NVAO • NEDERLAND

ASSOCIATE DEGREE CYBERSECURITY (007673)
HOGESCHOOL VAN AMSTERDAM

ADVIESRAPPORT

2 MEI 2019

NVAO • NEDERLAND

ASSOCIATE DEGREE CYBERSECURITY (007673)

Hogeschool van Amsterdam

BEPERKTE TOETS NIEUWE OPLEIDING ADVIESRAPPORT

2 MEI 2019

Inhoud

1 Samenvattend advies

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) ontving op 16 november 2018 een aanvraag voor een Toets Nieuwe Opleiding (TNO) voor de opleiding associate degree Cybersecurity (ad-opleiding Cybersecurity) van de Hogeschool van Amsterdam. NVAO heeft daarop een panel van experts gevraagd om alle aangeleverde informatie te bestuderen, het programma met de afgevaardigden van de instelling en opleiding tijdens een locatiebezoek te bespreken en een concluderend oordeel uit te spreken over de kwaliteit van de nieuwe opleiding.

Onderstaande overwegingen hebben een belangrijke rol gespeeld in de uiteindelijke beoordeling van het programma door het panel.

In Nederland bestaan er nog geen ad-opleidingen Cybersecurity. Het profiel van deze HvA-opleiding beoogt 'cybersecurityprofessionals op te leiden, die beschikken over *een brede basis in ICT,* aangevuld met specifieke kennis van en praktijkervaring met het *cybersecurityproces*. In het onderwijsconcept is aandacht voor het *lerend en reflecterend* vermogen van studenten, zodat studenten leren om te gaan met de snelle ontwikkelingen in het vakgebied'. Het panel waardeert de wijze waarop het ontwerpteam met de stakeholders (CSCMRA, werkveld, partners vanuit het ROC, collega's vanuit de bachelor-Cybersecurity) tot dit profiel is gekomen als positief. Het is actueel en vanuit het werkveld bestaat er grote behoefte aan.

Standaard 1 voldoet volgens het panel. De opleiding heeft een eigen beroeps- en opleidingsprofiel opgesteld. De keuze voor de zes kerntaken van de PTES-standaard, een internationale de facto industriestandaard voor penetration testing, en de formulering naar de drie beoogde leerresultaten (vertaald naar gedragscriteria) is transparant. De gedragscriteria zijn ingedeeld naar Methodisch handelen, Probleemoplossend vermogen, Samenwerken, Communiceren en Lerend vermogen en geformuleerd op ad-niveau (niveau 5). Er heeft ijking plaatsgevonden met een aantal relevante (inter-)nationale referentiekaders. De opleiding leidt op tot functies als 'ethical hacker, pentester of threat hunter'. Potentiële werkgevers voor deze studenten zijn: bedrijven, banken en (overheids-)organisaties. Het panel adviseert om juridische kennis, bijkomende technische kennis en verantwoord ethisch handelen aan de beoogde leerresultaten toe te voegen en de opleiding (naam) nog beter te positioneren. De (brede) naam Cybersecurity dekt niet geheel de lading van de opleiding met een inhoud die vooral gericht is op penetratietesting (dus offensief en in geringe mate defensief). Het panel raadt aan om in het profiel meer recht te doen aan de (bredere) inhoud.

Standaard 2 voldoet volgens het panel ten dele. Het gehanteerde onderwijsconcept (HILL) sluit goed aan bij de beoogde studenten. Er is sprake van afwisseling in leeromgevingen en van werkvormen met aandacht voor zelfsturing in het leerproces. De structuur van de eerste drie semesters is identiek: studenten werken vier dagen per week afwisselend aan praktijkopdrachten (OnTheJob) en aan fundamentele kennis en vaardigheden (Fundamentals). In de twee Boosterweken werken studenten (groepsgewijs en individueel) aan toepassing, integratie en professionele vaardigheden. Er is voldoende aandacht voor beroepsvraagstukken, vaardigheden en attitudes. De basiskennis van ICT- en Cybersecurity-methoden wordt voldoende aangereikt, internationalisering komt in beperkte mate aan de orde (Engelstaligheid in casuïstiek) en er is aandacht voor rapporteren (Nederlands). De opbouw van het programma bestaat uit steeds complexer wordende praktijkopdrachten, aangedragen door het werkveld. In het laatste semester wordt het afstudeerniveau in de afstudeeropdracht, waar studenten integraal werken aan de beoogde leerresultaten, geborgd. Als keuzemodule kunnen studenten onder andere een extern certificeringstraject volgen (zoals OSCP). De onderwijsleeromgeving (onderwijsvormen, studiebegeleiding, voorzieningen) en de kwaliteit van het docententeam voldoen. De *inhoudelijke* doorvertaling van beoogde leerresultaten naar leerdoelen (en BoKS) van het programma is nog niet voldoende transparant. Het panel heeft daarom als voorwaarde geformuleerd dat de doorvertaling (coverage) van de beoogde leerresultaten, met name bij de Fundamentals, ten aanzien van essentiële BoKS inzichtelijker moet worden. Hierbij moet in ieder geval kennis over relevante wetgeving, bijkomende technische kennis en verantwoord ethisch handelen zichtbaar zijn opgenomen in het curriculum.

Standaard 3 voldoet volgens het panel. De systematiek van toetsvormen is in lijn met het uitgangspunt 'assessment as learning': de summatieve toetsmomenten (beoordeling van opdrachten) zijn formatief ingebed in het leerproces van de student (op basis van feedback in gesprekken). Studenten denken zelf na over hoe zij de gedragsindicatoren willen gaan aantonen en welke bewijslast zij willen aanvoeren in hun portfolio. Het toetsconcept nodigt uit tot 'diepgaand leren'. De alignment tussen beoordelingscriteria en beoogde leerresultaten is aanwezig: alle gedragsindicatoren worden in de opleiding herhaaldelijk getoetst. Het panel vond de toetsvormen bij de (praktijk)opdrachten nog weinig overzichtelijk en de doorvertaling naar specifieke beoordelingscriteria niet transparant genoeg. Het panel raadt aan een totaaloverzicht te maken van ingezette toetsvormen en om per (praktijk)opdracht specifieke(re) eisen aan producten en beoordelingscriteria te formuleren. De uitvoering van summatieve en formatieve toetsen leunt sterk op individuele docenten en mentoren. De beoordeling van de afstudeeropdracht (eindtoets) gebeurt in het portfolioassessment, beoordeeld door de afstudeerbegeleider en een onafhankelijk assessor (vier ogen), mede op basis van de feedback van de bedrijfsbegeleider. Op basis van de gesprekken stelt het panel vast dat er veel wordt gekalibreerd en dat er gewerkt gaat worden met toetsdossiers, die door de examencommissie worden besproken. De kwaliteitszorg, de werkwijze van de examencommissie en de verantwoordelijkheden van de curriculum- en de blokcoördinatoren bij de toetsing, maken dat de commissie er vertrouwen in heeft dat de toetsing betrouwbaar wordt ingevuld.

Het panel komt tot een eindoordeel positief onder voorwaarden ten aanzien van de kwaliteit van de nieuwe opleiding associate-degree Cybersecurity van de Hogeschool van Amsterdam en adviseert de NVAO om overeenkomstig te besluiten.

Den Haag, 2 mei 2019

Namens het panel ter beoordeling van de beperkt Toets nieuwe opleiding
Associate degree Cybersecurity van de Hogeschool van Amsterdam,

Bart Preneel
(voorzitter)

Lieke Ravestein
(secretaris)

2 Introductie

2.1 Werkwijze panel

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) ontving op 16 november 2018 een aanvraag voor een Toets Nieuwe Opleiding (TNO) voor de opleiding Associate degree Cybersecurity van de Hogeschool van Amsterdam. Het succesvol doorlopen van een TNO procedure is een voorwaarde om als opleiding door de NVAO te worden erkend. Met het keurmerk van de NVAO mogen opleidingen de bij de opleiding behorende wettelijk beschermde getuigschriften of diploma's afgeven.

De procedure voor een nieuwe opleiding is iets anders dan de procedure die wordt gevolgd voor opleidingen die al zijn geaccrediteerd. Een TNO is in feite een planbeoordeling. Na de erkenning van de nieuwe opleiding zal de opleiding vallen onder de reguliere accreditatieprocedure.

Om de nieuwe opleiding te beoordelen, heeft de NVAO een panel van experts vastgesteld met de volgende samenstelling:
Voorzitter:
- Prof. dr. ir. Bart Preneel, gewoon hoogleraar Computerbeveiliging en Industriële Cryptografie, KU Leuven;

Leden:
- Drs. Janneke Jung, onderwijsmanager Associate degree ICT-service management, Hogeschool Rotterdam;
- John Fokker, head of Cyber Investigations, ATR, McAfee;
- Student-lid: Lars Blom, student ICT aan Fontys Hogeschool.

Het panel werd bijgestaan door Gijs Kremers, beleidsmedewerker NVAO, als procescoördinator en door Lieke Ravestein, als zelfstandig secretaris.

Bij de toetsing heeft het panel het Beoordelingskader voor de beperkte Toets Nieuwe Opleiding van de NVAO (Stcrt. 2016, nr 69458) in acht genomen.
Het panel heeft zich aan de hand van de door de opleiding verstrekte documenten op de beoordeling voorbereid. Op 14 maart 2019 is het panel bij elkaar geweest. Tijdens deze bijeenkomst zijn de eerste bevindingen van het panel besproken en nadere vragen geformuleerd voor het locatiebezoek.

Op 15 maart 2019 heeft het panel een locatiebezoek afgelegd. Tijdens dit bezoek is het panel in verschillende gespreksrondes van nadere informatie voorzien en zijn de vraagpunten aan de orde gesteld en in discussie gebracht. Het programma van het locatiebezoek is toegevoegd in bijlage 2. Na afloop van de gesprekken heeft het panel het geheel van bevindingen en overwegingen onderling besproken en vertaald naar voorlopige conclusies. Aan het eind van het bezoek heeft de panelvoorzitter die conclusies mondeling teruggekoppeld naar de opleiding. Op basis van de bevindingen, overwegingen en conclusies heeft de secretaris een conceptadvies opgesteld dat aan de panelleden is voorgelegd. Vervolgens heeft het panel dit concept van commentaar voorzien, waarna het conceptrapport is vastgesteld door de voorzitter. Het adviesrapport is op 17 april 2019 aan de opleiding voorgelegd ter controle op feitelijke onjuistheden. De opleiding heeft op 24 april 2019 gereageerd op het adviesrapport. Dit heeft geleid tot enkele aanpassingen, waarna het definitieve rapport is vastgesteld door de voorzitter. Het panel heeft dit advies in volledige onafhankelijkheid opgesteld en op 2 mei 2019 aan de NVAO aangeboden.

2.2 Panel rapport

Het eerste hoofdstuk van dit rapport bevat het samenvattend advies en het huidige hoofdstuk is de introductie.

Het derde hoofdstuk heeft een omschrijving van het programma waaronder de positionering van de opleiding binnen de instelling en binnen het hoger onderwijsbestel in Nederland.

Het panel geeft zijn bevindingen, overwegingen en conclusies weer in hoofdstuk 4 aan de hand van de onderwerpen en standaarden uit het relevante kader.

De bevindingen zijn de objectieve feiten zoals waargenomen door het panel in de aangeleverde documentatie en gedurende het locatiebezoek. De overwegingen bevatten de oordelen, meningen en zienswijzen van het panel en de mate waarop deze effect hebben op het uiteindelijke oordeel van het panel op de standaard. Op basis van de overwegingen wordt ook een algemeen eindoordeel uitgesproken.

Tot slot wordt in een tabel schematisch weergegeven wat de oordelen zijn per standaard.

3 Beschrijving van de instelling

3.1 Algemene gegevens

Instelling	:	Hogeschool van Amsterdam
Opleiding	:	associate degree Cybersecurity
Variant(en)	:	voltijd
Graad	:	associate degree
Afstudeerrichtingen	:	Geen
Locatie(s)	:	Amsterdam
Studieomvang (EC)	:	120
CROHO-onderdeel	:	domein Techniek

Voorstel voor indeling in een visitatiegroep: nader te bepalen

3.2 Profiel instelling

HvA biedt 72 bacheloropleidingen, 17 masteropleidingen en 3 associate degree-trajecten aan. De opleiding telt 4.066 medewerkers en 45.460 studenten (peildatum najaar 2018).
De instelling heeft zeven faculteiten, waaronder de Faculteit Digitale Media en Creatieve Industrie (de één-na-grootste in omvang).

HvA wil naast haar (huidige) bacheloropleiding ICT, aangeboden op de Faculteit Digitale Media en Creatieve Industrie, een nieuwe tweejarige Associate degree-opleiding Cybersecurity (ad-opleiding Cybersecurity) gaan aanbieden. De bacheloropleiding ICT bestaat uit vijf leerroutes, waaronder de - in omvang groeiende - leerroute Cybersecurity. Aan een nieuwe ad-opleiding Cybersecurity met een eigen niveau en werkveldgerichtheid zou volgens de eigen marktverkenningen grote behoefte bestaan in het werkveld en deze zou volgens plan ondergebracht worden in het HvA Community College, een aparte organisatorische eenheid binnen HvA speciaal ingericht voor ad-opleidingen[1].

HvA heeft bij nader inzien gekozen voor positionering bij de Faculteit Digitale Media en Creatieve Industrie. Uit het gesprek met het management blijkt dat deze positionering in de eerste plaats beter aansluit bij het streven om een 'doorlopende leerlijn' mogelijk te maken: vanuit het mbo 4-keuzedeel Cybersecurity aan het ROC van Amsterdam kan gekozen worden voor de ad-opleiding Cybersecurity HvA met daarna een eventuele doorstroom naar de (eigen) bacheloropleiding-Cybersecurity HvA. Om eventuele verdere doorstroom mogelijk te maken wil de HvA ook een nieuwe masteropleiding-Cybersecurity gaan ontwikkelen. In de tweede plaats profiteert de ad-opleiding Cybersecurity beter van de inhoudelijke verwantschap van de beide curricula ('natuurlijke habitat') en van de docenten van de bacheloropleiding. Door het management is tegelijkertijd ook aangegeven dat de herpositionering geen negatieve impact zal hebben op de ad-opleiding Cybersecurity: de opleiding is eigenstandig als ad-opleiding ontwikkeld door een breed samengesteld ontwerpteam. De curriculumcoördinator van de ad-opleiding Cybersecurity, die sturing heeft gegeven aan het ontwerpteam, is tevens de waarnemend opleidingsmanager van de bacheloropleiding ICT (de leiding blijft dus bij dezelfde functionaris). Tegelijkertijd zal de binding met het HvA Community College blijven bestaan: de expertise zal blijvend worden gedeeld.

3.3 Profiel Opleiding

In Nederland bestaan nog geen ad-opleidingen Cybersecurity. De ad-opleiding Cybersecurity van de HvA wil zich volgens het informatiedossier gaan richten op: '*De ad-cybersecurityprofessional die met zijn hbo werk - en denkniveau, zijn zelfstandigheid en zijn vakkennis in staat is om operationeel-tactische taken van (afgestudeerde) hbo- en wo-cyberprofessionals over te nemen, zodat deze zich kunnen richten op de meer strategische vraagstukken op het gebied van cybersecurity'.* Het profiel van de opleiding is gericht

[1] *In het informatiedossier werd nog gekozen voor positionering bij het HvA Community College.*

op ad-professionals die beschikken over *een brede basis in ICT* aangevuld met specifieke kennis over en ruime praktijkervaring met het *cybersecurityproces*. In het onderwijsconcept is veel aandacht voor het *lerend en reflecterend* vermogen van studenten, zodat studenten leren hoe ze steeds nieuwe kennis kunnen vergaren en hoe ze daarbij kunnen omgaan met de snelle ontwikkelingen in het vakgebied. Op 15 augustus 2018 heeft het Ministerie van Onderwijs, Cultuur & Wetenschap een positief besluit genomen over de macrodoelmatigheidsaanvraag. Volgens het informatiedossier is er in Nederland, en zeker in de metropoolregio Amsterdam, een grote vraag is naar dit type goed opgeleide cybersecurityprofessionals.

4 Beoordeling per standaard

In dit hoofdstuk wordt de evaluatie door het panel van de standaarden omschreven. Bij elke standaard geeft het panel zijn bevindingen, overwegingen en oordeel weer. De beoordeling is gebaseerd op de standaarden en criteria zoals beschreven in het Beoordelingskader voor de beperkte Toets Nieuwe Opleiding van de NVAO (Stcrt. 2016, nr 69458). De beoordeling komt tot stand op basis van een discussie met 'peers' over de inhoud en kwaliteit van de opleiding.

Over de standaarden geeft een visitatiepanel een gemotiveerd oordeel op een driepuntsschaal: voldoet, voldoet ten dele of voldoet niet. Vervolgens geeft het panel een gemotiveerd eindoordeel over de kwaliteit van de opleiding, ook op een driepuntsschaal: positief, positief onder voorwaarden, of negatief.

4.1 Standaard 1: Beoogde leerresultaten

De beoogde leerresultaten passen bij het niveau en de oriëntatie van de opleiding en zijn afgestemd op de verwachtingen van het beroepenveld en het vakgebied en op internationale eisen.

Bevindingen
Sinds 2014 participeert HvA in het CSCMRA (Cybersecurity Centre Metropoolregio Amsterdam), een publieke-private samenwerkingsorganisatie op het gebied van cybersecurity. Het CSCMRA heeft de HvA in juni 2018 het verzoek gedaan een ad-opleiding Cybersecurity te ontwikkelen. Samen met *stakeholders* zoals CSCMRA, een aantal bedrijven en het ROC van Amsterdam heeft het ontwerpteam het profiel voor de ad-opleiding Cybersecurity ontwikkeld. Aan het ontwerpteam namen vanuit de HvA deel: de curriculumcoördinator en docenten van de ad-opleiding, onderwijskundigen en docenten van de bacheloropleiding.

In het informatiedossier en *Beroeps- en Opleidingsprofiel ad-opleiding Cybersecurity* onderbouwt de opleiding haar profiel op basis van uiteenlopende bronnen[2]. In de eerste plaats wordt met deze opleiding beoogd aan te sluiten bij recente ontwikkelingen en risico's. Het gaat onder meer om: '*de complexiteit van ICT-voorzieningen en de toenemende afhankelijkheid daarvan, het toenemende gebruik van internetdiensten voor persoonsgegevens en de populariteit van sociale media leggen nieuwe kwetsbaarheden bloot, die kunnen leiden tot misbruik'*. Ook sluit de opleiding aan bij de maatschappelijk ervaren noodzaak om hier iets tegen te willen doen door uit te gaan van actuele definities van cybersecurity: *'Cybersecurity is het voorkomen van gevaar of schade, veroorzaakt door storing of uitval van ICT of door misbruik van ICT'*[3].

In de tweede plaats zijn de beoogde taken, bekwaamheden en functies waaraan de ad-cybersecurityprofessional moet voldoen in drie sessies met het werkveld en overige stakeholders besproken, waarbij is gekeken of de inhoud van de opleiding aansluit bij de behoefte van het bedrijfsleven. Hierbij is ook gekeken naar de 'kolom' van mbo-, hbo-bachelor- en wo-cybersecurity-opleidingen, waarbij is gelet op die aspecten waar de doorlopende leerlijn ontbreekt gericht op het 'operationeel-tactische' niveau. De opleiding leidt op tot professionals die vanuit een stevige basis in ICT gericht zijn op het cybersecurityproces. Het gaat in essentie om functies als 'ethical hacker, pentester of threathunter', maar ook breder - zoals cyber incident response professional, cyber threat analyst en security tester - bij bedrijven, banken en (overheids-)organisaties. Er is gekozen om de zes kerntaken

[2] *Bronnen: HBO-i (2014). Domeinbeschrijving Bachelor of ICT; European e-Compentence Framework (2016). European e-Compentence Framework 3.0; PTES standaard: een internationale standaard voor penetration testing; PvIB en QIS (2014). Beroepsprofielen Informatiebeveiliging; National Institute of Standards and Technology (NIST), US Department of Commerce (2018). Framework for Improving Critical Infrastructure Cybersecurity V1.1; SBB Kwalificatiedossiers MBO 4 keuzedelen ICT beheer en Security in systemen en netwerken.*
[3] *Zoals beschreven in de Nationale Cyber Security Strategie en door de Nationaal Coördinator Terrorismebestrijding en Veiligheid.*

van de PTES-standaard[4], een internationale industrie de facto standaard voor penetration testing, centraal te stellen (Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting). Deze standaard geeft volgens de opleiding een stevige methodische basis om actuele cybersecurityvraagstukken in de breedte te benaderen. Belangrijke bekwaamheden van deze professionals zijn onder andere: leren denken en handelen vanuit verschillende perspectieven, zowel vanuit de aanvaller als vanuit de organisatie, het werken met vertrouwelijke informatie, kritieke systemen en infrastructuren en het lerend vermogen.

Het ontwerpteam heeft in aansluiting op de zes kerntaken drie beoogde leerresultaten (fasen) van de opleiding geformuleerd. Kort samengevat gaat het om: Identify (inventariseren welke ICT-assets er zijn en welke beschermd moeten worden), Analysis (in kaart brengen van risico's en bedreigingen en op basis van de analyse van de ICT-assets de beveiliging testen), Exploit (ontdekken van kwetsbaarheden en op methodische en ethische wijze gevolgen van risico's aantonen en een advies geven voor te nemen maatregelen). In de formuleringen van de leerresultaten en de uitwerkingen naar beroepstaken, beroepsproducten, gedragsindicatoren en gedragscriteria zijn de gewenste bekwaamheden, het ad-niveau en de BoKS verwerkt. In diverse tabellen zijn de leerresultaten gelegd naast de gedragsindicatoren van niveau 5: Methodisch handelen, Samenwerken, Communiceren, Probleemoplossend vermogen en Lerend vermogen (EQF, NLQF, Vereniging Hogescholen) en naast de HBO-i indeling in activiteiten/architectuurlagen[5]. Ook is de algemene typering in rollen en niveaus (afgeleid van de leerresultaten) gelegd naast die van Mbo 4 (keuzedeel Cybersecurity) en Hbo-bachelor ICT (leerroute Cybersecurity).

In de diverse gesprekken van het panel met het management, de docenten en de vertegenwoordigers van het werkveld is de profilering en de onderbouwing daarvan besproken. Alle gesprekspartners, met name vertegenwoordigers van het werkveld, gaven aan dat er grote behoefte bestaat aan cybersecurityprofessionals met dit profiel. Een eerste punt in de diverse gesprekken was: het flexibel inzetten van het profiel. De opleiding wil het profiel vier keer per jaar gaan bespreken op actualiteit en relevantie met een onderwijsadviesraad bestaande uit vertegenwoordigers van de diverse stakeholders en zonodig het profiel bijstellen. Een tweede punt waar het panel aandacht voor vroeg was (los van flexibiliteit) het 'inpassen van specifieke technische en juridische kennis' in de beoogde leerresultaten. Kennis die essentieel is en die volgens het panel gekoppeld zou moeten worden aan beoogde leerresultaten. Hier is volgens de gesprekspartners aandacht voor, maar docenten willen dit ook niet te precies vastleggen. Een derde terugkerend punt tijdens de gesprekken was de keuze voor de brede naam van de opleiding 'Cybersecurity' versus de enigszins afgebakende inhoud van de opleiding (voornamelijk 'offensief'). Het ontwerpteam van de opleiding gaf aan dat het defensieve element enigszins is opgenomen, maar dat de focus van de opleiding in eerste instantie zal liggen op pentesting (offensief). In dit licht vroeg het panel aandacht voor: 'hoe de opleiding zich verhoudt tot het bredere cybersecuritykader van IEEE/ACM/IFIP[6]', het richtinggevend internationaal referentiekader voor academische opleidingen.

Overwegingen
Het panel vindt de wijze waarop het ontwerpteam in nauwe samenspraak met de stakeholders (CSCMRA, werkveld, partners vanuit het ROC, collega's vanuit de bachelor-Cybersecurity) gekomen is tot een profiel - rekening houdend met de kolom van mbo-, hbo- en wo-cybersecurity-opleidingen - positief. Het profiel is actueel en vanuit het werkveld bestaat er grote behoefte aan. Door het management en de docenten van de opleiding werd aangegeven dat de opleiding kiest voor een 'dynamisch profiel' dat meebeweegt met behoeftes (vraagarticulatie) uit het werkveld. Het panel vindt dit in principe positief, omdat het vakgebied en het werkveld enorm in beweging is.

[4] *Bij de PTES-standaard, die in 2009 is ontstaan vanuit het internationale bedrijfsleven, gaat het eigenlijk om zeven taken, maar de laatste taak Reporting heeft de opleiding toegevoegd aan (verdeeld over) de eerste zes taken.*
[5] *HBO-i (2014). Domeinbeschrijving Bachelor of ICT.*
[6] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

De opleiding heeft een eigen beroeps- en opleidingsprofiel opgesteld. De keuze voor de zes kerntaken van de PTES-standaard en de aansluitende formulering naar de drie beoogde leerresultaten (met uitwerkingen) is transparant en concreet. Vooral de gedragsindicatoren vindt het panel goed uitgewerkt: alle gedragscriteria zijn ingedeeld naar Methodisch handelen, Probleemoplossend vermogen, Samenwerken, Communiceren en Lerend vermogen. Er is aandacht voor rapporteren (Nederlands) en taalvaardigheid (Nederlands en Engels). De basiskennis van ICT- en Cybersecurity is vastgelegd en gekoppeld aan leerresulaten (beroepstaken en tevens fasen).

Ten aanzien van de onderbouwing van de keuze voor de PTES-standaard en leerresultaten merkt het panel op dat het ad-niveau, de inhoud en de orientatie goed is geborgd doordat er ijking heeft plaatsgevonden met relevante (inter-)nationale referentiekaders. Het panel onderschrijft deze keuze vanuit de context van de opleiding, waarbij met name het ad-niveau goed uit de verf komt.
Het panel mist wel een onderbouwing vanuit het (bredere en toonaangevende) internationale referentiekader van IEEE/ACM/IFIP. Ook al is dit laatste kader gericht op bachelor- en masteropleidingen, het panel geeft de opleiding ter overweging mede op basis van dit raamwerk te profileren[7]. Ten aanzien van keuze voor BoKS heeft het panel vastgesteld dat bepaalde technische, juridische kennis en vaardigheden in de leerresultaten (te) bondig zijn opgenomen. Het panel adviseert dan ook in ieder geval juridische kennis, bijkomende technische kennis en ethisch verantwoord handelen aan de beoogde leerresultaten toe te voegen (zie verder Standaard 2).

Het panel is van mening dat de opleiding zich nog beter kan positioneren. De (brede) naam Cybersecurity dekt niet geheel de inhoud van de opleiding die vooral gericht is op penetratietesting (offensief) en in mindere mate op advisering aan de opdrachtgever hoe kwetsbaarheden (risico's) te voorkomen of te verhelpen (defensief). Het panel raadt aan om in het profiel meer recht te doen aan de (bredere) inhoud.

Conclusie: Voldoet

4.2 Standaard 2: Onderwijsleeromgeving

Het programma, de onderwijsleeromgeving en de kwaliteit van het docententeam maken het voor de instromende studenten mogelijk de beoogde leerresultaten te realiseren.

Bevindingen
In het informatiedossier en het *Leerplanschema* is de inhoudelijke opbouw en structuur beschreven. De drie leerresultaten Identify, Analysis en Exploit bestrijken de eerste drie semesters, waarbij ieder semester is verdeeld over twee beroepstaken (één beroepstaak per blok van 15 EC): Identify is vertaald naar Blok 1 (Pre-engagement interaction) en Blok 2 (Intelligence gathering); Analysis is vertaald naar Blok 3 (Threat modelling) en Blok 4 (Vulnerability analysis) en Exploit is vertaald naar Blok 5 (Exploitation) en Blok 6 (Post-exploitation & advice). Het vierde en laatste semester staat in het teken van integratie van leerresultaten en is verdeeld over Blok 7 (Vrije keuzeruimte) en Blok 8 (Afstudeeropdracht). De afstudeeropdracht (15 EC) en de vrije keuzeruimte (15 EC) kunnen worden verdeeld over beide laatste blokken.

In het *Leerplanschema* is ieder blok (beroepstaak) *uitgewerkt* naar drie praktijkvraagstukken en opdrachten per leerlijn (5 EC per blok). In de *Studiegids, de Studiehandleidingen* die het panel heeft bekeken (1 t/m 4), de *Afstudeerhandleiding* en op de online leeromgeving (Brightspace) zijn de praktijkvraagstukken en opdrachten voorzien van werkvormen, ondersteunend materiaal, planning, beoordeling en herkansing[8]. Hierbij vormen de gedragsindicatoren (Methodisch handelen, Probleemoplossend vermogen, Samenwerken, Communiceren en Lerend vermogen) steeds de verbindende schakel. Vooral Methodisch handelen en Probleemoplossend vermogen zijn *inhoudelijk* geconcretiseerd, aansluitend bij de betreffende beroepstaak.

[7] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
[8] *In de Studiegids is ook docentinzet en studiemateriaal opgenomen.*

In het onderwijs van de eerste drie semesters is er gekozen voor een duidelijke *structuur* op basis van drie (interfererende) leerlijnen (zie Afbeelding bijlage 4 van dit rapport):

- *OnTheJob*, waarbij de student met een groep van medestudenten werkt aan actuele praktijkopdrachten ingebracht vanuit het werkveld. Dit kan in het cybersecuritylab of bij de opdrachtgever (twee dagen per week).
- *Fundamentals*, in de werkcolleges en door het maken van opdrachten worden de benodigde fundamentele kennis en vaardigheden door de opleiding aangereikt en door studenten toegepast (twee dagen per week). In jaar 1 ligt accent op Infrastructure Security, Operating System Security en Offensive Programming (Python). In jaar 2 ligt accent op Threat Intelligence en Threat Hunting.
- *Boosterweken*, vormen een verbindende schakel tussen de genoemde twee (parallelle) leerlijnen. Op een intensieve wijze werken studenten gedurende een week aan een combinatie van opdrachten, workshops, kennisdeling, rapporteren en presentaties. Er is ruimte voor actuele ontwikkelingen binnen het cybersecuritywerkveld (twee keer per blok gedurende een week).

In de afstudeermodule laat de student zien dat hij dat hij of zij zelfstandig, gestructureerd en ethisch verantwoord een cybersecurityopdracht uit de beroepspraktijk uitvoert, waarbij de leerresultaten integraal worden beheerst op niveau 5.

Het *didactisch concept* van ad-opleiding Cybersecurity is gebaseerd op het HILL-model[9]. Centraal staan: 1) praktijkvraagstukken in een rijke leeromgeving, 2) student aan het roer en 3) assessment as learning:

- 'Rijke leeromgeving' komt terug in leren op school, in het cybersecuritylab, bij de opdrachtgever en online. 'Praktijkvraagstukken' staan centraal in het cybersecuritylab waar mbo-, ad- en hbo-studenten met elkaar werken aan praktijkvraagstukken of in groepjes binnen bedrijven (OnTheJob).
- 'Student aan het roer': studenten krijgen ruimte om binnen de geformuleerde leerresultaten zelf praktijkopdrachten te mogen kiezen, zij kunnen variëren in tijd waarmee deze opdrachten kunnen worden ingeleverd (flexibele inlevermomenten) en zij mogen zelf nadenken over bewijslast. Tevens kunnen studenten in de keuzeruimte kiezen uit verschillende modules.
- Bij 'Assessment as learning' staat het lerend vermogen centraal; de begeleiding is passend bij de ontwikkelbehoefte van de student. Halverwege het blok wordt een formatief individueel voortgangsgesprek gevoerd met een docent en aan het eind van het blok een formatief professioneel gesprek met de mentor over het leerproces. Steeds wordt terug- en vooruitgeblikt.

In de gesprekken hebben het management en de docenten de inhoudelijke opbouw, de structuur en de didactische opzet van het curriculum toegelicht. Hierbij is eerst ingegaan op sturing van opdrachten. Bij het vaststellen van geschikte praktijkopdrachten voor de OntheJob-lijn selecteert de curriculumcoördinator samen met twee docenten die opdrachten die geschikt zijn voor het betreffende blok. Hierbij wordt gelet op complexiteit, reikwijdte van de opdracht en aansluiting bij de professionele ontwikkeling van de student (toename in niveaubeheersing). Voor het aandragen van praktijkopdrachten wordt samengewerkt met het CSCMRA, waarbij meer dan 80 bedrijven zijn aangesloten (zo werd bevestigd door het werkveld). Bij de OnTheJob-lijn wordt tijdens de eerste vier weken gestart op school om de studenten goed voor te bereiden op de praktijkopdrachten. Bij de vaststelling van de afstudeeropdracht wordt het onderwerp vooraf door een afstudeercommissie, bestaande uit docenten en vertegenwoordigers uit het werkveld, getoetst op niveau en relevantie.

Op enkele punten werd tijdens de gesprekken langer stilgestaan. Een *eerste* aspect is de doorvertaling ('coverage') van de beoogde leerresultaten in het curriculum. Het panel, dat voorafgaand aan de visitatie beschikte over de Studiehandleiding van blok 2 vond dat de inhoud van dit blok onvoldoende in lijn was met de uitgangspunten van het Leerplanschema (bijvoorbeeld de eindopdracht bij Blok 2 bevat een exploitatievraag die focus zou moeten zijn van semester 3). Daarnaast miste het panel aandacht in de doorvertaling voor de borging van essentiële kennis en vaardigheden zoals bepaalde technische kennis (beveiligingspolitiek, beveiligingsarchitectuur, beveiliging van web applicaties, hardware beveiliging, veilige software ontwikkeling), een juridische kader en ethisch verantwoord handelen. Met name bij aanvang van de opleiding moet hier volgens het panel al aandacht voor zijn. Het panel heeft deze aspecten voorgelegd aan de gesprekspartners van de opleiding. Zij gaven aan dat gedragsindicatoren met opzet wat algemener worden geformuleerd (zodat in het onderwijs voor

[9] *Didactisch Concept HvA community College: High Impact Learning that Lasts (HILL-model) van Philip Dochy. Doelen die met dit didactische model worden beoogd: diepgaand leren, zelfsturing en aansluiting bij de praktijk.*

meerdere methoden of tools kan worden gekozen). Aan ethiek wordt bij de diverse leerlijnen aandacht besteed. Ook worden studenten geacht bij aanvang van de opleiding een verklaring te ondertekenen die aangeeft dat de opgedane kennis en vaardigheden niet worden misbruikt. Juridische kennis is volgens docenten niet structureel ingebouwd, maar kan volgens hen wel worden gekozen als keuzevak.

Een *tweede* aspect is dat het didactisch model volgens het panel hoge eisen stelt aan docenten met het oog op de verschillende rollen die zij gaan vervullen (docent-examinator en mentor/ coach). Docenten hebben uitgelegd dat zij in staat zijn om zowel de ICT- en Cybersecurityvakken te geven als de meer communicatiegerichte vakken; daarnaast kan er rijkelijk geput worden uit het (gespecialiseerde) docentenkorps van de bachelor ICT-opleiding van de HvA.

Een *derde* aspect is dat vanaf september 2019 rekening gehouden wordt met een beperkte instroom van ongeveer 35 studenten. Uitgaande van een student-docentratio van 1: 24 gaat er waarschijnlijk worden gestart met twee groepen. De opleiding hecht eraan om 'kwalitatief goed en rustig te beginnen' met als streven 'de studenten te leren kennen'.

Een *vierde* aspect is de aandacht voor taal (Nederlands en Engels). Docenten hebben uitgelegd dat 'maatwerk' ook in het aanleren van Nederlands, centraal staat. In de eerste plaats wordt hier middels persoonlijke feedback aan de student - gericht op het presenteren en vele rapporteren - aandacht aan besteed. Ook kunnen er ondersteunende trajecten vanuit HvA worden aangereikt zoals Taaluniversum en het taalspreekuur van de dienst Studentzaken. Aan Engels wordt aandacht besteed doordat alle presentaties en powerpoints (docenten) en veel sjablonen (vanuit het werkveld) in het Engels zijn opgesteld. Er hoeft niet volledig in het Engels gerapporteerd te worden (maar dit mag wel).

Een *vijfde* aspect is het werken met of het inkopen van (delen van) programma's en certificaten bij aanbieders van geschikte trainingen zoals CICO, CCICO, CEH, OSCP (zoals vermeld op de literatuurlijst). Docenten gaven aan geen commerciële banden te hebben met de bedrijven, leveranciers van deze trainingen. Wel worden onderdelen van programma's gebruikt van bijvoorbeeld Cisco Networking Academy omdat het materiaal volgens hen goed is, zowel qua invulling als didactiek. In de keuzemodule kunnen studenten wel relevante externe certificeringstrajecten volgen.

Een *zesde* aspect betreft aansluiting op instromende studenten, studiebegeleiding en studeerbaarheid van het programma. Het panel vroeg zich af hoe de opleiding aansluit bij de verschillende instroom-niveaus en hoe hier op wordt ingespeeld in de studiebegeleiding. Studenten die toelaatbaar zijn (minimaal mbo-4 of havo) nemen deel aan de verplichte studiekeuzecheck (vragenlijsten en opdracht), het studiekeuzegesprek en ontvangen daarna een schriftelijk advies, dat als eerste document aan hun studentportfolio moet worden toegevoegd. Ook wordt er rekening gehouden met een 'aanloopniveau', waarbij studenten met wisselende snelheid door de opleiding kunnen gaan. Docenten noemen dat als een onderdeel niet wordt gehaald er getracht wordt flexibiliteit in te bouwen waarbij er al met een volgende fase gestart kan worden. In de didactiek wordt recht wordt gedaan aan diversiteit en differentiatie. Studenten kunnen als keuzemodule vaste onderdelen van de minor Information Security van de bacheloropleiding ICT van de HvA volgen (gericht op vergemakkelijken van de doorstroom naar de hbo-bachelor).

Een *zevende* aspect betreft de inrichting van de voorzieningen. Er wordt ervan uitgegaan dat studenten beschikken over een eigen laptop. Naast beschikbaarheid van internet en de online leeromgeving, zullen voldoende les- en werkruimtes beschikbaar zijn en adequaat worden ingericht (cybersecuritylab, werkcolleges, individuele werkruimtes en werkruimtes voor groepen).

Een *achtste* (en laatste) aspect betreft de opleidingsspecifieke kwaliteitszorg. Docenten geven aan bij aanvang van de opleiding in september 2019 zo snel mogelijk te willen starten met het formeren van een opleidingscommissie (OC) bestaande uit twee docenten en twee studenten. De rechten en plichten van deze commissie zijn vastgelegd in een HvA breed reglement.

Overwegingen
Het panel stelt vast dat het gehanteerde onderwijsconcept (HILL) met haar didactische uitgangspunten goed aansluit bij de beoogde studenten van ad-opleiding Cybersecurity. Er is sprake van een sterke afwisseling in leeromgevingen en werkvormen met voldoende individuele aandacht voor het leerproces.

De structuur is strak uitgewerkt: studenten werken vier dagen per week afwisselend aan praktijkopdrachten (OnTheJob) en aan het opdoen van fundamentele kennis en vaardigheden (Fundamentals). In de twee Boosterweken werken studenten (groepsgewijs en individueel) aan toepassing, integratie en professionele vaardigheden. De wisselwerking theorie en praktijk, waarbij de praktijkopdrachten in samenwerking met bedrijven worden vastgesteld, maakt de leerstof relevant en actueel. Ook de Boosterweken zijn volgens het panel representatrief voor 'hoe in het werkveld vaak moet worden gewerkt: onder tijdsdruk, intensief, gericht op samenwerking, vanuit complexe problemen handelend en met verantwoordelijkheid optreden'.

Het panel heeft geconstateerd dat de inhoud van het programma (leerplanschema) studenten op hoofdlijn in staat stelt om de beoogde leerresultaten te verwerven. De beroepstaken, globale leerinhouden, uitwerking naar gedragsindicatoren, invulling van werk- en toetsvormen van het onderwijsprogramma zijn deels 'in lijn' met deze leerresultaten; er is sprake van constructive alignment. Er is aandacht voor beroepsvraagstukken, vaardigheden en attitudes. Internationalisering komt aan de orde (Engelstaligheid in casuistiek) en er is voldoende aandacht voor rapporteren. Centraal in het programma staat: Infrastructure Security, Operating System Security en Offensive Programming, Python (jaar 1) en Threat Intelligence en Threat Hunting (jaar 2). Er is oog voor de opbouw van het programma door te werken met steeds complexere praktijkopdrachten en voor de borging van het afstudeerniveau in de afstudeeropdracht door een afstudeercommissie. In de keuzemodule kunnen studenten externe certificeringstrajecten volgen (zoals OSCP), wat het panel positief vindt, omdat een dergelijk certificaat in het werkveld veel wordt gevraagd. Vanuit het ontwerpteam is op basis van het leerplanschema en feedback van vertegenwoordigers van het werkveld gestuurd op het te ontwikkelen materiaal, zo blijkt ook uit gesprekken met management, werkveld en docenten.

Het panel heeft de eerste vier studiehandleidingen en het onderliggende studiemateriaal (Brightspace) bekeken en heeft kanttekeningen bij de doorvertaling (coverage) van de beoogde leerresultaten, gedragsindicatoren en BoKS - vanuit het leerplanschema - naar het concrete studiemateriaal (opdrachten met beoordelingscriteria, inhoud van lessen, planning, lesmateriaal). Het betreft vooral de leerlijn Fundamentals. De eerste is dat er in het bekeken studiemateriaal in zeer geringe mate wordt ingegaan op het defensieve aspect van cybersecurity. Dit is ook al bij Standaard 1 genoemd en hier wil het panel nu geen aanbeveling aan verbinden. Wel suggereert het panel de inhoud van het tweede jaar iets sterker op verdediging (blue-team) te richten. De tweede is dat er 'meerdere lagen' in leerdoelen lijken te zijn, waarbij vooral de verbinding met de leerdoelen van het studiemateriaal (Brightspace) nog onvoldoende transparant is. De derde is dat aan borging van essentiële kennis en vaardigheden (BoKS) niet die aandacht wordt besteed die het panel noodzakelijk acht. Concreet gaat het bij het laatste punt vooral om het ontbreken van een juridisch kader en bepaalde technische kennis (beveiligingspolitiek, beveiligingsarchitectuur, beveiliging van webapplicaties, hardware beveiliging, veilige softwareontwikkeling). Het panel is van mening dat wetgeving over hacking en privacy (GDPR) onontbeerlijk is voor het goed kunnen functioneren van cybersecurityprofessionals in het werkveld[10]. Het feit dat studenten dit als keuzevak kunnen kiezen biedt onvoldoende garantie dat *alle* studenten deze kennis bemachtigen. Het panel vindt het wenselijk dat bij aanvang van de studie hier al aandacht voor is in het programma, waarbij het panel suggereert dat alle ketenpartners (zoals Politie en Openbaar Ministerie) aan bod komen met als doel dat de student van meet af aan een goed besef krijgt over het juridische kader en ethische bezwaren. Aangezien de doorvertaling van de juridische, technische en ethische aspecten dus niet volledig inzichtelijk is in het feitelijke studiemateriaal wil het panel hier een voorwaarde aan verbinden.

Het panel is van oordeel dat de opleiding adequate instroomeisen hanteert (minimaal mbo-4 of havo) en een toelatingsprocedure heeft vormgegeven. Volgens het panel ondersteunen de geboden studiebegeleiding en de informatievoorziening de student in voldoende mate. De professionele ontwikkeling wordt begeleid door een vaste mentor en de studievoortgang door docenten. De opleiding wil een persoonlijk leerklimaat creëren waar de student 'gezien wordt, fouten mag maken en waar constructieve en waarderende feedback gemeengoed is'. Bij studenten met (taal)deficiënties is - vanuit

[10] *De kans is volgens het panel groot dat penetration testers in aanraking komen met juridische en zelfs strafrechtelijke discussies en dus een basisnoties moeten hebben van wetgeving (ook buiten Nederland).*

de persoonlijke begeleiding en voorzieningen vanuit de HvA - voldoende maatwerk mogelijk. Er is hierbij oog voor diversiteit en differentiatie.

Het panel heeft kennisgenomen van de cv's van zowel het kernteam als van docenten die breder inzetbaar zijn (vanuit de bacheloropleiding ICT) voor de ad-opleiding Cybersecurity. Het kernteam van docenten is volgens het panel in staat om een inhoudelijk, onderwijskundig en organisatorisch het programma te realiseren voor de ad-opleiding Cybersecurity. Het personeelsbeleid van de HvA (scholing, beoordeling) geldt ook voor deze opleiding. Wel hebben kerndocenten te maken met uiteenlopende rollen (docent-examinator, begeleider en mentor), wat volgens het panel mogelijk druk op hen kan leggen. 'Scheiding in rollen bewerkstelligen' is volgens het panel een aandachtspunt voor het management: minimaal op persoonsniveau of nog beter in verschillende docentrollen die door meerdere mensen worden vervuld (bijvoorbeeld een examinator is niet ook begeleider en ook nog mentor van dezelfde student in dezelfde studiefase).

Het panel stelt vast dat huisvesting en materiële voorzieningen voldoen en dat aan de opleidingsspecifieke kwaliteitszorg voldoende aandacht wordt besteed. De beleidskaders gericht op personeel, voorzieningen en kwaliteitszorg van de HvA gelden ook voor deze opleiding.

Alles overziend is het panel van mening dat de onderwijsleeromgeving en de kwaliteit van het docententeam in ruime mate voldoen, maar dat de inhoudelijke doorvertaling van het programma nog niet voldoende transparant is. Het panel heeft daarom als voorwaarde geformuleerd dat de doorvertaling (coverage) van de beoogde leerresultaten, met name bij de Fundamentals, ten aanzien van essentiële BoKS inzichtelijker moet worden. Hierbij moet in ieder geval kennis over relevante wetgeving, bijkomende technische kennis (zie hierboven) en verantwoord ethisch handelen zichtbaar terugkomen in het curriculum.

Conclusie: Voldoet ten dele.

4.3 Standaard 3: Toetsing

De opleiding beschikt over een adequaat systeem van toetsing.
Het toetsbeleid van de ad-opleiding Cybersecurity staat beschreven in het informatiedossier en het *Toetsplan,* het sluit aan bij het toetsbeleid en de toetskaders van HvA. In de *OER 2019-2020* en het *Toetsplan* is het verkorte toetsprogramma opgenomen waarbij wordt aangegeven dat iedere onderwijseenheid van 5EC wordt afgesloten met een opdracht (waarbij een tweede gelegenheid wordt geboden in het blok erna).

In de *Studiegids* en de studiehandleidingen staan de toetsvormen van de opdracht vermeld:
- bij de opdrachten van de OnTheJob-leerlijn wordt getoetst op basis van een portfolio met beroepsproduct, presentatie, reflectie en verantwoording;
- bij de Fundamentals- en Boosterweken wordt getoetst op basis van een portfolio met een variatie aan opdrachten.

Voor alle opdrachten is de normering identiek: er wordt beoordeeld met een cijfer (met 1 decimaal), dat gegeven wordt door de docent op basis van de beoordelingsformulieren met rubrics. In de beoordelingsformulieren wordt getoetst op 1) de aanwezigheid van bewijslast[11], en 2) op de gedragsindicatoren met beoordelingsschalen (nog niet bekwaam, bekwaam, gevorderd en excellent) gekoppeld aan een puntentelling en een cesuur.
Naast het summatief toetsen van de opdrachten door de docent wordt er gewerkt met formatief toetsen door de mentor conform het uitgangspunt 'assessment as learning' (zie Standaard 2). In bijlage 4 bij dit rapport is de toetssystematiek in een afbeelding weergegeven. In week 10 van ieder blok voert de (vaste) mentor een formatief professioneel gesprek; alleen bij de afstudeeropdracht wordt gewerkt met een portfolioassessment. Voorwaarde voor het toekennen van het eindcijfer per blok is dat het professionele gesprek of het portfolioassessment is afgerond.

[11] *Aan de volgende randvoorwaarden moet worden voldaan (Taalgebruik, APA, portfolio is volledig ingeleverd op Brightspace (inclusief plagiaattoets), het beroepsproduct moet een op zichzelf staands product zijn) om het portfolio te kunnen beoordelen.*

Bij de toetsing van afstudeeropdracht, zoals beschreven in de *Afstudeerhandleiding*, wordt gezamenlijk beoordeeld door de afstudeerbegeleider en een onafhankelijk assessor, die samen het portfolio en het assessment (de presentatie en verdediging) beoordelen en daarbij het advies van de bedrijfsbegeleider laten meewegen. Soms is er een externe beoordelaar aanwezig. De assessor speelt voornamelijk een rol bij de beoordeling van de afstudeeropdracht, is voorzitter tijdens de afstudeerzitting (het assessment) en vult het beoordelingsformulier in. Dit formulier is identiek aan de formulieren van de eerdere opdrachten, zij het dat de voorwaarden van het verantwoordingsdocument sterker toegesneden zijn op onderzoek en de stappen van het proces in de ontwikkeling van het beroepsproduct.

In diverse documenten geeft de opleiding aan dat in de visie op toetsing de twee functies van toetsen, namelijk 'leren en beoordelen', leidend zijn. Voor het beoordelings- en leerproces gelden dezelfde kaders. De toetsing is 'integraal': de leerresultaten, die het resultaat zijn van het leerproces, worden getoetst en vinden hun neerslag in (beroeps)producten en verantwoordingsdocumenten. Er zijn geen toetsen die zonder context en gefragmenteerd de onderliggende kennis- en vaardighedenbasis toetsen. Tijdens de *professionele gesprekken* wordt telkens gekeken naar het hele leerproces van de student in het licht van het curriculum en het beroepsprofiel (via de gedragscriteria). Elk blok start met een sessie waarin het beoogde leerresultaat van de periode wordt verkend evenals de gedragscriteria waaraan de student gaat werken. Feedup (waar ga ik naar toe?) en feedforward (suggesties voor aanpak van vraagstukken) staan centraal. Na afloop van de sessie neemt de student conclusies op in het ontwikkelplan, waarbij de feedback uit het vorige blok wordt meegenomen. Feedback verzamelen is dus een belangrijk onderdeel van het leerproces (vanuit docenten, opdrachtgevers in de praktijk, medestudenten en zelfreflectie) waarvoor de opleiding veel methoden en tools (zoals Feedbackfruits[12]).

De validiteit, betrouwbaarheid en transparantie van de toetsing en de toetssystematiek wordt op diverse wijzen geborgd:

- de curriculumcoördinator is verantwoordelijk voor de samenstelling van het toetsprogramma, conform de uitgangspunten van het toetsplan;
- de blokcoördinator is verantwoordelijk voor de kwaliteit van de toetsing van een blok en stemt hierbij af met het docententeam van het blok en met de curriculumcoördinator. Deze coördinator maakt van elk blok een toetsdossier[13];
- in de opleiding worden concrete afspraken gemaakt over regelmatige kalibratiesessies zowel tussen docenten onderling als met beoordelaars van andere hogescholen. Ook wordt de beoordeling /evaluatie van de eindtoetsing besproken in de onderwijsadviesraad (betrokkenheid vanuit werkveld);
- de examencommissie die is samengesteld uit een onafhankelijk voorzitter, een lid van de examencommissie en een extern-lid[14], borgt de kwaliteit van de toetsing en het eindniveau van de opleiding (afstudeeropdracht). Verder stelt de examencommissie jaarlijks de docent-examinatoren aan op basis van duidelijke criteria (gericht op kwalificaties zoals SKE, regelmatige bijscholing, kennis van de beroepspraktijk), wordt jaarlijks een borgingsagenda opgesteld, vinden jaarlijkse steekproefsgewijze controles plaats op toetsdossiers, zijn er adviesgesprekken met docenten op basis van hun toetsdossiers en wordt verslag gedaan van bevindingen in een jaarverslag.

In het gesprek met het panel hebben de leden van de examencommissie en onderwijskundig medewerker de zojuist beschreven werkwijze van de examencommissie bevestigd. Ook hebben zij een toelichting gegeven op hun visie op de gekozen toetssystematiek en de borging daarvan in het licht van eisen zoals betrouwbaarheid, validiteit en transparantie. De examencommissie vindt de vertaling van 'assessment as learning' naar de toetsgesprekscyclus bij ad-opleiding Cybersecurity zoals die bij ieder blok wordt herhaald, passend en vernieuwend. Deze opzet is ook binnen de HvA redelijk nieuw, alhoewel er bij andere opleidingen ervaring mee is opgedaan en er support is. De condities voor een goede invoering zijn volgens hen aanwezig: het kernteam van de opleiding staat er open voor, docenten zijn bereid om te leren en er is veel aandacht voor kwaliteitsborging binnen de opleiding en HvA.

---

[12] https://feedbackfruits.com/home

[13] *In het toetsdossier wordt opgenomen: de studiehandleiding met de beoordelingsformulieren, analyseresultaten en slagingspercentages/ studentevaluatie, feedback van het werkveld en van studenten, eigen ervaringen en aanpassingen n.a.v. de evaluatie.*

[14] *De voorzitter is docent Recht, tevens voorzitter van examencommissie SJD en Bestuurskunde, het lid van de examencommissie is docent bij de bacheloropleiding ICT en beschikt over inhoudelijke kennis van cybersecurity en het externe lid beschikt over expertise op niveau 5.*

Vervolgens is specifiek op enkele punten doorgepraat: Op de *eerste* vraag van het panel dat de gedragscriteria algemeen zijn en hoe beroepsproducten door de docenten feitelijk worden getoetst werd door leden van de examencommissie geantwoord dat in de studiehandleidingen opdrachten zijn opgenomen waaraan eisen zijn gesteld en/of waar wordt gewerkt met gespecificeerde rubrics.

Op de *tweede* vraag van het panel waarom er alleen vier-ogenbeleid is in de toetsing van de afstudeeropdracht, is door leden van de examencommissie geantwoord dat het professionele gesprekken met de mentor 'gelijkwaardig' wordt gevoerd. Dit moeten 'geen zware momenten' zijn. De conclusies van het gesprek worden telkens omgezet naar ontwikkelingsplannen. Er zijn waarborgen ter objectivering ingebouwd: er komen richtlijnen voor docenten hoe deze gesprekken te voeren, er wordt regelmatig gekalibreerd en studenten nemen het verslag van het gesprek met hun mentor op in hun portfolio. Bij de toetsing van de afstudeeropdracht zijn er ook regelmatige kalibreersessies en bekijken docenten-examinatoren elkaars beoordelingen (ook met externe collega's). Daarbij zijn er beoordelingsrichtlijnen indien de assessor en afstudeerbegeleider het samen oneens zijn.

Op de *derde* vraag van het panel dat er met studenten individuele afspraken worden gemaakt voor reparaties indien opdrachten met een onvoldoende zijn beoordeeld, geven leden van de examencommissie aan dat de invulling van herkansingstermijnen niet te zeer van een individuele docent mag afhangen; hierin moet vergelijkbaarheid worden vastgesteld (dit vindt de opleiding een aandachtspunt).

Overwegingen
Er wordt in de opleiding ad-opleiding Cybersecurity recht gedaan aan het onderwijs- en toetsconcept (conform het HILL-model en het *Toetsplan)*. De systematiek van toetsvormen is in lijn met het uitgangspunt 'assessment as learning': de summatieve toetsmomenten (beoordeling van opdrachten) zijn formatief ingebed in het leerproces van de student (op basis van feedback in gesprekken). Ook het uitgangspunt 'student aan het roer' komt terug doordat studenten zelf nadenken over hoe zij de gedragsindicatoren willen gaan aantonen en welke bewijslast zij willen aanvoeren in hun portfolio. Het panel vindt het onderwijs- en toetsconcept goed uitgewerkt: de hele toetsgesprekscyclus waarbij veel gewerkt wordt met feedback (en onderliggende tools) nodigt uit tot 'diepgaand leren'.

De alignment is aanwezig. Per opdracht vindt toetsing plaats op gedragsindicatoren. De (praktijk)opdrachten worden steeds complexer en alle gedragsindicatoren worden in de opleiding herhaaldelijk getoetst. Aangezien de gedragsindicatoren zijn afgeleid van de beoogde leerresultaten dekken de toetsen gezamenlijk de eindkwalificaties af. In de afstudeeropdracht wordt de beheersing van *alle* gedragsindicatoren op niveau 5 afgetoetst in het portfolioassessment.
Het panel heeft net als bij Standaard 2 kanttekeningen bij de doorvertaling. De *eerste* kanttekening is dat het toetsprogramma algemeen blijft: er wordt enkel uitgegaan van 'opdrachten', maar de onderliggende toetsvormen zijn niet overzichtelijk weergegeven. Wel kunnen deze gehaald worden uit de opdrachtbeschrijvingen in de studiehandleidingen, bijvoorbeeld 'een werkend product, een rapport, een verbetervoorstel, een procesverslag, een presentatie'. Het panel adviseert een totaaloverzicht te maken van toetsvormen om de variatie van toetsing tussen en binnen de leerlijnen beter vast te kunnen stellen. De *tweede* kanttekening is dat de gedragscriteria algemeen zijn verwoord in de beoordelingsformulieren met rubrics. De studenten moeten bij de summatieve toetsen van de opdrachten voldoen aan de beoordelingscriteria zoals beschreven in de opdrachten (in de studiehandleidingen). Het panel heeft geen volledig zicht gekregen op de beoordelingscriteria of specifieke rubrics die hierbij worden gebruikt (zoals genoemd door de leden van de examencommissie). Het tweede advies luidt om per opdracht bij specifieke leerdoelen (en BoKS) aansluitende eisen aan producten en beoordelingscriteria te formuleren. Op de beoordelingsformulieren moet, volgens het panel, naast een volledigheidscheck van de IT-opdracht zelf, steeds de inhoudelijke vraag centraal staan of de opdracht is uitgevoerd in lijn met de instructie (leerdoelen en specificaties opdracht) en de standaarden in het vak.

Gezien de afspraken in de opleiding rond borging van de toetsing (zie volgende tekstpassage) heeft het panel er vertrouwen in dat de opleiding hieraan verder werkt.

De uitvoering van de summatieve en formatieve toetsen leunt sterk op individuele docenten en mentoren. Alleen bij de beoordeling van de afstudeeropdracht wordt het vier-ogenbeleid in de toetsing gehanteerd. Op basis van de gesprekken met docenten en met de examencommissie stelt het panel vast dat er veel wordt gekalibreerd en dat er gewerkt gaat worden met toetsdossiers, die door de examencommissie worden bekeken en worden besproken met de docenten. De kwaliteitszorg rond toetsing, de werkwijze van de examencommissie en de vastgestelde verantwoordelijkheden van de curriculum- en de blokcoördinatoren maken dat de commissie er vertrouwen in heeft dat de toetsing voor de studenten betrouwbaar en transparant wordt ingevuld.

Conclusie: Voldoet

4.4 Graad en CROHO-onderdeel

Het panel adviseert om de volgende graad aan de opleiding toe te kennen: Associate degree

Het panel adviseert het volgende CROHO-onderdeel voor de opleiding: domein Techniek

4.5 Algemene conclusie over de kwaliteit van de opleiding

De kwaliteit van de nieuwe opleiding is positief onder voorwaarden.

Aanbevelingen:

- Het panel adviseert in ieder geval relevante juridische kennis, bijkomende technische kennis en verantwoord ethisch handelen aan de beoogde leerresultaten toe te voegen (Standaard 1).
- Het panel is van mening dat de opleiding zich nog beter kan positioneren. De (brede) naam Cybersecurity dekt niet geheel de inhoud van de opleiding die vooral gericht is op penetratietesting (offensief) en in mindere mate op advisering aan de opdrachtgever hoe kwetsbaarheden (risico's) te voorkomen of te verhelpen (defensief). Het panel raadt aan om in het profiel meer recht te doen aan de (bredere) inhoud (Standaard 1).
- Het panel adviseert een totaaloverzicht te maken van toetsvormen om de variatie van toetsing tussen en binnen de leerlijnen beter vast te kunnen stellen (Standaard 3).
- Het panel adviseert om per opdracht bij specifieke leerdoelen (en BoKS) aansluitende eisen aan producten en beoordelingscriteria te formuleren (Standaard 3).

Voorwaarde:

Het panel heeft daarom als voorwaarde geformuleerd dat de doorvertaling (coverage) van de beoogde leerresultaten, met name bij de Fundamentals, ten aanzien van essentiële BoKS inzichtelijker moet worden. Hierbij moet in ieder geval kennis over relevante wetgeving, bijkomende technische kennis (zie Overwegingen in paragraaf 4.2) en verantwoord ethisch handelen zichtbaar terugkomen in het curriculum (Standaard 2).

Deze voorwaarde moet uiterlijk 31 augustus 2019 aangeleverd zijn bij de NVAO.

5 Overzicht oordelen

Standaard	Oordeel
Beoogde leerresultaten *Standaard 1: De beoogde leerresultaten passen bij het niveau en de oriëntatie van de opleiding en zijn afgestemd op de verwachtingen van het beroepenveld en het vakgebied en op internationale eisen.*	Voldoet
Onderwijsleeromgeving *Standaard 2: Het programma, de onderwijsleeromgeving en de kwaliteit van het docententeam maken het voor de instromende studenten mogelijk de beoogde leerresultaten te realiseren.*	Voldoet ten dele
Toetsing *Standaard 3: De opleiding beschikt over een adequaat systeem van toetsing.*	Voldoet
Algemene conclusie	Positief onder voorwaarden

bijlage 1: Samenstelling panel

Voorzitter:
- Prof. dr. ir. Bart Preneel, gewoon hoogleraar informatiebeveiliging, KU Leuven;

Leden:
- Drs. Janneke Jung, onderwijsmanager Associate degree ICT servicemanagement, Hogeschool Rotterdam;
- John Fokker, head of Cyber Investigations, ATR, McAfee;
- Student-lid: Lars Blom, student ICT aan Fontys Hogeschool en NVAO getraind.

Alle panelleden hebben een onafhankelijkheids- en onpartijdigheidsverklaring ingevuld en ondertekend.

Het panel werd bijgestaan door Gijs Kremers, beleidsmedewerker NVAO, procescoördinator en Lieke Ravestein, ROOA, zelfstandig secretaris.

bijlage 2: Programma locatiebezoek

Het panel heeft een bezoek gebracht aan de locatie op 15 maart 2019
Locatie: Amsterdam
Programma:

Tijd	Onderwerp	Deelnemers
09.00 – 09.45	Ontvangst, materiaal inzien, vooroverleg panel	
09.45 – 10.15	De opleiding presenteert zich: - Het belang van de Ad Cybersecurity - Cybersecurity in de faculteit - Didactisch concept en opzet opleiding	
10.15 – 10.30	Pauze/intern overleg	
10.30 – 11.15	Gesprek met het management	• decaan Faculteit Digitale Media en Creatieve Industrie (FDMCI) • directeur HvA Community College • curriculumcoördinator Ad-Cybersecurity
11.15 – 11.30	Pauze/intern overleg	
11.30 – 12.30	Gesprek met ontwikkel-/docententeam	• drie docenten Ad-Cybersecurity • onderwijskundige HvA Community College
12.30 – 13.30	Intern overleg met besloten lunch	
13.30 – 14.15	Gesprek met examencommissie en onderwijskundige over toetsing	• voorzitter Examencommissie Ad-Cybersecurity, docent Recht opleiding Sociaal Juridische Dienstverlening, voorzitter van de examencommissie SJD, voorzitter van de examencommissie Bestuurskunde • lid Examencommissie Ad-Cybersecurity, docent Cybersecurity, lid Examencommissie HBO-ICT • extern lid Examencommissie Ad-Cybersecurity, interim manager Samara Consultant, expert Niveau 5 – *niet aanwezig tijdens visitatie* • onderwijskundige HvA Community College
14.15 – 14.30	Pauze/intern overleg	
14.30 – 15.15	Gesprek met vertegenwoordiging werkveld	• adviseur bij Qbit Cyber Security • eigenaar Digital Investigation, voorzitter Cyber Security Centre MRA • director Cyber Inc • managing director IRP
15.15 – 15.30	Pauze/intern overleg	
15.30 – 15.45	Ruimte voor aanvullende vragen van het panel of verduidelijking door het managementteam	Op verzoek van panel of managementteam Ad Cybersecurity
15.45 – 16.45	Pauze/intern overleg	
16.45 – 17.00	Terugkoppeling en feedback	Alle betrokkenen
17.00	Borrel	

bijlage 3: Overzicht van bestudeerde documenten

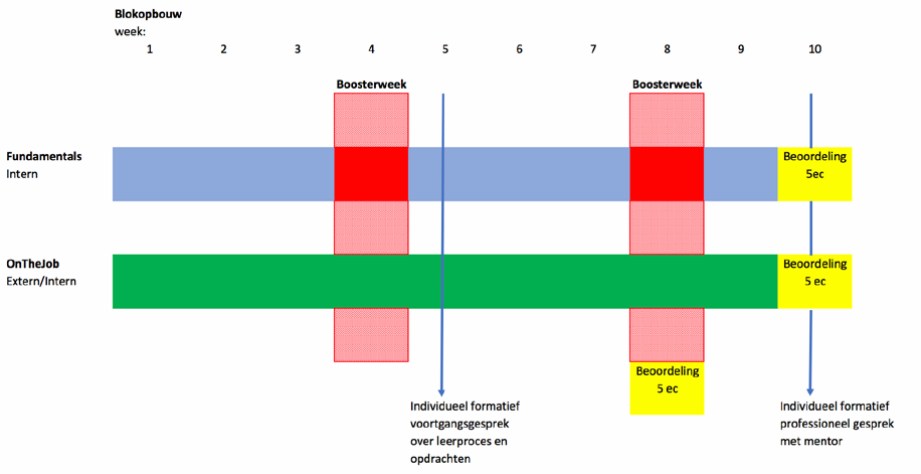
Informatiedossier en bijlagen (digitaal):
- Associate Degree Cybersecurity, informatiedossier ten behoeve van de aanvraag Beperkte Toets Nieuwe Opleiding, HVA, Amsterdam november 2018
- Addendum bij het informatiedossier Toets Nieuwe Opleiding Cybersecurity met referentienummer 007673, 19-02-2019
- Bronnenlijst/ literatuurlijst – jaar 1 Ad Cybersecurity

Map met bijlagen (november 2018):
1. Beroeps- en Opleidingsprofiel Cybersecurity
2. Leerplanschema
3. Studiegids
4. Didactisch Concept HvA Community College
5. Overzicht Personeel
6. Toetsplan
7. Onderwijs- en Examenregeling (OER) 2019-2010
8. Studiehandleiding Blok 2
9. Afstudeerhandleiding

Documenten beschikbaar gesteld tijdens locatiebezoek (maart 2019):
- Studiehandleiding Blok 1, 3 en 4
- Voorbeelden opdrachten leerlijnen 'OnTheJob, Fundamentals, Boosterweken'
- Dossier macrodoelmatigheidsaanvraag en instemming ministerie OC&W
- CV's beoogd docententeam
- European E-competence framework
- Profiel HBO ICT bachelor
- Profielen ICT security specialist PvIB
- Uitwerking Studiekeuzecheck
- Verslagen bijeenkomsten met werkveld over het opleidingsprofiel
- Verzoek Cyber Security Centre Metropoolregio Amsterdam tot starten opleiding Cybersecurity
- Bekrachtiging Beroeps- en opleidingsprofiel door Cyber Security Centre Metropoolregio Amsterdam
- Onderwijsvisie HvA
- Organogram HvA
- Toetsbeleid HvA
- Professionaliseringsplan HvA

Overige documenten
- Magazine 10, Niveau 5, Associate degrees: De Ad'er, een beeldschets, De beschrijving van het Ad-niveau, De verantwoording, De noodzaak van een niveaubeschrijving, november 2018

bijlage 4: Vorm van het curriculum ad-opleiding Cybersecurity



	SEMESTER 1		SEMESTER 2		SEMESTER 3		SEMESTER 4	
Leerresultaat	Identify		Analysis		Exploit		Integratie leerresultaten	
PTES-fase	Pre-en-gage-ment Interac-tion	Intelli-gence Gathering	Threat Modeling	Vulne-rability Analysis	Exploita-tion	Post-Ex-ploitation & Advice	Vrije keuzeruimte*	
							Afstudeeropdracht**	
Totaal aantal te behalen studiepunten per blok	15 EC	15 EC	15 EC	15 EC	15 EC	15 EC	15 EC	
Verdeling EC per leerlijn	5 EC	5 EC	5 EC	5 EC	5 EC	5 EC		
OnTheJob	5 EC	5 EC	5 EC	5 EC	5 EC	5 EC		
Fundamentals	5 EC	5 EC	5 EC	5 EC	5 EC	5 EC	15 EC	
Booster								
Professioneel gesprek	✔	✔	✔	✔	✔	✔	✔*	
Portfolioassessment								✔**

bijlage 5: Lijst met afkortingen

ad	associate degree
APA	American Psychological Association
ba	bachelor
BoKS	Body of Knowledge and Skills
CCISO	Certified Chief Information Security Officer
CEH	Certified Ethical Hacker
CISO	Chief Information Security Officer
EC	European Credits (studiepunten)
hbo	hoger beroepsonderwijs
HILL	High Impact Learning that Lasts
ma	master
mbo	middelbaar beroepsonderwijs
NVAO	Nederlands-Vlaamse Accreditatieorganisatie
OSCP	Offensive Security Certified Professional
PTES	Penetration Testing Execution Standard
wo	wetenschappelijk onderwijs

Het adviesrapport is tot stand gekomen in opdracht van de NVAO met het oog op beperkte toetsing van de nieuwe opleiding Associate degree Cybersecurity
Hogeschool van Amsterdam.

Aanvraagnummer: 007673

NVAO

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 28 • 2514 JK Den Haag
P.O. Box 85498 • 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net