INTERNSHIP ASSIGNMENT

SOC TRIAGING AUTOMATION

Contact

Cindy Van den Hoecke
careers@is4u.be

Nynox, an IS4U NV Division

Veldkant 33A
2550 Kontich
België

Stageopdracht

SOC Triaging Automation

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 heeft Nynox een automatisatieplatform gemaakt.

Nynox wil deze proof-of-concept verder onder de loep nemen om te kijken waar we naar een andere/aangepaste architectuur kunnen gaan.

Het takenpakket van de stagiair(s) bevat onder andere het herbekijken van volgende aspecten van het platform:

- Niveau aan microservices
  - Verdere opsplitsing van services nodig?
- Communicatie tussen services
  - ActiveMQ vs REST/Combo?
- Herbekijken programmeertaal van Python naar C#
  - Speed-up
  - ORM
    - Dapper vs Entity Framework
- De benodigde delen van de applicatie herschrijven/opsplitsen

Voorbeeld van een use case:

Nynox wordt gevraagd om een offense te onderzoeken waarin een programma een executable aanspreekt die gebruikt kan worden om aan privilege escalation te doen. Deze offense komt terecht bij een SOC-analist aan de hand van de SIEM.

1) De SOC-analist opent het offense en kijkt naar de events
2) De analist kijkt na of dit gepast gedrag is door middel van de volgende stappen
    - a. Is dit al eerder voorgekomen
    - b. Is dit programma malicious?
    - c. Wat is de parent van dit programma?
    - d. Welke andere acties ondernam dit programma?
    - e. Welke andere events zijn er gezien op deze server/workstation?

Minimale vereisten

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

- Productvergelijking van verschillende frameworks
- Demo-setup van de implementatie

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.