

Datum

13 maart 2024

Dossiernummers

DL484-24

Referentie

DLR Bachelor in de cybersecurity

DOMEINSPECIFIEK LEERRESULTATENKADER

Kwalificatie	:	Bachelor in de cybersecurity
Datum validatie	:	13 maart 2024
Studiegebied	:	Industriële wetenschappen en technologie (ISCED: 06 Information and Communication Technologies ICTs)
Niveau	:	
o Vlaamse Kwalificatiestructuur		6
o Codex Hoger Onderwijs		Profesionele bachelor
o Europese Hoger Onderwijs Ruimte (Dublin-descriptoren)		1 ^{ste} cyclus
o Europees Kwalificatiekader voor een Leven Lang Leren		6

Domeinspecifieke leerresultaten van de opleiding:

1. De bachelor in de cybersecurity analyseert de kritische bedrijfsprocessen, -data en -infrastructuur en doet een wezenlijke bijdrage tot cybersecurity by design en data protection by design door de identificatie, evaluatie en inperking van risico's en bedreigingen wat leidt tot een informatiebeveiligingsbeleid op, met inbegrip van strategische doelen, procedures, richtlijnen en policies.
2. De bachelor in de cybersecurity verzamelt, analyseert, structureert en deelt inzetbare informatie over threat intelligence die het gedrag, de motieven en het vermogen van cybercriminelen omvat, met inbegrip van phishing en ransomware.
3. De bachelor in de cybersecurity evalueert en verbetert in het volledige gamma van software, firmware en hardware technologieën de cybersecurity van (sub)systemen door opsporen, analyseren en afhandelen van bestaande aanvalsvectoren en kwetsbaarheden, dit door het inzetten van bestaande defensieve en offensieve beveiligingssoftware, inclusief het ontwikkelen van eigen scripts, penetration testing, reductie van de eigen digitale voetafdruk en participeren in red teaming oefeningen.
4. De bachelor in de cybersecurity selecteert en configureert de optimale technieken, met inbegrip van identificatie, authenticatie en autorisatie, en past deze toe binnen de gangbare omgevingen, inclusief fysieke en industriële omgevingen, voor elke fase van het cyberbeveiligingsproces

5. De bachelor in de cybersecurity draagt bij tot structureren en optimaliseren van een secure development life cycle waarbij elke fase afdoende wordt beschermd door een gepaste combinatie van technische en organisatorische maatregelen, toegespitst op specifieke vereisten binnen relevante domeinen.
6. De bachelor in de cybersecurity versterkt cybersecurity awareness, ondersteunt de nodige veranderingsprocessen en levert organisatiegericht advies op het vlak van architectuur en onderhoud van de beveiliging van data- en bedrijfsprocessen.
7. De bachelor in de cybersecurity realiseert preventie, detectie, respons, herstel en opsporing van cyberdreigingen en -aanvallen door keuze, toepassing en interpretatie van de geschikte technieken.
8. De bachelor in de cybersecurity communiceert, rapporteert en overlegt, minstens in het Nederlands en het Engels, op een professionele manier en aangepast aan het doelpubliek over cybersecurity incidenten en actieplannen met verschillende stakeholders.
9. De bachelor in de cybersecurity handelt met een ethische verantwoordelijkheid in de domeinen van cybersecurity, intelligence, data protection, cyber crime, forensische opsporing en cyber warfare, rekening houdend met het wettelijk en deontologisch kader en met impact op personen, organisaties en maatschappij.
10. De bachelor in de cybersecurity initieert, implementeert, onderbouwt, documenteert cybersecurity projecten op maat van de organisatie, werkt hierbij teamgericht in een multidisciplinaire context, stelt de juiste prioriteiten en toont een goed timemanagement, probleemoplossend vermogen en zelfkritische ingesteldheid.
11. De bachelor in de cybersecurity stuurt de eigen professionele ontwikkeling vanuit de opvolging en raadpleging van relevante bronnen en vanuit praktijkgericht onderzoek naar (inter)nationale ontwikkelingen in de cybersecurity en de domeinen die dit beïnvloeden met het oog op levenslang leren.

Basis :

- Gelet op artikel 16, 17 en 18 van het decreet van 30/04/2009 betreffende de kwalificatiestructuur;
- Gelet op artikel II.68 van de Codex Hoger Onderwijs gecodificeerd op 11/10/2013;
- Gelet op het reglement van de Nederlands-Vlaamse Accreditatieorganisatie van 01/02/2011 betreffende de validatie van de gezamenlijke domeinspecifieke leerresultaten van hogeronderwijsopleidingen in de Vlaamse Gemeenschap;
- Gelet op de VLIR/VLHORA-handleiding 2012 betreffende het uitschrijven van domeinspecifieke leerresultatenkaders.