THOMAS MORE

Central Logging met SIEM / SOAR

Projectplan

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

Stagebedrijf: Intersoft Electronics

2025 – 2026

Inhoudsopgave

1. INLEIDING 3
2. INTERSOFT ELECTRONICS 4
3. DOELSTELLINGEN 5
4. BUSINESS CASE 6
5. PLANNING 7
6. STATUS REPORT 8
7. LEGENDE 9

1. Inleiding

In dit document vindt u het project plan voor de stageopdracht "Central Logging met SIEM / SOAR", die wordt uitgevoerd bij Intersoft Electronics. Dit document dient als de formele leidraad voor de komende stageperiode en zorgt ervoor dat de doelen, verwachtingen en het verloop van het project vooraf helder zijn afgestemd tussen mijzelf als stagiair, de bedrijfsmentor op de werkvloer en de stagebegeleider vanuit de opleiding. Door de opdracht vooraf goed te structureren, biedt dit document een duidelijk overzicht van wat er de komende maanden onderzocht en gebouwd gaat worden om de IT-beveiliging van de organisatie te versterken.

In dit document komen de vaste onderdelen van de projectopdracht stapsgewijs aan bod. Allereerst wordt de bedrijfsachtergrond geschetst en de context van de opdracht toegelicht, waarbij de focus ligt op de noodzaak van centrale logging voor verouderde IT-omgevingen. Vervolgens beschrijft dit plan de concrete doelstellingen, zoals het vergelijken van geschikte oplossingen en het opzetten van een technische Proof-of-Concept, direct gevolgd door de business case die de toegevoegde waarde en risicoreductie voor de organisatie benadrukt. Tot slot geeft dit document een gedetailleerd overzicht van de projectplanning inclusief de belangrijkste mijlpalen, en wordt er vastgelegd op welke manier de voortgang wordt gerapporteerd en hoe de verantwoordelijkheden binnen het team zijn verdeeld.

2. Intersoft Electronics

Intersoft Electronics is een Belgisch bedrijf die radartechnologie en CNS-oplossingen ontwikkelt om luchtbeveiliging en luchtverkeersleiding te ondersteunen en zo het luchtruim veiliger te maken. Ze bouwen en leveren onder meer radarsystemen en modulaire radar(sub)systemen, voeren upgrades en integratieprojecten uit om bestaande radars te moderniseren en hun levensduur te verlengen, en bieden daarnaast gespecialiseerde test- en meetapparatuur en softwaretools voor radar- en navaid-metingen. Daarnaast ontwikkelt Intersoft ook NORA, een niet-roterende, elektronisch gestuurde radarantenne.

Binnen de organisatie draaien diverse kritieke processen op verouderde systemen (Legacy / End-of-Life). Deze systemen ontvangen geen beveiligingsupdates meer en kunnen vaak niet zomaar geüpgraded worden vanwege afhankelijkheden met specifieke applicaties of apparatuur. Omdat 'patchen' geen optie is, is de organisatie kwetsbaar. De enige manier om deze systemen toch veilig te houden, is door middel van zogenaamde 'Compensating Controls', waarvan strikte monitoring en centrale logging de belangrijkste zijn. Een SIEM-systeem helpt om loggegevens van deze oude systemen en het omliggende netwerkverkeer centraal te verzamelen, te analyseren en te correleren tot "events" of incidenten.

3. Doelstellingen

Tegen het einde van de stage moet er een onderzoek zijn uitgevoerd naar de compatibiliteit van verschillende SIEM- en SOAR-oplossingen met verouderde IT-omgevingen. Hierbij ligt de nadruk specifiek op het veilig onttrekken van loggegevens uit deze oude systemen, bijvoorbeeld door middel van agentless logging, legacy-compatible agents of netwerkmonitoring via tools zoals Suricata of Zeek. Binnen deze werkende testomgeving wordt de centrale logverzameling voor een selectie van de legacy systemen veilig opgezet, zonder de stabiliteit van deze fragiele systemen in gevaar te brengen. Onderdeel van deze PoC is tevens het inrichten van een SIEM-dashboard en het ontwikkelen van specifieke detectieregels en waarschuwingen (alerts) die gericht zijn op de kwetsbaarheden van legacy systemen. Het uiteindelijke eindproduct is een gedetailleerd adviesrapport. Dit rapport bevat een evaluatie van de PoC en een concrete aanbeveling voor de definitieve inrichting van de 'SOC stack' voor productief gebruik binnen de organisatie. De persoonlijke leerdoelen voor deze stage omvatten het opdoen van praktische ervaring met logmanagement en SIEM in een complexe omgeving, evenals het leren vertalen van beveiligingsrisico's in out-of-support omgevingen naar effectieve en functionele monitoring-eisen.

4. Business Case

Het op korte termijn vervangen van alle legacy systemen binnen de organisatie is financieel of technisch momenteel niet haalbaar. Echter, zonder actieve monitoring vormen deze systemen een blinde vlek binnen het netwerk en vormen ze een potentieel makkelijke ingang voor cyberaanvallen. Dit project voegt aanzienlijke waarde toe doordat het, door middel van centrale logging en monitoring, deze blinde vlek wegneemt. Dit zorgt voor een sterk verbeterde zichtbaarheid en een aanzienlijke risicoreductie, mogelijke incidenten kunnen veel sneller en accurater worden gedetecteerd, wat de impact van een eventuele aanval drastisch verkleint. Bovendien draagt het project direct bij aan de bedrijfscontinuïteit, omdat het de organisatie in staat stelt om de levensduur van noodzakelijke, maar verouderde systemen op een verantwoorde en veilige manier te verlengen. Tot slot vormen de inzichten en technische keuzes die voortkomen uit de Proof-of-Concept een waardevolle blauwdruk en sterke fundering voor de toekomstige inrichting van het Security Operations Center (SOC) van de organisatie.

5. Planning

Fase 1 Onderzoek & Project Plan (week 1 – 2)

- In kaart brengen van de legacy systemen, het netwerk en de huidige logging-mogelijkheden.
- Uitwerken van de benodigde virtuele machines voor de PoC.
- Mijlpaal: Goedkeuring op het technische ontwerp en de use cases.

Fase 2 Opzetten Basis Infrastructuur (week 3 - 4)

- Voorbereiden en inrichten van de benodigde virtuele machines voor de testomgeving.
- Installeren van de lokale (on-premise) SIEM-omgeving veilig binnen het afgesloten netwerk.
- Installeren van een MISP server voor Threat Intel.

Fase 3 Log Ingestie & SIEM Configuratie (week 5 - 8)

- Uitrollen van log-collectors op geselecteerde legacy systemen.
- Normaliseren van de logdata, bouwen van dashboards en configureren van specifieke detectieregels.
- Beginnende SOAR active response modules maken.
- Installeren van extra SIEM-omgeving voor switches en heel oude systemen.
- Mijlpaal: Werkende centrale logverzameling en succesvolle detectie van de use cases binnen de proof-of-concept.

Fase 4 SOAR & SIRP Integratie (week 9 - 10)

- Installeren en integreren van eigen applicatie met het systeem.
- Opzetten van een geautomatiseerde waarschuwings- en ticket workflow, zonder direct geautomatiseerd in te grijpen op de kwetsbare legacy systemen.
- Mijlpaal: De volledige incident-workflow is operationeel (een gesimuleerde aanval genereert nu automatisch een overzichtelijk ticket voor de analist).

Fase 5 Rapportage & Afronding (week 11 - 12)

- Volledig testen van de opgezette omgeving en het evalueren van de resultaten.
- Schrijven van het uiteindelijke adviesrapport voor de productieve inzet van de SOC-stack.
- Mijlpaal: Definitieve oplevering van het adviesrapport en de eindpresentatie aan de organisatie.

6. Status Report

Via mondelinge communicatie in de ochtend overleggen we wat ik vandaag allemaal ga doen en vertel ik wat ik de dag ervoor heb gedaan. Ook gebruik ik Confluence om mijn research op te schrijven. Later tijdens de realisatie fase ga ik ook Jira gebruiken om issues aan te maken voor het bouwen van de SOC.

7. Legende

SIEM (Security Information and Event Management): Een centraal systeem dat loggegevens uit het hele netwerk verzamelt, normaliseert, correleert en analyseert om beveiligingsincidenten te detecteren en hier waarschuwingen (alerts) voor te genereren.

SIRP (Security Incident Response Platform): Een applicatie die fungeert als 'case management' of ticketsysteem, speciaal gebouwd voor beveiligingsanalisten om incidenten gestructureerd te documenteren en af te handelen.

SOAR (Security Orchestration, Automation and Response): Een systeem dat beveiligingsprocessen en workflows automatiseert. Het koppelt verschillende tools aan elkaar en kan bijvoorbeeld automatisch data verrijken of tickets aanmaken.

SOC (Security Operations Center): Het team, de processen en de technologieën binnen een organisatie die verantwoordelijk zijn voor het continu monitoren, detecteren en afhandelen van cyberdreigingen.

VM (Virtual Machine): Een virtuele computer/server die als software draait op een fysieke server. Binnen dit project gebruikt om de verschillende applicaties veilig op te hosten.

PoC (Proof-of-Concept): Een praktische, afgebakende proefopstelling om aan te tonen dat een bedacht concept (zoals de gekozen SOC-stack) in de realiteit echt werkt.

Legacy Systeem: Verouderde hard- of software (zoals Windows Server 2008 of Windows XP) die geen beveiligingsupdates meer ontvangt (End-of-Life), maar nog wel essentieel is voor de bedrijfsvoering.