WELKOM!

CYBERSECURITY
FUNDAMENTALS

Module 1 - Wat is cybersecurity en cybercrime?

KICK-OFF

Datum: 02-02-2026

avans hogeschool

AGENDA INTRODUCTIEBIJEENKOMST

- Het module team
- De keuzemodule in vogelvlucht
- Programma van vandaag
  - Introductie
  - Elkaar leren kennen: OSINT-opdracht
  - Gastcollege

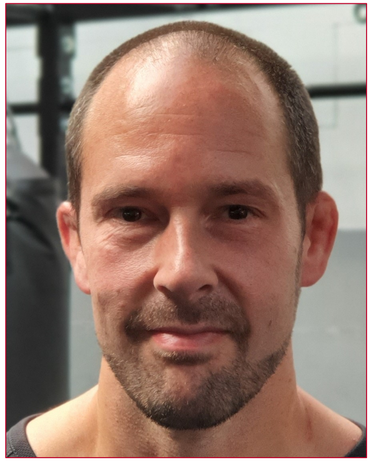
VOORSTELRONDJE DOCENTENTEAM

Maurice Snoeren

Ronald van Tienen

Ted Smets

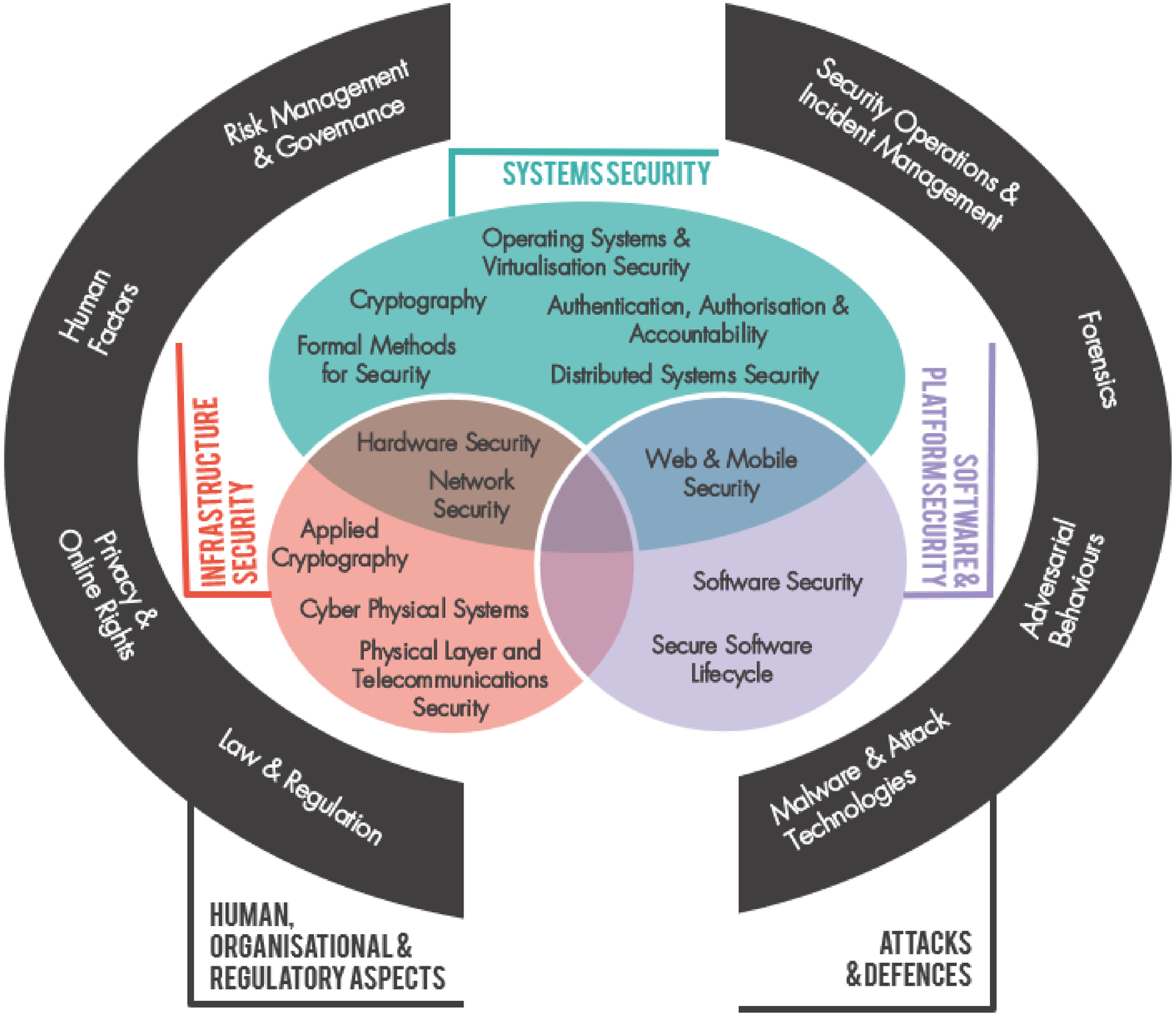
Ruud Hermans



Marcel de Groot

DE KEUZEMODULE IN VOGELVLUCHT

CYBOK


Risk Management & Governance
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
Law & Regulation
Privacy & Online Rights
Human Factors
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
SOFTWARE & PLATFORM SECURITY
Web & Mobile Security
Software Security
Secure Software Lifecycle
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
ATTACKS & DEFENCES

VERWACHTINGEN

- Eerste uitvoering van de keuzemodule
  - Heb je feedback of andere opmerkingen: Laat het ons weten!
- Inzet en groei staat centraal
- Projectgroepen: Samen werken en leren is essentieel
  - Maak afspraken met elkaar en kom deze na
  - Werken aan opdrachten en ga met elkaar de discussie aan
  - Neem elkaar mee, laat niemand achter
  - Focus groepsbegeleiding is samenwerking en oog voor elkaar
- Maak aantekeningen: Je onthoudt écht niet alles!

BELANGRIJKE DATA

Week	Periode 3	Ma	Di	wo	Do	Vr	
1	maandag 2 februari 2026	**2-2**	**3-2**	4-2	5-2	6-2	
2	maandag 9 februari 2026	9-2	10-2	11-2	12-2	13-2	
3	maandag 16 februari 2026	*16-2*	*17-2*	*18-2*	*19-2*	*20-2*	Carnaval
3	maandag 23 februari 2026	23-2	24-2	25-2	26-2	27-2	
4	maandag 2 maart 2026	**2-3**	3-3	4-3	5-3	6-3	
5	maandag 9 maart 2026	**9-3**	10-3	**11-3**	**12-3**	13-3	
6	maandag 16 maart 2026	16-3	17-3	18-3	19-3	**20-3**	
7	maandag 23 maart 2026	**23-3**	24-3	25-3	26-3	27-3	
8	maandag 30 maart 2026	30-3	31-3	1-4	2-4	3-4	goede vrijdag
9	maandag 6 april 2026	6-4	**7-4**	**8-4**	**9-4**	10-4	2de paasdag
10	maandag 13 april 2026	13-4	14-4	15-4	16-4	17-4	
		CGI	CGI			herkansing	

avans hogeschool

DOEL KICK-OFF

- Elkaar leren kennen
- Weten wat je te wachten staat
- Eerste stap in de wereld van cybersecurity: waarom is het belangrijk?

Leeruitkomst

01

Je analyseert en beschrijft actuele cybersecurityvraagstukken, neemt daarbij relevante normen, raamwerken en wet- en regelgeving in acht, en doet onderbouwde voorstellen voor passende technische, organisatorische en mensgerichte maatregelen. Je beschikt over basiskennis van de belangrijkste cybersecuritythema's en kunt de toepassing hiervan mondeling verantwoorden. Je legt je aanpak, bevindingen en adviezen overzichtelijk schriftelijk vast.

INHOUD & TOETSING

Code Osiris	Naam Onderwijseenheid	SBU	1e kans	2e kans
Periode 1		15		
M62821-01	Cybersecurity Fundamentals	15	Periode 1 Week 10 (ma / di)	Periode 1 Week 10 (vr)

- Iedere module wordt afgesloten met een formatieve toets aan de hand van beroepsproducten
- Toetsing individueel, waarin groepsinzet wordt meegenomen
- Aantekeningen en portfolio toegestaan tijdens toetsing
- Module wordt afgesloten met een Criterium Gericht Interview (CGI)

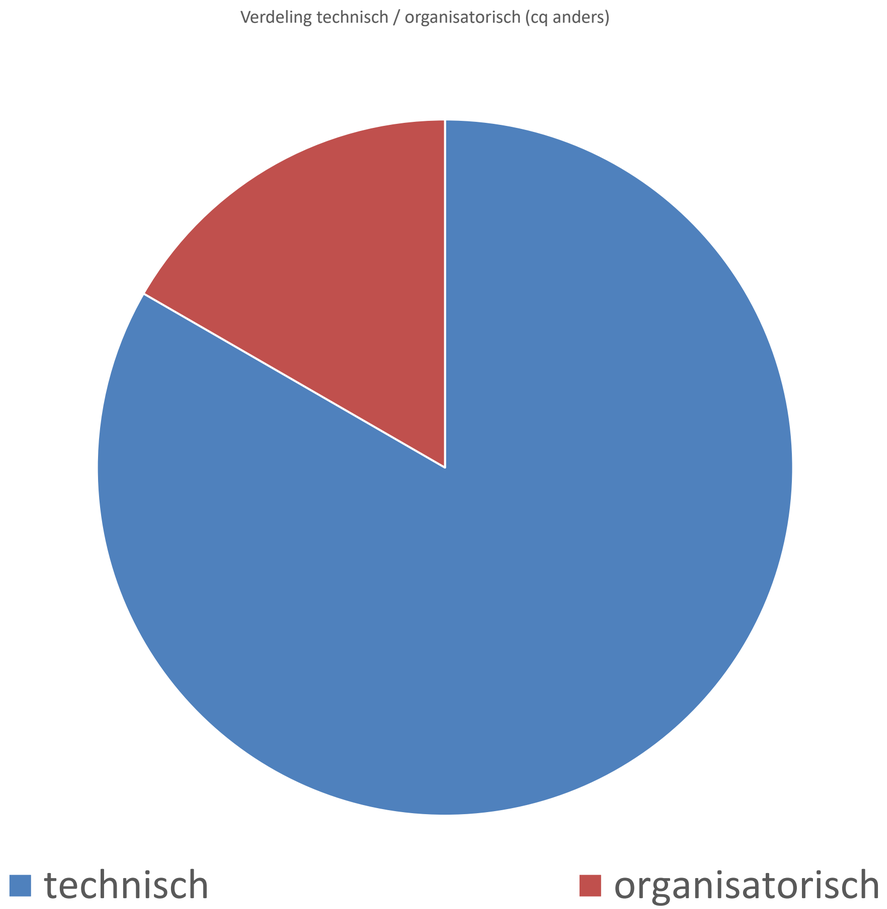
avans hogeschool

TOETSING

Module 1, 2 en 3: Fundament cybersecurity

Je bouwt gedurende de module een portfolio op met de uitwerkingen van opdrachten, praktijkcases en formatieve toetsen. In dit portfolio laat je zien hoe je actuele cybersecurityvraagstukken analyseert en beschrijft, met inachtneming van relevante normen, raamwerken en wet- en regelgeving. Op basis van je portfolio bereid je een korte presentatie voor waarin je verschillende cybersecurityvraagstukken toelicht, de gekozen aanpak beschrijft en onderbouwde technische, organisatorische en mensgerichte maatregelen voorstelt. Deze presentatie vormt de basis voor een criteriumgericht interview (CGI) met een assessor. Tijdens dit gesprek licht je jouw keuzes en bevindingen mondeling toe en toon je dat je beschikt over basiskennis van de belangrijkste cybersecuritythema's. Je kunt uitleggen hoe normen, raamwerken en wetgeving in de gekozen context worden toegepast en waarom de voorgestelde maatregelen passend zijn. Je mag je portfolio tijdens het gesprek raadplegen, maar wordt geacht voldoende voorbereid te zijn. Op basis van een rubric beoordelen de assessoren of de leeruitkomst is behaald.

VERDELING (60 STUDENTEN)



PORTFOLIO

- Je bouwt jouw persoonlijke portfolio op
- Werk hier de opdrachten, praktijdcases en formatieve toetsen uit
- Beschrijf jouw analyse van actuele cybersecurityvraagstukken
- Neem de normen, raamwerken en wet- en regelregeving in acht
- Je kan de CyBOK als basis nemen
- Tip: Zie het als jouw aantekeningen document, maak er geen onpersoonlijk knip en plak werk van!

COMMUNICATIE

- Programma, lesmateriaal, opdrachten e.d. via de module in Brightspace: https://brightspace.avans.nl/d2l/home/262418
- Communicatie (vragen, videogesprekken e.d.) via Teams (chat)
- Projectgroep: Eigen privé Teamskanaal (documenten, chat, …)

REFLECTIEOPDRACHT

- Reflecteer op jouw huidige visie over de cybersecurity expert:
  - Waarom heb je voor deze keuzemodule gekozen?
  - Wat denk je te gaan leren?
  - Wat denk je dat een cybersecurity expert moet weten, kunnen en doen?
- Leg dit vast in een digitaal document, je krijgt hiervoor 10 minuten.
- Voeg deze reflectie met de samenvatting van de OSINT opdracht die jullie straks gaan maken aan je portfolio toe.

*Aan het einde van de module maak je deze evaluatie weer.

WE KIJKEN UIT NAAR EEN MOOIE MODULE

Succes en veel plezier!

avans hogeschool

HET VERDERE PROGRAMMA VAN VANDAAG

1. Elkaar leren kennen aan de hand van een OSINT-opdracht

2. Gastcollege

OSINT

Leer je projectgroep kennen!

avans hogeschool

INTRODUCTIE OSINT

OSINT = OPEN-SOURCE INTELLIGENCE

- Het verzamelen en analyseren van openbaar beschikbare informatie om inzichten en inlichtingen te verzamelen.
- Deze aanpak stelt onderzoekers, analisten, journalisten en criminelen(!) in staat om waardevolle inzichten te halen uit een schat aan online gegevens.

TOEPASSINGEN

- Threat Intelligence: cyber, terrorisme, bedrijfsspionage
- Onderzoek: vermissingen, strafrecht, due dilligence
- Concurrentie: strategie en tactiek van concurrenten
- Geopolitieke ontwikkelingen: wereldwijde gebeurtenissen en bewegingen analyseren

https://www.bellingcat.com/

BRONNEN EN TECHNIEKEN

Online bronnen

- Zoekmachines
- Social media
- Forums
- Nieuwssites
- Blogs

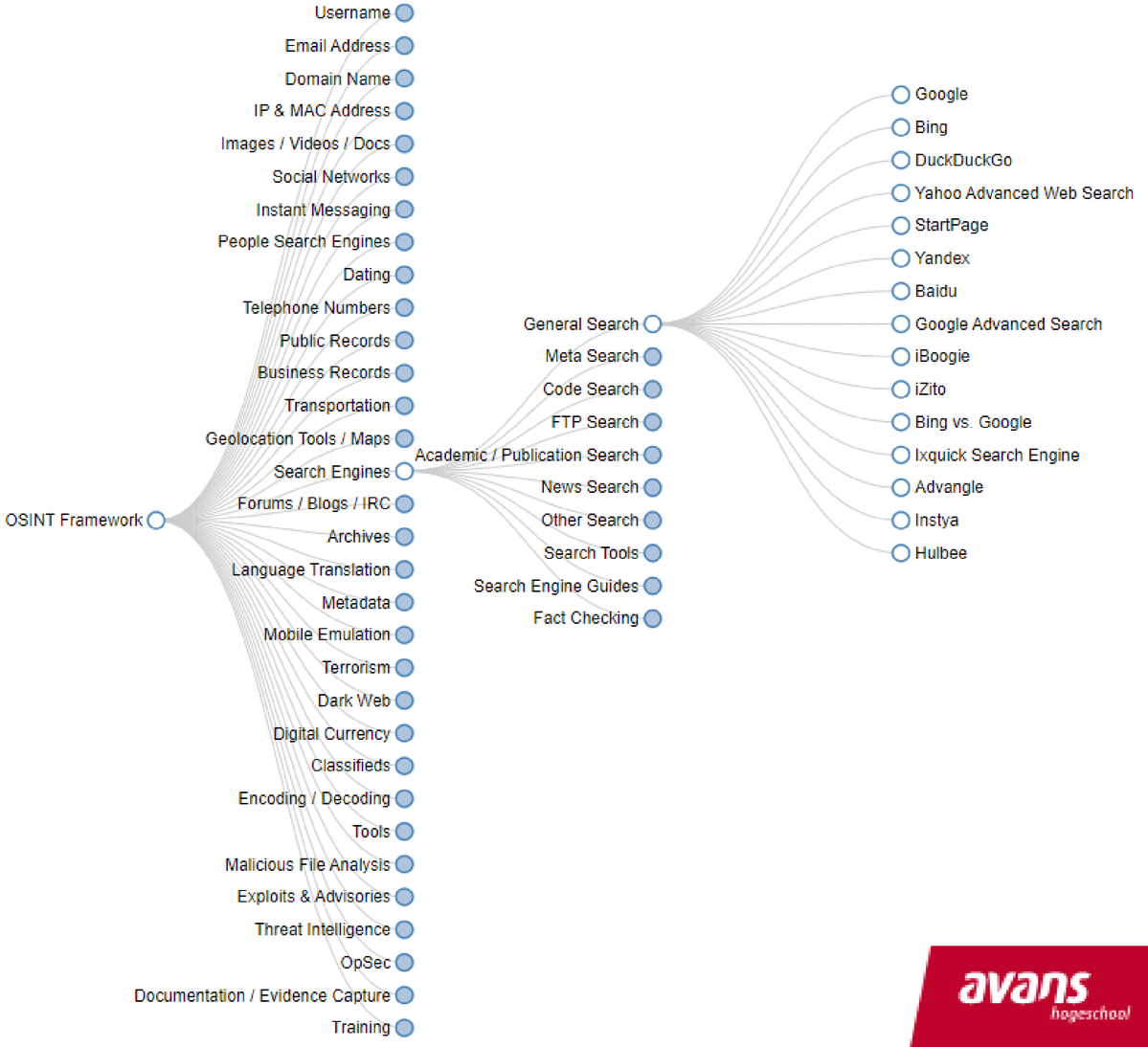
Databases

- Overheid
- Wetenschap
- Commercieel

Speciale tools

- Analyse metadata
- Geolocatie
- Webschrapers

https://osintframework.com/



OPDRACHT: LEER JE PROJECTLEDEN KENNEN (1/2)

Met wie zit je in een projectgroep? Identificeer jouw collega-studenten en verzamel basisinformatie over hen, zoals hun naam.

Gebruik OSINT-technieken (OSINT framework) om openbare beschikbare informatie over elk groepslid te vinden. Denk aan hun professionele profiel, hobby's, aanwezigheid social media, andere (online) activiteiten.

Analyseer de verzamelde informatie om inzicht te krijgen in de achtergronden, interesses en mogelijke bijdragen van je groepsleden!

OPDRACHT: LEER JE PROJECTLEDEN KENNEN (2/2)

4. Vat samen

5. Identificeer de sterke punten

6. Gebruik je inzichten!

Vat per groepslid de belangrijkste inzichten uit je OSINT-onderzoek samen.

Bepaal per groepslid de expertise, unieke vaardigheden en andere relevante eigenschappen die ieder in zou kunnen brengen.

Bespreek met elkaar hoe je op basis van de opgedane kennis over elkaar dit kan gebruiken om de samenwerking, communicatie en taakverdeling in de groep vorm te geven.

Leg dit vast in jouw portfolio.

KANTTEKENING PRIVACY

Weet met wat voor soort informatie je werkt! Het is openbare data, maar gaat wel over personen.

Respecteer de individuele privacy,

ga er netjes mee om!

PROJECTGROEPEN

- Zie Brightspace voor de projectgroepen.

AAN DE SLAG!

Ga uiteen in projectgroepen.

Beschikbare tijd stap 1 t/m 5 (individueel): 60 minuten.

Daarna stap 6 met alle groepsleden van je groep: 60 minuten.

SUCCES!

avans hogeschool

GASTCOLLEGE

Cybersecurity / Xander Koppelmans

Locatie: **HA-512** (Hogeschoollaan)

avans hogeschool