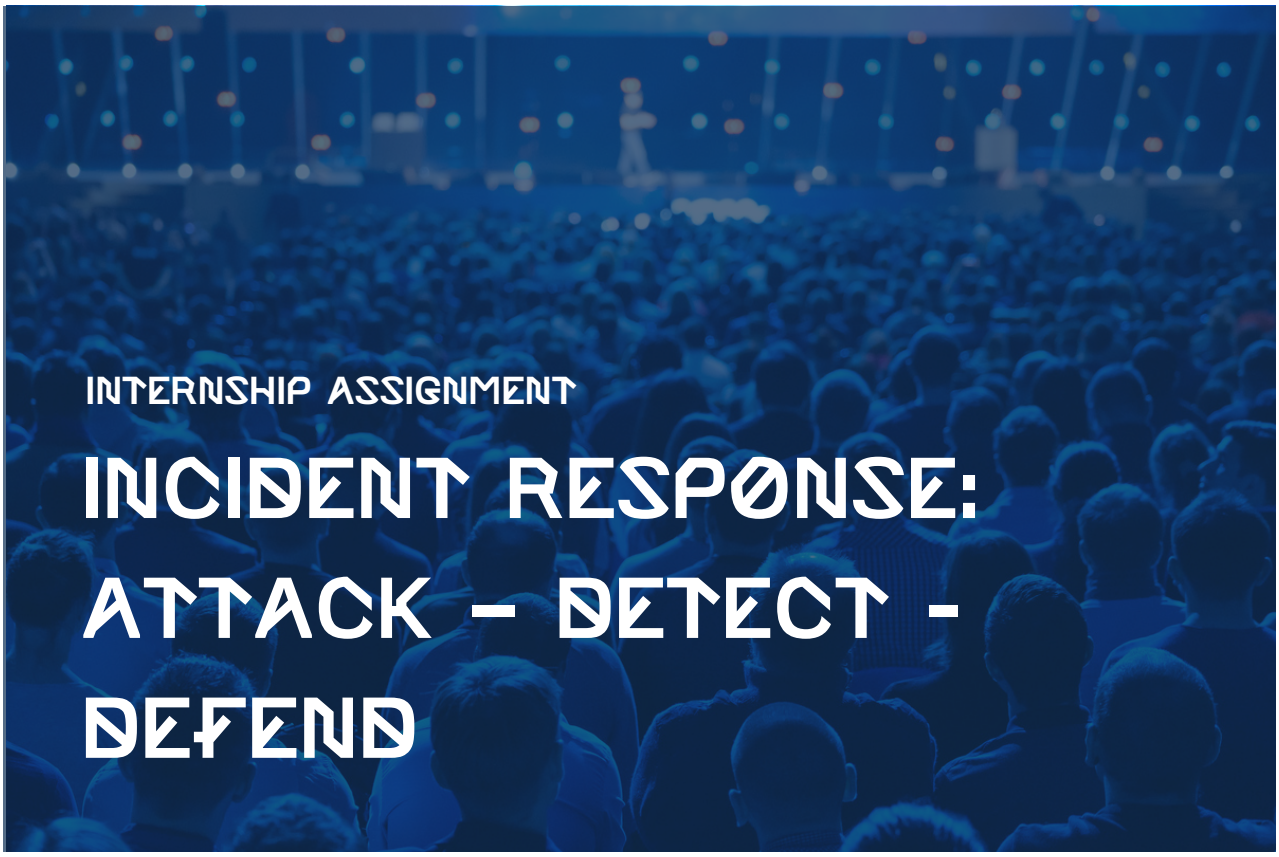

INTERNSHIP ASSIGNMENT

INCIDENT RESPONSE: ATTACK – DETECT - DEFEND

Contact

Cindy Van den Hoecke
careers@is4u.be

Nynox, an IS4U NV Division

Veldkant 7
2550 Kontich
België

Introductie Nynox

Nynox als spin-off van IS4U biedt sinds 2015 “Managed Security” diensten aan voor verscheidene klanten. Het portfolio van Nynox bestaat uit een combinatie van producten en diensten met als doel een 360° beeld te bieden aan klanten over hun “Security posture”.

Nynox beheert deze oplossingen vanuit een centraal Security Operations Centre. Data van verschillende producten wordt gecentraliseerd in een SIEM oplossing. Bijkomend wordt Nynox regelmatig opgeroepen om gehackte bedrijven te helpen bij het onderzoek van hoe hackers zijn binnengeraakt. Dit kan gaan van Phishing tot Ransomware aanvallen.

Omschrijving opdracht

De opdracht verloopt in meerdere fasen:

1. Zet een (basis) labo op
    - 1 AD (+ DNS)
    - 1-2 Windows Workstations
    - 1 Kali Linux
2. Doorloop de attack chain in het labo, documenteer deze en maak een rapport van de stappen.
    - Welke technieken zijn er gebruikt om zich in het labo te nestelen?
    - Welke stappen zijn ondernomen om data te verkrijgen en hoe is deze gebruikt?
    - Zijn er nieuwe onbekendere aanvalstechnieken om ongedetecteerd persistentie te behouden?
3. Voer een onderzoek uit a.d.h.v. de Nynox Incident Response Toolkit
    - Deze tool zal de belangrijkste artifacten verzamelen bij de geimpacteerde systemen.
    - Deze dienen onderzocht te worden om de stappen van de aanval te traceren.
    - Wat zien we wel of niet in de logs. Zijn er artifacten elders te vinden?
    - Zijn er andere dingen die we niet in de output terug vinden?

4. Maak een rapport van de gevonden data uit stap 3
    - Leg uit welke data dat gevonden is, wat de significantie is en wat de aanvaller hier mee probeerde te bereiken.
5. Omschrijf toekomstige preventieve maatregelen
    - Incident Response is niet enkel het weten wat er gebeurd is. Een belangrijk aspect is buiten de containment ook het voorkomen dat aanvallers dezelfde manier kunnen gebruiken om binnen te geraken.

Minimale vereisten

De studenten wordt gevraagd minimaal de volgende functionaliteiten op te leveren:

- Succesvolle aanval uitvoeren op een eigen omgeving + documentatie
- Queries opstellen om data te vinden in de afgeleverde artifacten
- Gevonden Indicators of Compromise oplijsten + documentatie

Optioneel

- Automatisatie van de aanval

Technologieën / Concepten betrokken bij deze opdracht

- ELK-stack
- Cloud
- Data-analyse
- PowerShell
- Python

Projectmethodologie

Nynox maakt voor haar projecten gebruik van agile projectmethodologieën zoals SCRUM. Het hierboven beschreven project vormt hier geen uitzondering op. Deze methodologieën stellen de kwaliteit van softwareoplossingen centraal. Dit wordt bereikt door het project op te delen in kortere iteraties en een zeer intense communicatie binnen en buiten het projectteam. Intensieve communicatie is inherent aan agile en leidt bijgevolg tot een doorgedreven stagebegeleiding.