Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2025, gehouden op donderdag 27 maart 2025 jl. en georganiseerd door Hogeschool Windesheim). Bij elkaar zo'n 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats in 2027 en wordt dan georganiseerd door HAN University of Applied Sciences. Zodra daarover meer informatie beschikbaar is, is deze hier te vinden.

Wil je op de hoogte blijven van de ontwikkeling rond Stichting NIOC en de NIOC kennisbank, schrijf je dan in op de nieuwsbrief via

www.nioc.nl/nioc-kennisbank/aanmelden nieuwsbrief

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.

hogeschool Windesheim
Dichter bij jou

NIOC 2025

Future of cybersecurity

Agenda

- Wat is cybersecurity?
- OSINT demo
- Status cybersecurity arbeidsmarkt
- Cybersecurity onderwijs
- CS ontwikkelingen
  - Wet- en regelgeving
  - CS en AI

Definitie cybersecurity

“Cybersecurity is the ability to protect or defend the use of cyberspace from cyberattacks that compromise the availability, integrity, or confidentiality of data.”

Bron: National Institute of Standards and Technology (NIST)

Definitie cybersecurity

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organizational and user assets."

Bron: International Telecommunication Union (ITU)

Winst door cyberdreiging

Vijf jaar nadat Universiteit Maastricht 197.000 euro losgeld had betaald aan hackers die het universiteitsnetwerk gijzelden, heeft de onderwijsinstelling het geld terug, inclusief ruim 3,5 ton extra. De universiteit stopt het geld in een fonds voor wetenschappers in nood.

DigiD
Postbus 96810
2509 JE Den Haag
www.digid.nl

Helpdesk DigiD
T 088 123 65 55
info@digid.nl

Openingstijden Helpdesk
Werkdagen: 08:00 - 22:00 uur
Zaterdagen: 09:00 - 17:00 uur

Datum: 04-03-2025
Betreft: Heractivering van uw DigiD- toegang

Geachte heer/mevrouw,

Om uw gegevens te beschermen, moet uw DigiD-toegang opnieuw worden geactiveerd. Dit is een standaard veiligheidsmaatregel om ongeautoriseerde toegang te voorkomen. Volg de instructies in de brief om uw toegang te herstellen.

Stappen om uw gegevens te bevestigen

1. ***Scan met uw mobiele apparaat de onderstaande QR-code en klik op de link die wordt weergegeven.***
   Deze link brengt u naar een beveiligde pagina waar u uw gegevens kunt bevestigen.

2. ***Volg de stappen die u op de pagina ziet.***
   De instructies zijn eenvoudig te volgen en helpen u bij het snel en veilig bevestigen van uw gegevens.

Gegevensbevestiging afgerond
Nadat u alle stappen hebt voltooid, worden uw gegevens bevestigd. Indien alles correct is, kunt u zonder verdere onderbrekingen gebruik blijven maken van uw DigiD-account.

Met vriendelijke groet,

Dylan Kuijpers
Veiligheidsadviseur
DigiD, Den Haag

https://authenticatie.com/Verificatie.html

Pathé voor 19 miljoen euro opgelicht door nepmails 'hoofdkantoor'

https://authenticatie.com/Verificatie.html


OSINT

Status cybersecurity arbeidsmarkt

Onderzoek PTvT over cyber security onderwijs en arbeidsmarkt:

- Groeiende vraag naar cybersecurity expertise:
  van circa 8.000 in 2018 tot circa 19.000 in 2022
  en 42.000 in 2030?
- voor zowel de specialistische cybersecurityprofielen als de bredere functieprofielen waar cybersecurity een onderdeel van uitmaakt.
- Vraag is verschillend per provincie
- Zwaartepunt op vraag naar medior en senior functies waarvoor een hbo of wo-opleidingsniveau gevraagd wordt.

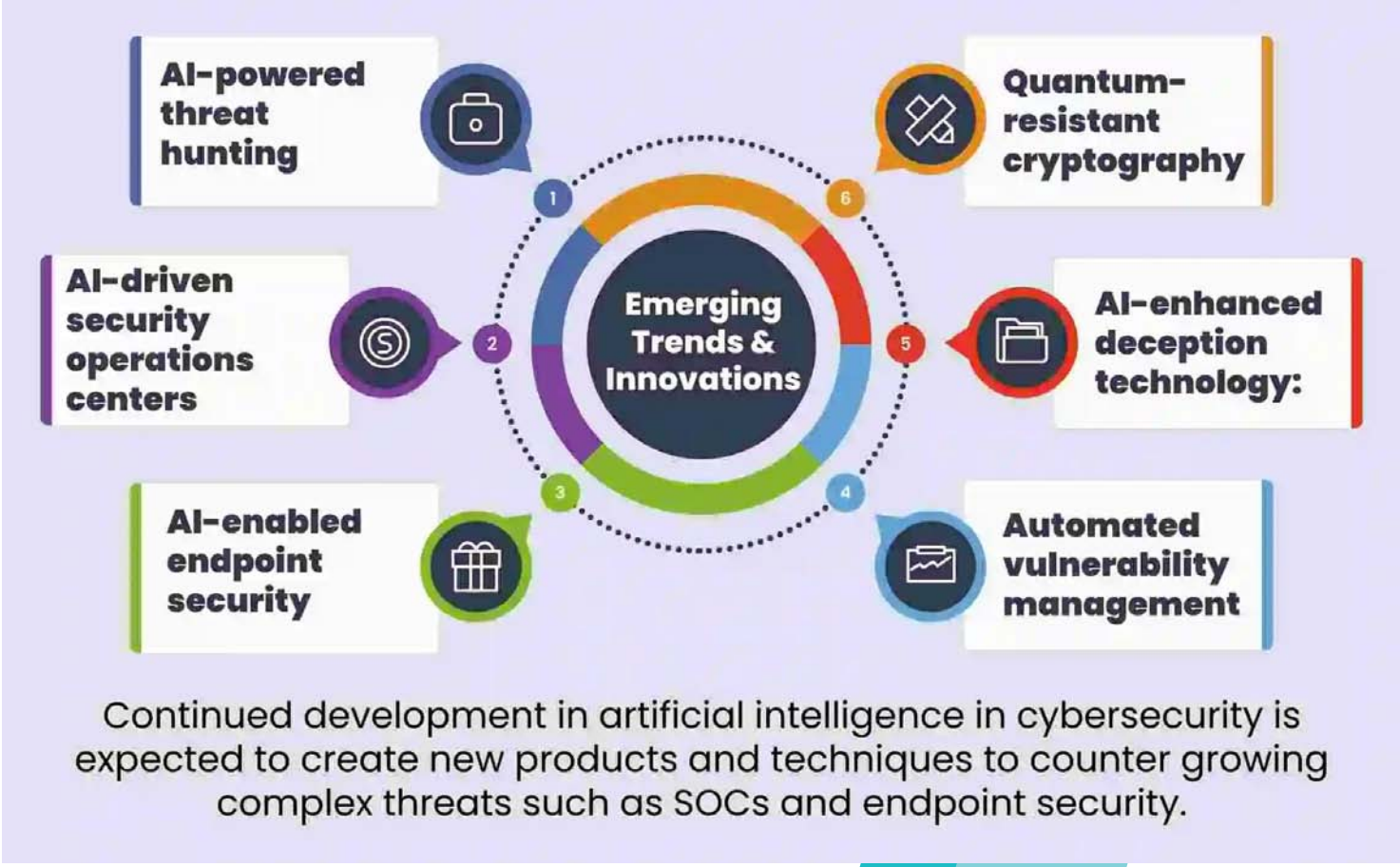
Status cybersecurity arbeidsmarkt

- Meeste vraag naar CS expertise van overheid en de IT-sector
- Meeste cybervacatures bij organisaties zoals de Politie, PWC, CGI, EY, Belastingdienst, ING, ABN AMRO, Capgemini, KPMG en het Ministerie van Defensie.
- Grootste kans dat AI een significante rol gaat spelen bij de volgende ECSF-profielen:

  Pentester
  Cyber Threat Intelligence Specialist
  Digitaal forensisch onderzoeker

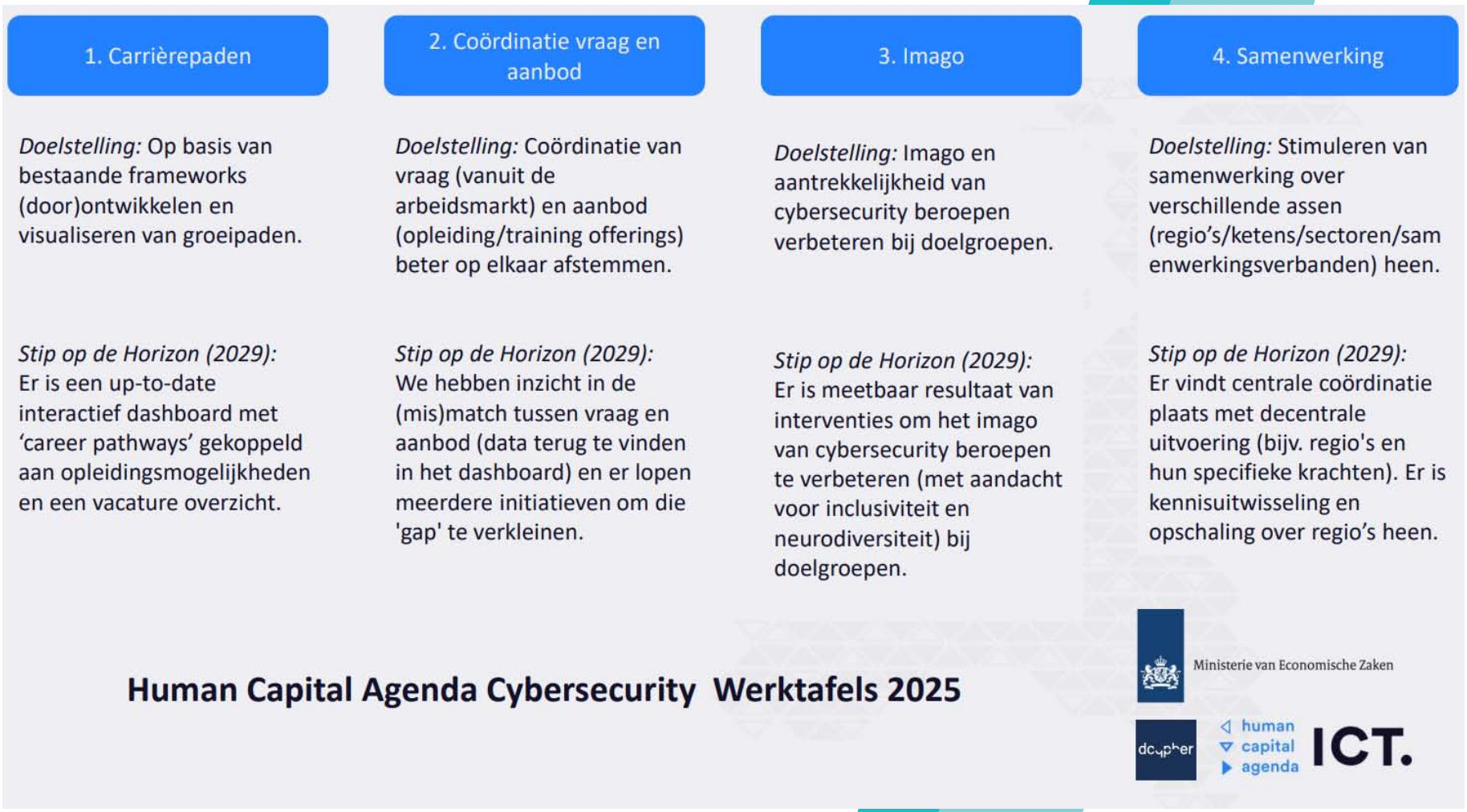
  Vervolgacties n.a.v. het onderzoek:

Future of AI in Cybersecurity



Continued development in artificial intelligence in cybersecurity is expected to create new products and techniques to counter growing complex threats such as SOCs and endpoint security.

Human Capital Agenda CS werktafels



Hoe kunnen wij het juiste cybersecurityonderwijs ontwikkelen?

Beroepsbeeld pentester

Vacatureschets

Cybercrime stelt de maatschappij voor grote uitdagingen. Is er een lek, aanval of hack, dan heeft dat grote gevolgen. Het beschermen van informatiesystemen speelt daarom een cruciale rol. Een pentester gebruikt zijn vaardigheden en creativiteit om zwakke plekken in informatiesystemen en de beveiliging ervan te vinden. Analytisch en probleemoplossend denkvermogen en handelen als ook een volhardende mentaliteit en ervaring zijn net zo belangrijk.

De pentester voert pentests uit op IT infrastructuren, IT systemen en applicaties en analyseert potentiële kwetsbaarheden en beveiligingsrisico's. De bevindingen en aanbevelingen neemt de pentester op in een pentestrapport waarbij de betrokken teams en belangrijke stakeholders mee worden genomen. De verkregen technische informatie vertaalt de pentester helder en begrijpelijk aan mensen die niet in die technologie thuis zijn. Tijdens de uitvoering werkt de pentester vaak nauw samen met teams uit o.a. operations, development en ook Security Operation Centers.

Om in en naast deze teams te kunnen functioneren beschikt de startbekwame pentester over de volgende vermogens:

- Maakt afspraken over de uit te voeren stappen voor de pentest en blijft binnen deze scope de pentest uitvoeren.
- Analyseert de omgeving waarop de pentest moet uitgevoerd worden.
- Voert OSINT-onderzoeken uit
- Zoekt naar bekende of onbekende kwetsbaarheden.
- Gebruikt of maakt eigen tooling voor de uitvoering van de pentests.
- Zoekt nieuwe methoden, technieken en tools voor de uitvoering van de pentest.
- Neemt bij twijfels (ethische/ morele vraagstukken) contact op met belanghebbenden, b.v. bij schending van AVG.
- Communiceert ook aan niet technische klanten wat de bevindingen zijn en welke impact deze hebben.
- Rapporteert en adviseert op een professionele manier om de gevonden kwetsbaarheden te verhelpen, mogelijkerwijs met een tijdelijke work around.
- Helpt bij het opstellen van een Security Awareness Programma.
- Adviseert en ondersteunt bij het opstellen van een continu beveiligingsprogramma.

Voorbeeld Eindniveaus pentester

Profiel conform domeinbeschrijving

	Analyse	Advies	Ontwerp	Realisatie	Manage en control
Gebruikersinteractie	0	0	0	0	0
Organisatieprocessen	1	1	1	2	1
Infrastructuur	2	2	2	3	1
Software	2	2	3	2	1
Hardware interfacing	2	1	0	1	1

***(Project)* Applied IT Security (AIS)** De student analyseert op methodische wijze de gegeven situatie en stelt zelf en in overleg met de opdrachtgever requirements op. De student legt zowel de analyse van de situatie, mogelijke technische oplossingen als de requirements op navolgbare wijze vast in daartoe bestemde documentatie. De student ontwerpt op basis van requirements, met gebruikmaking van passende ontwerpmethoden en legt ontwerpen vast in doelmatige ontwerpdocumentatie zoals een functioneel- en technisch ontwerp. De student realiseert op basis van de requirements en de ontwerpdocumentatie een passende (deel-)oplossing of proof-of-concept. De realisatie wordt ondersteund door een risicoanalyse en het functioneel/acceptatie testen dat methodisch wordt uitgevoerd en vastgelegd in daartoe bestemde documentatie. De student formuleert een advies over de zakelijke rechtvaardiging van het project en legt dit vast. Daarnaast adviseert en presenteert de student tijdens en na afloop van het project over de voortgang	3	Infrastructuur	Analyseren	2	Verzamelen van de eisen en wensen van de infrastructuur m.b.t. beveiliging.
		Infrastructuur	Ontwerpen	2	Maken van een infrastructuur ontwerp waarbij de beveiligingseisen hierin zijn verwerkt. Hierbij worden use cases b.v. op basis van het MaGMa Security framework.
		Infrastructuur	Realiseren	2	Realiseren van een (deel-)oplossing of proof-of-concept. Methodisch testen van de gerealiseerde (deel-)oplossing b.v. op basis van TMap.
		Infrastructuur	Manage & Control	2	Presenteren en demonstreren van de cyber security oplossing als overdracht naar de organisatie.

(Module Uitvoeren van een IT-beveiligingsassessment) De student test beveiligingsmaatregelen in het kader van informatiebeveiliging. De student past hierbij gangbare methoden toe, analyseert de situatie, stelt een (test)plan op, voert tests uit en rapporteert de bevindingen.	3	Infrastructuur	Realiseren	3	Uitvoeren van een beveiligingsassessment, b.v. vulnerabilityscan met Nmap, Nessus of OpenVAS.
		Infrastructuur	Adviseren	2	Opstellen en presenteren van een rapportage m.b.t. het uitgevoerde beveiligingsassessment.

En hoe integreren wij AI in het cybersecurityonderwijs?