# hbo-master Master Cyber Security Engineering

## De Haagse Hogeschool

28 maart 2018

NVAO uitgebreid Toets nieuwe opleiding Adviesrapport

**Inhoud**

# 1 Samenvattend advies

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) ontving op 19 oktober 2017 een aanvraag voor een Toets Nieuwe Opleiding (TNO) voor de opleiding hbo-masteropleiding Cyber Security Engineering van De Haagse Hogeschool. 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.

In hoofdlijnen is het panel positief over de kwaliteit van de nieuwe hbo-masteropleiding CSE. Sterke punten zijn het beroepsgerichte karakter en de breedte van de opleiding. Het panel is van mening dat de Haagse Hogeschool een stevig programma heeft neergezet, dat goed aansluit bij ontwikkelingen in de markt.

De masteropleiding CSE wil professionals opleiden om een leidende rol als technisch specialist in het domein van cybersecurity te vervullen. Die focus ligt op een integrale benadering van cybersecurity, waarbij een praktijkgeoriënteerde invalshoek gecombineerd wordt met een wetenschappelijke basis. De eindkwalificaties zijn gebaseerd op het profiel van de PvIB (de beroepsvereniging van informatiebeveiligers) ICT-beveiligingsspecialist op masterniveau. Op het vlak van de competenties ziet het panel een goed evenwicht tussen de ‘soft skills’ en de meer harde, technische competenties.

Het programma bestaat uit vier semesters van 15 ects. Het panel kan zich vinden in de opbouw van het programma. De techniek is geconcentreerd in het tweede semester, maar er zit ook voldoende techniek in de beide andere semesters. Het programma is breed, maar biedt voldoende mogelijkheden om de invulling aan te passen aan de actualiteit. Wel is het panel van mening dat het systeem van leerlijnen niet onderhoudbaar is. Het panel adviseert het aantal leerlijnen terug te brengen en het systeem transparanter te maken. Daarnaast adviseert het panel de opleiding om een sterkere invulling aan internationalisering te geven.

Het panel kan zich eveneens vinden in de vormgeving van het programma. De combinatie van praktijk- en onderzoekgerichtheid legt een goede basis voor de werkcolleges en opdrachten. Wel is het panel van mening dat de opzet van de ICT-labs, waarin studenten oefenen met concrete opdrachten op het gebied van cybersecurity, ambitieuzer en innovatiever zou kunnen zijn.

De opleiding werkt met een team van ongeveer 5 à 6 vaste kerndocenten. Gezamenlijk zorgen zij voor de structuur, de samenhang en het niveau van het programma. Het panel heeft een positief beeld van de deskundigheid en betrokkenheid van de docenten. Wel acht het panel het van belang dat de docenten in staat gesteld worden om hun vak bij te houden of hun onderwijs te actualiseren. Het panel adviseert de docenten meer tijd te geven voor onderzoek en scriptiebegeleiding.

De masteropleiding is bedoeld voor professionals met ten minste twee jaar werkervaring in ICT of ICT-security en een academisch denkniveau. Het panel is van mening dat de intakeprocedure goed is geregeld. De groepen zijn klein, met maximaal 25 deelnemers. Ook de studiebegeleiding en de informatievoorziening zijn afdoende geregeld.

De opleiding voldoet in de visie van het panel aan de formele voorwaarden voor toetsing. Het toetshandboek bevat een heldere visie en richtlijnen en de procedures zijn duidelijk en

volledig. De toetsen voldoen aan het vierogenprincipe. De examencommissie en de toetscommissie vervullen hun taken naar behoren. Wel adviseert het panel om te zorgen voor voldoende deskundigheid op het gebied van cybersecurity binnen de examencommissie. Daarnaast adviseert het panel om de urenbegroting voor deze commissies te verruimen; met name de tijd die de toetscommissie voor haar werkzaamheden heeft gekregen, is zeer beperkt.

Het panel komt op grond van deze overwegingen tot een **positief** eindoordeel ten aanzien van de kwaliteit van de nieuwe post-initiële hbo-masteropleiding Cyber Security Engineering van De Haagse Hogeschool en adviseert de NVAO overeenkomstig te besluiten.

Den Haag, 28 maart 2018

Namens het panel ter beoordeling van de uitgebreide Toets nieuwe opleiding hbo-masteropleiding Cyber Security Engineering van De Haagse Hogeschool,

prof. dr. ir. Bart Preneel,
(voorzitter)

drs. Erik van der Spek
(secretaris)

# 2 Introductie

## 2.1 Werkwijze panel

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) ontving op 19 oktober 2017 een aanvraag voor een Toets Nieuwe Opleiding (TNO) voor de hbo-masteropleiding Cyber Security Engineering (CSE) van De Haagse Hogeschool. 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 wettelijk beschermde getuigschriften of diploma's afgeven die bij de opleiding horen.

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

Om de nieuwe opleiding te beoordelen, heeft de NVAO een panel samengesteld met de volgende experts:

- Prof.dr.ir. B (Bart) Preneel, hoogleraar Computerbeveiliging en Industriële Cryptografie aan de KU Leuven (voorzitter);
- Ir. C.J. (Kees) Rijsenbrij (panellid); hogeschool hoofdocent en opleidingsmanager HBO-ICT bij de Hogeschool van Amsterdam;
- M. (Michael) Pols (panellid), Security Officer bij The Future Group;
- K. (Kevin) Voorn (student-panellid), student HBO-ICT aan de Hanzehogeschool Groningen.

Het panel werd bijgestaan door Ed Lansink, beleidsmedewerker NVAO, als procescoördinator en door Erik van der Spek, Hendrikx Van der Spek als secretaris.

Bij de toetsing heeft het panel het Beoordelingskader voor de uitgebreide Toets nieuwe opleiding van de NVAO (Stcrt. 2016, nr 69458) in acht genomen.

De opleiding heeft een informatiedossier met bijlagen verstuurd. Het panel heeft zich aan de hand van deze documenten op de beoordeling voorbereid. Op 2 februari 2018 is het panel bij elkaar geweest. Tijdens deze bijeenkomst zijn de eerste bevindingen van het panel besproken en vragen geformuleerd voor het locatiebezoek.

Op 7 februari 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 de bevindingen en overwegingen onderling besproken en vertaald naar voorlopige conclusies. Aan het eind van het bezoek heeft de panelvoorzitter die conclusies teruggekoppeld naar de opleiding.

Op basis van de bevindingen, overwegingen en conclusies heeft de secretaris een conceptadvies opgesteld dat aan de panelleden is voorgelegd. De panelleden hebben dit concept van commentaar voorzien, waarna het conceptrapport is vastgesteld door de voorzitter. Het adviesrapport is op 13 maart 2018 aan de opleiding voorgelegd ter controle op feitelijke onjuistheden. De opleiding heeft op 26 maart 2018 gereageerd op het adviesrapport. Dit heeft geleid tot enkele kleine aanpassingen, waarna het definitieve

rapport is vastgesteld door de voorzitter. Het panel heeft dit advies in volledige onafhankelijkheid opgesteld en op 28 maart 2018 aan de NVAO aangeboden.

### 2.2 Opzet van het panelrapport

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

In het derde hoofdstuk vindt u een korte schets van de opleiding en de instelling. In dit hoofdstuk gaan we ook in op de positionering van de opleiding binnen de instelling en binnen het hoger onderwijsbestel in Nederland.

De kern van het rapport is hoofdstuk 4. Dit hoofdstuk volgt de onderwerpen en standaarden uit het beoordelingskader voor nieuwe opleidingen. Per standaard geeft het panel zijn bevindingen, overwegingen en conclusies weer. De bevindingen zijn gebaseerd op de waarnemingen van het panel in de aangeleverde documentatie en tijdens 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 spreekt het panel ook een algemeen eindoordeel uit. Tot slot wordt in een tabel weergegeven wat de oordelen per standaard zijn.

# 3 Beschrijving van de opleiding

## 3.1 Algemeen

| | |
|---|---|
| Instelling: | De Haagse Hogeschool |
| Opleiding: | hbo-master Cyber Security Engineering |
| Variant(en): | Deeltijd 2 jaar (24 maanden) |
| Graad: | Master of Science (MSc) |
| Afstudeerrichtingen: | n.v.t. |
| Locatie(s): | Delft, Den Haag, Zoetermeer |
| Studieomvang (EC): | 60 |
| CROHO-onderdeel | techniek |

Voorstel voor indeling in een visitatiegroep: P.M.

## 3.2 Profiel instelling

De Haagse Hogeschool is een middelgrote hbo-instelling met vestigingen in Den Haag, Delft en Zoetermeer. In 2017 bestond de instelling 30 jaar. De Haagse Hogeschool biedt ruim 65 bacheloropleidingen en ongeveer 15 masteropleidingen aan; daarnaast verzorgt de instelling ook post-hbo-opleidingen. Ongeveer 26.000 studenten volgen er een opleiding en er werken ruim 1.900 medewerkers, waarvan 65% in een onderwijzende en 35% in een ondersteunende functie.

Het onderwijs is georganiseerd in zeven faculteiten en één academie, de Academie voor Masters en Professional Courses. Het onderzoek is ingericht rondom vier centrale onderzoeksthema's: The Next Economy, Kwaliteit van Leven: Mens en Technologie, Goed Bestuur voor een Veilige Wereld en Connected Learning. De Haagse Hogeschool richt zich in de komende jaren onder meer op de doorontwikkeling van het internationale profiel (de studenten vertegenwoordigen bijna 150 nationaliteiten) en de bevordering van wereldburgerschap.

De masteropleiding Cyber Security Engineering is ontwikkeld in samenwerking met de Stichting Cyber Security Academy (CSA). De CSA is een initiatief van de Gemeente Den Haag, waarin de Haagse Hogeschool, de Universiteit Leiden en de Technische Universiteit Delft samenwerken. De CSA is gevestigd op de campus van The Hague Security Delta; hier wordt het grootste deel van de opleiding verzorgd.

## 3.3 Profiel opleiding

De masteropleiding Cyber Security Engineering (CSE) is ontwikkeld om een oplossing te bieden voor het groeiende tekort aan goed opgeleide technische cybersecurityspecialisten op de arbeidsmarkt. Het is de eerste technische masteropleiding die is opgesteld op basis van de profielen van de beroepsvereniging van informatiebeveiligers en cybersecurity-professionals (PvIB). De nieuwe master geeft invulling aan het profiel ‘ICT-beveiligingsspecialist op masterniveau’.

De masteropleiding CSE wil professionals die werkzaam zijn in de beroepspraktijk opleiden tot technisch specialist in het domein van cybersecurity. De focus ligt op het onderzoeken van cybersecurityproblematiek in complexe situaties en het ontwikkelen van ICT-

gerelateerde securityoplossingen. Het gaat met name om technologische aspecten in de specifieke context van organisaties en hun samenwerkingspartners.

De opleiding wordt verzorgd in deeltijd. Het programma is opgebouwd uit vier semesters:
1. Conceptualisering cybersecurity
2. Cybersecurity bouwstenen
3. Cybersecurity in sectoren en trends
4. Thesis

De kern van de opleiding is het aanbrengen van een gedegen inzicht in de technologische aspecten van cybersecurity. Daarbij is het de bedoeling dat de technische specialist een goed oog heeft voor de verwevenheid van technische problemen en oplossingen in een organisatie met niet-technische aspecten om daarop te anticiperen bij het ontwikkelen van ICT-gerelateerde security-oplossingen.

Bij Nederlandse universiteiten worden verschillende masteropleidingen op het gebied van cybersecurity aangeboden, onder andere bij de TU Delft en de Universiteit van Amsterdam. Dit zijn academisch georiënteerde opleidingen, in tegenstelling tot de masteropleiding CSE. Verder wordt bij de Cyber Security Academy zelf ook een executive master Cyber Security aangeboden. Deze executive master richt zich vooral op bestuurlijk-organisatorische aspecten van cybersecurity, terwijl in de nieuwe master de technische kant veel sterker is neergezet.

# 4 Opleidingsbeoordeling

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 uitgebreide 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 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, het vakgebied en op internationale eisen.*

*Bevindingen*
De masteropleiding Cyber Security Engineering wil professionals opleiden om een leidende rol als technisch specialist in het domein van cybersecurity te vervullen. De focus ligt hierbij, aldus het informatiedossier, op het onderzoeken van cybersecurityproblematiek in complexe situaties en het ontwikkelen van ICT-gerelateerde securityoplossingen die passen bij de doelstellingen van organisaties. Het gaat met name om technologische aspecten, maar dan wel in de specifieke context van een organisatie.

De Haagse Hogeschool signaleert een tekort aan goed opgeleide cybersecurity-professionals, zowel op technisch als op bestuursmatig gebied. Verschillende onderzoeken van de overheid en koepelorganisaties ondersteunen deze observatie, blijkt uit het dossier. Dit tekort is niet beperkt tot Nederland, maar geldt ook voor de omringende landen. De nieuwe opleiding is erop gericht om een deel van dit tekort weg te nemen: de opleiding levert ICT-beveiligingsspecialisten op masterniveau af.

De nieuwe master is gebaseerd op het profiel van de PVIB (de beroepsvereniging van informatiebeveiligers en cybersecurity-professionals) voor ICT-beveiligingsspecialist op masterniveau. Dit profiel is gebruikt om een toepassingsgerichte wetenschappelijke opleiding te ontwikkelen. De kern van dit profiel is dat de studenten een gedegen inzicht verwerven in de technologische aspecten van cybersecurity. De cyberspecialist moet een goed oog hebben voor de verwevenheid van technische problemen en oplossingen in een organisatie aan de ene kant met niet-technische aspecten aan de andere kant. Die verwevenheid vormt het uitgangspunt bij het ontwikkelen van ICT-gerelateerde security-oplossingen.

De eindkwalificaties zijn gebaseerd op het PvIB-profiel ICT-beveiligingsspecialist op masterniveau. Het omvat competenties op de volgende acht thema's:

1. Risicomanagement
2. Informatiebeveilingsmanagement

3. Volgen van technologische ontwikkelingen
4. Oplossingen implementeren
5. Onderzoek
6. Analytisch vermogen
7. Communicatie en overtuigingskracht
8. Integriteit

*Overwegingen*
Het panel kan zich vinden in de focus van de nieuwe masteropleiding. Die focus ligt op een integrale benadering van cybersecurity, die een praktijkgeoriënteerde invalshoek combineert met een wetenschappelijke basis. Dat de opleiding eerder de breedte dan de diepte zoekt, kan het panel billijken: de opleiding richt zich op een werkterrein met veel toepassingen.

De opleiding gaat uit van het beroepsprofiel dat is opgesteld door het Platform van Informatiebeveiligers (PvIB). Het panel kan zich hierin vinden, maar is wel van mening dat de opleiding aansluiting zou moeten zoeken bij cybersecurity-opleidingen in het buitenland, om een sterkere relatie te leggen tussen het Nederlandse platform en internationale referentiekaders, zoals het document van de Joint Task Force on Cybersecurity Education (ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8).

Het panel heeft zich verdiept in nut en noodzaak van de nieuwe masteropleiding, zowel in relatie tot de executive master Cyber Security (eveneens van de Cyber Security Academy, CSA) als in relatie tot vergelijkbare opleidingen van andere instellingen. Een presentatie van de CSA heeft geholpen om hierin meer inzicht te krijgen. Het panel constateert dat de bestaande executive master meer maatschappelijk-bestuurlijk is georiënteerd, meer gericht is op governance en in verhouding minder technologie bevat. Bij de nieuwe master neemt de technologie een grotere plaats in, en deze master is meer gericht op bedrijven en organisaties en minder op de overheid.

Ook andere universiteiten, zoals de TU Delft en de UvA, bieden masteropleidingen op het gebied van cybersecurity aan. Het grote verschil, aldus de vertegenwoordigers van de CSA, is dat de nieuwe masteropleiding van de Haagse Hogeschool zicht richt op mensen die al een aantal jaren in de beroepspraktijk werken. De masteropleiding in Delft richt zich op jonge mensen zonder ervaring; het is een tweejarige master met een sterk onderzoekskarakter en met een uitgebreide training in allerlei technische vakken. De nieuwe Haagse opleiding is een éénjarige master (twee jaar in deeltijd), veronderstelt veel praktische kennis, en richt zicht op een instroom die zijn eigen praktijkproblemen meeneemt. Dat resulteert in een sterke balans tussen onderzoek en praktijk.

Op het vlak van de competenties ziet het panel een goed evenwicht tussen de ‘soft skills’ en de meer harde, technische competenties. Soft skills, zoals communicatieve vaardigheden, schrijven en presenteren, krijgen veel gewicht. Wat betreft de technische competenties baseert de opleiding zich op het beroepsprofiel, dat regelmatig wordt bijgesteld. De moduleomschrijvingen bevatten voldoende ruimte om de kerndocenten in staat te stellen de eigen onderdelen te actualiseren. Dus de opleiding ligt op hoofdlijnen vast, maar de docenten zorgen voor de concrete invulling. Het panel kan zich hierin vinden.

*Conclusie:* voldoet

## 4.2 Programma

### 4.2.1 Oriëntatie

*Standaard 2: Het programma maakt het mogelijk om passende (professionele of academische) onderzoeks- en beroepsvaardigheden te realiseren.*

*Bevindingen*
Beroepsvaardigheden en academische vaardigheden nemen volgens de Haagse Hogeschool een belangrijke plaats in de opleiding in. Dit blijkt ook uit het gewicht dat aan de professionele competenties wordt toegekend (zie 4.1). Uit de contacten met het beroepenveld is gebleken welke beroepsvaardigheden in de opleiding aan de orde moeten komen. Bovendien zijn de studenten afkomstig uit het werkveld en hebben ze minimaal twee jaar praktijkervaring in een relevante functie.

De scholing van beroepsvaardigheden wordt ondersteund door docenten met praktijkervaring (een deel van de docenten is werkzaam in de beroepspraktijk) en gastdocenten. Praktische vaardigheden worden verder ontwikkeld in professional skills workshops, ICT-labs (bijvoorbeeld voor het analyseren van cyberaanvallen) en praktijkgerichte opdrachten en case studies.

Bij de academische vaardigheden kan de opleiding steunen op drie lectoren vanuit het Center of Expertise Cyber Security. Twee van de drie lectoren zijn nauw betrokken bij de ontwikkeling en uitvoering van het curriculum. Bij elke module wordt daarnaast minimaal één gepromoveerde docent ingezet. Verder is de scholing van onderzoeksvaardigheden uitgewerkt in de onderzoeksleerlijn. Het ontwikkelen van onderzoeksvaardigheden komt in elke module aan de orde. De onderzoeksleerlijn sluit af met het schrijven van de thesis, waarbij de studenten zelfstandig een onderzoeksopdracht moeten uitvoeren.

*Overwegingen*
De opleiding wordt naar eigen zeggen gekenmerkt door een benadering die zowel onderzoek- als praktijkgericht is; de problemen komen uit de praktijk, maar ze worden op een wetenschappelijke manier opgelost. Het panel kan zich vinden in deze karakterisering. De beroepsgerichte invulling is in de beleving van het panel het sterkste ontwikkeld. Die komt in een aantal facetten tot uiting: de koppeling van de beroepspraktijk van de studenten aan de opleidingsvraagstukken, de praktische insteek van de docenten (docenten met praktijkervaring en gastdocenten) en de eigen ervaring die de studenten in hun opleiding inbrengen.

De Adviescommissie, met vertegenwoordigers van het beroepenveld, is sterk betrokken geweest bij de totstandkoming van de opleiding. Een aantal bedrijven, zoals Deloitte en Fox-IT, is heel belangrijk voor de opleiding; vertegenwoordigers van deze bedrijven verzorgen ook (onderdelen van) cursussen. In de komende periode gaat het er vooral om de actualiteit van het programma te bewaken. Hiertoe zal de opleiding nagaan of de zittende commissie lacunes vertoont.

De onderzoeksgerichtheid van de nieuwe masteropleiding is in de visie van het panel minder geprononceerd, maar neemt desalniettemin een duidelijke plaats in. Onderzoek wordt in de opleiding gepositioneerd vanuit drie werelden: de beroepspraktijk, de wereld van de student die werkt aan zijn of haar onderzoekend vermogen (de competentie), en de

wereld van de wetenschap (methodologische eisen). Die drie aspecten worden uitgewerkt met behulp van de onderzoeksleerlijn. Het gaat daarbij om toegepast onderzoek. Daarbij acht de opleiding het van groot belang dat de probleemanalyse goed is ingebed in de beroepspraktijk, en dat aan het slot de conclusies ook weer worden terugvertaald naar het beroepenveld. Het panel kan zich hierin vinden, maar is wel van mening dat eindkwalificatie 6 ('zelfstandig onderzoek kunnen doen en daarover publiceren') ambitieus is voor deze doelgroep.

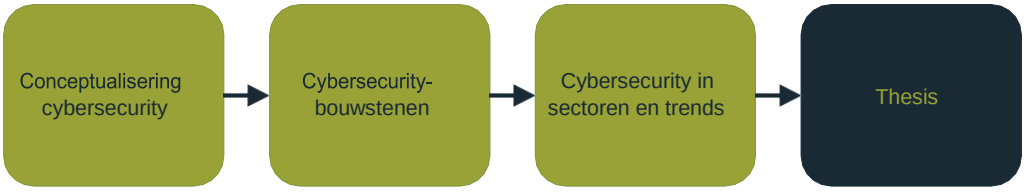
Tot slot stimuleert de opleiding de studenten om hun masterthesis in enige vorm te publiceren. Het panel is van mening dat deze stimulans zou moeten resulteren in beleid voor de wijze waarop de opleiding wil omgaan met kennisdisseminatie. Het panel adviseert de opleiding om zo'n beleid te ontwikkelen, inclusief streefgetallen voor publicaties.

*Conclusie:* voldoet

### 4.2.2 Inhoud van het programma

*Standaard 3: De inhoud van het programma biedt studenten de mogelijkheid om de beoogde leerresultaten te bereiken.*

*Bevindingen*
Het programma bestaat uit vier semesters van 15 ects. Elk semester staat in het teken van een bepaald thema:




Semester 1 brengt het 'speelveld' van cybersecurity in kaart. In dit semester ontwikkelen de studenten een gemeenschappelijk denkkader en worden hun kennis en vaardigheden op een gelijk niveau gebracht. In semester 2 staat de techniek centraal: in dit semester verdiept de student zich in cyberdreigingen en –kwetsbaarheden, plus de verdediging daartegen. In dit semester komen cyberaanvallen, pen-testing en malware aan de orde, evenals de verschillende soorten beveiligingsmaatregelen. In semester 3 wordt de kennis uit de voorgaande semesters toegepast op organisaties in verschillende sectoren, zoals de financiële sector, de zorg en een aantal vitale sectoren. In semester 4 wordt de studie afgerond met een zelfstandig onderzoek en het schrijven van de thesis.

De eerste drie semesters bestaan elk uit drie modules van zeven weken (5 ects).Elke module bevat een aantal vakken en een of meer projectopdrachten. Iedere module sluit af met een toetsing in de vorm van een (module) tentamen en/of een projectassessment.

Het programma ziet er als volgt uit:


De opleiding wordt gestructureerd aan de hand van leerlijnen. De opleiding heeft 18 leerlijnen benoemd; naast algemene leerlijnen als ‘Onderzoeksvaardigheden’ en ‘Communicatieve vaardigheden’ zijn dat ook tamelijk specifieke thema’s zoals ‘Hacking en malware’ en ‘De menselijke factor’.

De opleiding signaleert dat cybersecurity een wereldomvattende problematiek betreft en dat cyberdreigingen vaak grensoverschrijdend zijn. Daarom bevat het curriculum de nodige internationale elementen, bijvoorbeeld internationale casuïstiek. De opleiding wordt in het Nederlands gegeven, maar vrijwel alle literatuur is in het Engels. De opleiding besteedt verder aandacht aan communiceren in het Engels, een deel van de colleges en opdrachten is Engelstalig en de studenten worden gestimuleerd om de masterthesis in het Engels te schrijven.

*Overwegingen*
Het panel constateert dat de opleiding een breed curriculum aanbiedt; het is eerder een programma in de breedte dan in de diepte. Dat wordt ook bevestigd door de studenten (van de Executive master). Aan de andere kant stelt het panel vast dat de onderwerpen die aan de orde komen, wel allemaal thuishoren in deze opleiding. Bovendien hebben de studenten door hun werkervaring veel voorkennis, waardoor ze bepaalde thema’s snel tot zich kunnen nemen. Overigens signaleert het panel ondanks de brede scope toch nog een aantal omissies: hardware security en certificering van producten zouden volgens het panel ook een plaats in het programma moeten krijgen.

Het vakgebied van cybersecurity is sterk in beweging. Dat maakt actualisering een uitdaging. De docenten geven aan dat de basistechnieken een constante factor vormen, maar dat het programma voldoende flexibiliteit biedt om nieuwe ontwikkelingen of incidenten op te nemen. Bovendien bestaat de mogelijkheid om gastdocenten in te huren die kunnen inspelen op nieuwe trends. Tot slot is één module (module 9, Trends) geheel gericht op de actualiteit. Het panel kan zich hierin vinden.

Het panel vindt de opbouw van het programma goed. De techniek is geconcentreerd in het tweede semester, maar er zit ook voldoende techniek in de beide andere semesters. Het panel herkent de ‘sandwichconstructie’ die ten grondslag ligt aan de opbouw: in het eerste halfjaar ligt de focus vooral op de organisatorische context, in het tweede halfjaar staat de

techniek centraal, in het derde halfjaar komen de verschillende bedrijfssegmenten op de voorgrond.

Het panel is kritisch over het systeem van leerlijnen; in de visie van het panel is dit systeem niet onderhoudbaar. Veel zogenoemde leerlijnen zijn eerder thema's, die soms slechts in één module aan de orde komen. Het panel kan zich voorstellen dat het denken in de huidige leerlijnen zinvol is geweest in de ontwikkelingsfase, maar is van mening dat het systeem in de implementatiefase transparanter en eenvoudiger zou moeten worden.

Tot slot kan het panel zich verplaatsen in de plaats die het Engels in de opleiding inneemt. De opleiding heeft gekozen voor een hybride vorm; weliswaar is Nederlands de instructietaal, maar de plaats van het Engels – in de literatuur, een deel van de opdrachten en een deel van de werkcolleges – is aanzienlijk. De studenten moeten ook het Engelstalige vakjargon op het gebied van cybersecurity kennen. Aan de andere kant vindt het panel de invulling van de internationalisering aan de magere kant. Het panel adviseert om daar een sterkere invulling aan te geven, vooral als het gaat om de inhoud van het onderwijs.

*Conclusie:* voldoet

### 4.2.3 Leeromgeving

*Standaard 4: De vormgeving van het programma zet aan tot studeren en biedt studenten de mogelijkheid om de beoogde leerresultaten te bereiken.*

*Bevindingen*
De opleiding noemt zichzelf onderzoekgericht en praktijkgericht. Deze twee invalshoeken bepalen grotendeels de vormgeving van het programma. Om te beginnen de gerichtheid op de praktijk. In elke module worden casestudies gebruikt, afkomstig uit de praktijk van de deelnemers of van de docenten. De praktijkvoorbeelden helpen de studenten om geleerde kennis toe te passen of nieuwe kennis te ontwikkelen.

Kant-en-klare oplossingen zijn binnen de cybersecurity meestal niet beschikbaar. Studenten moeten onderzoek doen naar cybersecurityproblemen en ze moeten de bruikbaarheid van oplossingen kunnen toetsen. Dat veronderstelt het vermogen om praktijkgericht onderzoek uit te voeren; design science research speelt daarbij een belangrijke rol. In elke module voeren studenten opdrachten uit, waarbij ze hun academische onderzoeksvaardigheden ontwikkelen.

De opleiding maakt gebruik van verschillende werkvormen. De meest voorkomende zijn werkcolleges, gastcolleges en workshops. Specifiek voor cybersecurity zijn daarnaast de lab-workshops ontwikkeld: een lab is een IT-leeromgeving waarin studenten opdrachten en experimenten kunnen uitvoeren. Het is een voorziening, maar ook een geroosterde activiteit.

De labs bieden de studenten veel vrijheid om te experimenteren. Ze kunnen in de labs daadwerkelijk IT-systemen doorzoeken, bijvoorbeeld om kwetsbaarheden te vinden of om een cyberaanval af te slaan. De opleiding brengt verschillende omgevingen tot stand, bijvoorbeeld om studenten certificaten te laten aanmaken (PKI) en beveiligingsoplossingen

te laten programmeren en implementeren. Eén lab omvat een geïsoleerde omgeving om te experimenteren met malware in het kader van ‘offensive testing’ (module 5).

*Overwegingen*
Het panel kan zich op hoofdlijnen vinden in de vormgeving van het programma. De combinatie van praktijk- en onderzoekgerichtheid legt een goede basis voor de werkcolleges en opdrachten. Het panel ziet voldoende variatie in de werkvormen, hoewel de werkcolleges en (groeps)opdrachten wel duidelijk domineren.

Het panel heeft een korte presentatie gekregen over de ICT-labs en heeft met belangstelling kennisgenomen van de opzet. We constateren dat de basisvoorzieningen in deze labs aanwezig zijn, maar zijn van mening dat de opleiding op dit punt ambitieuzer en innovatiever zou kunnen zijn. Een voorbeeld is het gebruik van de meest recente tools om software te verifiëren op zwakheden of een lab waarin de security risico’s van verschillende hardwarecomponenten getest worden. Een speelsere mogelijkheid is Capture the Flag, waarin een groep hackers (red team) de strijd aanbindt met cybersecurity professionals (blue team). Het panel adviseert de opleiding om de labs meer invulling en een grotere plaats in het curriculum te geven.

Wat betreft de studielast heeft het panel de indruk dat het zwaartepunt van de opleiding in het tweede semester ligt. In dit semester komen de cybersecurity-bouwstenen en daarmee de meeste technische onderwerpen aan de orde. De opleiding heeft de literatuur nog niet geteld, dus een onderbouwde berekening van de studielast is nog niet mogelijk. Het panel adviseert de opleiding om na telling goed te inventariseren of de studielast evenwichtig is verdeeld en zo nodig aanpassingen door te voeren.

*Conclusie:* voldoet

### 4.3 Instroom

*Standaard 5: Het programma sluit aan bij de kwalificaties van de instromende studenten.*

*Bevindingen*
De masteropleiding is bedoeld voor professionals met ten minste twee jaar werkervaring in ICT of ICT-security en een academisch denkniveau. Zij moeten voldoen aan de volgende instroomeisen:

1. Een afgeronde bacheloropleiding (hbo of wo) in technische informatica, ICT, cybersecurity, of gelijkwaardig.
2. Minimaal twee jaar werkervaring op het gebied van ICT of cybersecurity.
3. Een werkkring waarin de student opdrachten kan uitvoeren.

Met iedere kandidaat wordt een intakegesprek van ongeveer een halfuur gehouden waarin de bovenstaande punten aan de orde komen. Bij dit gesprek zijn drie vertegenwoordigers van de opleiding aanwezig. Ze gaan tijdens het gesprek ook in op de motivatie van de student en diens passie voor cybersecurity. Tijdens het intakegesprek wordt ook gesproken over de verwachting van de student en over de consequenties van een combinatie van een opleiding, baan en privéleven. De programmamanager beslist uiteindelijk over toelating tot de opleiding.

*Overwegingen*
Het panel is van mening dat de intakeprocedure goed is geregeld. De procedure, besluitvorming en criteria zijn duidelijk omschreven en de goede onderwerpen komen erin aan de orde. Studenten met deficiënties wordt geadviseerd om hun vaardigheden bij te spijkeren. Ook de studenten van de Executive master die het panel heeft gesproken, waren tevreden over de intakeprocedure en vonden dat de vertegenwoordigers van de opleiding een duidelijk beeld hadden geschetst.

*Conclusie: v*oldoet

### 4.4 Personeel

*Standaard 6: Het docententeam is gekwalificeerd voor de inhoudelijke en onderwijskundige realisatie van het programma en de omvang ervan is toereikend.*

*Bevindingen*
De opleiding werkt met een team van 5 à 6 vaste kerndocenten. Deze docenten zijn betrokken (geweest) bij de ontwikkeling van de opleiding. Gezamenlijk zorgen zij voor de structuur, de samenhang en het niveau van het programma. De meeste kerndocenten zijn gepromoveerd, twee van hen zijn werkzaam als lector bij De Haagse Hogeschool. De lectoren bieden studenten de mogelijkheid om deel te nemen aan onderzoeksprojecten van de lectoraten. Bovendien zijn zij direct betrokken bij het invullen van de onderzoeksleerlijn in het curriculum.

Naast de kerndocenten zijn verschillende andere docenten bij de master betrokken. Ten minste 80% van de docenten beschikt over een relevante master of hoger. Tot slot worden ook gastdocenten ingezet: dit zijn professionals uit de beroepspraktijk, deels afkomstig uit het netwerk van de Cyber Security Academy.

Het personeelsbeleid van de opleiding is gebaseerd op het Strategisch Personeelsbeleid 2013-2017 van de Academie voor Masters & Professional Courses. Het panel heeft dit document ingezien tijdens het locatiebezoek. De Haagse Hogeschool biedt verschillende opleidingsmogelijkheden aan voor docenten. De docenten kunnen daarvoor gebruik maken van het opleidingscentrum van de hogeschool, *The Hague centre for teaching and learning* (HCTL). Vrijwel alle vaste staf beschikt over een Basiskwalificatie Onderwijs (BKO).

*Overwegingen*
Het panel heeft kennisgemaakt met een aantal docenten en heeft een positief beeld van hun deskundigheid en betrokkenheid. Het wetenschappelijk niveau is voldoende: naast een aantal gepromoveerde docenten beschikt de opleiding over een groot aantal docenten met een masteropleiding. Ook hebben veel docenten een voldoende aantal publicaties op hun naam staan.

Toch heeft het panel ook een aantal aandachtspunten bij het docententeam. Een eerste punt is dat sommige docenten weinig tijd beschikbaar hebben voor onderzoek: voor sommige docenten is de onderzoekstijd beperkt tot één dag per week. In de visie van het panel is dat te weinig, zeker gezien de snelle ontwikkelingen op het gebied van cybersecurity. Het panel acht het belangrijk dat de docenten in staat gesteld worden om hun

vak bij te houden of hun onderwijs te actualiseren; daarvoor is het nodig dat zij zich verder kunnen ontwikkelen binnen het onderzoek of binnen het werkveld.

Het valt het panel op dat ook buiten de onderzoekstijd de urenbegroting van de opleiding krap is bemeten. Het panel heeft vernomen dat voor de gehele uitvoering van de opleiding 1,3 fte beschikbaar is; dat lijkt het panel aan de lage kant. Meer specifiek is voor begeleiding van een masterthese 20 uur beschikbaar. Het panel adviseert de opleiding de beschikbare uren te evalueren en waar nodig en mogelijk te verruimen.

*Conclusie: v*oldoet

### 4.5 Voorzieningen

*Standaard 7: De huisvesting en de materiële voorzieningen zijn toereikend voor de realisatie van het programma.*

*Bevindingen*
Het meeste onderwijs vindt plaats in het gebouw van de Haagse Security Delta. Deze locatie beschikt over verschillende multifunctionele leslokalen met presentatievoorzieningen, draadloos internet en voldoende aansluitingen voor laptops en tablets. Studenten kunnen gebruikmaken van werkplekken met PC en vergaderruimten. Het panel heeft een bezoek gebracht aan deze locatie en is van mening dat de voorzieningen goed zijn.

De studenten kunnen daarnaast gebruik maken van de faciliteiten van De Haagse Hogeschool. Dit betreft zowel de faciliteiten van de Academie voor Masters & Professional Courses als de centrale faciliteiten van het hoofdgebouw, waaronder de bibliotheek. Studenten kunnen desgewenst vanuit huis toegang krijgen tot de wetenschappelijk publicaties, zoekmachines en databases.

Hierboven is bij 4.2, Vormgeving van het onderwijs, ingegaan op lab-voorzieningen. De opleiding heeft een virtuele cloud-omgeving ingericht, die op afstand gebruikt kan worden door studenten vanaf de laptop of PC. Dit stelt de studenten in staat om alleen of in groepsverband security-gerelateerde experimenten uit te voeren.

*Overwegingen*
Het panel heeft een bezoek aan de locatie van de HSD gebracht en is van mening dat deze accommodatie beschikt over goede voorzieningen. Ook de studenten zijn tevreden over deze voorzieningen. De nabijheid van security-gerelateerde bedrijven zorgt voor een stimulerende omgeving. De bibliotheek van De Haagse Hogeschool voldoet aan de eisen. Voor opmerkingen over de inzet van het ICT-lab verwijzen we naar 4.2.

*Conclusie:* voldoet

### 4.6 Gerealiseerde eindkwalificaties

*Standaard 8: De studiebegeleiding en de informatievoorziening aan studenten bevorderen de studievoortgang en sluiten aan bij de behoefte van studenten.*

*Bevindingen*
De studiebegeleiding is afgestemd op werkende deeltijdstudenten. Al bij de intake wordt duidelijk gemaakt dat de studenten een balans moeten vinden tussen studie, werk en privé. De groepen zijn klein: het maximale aantal studenten is 25. De studenten leren elkaar snel kennen, onder andere door activiteiten tijdens de introductiedag. Informatie krijgen de studenten tijdens de intake en de introductiedag en daarna via Blackboard.

De studenten worden begeleid door een programmamanager. De programmamanager is tijdens de lesdagen beschikbaar en spreekt de studenten regelmatig over zaken als studiebelasting, studievoortgang en mogelijke belemmeringen. De programmamanager heeft toegang tot het online registratiesysteem Osiris. Hij kan dus de studieresultaten in de gaten houden en deze zo nodig deze bespreken tijdens met de studenten. Na ieder semester vinden er individuele voortgangsgesprekken plaats.

*Overwegingen*
Het panel is van mening dat de studiebegeleiding en de informatievoorziening afdoende zijn geregeld. De intake en introductiedag zorgen voor een goede start. Met maximaal 25 studenten zijn de groepen klein en de lijnen kort. De studenten met wie het panel gesproken heeft, waren tevreden over de begeleiding en de informele sfeer bij de opleiding.

*Conclusie: v*oldoet

### 4.7 Kwaliteitszorg

*Standaard 9: De opleiding kent een expliciete en breed gedragen kwaliteitszorg, bevordert de kwaliteitscultuur en is gericht op ontwikkeling.*

*Bevindingen*
De kwaliteitszorg van de opleiding is gebaseerd op de kwaliteitszorg van de Academie voor Masters & Professional Courses (de masteropleidingen van De Haagse Hogeschool). De kaders, richtlijnen en streefdoelen zijn vastgelegd in een kwaliteitshandboek, dat het panel heeft ingezien tijdens het locatiebezoek.

Binnen de opleiding worden alle modules na afloop geëvalueerd. Dat gaat aan de hand van anonieme digitale studentevaluaties met ongeveer twintig parameters. De resultaten van de evaluaties worden besproken door de docenten en de programmamanager. De kerndocenten komen regelmatig bijeen met de programmanager om de resultaten van de evaluaties te bespreken. Als de opleiding start, komt er ook een opleidingscommissie die toegang krijgt tot de resultaten van de evaluaties. Het programma wordt jaarlijks geëvalueerd door de studenten die het gehele programma hebben doorlopen.

Bij de lopende (executive) master Cyber Security worden de resultaten van de evaluaties besproken met de studenten in zogenoemde focusgesprekken. Die bieden de gelegenheid meer in detail op de bevindingen en de wensen van studenten in te gaan. Het is de intentie om ook in de nieuwe masteropleiding dergelijke gesprekken te gaan houden.

De betrokkenheid van de beroepspraktijk krijgt gestalte binnen de Adviescommissie, die actief betrokken is geweest bij het ontwikkelen van het curriculum. De commissie komt twee

maal per jaar bijeen om ervoor te zorgen dat de inhoud van het curriculum recht doet aan de ontwikkelingen op het gebied van cybersecurity. De Adviescommissie adviseert de programmamanager.

*Overwegingen*
Het panel is van mening dat de kwaliteitszorg bij de nieuwe masteropleiding CSE goed is geregeld. De kwaliteitszorg van de Academie voor Masters & Professional Courses legt een degelijke basis. Er is veel aandacht voor de rol van de studenten bij de evaluaties, het panel is positief over het voornemen om focusgesprekken te gaan voeren.

*Conclusie: v*oldoet

### 4.8 Toetsing

*Standaard 10: De opleiding beschikt over een adequaat systeem van toetsing.*

*Bevindingen*
De basis voor de toetsing wordt gevormd door het toetshandboek van de Academie voor Masters & Professional Courses. In dit toetshandboek zijn de visie, het beleid en de uitvoering van de toetsing binnen de opleidingen van de academie vastgelegd. Het panel heeft het toetshandboek ingezien en is van mening dat dit handboek aan de maat is. Voor de academie als geheel is een Toetsplan 2.0 in ontwikkeling. Dat gaat alle toetsen van een opleiding omvatten; die worden dus van te voren vastgesteld door de examencommissie.

De examencommissie is belast met het borgen van de kwaliteit van de toetsen en examens. Het panel heeft een gesprek met deze commissie gehad. De examencommissie is betrokken bij verzoeken tot vrijstellingen: het algemene beleid van de masteropleidingen is om geen vrijstellingen te verenen. Verder benoemt de examencommissie ook de examinatoren.

Voor iedere toets is een toetsmatrijs beschikbaar. Iedere toets wordt bekeken door ten minste één vakgenoot. De examencommissie wijst zowel de samensteller als de reviewer van de toetsen aan. De programmamanager controleert in hoeverre de toets overeenkomt met de leerdoelen en de lesinhoud. De academie beschikt ook over een toetscommissie; de examencommissie heeft de toetscommissie opdracht gegeven om twee keer per jaar een steekproef van ontwikkelde toetsen en beoordelingen te evalueren.

*Overwegingen*
De opleiding voldoet in de visie van het panel aan de formele voorwaarden voor toetsing. Het toetshandboek bevat een heldere visie en richtlijnen en de procedures zijn duidelijk en volledig. De toetsen voldoen aan het vierogenprincipe. De examencommissie en de toetscommissie vervullen hun taken naar behoren.

Het panel heeft wel een aantal kanttekeningen bij de samenstelling en de beschikbare tijd van deze commissies. Ten eerste stelt het panel vast dat er geen specifieke deskundigheid op het gebied van cybersecurity binnen de examencommissie aanwezig is. Het panel adviseert deze commissie aan te vullen zodat in deze lacune wordt voorzien. Daarnaast stelt het panel vast dat de tijd die de leden van de examencommissie en de toetscommissie voor hun werkzaamheden beschikbaar hebben, erg beperkt is. Dat geldt met name voor de

leden van de toetscommissie, die in 25 uur op jaarbasis vier opleidingen moeten beoordelen. De commissie adviseert met klem om deze urenbegroting te verruimen.

*Conclusie:* voldoet

### 4.9 Graad en CROHO-onderdeel

Het panel adviseert om de volgende graad aan de opleiding toe te kennen: Master of Science (MSc)
Het panel adviseert het volgende CROHO-onderdeel voor de opleiding: techniek

### 4.10 Algemene conclusie over de kwaliteit van de opleiding

In hoofdlijnen is het panel positief over de kwaliteit van de nieuwe hbo-masteropleiding CSE. Sterke punten zijn het beroepsgerichte karakter en de breedte van de opleiding. Het panel is van mening dat de Haagse Hogeschool een stevig programma heeft neergezet, dat goed aansluit bij ontwikkelingen in de markt. De combinatie van technische verdieping en verbreding met de nodige aandacht voor soft skills is een goede keuze. De docenten zijn sterk betrokken bij de opleiding en brengen voldoende deskundigheid in; de lectoren zorgen voor een koppeling met onderzoek. De belangrijkste verbeterpunten zijn een sterkere invulling van de ICT-labs, meer aandacht voor internationalisering, een transparanter systeem van leerlijnen en meer tijd voor een aantal wezenlijke activiteiten, zoals de begeleiding van de thesis en de werkzaamheden van de toetscommissie.

### 4.11 Aanbevelingen

1. Het panel is van mening dat het systeem van leerlijnen niet onderhoudbaar is. Het panel adviseert het aantal leerlijnen terug te brengen en het systeem transparanter te maken.
2. Het panel adviseert om een sterkere invulling aan de internationalisering te geven, vooral als het gaat om de inhoud van het onderwijs.
3. Het panel adviseert om beleid te ontwikkelen voor de wijze waarop de opleiding wil omgaan met kennisdisseminatie en de ambitie om studenten te laten publiceren, inclusief streefgetallen.
4. Het panel is van mening dat de opleiding ambitieuzer en innovatiever zou kunnen zijn bij de invulling en toepassing van de ICT-labs. Het panel adviseert de opleiding om de labs een grotere plaats in het curriculum te geven.
5. Het panel adviseert de opleiding om na telling van de literatuur goed te inventariseren of de studielast evenwichtig is verdeeld en zo nodig aanpassingen door te voeren.
6. Het panel adviseert de opleiding om de uren die beschikbaar zijn voor onderzoek te verruimen; voor een deel van de docenten is de beschikbare onderzoekstijd in die visie van het panel te beperkt. Daarnaast adviseert het panel ook het aantal uren dat beschikbaar is voor de begeleiding van de thesis (nu 20 uur) te verruimen.
7. Het panel stelt vast dat er geen specifieke deskundigheid op het gebied van cybersecurity binnen de examencommissie aanwezig is. Het panel adviseert deze commissie aan te vullen zodat in deze lacune wordt voorzien.

8. De tijd die de leden van de toetscommissie voor hun werkzaamheden beschikbaar hebben, is in de visie van het panel te beperkt. De commissie adviseert met klem om deze urenbegroting te verruimen.

# 5 Overzicht oordelen

| Standaard | Oordeel |
|---|---|
| **Beoogde leerresultaten**<br>*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 |
| **Programma – Oriëntatie**<br>*Standaard 2: Het programma maakt het mogelijk om passende (professionele of academische) onderzoeks- en beroepsvaardigheden te realiseren.* | Voldoet |
| **Programma – Inhoud**<br>*Standaard 3: De inhoud van het programma biedt studenten de mogelijkheid om de beoogde leerresultaten te bereiken* | Voldoet |
| **Programma – Leeromgeving**<br>*Standaard 4 : De vormgeving van het programma zet aan tot studeren en biedt studenten de mogelijkheid om de beoogde leerresultaten te bereiken.* | Voldoet |
| **Instroom**<br>*Standaard 5 : Het programma sluit aan bij de kwalificaties van de instromende studenten.* | Voldoet |
| **Personeel**<br>*Standaard 6 : Het docententeam is gekwalificeerd voor de inhoudelijke en onderwijskundige realisatie van het programma en de omvang ervan is toereikend* | Voldoet |
| **Voorzieningen**<br>*Standaard 7 : De huisvesting en de materiële voorzieningen zijn toereikend voor de realisatie van het programma.* | Voldoet |
| **Gerealiseerde eindkwalificaties**<br>*Standaard 8 : De studiebegeleiding en de informatievoorziening aan studenten bevorderen de studievoortgang en sluiten aan bij de behoefte van studenten.* | Voldoet |
| **Kwalitietszorg**<br>*Standaard 9 : De opleiding kent een expliciete en breed gedragen kwaliteitszorg, bevordert de kwaliteitscultuur en is gericht op ontwikkeling.* | Voldoet |
| **Toetsing**<br>*Standaard 10 : De opleiding beschikt over een adequaat systeem van toetsing.* | Voldoet |
| | |
| **Algemene conclusie** | **Positief** |

# Bijlage 1: Samenstelling panel

- Prof.dr.ir. B (Bart) Preneel, hoogleraar Computerbeveiliging en Industriële Cryptografie aan de KU Leuven (voorzitter);
- Ir. C.J. (Kees) Rijsenbrij (panellid); hogeschool hoofdocent en opleidingsmanager HBO-ICT bij de Hogeschool van Amsterdam;
- M. (Michael) Pols (panellid), Security Officer bij The Future Group;
- K. (Kevin) Voorn (student-panellid), student HBO-ICT aan de Hanzehogeschool Groningen.

**Prof.dr.ir. B. Preneel**
Bart Preneel is professor en hoofd van de onderzoeksgroep COSIC bij KU Leuven. Zijn voornaamste onderzoek gaat over cryptografie, informatieveiligheid en privacy. Preneel verzorgt in zijn hoedanigheid als professor colleges bij de KU Leuven over cryptografie, netwerkveiligheid en algebra. Daarnaast is hij visiting professor geweest bij de technische universiteit Denemarken, Ruhr Universiteit Bochum, Technische Universiteit Graz, Universiteit Bergen en Universiteit Gent. Preneel heeft ervaring als panelvoorzitter bij een Toets Nieuwe Opleiding Cyber Security.

**Ir. C.J. Rijsenbrij**
Kees Rijsenbrij is van 2002 tot 2017 opleidingsmanager van de informatica-opleidingen van de Hogeschool van Amsterdam geweest en sindsdien Hogeschool-hoofddocent. Als opleidingsmanager is hij verantwoordelijk geweest en nauw betrokken bij het ontwikkelen van onderwijs binnen de informatica-opleidingen van de HvA. Hij neemt deel aan structurele samenwerkingsverbanden binnen en buiten Europa. Hij gaat geregeld op uitwisseling bij collega-universiteiten in het buitenland. Hij heeft de afgelopen jaren deelgenomen aan verschillende visitatiecommissies voor Informatica en HBO-ICT-opleidingen in Nederland.

**M. Pols**
Michael Pols is zelfstandige bij The Future Group en werkt van daaruit als senior informatieconsultant bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Hij is daarnaast docent Data Privacy Officer Foundation Track bij de Hogeschool van Arnhem en Nijmegen.

**K. Voorn, (student-lid)**
Kevin Voorn maakt deel uit van de NVAO-pool van student-leden. Hij studeert aan de opleiding HBO-ICT van de Hanzehogeschool Groningen met als specialisatie Network & Security Engineering.

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

Het panel werd bijgestaan door Ed Lansink, beleidsmedewerker NVAO, procescoördinator en Erik van der Spek, directeur Hendrikx Van der Spek, secretaris.

## Bijlage 2: Programma locatiebezoek

Het panel heeft een bezoek gebracht aan de Cyber Security Academy op 7 februari 2018.

**Locatie**: Cyber Security Academy, HSD Campus, Wilhelmina van Pruisenweg 104 in Den Haag.

**Programma**:

| Tijd | Onderwerp | Aanwezigen |
|---|---|---|
| 08:30 – 08:45 | **Ontvangst & Kennismaking** | |
| 08:45 – 09:15 | **Intern vooroverleg panel** | |
| 09:15 – 10:30 | **Oriëntatie & doelgroep Presentatie van Cyber Security Academy en M&PC** | • Dhr. prof. dr. ir. J. van den Berg (Jan), Wetenschappelijk Directeur CSA<br>• Dhr. drs. C.M.B. Berendsen (Clemens), Faculteitsdirecteur Academie voor Masters & Professional Courses<br>• Dhr. dr. M.E.M. Spruit (Marcel), Kerndocent<br>• Dhr. Ir. J.C. Wessels (Jan), ISO bij Rabobank<br>• Mw. J. Conquet, (Jessica), Global CISO bij PayU en voorzitter PvIB |
| 10:45 – 11:30 | **Borging eindniveau** | • Dhr. dr. S.H. Beltman (Schelte), Kerndocent Thesis<br>• Dhr. J. den Ouden (Jordi), MBA Voorzitter toetscommissie<br>• Dhr. drs. M.G.M. Geerdink (Michaël), Examencommissie |
| 11.45 – 12.30 | **Onderwijsleeromgeving** | • Dhr. dr. M.E.M. Spruit (Marcel), Kerndocent<br>• Mw. drs. M. Konings (Maaike), Onderwijskundig adviseur<br>• Dhr. dr. ir. P. Burghouwt (Pieter), Kerndocent |
| 12.30 – 13.30 | **Lunch** | |
| 13.30 – 14.15 | **Sessie 4: Presentatie lab** | • Dhr. dr. ir. P. Burghouwt (Pieter), Kerndocent<br>• Dhr. ir. G.A. Mijnarends (Gerard), Kerndocent |
| 14.30 – 15.00 | **Gesprek met studenten** | • Dhr. mr. ir. drs. APM Pols (Paul), student<br>• Dhr. ir. M.J.G. Dirksen (Mark), |

| | | |
|---|---|---|
| | | student<br>• Dhr. R.A.J. Pauwels (Rob), student |
| 15.15 – 16.00 | **Docenten en begeleiding, Organisatie en kwaliteit** | • Dhr. R.F. Visser (René) Kerndocent<br>• Dhr. dr.ir. M. Maris (Marinus) Kerndocent<br>• Mw. Dr. E.K. Cortez (Elif), docent<br>• Mr. drs. mr. ir. M. Meuleman (Marcel), Programme director Finance & Risk<br>• Mw. Drs. M. Cruq (Mariola) Projectleider |
| 16.00 – 17.00 | **Intern paneloverleg** | |
| 17.00 – 17.30 | **Terugkoppeling door de panelvoorzitter** | |

# Bijlage 3: Overzicht van bestudeerde documenten

*Informatiedossier opleiding/instelling*
- Informatiedossier Masteropleiding Cyber Security Engineering (CSE)
- Bijlagen

*Documenten beschikbaar gesteld tijdens locatiebezoek*

**Algemene documenten M&PC**
- Meerjarenbeleidsplan 2017-2022
- Visie op Masteronderwijs
- Jaarplan 2018
- Jaarverslag Masters Examencommissie 2016-2017
- Onderwijsvisie- en kader
- Toetsing in de Masteropleidingen
- Ontwikkelen van onderzoekend vermogen in de masteropleidingen
- Master Thesis Manual
- Handboek kwaliteitszorg
- Professionaliseringsplan 2017

**Achtergrondinformatie MCSE**
- Beroepsprofielen Informatiebeveiliging 2.0 (PViB, 2017)
- Onderzoek naar kwalificatie en certificatie van informatiebeveiligers (Spruit & Noord, 2011)
- Behoefte vanuit de arbeidsmarkt aan cyber security opleidingen (PBLQ, HEC, 2012)
- Arbeidsmarkt voor Cyber Security Professionals (PLATO, 2014)
- Presentie Arbeidsmarkt voor Cyber Security Professionals (PLATO, april 2015)
- Inspiratiesessie 'Cybersecurity in het onderwijs' (PLATO BV en Ockham IPS, 2015)
- Economische kansen Nederlandse Cybersecurity (Verdonck, Klooster & Associates, 2016)
- Verslagen overleggen werkveld en curriculumcommissie (2016-2017)

**Opleidingsinformatie MCSE**
- Studiehandleidingen
- Master Thesis Manual
- Onderzoekslijn in de Master Cyber Security Engineering
- Toetsmatrijzen
- Intakeprocedure
- CV's kerndocenten
- Docentenoverzicht per module
- Opleidingskader

*Overige documenten*
- Toegang tot de digitale leeromgeving (Blackboard)
- Toegang tot de digitale literatuur via de bibliotheek van de Haagse Hogeschool

## Bijlage 4: Lijst met afkortingen

| | |
|---|---|
| ba | bachelor |
| BKO | Basiskwalificatie Onderwijs |
| CSE | Cyber Security Engineering |
| CSA | Cyber Security Academy |
| EC | European Credits (studiepunten) |
| hbo | hoger beroepsonderwijs |
| HCTL | The Hague centre for teaching and learning |
| HSD | Haagse Security Delta |
| ICT | Informatie- en Communicatietechnologie |
| ma | master |
| NVAO | Nederlands-Vlaamse Accreditatieorganisatie |
| PKI | Public Key Infrastructure |
| PvIB | Platform voor Informatiebeveiligers |
| wo | wetenschappelijk onderwijs |

Het adviesrapport is tot stand gekomen in opdracht van de NVAO met het oog op de uitbreide toetsing van de nieuwe hbo-masteropleiding Cyber Security Engineering van De Haagse Hogeschool.

Nederlands-Vlaamse Accreditatieorganisatie (NVAO)
Parkstraat 28
Postbus 85498 | 2508 CD DEN HAAG
T 31 70 312 23 00
E info@nvao.net
W www.nvao.net

Aanvraagnummer 006061