ACEN

STAGE

Attack Detect Defend

Beschrijving van de opdracht

ACEN is een toonaangevende aanbieder van totaaloplossingen voor cybersecurity in België. We bieden organisaties van elke omvang en uit alle sectoren de bescherming die ze nodig hebben tegen cyberdreigingen. Ons team van experts beschikt over ruime ervaring en expertise en levert oplossingen op maat die inspelen op de specifieke noden van elke klant. We blijven voortdurend op de hoogte van de nieuwste dreigingen en technologieën, zodat onze klanten potentiële beveiligingsincidenten steeds een stap voor blijven.

Het doel van deze opdracht is stagiairs kennis te laten maken met zowel offensieve (red team) als defensieve (blue team) beveiligingspraktijken. Het project is opgedeeld in verschillende fases, waarbij de stagiairs de details en de uitvoering grotendeels zelf bepalen.

De opdracht bestaat uit de volgende fases:

1 Omgeving

a) Een labomgeving opzetten.
b) Een SIEM-oplossing onderzoeken en uitrollen.

2 Aanval

a) Verschillende aanvalstechnieken en beschikbare tools onderzoeken.
b) De eerder onderzochte aanvalsketen uitvoeren.

3 Onderzoek

a) Bestaande forensische artefacten en beschikbare tools onderzoeken.
b) Een forensisch onderzoek uitvoeren.

4 Rapportage

a) Een managementsamenvatting van de gesimuleerde aanval opstellen, zowel vanuit offensief als defensief perspectief.
b) Een tijdlijn van het incident opstellen.

5 Hardening

a) Mogelijke mitigaties voor de aanvalsketen onderzoeken.
b) Hardeningmaatregelen implementeren en nagaan of ze de aanval effectief verhinderen.

6 Retrospectief

a) Wordt door de stagiairs zelf bepaald in de loop van de opdracht.

Doelstelling

Minimale vereisten

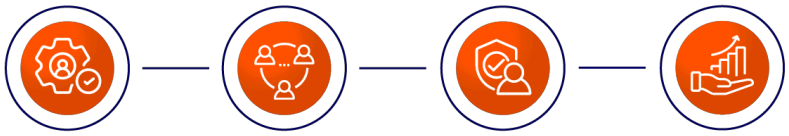
Van de studenten wordt verwacht dat ze minstens het volgende opleveren:

- Een geslaagde aanval op een labomgeving.
- Een beknopt incidentrapport over de gesimuleerde aanval.
- Documentatie van zowel de methodologie als de resultaten van elke fase.

Methodologie

ACEN past in zijn projecten agile projectmethodologieën zoals Scrum toe, en deze opdracht vormt daarop geen uitzondering. Bij deze methodologieën staat de kwaliteit van softwareoplossingen centraal. Dat wordt bereikt door het project in nauwe samenwerking met de stagiairs in fases op te delen en door intensief te communiceren, zowel binnen als buiten het projectteam. Voortdurende communicatie is inherent aan agile methodologieën en zorgt bijgevolg voor een grondige begeleiding en ondersteuning tijdens de stage.

Profiel



Expertise **Samenwerking** **Integriteit** **Innovatie**

Contactgegevens

Contactpersoon	Cindy Van den Hoecke	**cindy.vandenhoecke@acen.eu**