NVAO • NEDERLAND

TOETS NIEUWE OPLEIDING

ASSOCIATE DEGREE

AD CYBERSECURITY

Hogeschool Utrecht

ADVIESRAPPORT

5 JULI 2023

Inhoud

1 Procedure NVAO

Het succesvol doorlopen van een procedure toets nieuwe opleiding (TNO) is een voorwaarde voor erkenning door de Nederlands-Vlaamse Accreditatieorganisatie (NVAO). Pas na deze kwaliteitstoets kan de instelling de bij de opleiding behorende wettelijk beschermde getuigschriften of diploma's afgeven.

De procedure voor een nieuwe opleiding is iets anders dan voor bestaande opleidingen die al zijn geaccrediteerd. Een TNO is een *plan*beoordeling. Na accreditatie valt ook de nieuwe opleiding onder de reguliere accreditatieprocedure.

Een NVAO-panel van deskundigen toetst de kwaliteit van de nieuwe opleiding tijdens een locatiebezoek aan de universiteit of hogeschool. Een discussie tussen *peers* vormt de basis van de beoordeling en resulteert in een adviesrapport. Informatie over de invulling van het locatiebezoek en een overzicht van het bestudeerde materiaal zijn opvraagbaar bij de NVAO.

De beoordeling is gebaseerd op de standaarden zoals beschreven in het Beoordelingskader voor de beperkte toets nieuwe opleiding van de NVAO (Stcrt. 2019, nr. 3198). Over de standaarden geeft het panel 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.

Dit adviesrapport bevat de bevindingen, overwegingen en oordelen van het panel alsook de sterke punten en aanbevelingen. Op basis van dit rapport neemt de NVAO een accreditatiebesluit. Een beknopt adviesrapport is eveneens beschikbaar. De NVAO publiceert beide rapporten.[1]

Meer informatie over de NVAO-werkwijze en de (tijdelijke) TNO-procedure is te vinden op www.nvao.net.

[1] https://www.nvao.net/nl/besluiten

2 Nieuwe opleiding

2.1 Algemene gegevens

Instelling	Hogeschool Utrecht
Opleiding	Associate degree Cybersecurity
Varianten	Voltijd
Graad	Associate degree
Locaties	Amersfoort
Studieomvang	120 EC[2]
Croho[3] onderdeel	Techniek

2.2 Profiel

Hogeschool Utrecht (HU) verzorgt vanuit 19 instituten voor circa 37.000 studenten een breed palet aan opleidingen op Associate degree-, bachelor- en masterniveau. Per 1 februari 2024 heeft het Instituut voor Associate degrees het voornemen te starten met de Associate degree Cybersecurity. De HU biedt deze voltijdopleiding van twee jaar aan vanuit haar locatie in Amersfoort.

Deze opleiding is in nauwe samenwerking met het regionale werkveld tot stand gekomen. De Ad Cybersecurity beoogt professionals op te leiden die verbindingen kunnen maken tussen IT en Cybersecurity. Het onderwijsprogramma is zowel gericht op penetratietesting (offensief) als op het meedenken over en adviseren hoe organisaties kwetsbaarheden en risico's kunnen voorkomen of verhelpen (defensief). In principe zijn alle studenten die voldoen aan de wettelijke instroomeisen welkom zich in te schrijven.

2.3 Panel

Samenstelling

- Bart Preneel, *voorzitter*, gewoon hoogleraar en diensthoofd van de Computer Security & Industrial Cryptography (Cosic) onderzoeksgroep aan de Katholieke Universiteit Leuven;
- Martin Molema, *lid*, docent bij de Academie ICT & Creative bij NHL Stenden Hogeschool;
- Pim Sewuster, *lid*, Cybersecurity-expert bij ING;
- Suzet van Gaalen, *student-lid*, recent afgestudeerde van de opleiding Associate degree Commerciële Economie van Fontys Hogescholen en voormalig lid opleidingscommissie.

Ondersteuning

- Reinier Gerritzen, *secretaris*
- Laura Oosterveld, *NVAO-beleidsmedewerker en procescoördinator*

Locatiebezoek

24 mei 2023, Hogeschool Utrecht, locatie Amersfoort

[2] European Credits

[3] Centraal Register Opleidingen Hoger Onderwijs

3 Oordeel

Het NVAO-panel oordeelt positief onder voorwaarden over de kwaliteit van de Associate degree Cybersecurity van de Hogeschool Utrecht.

De opleiding is er op basis van uitgebreid vooronderzoek in geslaagd een passend beroepsprofiel op te stellen. Daarbij heeft de Ad Cybersecurity zich mede gebaseerd op relevante (inter)nationale kaders en consulteerde zij meermalen een representatieve vertegenwoordiging van regionale werkveldpartners en andere onderwijsinstellingen. De gekozen competenties en leeruitkomsten passen goed bij het profiel en de opleiding heeft deze op het juiste Ad-niveau beschreven.

De Ad Cybersecurity richt een helder opgebouwd onderwijsprogramma in dat naarmate de studie vordert steeds praktijkgerichter wordt. De didactische aanpak is sterk en past goed bij de doelgroep van de Ad-student. Het bevlogen en didactisch bekwame docententeam is op haar taak toegerust. Het is de intentie van de instelling aan het team nog een docent met werkervaring in cybersecurity toe te voegen. Inhoudelijk maakt de opleiding vaak logische keuzes, al maakt zij niet altijd voldoende duidelijk hoe diepgaand zij de verschillende thema's aanbiedt en wat zij daarin van studenten verwacht. Het programma is verder zeker arbeidsmarktgericht, maar nog niet uitgesproken vernieuwend. Daar valt volgens het panel nog winst te behalen. De Ad Cybersecurity richt een toetssysteem in dat het leerproces van de studenten goed ondersteunt. De sterke examencommissie en toetscommissie zien actief toe op de kwaliteit van de toetsing. Wel behoeft de toetsdocumentatie op meerdere punten nog nadere schriftelijke uitwerking om de eisen voor studenten beter inzichtelijk te maken.

Hoewel de basis van de opleiding goed staat, signaleert het panel een essentieel verbeterpunt. Van het eerste jaar van het onderwijsprogramma is de eerste periode A veel gedetailleerder uitgewerkt dan de overige drie periodes. Het panel legt de Ad Cybersecurity daarom de volgende voorwaarde op: het team dient periode B, C en D verder uit te werken met uitgebreidere cursuswijzers, concrete opdrachten, passende beroepsproducten en onderwijsmateriaal voor docenten. Verder dient het team duidelijk te maken welke vakinhoud per periode centraal staat, inclusief de mate van diepgang en het verwachte niveau daarvan. Het panel wijst erop dat deze aanvullingen van het cursusmateriaal consequenties hebben voor de verschillende toetsmomenten en toetscriteria die het panel graag meegenomen ziet in de gedetailleerde uitwerking. De documentatie om aan deze voorwaarde te voldoen legt de opleiding uiterlijk acht weken voorafgaand aan de start van de opleiding (1 februari 2024) aan het panel voor.

Gezien de open en lerende houding die docenten in de gesprekken toonden en het ontwikkelproces tot nu toe, vertrouwt het panel erop dat de opleiding voorafgaand aan de start aan deze voorwaarde kan voldoen.

Standaard	**Oordeel**
1. Beoogde leerresultaten	Voldoet
2. Onderwijsleeromgeving	Voldoet ten dele
3. Toetsing	Voldoet
Eindoordeel	*positief onder voorwaarden*

4 Sterke punten

Het panel constateert de onderstaande sterke punten:

1. Betrokken werkveld – In het uitgebreide vooronderzoek heeft de opleiding een breed scala aan organisaties uit het werkveld geraadpleegd om input te geven op het beroepsprofiel. Deze werkveldpartners geven aan dat zij veel kansen zien voor afgestudeerden van de Ad Cybersecurity.

2. Bevlogen docenten– Het docententeam is zeer gedreven en enthousiast. Zij tonen een grote betrokkenheid bij de nieuwe opleiding en een sterke interesse in het vakgebied van Cybersecurity.

3. Didactische aanpak – In deze opleiding werken studenten in leerteams en krijgen zij gevarieerde werkvormen aangeboden. De manier waarop de Ad Cybersecurity de onderwijsperiodes en onderwijsweken inricht, helpt studenten actief te studeren.

4. Programmatisch Toetsen – Het toetssysteem van de Ad Cybersecurity is zo vormgegeven dat studenten regelmatig tussentijdse producten opleveren waar zij feedback op krijgen. Daarmee ondersteunt de opleiding hun leerproces op goede wijze.

5. Examencommissie – De examencommissie en toetscommissie zijn actief betrokken bij de Ad Cybersecurity en houden goed toezicht op de kwaliteit van de toetsing en op het Associatie degree-niveau van de opleiding.

5 Aanbevelingen

Met het oog op de verdere ontwikkeling van de opleiding doet het panel een aantal aanbevelingen. Deze aanbevelingen doen geen afbreuk aan het positieve oordeel over de kwaliteit van de opleiding.

1. Vakinhoud – Verhelder de Body of Knowledge & Skills (BoKS) voor het gehele onderwijsprogramma. Expliciteer wat een goede verhouding is tussen de verschillende cybersecuritythema's en operationaliseer per thema wat het verwachte niveau is dat studenten moeten bereiken. Werk tevens nader uit wat de benodigde vakinhoud is in het praktijkproject in het tweede leerjaar.

2. Toekomstgericht – Verrijk het onderwijsprogramma met meer innovatieve elementen. Betrek vooruitstrevende werkveldpartners en het lectoraat Cybersecurity van de HU daarbij.

3. Diverse inbreng werkveld – Zorg voor een werkveldcommissie met een evenwichtige verdeling tussen private en publieke organisaties. Voeg daar indien mogelijk vernieuwende cybersecurityorganisaties aan toe en overweeg leden te laten rouleren. Verduidelijk tevens de verwachte inbreng van de gastdocenten in het programma.

4. Toetsing – Werk verschillende aspecten van de toetsing nader schriftelijk uit om de eisen voor studenten duidelijker te maken.

5. Afstuderen – Formuleer nadere criteria voor het afstuderen en uniformeer het beslissingsformulier met die van de overige onderwijseenheden.

6 Beoordeling

6.1 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.

Oordeel
Voldoet

Bevindingen en overwegingen

Relevantie opleiding
Hogeschool Utrecht (Hierna: HU) is vanuit het Instituut voor Associate degrees (hierna: het IAd), in Amersfoort voornemens te starten met de Associate degree-opleiding Cybersecurity (hierna: Ad Cybersecurity of de opleiding). In het dossier, dat volgens het panel qua helderheid, consistentie en nauwkeurigheid te wensen overliet, beschrijft het ontwikkelteam verschillende actuele technologische ontwikkelingen die vergaande risico's voor organisaties en individuen met zich meebrengen. Daarmee onderbouwt zij goed hoe relevant deze opleiding in dit digitale tijdperk is. De tweejarige voltijdopleiding leidt studenten op tot cybersecurity-specialisten die terecht kunnen binnen bedrijven, banken en (overheids)organisaties. De beoogde professionals kunnen verbindingen maken tussen IT en cybersecurity. Ze richten zich daarbij zowel op penetratietesting (offensief) als op het meedenken over en adviseren hoe hun organisaties kwetsbaarheden en risico's kunnen voorkomen of verhelpen (defensief).

Betrokkenheid werkveld
Uit het dossier en de gesprekken blijkt dat het ontwikkelteam bij de totstandkoming van de Ad Cybersecurity uitgebreid vooronderzoek heeft verricht. Zo heeft het team een analyse gedaan van tientallen vacatures in het werkveld van cybersecurity. Tevens raadpleegden zij op meerdere momenten in het traject verschillende regionale cybersecurity gerelateerde bedrijven, lokale overheden en andere onderwijsinstellingen. In de gesprekken bevestigen de werkveldpartners hun herhaaldelijke actieve betrokkenheid bij de opleiding. Zij geven aan dat hun organisaties veel behoefte hebben aan professionals met een gedegen cybersecurityopleiding zoals de HU die beoogt. Ze beschrijven daarbij concrete rollen in hun organisaties die afgestudeerden kunnen vervullen.

De betrokkenheid van het werkveld is sterk. Voor het panel is nog niet duidelijk geworden wat de huidige status van de werkveldcommissie is. Daarom doet het panel de aanbeveling dat de opleiding een werkveldcommissie opricht met een evenwichtige verdeling tussen private en publieke organisaties. Idealiter voegt de opleiding daar vertegenwoordigers van vernieuwende cybersecurityorganisaties aan toe. Een verdere overweging kan tot slot zijn om werkveldleden te laten rouleren om een diverse kijk op het vakgebied te stimuleren.

Beroepsprofiel
Voor de ontwikkeling van het beroepsprofiel baseert de opleiding zich onder meer op informatie van het Platform voor Informatiebeveiliging en op het European Cybersecurity Skills Framework van de European Union Agency for Cybersecurity. Alle aspecten van het eerder vermelde vooronderzoek resulteren in een beroepsprofiel voor deze Ad Cybersecurity. De opleiding noemt daarin een breed palet aan functietitels die afgestudeerden kunnen vervullen en taken

die zij kunnen uitvoeren. Dat leidde voor het panel tot de vraag in hoeverre het haalbaar is om studenten in twee jaar op te leiden voor zo'n variëteit aan rollen, hoe de verhouding tussen de (inhoudelijke) breedte en de diepte is in de opleiding en welke taken de afgestudeerden daadwerkelijk goed kunnen uitvoeren als zij zijn afgestudeerd.

Het ontwikkelteam herkent zich in deze bevinding van het panel. Het was voor de ontwikkelaars een uitdaging een goed midden te vinden tussen ambitie en de vertaling daarvan in het onderwijs. Het team wil studenten zo breed mogelijk laten kennismaken met allerlei relevante en interessante cybersecuritythema's. Tegelijkertijd moet dat wel haalbaar zijn in het opleidingsprogramma. In dat proces is het team in overleg met het werkveld steeds scherpere keuzes gaan maken. Voor de verdieping kiest de opleiding ervoor veel aandacht te besteden aan de vier stappen van de Penetration Testing Execution Standard (PTES). Studenten leren dan in de huid te kruipen van cybercriminelen om zo organisaties te kunnen adviseren wat de zwakke plekken zijn in hun systeem. Daarmee geeft Ad Cybersecurity studenten een rode draad voor de verschillende (offensieve en defensieve) thema's die cybersecurity bevat en biedt zij studenten tevens een concrete rol die zij kunnen vervullen. Daarnaast maken studenten in de opleiding kennis met een breder palet aan thema's om deze in organisaties te kunnen herkennen. In de afstudeerfase kunnen ze zich verder verdiepen in een bepaald thema. De opleiding heeft het panel met aanvullende stukken en in de beantwoording van de vragen tijdens het locatiebezoek overtuigd van de gemaakte keuzes.

Leerresultaten
Het panel constateert dat het ontwikkelteam voor de Ad Cybersecurity een passende set van leerresultaten heeft beschreven. Positief is dat uit het dossier en de gesprekken blijkt dat het team zich tevens heeft verdiept in de opleidingsprofielen van andere Nederlandse Ad- en bacheloropleidingen op het gebied van cybersecurity en regionale mbo-opleidingen consulteerde.

De opleiding formuleert zeven competenties om invulling te geven aan het beroepsprofiel. Zes daarvan zijn generiek en gelden voor alle opleidingen van het IAd. Deze zijn afgeleid van de generieke leerresultaten voor de Associate degree van het Overlegplatform van de Vereniging Hogescholen. Daarbij formuleert de Ad Cybersecurity één opleidingsspecifieke competentie namelijk 'Verbinden & Schakelen'. Ondanks de generieke titel van deze competentie is het voor het panel tijdens de gesprekken duidelijk geworden dat deze een sterk inhoudelijke component heeft. Deze specifieke competentie ziet toe op het vergroten van het bewustzijn van cybersecuritythema's in verschillende hiërarchische lagen in de organisatie. Het panel ondersteunt deze essentiële toevoeging op de generieke competenties om invulling te geven aan de complexiteit van de materie en de relatieve onbekendheid daarmee in (veel) organisaties. Om invulling te kunnen geven aan het onderwijs heeft het ontwikkelteam de competenties vervolgens met behulp van de Core Tuning-methodiek doorvertaald naar acht leeruitkomsten.

Niveau
Het ontwikkelteam heeft de leerresultaten goed op Ad-niveau beschreven. In het dossier maakt de opleiding duidelijk hoe zij de generieke en opleidingsspecifieke competenties en de leeruitkomsten afstemt met de niveau 5 beschrijvingen van het eindniveau zoals deze zijn uitgewerkt door het Overlegplatform Associate degrees en zijn beschreven in het Nederlands Kwalificatiekader (NLQF). In die documenten zijn deze niveaus gekoppeld aan de niveaubeschrijvingen van het European Qualification Framework (EQF) en de Dublin Descriptoren Short Cycle. Verder geven de gesprekspartners tijdens het locatiebezoek blijk van

goed zicht op het Ad-niveau en hoe dat zich onderscheidt van mbo-niveau 4 en bachelor niveau 6. Het panel wordt gesterkt in deze overtuiging doordat het IAd reeds een zestiental Ad-opleidingen verzorgt. Het instituut heeft nauwe contacten met de inpandige mbo-opleidingen, alsmede met aanverwante bacheloropleidingen van de HU. De vertegenwoordigers van het werkveld geven in de gesprekken tot slot aan concrete ideeën te hebben van waar een afgestudeerde Ad-er Cybersecurity in de verschillende organisaties op operationeel-tactisch niveau gepositioneerd kan worden. Zij realiseren zich tegelijkertijd dat het profiel van de Ad Cybersecurity-professional de komende jaren in hun organisaties nadere inkleuring dient te krijgen als de eerste studenten en afgestudeerden van deze opleidingen in praktijkomgevingen gaan opereren.

Internationaal perspectief
Het team geeft aan dat de Ad Cybersecurity met name een regionale focus heeft. Tegelijkertijd heeft het vakgebied sterk een internationaal karakter en kent het veel Engelse vakterminologie. Studenten komen met name in aanraking met het internationale aspect van cybersecurity in de projecten en via de inbreng van gastdocenten uit het internationaal georiënteerde werkveld. De opleiding verwacht van studenten van deze Nederlandstalige opleiding dat zij Engelse teksten uit het vakgebied kunnen lezen. Een cursus Engels vormt daarom onderdeel van het programma. Een buitenlandse stage behoort voor de studenten die dat graag willen tot de mogelijkheden. Verder zet het IAd het programma 'Internationalisation at home' van Nuffic in. Studenten doen daarmee in het onderwijs internationale en interculturele vaardigheden op zonder daarvoor per se naar het buitenland te hoeven gaan. Op deze wijze maakt de Ad Cybersecurity duidelijke keuzes die volgens het panel goed passen bij de regionale oriëntatie en beoogde doelgroep van de opleiding. De Engelstalige opleidingsnaam is tot slot een voor de hand liggende keuze voor deze opleiding daar de term Cybersecurity volledig is ingeburgerd in Nederland.

Het panel oordeelt op basis van voorgaande dat de opleiding erin is geslaagd om op basis van uitgebreid vooronderzoek een adequaat beroepsprofiel op te stellen. Daarbij baseerde de Ad Cybersecurity zich mede op relevante (inter)nationale kaders en consulteerde zij meermalen een representatieve vertegenwoordiging van regionale werkveldpartners en andere onderwijsinstellingen. De competenties en leeruitkomsten passen goed bij het profiel en de opleiding beschrijft deze op het juiste Ad-niveau. Het internationale perspectief komt gezien de aard en doelgroep van de Ad Cybersecurity voldoende aan bod.

6.2 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 `.

Oordeel
Voldoet ten dele

Bevindingen en overwegingen

Opbouw programma
Het opleidingsprogramma kent een heldere opbouw. De Ad Cybersecurity heeft het beroepsprofiel, de competenties en de leeruitkomsten adequaat doorvertaald naar de verschillende onderwijsonderdelen. De opleiding maakt met behulp van het ZELCOM-model goed inzichtelijk hoe zij gedurende het programma een steeds grotere mate van zelfstandigheid van studenten verwacht. Docenten geven in de gesprekken aan dat zij studenten in de eerste

periode zowel inhoudelijk als qua leervaardigheden nog stevig begeleiden. Naarmate het leerjaar vordert laten zij studenten meer los. Het niveau en de complexiteit van de opdrachten neemt zichtbaar toe in de opleiding.

In het eerste jaar, bestaande uit vier periodes, vormt de PTES de rode draad in het onderwijsprogramma. In elk van de periodes komt een (volgende) stap uit deze teststandaard aan bod. Studenten leggen daarmee een (kennis)basis, leren hoe ze verschillende cybersecurity-standaarden en -tools op de juiste manier kunnen inzetten en leren deze in een grotere context te plaatsen. In het dossier stelt de opleiding te werken met vijf leerlijnen, waaronder 'Cybersecurity Knowledge Base' en 'Compliance & Awareness'. De verbanden tussen de generieke competenties, leerlijnen en technische vakinhoud zijn echter nog niet voldoende helder terug te vinden in de beschikbare documenten.

De praktijkgerichtheid van de Ad Cybersecurity komt in het eerste jaar vooral terug doordat studenten veel aan beroepsproducten werken teneinde hun leeruitkomsten aan te tonen. De twee semesters van het tweede leerjaar zijn nadrukkelijk praktijkgerichter. De opleiding organiseert in het eerste semester een praktijkproject in samenwerking met het werkveld. Daarna volgt een afstudeersemester waarin studenten zelfstandig een cybersecurityvraagstuk in een organisatie onderzoeken.

Werkvormen & didactiek
Het panel is positief over de didactische aanpak van de Ad Cybersecurity. De opleiding verwacht studenten van deze voltijdopleiding op maandag, dinsdag en donderdag op school. Elke week krijgen studenten een gezamenlijke weekstart en -afsluiting. Conform de didactische uitgangspunten van het IAd werken studenten en docenten samen in leerteams van zes tot acht studenten. Een leerteamcoach die tevens de studieloopbaanbegeleider is, begeleidt ze daarbij. Hierdoor is er veel ruimte voor begeleiding en feedback.

Tijdens de schooldagen biedt de opleiding studenten een rijke variëteit aan werkvormen aan. Zij spant zich in de opdrachten zo vorm te geven dat studenten op studiedagen zelfstandig of (digitaal) samen aan hun opdrachten werken. Studenten dienen elke periode bepaalde beroepsproducten op te leveren. De opleiding deelt deze vaak op in kleinere, afgeronde taken waardoor studenten tussentijds steeds deelprestaties opleveren. De ervaring binnen het IAd leert dat dat voor deze doelgroep motiverend werkt. Uit de gesprekken blijkt dat docenten en studenten volgens de Agile-methode in sprints werken. Dit is een recente beslissing die in het dossier nog niet naar voren kwam, maar het panel vindt dat een goede werkwijze. Deze sluit mooi aan bij de wijze waarop men in de beroepspraktijk vaak werkt en bij de feedbackcultuur die de opleiding conform de didactische visie van het IAd inricht.

Inhoud
De opleiding maakt overwegend inhoudelijke keuzes die passen bij het profiel, maar werkt deze gekozen thema's niet altijd gedetailleerd genoeg uit. In de cursuswijzers noemt het team veel relevante cybersecuritythema's en komen onderwerpen als privacy, compliance, awareness en (Europese) regelgeving aan bod. Tevens leren studenten de basis van programmeren met onder meer Python en is er elke periode aandacht voor ethisch handelen. Minder duidelijk maakt de opleiding echter hoe diepgaand zij deze thema's en vaardigheden behandelt en op welk niveau studenten deze dienen te beheersen. Vaak blijft het ontwikkelteam bij het noemen van overkoepelende thema's, zoals cloud security, cryptografie of security information & event management, zonder deze vergaand uit werken. Voorgaande leidt voor het panel tot de

aanbeveling dat de opleiding voor het gehele programma de Body of Knowledge & Skills (BoKS) dient te verhelderen. Daarbij dient het team te expliciteren wat de goede verhouding is tussen de verschillende (technische en niet-technische) cybersecuritythema's en te operationaliseren wat de verwachte mate van inhoudelijke diepgang is die studenten van deze opleiding op Ad-niveau moeten bereiken.

Tevens lijkt de aangeboden vakinhoud in het eerste semester van het tweede jaar nog niet te zijn uitgekristalliseerd. In de gesprekken geeft het team aan daarin naast het praktijkproject met inhoudelijke themadagen te gaan werken, maar dat het de thema's daarvan nog moet bepalen. Op dit punt doet het panel de aanbeveling om bij de doorontwikkeling van jaar 2 nader vast te leggen welke vakinhoud daarin aan bod komt en deze keuzes af te stemmen met de omvang en/of inrichting van het praktijkproject.

Toekomstgericht
Het panel constateert dat de opleiding met de huidige inhoudelijke keuzes professionals beoogt af te leveren die kunnen omgaan met de vraagstukken zoals die op dit moment in de regionale organisaties spelen. Het werkveld bevestigt in de gesprekken dat daar hun behoefte ligt. Daarmee is de Ad Cybersecurity thans zeker arbeidsmarktgericht, maar nog niet uitgesproken vernieuwend of toekomstgericht. Hier ligt volgens het panel nog een ontwikkelkans. De opleiding zou, bijvoorbeeld in het derde semester, nog meer de nadruk kunnen leggen op het aanbieden van innovatieve elementen uit het vakgebied. Het panel raadt aan daarbij vooruitstrevende werkveldpartners en het lectoraat Cybersecurity van de HU te betrekken. Tot slot acht het panel het raadzaam aan de komende jaren in samenspraak met het werkveld scherp te blijven kijken of PTES de beste rode draad blijft voor het programma.

Cursuswijzers
De opleiding werkt het programma uit in cursuswijzers. De mate van uitwerking per onderwijsonderdeel varieert nog te sterk. Tijdens het locatiebezoek heeft het panel uitvoerig met het team hierbij stilgestaan. In de gesprekken blijkt dat het opleidingsteam het programma mondeling veel beter kan toelichten dan uit de aangeleverde stukken duidelijk werd. Bij het panel is het beeld ontstaan dat, hoewel het team duidelijk op de goede weg is in het neerzetten van een voldragen opleidingsprogramma, er ook nog zaken in ontwikkeling zijn. Het spanningsveld tussen het ambitieniveau van de opleiding en de praktische haalbaarheid daarvan in het programma, is in de cursusbeschrijvingen zichtbaar. Bepaalde documenten zijn inmiddels (deels) achterhaald of voortschrijdend inzicht heeft het team doen besluiten andere keuzes te maken of zaken aan te passen.

Het panel begrijpt dat het dynamische gebied van cybersecurity uitnodigt tot doorlopend onderzoeken en meebewegen met de praktijk. Tegelijkertijd is het belangrijk dat de opleiding het curriculum tijdig op hoofdlijnen vaststelt en de aandacht richt op de concrete invulling van het onderwijsprogramma. Het panel constateert namelijk dat periode A veel gedetailleerder uitgewerkt is dan de overige drie periodes van jaar 1. Zij beoordeelt dat als een essentieel verbeterpunt en legt de Ad Cybersecurity derhalve de volgende voorwaarde op. Het team dient periode B, C en D verder uit te werken. De ontwikkelaars dienen te zorgen voor meer uitgebreide cursuswijzers, concrete opdrachten, passende beroepsproducten en onderwijsmateriaal voor docenten. Verder dient het team duidelijk te maken welke vakinhoud per periode centraal staat en welk niveau en mate van diepgang de opleiding daarin van deze Ad-studenten verwacht. Ook dient de opleiding helder aan te geven hoe die inhoud overeenkomt met de leerlijnen en competenties. Het panel verwacht dat voorgaande aanpassingen ertoe leiden dat de Ad

Cybersecurity voor studenten beter inzichtelijker maakt hoe het programma is opgebouwd en wat de opleiding in de verschillende periodes precies van hen verwacht.

Het panel wijst erop dat deze aanvullingen in het cursusmateriaal consequenties hebben voor de verschillende toetsmomenten en toetscriteria die het panel graag meegenomen ziet in de gedetailleerde uitwerking. De documentatie om aan deze voorwaarde te voldoen legt de opleiding uiterlijk acht weken voorafgaand aan de start van de opleiding (1 februari 2024) aan het panel voor.

Instroom
De instroomeisen en intakeprocedure van de Ad Cybersecurity zijn helder voor het panel. De opleiding is voornemens te starten per 1 februari 2024. In principe is elke student toelaatbaar die voldoet aan de wettelijke instroomeisen. Het team is zich ervan bewust dat de instromende studentpopulatie zeer divers kans zijn. De opleiding organiseert matchingsdagen voor de studenten die zich aanmelden waarin studenten een (niet bindend) studieadvies krijgen en dat vindt het panel positief. Eventuele deficiënties in bijvoorbeeld wiskunde, Nederlands of Engels kunnen studenten wegwerken nadat zij gestart zijn. De Ad Cybersecurity biedt hier HU- of instituutsbrede ondersteuning voor. Het panel raadt de opleiding aan om, bijvoorbeeld met formatieve toetsen, al vroeg in de eerste periode samen met studenten te onderzoeken wat zij nodig hebben. De docenten geven aan dat zij door het werken in leerteams verwachten dat zij snel signaleren op welke terreinen studenten extra ondersteuning nodig hebben. Dat vindt het panel positief, ook om vroegtijdig eventuele andere kennishiaten te kunnen signaleren en daarop in te spelen.

Studenten kunnen geen vrijstellingen krijgen. Studenten met bepaalde voorkennis of werkervaring kunnen wel een voordeel hebben. Deze kennis of ervaring kan hen in staat stellen om de leeruitkomsten met minder leeractiviteiten aan te tonen. Conform het beleid van het IAd kunnen afgestudeerden doorstromen naar een (individuele leerroute binnen een) bacheloropleiding van de HU. Voor de Ad Cybersecurity is dat de opleiding Cybersecurity & Cloud Duaal.

Docenten & begeleiding
Een team van vier docenten zal het inhoudelijke onderwijs en de begeleiding van studenten in de leerteams gaan verzorgen. Daarnaast geeft het management aan dat zij docenten van andere opleidingen binnen het IAd voor begeleiding en toetsing kunnen inzetten. Het kernteam maakt op het panel een zeer gedreven en enthousiaste indruk. Zij tonen een grote betrokkenheid bij de nieuwe opleiding en een sterke interesse in het vakgebied van cybersecurity. Zij geven aan dat zij voldoende tijd en mogelijkheden ervaren om zichzelf, ook vakinhoudelijk, te professionaliseren.

Tegelijkertijd dekt het team thans nog niet de volledige benodigde breedte van aan cybersecurity gerelateerde thema's af. Op dit moment staat een vacature uit voor een extra docent voor deze opleiding. Werkervaring op het gebied van cybersecurity is daarbij een belangrijke eis en dat is positief. Het panel verwacht verder dat de opleiding sterk kan profiteren van de aanstelling van een lector Cybersecurity bij de HU die officieel benoemd wordt per juni 2023. Verder is de Ad Cybersecurity voornemens te werken met gastdocenten. Navraag tijdens de gesprekken wijst uit dat het team de inzet daarvan nog niet heeft geconcretiseerd. De invulling van de inzet van gastdocenten behoeft volgens het panel derhalve nadere uitwerking. Uit de gesprekken met het

werkveld blijkt dat de animo om bij te dragen aan deze opleiding groot is. Dat geeft het panel het vertrouwen dat de opleiding hieraan richting de start nadere invulling kan geven.

Uit het dossier blijkt dat de teamleden beschikken over Basiskwalificatie of Seniorkwalificatie Didactische Bekwaamheid en Basiskwalificatie Examinering of thans via een maatwerktraject van het IAd bezig zijn deze te behalen. Positief punt is verder dat de docenten verschillende achtergronden hebben in het mbo-, Ad-, en/of hbo-onderwijs waardoor zij als team goed zicht hebben op de doelgroep van deze nieuwe opleiding.

Het panel concludeert op basis van voorgaande dat de Ad Cybersecurity een onderwijsprogramma met een logische opbouw heeft ontwikkeld. Het programma kent een duidelijke toename in verwachte zelfstandigheid en complexiteit en wordt naarmate de studie vordert steeds praktijkgerichter. De didactische aanpak is sterk en past goed bij de doelgroep van de Ad-student. Het bevlogen en didactisch bekwame docententeam is, zeker met de beoogde extra docent en de mogelijke aansluiting bij het lectoraat, inhoudelijk toegerust op haar taak. De opleiding maakt in de inhoud vaak logische keuzes, al maakt zij niet altijd voldoende duidelijk hoe diepgaand zij de verschillende thema's aanbiedt en wat zij daarin van studenten op Ad-niveau verwacht. Het programma is niet uitgesproken vernieuwend dus daar valt volgens het panel nog winst te behalen. Hoewel het panel veel positieve punten ziet, is het onderwijsprogramma van het eerste jaar van de Ad Cybersecurity in drie van de vier periodes nog te sterk in ontwikkeling. Deze constatering leidt tot het oordeel dat de onderwijsleeromgeving ten dele voldoet. Daarom stelt het panel de voorwaarde dat de opleiding de drie periodes voorafgaand aan de start op verschillende punten nader dient uit te werken. Gezien de open en lerende houding die docenten in de gesprekken toonden en het ontwikkelproces tot nu toe, vertrouwt het panel erop dat de opleiding voorafgaand aan de start (1 februari 2024) aan deze voorwaarde kan voldoen.

6.3 Standaard 3: Toetsing

De opleiding beschikt over een adequaat system van toetsing.

Oordeel
Voldoet

Bevindingen en overwegingen

Programmatisch Toetsen
In de verschillende toetsdocumenten van het IAd en de opleiding in het dossier beschrijft de Ad Cybersecurity dat zij werkt met het toetssysteem van programmatisch toetsen (PT). Tijdens het locatiebezoek kreeg het panel ook een presentatie over PT waarin het team goed duidelijk maakt hoe zij hieraan in de opleiding invulling geeft. PT legt de nadruk op 'toetsing als leerinstrument' en voorziet daartoe in veel tussentijdse formatieve toetsmomenten. Voor de toetspraktijk van de Ad Cybersecurity houdt dit in dat studenten zelf bewijs verzamelen van hun competentieontwikkeling. Gedurende een periode of semester werken studenten aan de beroepsproducten en de deelprestaties die daaronder vallen. Voor periode 1 heeft het panel nadere toelichting gekregen op een voorbeeld daarvan, namelijk het opstellen van een netwerkplan inclusief alle deelprestaties die daaronder vallen. Meermalen tijdens een onderwijseenheid vragen studenten feedback aan docenten en eventuele andere partijen op de deelprestaties. Deze feedbackmomenten worden datapunten genoemd. Studenten doen daarvan verslag en leggen deze datapunten vast in een systeem (FeedPulse). Ze formuleren

leerdoelen voor de voortgang van hun ontwikkeling. De opleiding heeft alle datapunten per onderwijseenheid op hoofdlijnen uitgewerkt.

Het panel is positief over deze toetswijze. Studenten krijgen tussentijds regelmatig feedback en feed forward waardoor dit toetssysteem hun leerproces goed ondersteunt. De verschillende digitale systemen faciliteren het toetsproces op goede wijze. De toetsing van de opleiding is in lijn met het toetsbeleid van de HU en dat van het IAd. Het instituut heeft merkbaar al veel ervaring met PT doordat alle Ad-opleidingen van het instituut sinds de start van het instituut in 2019 daarmee werken.

Beoordelingsproces
Elke periode of semester plaatsen studenten alle datapunten in een portfolio. Datapunten bestaan uit verschillende soorten bewijsmiddelen zoals verslagen, reflecties, beroepsproducten, et cetera. Aan het eind van een periode of semester beoordelen één of meerdere examinatoren of de inhoud van het portfolio en de samenhang van de producten voldoen. De beoordelingscriteria daarvoor legt de opleiding vast in beslissingsformulieren waarin de opleiding uitwerkt wanneer een prestatie onder, op of boven niveau is. Indien studenten voldoen aan de gestelde eisen dan bemachtigen zij hun studiepunten voor die onderwijseenheid. Wanneer nodig kunnen studenten (delen) van hun portfolio na tien weken herkansen.

In de basis is dit beoordelingsproces voldoende inzichtelijk voor het panel. Om de eisen voor studenten nog verder te verduidelijken is het aan te bevelen dat de opleiding op verschillende aspecten een nadere documentatieslag maakt. Op dit punt ervaart het panel ook dat de mondelinge uitleg van het team meer helderheid schept dan is terug te vinden in het dossier. Concreet kan de opleiding inzichtelijker maken hoe de beroepsproducten en beoordelingsmomenten samenhangen en hoe elke (beroeps)product concreet bijdraagt aan de specifieke competentie of leeruitkomst die in die onderwijseenheid centraal staat. Verder is het raadzaam dat de opleiding in de cursuswijzers expliciteert dat (beroeps)producten altijd vergezeld dienen te gaan van feedback van docenten, peers en/of mensen uit de praktijk. Een ander punt is dat voor het panel nog niet is vast komen te staan of de Ad Cybersecurity na elke periode of semester een assessmentgesprek voert met studenten of dat de examinatoren de portfoliotoetsing enkel schriftelijk afdoen. In de gesprekken benoemt het team dat ze aan het einde van de laatste periode alles wat studenten in de vorige periodes leerden nog eens aan bod wil laten komen. Daarop volgt een afsluitend assessment. . Dit assessment is in de documentatie echter niet terug te vinden. Daardoor is voor het panel onduidelijk in hoeverre de Ad Cybersecurity hierin met name zaken nogmaals toetst of dat zij ook nieuwe onderwerpen examineert.De opleiding kan het toetssysteem verder verbeteren door op voorgaande punten nadere, schriftelijke duidelijkheid te scheppen richting studenten en docenten.

Beslissingsformulieren
De beslissingsformulieren geven in de basis richting aan het leerproces van de studenten en de toetsing daarvan door de assessoren. De opleiding dient aan deze formulieren de nog ontbrekende (invul)ruimte toe te voegen waarin de assessoren hun oordeel per leeruitkomst onderbouwen. De vertegenwoordigers van de examencommissie herkennen deze bevinding van het panel en zijn dezelfde mening toegedaan.

Validiteit en betrouwbaarheid
De Ad Cybersecurity neemt verschillende goede maatregelen om de kwaliteit van de toetsing te waarborgen. De examencommissie stelt de examinatoren aan op basis van de eisen vastgelegd

in het toetsbeleid van het IAd. De opleiding vergroot de betrouwbaarheid van de toetsing door te werken met verschillende soorten toetsbare prestaties en feedback van meerdere partijen. De opleiding voorziet in periodieke kalibratie. Van deze bijeenkomsten dient zij verslag te doen richting de examencommissie. Verder schrijft het toetsbeleid voor dat elke onderwijseenheid van 30 EC door minimaal twee assessoren (vier ogen) moet worden beoordeeld. De Ad Cybersecurity geeft aan dat tevens voor de periodes van 15 EC zo te gaan doen. Dat is positief en vraagt tegelijkertijd in de praktijk een extra inspanning van docenten.

Afstuderen
De opleiding werkt de afstudeerfase in het dossier verder uit. Voor het afstuderen formuleert de opleiding twee specifieke leeruitkomsten. Uit het toetsplan blijkt dat alle zeven competenties in het praktijkvraagstuk dienen terug te komen. De leeruitkomsten bieden studenten en organisaties een bepaalde mate van eigen invulling voor het praktijkvraagstuk. De opleiding dient het vraagstuk voorafgaand aan de stage goed te keuren. In de gesprekken geven de werkveldvertegenwoordigers voorbeelden van concrete opdrachten die zij voor deze Ad-studenten in hun organisaties zien. Een docentbegeleider en een praktijkbegeleider ondersteunen studenten bij de praktijkopdracht. Tijdens het afstudeertraject voorziet de opleiding in drie contactmomenten tussen begeleiders en student. Ook zijn er driewekelijkse terugkomdagen wat het panel positief vindt.

Twee examinatoren beoordelen de student door middel van een assessment inclusief criteriumgericht interview. De praktijkbegeleider is geen officiële examinator, maar geeft gedurende het proces in de datapunten wel schriftelijke feedback op de prestaties van de studenten die wordt meegenomen in de eindbeoordeling. Op deze wijze werkt de Ad Cybersecurity het proces van het afstuderen en de toetsing daarvan in de basis goed uit. Inhoudelijk krijgen deze Ad-studenten echter nog weinig richting bij de prestaties die de opleiding tijdens het afstuderen van hen verwacht. Dat komt mede doordat het beslissingsformulier nog erg algemeen is en afwijkt van die van de overige modules. Het panel doet de aanbeveling als de Ad Cybersecurity is gestart nadere criteria voor het afstuderen te formuleren en de beslissingsformulieren te uniformeren.

Examencommissie & toetscommissie
De zeskoppige examencommissie van het IAd is verantwoordelijk voor de borging van de toetsing van de Ad Cybersecurity. Een instituutsbrede toetscommissie ondersteunt haar daarbij. In de gesprekken sprak het panel met taakvolwassen en positief kritische commissieleden met een duidelijke visie op en ervaring met PT. De opleiding heeft deze commissies tijdig in het ontwikkelproces van de Ad Cybersecurity betrokken en input gevraagd op de toetsdocumentatie. De examencommissie heeft goed zicht op het niveau doordat de IAd reeds veel Ad-opleidingen aanbiedt en deze allemaal werken met de zes generieke competenties.

Voordat de opleiding start, zal de examencommissie conform haar beleid de toetsdocumentatie nog verifiëren. Tevens controleert zij voor één of twee periodes uit jaar 1 de toetsing in zijn geheel op consistentie en volledigheid. Het panel is hier positief over, mede omdat de examencommissie zo een extra check kan doen op de mogelijke implicaties die de onder standaard 2 gesteld voorwaarde op de invulling van de toetsing kan hebben. Tot slot, overziet de examencommissie de periodieke kalibratie van de toetsing als de opleiding is gestart.

Het panel constateert dat de opleiding conform het toetsbeleid van het instituut met PT een toetssysteem inricht dat het leerproces van de studenten goed ondersteunt. De Ad

Cybersecurity werkt dit systeem in de basis goed uit. Wel behoeft de toetsdocumentatie nog op meerdere vlakken nadere schriftelijke uitwerking teneinde de eisen voor studenten beter inzichtelijk te maken. De opleiding neemt adequate maatregelen om valide en betrouwbaar te toetsen. De sterke examencommissie en toetscommissie zijn actief betrokken bij de borging hiervan en voeren hun controlerende en adviserende taak goed uit.

6.4 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: Techniek

Afkortingen

Ad:	Associate degree
BoKS	Body of Knowledge & Skills
CROHO:	Centraal Register Opleidingen Hoger Onderwijs
EC:	European Credits
Hbo:	Hoger beroepsonderwijs
HU:	Hogeschool Utrecht
IAd	Instituut voor Associate degrees
Mbo	Middelbaar beroepsonderwijs
PTES	Penetration Test Execution Standard
PT	Programmatisch Toetsen

Het adviesrapport is tot stand gekomen in opdracht van de NVAO met het oog op de beperkte toetsing van de nieuwe opleiding Ad Cybersecurity van de Hogeschool Utrecht

Aanvraagnummer: AV-1759

NVAO

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG 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