Hogeschool van Amsterdam

Administratieve gegevens opleiding

Basisgegevens

Naam instelling	Hogeschool van Amsterdam
Contactgegevens	Postbus 1025 1000 BA Amsterdam
Faculteit	Faculteit Digitale Media en Creatieve Industrie (FDMCI)
Naam opleiding	Master of Science Cyber Security
Titel	MSc
Voertaal	Nederlandstalig
Opleidingsniveau	Master
Inhoud	De masteropleiding Cyber Security leidt professionals op die, vanuit een stevige basis in de ICT, kennis hebben van en ervaring hebben met het cybersecurityproces. De inhoud van de beoogde master wordt naar de indeling van Spruit en Van Noord[1] het best aangemerkt als een opleiding tot technisch dominante specialistische cybersecurity functies, met een overlap naar de specialistische tactisch-strategische cybersecurity functies [2]. De masterstudenten onderzoeken op tactisch en strategisch niveau: - Welke ICT-assets er ingezet dan wel beschermd moeten worden binnen de context van een organisatie. - Welke risico's, bedreigingen en kwetsbaarheden er te vinden zijn bij een organisatie. - Welke maatregelen genomen moeten worden om kwetsbaarheden en risico's aan te tonen, te verhelpen - Welke maatregelen genomen moeten worden om kwetsbaarheden en risico's te vermijden, te mitigeren of anders tegemoet te treden - Hoe zij de opdrachtgever op passende wijze kunnen informeren en adviseren met betrekking tot bovenstaande. Zij doen dit onderzoek systematisch en methodisch in lijn met de visie en het beleid van de organisatie. Zij zijn tevens in staat om een visie en beleid ten aanzien van security voor de organisatie te ontwikkelen. Tijdens de masteropleiding ontwikkelt de masterstudent Cyber Security zich in de complexe beroepsuitoefening, multidisciplinair werken, coördinatie en besturing ten behoeve van innovatie van de ICT-professie en in het functioneren op strategisch niveau. Bij de ontwikkeling van de professionele vaardigheden liggen de accenten op het niveau van coördinatie, innovatie en specialisatie. De leeruitkomsten beschrijven de inhoud, het gedrag en de attitude vanuit het perspectief van de Master of Science Cyber Security bij het toepassen van professionele en technische vaardigheden om oplossingen te creëren voor praktijkgerichte, situationele problemen op het gebied van cybersecurity, binnen een complexe context.

[1] Beroepsprofielen Informatiebeveiliging 2.0. Een basis voor uniforme kwalificatie van informatiebeveiligers, M. Spruit en F. van Noord. 2017 (Bijlage 1)

[2] Arbeidsmarkt Cyber Security professionals, Plato, 2014, blz. 29-30 (Bijlage 2)

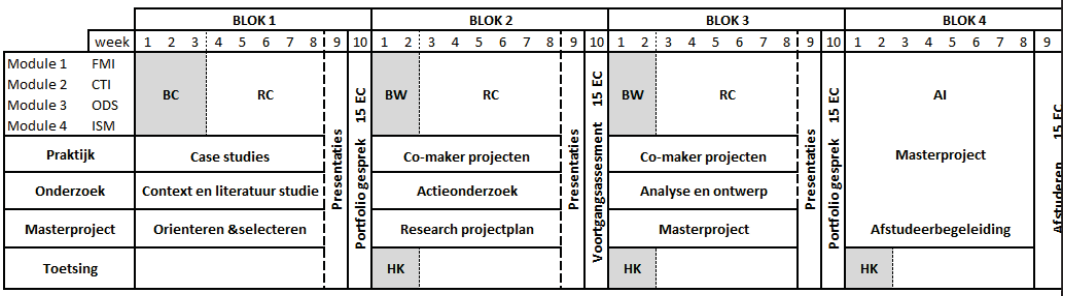
	In deze professionele masteropleiding[3] verwerven studenten kennis en ontwikkelen ze vaardigheden op masterniveau (EQF 7)[4] die verwoord zijn in de volgende leeruitkomsten: 1. ***Architectuur:*** De MSc Cyber Security analyseert, in nauwe communicatie met belanghebbenden, de feitelijke situatie en vereisten, adviseert opdrachtgevers over mogelijke benaderingen en ontwikkelt iteratief een architectuur van veilige (*enterprise*) informatie-infrastructuren op basis van geaccepteerde en verantwoordbare principes. 2. ***Methoden en technieken:*** Samenwerkend met de opdrachtgever ontwerpt, ontwikkelt, implementeert en documenteert de MSc Cyber Security informatie-infrastructuren en adviezen daaromtrent die zijn gefundeerd op de principes van *cyber threat intelligence*, offensieve en defensieve technieken, en forensische en analytische methoden, die passen in de architectuur en information security management. 3. ***Actieonderzoek:*** De MSc Cyber Security onderzoekt vraagstellingen en oplossingsrichtingen volgens de technieken van op basis van gericht literatuur- en situationeel onderzoek via een verantwoordbaar onderzoeksontwerp, gegevensinwinning, analyse en advies. 4. ***Professionele vaardigheden:*** De MSc Cyber Security werkt en managet onderzoekend en probleemoplossend in een complexe multidisciplinaire en specialistische context met interacterende factoren en innovatieve, breed toepasbare toekomstgerichte concepten op basis van persoonlijk leiderschap en doelgerichte interactie. De leeruitkomsten zijn consistent met de HBO-I domeinbeschrijving (2018)[5] voor een professional masterprogramma met een verdieping op niveau vier. Op dit hoogste niveau van beheersing worden de activiteiten Analyse en Advies gerealiseerd in de architectuurvlakken Infrastructuur, Software en Bedrijfsprocessen (leeruitkomsten 1,2) en in het architectuurvlak Infrastructuur zijn dat de activiteiten Ontwerp en Management (Leeruitkomsten 3,4).
Inrichting van de opleiding	Het masterprogramma bestaat uit een intensief eenjarig voltijdprogramma met 4 blokperiodes van 10 weken en omvat totaal 60 EC. Het programma heeft 4 programmalijnen: de kennislijn, de praktijklijn, de onderzoekslijn en het masterproject waarop de student afstudeert. De kennislijn is ingericht met de vier hieronder genoemde inhoudelijke modulen; de praktijklijn met actuele projecten op basis van praktijkopdrachten vanuit het bedrijfsleven of het lectoraat; de onderzoekslijn omvat de onderzoekscomponenten die relevant zijn voor het vakgebied en ondersteunt tevens de projecten en het masterproject. De vierde programmalijn wordt gevormd door het masterproject.

[3] Conform De professionele masterstandaard van de Vereniging Hogescholen, juni 2019 (Bijlage 3)

[4] Toelichting EQF/NLQF 7: De professionele masterstandaard van de Vereniging Hogescholen, juni 2019, blz 12 tot tn met 15

[5] HBO-I domeinbeschrijving 2018 (Bijlage 4)

Hogeschool van Amsterdam

	De inhoud van de masteropleiding Master of Science Cyber Security van de HvA richt zich op vier kennisdomeinen: - **Forensics & Malware Investigation (FMI)**, waarin Cyber Forensics, Operating Systems Forensics, Mobile Device Forensics, Malicious Software Analysis, Malware Analysis, Malicious Documents and Memory Forensics, en Big-Data Forensics behandeld worden. - **Cyber Threat Intelligence (CTI**) waarin Cyber Threat Modelling, Intrusion analysis, Threat identification, Threat Data Detectie, Threat Intelligence Sources, Threat Data Structuring, Threat Collection Analyse, Cyber Threat Intelligence en Cyber Threat Campaigns en Reporting aan bod komen. - **Offensive & Defensive Security (ODS)** waarin onder andere Scanning and Exploitation, Vulnerability Detection and Exploit Development en Countermeasures worden behandeld. - **Information Security Management (ISM)** waarin Governance, Wet- en regelgeving, Compliance, Secure Design, Change Management, Information Security Incident Management and Response en Business Continuity Planning and Disaster Recovery behandeld worden.  ***Afkortingen: BC = bootcamp; RC = responsiecolleges; BW = boosterweken; AI = afstudeerintervisie; HK = herkansingsperiode*** Tijdens het masterprogramma werken de studenten de eerste drie blokken in projectteams aan een actuele en complexe cybersecurity-opdracht voor bedrijven en/of een lectoraat. Kenmerkend voor het werken in het vakgebied cybersecurity is het werken met vertrouwelijke informatie, kritieke systemen en infrastructuren. In het gehele onderwijsprogramma komen ethiek en integriteit aan de orde onder de noemers: the Relationship to Ethical Concerns; Governance; Privacy; Wet- en regelgeving en Compliance, naast risicomanagement en de invloed van menselijke factoren.
Studielast	60 EC (à 28 SBU)
Vorm van de opleiding	Voltijdmaster
Vestigingsplaats	Amsterdam
Geplande startdatum	September 2020
Doelgroep van de opleiding	Potentiële masterstudenten hebben een BSc-diploma Informatica/BSc-diploma HBO-ICT
Beoogde instroom	Jaarlijkse start in september. Instroom opbouwend: cohort 2020: 25 studenten; cohort 2021: 25 studenten; vanaf 2022: 50 studenten.
Croho (sub)onderdeel en motivering	Techniek, dit is een onderdeel van de doorlopende leerlijn cybersecurity, AD, BA en MA