten hun meest waardevolle activa en de bedreigingen identificeren die hen in gevaar brengen. Weten hoe de informatie wordt opgeslagen, wie toegang heeft en hoe de gegevens worden beschermd zijn drie kritische vragen om een optimale gegevensbescherming.
- **Cloud beveiliging.** Er zijn verschillende bedreigingen met name voor de beveiliging van de cloud. Enkele van de top gevaren zijn datalekken, systeem kwetsbaarheid exploits, gekaapte accounts, onvoldoende zorgvuldigheid, en kwaadaardige insiders.
- **Netwerkbewaking en toegangsbeheer.** De organisatieheeft ook professionals nodig die weten wat ze zoeken en snel beslissingen kunnen nemen wanneer verdacht gedrag wordt gedetecteerd.
- **Veiligheidsanalyse.** Om innovatieve oplossingen te bouwen om te voorkomen dat hackers bedrijfsnetwerken betreden en gevoelige gegevens stelen.
- **Gegevensbeveiliging.** Vooral belangrijk voor organisatiesopkwetsbare gebieden, zoals gezondheidszorg en financiële dienstverlening.

Wat vindt u in dit document?

Uitgaande van deze expertisegebieden hebben we verschillende eenheden van competenties en leerresultaten en beoordelingscriteria gedefinieerd. Dat hebben we gedaan, waarbij ook rekening wordt gehouden met verschillende professionele profielen.

In het volgende hoofdstuk leggen we uit welke methodologie we gebruikten om dat te doen en bouwen we ons gezamenlijke beroepsonderwijs-curriculum in cybersecurity, maar eerst willen we dat je begrijpt hoe je dit document gebruiken:

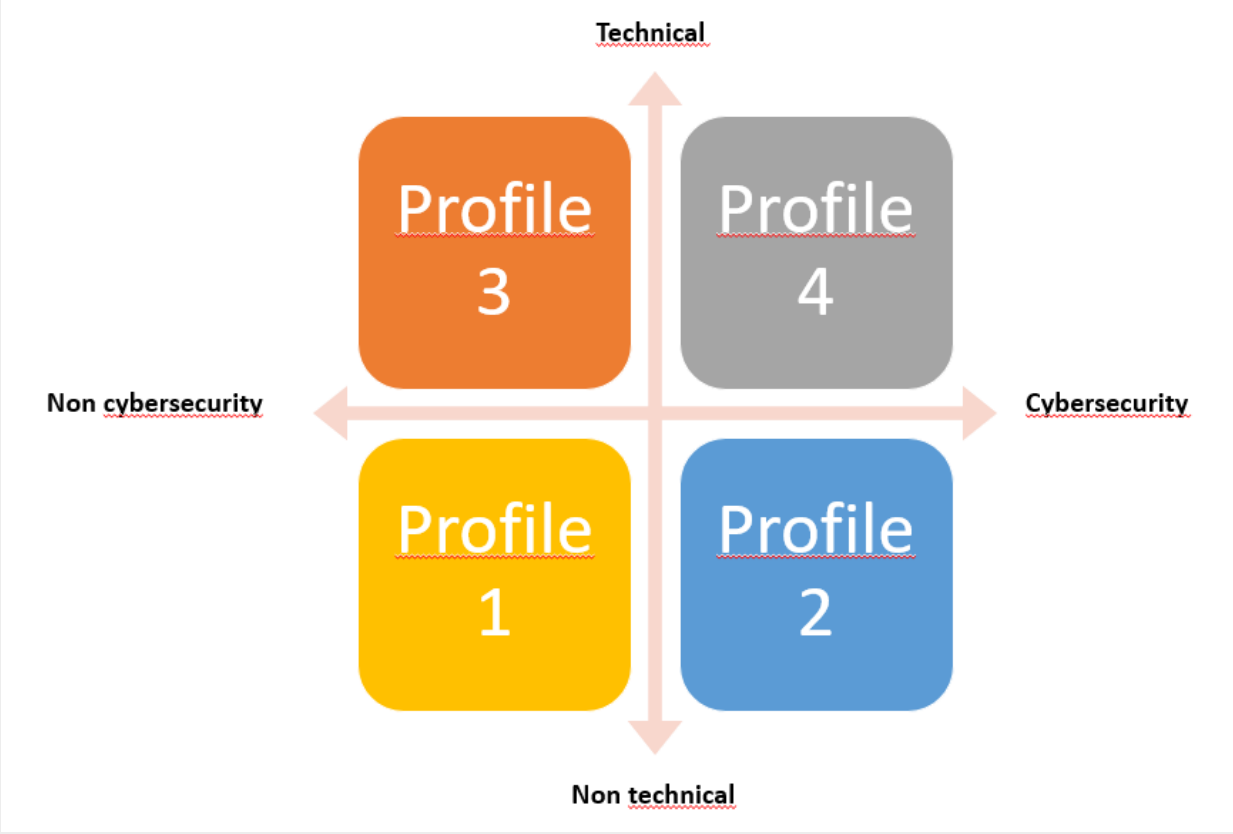
- Als u een beroepsonderwijs leraar, u gebruik maken van het volledige curriculum of slechts delen van het. Afhankelijk van wie u aanpakken en uw doelstellingen, vindt u dat u slechts enkele eenheden nodig, de meeste van hen of zelfs allemaal! Ongeacht het aantal eenheden, u ze gebruiken om cyberbeveiliging en informatiebeveiliging pillen en praktijken in een bestaand programma voor beroepsonderwijs en /or te introduceren en / of u nieuwe opleidingsprogramma's ontwerpen die ons curriculum (geheel of gedeeltelijk) nemen zoals het is of aan te passen, het invullen van het met alle andere inhoud die u relevant vinden. Wat betreft de levering van het curriculum, hebben we ook een aantal trainingsmaterialen, die betrekking hebben op de verschillende eenheden van de competentie, dat is onze output nummer 2 "O2. uitdagingen op het gebied van cyberveiligheid". U beide documenten samen of afzonderlijk gebruiken, maar houd er rekening mee dat O2 is gebouwd op O1.
- Als u een bedrijf bent, u beide outputs gebruiken voor interne training van uw werknemers of zelfs alleen O1, om een opleidingsprovider te vragen een training te ontwerpen die bepaalde eenheden omvat die belangrijk zijn voor uw organisatie,of zelfs als ondersteuning om het profiel van een toekomstige werknemer te definiëren tijdens een wervingsproces.
- Als u een onderwijsautoriteit bent die verantwoordelijk is voor het ontwerpen van leerplannen, u deze output interessant vinden om te bekijken en te zien welke mogelijke eenheden kunnen worden geïmplementeerd in een verscheidenheid van programma's voor beroepsonderwijs en -opleiding of zelfs in een specialisatieprogramma dat volledig gewijd is aan cyberbeveiliging. De bibliografie die we gebruikten, waarnaar in het laatste hoofdstuk wordt verwezen, kan ook nuttig zijn.

Gebouwd volgens een modulaire structuur (LO gegroepeerd in eenheden die samen of onafhankelijk worden opgeleid) in de vorm van een matrix, waarbij de eenheden van competentie en kolommen de leerresultaten die aan elke eenheid zijn gekoppeld, worden gelijnd.

2. Methodologie

Uitgaande van de expertisegebieden die in het vorige hoofdstuk werden beschreven, was de volgende stap die we hebben gezet om verschillende professionele profielen en hun relatie tot cybersecurity te karakteriseren.

We hebben 4 soorten profielen gedefinieerd:



- **Profiel 1** verzamelt professionals die binnen niet technische profielen liggen en die niet veel kennis en vaardigheden op het gebied van cybersecurity nodig hebben vanwege hun beroep, alleen die welke nodig zijn voor een persoon (bijvoorbeeld een fornuis, een automonteur, een loodgieter, een verpleegkundige...). Modules/competentie-eenheden zijn gericht op bewustwording (cybersecurityhygiëne) en zullen zich bezighouden met dreigingstypen, goede praktijken in sociale media, bedreigingen en basisbewustzijn van cyberbeveiliging.

- **Profiel 2** verzamelt professionals die binnen niet technische profielen liggen, maar die vanwege de aard van hun werk een hoger niveau van expertise op het gebied van cybersecurity nodig hebben, vooral omdat ze gevoelige informatie beheren (bijvoorbeeld een persoon die bij een bank werkt, een accountant, een persoon die in een verzekeringsmaatschappij werkt, de administratie van een ziekenhuis...). Modules/competentieeenheden zullen zich voornamelijk richten op gegevensbescherming (regelgeving...) en veilige gegevensuitwisseling.

- **Profiel 3** verzamelt professionals die binnen technische profielen liggen, maar die slechts beperkte kennis en vaardigheden nodig hebben met betrekking tot cybersecurity, voornamelijk gerelateerd aan hun taken (een persoon die werkt in een CNC-machine, in robotica... binnen de context van een onderling verbonden industrie, digitale industrie, IoT). De competentie-eenheden in dit profiel zullen zich richten op cybersecurity in verband met de verbinding tussen OT en IT.

- **Profiel 4** verzamelt professionals met een technisch profiel (achtergrond in IT) en met gespecialiseerde kennis en vaardigheden op het gebied van cybersecurity op het gebied van bescherming/preventie, monitoring en forensisch onderzoek. De competentie-eenheden zullen zich bezighouden met de analyse van kwetsbaarheden, security management, perimetrale beveiliging en forensische analyse.

Deze 4 profielen werden gedefinieerd en beschreven tijdens de eerste vergadering van het project in Tallinn. Een verduidelijking verdient te worden vermeld: De profielen zijn niet gericht op een bepaald EQF-niveau. Het zal de definitie van de leerresultaten samen met de beoordelingscriteria zijn die de gebruiker

zullen begeleiden om te beslissen of het haalbaar is om op een bepaalde doelgroep van toepassing te zijn. Echter, bij het ontwerpen van het curriculum hebben we rekening houden met het volgende in gedachten:

- Eenheden met betrekking tot profiel 1 werden gedefinieerd met het oog op elk niveau of een programma voor beroepsonderwijs en -opleiding, aangezien zij betrekking hebben op zeer fundamentele aspecten van cyberbeveiliging die zowel op professioneel als op persoonlijk niveau van toepassing zijn. Laten we zeggen dat ze zijn gericht op cyberhygiëne en bewustzijn, die echter niet wordt onderwezen in beroepsonderwijs en -opleiding programma's die betrekking hebben op elementaire digitale vaardigheden die de meeste mensen, echter niet have (zie https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework en http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf)
- Eenheden met betrekking tot profiel 2 werden gedefinieerd met in het achterhoofd een EQF-niveau van 3-5. We dachten aan programma's voor beroepsonderwijs en -opleiding, zoals bedrijfskunde, financiën, gezondheidszorg of e-business en retail.
- Eenheden met betrekking tot profiel 3 werden gedefinieerd met in het achterhoofd een EQF-niveau van 3-5, speciaal gericht op industriële gebieden zoals CNC-programmering, robotica, elektriciteit, elektronica of automatisering.
- Eenheden met betrekking tot profiel 4 werden gedefinieerd met in het achterhoofd een EQF niveau 4-5 met een IT-achtergrond zoals app-ontwikkeling, programmering of IT-netwerken beheer.

De definitie van leerresultaten en beoordelingscriteria die voor elke eenheid werden vastgesteld, was een van de meest uitdagende onderdelen van dit document. De beschikbare informatie was echt uitgebreid, zodat het definiëren van specifieke eenheden was ook moeilijk, maar rekening houdend met de profielen gedefinieerd door ons en de gebieden van expertise in cybersecurity gedefinieerd door het SANS Instituut maakte het makkelijker. Het vereenvoudigen van die hoeveelheid informatie in de definitie van specifieke leerresultaten was een ingewikkelder proces, dat verschillende stappen doorging waarbij we begonnen met 12-20 leerresultaten per eenheid (en nog meer beoordelingscriteria!) voor de groep leerresultaten, zodat het beter beheersbaar zou kunnen zijn, waarbij we een aantal van hen konden toetreden en vereenvoudigen. Hier een voorbeeld van dit, van dit:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test **(This unit is based on the work roles described for: "system test and evaluation specialist" and "Information systems security developer" in the NICE**	U1LO1. The learner is able to determine the level of assurance of developed capabilities based on test results.
	U1LO2. The learner is able to test plans to address specifications and requirements.
	U1LO3. The learner is able to install and maintain network infraestructure device operating system software (e.g., IOS, firmware)
	U1LO4. The learner is able to make recommendations based on test results.
	U1LO5. The learner is able to determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated
	U1LO6. The learner is able to validate specifications and requirements for testability.
	U1LO7. The learner is able to analyze the results of software, hardware or interoperability testing.
	U1LO8. The learner is able to perform developmental testing on systems under development.
	U1LO9. The learner is able to perform interoperability testin on systems exchanging eletronic information with other systems.
	U1LO10. The learner is able to perform operational testing.
	U1LO11. The learner is able to test, evaluate and verify hardware and/or software to determine compliance with defined specifications and requirements.
	U1LO12. The learner is able to record and manage test data.
	U1LO13. The learner is able to develop and direct system testing and validation procedures and documentation.
	U1LO14. The learner is able to identify and direct the remediation of technical problems encountered during testing and implementaion of new systems
	U1LO15. The learner is able to identify, assess and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization´s evaluation and validation requirements.
	U1LO16. The learner is able to perform risk analysis (e.g. threat, vulnerability and probability of occurrence) whenevar an application or system undergoes a major change.
	U1LO17. The learner is able to utilize models and simulations to analyze or predict system performance under different operating conditions
	U1LO18. The learner is able to test and evaluate secure interfaces between information systems, physical systems and/or embedded technologies.
	U1LO19. The learner is able to perform an information security risk assessment.
	U1LO20. The learner is able to perform security reviews and identify security gaps in architecture.

Aan dit:

UNITS OF COMPETENCE	LEARNING OUTCOMES
Unit 1. Penetration test	U1LO1. The learner is able to identify and apply the phases of the Audit Process
	U1LO2. The learner is able to collect evidences
	U1LO3. The learner is able to search and exploit vulnerability
	U1LO4. The learner is able to do a vulnerability report

In sommige gevallen hebben we dit vereenvoudigingsproces zelf uitgevoerd, maar in het geval van de profielen 3 en 4 (inhoudelijk ingewikkelder) hebben we meegeteld met de hulp van onze geassocieerde partners in Spanje en Nederland.

Een laatste vraag om in gedachten te houden is dat profielen niet noodzakelijkerwijs exclusief zijn, d.w.z;zelfs als we verschillende eenheden voor verschillende profielen hebben gedefinieerd, u op uw gemak eenheden uitwisselen en iemand van profiel 3 een activiteit geven vanuit profiel 2 of vice versa. Dat hangt af van uw doelgroep en uw doelstellingen. Bij het ontwerpen van de uitdagingen hebben we hiermee rekening gehouden en bepalen we welke voorkennis of

achtergrond een persoon nodig heeft om een specifieke uitdaging uit te voeren. Of... je zou zelfs gek kunnen worden en profielen kunnen mixen om een meer multidisciplinaire aanpak te hebben!

Zoals u zien, is het ontwerp van ons curriculum flexibel genoeg om te worden aangepast aan verschillende programma's en niveaus voor beroepsonderwijs en -opleiding en aan verschillende soorten professionals. Ga gewoon en neem een kijkje op de eenheden meer geschikt voor uw doelstellingen!

3. Het CyVETsecurity curriculum

	EENHEDEN	LEERRESULTATEN	EVALUATIECRITERIA
Profiel 1	Unit 1. Bescherming van apparaten en digitale inhoud	U1LO1. De leerling kan fysieke en virtuele risico's in verband met technologie identificeren	De leerling groepeert meerdere risico's in 3 fysieke en 3 virtuele.
		U1LO2. De leerling is in staat om de strategieën te implementeren om risico's te voorkomen en werkt zichzelf op dit gebied bij	De leerling beschrijft een strategie om te voorkomen dat hij gecompromitteerd wordt
		U1LO3. De leerling kan een antivirusprogramma installeren	De leerling installeert een antivirusprogramma op een virtuele machine
		U1LO4. De leerling kan zichzelf tegen fraude beschermen door veilige wachtwoorden te gebruiken.	De leerling identificeert de veilige wachtwoorden uit een lijst met veel wachtwoorden
		U1LO5. De leerling kan verschillende kwetsbare apparaten beschermen tegen digitale bedreigingen (malware, virussen ...)	De leerling identificeert welke kwetsbare apparaten zijn en de mechanismen voor hun bescherming
		U1LO6. De leerling is in staat om gevoelige / waardevolle informatie en voor aanvallen vatbare sectoren te identificeren	De leerling identificeert gevoelige gegevens en variaties in aanvallen, afhankelijk van de sectoren
	Unit 2. Bescherming van persoonsgegevens en digitale identiteit	U2LO1. De leerling kan zich adequaat gedragen in de digitale wereld en zijn / haar digitale trace goed beheren	De leerling kent GDPR De leerling beschrijft hoe Google Analytics werkt De leerling begrijpt het concept van een digitale voetafdruk en legt het uit
		U2LO2. De leerling kan de gevaren van diefstal of misbruik van zijn / haar digitale identiteit door anderen identificeren.	De leerling identificeert scenario's waarin zijn gegevens verkeerd kunnen worden gebruikt De leerling beschrijft de term 'identiteitsdiefstal' en waardeert het risico dat dit gebeurt
		U2LO3. De leerling is in staat om informatie met betrekking tot andere mensen te beschermen tegen zijn / haar omgeving (als werknemer, als vriend ...)	De leerling identificeert technieken die worden gebruikt om PII te beschermen
		U2LO4. De leerling kan online informatie over zichzelf opzoeken, wissen en / of wijzigen.	De leerling legt uit hoe PII die bij een organisatie wordt bewaard, kan worden gewist / gewijzigd. De leerling verzamelt zijn / haar digitale voetafdruk.
		U2LO5. De leerling kan zijn / haar eigen digitale trace beheren.	De leerling beheert zijn / haar digitale voetafdruk
		U2LO6. De leerling kan kritisch handelen bij het online delen van informatie over zichzelf.	De leerling demonstreert de juiste controletechnieken bij het online delen van PII
		U2LO7.De leerling kan gebruik maken van meerdere digitale identiteiten, gericht op verschillende doelstellingen.	De leerling maakt meerdere sociale media-accounts aan en onderscheidt deze voor werk en persoonlijk.

Profiel 2	**Unit 3. Beheer van informatiebeveiliging en regelgeving**	U3L01. De leerling is in staat het belang van informatiebeveiliging en de betekenis ervan voor de organisatie te begrijpen	De leerling legt duidelijk uit welke de informatiebeveiligingsrichtlijnen van de organisatie zijn. De leerling stelt verbeteringen van de verstrekte richtlijnen voor.
		U3L02. De leerling kan basiswetten, voorschriften en ethische principes van cybersecurity en informatiebeveiligingsinstructies identificeren (bijvoorbeeld GDPR en ISO 27000)	De leerling identificeert kernconcepten, voorschriften en procedures van informatiebeveiliging en cybersecurity. De leerling past regels toe met betrekking tot informatiebeveiliging.
		U3L03. De leerling kan zijn / haar eigen werk plannen op basis van informatiebeveiligingsinstructies op de werkplek	De leerling werkt met het toepassen van informatiebeveiligingsinstructies
		U3L04. De leerling kan werken met de beveiliging van tele- / datacommunicatie: vertrouwelijkheid, integriteit, beschikbaarheid	De leerling legt de betekenis van vertrouwelijkheid, integriteit en beschikbaarheid uit. De leerling legt uit wat de mogelijke gevolgen zijn van het verbreken van de vertrouwelijkheid.
		U3L05. De leerling kan de veiligheidstraining van het personeel uitvoeren: veiligheidsrichtlijnen, controle en monitoring	De leerling stelt een korte set instructies op over informatiebeveiliging voor een organisatie of een groep personeel van een organisatie.
	Unit 4. Informatiebeveiliging als onderdeel van de beveiligingspraktijken van organisaties	U4L01. De leerling kan informatierisico's op de werkplek observeren, beoordelen, voorkomen en rapporteren	De leerling benoemt de bedreigingen en risico's voor de gegevensbeveiliging waarmee hij / zij in zijn / haar dagelijkse werk wordt geconfronteerd. De leerling past maatregelen toe om de gegevensbescherming te waarborgen.
		U4L02. De leerling kan de beveiligingssystemen van de organisatie gebruiken in relatie tot informatiebeveiliging	De leerling gebruikt de beveiligingssystemen van de organisatie in relatie tot informatiebeveiliging.
		U4L03. De leerling kan de fysieke beveiliging in de gebouwen beheren	De leerling identificeert verschillende fysieke veiligheidssituaties in de organisatie.
		U4L04. De leerling kan veilig werken in mobiele en cloudservices	De leerling past maatregelen toe om veilig te werken in een virtuele omgeving
		U4L05. De leerling kan zorgen voor opslag en bescherming van materiaal en gegevens	De leerling bewaart en beschermt materiaal en gegevens.
		U4L06. De leerling kan de basisprincipes van softwareveiligheid toepassen: besturingssystemen, applicaties	De leerling gebruikt veilig persoonlijke apparaten en applicaties
	Unit 5. Inleiding tot cyberbeveiliging	U5L01. De leerling is in staat kritische informatie van verschillende media te identificeren	De leerling vergelijkt en analyseert kritisch informatie die is verkregen uit verschillende media en identificeert de meest kwetsbare
		U5L02. De leerling kan de kwetsbaarheid van kritieke infrastructuur voor de samenleving inschatten	De leerling identificeert kwetsbaarheden van de kritieke infrastructuur in de samenleving
		U5L03. De leerling kan cyberaanvallen en -bedreigingen identificeren	De leerling geeft een lijst van veelvoorkomende cyberaanvallen en bedreigingen die kunnen plaatsvinden, rekening houdend met de informatie die op zijn / er werk wordt beheerd

	EENHEDEN	LEERRESULTATEN	EVALUATIECRITERIA
Profiel 3	Unit 1. Basiskennis ICT	U1LO1. De leerling heeft basiskennis over cyberbeveiliging	De leerling weet wat cyberveiligheid is.
		U1LO2. De leerling heeft basiskennis over ICT-systemen	De leerling kent de basisprincipes van het werken met ICT
		U1LO3. De leerling is zich bewust van gevaar	De leerling is op de hoogte van het DATA-lek
		U1LO4. De leerling heeft een basiskennisnetwerk	De leerling begrijpt de basisprincipes van netwerken.
	Unit 2. Bedrijfsprocedures en machines	U2LO1. De leerling kan zich adequaat gedragen in de digitale wereld en zijn / haar digitale trace goed beheren	De leerling kent GDPR De leerling beschrijft hoe Google Analytics werkt De leerling begrijpt het concept van een digitale voetafdruk en legt het uit
		U2LO2. De leerling kan de gevaren van diefstal of misbruik van zijn / haar digitale identiteit door anderen identificeren.	De leerling identificeert scenario's waarin zijn gegevens verkeerd kunnen worden gebruikt De leerling beschrijft de term 'identiteitsdiefstal' en waardeert het risico dat dit gebeurt
		U2LO3. De leerling is in staat om informatie met betrekking tot andere mensen te beschermen tegen zijn / haar omgeving (als werknemer, als vriend ...)	De leerling identificeert technieken die worden gebruikt om PII te beschermen
		U2LO4. De leerling kan online informatie over zichzelf opzoeken, wissen en / of	De leerling legt uit hoe PII die bij een organisatie wordt bewaard, kan worden gewist / gewijzigd. De leerling verzamelt zijn / haar digitale voetafdruk.
		U2LO5. De leerling kan zijn / haar eigen digitale trace beheren.	De leerling beheert zijn / haar digitale voetafdruk
		U2LO6. De leerling kan kritisch handelen bij het online delen van informatie over zichzelf.	De leerling demonstreert de juiste controletechnieken bij het online delen van PII
		U2LO7.De leerling kan gebruik maken van meerdere digitale identiteiten, gericht op verschillende doelstellingen.	De leerling maakt meerdere sociale media-accounts aan en onderscheidt deze voor werk en persoonlijk.

Profiel 4	**Eenheid 1. Penetratietest**	U1L01. De leerling is in staat de fasen van het auditproces te identificeren en toe te passen	De fasen van het auditproces zijn duidelijk geïdentificeerd De test wordt uitgevoerd volgens de fasen van het auditproces, waarbij hardware en / of software wordt geëvalueerd en geverifieerd om te bepalen of aan de gedefinieerde specificaties of vereisten is voldaan
		U1L02. De leerling kan bewijzen verzamelen	Omvang, infrastructuur, middelen en steekproefomvang om ervoor te zorgen dat de systeemvereisten voldoende worden aangetoond. Testgegevens worden correct geregistreerd en beheerd.
		U1L03. De leerling kan kwetsbaarheid zoeken en misbruiken	Er worden modellen en simulaties gebruikt om de systeemprestaties te analyseren of te voorspellen. Resultaten van testresultaten van software, hardware of interoperabiliteit worden correct geanalyseerd. Evaluatie van beveiligde interfaces tussen informatiesystemen, fysieke systemen en / of ingebedde technologieën wordt uitgevoerd om te zoeken naar kwetsbaarheid
		U1L04. De leerling kan een kwetsbaarheidsrapport doen	Kwetsbaarheden in informatie en beveiligingslekken in de architectuur worden correct geïdentificeerd. Aanbevelingen op basis van testresultaten worden op een concrete en duidelijke manier gegeven
	Unit 2. Beheer en governance van beveiliging	U2L01. De leerling kent en begrijpt normen en veiligheidsvoorschriften (ISO, ISACA, NIST)	Best practices van IT-beheer door gebruik te maken van een bekend raamwerk (bijv. ITIL) worden uitgelegd. Normen voor het beheer van informatiebeveiliging (bijv. ISO / IEC 27001/27002) worden toegepast.
		U2L02. De leerling kan informatiebeveiligingsbeheer (ISMS) implementeren	De rol van informatie vanuit strategisch oogpunt wordt uitgelegd. Rollen en belanghebbenden in informatietechnologie worden geïdentificeerd. Bedrijfsstrategie en ICT-strategie zijn op elkaar afgestemd. Er worden aanbevelingen gegeven over hoe gegevens in de organisatie moeten worden beheerd volgens de beveiligingsdocumentatie.
		U2L03. De leerling kan een risicoanalyse uitvoeren	Er worden kwetsbaarheids- en dreigingsanalyses uitgevoerd als onderdeel van de bedrijfsimpactanalyse. Beveiligingsdocumentatie op basis van monitoringresultaten wordt bijgewerkt.
		U2L04. De leerling is in staat om te werken volgens de regels over persoonlijke informatie (RGPD)	Er wordt rekening gehouden met nationale en internationale regelgeving met betrekking tot gegevensbescherming
	Unit 3. Beveiligingsontwikkeling	U3L01. De leerling is in staat om veilige programmeertechnieken te identificeren	Cybersecurity-ontwerpen voor systemen en netwerken worden ontwikkeld of geïntegreerd. Er worden beveiligde configuratiebeheerprocessen toegepast. Bij het programmeren wordt rekening gehouden met beschermingsmiddelen om inbraak tot een minimum te beperken
		U3L02. De leerling kan apps ontwikkelen met informatielevering (certificaten, protocollen, handtekeningen)	Apps worden ontwikkeld met gebruikmaking van op handtekeningen gebaseerde machtigingen. Toegang tot de inhoudproviders van apps is uitgeschakeld. Er worden apps ontwikkeld die een netwerkbeveiligingsconfiguratie toevoegen.
		U3L03. De leerling kan apps ontwikkelen zonder datalekken (autorisatie en toegang)	Er worden apps ontwikkeld die privégegevens opslaan in interne opslag. Geldigheid van gegevens wordt gecontroleerd
		U3L04. De leerling kan werken volgens de voorschriften (ASVS)	Het ontwerpen, ontwikkelen en testen van webapplicaties gebeurt met inachtneming van de Application Security Verification Standards (ASVS)

	Unit 4. Forensische analyse	U4LO1. De leerling is in staat forensische analysefasen te identificeren en toe te passen	Stadia worden geïdentificeerd en gevolgd bij het toepassen van een forensische analyse. Bevindingen worden verstrekt in overeenstemming met vastgestelde rapportageprocedures.
		U4LO2. De leerling kan apparaten klonen	Er worden geluidsduplicaten gemaakt van harde schijven, floppy diskettes, cd's, mobiele telefoons of gps.
		U4LO3. De leerling kan diverse analyses uitvoeren	Er wordt een analyse van logbestanden, bewijsmateriaal en andere informatie uitgevoerd om de beste methoden te bepalen voor het identificeren van de daders van een netwerkinbraak. Informatie waartoe toegang is verkregen nadat een inbreuk is vastgesteld. Netwerkverkeer dat verband houdt met kwaadaardige activiteiten, wordt opgevangen en geanalyseerd.
		U4LO4. De leerling kan informatie herstellen	De herstelde gegevens worden onderzocht om de relevantie van de inbraak te bepalen. Gegevens worden geëxtraheerd met behulp van data-carving-technieken (Forensic Tool Kit, Foremost...) In beslag genomen gegevens worden ontsleuteld.
	Unit 5. Perimetrale beveiliging	U5LO1. De leerling kan technieken voor communicatiebeveiliging implementeren	E-mail en webservers zijn beveiligd. Firewall voor serverbeveiliging is geconfigureerd. DNS- en DHCP-serverbeveiliging is gegarandeerd. Beveiligingsvereisten worden gecommuniceerd naar andere afdelingen in de organisatie.
		U5LO2. De leerling kan een netwerk ontwerpen en implementeren volgens het beveiligingsmodel	Mogelijke defecten van kritieke componenten worden geïdentificeerd. Er worden maatregelen genomen om de gevolgen van een mislukking te verzachten. Netwerkverbindingen zijn versleuteld. Draadloze netwerken worden beschermd met codering en wachtwoordsystemen. Het opslaan van back-upbestanden is geautomatiseerd in een lokaal of wereldwijd netwerk en beschermd tegen ongeoorloofd gebruik.
		U5LO3. De leerling kan authenticatie- en identiteitsbeheersystemen (SSO) identificeren	Het AAA-model (authenticatie, autorisatie en boekhouding) wordt geïmplementeerd. VPN-beleid wordt beheerd. Single sing-on-systemen zijn geïntegreerd in web- en mobiele apps.
		U5LO4. De leerling kan oplossingen voor gebeurtenisbeheer identificeren	De belangrijkste leveranciers van SIEM-systemen worden geïdentificeerd. De beste oplossing die past bij de behoeften van de organisatie en budgetefficiëntie wordt geselecteerd.

4. Bibliografie

- Internationale Organisatie van Normalisatie. *ISO/IEC 27000:2018*

  https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

- Europees kader voor digitale competentie voor burgers. *DigComp in actie. Een gebruikersgids voor het Europees digitaal competentiekader.*

  http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf

- National Institute of Standards and Technology. Nationaal Initiatief voor Cybersecurity Onderwijs (NICE). Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

- Nationaal Instituut voor Onderwijstechnologieën en Lerarenopleiding (INTEF). *Gemeenschappelijk kader voor digitale lerarencompetentie*. 2017. https://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-de-Competencia-Digital-Docente.pdf