Contact

Cindy Van den Hoecke
careers@is4u.be

Nynox, an IS4U NV Division

Veldkant 33A
2550 Kontich
België

Stageopdracht

Incident Response Automation

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 binnen geraakt. Dit kan gaan van Phishing tot Ransomware aanvallen.

Omschrijving

Nynox wil graag de mogelijkheid onderzoeken om een groot onderdeel van dit onderzoek te automatiseren om er zo voor te zorgen dat onze onderzoekers zo snel mogelijk aan de slag kunnen gaan met data analyse. Het doel is om Patient Zero of enige Indicator of compromise te kunnen identificeren.

Het automatiseren hiervan zal gebeuren door al de data die onze zelfgeschreven toolkit verzameld heeft te sturen naar bv. een Elastic Logstash. De data zal dan verwerkt worden met Python om alle hashes en IP adressen op te zoeken bij threat intelligence feeds zoals Alienvault. De output hiervan zal dan gebruikt worden om onze onderzoekers een startpunt te geven voor het onderzoek maar ook om terug te koppelen naar een centrale SIEM oplossing om een bredere analyse te maken van de data die hier binnenkomt.

Minimale vereisten

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

- Data centraliseren en normaliseren via een Elastic Logstash
- De data verwerken en analyseren aan de hand van verschillende threat intelligence feeds.
- Een gestructureerd rapport van de verwerkte data afleveren.

Optioneel:

- De oplossing integreren in beschikbare cloud producten.

Technologieën / Concepten betrokken bij deze opdracht

- DevSecOps
- Python
- Logstash
- Cloud
- Data-analyse
- Ansible

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.