

Bijlage 02

Programma van Wensen

Ten behoeve van marktconsultatie

Behorend bij

Raamovereenkomst Security Operations Center (SOC)

Status : Concept
Versie : 260430-1
Datum : 30-04-2026

Inhoudsopgave

1	Inleiding	3
1.1.1	Basis - Monitoring & detectie	3
1.1.2	Basis - Beveiligingsincident response	3
1.1.3	Basis - Threat intelligence	6
1.1.4	Basis - Rapportage & dashboards	6
1.1.5	Basis - Use case management	6
1.1.6	Basis - Knowledge transfer	6
2	Optionele / aanvullende diensten	6
2.1	Optioneel - Vulnerability Management	6
2.2	Optioneel - Situational awareness	6
2.3	Optioneel - Threat hunting	7
2.4	Optioneel - Forensics	7
2.5	Optioneel - Tabletop	7
2.6	Optioneel - Uitrol sensoren	8

1 Inleiding

Deze bijlage bevat een programma van wensen met betrekking tot de mogelijke inrichting en doorontwikkeling van de SOC-dienstverlening. De wensen zijn bedoeld als verkenning van functionaliteiten en innovaties die kunnen bijdragen aan een effectieve, toekomstbestendige en hoogwaardige SOC-dienst.

In het kader van de marktconsultatie worden marktpartijen uitgenodigd om te reflecteren op deze wensen en aan te geven in hoeverre deze naar hun oordeel zinnig, haalbaar, onderscheidend en doelmatig zijn. Daarbij wordt tevens gevraagd eventuele alternatieve oplossingsrichtingen of aandachtspunten te benoemen.

De wensen hebben onder meer betrekking op geavanceerde detectietechnieken, automatisering, dataverrijking, dashboards, threat intelligence en kennisdeling. De uitkomsten van de marktconsultatie kunnen door Opdrachtgever worden gebruikt bij de verdere uitwerking van de aanbestedingsdocumenten.

1.1.1 Basis - Monitoring & detectie

1 Security monitoring

Wensen	
W1	Geavanceerde detectietechnieken
	Opdrachtnemer maakt gebruik van geavanceerde detectietechnieken, waaronder gedragsmodellen en machine-learning gebaseerde analysemethoden. Indien deze technieken (deels) niet worden toegepast, licht Opdrachtnemer schriftelijk toe welke alternatieve methoden worden ingezet om een gelijkwaardig detectieniveau te waarborgen.
	<i>Doel:</i> Versterken van detectiecapaciteit en vroegtijdige identificatie van afwijkend gedrag en geavanceerde dreigingen
	<i>Resultaat:</i> Inzicht voor Deelnemer in toegepaste detectietechnieken en alternatieve methoden, inclusief onderbouwing van effectiviteit.

1.1.2 Basis - Beveiligingsincident response

2 Incident response

2.1 Eventmanagement

2.2 Incidentmanagement

2.3 CSIRT activatie

1.1.2.1 Basis - Event management

2.1 Eventmanagement

Wensen	
W2	Eventkwaliteit en filtering
	De Opdrachtnemer detecteert automatisch "noisy" logbronnen en genereert voorstellen voor fine tuning en sanering, zodat eventstromen consistent en betrouwbaarder worden. De Opdrachtnemer past machine learning toe voor dynamische suppressie van false positives, zonder verlies van context, en hanteert vooraf gedefinieerde kwaliteitsscores per eventtype (bijv. completeness, fidelity, relevance). De Opdrachtnemer correleert automatisch gerelateerde events tot samengestelde "event clusters", zodat anomalieën sneller inzichtelijk zijn.
	<i>Doel:</i> Verbeteren van de betrouwbaarheid, consistentie en bruikbaarheid van binnenkomende events door automatisch identificeren en optimaliseren van "noisy" logbronnen, false positives te reduceren en gerelateerde events te clusteren.
	<i>Resultaat:</i> Eventstromen zijn consistent en betrouwbaarder; afwijkingen en anomalieën worden sneller zichtbaar en bruikbaar voor analyse.
W3	Eventverrijking en contextualisering
	De Opdrachtnemer verrijkt events automatisch met aanvullende context, waaronder asset criticality, CMDB-data, geolocatie, gebruikersprofielen, OSINT-indicatoren en MITRE ATT&CK-tags, zodat events nauwkeuriger kunnen worden beoordeeld. De Opdrachtnemer voert inline risico-inschattingen uit (Low/Medium/High/Severe) op basis van gedrags- en contextgegevens. De Opdrachtnemer koppelt events aan businessprocessen om de potentiële impact direct inzichtelijk te maken.
	<i>Doel:</i> Verhogen van de kwaliteit van eventanalyse door events automatisch te verrijken met relevante contextinformatie, risico-inschattingen en koppelingen aan businessprocessen.
	<i>Resultaat:</i> Events kunnen sneller en nauwkeuriger worden beoordeeld; de impact op kritieke processen is direct inzichtelijk.
W4	Optimalisatie van eventstromen
	De Opdrachtnemer levert near-real-time dashboards (< 5 seconden latency) voor eventvolumes, trends en anomalieën, inclusief visualisatie van eventflows per technologie, business unit of logbron. De Opdrachtnemer detecteert eventgaps en meldt ontbrekende logs direct, en gebruikt predictive analytics om toekomstige eventvolumes op basis van historische data te voorspellen.
	<i>Doel:</i> Continu inzicht en overzicht in eventvolumes, trends en anomalieën bieden door near-real-time dashboards, detectie van ontbrekende logs en voorspellende analyses.
	<i>Resultaat:</i> Eventstromen worden proactief gemonitord en beheerd; potentiële hiaten en toekomstige volumes worden tijdig gesignaleerd.

1.1.2.2 Basis - Beveiligingsincident management

2.2 Incidentmanagement

Wensen	
W5	Voorspellende Beveiligingsincidentdetectie
	De Opdrachtnemer levert voorspellende incidentdetectie op basis van AI- en machine-learningtechnieken, waarmee potentiële Beveiligingsincidenten vroegtijdig kunnen worden geïdentificeerd voordat deze zich voordoen. Deze functionaliteit maakt aantoonbaar onderdeel uit van het detectie- en preventieproces zoals vastgelegd in de SLA.
	<i>Doel:</i> Vroegtijdig identificeren van potentiële Beveiligingsincidenten door toepassing van AI- en machine-learningtechnieken, zodat risico's proactief kunnen worden beheerd.
	<i>Resultaat:</i> Potentiële Beveiligingsincidenten worden gedetecteerd voordat deze daadwerkelijk plaatsvinden; de detectiefunctie is aantoonbaar onderdeel van het afgesproken detectie- en preventieproces.
W6	Geautomatiseerde root-causeanalyse
	De Opdrachtnemer levert geautomatiseerde root-causeanalyse waarmee de onderliggende oorzaak van Beveiligingsincidenten automatisch wordt vastgesteld, met als doel het versnellen en verbeteren van het herstelproces. De geautomatiseerde root-causeanalyse is geïntegreerd in het incidentanalyse- en herstelproces zoals beschreven in de SLA.
	<i>Doel:</i> Versnellen en verbeteren van het herstelproces door automatisch de onderliggende oorzaken van Beveiligingsincidenten vast te stellen.
	<i>Resultaat:</i> De oorzaak van Beveiligingsincidenten wordt automatisch geïdentificeerd en geïntegreerd in het analyse- en herstelproces, waardoor reactietijden en oplossingskwaliteit verbeteren.
W7	Automatische dreigingsverrijking van incidenten
	De Opdrachtnemer verrijkt Beveiligingsincidenten automatisch met actuele dreigingsinformatie door middel van een geïntegreerde threat-intelligencekoppeling, zodat Beveiligingsincidenten sneller en nauwkeuriger kunnen worden geduid.
	<i>Doel:</i> Verbeteren van de nauwkeurigheid en snelheid van incidentanalyse door automatische verrijking van Beveiligingsincidenten met actuele dreigingsinformatie via een geïntegreerde threat-intelligencekoppeling.
	<i>Resultaat:</i> Beveiligingsincidenten kunnen sneller en accurater worden beoordeeld, waardoor prioritering, escalatie en mitigatie effectiever verlopen.

1.1.2.3 Basis - CSIRT activatie

2.3 CSIRT activatie

Geen wensen benoemd.

*1.1.3 Basis - Threat intelligence***3 Threat intelligence**

Wensen	
W8	Certificeringen zoals CTIA, GCTI of vergelijkbaar zijn een pré.

*1.1.4 Basis - Rapportage & dashboards***4 Rapportage en dashboarding**

Geen wensen benoemd.

*1.1.5 Basis - Use case management***5 Use case management**

Wensen	
W9	Certificeringen zoals SIEM Engineer, GCIA of vergelijkbaar zijn een pré.

*1.1.6 Basis - Knowledge transfer***6 Knowledge transfer**

Wensen	
W10	Opdrachtnemer biedt een online kennisplatform met actuele informatie, best practices en FAQ's.

2 Optionele / aanvullende diensten**2.1 Optioneel - Vulnerability Management**

Wensen	
W11	Opdrachtnemer stelt een real-time vulnerability dashboard beschikbaar met inzicht in het vulnerability management per Deelnemer.
W12	Opdrachtnemer stelt een real-time vulnerability dashboard beschikbaar met inzicht in het vulnerability management van alle Deelnemers.

2.2 Optioneel - Situational awareness

Wensen	
--------	--

W13	Opdrachtnemer gebruikt AI/ML-technieken voor detectie van afwijkende patronen.
W14	Gebruikers kunnen zelf filters, dashboards, zoekopdrachten en meldingsinstellingen configureren zónder tussenkomst van de Opdrachtnemer.

2.3 Optioneel - Threat hunting

Geen wensen benoemd.

2.4 Optioneel – Forensics

Geen wensen benoemd.

2.5 Optioneel – Tabletop

Wensen	
W15	Gebruik tooling Deelnemer
	Opdrachtnemer maakt tijdens tabletop-simulaties en oefeningen gebruik van door Deelnemer beschikbaar gestelde tooling, waaronder ten minste SIEM- en SOAR-platformen, teneinde realistische en praktijkgerichte scenario's te ondersteunen.
W16	Scenario-varianten en stress-tests
	Opdrachtnemer levert aanvullende scenario-varianten die inspelen op zeldzame, complexe of gecombineerde dreigingen, inclusief stress-testsituaties om besluitvorming en samenwerking onder hoge druk te evalueren.
W17	Cross-Deelnemer oefeningen
	Opdrachtnemer faciliteert tabletop-oefeningen waarbij meerdere Deelnemers gezamenlijk deelnemen, met focus op ketenafstemming en gezamenlijke besluitvorming bij incidenten die meerdere partijen raken.
W18	Digitale en interactieve oefenomgevingen
	Opdrachtnemer levert digitale, interactieve platforms of simulaties ter ondersteuning van de tabletop, zodat Deelnemers in een gecontroleerde omgeving beslissingen kunnen nemen en direct feedback krijgen.
W19	Trend- en benchmarkrapportages
	Opdrachtnemer levert periodieke analyses waarin lessons learned van meerdere tabletop-oefeningen worden gebundeld, inclusief trends, verbeterpunten en benchmarking ten opzichte van eerdere oefeningen of andere Deelnemers.
W20	Trainingsmateriaal en scenario-gidsen
	Opdrachtnemer verstrekt ondersteunend materiaal, zoals handleidingen, scenario-gidsen en best practices, voor Deelnemers die tabletop-oefeningen voorbereiden of intern willen repliceren.
W21	Opvolging van verbeteracties
	Opdrachtnemer levert een gestructureerd overzicht van voorgestelde verbeteracties per oefening, inclusief status van implementatie en aanbevelingen voor verdere optimalisatie van processen en procedures.

2.6 Optioneel - Uitrol sensoren

Geen wensen benoemd.