# Bijlage 7
# Optionele functionele eisen en wensen voor SOC-SIEM
# Openbare Europese aanbesteding

Digitale Werkplek & IT-dienstverlening
ten behoeve van de Vervoerregio Amsterdam

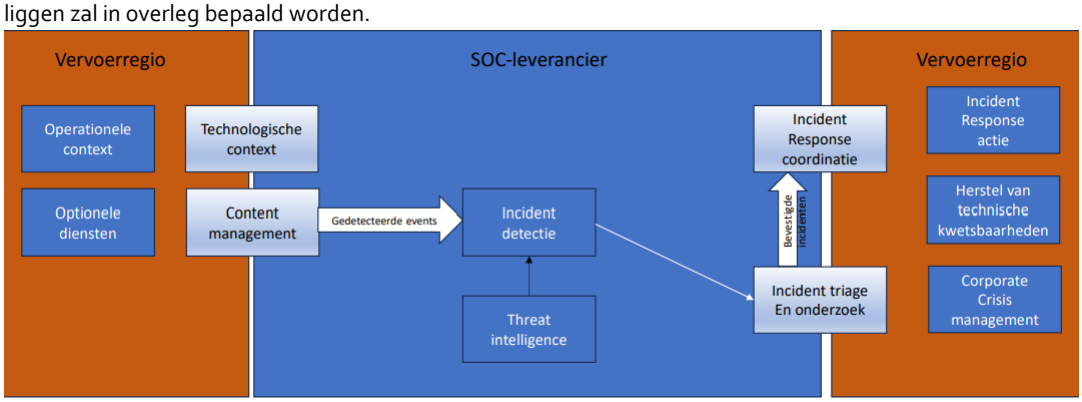
De in deze bijlage opgenomen functionele eisen en wensen zijn optioneel. Inschrijvers kunnen het maximale aantal punten voor dit onderdeel verdienen door hieraan te voldoen. Indien een inschrijver niet volledig aan deze optionele eisen voldoet, zal dit leiden tot een lagere score op onderdeel 2.

Vervoerregio Amsterdam

# Inhoudsopgave

## 1 FUNCTIONELE SCOPE

Vervoerregio wil security monitoring op een hybride wijze inrichten waarbij functies (gedeeltelijk) worden uitbesteed naar de Inschrijver. Vervoerregio zal interne capaciteiten ontwikkelen voor het IT- domein (en optioneel het OT-domein), om adequate opvolging te kunnen geven aan gedetecteerde potentiële incidenten door het Managed SOC. Deze verdeling van verantwoordelijkheden is schematisch weergegeven in het schema hieronder. Hoe de grenzen tussen de partijen precies zullen liggen zal in overleg bepaald worden.




In de onderstaande tabel worden de verschillende onderdelen beschreven, evenals wie verantwoordelijk is voor elk onderdeel:

| Onderdeel | Omschrijving | Toebedeeld aan |
|---|---|---|
| **Threat Intelligence** | Threat Intelligence (TI) is het verzamelen/verspreiden/delen van op feiten gebaseerde informatie over dreigingen (IoC's), met als doel om het ontstane risico zo snel mogelijk af te dekken en mogelijke schade tot een minimum te beperken.<br><br>De Inschrijver zal 24 * 7 de informatievergaring van en initiële normalisatie, correlatie en analyse op deze informatie uitvoeren. Op basis van deze analyse kunnen (additionele) security monitoring rules worden bepaald die dienen te worden geïmplementeerd in het gebruikte analyticsplatform.<br><br>Geanalyseerde intelligence dient te leiden tot proactieve maatregelen voor het landschap van de Vervoerregio, teneinde security incidenten te voorkomen. De uitvoering van deze maatregelen dienen door óf in opdracht van Vervoerregio uitgevoerd te worden. | Inschrijver |
| **Technologi-sche Context** | De Inschrijver dient informatie van het technologische landschap tot haar beschikking te hebben om de taken efficiënt en effectief te kunnen uitvoeren. Gedurende operatie zal het ook kunnen zijn dat door ervaring en lessons learned zij informatie kan toevoegen aan deze technologische context, bijvoorbeeld doordat zij meer inzage heeft in het landschap of specifieke systemen dan momenteel is vastgelegd binnen Vervoerregio. Vervoerregio is primair verantwoordelijk voor het (initieel) opstellen, beschikbaar maken en up-to-date houden van deze informatie. De Inschrijver is verantwoordelijk voor het aangeven welke informatie zij nodig heeft voor het effectief en efficiënt kunnen uitvoeren van haar taken, en voor het up-to-date blijven met deze informatie. | Inschrijver & Vervoerregio |
| **Operationele Context** | De Inschrijver dient context over (kritieke) bedrijfsprocessen, projecten, systemen en applicaties tot haar beschikking te hebben om de overige taken efficiënt en effectief te kunnen uitvoeren. Gedurende operatie zal het ook kunnen zijn dat door ervaring en lessons learned zij informatie kan toevoegen aan deze context. Vervoerregio is echter verantwoordelijk voor het (initieel) opstellen, beschikbaar maken en up-to-date houden van deze informatie. De Inschrijver is verantwoordelijk voor het aangeven welke informatie zij nodig heeft voor het effectief en efficiënt kunnen uitvoeren van haar taken, en voor het up-to-date blijven met deze informatie. | Vervoerregio |
| **Content management** | Vervoerregio is zelf verantwoordelijk voor de eindsystemen die als bronnen zullen dienen (de te monitoren objecten) en Vervoerregio zal derhalve de configuratie van | Inschrijver & Vervoerregio |

| | | |
|---|---|---|
| | die systemen instellen zodat de juiste data bij de Inschrijver komt om vervolgens analyse en detectie te kunnen uitvoeren (op basis van de door Threat Intelligence, Technologische Context en Operationele Context gedefinieerde Use Cases / detectiescenario's, en zoals benodigd voor de technologie zoals door de Inschrijver gebruikt wordt.<br><br>Echter, het bepalen van de type en hoeveelheid informatie die benodigd is evenals het beheren en normaliseren van deze informatie zodra deze bij de security monitoring oplossing aankomt, als ook het mede opstellen van de Use Cases / detectiescenario's, filters en analytics en deze technisch implementeren teneinde Incident Detection te kunnen uitvoeren is de verantwoordelijkheid van de Inschrijver. | |
| **Incident Detectie** | Op basis van de (mede door Threat Intelligence opgestelde) Use Cases zal de Inschrijver verzorgen dat op de aangeleverde data (zoals in Content Management bepaald) de juiste analyses worden uitgevoerd, zodat alerts worden gegenereerd met zo min mogelijk false positives. | Inschrijver |
| **Incident Triage & Onderzoek** | Zodra er (in Incident Detection) alerts worden gegenereerd zal de Inschrijver de eerstelijns functie en (voor het IT-domein en optioneel het OT-domein) tweedelijns functie vervullen, en derhalve de eerste analyses op deze alerts uitvoeren. In het geval geverifieerde incidenten worden gedetecteerd (Indicators of Compromise) worden deze geëscaleerd naar de Vervoerregio security incident coördinator, die verantwoordelijk is voor de afhandeling van security incidenten.<br>Wanneer na de analyse van de Inschrijver niet met zekerheid een false positive kan worden uitgesloten noch een geverifieerd incident, zal de Inschrijver Events of Interest doorsturen naar de security incident coordinator binnen de Vervoerregio. Hier zal bij enige twijfel het incident doorgestuurd worden. Deze rol wordt vervuld door de security incident coördinator, die deze events of interest ter analyse intern doorstuurt. Deze tweedelijns functie binnen Vervoerregio dient eveneens toegang te hebben tot het door de Inschrijver gebruikte analyticsplatform om zelf eigen triage te kunnen uitvoeren. | Inschrijver & Vervoerregio |
| **Incident Response Coördinatie** | Vervoerregio is zelf verantwoordelijk voor de coördinatie van de uitvoer van het security incident response proces en onderliggende stappen. Echter, Inschrijver zal adviseren over te nemen stappen en eveneens vanuit haar optiek erop toezien dat geïdentificeerde incidenten daadwerkelijk worden gesloten. | Vervoerregio & Inschrijver |
| **Incident Response Actie** | Incident Response Actie is het daadwerkelijk uitvoeren van security incident response plannen en het nemen van acties om business impact te minimaliseren. Vervoerregio is verantwoordelijk voor de uitvoer van deze acties. Echter wil Vervoerregio graag playbooks en scenario's opstellen waarbij er baat is bij het snel en autonoom handelen van de Inschrijver. Hierbij is te denken aan het isoleren van incidenten door bepaalde werkplekken waar mogelijk gebruik makend van Vervoerregio' servicemanagement of SOAR-oplossing. De details hieromtrent zijn nader te bepalen door Vervoerregio in samenwerking met de Inschrijver. | Vervoerregio |

## 2 OPTIONELE DIENSTEN

Vervoerregio voorziet een aantal potentiële uitbreidingen op de functionele scope van de opdracht. De keuze of deze diensten daadwerkelijk worden afgenomen wordt vóór afronding van implementatie Fase 2 gemaakt. Vervoerregio behoudt zich het recht voor om ieder van deze optionele diensten niet af te nemen en Vervoerregio behoudt zich het recht voor om ieder van deze diensten door een andere partij dan Inschrijver te laten leveren.

De volgende diensten zijn optionele functionele scope:

- Vulnerability Management
- Threat Hunting
- Endpoint Detection & Response (EDR)

## 2.1 Vulnerability Management

Vulnerability Management omvat het periodiek identificeren en classificeren van kwetsbaarheden op het gebied van informatiebeveiliging. Deze identificatie wordt gedaan door de omgeving van Vervoerregio te scannen naar bekende kwetsbaarheden.
Op dit moment wordt binnen Vervoerregio gedacht aan:

- Een Vulnerability Systeem (voor de interne netwerken);
- Diverse logbronnen van leveranciers en overige bronnen zoals bijv. NCSC.

Binnen deze optionele dienst verwacht Vervoerregio het volgende:

- Volledige zichtbaarheid op alle bekende kwetsbaarheden in de IT omgeving van Vervoerregio;
- Realtime dashboard/rapportage waarin de gevonden kwetsbaarheden en toegekende classificatie inzichtelijk is;
- Aanbevelingen voor remediering van de kwetsbaarheden, dan wel alternatieve mitigerende maatregelen in het geval er geen daadwerkelijke oplossing beschikbaar is.

## 2.2 Threat Hunting

Threat Hunting is een actieve (cyber)security activiteit, waarbij proactief wordt gezocht naar geavanceerde bedreigingen ten aanzien van het landschap van Vervoerregio. Deze actie is aanvullend op de meer passieve bedreigingen analyses op basis van analyses en het scannen naar bekende kwetsbaarheden.
Het tijdig kunnen detecteren van onbekende kwetsbaarheden, het onderkennen van verdacht gedrag en het onderscheiden van nieuwe/onverwachte communicatiepatronen is belangrijke toevoeging in het portfolio van beschermingsmaatregelen.
Binnen deze dienst verwacht Vervoerregio het volgende:

- Moderne, op Artificial Intelligence (AI) gebaseerde, detectie;
- Signalering over potentiële aanvallen, waardoor Vervoerregio een hoge bescherming tegen zogenaamde "zero day" en "Advanced persistent threat" scenario's bereikt;
- Realtime dashboard/rapportage waarin de gevonden kwetsbaarheden en toegekende classificatie inzichtelijk is;
- Aanbevelingen voor remediëring van de kwetsbaarheden, dan wel alternatieve mitigerende maatregelen in het geval er geen daadwerkelijke oplossing beschikbaar is.

## 2.3 EndPoint Detection & Response

Endpoint Detection & Response (EDR) is de set aan tools en maatregelen die worden gebruikt om eindpunten (computerhardware) in een ICT omgeving te beschermen tegen bedreigingen. De tooling wordt geïnstalleerd op het apparaat van de eindgebruikers en de monitoring data wordt centraal opgeslagen en geanalyseerd. Bij detectie van een aanval worden onmiddellijk maatregelen genomen om het apparaat te isoleren.

Binnen deze dienst verwacht Vervoerregio het volgende:

- Bewaking van de apparaten van eindgebruikers, ook als deze geen actieve netwerkverbinding met de Vervoerregio omgeving hebben;
- Detectie van wijzigingen en activiteiten op de apparaten, die een bedreiging voor Vervoerregio kunnen opleveren;
- Realtime dashboard/rapportage waarin de gevonden kwetsbaarheden en toegekende classificatie inzichtelijk is;
- Maatregelen op het apparaat om een aanval te stoppen en de impact te minimaliseren.