#INFORMATICA

BESPAAR MET DE KMO-PORTEFEUILLE

CYBERCRIMINALITEITS- EN BEVEILIGINGSEXPERT

CYBERVEILIGHEID: IS UW ONDERNEMING ER KLAAR VOOR?

OMSCHRIJVING

Introductie

Klassikale sessies worden telkens op woensdagavond (18u30-22u) in de campus Brugge georganiseerd, aangevuld met e-leren, projectintegratie op de werkvloer en individuele coaching.

De bedrijfswereld staat voor nieuwe uitdagingen op het gebied van computerbeveiliging: een nieuw wettelijk kader (de “NIS”-richtlijn, de recente Europese verordening betreffende de bescherming van persoonsgegevens), de uitdagingen van de digitale economie en de cyberveiligheid, nieuwe vormen van cybercriminaliteit, ...

Dit intensief jaartraject helpt de netwerkbeheerder hier met veel diepgang de nodige vaardigheden te ontwikkelen om aan deze noden tegemoet te komen.

Het traject bevat een totaalbeeld inzake informatiebeveiliging, frameworks en controles, ethical hacking, pentesting, cryptografie, forensics, emergency response en risico management.

Via actuele cases, hands-on labs (CTF hacking challenges), werkplekleren en aanvullende e-content zorgt de vakexperten voor inzicht en onmiddellijke toepasbaarheid van deze competenties. Binnen alle onderdelen werken we een aanpak, template of dergelijke uit die je zo kan implementeren in de werkomgeving.

Omschrijving

Binnen bedrijven en organisaties is IT-beveiliging veelal geen kernactiviteit waardoor de toegevoegde waarde van dit kennisdomein erin bestaat zijn of haar cybersecuritykennis en -vaardigheden aan te wenden. Het traject bevat een totaalbeeld inzake pentesting, cryptografie, forensics, emergency response en risico management. Hierbij wordt gefocust op een ruim toepassingsbereik van digitale beveiligingsfacetten. Via actuele cases, hands-on labs, werkplekleren en aanvullende e-content zorgen de verschillende vakexperten voor inzicht en onmiddellijke toepasbaarheid van deze competenties.

Voor wie is deze opleiding bestemd?

Veiligheidsadviseurs, system admins, network admins, webadmins, netwerk administrators, netwerk designers en architecten, systeem architecten en andere professionele profielen die de integriteit van de network en system infrastructuur moet verzekeren.

Toelatingsvoorwaarden

Om toegelaten te worden in de opleiding dien je aan minstens één van volgende voorwaarden te voldoen:

- OF Aantoonbare ervaring: minimum twee jaar professionele beroepservaring binnen de vooropgezette doelgroep als zelfstandige of loontrekkende.
- OF Kwalificatiebewijs dat voorkennis netwerkskills in kaart brengt.

Methodologie

De lessen worden in het Nederlands gegeven, maar het cursusmateriaal is in het Engels zodat je perfect bent voorbereid op eventuele Engelstalige certificering-examens.

BYOD

Breng je eigen laptop (mac of pc) mee naar de les die beschikt over:

- 60 GB vrije schijfruimte
- CPU met hardwareversnelling ifv virtualisaties
- Administrator rechten

Ook een USB Flash Drive kan handig zijn om projecten te bewaren.

Modern leren: digitale leeromgeving, individuele coaching en projectleren

- E-LEREN

Het opleidingstraject voorziet flankerende e-leercontent om diepgaande en aanvullende kennis aan te reiken. Het traject integraal via afstandsonderwijs volgen is niet mogelijk.

- PROJECTLEREN

De opleiding bevat 38 uren werkplekleren met als doelstelling om de eerder verworven kennis in de opleiding volgens twee vooraf gedefinieerde opdrachten toe te passen binnen jouw professionele context. De aangeleerde vaardigheden worden zo onmiddellijk toegepast in de praktijk. Natuurlijk gaan we jou hierbij intensief begeleiden via individuele coaching.

In functie van dit projectleren kan een NDA met de tewerkgestelde organisatie afgesloten worden.

Deze opleiding is bijgevolg geen *ik-kom-naar-de-les-en-de-docent-zal-het-mij-wel-vertellen-opleiding*. De waarde van de opleiding komt pas tot zijn recht mits een actieve participatie van de deelnemers en een constructieve onderlinge samenwerking. Case, praktijkopdrachten, project op jouw werkvloer zijn verweven doorheen de opleiding.

EXAMENS

Per nieuwe module neemt de competentiegroei gradueel toe.

Deelnemen aan een vervolg-module kan pas indien je via evaluatie hebt bewezen dat je over de vereiste kennis en vaardigheid beschikt uit de voorgaande module.

Mede ifv hiervan vormt de aanwezigheid tijdens de klassikale sessie een vereiste.

PROGRAMMA

MODULE Inleiding tot cybercriminaliteit

In deze inleidende module komen diverse basisconcepten aan bod. Allereerst brengen we de beoogde doelen in kaart die we met IT beveiliging willen bereiken. Vervolgens kijken we naar de bedreigingen en aanvalsmogelijkheden (threat landscape) die de basis vormen voor deze bedreigingen.

Tot slot worden een aantal fundamentele security-principes en -controls behandeld.

MODULE Bedreiging in kaart brengen & aanpakken + Werkplekleren

Inschatten van technische security controles, Port scanning, Intrusion detectie, Ethical hacking Penetration testing

Dit is uiteraard voornamelijk een praktisch onderdeel.

Scans zijn een essentiële stap, maar het interpreteren van de resultaten is waar de werkelijke kunst zit. Daarom wordt er een stapje verder gegaan en krijgen de cursisten de kans om aan de slag te kunnen gaan met de resultaten van hun scans. Het wordt een cursus *'out of the box'* denken.

Aan deze module is tevens een luik projectwerk gekoppeld waarbij de aangeleerde vaardigheden binnen de werkomgeving worden toegepast.

MODULE Reactie bij incidenten

Topics: incident response team, Digital forensics, Overzicht security incidenten en aanbevolen acties

Ondanks alle preventieve maatregelen valt een cyberincident nooit uit te sluiten. Wanneer een organisatie getroffen wordt, ben je best goed voorbereid. Een goed responsplan stelt je in staat om snel te ageren en zo de schade en de herstelkosten te beperken.

Het efficiënt reageren op incidenten vraagt technologische aanpassingen en een gepaste rapportering. Soms dienen ook bedrijfsprocessen aangepakt te worden.

MODULE Managementskills + Werkplekleren

Beleidskader en –documenten, Business Impact Analyse & Business Continuity Plan

Aan deze module is een luik projectwerk gekoppeld, waarbij de aangeleerde vaardigheden via individuele coaching geïntegreerd worden binnen jou specifieke beroepscontext.

Deze opdracht vult tevens de insteek voor de eindproef.

EINDPROEFverdediging

DOCENT

- Nick Pieters - NSE4 - 6, CISSP
- Alvin Demeyer - CEH

PARTNERS

FROM PRACTICE-ORIENTED TRAININGS TO EMPLOYABLE IT EXPERTS

ESF - 2016-2019

De doelstelling van het project is het verhogen van de innovatiegraad in het ICT-opleidingsaanbod en de tewerkstellingsgraad in de ICT-sector via innovatieve en toegepaste (in de vorm van duale en digitale) leertrajecten. Deze verschillen van het reeds bestaande IT-opleidingsaanbod door de innovatiefactor en flexibiliteit om in te spelen op de noden binnen de IT-markt. De integratie en volwaardige uitbouw van duaal leren in deze opleidingen lijkt cruciaal.

Het gecertificeerde opleidingstraject Cybercriminaliteits- en beveiligingsexpert heeft deze duale leercomponent geïntegreerd.