MAKE IT WORK

CURRICULUM

SECURITY

SECURITY

Organisaties zijn steeds afhankelijker van informatie en de onderliggende infrastructuur, die veelal is verbonden met internet. Medewerkers van organisaties worden geconfronteerd met spam, malware, virussen, social engineering en allerlei andere bedreigingen. Daardoor komt het onderwerp beveiliging steeds hoger op de bedrijfsagenda. Voorkomen moet worden dat de continuïteit van de bedrijfsprocessen, en daarmee die van de organisatie, in gevaar komt. Het fundament van Security bestaat uit drie onderdelen: mensen, processen en technologie. Deze onderdelen vormen belangrijke schakels in organisaties, maar worden ook blootgesteld aan verschillende veiligheidsdreigingen.

Security richt zich op het beschermen en beveiligen van waardevolle bezittingen van een organisatie, zoals bijvoorbeeld de ICT-infrastructuur en software, tegen allerlei bedreigingen. De beschikbaarheid, integriteit en vertrouwelijkheid van deze bezittingen moeten worden gewaarborgd.

MAKE IT WORK

PROFIEL SECURITY SPECIALIST

Een Security Specialist heeft als belangrijk verantwoordelijkheidsgebied de operationele aspecten van de informatiebeveiliging. Daardoor bezit de Security Specialist kennis en vaardigheden op het gebied van systeem- en netwerktechnologie. Naast dit technisch perspectief, heeft de Security Specialist te maken met veiligheid van bedrijfsprocessen en de menselijke invloed daarbij. Ook treft de Security Specialist maatregelen die verschillend van aard zijn en als doel hebben:

- het voorkomen van beveiligingsincidenten (preventieve maatregelen)
- het opsporen van beveiligingsincidenten (detectieve maatregelen)
- het beperken van nadelige gevolgen van beveiligingsincidenten (repressieve maatregelen)
- het teruggaan naar de normale situatie (correctieve maatregelen)

MAKE IT WORK

OVERZICHT MAKE IT WORK SECURITY

De Make IT Work omscholingsrichting Security bestaat uit drie onderdelen:

1. Fundamentals - waarin de technische vakinhoud wordt bijgebracht.
2. Boosters - voor het toepassen van de vakinhoud.
3. Begeleiding - voor bewaken voortgang en reflectie.

MAKE IT WORK

OVERZICHT MAKE IT WORK SECURITY

Week	Activiteiten	Uur
1 – 3	Fundamentals 1: Infrastructure Security, Operating Systems Security, Offensive Programming Booster 1: Pre-engagement Interaction Begeleiding: coaching en professioneel gesprek	72 42 6
4 - 6	Fundamentals 2: Infrastructure Security, Operating Systems Security, Offensive Programming Booster 2: Intelligence Gathering Begeleiding: coaching en professioneel gesprek	72 42 6
7 - 9	Fundamentals 3: Infrastructure Security, Operating Systems Security, Offensive Programming Booster 3: Threat Modeling Begeleiding: coaching en professioneel gesprek	72 42 6
10	'Boosterweek'	40
11 - 13	Fundamentals 4: Infrastructure Security, Operating Systems Security, Offensive Programming Booster 4: Vulnerability Analysis Begeleiding: coaching en professioneel gesprek	72 42 6
14 - 16	Fundamentals 5: Threat Intelligence, Monitoring, Ethical Hacking Booster 5: Monitoring Begeleiding: coaching en professioneel gesprek	72 42 6
17 - 19	Fundamentals 6: Threat Intelligence, Monitoring, Ethical Hacking Booster 6: Threat Intelligence Begeleiding: coaching en professioneel gesprek	72 42 6
20	'Boosterweek'	40

INHOUD CURRICULUM SECURITY - FUNDAMENTALS

Tijdens de opleiding doorloop je 6 fundamentals. Je ontwikkelt fundamentele basiskennis en –vaardigheden die je nodig hebt als cybersecurityprofessional. Dit leer je in werkcolleges en via praktijkgerichte opdrachten op het gebied van veiligheid van infrastructuur en operationele systemen van organisaties, Ook werk je verder aan je programmeervaardigheden. Voor alle onderdelen zijn er werkcolleges, opdrachten en een eindopdracht.

De onderstaande tabel geeft weer wat de opzet van de lesweken is waarin de fundamentals centraal staan. Dat zijn de lesweken 1 t/m 9 en 11 t/m 19.

Dag	Activiteiten	Uren
Maandag	Fundamentals	8
Dinsdag	Fundamentals	8
Woensdag	Fundamentals	8
Donderdag	Booster Begeleiding	6 2
Vrijdag	Booster	8

MAKE IT WORK

FUNDAMENTALS – LEERDOELEN EN COMPETENTIES

Methodisch handelen

- Je kan een stappenplan toepassen bij het oplossen van een vraagstuk.
- Je maakt op methodische wijze gebruik van openbare bronnen om informatie te verzamelen.
- Je kan het probleem op gestructureerde wijze in kaart brengen en oplossen.

Probleemoplossend vermogen

- Je kan de opdracht vertalen naar een cybersecurity-vraagstuk en een plan van aanpak.
- Je kan eventuele knelpunten signaleren tijdens het uitvoeren van de opdracht.
- Je kan die eventuele knelpunten oplossen.
- Je kan de scope van de opdracht bewaken.
- Je kan methoden en technieken op een juiste manier selecteren en toepassen.
- Je kan resultaatgericht handelen tijdens het uitvoeren van de opdracht.

Communiceren

- Je kan op passende wijze beroepsgerichte informatie delen met medecursisten, collega's en de opdrachtgever.

MAKE IT WORK

FUNDAMENTALS 1 T/M 4

Je verwerft kennis en vaardigheden over:

- Infrastructure Security
- Operating System Security
- Offensive Programming

ONDERWERPEN FUNDAMENTALS 1

- Basiskennis netwerken, nadruk op netwerkprotocollen en hun kwetsbaarheden
- Risico's analyseren vanuit het OSI-model en TCP/IP model
- IPV4 en IPv6 Adressering
- Operating systems: Windows en Linux
- Programmeervaardigheden, basiskennis Python en van daaruit Python voor penetration testing
- Ethisch handelen en beroepscodes

MAKE IT WORK

ONDERWERPEN FUNDAMENTALS 2

- Routing en switching: functionaliteit, kwetsbaarheden en risico's
- Netwerkservices (DHCP, DNS, FTP, Email, SSH, HTTP) en bijbehorende risico's
- Operating systems: Windows en Linux
- Methoden en technieken (Intelligence gathering, Portscanning, Shodan, Maltego, Social Engineering)
- OSINT
- Programmeervaardigheden, basiskennis Python en van daaruit Python voor penetration testing
- Ethisch handelen en beroepscodes
- Rapporteervaardigheden
- Nieuwe actuele kennis en vaardigheden die aansluiten bij de opdrachten en behandelde thema's

MAKE IT WORK

ONDERWERPEN FUNDAMENTALS 3

- Infrastructure security: Firewall, IPS/IDS, VPN, secure LAN
- Methoden en technieken op het gebied van threatmodeling (MT2016)
- Operating systems: Mobile en Internet of Things
- Programmeervaardigheden, basiskennis Python en van daaruit Python voor penetration testing
- Rapporteervaardigheden
- Ethisch handelen en beroepscodes
- Nieuwe actuele kennis en vaardigheden die aansluiten bij de opdrachten en behandelde thema's

MAKE IT WORK

ONDERWERPEN FUNDAMENTALS 4

- CyberOperations: malware, cryptographic systems, SOC
- Operating systems: Mobile en Internet of Things
- Technieken om Vulnerability analysis (scanning, enumeration) uit te voeren
- Programmeervaardigheden, basiskennis Python en van daaruit Python voor penetration testing
- Ethisch handelen en beroepscodes
- Nieuwe actuele kennis en vaardigheden die aansluiten bij de opdrachten en behandelde thema's

MAKE IT WORK

FUNDAMENTALS 5 & 6

Je verwerft kennis en vaardigheden over:

- Threat Intelligence
- Monitoring
- Ethical Hacking

THEMA'S FUNDAMENTALS 5

Threat Intelligence

- Wat is Threat Intelligence?
- Global threat intelligence
- Threat Intellkigence Reports
- Hunting, Features Extraction, Behaviour Extraction
- Operational en Strategic intelligence
- Threat Intelligence Lifecycle
- Risk Modeling

Monitoring

- Wat verstaan we onder monitoring
- Algemene begrippen (Logging, Correlatie, SIEM…)
- Stukje geschiedenis
- Intrusion Detectie, Intrusion Prevention
- Pakketten analyse
- Tooling zoals SiLK, Security Onion, Logstash, Netflow, Snort

Ethical Hacking

- Scoping, wettelijke kaders en opdracht
- Enumeratie - Offensief en OSINT
- Analyse en identificatie van kwetsbaarheden
- Exploitatie van kwetsbaarheden
- Exploitatietechnieken
- OWASP-kwetsbaarheden
- Social Engineering
- Rapportage

MAKE IT WORK

THEMA'S FUNDAMENTALS 6

Threat Intelligence

- Clustering & Correlation
- Threat Sharing
- Attribution
- National Intelligence Strategy of The United States
- Tracking and Taking Down
- Threat Modeling and Technology Profiling

Monitoring

- Monitoring requirements, compliance
- Event management, Correlation
- Use cases for monitoring
- Building a SOC
- Context integration, link naar Threat Intelligence
- Data driven monitoring (AI engines)
- Forensics, automated investigations
- Visit of a real SOC

Ethical Hacking

- Scoping, wettelijke kaders en opdracht
- Enumeratie - Offensief en OSINT
- Analyse en identificatie van kwetsbaarheden
- Exploitatie van kwetsbaarheden
- Exploitatietechnieken
- OWASP-kwetsbaarheden
- Social Engineering
- Rapportage

MAKE IT WORK

BOOSTERWEEK

Het uitgangspunt van de boosterweek is de verbinding maken tussen de fundamentals en de praktijk. Je voert je projecten uit waarmee je de opgedane kennis en vaardigheden uit de fundamentals toepast in een project binnen de context van je toekomstige werkgever.

BEGELEIDING

Tijdens de coaching en het professioneel gesprek kijk je met je studiebegeleider naar je voortgang. Je bespreekt het leerproces en de resultaten om zo te kijken welke ontwikkelingen je hebt doorgemaakt. Daarnaast krijg je ook feedback en feed forward.

BEGELEIDING: LEERDOELEN EN COMPETENTIES

Methodisch handelen

- Je kan op gestructureerde wijze relaties tussen relevante ICT-assets, processen en mensen in kaart brengen.
- Je kan een onderbouwde keuze maken voor geschikte tools en methodes.
- Je maakt op methodische wijze gebruik van openbare bronnen om informatie te verzamelen.
- Je kan op gestructureerde wijze resultaten vastleggen, waarbij navolgbaar is hoe de resultaten tot stand zijn gekomen.

Probleemoplossend vermogen

- Je kan de vraag van de opdrachtgever vertalen naar een cybersecurity-vraagstuk en een plan van aanpak.
- Je kan eventuele knelpunten signaleren tijdens het uitvoeren van de opdracht.
- Je kan die eventuele knelpunten oplossen.
- Je kan de scope van de opdracht bewaken.

Samenwerken

- Je kan binnen een team een rol nemen en aantoonbaar waarde toevoegen.
- Je bent in staat om relevante partijen bij een specifieke situatie in het proces te betrekken.
- Je werkt binnen een team resultaat- en oplossingsgericht.

MAKE IT WORK

BEGELEIDING: LEERDOELEN EN COMPETENTIES

Communiceren

- Je kan binnen het eigen team helder communiceren.
- Je kan bevindingen helder overbrengen aan de opdrachtgever.
- Je kan de werkzaamheden, de gemaakte keuzes en genomen acties helder verwoorden.
- Je kan op passende wijze beroepsgerichte informatie delen met medecursisten, collega's en de opdrachtgever.
- Je kan op heldere wijze een presentatie geven, rekening houdend met het publiek.

Lerend vermogen

- Je kan reflecteren op de eigen rol en (ethisch) handelen bij het uitvoeren van de inventarisatie.
- Je maakt weloverwogen keuzes ten aanzien van het eigen gedrag, de organisatie en de omgeving.
- Je kan eigen leervragen formuleren.
- Je kan de opgedane kennis delen met anderen.

MAKE IT WORK

WWW.IT-OMSCHOLING.NL