INTERNSHIP ASSIGNMENT

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE AS A SERVICE

Contact

Cindy Van den Hoecke
careers@is4u.be

Nynox, an IS4U NV Division

Veldkant 33A
2550 Kontich
België

Stageopdracht

SOAR as a Service

Omschrijving

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. Om de analisten tijdens interventies van bijkomende informatie te voorzien overweegt Nynox de implementatie van een SOAR-oplossing.

Nynox wil onderzoeken hoe de opzet en configuratie van een multi-tenant SOAR-omgeving werkt en welke automatisatie oplossingen deze biedt voor het verrijken van offenses uit de centrale SIEM oplossing. Het “as a service” aanbieden van SOAR betekent dat er één centrale omgeving bij Nynox gebruikt kan worden voor meerdere klanten. Deze klanten kunnen dan gebruik maken van de oplossing zonder dat ze deze zelf hoeven te beheren.

Nynox wenst tijdens deze stage minstens drie producten te vergelijken op basis van de noden die zich nu, en in de toekomst, stellen. De stage zal bestaan uit een behoefteanalyse, productvergelijking en een demo-configuratie van één of meerdere SOAR-oplossingen aan de hand van enkele use cases.

Voorbeeld van een use case:

Nynox wordt gevraagd om een phishing mail te onderzoeken. Deze aanvraag komt terecht bij een SOC-analist, hij is van mening dat verder onderzoek nodig is.

1) De SOC-analist forward de mail in kwestie als bijlage naar een centrale mailbox
2) SOAR-tool monitort centrale mailbox en creëert een incident voor verdere opvolging
3) Het incident wordt verrijkt met data uit de attachment
    - a. Mail headers
    - b. Mail body
4) SOAR-tool maakt een incident checklist op basis van een op voorhand gedefinieerde playbook
5) De SOC-analist krijgt een overzicht van de gevonden informatie en de te ondernemen stappen

Minimale vereisten

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

- Behoefteanalyse
- Productvergelijking
- Demo-setup van het gekozen product

Optioneel:

- Additionele demo-setup

Projectmethodologie

Nynox maakt voor haar projecten gebruik van agile projectmethodologieën zoals XP en 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.