THOMAS MORE

Central Logging met SIEM / SOAR

Reflectie

Alexander Conserva
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

Stagebedrijf: Intersoft Electronics

2025 – 2026

Inhoudsopgave

1. INLEIDING _____ 3

2. INHOUDELIJKE REFLECTIE _____ 4

3. PERSOONLIJKE REFLECTIE _____ 5

1. Inleiding

Dit document vormt de afrondende reflectie van mijn afstudeerstage bij Intersoft Electronics. Tijdens deze periode heb ik gewerkt aan het project "Central Logging met SIEM / SOAR". In dit reflectiedocument blik ik terug op de afgelopen maanden. In het eerste deel, de inhoudelijke reflectie, bespreek ik de concrete realisaties van het project en de waarde hiervan voor de organisatie. Vervolgens sta ik in de persoonlijke reflectie stil bij mijn eigen leerproces, de competenties die ik heb ontwikkeld en de uitdagingen die ik gaandeweg heb overwonnen.

2. Inhoudelijke reflectie

Tijdens deze stage heb ik met succes een Proof of Concept (PoC) gebouwd voor een robuuste logmanagement- en monitoringoplossing, specifiek afgestemd op verouderde (legacy) IT-omgevingen. Ik heb een gelaagde architectuur ontworpen waarbij ik gebruik heb gemaakt van Wazuh als centraal SIEM-systeem, Vector als log-router voor ongestructureerde data en een MISP-server voor Threat Intelligence.

Omdat bestaande SOAR-tools (zoals Shuffle of TheHive) en de standaard Wazuh-dashboards niet voldeden aan de specifieke eisen voor deze legacy-omgeving, heb ik bovendien een volledige eigen applicatie ontwikkeld. Dit fungeert als het centrale dashboard met geautomatiseerd case management, auditieve alarmering en een geïntegreerde AI-assistent voor snelle loganalyse.

Voor de organisatie levert dit een aanzienlijke risicoreductie op. De blinde vlekken van de uiterst fragiele legacy-systemen zijn weggenomen zonder de stabiliteit ervan in gevaar te brengen. Dankzij de Discord-integratie en de eigen applicatie kunnen beveiligingsanalisten nu veel sneller en accurater reageren op incidenten.

De doelstellingen uit het initiële projectplan zijn succesvol gerealiseerd in de testomgeving. De gebouwde PoC functioneert en bewijst dat de gekozen SOC-stack in de realiteit werkt. Voor systemen die buiten de actieve SIEM-monitoring vallen, is er tevens een succesvol traject uitgewerkt met Graylog voor langdurige logretentie ten behoeve van compliance.

Voor de definitieve productieomgeving adviseer ik de opdrachtgever het volgende:

- Behoud de huidige architectuur: Gebruik Wazuh als primaire SIEM voor actieve monitoring en de ontwikkelde maatwerkapplicatie als primair dashboard.
- Voorzichtige SOAR-uitrol: Schakel de geautomatiseerde 'active response' (zoals het automatisch blokkeren van IP-adressen via MISP) gefaseerd en met uiterste zorg in, om verstoring van bedrijfskritische processen te vermijden.
- Principle of Least Privilege: Behoud de strikte toegangscontrole voor API-koppelingen. Laat de applicatie uitsluitend via specifieke serviceaccounts met minimale leesrechten communiceren met de Wazuh API, in plaats van met beheerdersaccounts.
- In-house Certificatenbeheer: Zorg ervoor dat alle netwerkcommunicatie van de applicatie veilig versleuteld blijft via SSL/TLS. Maak hiervoor gebruik van de in-house certificatenoplossing van het bedrijf om de geldigheid en veiligheid van deze verbindingen te garanderen.
- Standaardisatie: Pas het hardening consequent toe op alle nieuwe besturingssystemen om de veiligheid van de infrastructuur structureel te waarborgen.

3. Persoonlijke reflectie

Tijdens dit traject heb ik de academische theorie rondom cybersecurity succesvol weten te vertalen naar zeer praktische oplossingen in een bedrijfsomgeving. Binnen mijn eigen project ben ik sterk gegroeid in applicatieontwikkeling en netwerkarchitectuur. Door de maatwerkapplicatie te ontwerpen volgens Zero-Trust principes heb ik geleerd om veilige IT-oplossingen te ontwerpen en te ontwikkelen met aandacht voor de gemaakte afspraken. Ook heb ik geleerd om flexibel te zijn en onderbouwde keuzes te maken wanneer technologieën tegenvielen zoals toen NXlog bijvoorbeeld te zwaar bleek voor de server, heb ik de alternatieven geëvalueerd en succesvol geschakeld naar Vector.

Wat deze stage voor mij persoonlijk het meest waardevol maakte, was de kennis die ik heb opgedaan buiten de strikte grenzen van mijn project. Ik hecht veel waarde aan levenslang leren en heb dit in de praktijk gebracht door veelvuldig mee te kijken en mee te denken met mijn stagebegeleider. Hierdoor heb ik een realistisch beeld gekregen van de dagelijkse werking van een Security Operations Center en de bijbehorende uitdagingen.

- Ik heb waardevolle inzichten opgedaan in enterprise IT-oplossingen en hoe deze worden geconfigureerd en beheerd.
- Ik heb in de praktijk kennisgemaakt met de betaalde SIEM/SOAR-oplossing van het bedrijf, diverse software voor vulnerability management, Microsoft Entra en Intune.
- Ik heb geleerd hoe complex wetgevingen en compliance in de praktijk zijn en hoeveel tijd dit in beslag neemt.
- Dit inzicht in bedrijfsbrede policies helpt mij enorm om in de toekomst rekening te houden met regelgeving en om maatschappelijk verantwoord te handelen.

Op het vlak van communicatie en samenwerking kijk ik terug op een erg soepel traject. Echte niet-technische obstakels of grote frustraties ben ik niet tegengekomen. Dit is grotendeels te danken aan de uitstekende begeleiding en de open sfeer op het kantoor. Ik kon altijd met vragen terecht bij mijn stagebegeleider, die mij uitstekend hielp met meedenken en mij telkens in de juiste richting stuurde. De sfeer met de collega's was erg prettig.

Tot slot kijk ik met een enorm positief gevoel terug op deze stageperiode bij Intersoft Electronics. Het was een ontzettend leerzame ervaring waarin ik niet alleen mijn technische vaardigheden als Cloud & Cyber Security student in de praktijk heb kunnen brengen, maar ook enorm ben gegroeid als professional. De combinatie van het zelfstandig uitwerken van een complexe Proof of Concept en de kans om te leren van de bredere bedrijfsprocessen en beveiligingsstrategieën, heeft mij een stevige fundering gegeven voor de toekomst. Het heeft mij perfect voorbereid op de volgende stap in mijn carrière.