

Bijlage 02a

Specificatie van de Prestatie | Diensten

Programma van Eisen

Behorend bij

Raamovereenkomst Security Operations Center (SOC)

Status : Definitief
Versie : 1.0
Datum : 06-08-2026

Inhoudsopgave

1	Inleiding	3
1.1	Intellectuele eigendomsrechten (IP) en overdraagbaarheid.....	3
1.2	Toelichting bij SLA-parameters (KPI's)	4
1.3	Overkoepelende rapportage-eis.....	5
1.4	Service Credit regime	6
2	Diensten.....	8
2.1	Algemeen.....	8
3	Basis SOC-diensten	10
3.1	Basis - Monitoring & detectie	11
3.2	Basis - Beveiligingsincident response	20
3.2.1	Basis - Event management	20
3.2.2	Basis - Beveiligingsincident management.....	23
3.2.3	Basis - CSIRT activatie	31
3.3	Basis - Threat intelligence	35
3.4	Basis - Rapportage & dashboards	39
3.5	Basis - Use case management	42
3.6	Basis - Knowledge transfer	47
4	Optionele / aanvullende diensten	52
4.1	Optioneel - Vulnerability Management.....	53
4.2	Optioneel - Situational awareness	57
4.3	Optioneel - Threat hunting	63
4.4	Optioneel - Forensics.....	66
4.5	Optioneel - Tabletop.....	70
4.6	Optioneel - Uitrol sensoren	73
5	Implementatie.....	78
	Bijlage A - SLA-overzicht per dienst (SOC)	82

1 Inleiding

Deze bijlage beschrijft de Eisen ten aanzien van de door Opdrachtnemer te leveren SOC-dienstverlening. De Eisen hebben betrekking op de functionele en operationele aspecten van de dienstverlening, waaronder de uit te voeren activiteiten, processen, verantwoordelijkheden en de wijze waarop Opdrachtnemer invulling geeft aan de gevraagde diensten.

De in deze bijlage opgenomen Eisen zijn in beginsel generiek van aard. Dit betekent dat deze Eisen van toepassing zijn op alle door Opdrachtnemer te leveren diensten binnen de scope van de Raamovereenkomst en voor alle Deelnemers die gebruikmaken van de dienstverlening, tenzij expliciet anders is aangegeven of de aard van een specifieke Eis anders vereist.

Opdrachtnemer dient de dienstverlening uit te voeren in overeenstemming met de in deze bijlage opgenomen Eisen en in samenhang met de architectuurvereisten zoals opgenomen in Bijlage 2b (Architectuur) en de kwaliteits- en prestatie-eisen zoals opgenomen in Bijlage 2c (Kwaliteits- en prestatie-eisen).

Voorts wordt Opdrachtnemer nadrukkelijk gewezen op de samenhang met de in Bijlage 2c (Kwaliteits- en prestatie-eisen) opgenomen financiële en contractuele uitgangspunten. In dat kader geldt dat Opdrachtnemer niet gerechtigd is kosten in rekening te brengen die niet expliciet zijn opgenomen in de overeengekomen Tarieflijst. Alle kosten die redelijkerwijs noodzakelijk zijn voor de uitvoering van de in deze bijlage beschreven dienstverlening dienen volledig te zijn verdisconteerd in de overeengekomen Tarieven. Dit uitgangspunt is onlosmakelijk verbonden met de in deze bijlage opgenomen Eisen en dient door Opdrachtnemer te worden betrokken bij de inrichting, uitvoering en doorontwikkeling van de SOC-dienstverlening.

1.1 Intellectuele eigendomsrechten (IP) en overdraagbaarheid

De SOC-dienstverlening die Deelnemers afnemen wordt bekostigd met publiek geld. Vanuit dit uitgangspunt streeft Opdrachtgever ernaar dat de resultaten die tijdens de uitvoering van de Prestatie worden ontwikkeld, waar mogelijk, beschikbaar komen als open en gemeenschappelijk bruikbare resultaten binnen de overheid. Deze resultaten dienen niet onnodig te worden beperkt door beperkingen voortvloeiend uit intellectuele eigendomsrechten van Opdrachtnemer of derden, voor zover dit redelijkerwijs mogelijk is en binnen de kaders van toepasselijke wet- en regelgeving.

Opdrachtgever onderkent dat Opdrachtnemer gebruik kan maken van bestaande intellectuele eigendomsrechten en generieke bouwstenen. Dit laat onverlet dat Opdrachtgever en Deelnemers beschikken over volledige, niet-exclusieve, eeuwigdurende en overdraagbare gebruiksrechten op alle resultaten, configuraties, detectieregels, use cases, automatiseringen en documentatie die in het kader van de dienstverlening worden ontwikkeld of toegepast binnen de omgeving van de Deelnemer. Deze rechten omvatten in ieder geval het recht tot gebruik, wijziging, hergebruik en overdracht aan andere overheidsorganisaties of een opvolgende opdrachtnemer.

Architectuuruitgangspunt en uitvoering van detectie

Uitgangspunt binnen deze aanbesteding is dat de SOC-dienstverlening primair wordt uitgevoerd binnen de SIEM-omgeving van de Deelnemer. Opdrachtnemer richt detectieregels, use cases, correlatieregels en automatiseringen in en voert deze uit binnen deze omgeving.

Het structureel uitvoeren van detectie, correlatie of use case-verwerking buiten de SIEM-omgeving van de Deelnemer (bijvoorbeeld in een eigen platform of oplossing van Opdrachtnemer) is uitsluitend toegestaan indien:

- dit aantoonbaar noodzakelijk is voor de betreffende dienst; en
- dit vooraf expliciet en schriftelijk is overeengekomen met Opdrachtgever of de betreffende Deelnemer.

Structurele extractie of duplicatie van logdata, events of securitydata naar systemen buiten de SIEM-omgeving van de Deelnemer is niet toegestaan, tenzij dit noodzakelijk is voor een

overeengekomen aanvullende dienst. In dergelijke gevallen blijft de eigendom, controle en overdraagbaarheid van de detectielogica en resultaten geborgd conform deze bepaling.

Onderscheid standaard en maatwerk

In aanvulling hierop wordt onderscheid gemaakt tussen:

- generieke (standaard) detectieregels en use cases van Opdrachtnemer; en
- detectieregels en use cases die specifiek voor Opdrachtgever en/of Deelnemers worden ontwikkeld of aangepast.

Voor alle detectieregels en use cases die specifiek voor Opdrachtgever en/of Deelnemers zijn ontwikkeld of aangepast, geldt dat:

- Opdrachtgever en Deelnemers een onbeperkt, niet-exclusief, eeuwigdurend en overdraagbaar gebruiksrecht verkrijgen;
- deze detectieregels en use cases bij beëindiging van de overeenkomst volledig overdraagbaar zijn aan Opdrachtgever en/of een opvolgende opdrachtnemer;
- Opdrachtnemer zorgdraagt voor volledige, actuele documentatie en exporteerbaarheid in een gangbaar en herbruikbaar formaat, zodanig dat feitelijke overdracht en herimplementatie mogelijk is.

Opdrachtnemer zal detectieregels en use cases die inhoudelijk zijn afgestemd op de specifieke risico's, architectuur, dreigingscontext of bedrijfsprocessen van Opdrachtgever en/of Deelnemers niet aanmerken als generieke standaardcomponenten met als doel overdraagbaarheid te beperken.

Ten aanzien van generieke detectieregels en use cases van Opdrachtnemer, die niet specifiek voor Opdrachtgever en/of Deelnemers zijn ontwikkeld en uitsluitend binnen de eigen oplossing van Opdrachtnemer worden toegepast, geldt dat:

- het intellectueel eigendom bij Opdrachtnemer blijft;
- Opdrachtgever en Deelnemers gedurende de looptijd beschikken over een gebruiksrecht voor zover noodzakelijk voor de dienstverlening;
- geen overdracht van eigendom wordt geëist.

Overdraagbaarheid en exit

Opdrachtnemer waarborgt dat bij beëindiging van de overeenkomst de volledige operationele detectiecapaciteit, inclusief detectieregels, use cases, automatiseringen en configuraties, zonder significante functionele achteruitgang kan worden overgenomen door Opdrachtgever of een opvolgende opdrachtnemer.

Opdrachtnemer zorgt ervoor dat maatwerk detectieregels en use cases tooling-onafhankelijk of tooling-migreerbaar worden vastgelegd, tenzij aantoonbaar niet mogelijk.

Opdrachtnemer werkt actief en volledig mee aan een zorgvuldige overdracht, inclusief kennisoverdracht, documentatie en ondersteuning bij herimplementatie.

Transparantie en verantwoording

Opdrachtnemer verstrekt inzicht in de werking en effectiviteit van de toegepaste detectieregels en use cases, onder meer door:

- rapportages over detectiekwaliteit en effectiviteit;
- mapping naar gangbare en actuele frameworks (bijv. MITRE ATT&CK);
- inzicht in dekking en eventuele hiaten.

1.2 Toelichting bij SLA-parameters (KPI's)

Opdrachtgever respectievelijk de Deelnemer onderkent dat het behalen van de overeengekomen SLA-parameters binnen de SOC-dienstverlening in veel gevallen afhankelijk is van factoren die (mede) buiten de directe invloedssfeer van Opdrachtnemer liggen, waaronder de kwaliteit,

volledigheid en tijdigheid van aangeleverde data, de beschikbaarheid van bronsystemen, en handelingen of wijzigingen binnen de omgevingen van Opdrachtgever en de Deelnemers.

Het niet behalen van een SLA-parameter kwalificeert derhalve niet zonder meer als een toerekenbare tekortkoming van Opdrachtnemer. Van een tekortkoming is uitsluitend sprake voor zover het niet behalen van de SLA-parameter aantoonbaar is toe te rekenen aan handelen of nalaten van Opdrachtnemer.

In alle gevallen waarin een SLA-parameter niet wordt gerealiseerd, ongeacht de toerekenbaarheid, geldt dat Opdrachtnemer:

- een root cause analyse (RCA) uitvoert naar de onderliggende oorzaak of oorzaken;
- de uitkomsten hiervan transparant deelt met Opdrachtgever respectievelijk de Deelnemer;
- een concreet, navolgbaar en toetsbaar verbeterplan opstelt gericht op het voorkomen van herhaling;
- in afstemming met Opdrachtgever nadere mitigerende maatregelen en/of aanvullende afspraken vastlegt.

Indien uit de root cause analyse blijkt dat het niet behalen van de KPI (mede) wordt veroorzaakt door factoren binnen de invloedsfeer van Opdrachtgever en/of de Deelnemers, treden partijen in overleg om:

- passende maatregelen te treffen; en
- waar nodig de onderliggende randvoorwaarden, werkwijzen of afspraken aan te passen.

Partijen handelen hierbij vanuit het gezamenlijke belang van een effectieve en continu verbeterende SOC-dienstverlening, waarbij transparantie, samenwerking en lerend vermogen centraal staan.

De informatievoorziening ter ondersteuning van bovenstaande verplichtingen vindt plaats conform paragraaf 1.3 (Overkoepelende rapportage-eis).

1.3 Overkoepelende rapportage-eis

Opdrachtnemer waarborgt dat Opdrachtgever en Deelnemers te allen tijde beschikken over volledige, actuele, consistente en herleidbare informatie over de uitvoering en prestaties van de SOC-dienstverlening, zodanig dat sturing, risicobeheersing, verantwoording en continue verbetering aantoonbaar worden ondersteund.

De vereiste informatie wordt beschikbaar gesteld via rapportages en/of onderliggende systemen en tooling (zoals ITSM-systemen, SIEM/SOAR-platformen, dashboards of andere registratiesystemen). Opdrachtnemer is vrij in de vorm, structuur en opbouw van rapportages en informatievoorziening, mits de informatie volledig, actueel, consistent en herleidbaar beschikbaar is voor Opdrachtgever en Deelnemers.

Opdrachtnemer waarborgt dat de volgende informatie aantoonbaar beschikbaar is:

- a. een integraal en samenhangend overzicht van prestaties, gebeurtenissen en risico's over de relevante periode;
- b. trendanalyses gericht op het identificeren van structurele patronen, afwijkingen en ontwikkelingen in dreigingen en incidenten;
- c. root cause analyses van significante beveiligingsincidenten en afwijkingen, inclusief onderliggende oorzaken en relevante ketenafhankelijkheden;
- d. volledig en herleidbaar inzicht in incidenten, alerts, meldingen en use cases, inclusief historie, statusovergangen en audit-trail;
- e. inzicht in de backlog van bevindingen, incidenten, verbetermaatregelen en openstaande acties, inclusief ouderdom (ageing), prioritering en expliciet onderscheid tussen actieve en geblokkeerde items, waarbij afhankelijkheden van Deelnemers en/of Derden inzichtelijk worden gemaakt;

- f. concrete, navolgbare en toetsbare verbetermaatregelen, inclusief voortgang, eigenaarschap en verwachte impact;
- g. een expliciete duiding van risico's, trends en knelpunten die aanleiding geven tot sturing, besluitvorming of escalatie.

De beschikbare informatie is onderling consistent en herleidbaar tot onderliggende data en registraties, waaronder logdata, detecties, incidentregistraties en workflow- of ticketsystemen. Opdrachtnemer stelt Opdrachtgever en Deelnemers in staat om desgevraagd detailinformatie in te zien en licht de informatievoorziening op verzoek nader toe.

Opdrachtnemer waarborgt dat de informatievoorziening aantoonbaar wordt benut ter ondersteuning van de governance van de dienstverlening, waaronder operationele, tactische en strategische overleggen, en dat de voortgang van verbetermaatregelen structureel wordt gemonitord en inzichtelijk gemaakt.

1.4 Service Credit regime

Onverminderd het bepaalde in paragraaf 1.2 geldt dat Opdrachtgever respectievelijk de Deelnemer een Service Credit kan toepassen indien SLA-parameters structureel niet worden gerealiseerd en de Opdrachtnemer onvoldoende opvolging geeft aan de vereiste verbetermaatregelen.

Een Service Credit wordt uitsluitend toegepast indien:

- sprake is van een herhaaldelijke overschrijding van een SLA-parameter binnen een aaneengesloten periode van drie (3) maanden; en
- Opdrachtnemer, naar het oordeel van Opdrachtgever respectievelijk de Deelnemer, onvoldoende invulling geeft aan de uitvoering van de root cause analyse en/of het overeengekomen verbeterplan; en
- de overschrijding van de SLA-parameter geheel of gedeeltelijk toerekenbaar is aan Opdrachtnemer.

Van een herhaaldelijke overschrijding is in ieder geval sprake indien binnen een aaneengesloten periode van twaalf (12) maanden:

- drie (3) of meer meetperioden voorkomen waarin dezelfde SLA-parameter niet wordt gerealiseerd; of
- in meer dan twintig procent (20%) van de meetperioden de betreffende SLA-parameter niet wordt gerealiseerd.

De Service Credit betreft een financiële korting op de factuur van de betreffende Deelnemer waarop de tekortkoming betrekking heeft, en wordt toegepast op de eerstvolgende factuur na vaststelling. Service Credits zijn cumulatief toepasbaar.

Tenzij anders overeengekomen, geldt de volgende staffel:

- eerste herhaaldelijke overschrijding: 5% korting op de maandelijkse vergoeding van de betreffende Dienst die de Deelnemer (Nadere overeenkomst) gefactureerd krijgt;
- tweede opeenvolgende herhaaldelijke overschrijding: 10% korting;
- derde en volgende opeenvolgende herhaaldelijke overschrijdingen: 15% korting.

Opdrachtgever respectievelijk de Deelnemer kan besluiten de toepassing van een Service Credit op te schorten indien Opdrachtnemer met een overtuigende root cause analyse en een concreet en toetsbaar verbeterplan aannemelijk maakt dat herstel binnen afzienbare termijn plaatsvindt. Opdrachtgever behoudt in dat geval het recht om de opgeschorte Service Credit alsnog toe te passen indien de verbetering uitblijft.

Service Credits laten onverlet:

- de verplichting van Opdrachtnemer tot nakoming van de SLA-parameters;
- het recht van Opdrachtgever respectievelijk de Deelnemer om aanvullende maatregelen te treffen in geval van aanhoudende tekortkomingen;

- eventuele overige contractuele rechten, waaronder beëindiging bij een tekortkoming van wezenlijke betekenis.

Service Credits worden uitsluitend toegepast voor zover de niet-nakoming van de SLA-parameter niet het gevolg is van aantoonbare factoren buiten de invloedssfeer van Opdrachtnemer.

2 Diensten

2.1 Algemeen

De Raamovereenkomst biedt Deelnemers de mogelijkheid om SOC-diensten af te nemen ter ondersteuning van hun verantwoordelijkheden op het gebied van informatiebeveiliging en cyberweerbaarheid. De afname van SOC-diensten start altijd met de Basis SOC-diensten voor IT-en/of OT-omgevingen. Hiertoe sluit de Deelnemer een Nadere Overeenkomst met de Opdrachtnemer. Optionele SOC-diensten kunnen aanvullend worden afgenomen, maar maken geen onderdeel uit van het verplichte basispakket.

Verantwoordelijkheidsverdeling (rollen en verantwoordelijkheden)

De Deelnemer blijft te allen tijde eindverantwoordelijk voor:

- Het informatiebeveiligingsbeleid.
- De naleving van wet- en regelgeving, waaronder de Cyberbeveiligingswet (Cbw - NIS2-richtlijn).
- Besluitvorming over risicoacceptatie, escalatie en herstelmaatregelen.
- Aansturing van interne en externe stakeholders.

De Opdrachtnemer is verantwoordelijk voor de uitvoering van de overeengekomen SOC-diensten, waaronder:

- Het operationeel uitvoeren van monitoring, detectie, analyse en rapportage.
- De Opdrachtnemer is verantwoordelijk voor het continu monitoren van overeengekomen logbronnen, het tijdig detecteren van security Events conform use cases en detectieregels, een het analyseren en kwalificeren van deze Events tot incidenten, inclusief prioritering en initiële duiding, binnen de afgesproken SLA's. Het adviseren van de Deelnemer over benodigde opvolgacties.
- Het ondersteunen van de Deelnemer bij incidentafhandeling conform overeengekomen processen en SLA's.

De Deelnemer en Opdrachtnemer werken hierbij samen volgens vastgelegde rollen, verantwoordelijkheden, escalatiepaden en communicatieafspraken, die per Nadere Overeenkomst nader worden uitgewerkt.

Regieorganisatie

De centrale regiefunctie van uit de Opdrachtgever is belegd bij IPO/BIJ12. De centrale regiefunctie coördineert, stuurt en bewaakt namens de gezamenlijke provincies de SOC-dienstverlening, met als doel het borgen van kwaliteit, samenhang en continuïteit zonder zelf operationele taken uit te voeren. De functie combineert contract- en leveranciersmanagement met interprovinciale afstemming, waarbij zowel formele sturing (SLA's en contracten) als inhoudelijke coördinatie en doorontwikkeling worden geborgd. Daarmee fungeert de regieorganisatie als verbindende schakel tussen provincies en leverancier en bewaakt zij de gezamenlijke belangen, risico's en prestaties.

Koppeling met de Cyberbeveiligingswet

De Basis SOC-diensten zijn ingericht ter ondersteuning van de verplichtingen uit hoofde van de Cyberbeveiligingswet (Cbw) en sluiten aantoonbaar aan op de daarin opgenomen verplichtingen ten aanzien van zorgplicht, risicobeheersing en incidentmelding.

De dienstverlening ondersteunt Deelnemers in het bijzonder bij de uitvoering van verplichtingen met betrekking tot het treffen van passende en evenredige technische, organisatorische en operationele beveiligingsmaatregelen, waaronder:

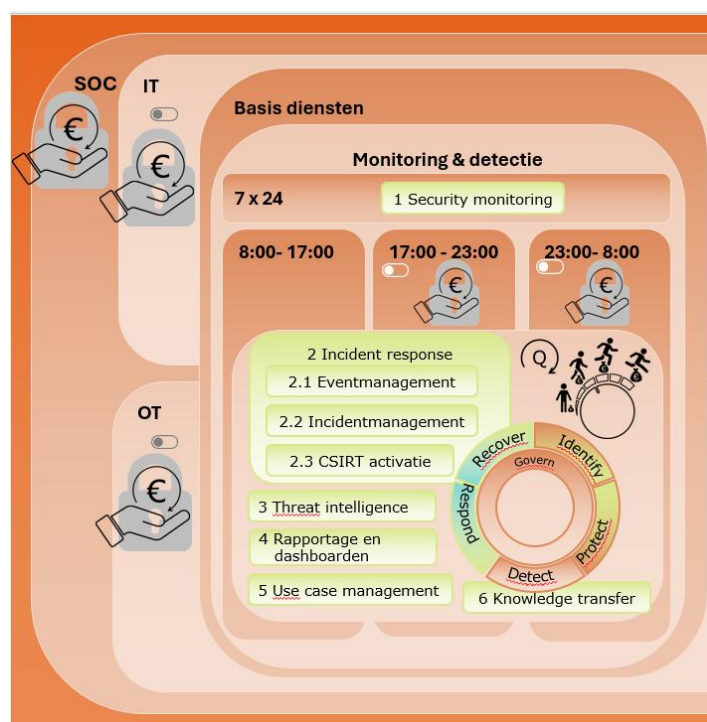
- continue monitoring en detectie van dreigingen;
- incidentdetectie en -analyse;
- logmanagement en het verkrijgen en behouden van zichtbaarheid op netwerk- en informatiesystemen;
- het toepassen en ondersteunen van risico gebaseerde beveiligingsmaatregelen.

Daarnaast ondersteunen de Basis SOC-diensten bij het voldoen aan verplichtingen inzake het melden van beveiligingsincidenten, waaronder:

- het tijdig detecteren en classificeren van significante beveiligingsincidenten;
- het analyseren en voorbereiden van incidentmeldingen richting bevoegde autoriteiten;
- het vastleggen en beschikbaar stellen van relevante informatie ten behoeve van melding, opvolging en verantwoording.

De Basis SOC-diensten vormen daarmee een essentieel ondersteunend middel voor Deelnemers om invulling te geven aan hun wettelijke verplichtingen onder de Cbw. De inzet van deze diensten laat onverlet dat de Deelnemer te allen tijde verantwoordelijk blijft voor de naleving van de Cyberbeveiligingswet en de daarop gebaseerde besluitvorming.

3 Basis SOC-diensten



Figuur 1. Basis SOC-diensten

Opdrachtnemer levert op verzoek van de Deelnemer Basis SOC-dienst die een solide fundament biedt voor het detecteren, analyseren en opvolgen van cyberdreigingen in zowel IT- als OT-omgevingen. Het doel is om continu inzicht te geven in beveiligingsrisico's en snel te reageren op Beveiligingsincidenten, zodat bedrijfscontinuïteit en compliance worden gewaarborgd.

De basis SOC-dienst bestaat uit de volgende kerncomponenten:

1. Security Monitoring

- Real-time bewaking van IT- en of OT-omgevingen via koppeling van de SIEM van de Opdrachtnemer met die van de Deelnemer.
- Security monitoring is een doorlopende activiteit en vormt de basis voor alle SOC-functionaliteit.
- Detectie van afwijkingen en verdachte activiteiten. Opvolging vindt plaats binnen Beveiligingsincident Response.

2. Beveiligingsincident Response

- Analyse en opvolging van Beveiligingsincidenten.
- Inclusief Eventmanagement, Beveiligingsincidentmanagement, playbooks en CSIRT-activatie voor ernstige Beveiligingsincidenten.
- *Doel:* snelle mitigatie en herstel om impact te minimaliseren.

3. Threat Intelligence

- Verrijking van detectie met actuele dreigingsinformatie.
- Proactieve signalering van nieuwe aanvalstechnieken en trends.

4. Rapportage en Dashboards

- Periodieke rapportages en interactieve dashboards voor inzicht in status, trends en verbeterpunten.
- Ondersteunt compliance en strategische besluitvorming.
- Evaluatie en optimalisatie ook vanuit kosten perspectief.

5. Use Case Management

- Detectieregels, use-cases te ontwikkelen, implementeren, onderhouden en te optimaliseren op basis van risico's en dreigingslandschap.
- Continue optimalisatie om relevantie en effectiviteit te waarborgen.

6. Knowledge Transfer

- Structurele kennisoverdracht naar de Deelnemer.
- *Doel:* vergroten van interne expertise en samenwerking met het SOC.

3.1 Basis - Monitoring & detectie

1 Security monitoring

Doel: Continu bewaken van systemen, netwerken en applicaties op afwijkingen, dreigingen en verdachte activiteiten.

Events vormen de basis voor detectie. Alerts worden gegenereerd op basis van analyse van Events. Alerts die na triage en analyse worden bevestigd als dreiging met (potentiële) impact, worden geclassificeerd als beveiligingsincidenten.

Het Service window is van toepassing op alle activiteiten die menselijke tussenkomst vereisen. Geautomatiseerde detectie-, correlatie- en alarmeringsprocessen functioneren continu (24/7), onafhankelijk van het Service window.

Wat valt hieronder?

- Verzamelen, normaliseren en analyseren van logs en telemetry.
- Real-time correlatie en detectie (SIEM, UEBA, IDS/IPS, EDR/XDR).
- Gebruik van detectieregels, use-cases, threat intelligence en gedragsanalyse.
- Signaalgeneratie (alerts) bij verdachte gebeurtenissen.
- 24/7 monitoring.

Kernvraag: Wordt een potentiële dreiging opgemerkt?

Resultaat: Een alert die verder beoordeeld moet worden.

Eisen	
	Koppeling, datastromen en logvolledigheid
A.1	Opdrachtnemer realiseert en onderhoudt op verzoek van de Deelnemer een koppeling tussen de SOC-dienstverlening en de ticketing- en ITSM-systemen van de Deelnemer (bijv. ServiceNow of TOPdesk). De koppeling ondersteunt een efficiënte en traceerbare workflow voor registratie, triage, escalatie en afhandeling van alerts en Beveiligingsincidenten, waarbij regie bij de Deelnemer wordt geborgd. De koppeling is gebaseerd op open standaarden en API's en heeft geen negatieve impact op de performance of beschikbaarheid van het ITSM-systeem.

A.2	Opdrachtnemer hanteert een gestandaardiseerd incident- en escalatiekader op hoofdlijnen, dat minimaal omvat: • uniforme classificatie van security-events en incidenten; • prioriteitsniveaus en bijbehorende responstijden; • escalatieregels en communicatiemomenten; • statusovergangen en minimale registratievereisten. Dit kader wordt consistent toegepast over alle Deelnemers.
A.3	Binnen het gestandaardiseerde kader ondersteunt Opdrachtnemer Deelnemer-specifieke inrichting van: • workflows en statussen; • prioriteringsmodellen; • autorisatiestructuren; • integratie met interne processen. Afwijkingen worden beheerst en gedocumenteerd, zonder afbreuk te doen aan de uniformiteit van het incident- en escalatiekader.
A.4	Opdrachtnemer waarborgt dat: • alle relevante incidentinformatie tijdig en volledig wordt gesynchroniseerd tussen SOC en ITSM; • dubbele registratie en inconsistenties worden voorkomen; • de Deelnemer real-time of near real-time inzicht heeft in status en voortgang.
A.5	Opdrachtnemer bewaakt de kwaliteit van logaanlevering (log health monitoring) voor de in scope zijnde databronnen en controleert periodiek en geautomatiseerd op: • beschikbaarheid van logaanlevering; • vertraging (latency) in logstromen; • afwijkingen in logvolume of -patronen; • technische fouten in dataverwerking (bijv. parsing of connectoren). Opdrachtnemer meldt afwijkingen proactief aan de Deelnemer, inclusief impactanalyse, advies en herstelvoorstellen. De intensiteit en frequentie van log health monitoring worden afgestemd op de kritikaliteit van databronnen en vastgelegd in het DAP.
A.6	Opdrachtnemer past log health monitoring risicogebaseerd toe: • Voor kritieke systemen: near real-time monitoring en snelle signalering van uitval. • Voor overige systemen: periodieke controle en trendanalyse. De indeling van kritikaliteit wordt in overleg met Deelnemer vastgesteld en vastgelegd in het DAP.

A.7	Deelnemer verstrekt een actuele, volledige en gevalideerde assetlijst (CMDB), inclusief classificatie, kriticititeit en eigenaarschap, die als basis dient voor de scope van monitoring. Opdrachtnemer toetst deze lijst op plausibiliteit en volledigheid in relatie tot de ingerichte monitoring en adviseert Deelnemer over noodzakelijke aanvullingen voor effectieve detectie. Opdrachtnemer is uitsluitend verantwoordelijk voor monitoring, detectie en analyse van systemen en databronnen die: • door Deelnemer zijn opgenomen in de scope, en • technisch zijn aangesloten op de monitoringvoorzieningen (bijv. SIEM). Systemen of databronnen die niet zijn opgenomen in de CMDB of niet zijn aangesloten op monitoring vallen buiten de verantwoordelijkheid van Opdrachtnemer. Opdrachtnemer signaleert, voor zover redelijkerwijs mogelijk, ontbrekende of niet-aangesloten kritieke systemen en adviseert Deelnemer hierover.
A.8	Waar van toepassing ondersteunt Opdrachtnemer OT-specifieke protocollen en logformaten (zoals Modbus, DNP3 en OPC UA) voor volledige en betrouwbare monitoring van OT-omgevingen.
Eventselectie, detectiescope en use-case ontwikkeling	
A.9	Opdrachtnemer en Deelnemer stellen gezamenlijk een formele Event-selectielijst op die als uitgangspunt dient voor de inrichting van monitoring en detectie. De Event-selectielijst bevat minimaal per databron en/of use case: • type databron en logcategorie (bijv. identity, endpoint, netwerk, applicatie, OT); • specifieke events/logvelden die worden verzameld; • doel van de logging (bijv. detectie, forensics, compliance); • retentieperiode; • aanleverfrequentie en verwachte latency; • prioriteit/kritikaliteit van de databron; • relatie met detectieregels en use cases. Opdrachtnemer hanteert hierbij gangbare standaarden en best practices (bijv. MITRE ATT&CK, NIST, Microsoft Sentinel best practices) en vertaalt deze naar de specifieke context van de Deelnemer. De Event-selectielijst wordt: • initieel opgesteld tijdens de implementatiefase; • minimaal halfjaarlijks geëvalueerd; • tussentijds geactualiseerd bij relevante wijzigingen, waaronder: • wijzigingen in IT/OT-landschap; • nieuwe dreigingen of kwetsbaarheden; • wijzigingen in wet- en regelgeving; • lessons learned uit incidenten of threat hunting. Wijzigingen worden afgestemd met Deelnemer en vastgelegd in het DAP.
A.10	Opdrachtnemer adviseert actief over optimalisatie van logging ter balans tussen detectiekwaliteit, performance en kosten.
A.11	Opdrachtnemer ontwikkelt en onderhoudt detectieregels, use-cases en op basis van actuele dreigingsinformatie (threat intelligence) uit meerdere betrouwbare bronnen, waaronder sectorspecifieke feeds. Correlatie- en gedragsanalyses worden toegepast om afwijkingen vroegtijdig te identificeren en om te zetten naar alerts.

	Monitoring en detectie
A.12	Opdrachtnemer voert 24/7/365 monitoring uit op alle overeengekomen IT- en OT-assets, inclusief real-time correlatie, alerting en triage, conform de overeengekomen SLA-parameters.
A.13	Opdrachtnemer past met de Deelnemer detectiemechanismen toe die gericht zijn op het identificeren van afwijkingen in gebruikers-, netwerk-, applicatie- en systeemgedrag. Hierbij wordt minimaal gebruikgemaakt van zowel anomaly-based als signature-based detectie, afgestemd met de Deelnemer.
A.14	Opdrachtnemer maakt in samenspraak met de Deelnemer gebruik van een combinatie van geautomatiseerde detectietechnieken (zoals machine learning, gedragsanalyse en rule-based correlatie) en handmatige validatie van detecties door gekwalificeerde SOC-analisten. Opdrachtnemer waarborgt dat de ingezette analisten aantoonbaar beschikken over relevante kennis en expertise op het gebied van Security Operations, threat detection en incidentanalyse. Deze expertise wordt onderbouwd door één of meer erkende en actuele certificeringen binnen het SOC-domein, zoals onder meer: • CompTIA CySA+ • GIAC (bijv. GCIA, GCIH) • ISC2 (bijv. SSCP, CISSP) • of andere aantoonbaar gelijkwaardige, marktconforme certificeringen Opdrachtnemer toont op verzoek van de Opdrachtgever aan dat: • de ingezette analisten beschikken over passende certificeringen en/of aantoonbare werkervaring; • certificeringen actueel en relevant zijn voor de uit te voeren werkzaamheden; • de samenstelling van het SOC-team aansluit bij de complexiteit en aard van de dienstverlening
A.15	Opdrachtnemer verwerkt alle ontvangen security-Events via een geïntegreerde detectieketen bestaande uit normalisatie, correlatie en detectie. De detectietijd wordt gemeten vanaf het moment van verwerking van Events in het SOC-platform, tot het moment waarop een Alert wordt gegenereerd.
	Evaluatie en actualisatie van detectieregels
A.16	Opdrachtnemer evalueert alle kritieke detectieregels maandelijks en de overige detectieregels minimaal elk kwartaal op effectiviteit, het aantal false positives en de aanwezigheid van nieuwe of gewijzigde dreigingen. Bevindingen worden gedocumenteerd en detectieregels worden waar nodig aantoonbaar aangepast en met de Deelnemer besproken. Ad-hoc evaluaties en aanpassingen vinden plaats bij nieuwe dreigingen of relevante beveiligingsincidenten.

	Normenkaderconformiteit security monitoring
A.17	De door Opdrachtnemer geleverde security-monitoringdienst voldoet aantoonbaar aan de relevante bepalingen uit de Cbw, ISO/IEC 27001 en de Baseline Informatiebeveiliging Overheid (BIO). Voor de invulling van de beheersmaatregelen wordt aangesloten bij ISO/IEC 27002 of een aantoonbaar gelijkwaardig normenkader. Opdrachtnemer levert desgevraagd bewijs van deze conformiteit, bijvoorbeeld in de vorm van certificeringen, verklaringen of auditrapportages.
	Aantoonbare expertise in OT-security monitoring
A.18	Opdrachtnemer beschikt aantoonbaar over kennis en ervaring met OT-security monitoring in industriële omgevingen, waarbij gangbare OT-securityprincipes worden toegepast, mede gebaseerd op richtinggevende kaders zoals IEC 62443. Deze expertise omvat ten minste: • het toepassen van passieve monitoring binnen industriële netwerken (o.a. Purdue Zone 2 en 3), zonder verstoring van operationele processen; • het analyseren en interpreteren van OT-specifieke netwerkprotocollen, waaronder Modbus/TCP, DNP3, IEC 61850 en BACnet; • het toepassen van OT-specifieke dreigingsmodellen en aanvalstechnieken, waaronder MITRE ATT&CK for ICS; • het opereren met awareness van OT-architecturen, segmentatie en afhankelijkheden tussen IT- en OT-domeinen; • afstemming met OT-beheerders gericht op het waarborgen van continuïteit, veiligheid en beschikbaarheid van operationele processen. De Opdrachtnemer richt OT-monitoring proportioneel en gefaseerd in, passend bij de aard, omvang en volwassenheid van de OT-omgevingen van de Deelnemer.
	Randvoorwaarden
A.19	De in deze paragraaf opgenomen SLA-parameters zijn mede afhankelijk van de kwaliteit, beschikbaarheid en tijdigheid van de door de Deelnemer aangeleverde logbronnen, netwerkverbindingen en onderliggende (cloud)platformen. De volgende randvoorwaarden zijn van toepassing: - Deelnemer draagt zorg voor correcte, volledige en tijdige configuratie van logbronnen; - Deelnemer waarborgt dat logaanlevering plaatsvindt binnen overeengekomen specificaties (zoals latency en beschikbaarheid); - Eventuele beperkingen of vertragingen in onderliggende platformen vallen buiten de directe beïnvloedingssfeer van Opdrachtnemer. Indien niet wordt voldaan aan deze randvoorwaarden, worden de betreffende SLA-parameters aangemerkt als best effort in plaats van resultaatsverplichting.

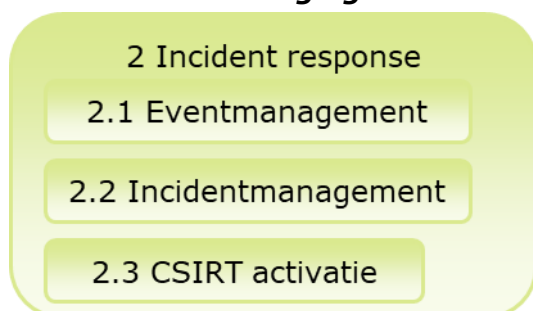
SLA-paramaters	
A.20	Beschikbaarheid monitoringplatform
	SLA: Opdrachtnemer draagt zorg voor de beschikbaarheid van het monitoringplatform en de daarop ingerichte SOC-dienstverlening. Voor zover de dienstverlening afhankelijk is van onderliggende platformen van derden, waaronder Microsoft Sentinel, geldt dat de beschikbaarheid van deze componenten wordt bepaald door de SLA's van de betreffende leverancier.
	Opdrachtnemer garandeert een minimale beschikbaarheid van 99,95% per kalendermaand voor de door Opdrachtnemer beheerde componenten en configuraties, exclusief vooraf overeengekomen onderhoudsvensters en aantoonbare verstoringen in onderliggende platformdiensten van derden.
	Doel: Continu en betrouwbaar toezicht op IT- en OT-systemen.
A.21	Logontvangst en logvolledigheid (Visibility Rate)
	SLA: Opdrachtnemer waarborgt een logvolledigheid van $\geq 98\%$ voor alle overeengekomen logbronnen, mits deze correct, volledig en tijdig door de Deelnemer of bronsystemen worden aangeleverd.
	SLA: (kritieke logbronnen): Bij uitval of significante afwijkingen ($>5\%$ dataverlies of >10 minuten onderbreking) in kritieke logbronnen meldt Opdrachtnemer dit binnen maximaal 30 minuten na detectie aan de Deelnemer.
	SLA (niet-kritieke logbronnen): Bij uitval of afwijkingen in niet-kritieke logbronnen meldt Opdrachtnemer dit binnen maximaal 4 uur of in de eerstvolgende periodieke rapportage, afhankelijk van de impact en duur van de afwijking.
	SLA (vertraging logaanlevering): De maximale vertraging in logaanlevering bedraagt ≤ 60 seconden vanaf het moment van succesvolle ontvangst van logdata, tenzij aantoonbaar veroorzaakt door onderliggende platformdiensten of schriftelijk afwijkend overeengekomen.
	SLA (proactieve detectie): Opdrachtnemer monitort actief de beschikbaarheid en kwaliteit van logstromen en onderneemt direct actie bij afwijkingen, ongeacht meldverplichtingen.
	Doel: Volledige zichtbaarheid van systemen en betrouwbare detectiemogelijkheden.
A.22	Logretentie
	SLA: De retentieperiodes zijn gebaseerd op: (a) Cyberbeveiligingswet (Cbw) en onderliggende regelgeving (implementatie van NIS2) – voor zover van toepassing op logging, beschikbaarheid en bewaartermijnen; (b) BIO 2.0 Maatregel 8.15 (logregistratie); (c) AVG Artikel 5(1)e (opslagbeperking); en (d) forensische vereisten conform ENISA Good Practice Guide for Incident Management. Bij strijdigheid geldt de langste termijn. Deze retentieperiodes zijn van toepassing op alle IT- en OT-logbronnen binnen de overeengekomen monitoringscope.
	Doel: Ondersteuning van forensische analyses en compliance.

A.23	Eventnormalisatie	
	SLA:	Opdrachtnemer normaliseert alle ontvangen Events binnen 5 minuten naar het overeengekomen standaardformaat (bijv. CEF, JSON, ECS).
	Doel:	Consistente verwerking, correlatie en analyse over alle logbronnen heen.
A.24	Eventcorrelatie	
	SLA:	Opdrachtnemer correleert alle genormaliseerde Events binnen 5 minuten na normalisatie, waarbij afwijkingen in kritieke systemen zichtbaar worden in het SOC.
	Doel:	Vroege detectie van dreigingen en reductie van false positives. Maximaliseren van detectiedekking en minimaliseren van blind spots.
A.25	Mean Time To Detect (MTTD)	
	SLA:	Critical alerts worden gedetecteerd en geclassificeerd binnen ≤ 10 minuten.
	SLA:	High alerts worden gedetecteerd en geclassificeerd binnen ≤ 20 minuten.
	Doel:	Tijdige identificatie van afwijkingen en potentiële beveiligingsincidenten.
A.26	Detectieregels en use-case evaluatie	
	SLA:	Alle detectieregels en use-cases worden minimaal per kwartaal geëvalueerd op effectiviteit, false positives en aansluiting op actuele dreigingen. Aanpassingen worden aantoonbaar gedocumenteerd en gedeeld met Deelnemer.
	Doel:	Continu verbeteren van detectiecapaciteit en reductie van false positives.
A.27	Normenkaderconformiteit	
	SLA:	Security monitoring wordt continu geleverd ter ondersteuning van de zorgplicht uit de Cbw.
	SLA:	Op verzoek verstrekt Opdrachtnemer bewijs van conformiteit, zoals certificeringen of auditrapportages.
	Doel:	Garanderen van compliance en aansluiting op relevante wet- en regelgeving.
A.28		
A.29	Operationele Deliverables	
	Realtime alerts en meldingen	
	Opdrachtnemer levert 24/7/365 realtime meldingen van Alerts en Beveiligingsincidenten op alle overeengekomen IT- en OT-assets. alerts worden geclassificeerd conform de met de Deelnemer overeengekomen prioriteits- en impactniveaus.	

A.30	Periodieke Rapportages
	Maandelijkse SOC-rapportage
	Opdrachtnemer stelt maandelijks informatie beschikbaar die voldoet aan de overkoepelende rapportage-eis zoals opgenomen in paragraaf 1.3. Deze informatie wordt beschikbaar gesteld via rapportages en/of onderliggende systemen en tooling en omvat ten minste: - aantal en type gegenereerde alerts; - trends; - prestaties ten opzichte van overeengekomen SLA-parameters; - logvolledigheid en logbronstatus; - herhaalde kwetsbaarheden en Beveiligingsincidenttypen; - aanbevelingen voor verbetering.
A.31	Kwartaalrapportage Security Posture
	Opdrachtnemer stelt per kwartaal security posture-informatie beschikbaar die voldoet aan de overkoepelende rapportage-eis zoals opgenomen in paragraaf 1.3 Overkoepelende rapportage-eis., inclusief trendanalyses, GAP-analyses ten opzichte van relevante normen (BIO, Cbw, NIST CSF), use-case effectiviteit en verbeteradviezen.
A.32	Jaarlijkse Management Evaluatie
	Opdrachtnemer levert minimaal maandelijks een rapportage met een integraal overzicht van de SOC-prestaties, High en Critical beveiligingsincidenten en de opvolging daarvan, inclusief relevante trends en bijzonderheden. Daarnaast levert Opdrachtnemer jaarlijks een managementrapportage met een integraal overzicht van de SOC-dienstverlening, waaronder de belangrijkste prestaties, High en Critical beveiligingsincidenten over het jaar, de voortgang van verbetermaatregelen, de ontwikkeling in volwassenheid en een roadmap voor het daaropvolgende jaar.
A.33	Detectie Deliverables
	Correlatie- en detectieregels
	Opdrachtnemer levert alle gebruikte correlatieregels, detectiescripts en gedragsanalyses die worden ingezet binnen de SIEM/SOAR-omgeving van de Deelnemer, inclusief bijbehorende documentatie en versiebeheer. De documentatie bevat ten minste: - het doel van de detectieregel of analyse; - de onderliggende logbronnen; - de detectielogica en drempelwaarden; - de koppeling met relevante MITRE ATT&CK-technieken (indien van toepassing); de prioriteit of impactclassificatie van de detectie binnen het incidentclassificatiemodel.

	Logging & Integratie Deliverables
A.34	Logintegratieplan
	Opdrachtnemer waarborgt dat informatie over de volledigheid, tijdigheid, juistheid en beschikbaarheid van logaanlevering per bron aantoonbaar beschikbaar is voor de Deelnemer, inclusief bevindingen, risico's en hersteladviezen, conform paragraaf 1.3 Overkoepelende rapportage-eis.
A.35	Log Health Monitoring Rapportage
	Opdrachtnemer levert maandelijks een rapportage over de volledigheid, tijdigheid, juistheid en beschikbaarheid van logaanlevering per bron, inclusief bevindingen, risico's en hersteladviezen.
A.36	Advies- en Verbetering Deliverables
	Verbeterplannen Security Monitoring
	Opdrachtnemer levert op periodieke basis (minimaal jaarlijks) een verbeterplan met aanbevelingen voor procesverbetering, detectieverbetering, aanvullende sensoren, logbronnen en volwassenheidsgroei.

3.2 Basis - Beveiligingsincident response



Opdrachtnemer levert Beveiligingsincident Response tijdens kantooruren voor de IT- en of OT-omgeving. Opdrachtnemer breidt Beveiligingsincident Response uit op verzoek van de Deelnemer tijdens Werkdagen tijdens avonduren (17:00 – 23:00). Opdrachtnemer breidt Beveiligingsincident Response uit op verzoek van de Deelnemer uit naar alle dagen van de week en alle uren in een dag (7x24).

3.2.1 Basis - Event management

2.1 Eventmanagement

Doel: Structuur en kwaliteit van het omgaan met *Alerts* (gebaseerd op onderliggende Events) waarborgen — voordat wordt vastgesteld dat er sprake is van een Beveiligingsincident.

Wat valt hieronder?

- Prioritering en categorisering van alerts (critical/high/medium).
- Triage en eerste menselijke beoordeling.
- Filteren van false positives.
- Escalatieregels toepassen (bijv. naar Beveiligingsincidentmanagement bij confirmed Beveiligingsincident).
- Workflow in ITSM-systeem (TOPdesk, ServiceNow).
- Optimaliseren van alertkwaliteit (false positives en negatives reduceren).

Kernvraag: *Is deze Alert een echt Beveiligingsincident, en zo ja, wat moet ermee gebeuren?*

Resultaat:

- Geen Beveiligingsincident → Alert sluiten (false positive / benign) + regeloptimalisatie.
- Wel Beveiligingsincident → escalatie naar Beveiligingsincidentmanagement.

Eisen	
	Verzameling, verwerking en kwaliteit van security Events
A.37	Opdrachtnemer verzamelt, ontvangt en verwerkt alle relevante security Events uit de overeengekomen logbronnen, waaronder ten minste netwerkcomponenten, servers, endpoints, cloudomgevingen, OT-devices en applicaties.
A.38	Opdrachtnemer controleert continu de volledigheid, juistheid en tijdigheid van de aangeleverde logs (log health monitoring) en meldt afwijkingen proactief aan Deelnemer, inclusief advies voor herstel.
A.39	Opdrachtnemer normaliseert alle ontvangen Events naar een uniform, overeengekomen formaat (zoals CEF, JSON of ECS), zodat consistente correlatie, analyse en rapportage mogelijk zijn.

	Analyse, detectie en triage
A.40	Opdrachtnemer analyseert alerts (gebaseerd op gecorreleerde events) om te bepalen of sprake is van een beveiligingsincident
A.41	Opdrachtnemer voert proactieve triage uit conform een overeengekomen classificatiemodel, waarbij Alerts worden gevalideerd, geprioriteerd en waar nodig voorbereid voor escalatie.
	Eventmanagementdienst en scope
A.42	Opdrachtnemer levert een volledige Eventmanagementdienst gericht op het tijdig identificeren, analyseren, classificeren, escaleren, rapporteren en ondersteunen bij het oplossen van Beveiligingsincidenten. De dienst omvat ten minste: bewaking van IT- en OT-infrastructuur, detectie van afwijkende activiteiten, Event-triage, escalatie naar relevante teams en ondersteuning bij herstel conform vastgestelde procedures en SLA-paramaters.
A.43	Opdrachtnemer levert Eventmanagement voor zowel IT- als OT-omgevingen. Hierbij ondersteunt Opdrachtnemer OT-specifieke protocollen, risico's en Beveiligingsincidentprocedures. Deelnemer bepaalt de functionele scope per omgeving.
	Analytics en AI-mogelijkheden
A.44	De Opdrachtnemer past AI-assisted Event grouping toe voor sneller root-cause-onderzoek.
A.45	De Opdrachtnemer detecteert zeldzame of afwijkende Eventclusters ("rare Event detection") en genereert automatisch samenvattingen van Eventanomalieën.
	SOAR
A.46	Opdrachtnemer integreert een SOAR-platform (of gelijkwaardige automatisering binnen Microsoft Sentinel via Logic Apps/Automation Rules) voor geautomatiseerde respons op standaard beveiligingsscenario's. Alle SOAR-playbooks zijn gedocumenteerd, getest en eigendom van de Deelnemer.
SLA-paramaters	
A.47	Mean Time To Acknowledge (MTTA) / Start Triage
	SLA: triage start vanaf het moment waarop een analist de alert actief in behandeling neemt en een eerste beoordeling uitvoert.
	SLA: Opdrachtnemer voert triage uit op alle ontvangen alerts, waarbij alerts worden gevalideerd, geprioriteerd en geclassificeerd.
	SLA: Critical alerts worden erkend en geanalyseerd binnen ≤ 10 minuten.
	SLA: High alerts worden erkend en geanalyseerd binnen ≤ 30 minuten.
	Doel: Snelle start van triage en reductie van risico's door snelle menselijke beoordeling.
A.48	Escalatie
	SLA: Bevestigde beveiligingsincidenten worden binnen ≤ 10 minuten geëscaleerd naar Beveiligingsincidentmanagement.

	Doel: Snelle signalering en tijdige escalatie van incidenten met minimale vertraging.
A.49	Eventrapportage en audit-trail
	SLA: Alle alerts, triagestappen en beslismomenten worden binnen 24 uur volledig gedocumenteerd en opgenomen in de audit-trail.
	Doel: Volledige traceerbaarheid, compliance (BIO, Cbw, ISO 27001) en ondersteuning bij incidentanalyse.
A.50	Beschikbaarheid Eventmanagementteam
	SLA: Opdrachtnemer garandeert 24/7 beschikbaarheid van het Eventmanagementteam voor triage en escalatie van kritieke Alerts (of binnen overeengekomen openingstijden).
	Doel: Ononderbroken monitoring en snelle interventie bij verdachte activiteiten.
Deliverables	
A.51	Triage-analyses
	Opdrachtnemer levert bij elke melding een triage-analyse, inclusief risico-inschatting, classificatie, eerste duiding en een advies voor opvolging of onmiddellijke mitigerende acties.
A.52	Alert-triage rapportages
	Opdrachtnemer waarborgt dat informatie over uitgevoerde Alert-triage aantoonbaar beschikbaar is, inclusief aard van de gebeurtenissen, toegepaste analyses en genomen vervolgacties, conform paragraaf 1.3 Overkoepelende rapportage-eis.
A.53	Classificatie- en prioriteringsrapporten
	Opdrachtnemer waarborgt dat inzicht beschikbaar is in de classificatie en prioritering van gedetecteerde security-Events, inclusief onderbouwing van urgentie en risico-inschatting, conform paragraaf 1.3 Overkoepelende rapportage-eis.
A.54	ITSM-tickets en workflowlogs
	Opdrachtnemer levert gestructureerde ITSM-tickets en bijbehorende workflowlogs waarin alle uitgevoerde handelingen, besluitmomenten en statuswijzigingen volledig en reproduceerbaar zijn vastgelegd.
A.55	False-positive optimalisatielijsten
	Opdrachtnemer levert overzichtslijsten met geanalyseerde false positives, inclusief voorgestelde verbeteringen aan detectieregels en aanbevelingen ter optimalisatie van de alert kwaliteit.
A.56	Event-contextualisatieoverzichten
	Opdrachtnemer levert overzichten waarin security-Events worden verrijkt met contextinformatie (zoals asset-waarde, dreigingsniveau, MITRE-koppeling of business-impact), teneinde een juiste prioritering en opvolging te ondersteunen.

	Escalatie- en opvolgrapportages
A.57	Opdrachtnemer waarborgt dat informatie over geëscaleerde Events aantoonbaar beschikbaar is, inclusief escalatiestappen, overdrachtsmomenten, responstijden en behaalde SLA's, conform paragraaf 1.3 Overkoepelende rapportage-eis.

3.2.2 Basis - Beveiligingsincident management

2.2 Incidentmanagement

Doel: Beheersen, beperken en oplossen van een *bevestigd Beveiligingsincident*.

Wat valt hieronder?

- Bevestiging van het Beveiligingsincident (Beveiligingsincident classification).
- Communicatie en coördinatie met Deelnemer (b.v. CISO, IT, directie).
- Containmentmaatregelen (bijv. isoleren endpoints).
- Root-cause analysis, forensics (indien overeengekomen).
- Ondersteunen van herstel en hersteladvies.
- Eindrapportage, lessons learned, verbeterplan.
- Noodzakelijke notificaties (o.a. AP, NCSC) volgens de Cbw en AVG.

Kernvraag: *Hoe beperken we de schade, herstellen we de situatie en voorkomen we herhaling?*

Resultaat: Beveiligingsincident opgelost + verbetermaatregelen.

Prioriteit	Omschrijving	Voorbeelden	Reactietijd (SLA)
P1 – Kritiek	Zeer ernstig incident, direct impact op kritieke processen	Ransomware-aanval, actieve exploit, kritieke systeemcompromis, ernstige datalekken, systeemuitval van kernprocessen	30 min – 1 uur
P2 – Hoog	Hoog risico, significante impact, niet direct business-stopping	Malware-infectie, privilege escalation, verdachte exfiltratie, niet-kritieke systeemcompromis, kwetsbaarheid met exploitpotentieel	1 – 4 uur
P3 – Medium	Beperkt risico, geen directe kritieke impact	Misconfiguratie, verdachte login, phishing-click, policy violation, niet-kritieke vulnerability, kleine operationele afwijkingen	4 – 24 uur

Responsbevoegdheden en mandaatniveaus

De mate waarin de Opdrachtnemer bevoegd is om responsmaatregelen uit te voeren bij Beveiligingsincidenten kan per Deelnemer verschillen. Daarom wordt gewerkt met mandaatniveaus voor incidentrespons, waarbij de rol en bevoegdheden van de Opdrachtnemer vooraf expliciet worden vastgelegd.

Voor aanvang van de dienstverlening stemmen Deelnemer en Opdrachtnemer gezamenlijk af welk responsmandaat geldt voor de betreffende Deelnemer of voor specifieke systemen, use-cases of incidenttypen.

De volgende mandaatniveaus worden onderscheiden.

Mandaatniveau 1 – Signalering en escalatie

Binnen dit mandaatniveau vervult de Opdrachtnemer primair een detectie- en analysefunctie.

De Opdrachtnemer:

- detecteert en analyseert beveiligingsmeldingen en mogelijke Beveiligingsincidenten;
- verricht triage en initiële analyse;
- classificeert en prioriteert het incident;
- escaleert het incident volgens vooraf vastgestelde procedures naar de Deelnemer of geautoriseerde Derden;
- levert analyse en aanbevelingen voor mogelijke mitigatiemaatregelen.

Binnen dit mandaatniveau voert de Opdrachtnemer geen technische wijzigingen uit in de infrastructuur van de Deelnemer.

Mandaatniveau 2 – Gecoördineerde respons

Binnen dit mandaatniveau ondersteunt de Opdrachtnemer actief bij de coördinatie en voorbereiding van responsmaatregelen.

De Opdrachtnemer:

- analyseert en valideert het Beveiligingsincident;
- adviseert over containment-, mitigatie- en herstelmaatregelen;
- bereidt technische responsacties voor;
- coördineert de uitvoering van maatregelen door de Deelnemer of geautoriseerde Derden;
- ondersteunt bij communicatie en escalatie richting betrokken stakeholders.

Technische acties worden in dit mandaatniveau uitgevoerd door de Deelnemer of geautoriseerde Derden, tenzij anders overeengekomen.

Mandaatniveau 3 – Uitvoerende respons

Binnen dit mandaatniveau is de Opdrachtnemer, binnen vooraf overeengekomen kaders, bevoegd om technische responsmaatregelen uit te voeren binnen de infrastructuur van de Deelnemer.

Voorbeelden van dergelijke maatregelen kunnen zijn:

- isoleren van endpoints of systemen;
- blokkeren of resetten van accounts;
- aanpassen van security policies;
- blokkeren van netwerkverkeer of indicatoren;
- activeren van vooraf gedefinieerde response playbooks.

Deze maatregelen worden uitsluitend uitgevoerd:

- op basis van vooraf afgestemde procedures en use-cases;
- met expliciet toegekende toegangsrechten;
- binnen de overeengekomen mandaatgrenzen;
- Onder de verantwoordelijkheid van de Deelnemer.

Alle uitgevoerde acties worden volledig gelogd, gedocumenteerd en auditeerbaar vastgelegd.

Vastlegging van mandaat en procedures

De exacte invulling van het responsmandaat wordt per Deelnemer vastgelegd in operationele documentatie, waaronder bijvoorbeeld:

- incident response playbooks;

- SOC-runbooks;
- escalatieprocedures;
- toegangs- en autorisatiemodellen.

De Opdrachtnemer waarborgt dat:

- alle responsactiviteiten reproduceerbaar en auditeerbaar zijn;
- verantwoordelijkheden tussen Opdrachtnemer, Deelnemer en eventuele Derden duidelijk zijn vastgelegd;

wijzigingen in het responsmandaat uitsluitend plaatsvinden na schriftelijke afstemming met de Deelnemer.

Ongeacht het mandaatniveau blijft de Deelnemer eindverantwoordelijk voor:

- Besluitvorming rondom incidentafhandeling;
- Externe communicatie en wettelijke meldingen (conform Cbw).

Eisen	
	Scope van de dienst
A.58	Opdrachtnemer levert de dienst Beveiligingsincidentmanagement, gericht op het tijdig detecteren, analyseren, valideren oplossen met de Deelnemer of geautoriseerde Derden en evalueren van Beveiligingsincidenten en verstoringen, met als doel de impact op de bedrijfsvoering van de Deelnemers te minimaliseren en herhaling te voorkomen door structurele verbetermaatregelen. Beveiligingsincidentmanagement wordt gemeten vanaf het moment dat een Alert door het Eventmanagementproces is geclassificeerd als een incident.
A.59	Opdrachtnemer levert de basisdienst Beveiligingsincidentmanagement voor zowel IT- als OT-omgevingen, inclusief de specifieke risico's, protocollen en systemen die voor deze omgevingen gelden, tenzij in de Opdracht anders is gespecificeerd per Deelnemer.
	Methodiek en standaardisatie
A.60	Opdrachtnemer hanteert een gestandaardiseerde en aantoonbaar gedocumenteerde Beveiligingsincident Response-methodologie (bijvoorbeeld SANS of NIST 800-61r2) en kan dit proces desgevraagd toelichten aan de Opdrachtgever, inclusief rollen, taken, escalatiestappen en communicatiemomenten.
A.61	Opdrachtnemer maakt bij de uitvoering van Beveiligingsincidentanalyse en prioritering aantoonbaar gebruik van: - het MITRE ATT&CK® framework voor dreigingsduiding, inclusief de koppeling van waargenomen activiteiten aan relevante tactieken, technieken en procedures (TTP's); - de Common Vulnerability Scoring System (CVSS), versie 3.1 of hoger, als gestandaardiseerde methode voor het scoren van de ernst en impact van kwetsbaarheden; - kwetsbaarheidsinformatie afkomstig uit meerdere, betrouwbare en internationaal erkende bronnen, waaronder waar beschikbaar de European Vulnerability Database (EUVD) en andere relevante Europese en/of internationale databronnen. Opdrachtnemer waarborgt dat kwetsbaarheidsbeoordeling en prioritering gebaseerd zijn op een gevalideerde en reproduceerbare methodiek, en dat afhankelijkheid van enkelvoudige informatiebronnen wordt geminimaliseerd door toepassing van bronverificatie en/of bronredundantie.

A.62	Opdrachtnemer hanteert een gestandaardiseerd classificatiemodel voor Beveiligingsincidenten, gebaseerd op impact, urgentie en kans. Dit classificatiemodel wordt vooraf afgestemd en ter goedkeuring voorgelegd aan de Opdrachtgever en afgestemd op de kritieke processen van de Deelnemers.
	Uitvoering van Beveiligingsincident Response
A.63	Opdrachtnemer handelt Beveiligingsincident Response-activiteiten af binnen de overeengekomen Service Windows en de bijbehorende SLA-parameters, waaronder in ieder geval reactietijd, hersteltijd, escalatietijd en communicatiemomenten.
A.64	Opdrachtnemer markeert een Beveiligingsincident als voorgesteld gesloten en stelt Deelnemer hiervan schriftelijk in kennis, onder gelijktijdige verstrekking van het bijbehorende beveiligingsincidentrapport. Deelnemer heeft vanaf het moment van ontvangst van deze kennisgeving een termijn van twee (2) Werkdagen om gemotiveerd bezwaar te maken tegen de voorgestelde afsluiting. Indien Deelnemer binnen deze termijn geen bezwaar indient, wordt het betreffende Beveiligingsincident geacht definitief te zijn afgesloten per het moment van de oorspronkelijke kennisgeving. Indien Deelnemer binnen de gestelde termijn gemotiveerd bezwaar maakt, wordt de voorgestelde afsluiting geacht te zijn opgeschort en blijft het Beveiligingsincident open. Opdrachtnemer is in dat geval gehouden het incident opnieuw te behandelen en passende vervolgacties te ondernemen, totdat overeenstemming is bereikt over afsluiting, dan wel totdat de grond voor het bezwaar is weggenomen. De door Opdrachtnemer gehanteerde procedure voor incidentafsluiting en bezwaar dient aantoonbaar onderdeel te zijn van de gehanteerde SOC-processen en dient reproduceerbaar en auditbaar te zijn.
	Beschikbaarheid en service levels
A.65	Opdrachtnemer levert Beveiligingsincident Response binnen de overeengekomen Service Levels, bestaande uit de volgende varianten: Basispakket Beveiligingsincident Response tijdens kantoor tijden (08:00–17:00 uur op Werkdagen). Uitbreidingsoptie 1 Beveiligingsincident Response op verzoek van de Deelnemer tijdens Werkdagen buiten kantoor tijden (17:00–23:00 uur). Uitbreidingsoptie 2 Beveiligingsincident Response op verzoek van de Deelnemer 24 uur per dag, 7 dagen per week (7×24). De Deelnemer kan per variant kiezen, conform de opdrachtverstrekking.
	Verbetering en rapportage
A.66	Opdrachtnemer levert proactief advies over verbetermaatregelen op basis van trends, patronen en herhaalde elementen in de geregistreerde Beveiligingsincidenten.

	Samenwerking derden		
A.67	De Deelnemer is bevoegd een private of publieke partij aan te wijzen die optreedt als contactpunt en gemachtigde in het kader van Beveiligingsincident Response. De Deelnemer en Opdrachtnemer leggen voorafgaand aan de dienstverlening schriftelijk vast welke bevoegdheden, verantwoordelijkheden en communicatierechten deze partij heeft namens de Deelnemer. Opdrachtnemer beschouwt deze partij als volledig bevoegd binnen de vastgelegde kaders.		
	Coördinatie bij gedeelde beveiligingsincidenten		
A.68	Indien een Beveiligingsincident een dreiging vormt voor meerdere Deelnemers, vervult de Opdrachtnemer een coördinerende rol. Dit omvat het: 1. Tijdig informeren van alle betrokken Deelnemers en, indien van toepassing, de Opdrachtgever (regieorganisatie); 2. Afstemmen van analyse- en responsactiviteiten tussen de betrokken Deelnemers; 3. Coördineren van gezamenlijke mitigatie- en herstelmaatregelen; 4. Documenteren van acties, besluiten en communicatie met alle betrokken partijen.		
SLA-paramaters			
A.69	Reactie Tijd Opdrachtnemer (RTO)		
	SLA: Opdrachtnemer neemt binnen de volgende Reactietijden contact op met de Deelnemer of geautoriseerde Derden.		
	Prioriteit	Reactietijd in % van de gevallen binnen:	
		80%	100%
	P1 – Kritiek	30 minuten	1 uur
	P2 – Hoog	1 uur	4 uur
	P3 – Medium	4 uur	24 uur
Doel: Tijdige en correcte prioritering van incidenten voor adequate respons.			
A.70	Mean Time To Contain (MTTC)		
	Opdrachtnemer realiseert met de Deelnemer of geautoriseerde Derden de volgende maximale containertijden voor vastgestelde Beveiligingsincidenten: a. Critical Beveiligingsincidenten: ≤ 4 uur b. High Beveiligingsincidenten: ≤ 8 uur		
	De containmenttijd wordt gemeten vanaf het moment van formele Beveiligingsincidentclassificatie door Opdrachtnemer tot het moment waarop adequate containmentmaatregelen aantoonbaar zijn toegepast.		

A.71	Mean Time To Investigate (MTTI) Opdrachtnemer voert met de Deelnemer of geautoriseerde Derden voor alle Beveiligingsincidenten de vereiste onderzoeksactiviteiten uit binnen de volgende maximale analysetijden: a. Critical Beveiligingsincident: initiële analyse ≤ 2 uur; volledige analyse ≤ 24 uur b. High Beveiligingsincident: initiële analyse ≤ 4 uur; volledige analyse ≤ 48 uur De analysetijd wordt gemeten vanaf het moment van formele Beveiligingsincidentclassificatie.
A.72	Mean Time To Recover / Resolve (MTTR) Opdrachtnemer draagt zorg voor mitigatie en/of afhandeling van Beveiligingsincident binnen de volgende maximale oplostijden: a. Critical Beveiligingsincident: ≤ 48 uur b. High Beveiligingsincident: ≤ 72 uur Indien herstel afhankelijk is van Deelnemer of Derden, levert Opdrachtnemer uiterlijk binnen 24 uur een gedetailleerd en uitvoerbaar mitigatie- of hersteladvies. De oplostijd wordt gemeten vanaf het moment van formele classificatie als Beveiligingsincident tot het moment waarop het Beveiligingsincident is gemitigeerd of opgelost, voor zover dit binnen de invloedssfeer van de Opdrachtnemer ligt.
A.73	Root Cause Analysis (RCA) Opdrachtnemer levert voor alle Critical en High Beveiligingsincidenten een volledige en aantoonbaar onderbouwde Root Cause Analysis (RCA) aan binnen 5 Werkdagen na afsluiting van het Beveiligingsincident. De RCA bevat minimaal: oorzaak, aanvalsvector, gebruikte TTP's, tijdlijn, getroffen systemen, effect op dienstverlening, getroffen maatregelen en aanbevelingen. Opdrachtnemer kan ervan uitgaan dat de Deelnemer of geautoriseerde Derden alle medewerking verlenen met hun noodzakelijke inbreng voor de Root Cause Analysis.

A.74	Beveiligingsincidentcommunicatie en escalatie
	Opdrachtnemer hanteert de volgende maximale communicatietermijnen: - Eerste Beveiligingsincidentmelding aan Deelnemer: ≤ 15 minuten na classificatie als Beveiligingsincident; - Statusupdates: - Critical Beveiligingsincidenten: minimaal elke 1 uur - High Beveiligingsincidenten: minimaal elke 4 uur Alle communicatie wordt vastgelegd in het Beveiligingsincidentbeveiligingscoördinator systeem van Deelnemer of via de overeengekomen ITSM-koppeling.
A.75	<i>SLA:</i> Indien een Beveiligingsincident wordt geclassificeerd als Critical (P1), ondersteunt de Opdrachtnemer tijdige escalatie naar het CSIRT van de Deelnemer. CSIRT-escalatie vindt plaats binnen 30 minuten na classificatie als Critical beveiligingsincident (zie ook 3.2.3 CSIRT activatie). Indien een Beveiligingsincident wordt geclassificeerd als Critical (P1), ondersteunt de Opdrachtnemer tijdige melding naar het sectorale CSIRT (NCSC). Melding bij het sectorale CSIRT vindt plaats binnen 24 uur.
A.76	Forensische veiligstelling (optioneel inzetbaar)
	Indien forensische veiligstelling noodzakelijk is, start Opdrachtnemer de forensische dataverzameling binnen 1 uur na verzoek van Deelnemer en levert een volledig forensisch datapakket binnen 48 uur, tenzij anders overeengekomen. Alle data wordt veiliggesteld conform ISO 27037, chain-of-custody-richtlijnen en wettelijke vereisten.
A.77	Beveiligingsincidentdocumentatie en -rapportage
	Opdrachtnemer levert voor alle Critical en High Beveiligingsincidenten een volledig Beveiligingsincidentrapport aan binnen 5 Werkdagen na afsluiting. Het rapport bevat minimaal: classificatie, impact, oorzaak, detectiepad, tijdlijnen, schakeling met SOC-processen, uitgevoerde acties, resterende risico's en structurele aanbevelingen.
A.78	Wettelijke meldplichten (Cbw, AVG, BIO)
	Bij constatering van een (mogelijk) meldingsplichtig incident informeert Opdrachtnemer de Deelnemer binnen 1 uur na eerste detectie. Opdrachtnemer levert alle technische bevindingen, logs en indicators of compromise (IoC's) die noodzakelijk zijn voor de Cbw-vroegtijdige waarschuwing (24 uur) en incident notification (72 uur), uiterlijk binnen 4 uur na constatering, ongeacht of de Deelnemer hierom heeft verzocht.
Deliverables	
A.79	Escalatieoverzichten
	Opdrachtnemer waarborgt dat inzicht beschikbaar is in geëscaleerde Beveiligingsincidenten, inclusief reden van escalatie, genomen acties en resterende risico's, conform paragraaf 1.3 Overkoepelende rapportage-eis.

A.80	Periodieke overlegsessies
	Opdrachtnemer neemt deel aan periodieke overleggen met de Deelnemer, waaronder minimaal: a. maandelijks SOC-operational overleg; b. kwartaal strategisch overleg; c. use-case en detectie-refinement-sessies. De beschikbare informatie zoals bedoeld in paragraaf 1.3 Overkoepelende rapportage-eis vormt de basis voor sturing, besluitvorming en escalatie binnen deze overleggen.
A.81	Beveiligingsincidentrapportages
	Opdrachtnemer levert voor ieder door hem geanalyseerd of behandeld Beveiligingsincident een Beveiligingsincidentrapportage, inclusief root-cause analyse, impactanalyse, tijdlijn, gebruikte TTP's, genomen maatregelen en aanbevelingen.
A.82	Overdrachtsrapportages
	Opdrachtnemer levert bij relevante Beveiligingsincidenten, wijzigingen of bij contractbeëindiging overdrachtsrapportages met alle relevante documenten, configuraties, detectiecontent en logdata, in een overdraagbaar formaat.

3.2.3 Basis - CSIRT activatie

2.3 CSIRT activatie

Doel: Het tijdig en gecontroleerd activeren van het Computer Security Incident Response Team (CSIRT) van de Deelnemer om ernstige of potentiële Beveiligingsincidenten snel, gecoördineerd en effectief te kunnen afhandelen.

Wat valt hieronder?

- Classificatie en escalatie van security-Beveiligingsincidenten op basis van vooraf vastgestelde criteria (bijv. impact, urgentie, type bedreiging).
- Formele activering van het CSIRT wanneer een Beveiligingsincident boven een vooraf bepaalde drempelwaarde uitkomt.
- Mobilisatie van noodzakelijke rollen en expertise, waaronder:
 - Beveiligingsincidentmanager
 - Technisch analisten (forensics, malware, netwerk)
 - Communicatieadviseur
 - Privacy officer / FG
 - Juridische ondersteuning
- Coördineren van de responsactiviteiten, zoals:
 - Beheersmaatregelen (containment)
 - Herstelacties
 - Onderzoek naar oorzaak (root cause)
 - Terugdringen van verdere schade
- Communicatie en notificaties, waaronder:
 - Interne meldingen (IT, management, directie)
 - Wettelijke meldplicht (bijv. AP, NCSC, sector-CERTs)
 - Communicatie naar ketenpartners of leveranciers
- Documenteren van alle acties en besluiten gedurende het Beveiligingsincident.
- Ondersteuning bij besluitvorming door het leveren van actuele technische en tactische inzichten.
- Documenteren van alle acties en besluiten gedurende het Beveiligingsincident, inclusief analyse-informatie en communicatie met interne en externe partijen, met inachtneming van geldende bewaartermijnen.
- Afsluiting en post-Beveiligingsincident review, inclusief aanbevelingen voor verbetermaatregelen.

Kernvraag: *Wanneer en hoe moet het CSIRT worden geactiveerd om een ernstig Beveiligingsincident effectief te beheersen en schade te beperken?*

Resultaat: Een gecoördineerde inzet van het CSIRT, gericht op snelle stabilisatie van de situatie, minimalisering van schade, en volledige documentatie en evaluatie van het Beveiligingsincident.

Eisen	
	Algemene samenwerking en wettelijke kaders
A.83	Opdrachtnemer borgt dat de samenwerking met (sectorale of externe) CSIRTs plaatsvindt conform de geldende wet- en regelgeving en relevante sectorale normen, waaronder in ieder geval Cbw, BIO en ISO 27035. Afwijkingen worden door Opdrachtnemer gerapporteerd en voorzien van verbetervoorstellen.
A.84	Opdrachtnemer onderhoudt structurele en aantoonbare samenwerking met het NCSC en relevante sectorale CSIRTs, conform wettelijke verplichtingen en sectorguidelines.

	Escalatie, activatie en rolverdeling
A.85	Opdrachtnemer faciliteert en ondersteunt de tijdige activatie van het (Deelnemer, sectorale of externe) CSIRT en handelt daarbij conform vooraf overeengekomen verantwoordelijkheden, escalatiepaden en communicatiestandaarden.
A.86	Opdrachtnemer beschikt over actuele, gedocumenteerde en periodiek (minimaal jaarlijks) geteste escalatieprocedures tussen Deelnemer, Opdrachtnemer en CSIRT.
A.87	Opdrachtnemer escaleert Critical Beveiligingsincidenten (P1) naar het CSIRT van de Deelnemer op basis van vooraf vastgestelde en door alle betrokken partijen goedgekeurde procedures.
	Afstemming tijdens Beveiligingsincidenten
A.88	Opdrachtnemer stemt tijdens Beveiligingsincidenten nauw af met het Deelnemers CSIRT over escalaties, containment-maatregelen, forensische veiligstelling, analyseactiviteiten en de overdracht van relevante logs en artefacten.
A.89	Opdrachtnemer adviseert Deelnemer actief bij besluitvorming over containment, mitigatie en herstel, en zorgt dat relevante informatie realtime of near-realtime beschikbaar is voor het CSIRT van de Deelnemer.
A.90	Opdrachtnemer garandeert 24/7 beschikbaarheid van een Beveiligingsincidentcoördinator (inclusief achterwacht) tijdens CSIRT-activaties. De Beveiligingsincidentcoördinator is verantwoordelijk voor: • centrale regie en coördinatie van de incidentafhandeling; • afstemming met Deelnemer(s) en relevante stakeholders; • bewaking van voortgang, prioriteiten en besluitvorming; • aansturing van betrokken SOC-analisten en eventuele specialistische rollen; • tijdige en eenduidige communicatie (inclusief escalaties); • borging van dossiervorming en overdracht. De rol van Beveiligingsincidentcoördinator kan worden ingevuld door een dienstdoende SOC-analist, mits: • deze aantoonbaar beschikt over voldoende senioriteit en ervaring met incidentcoördinatie; • de rol en verantwoordelijkheden expliciet zijn belegd en vastgelegd; • de coördinatietask niet conflicteert met uitvoerende analysewerkzaamheden; • waar nodig aanvullende capaciteit (bijv. extra analist) wordt ingezet. Opdrachtnemer borgt dat bij complexe of grootschalige incidenten tijdig opschaling plaatsvindt naar een dedicated coördinator.
	Informatie-uitwisseling en technische eisen
A.91	Opdrachtnemer wisselt tijdig, volledig en accuraat informatie uit over dreigingen, kwetsbaarheden en Beveiligingsincidenten met CSIRTs, met inachtneming van alle relevante classificatie- en TLP-richtlijnen.
A.92	Opdrachtnemer gebruikt uitsluitend door de Deelnemer goedgekeurde, versleutelde communicatiemiddelen (zoals TLS, VPN of end-to-end encrypted messaging) voor alle informatie-uitwisseling met CSIRTs.

A.93	Opdrachtnemer hanteert standaard Beveiligingsincidentformaten, waaronder in ieder geval IEP, STIX en/of TAXII, evenals TLP-classificatie voor alle meldingen, rapportages en informatie-overdracht aan CSIRTs.
A.94	Opdrachtnemer zorgt dat relevante logging, telemetry, artefacten en alert-data tijdig, volledig en in forensisch verantwoorde vorm beschikbaar zijn voor CSIRTs.
A.95	Opdrachtnemer hanteert formele chain-of-custody-procedures voor alle digitale bewijsmaterialen die met het CSIRT worden gedeeld.
A.96	Opdrachtnemer hanteert overeengekomen SLA's/OLA's voor informatie-uitwisseling met CSIRTs, waaronder maximale responstijden op informatieverzoeken.
	Contactstructuur
A.97	De Opdrachtnemer stelt telefoonnummer beschikbaar inclusief achterwacht die 24/7 bereikbaar zijn en fungeren als aanspreekpunten voor CSIRT afstemming.
	Oefenen, testen en evalueren
A.98	Opdrachtnemer neemt minimaal jaarlijks deel aan gezamenlijke Beveiligingsincident-response-oefeningen met het CSIRT van de Deelnemer en verwerkt de daarbij behaalde leerpunten aantoonbaar in relevante procedures, werkinstructies en verbeterplannen.
A.99	Opdrachtnemer evalueert minimaal jaarlijks de samenwerking met het CSIRT van de Deelnemer en stelt concrete, toetsbare verbetervoorstellen op, die worden opgenomen in een gezamenlijk verbeterplan.
	Externe communicatie
A.100	Opdrachtnemer stemt met het CSIRT van de Deelnemer af welke externe communicatie wordt verricht bij majeure Beveiligingsincidenten, waaronder (indien van toepassing) persvoorlichting, woordvoering en overige externe berichtgeving.
SLA-paramaters	
A.101	Beschikbaarheid incidentcoördinator
	SLA: Opdrachtnemer garandeert dat vanaf dat de eerste Deelnemer 24/7 dienstverlening afneemt, een 24/7 beschikbaarheid van een aangewezen incidentcoördinator voor CSIRT-activaties, inclusief bereikbare achterwacht.
	Doel: Ononderbroken coördinatie van escalaties en communicatie bij beveiligingsincidenten.
A.102	Reactietijd op incidentmeldingen
	SLA: Opdrachtnemer bevestigt ontvangst en start coördinatie binnen 15 minuten na escalatie van een ernstig beveiligingsincident naar CSIRT.
	Doel: Tijdige activering van CSIRT en minimale vertraging in containment- en mitigatiemaatregelen.

A.103	Escalatie van ernstige incidenten
	SLA: Alle incidenten die voldoen aan vooraf gedefinieerde criteria (bijv. high-severity of impact op kritieke processen) worden binnen 30 minuten geëscaleerd naar CSIRT, conform gedocumenteerde procedures.
	Doel: Consistente en tijdige escalatie bij kritieke incidenten.
A.104	Uitwisseling van relevante data en logs
	SLA: Alle relevante logging, telemetry, artefacten en alert-data worden binnen 1 uur na CSIRT-activatie beschikbaar gesteld, in forensisch verantwoorde vorm en volgens afgesproken chain-of-custody procedures.
	Doel: Efficiënte analyse, containment en herstel door CSIRT.
A.105	Gebruik van beveiligde communicatiekanalen
	SLA: Alle communicatie met CSIRT vindt plaats via versleutelde en door Deelnemer goedgekeurde kanalen (bijv. TLS, VPN, end-to-end messaging).
	Doel: Bescherming van gevoelige informatie en naleving van security policies.
A.106	Joint decision making en real-time informatie
	SLA: Opdrachtnemer neemt actief deel aan gezamenlijke besluitvorming met CSIRT over containment, mitigatie en herstel, waarbij relevante informatie realtime of near-realtime beschikbaar is.
	Doel: Effectieve en gecoördineerde respons tijdens incidentafhandeling.
A.107	Evaluatie van samenwerking
	SLA: Opdrachtnemer evalueert minimaal één keer per jaar de samenwerking met CSIRT en rapporteert concrete verbetervoorstellen, inclusief opname in een verbeterplan.
	Doel: Continu verbeteren van procedures, escalatiepaden en samenwerking met CSIRT.
Deliverables	
	Activerings- en inzetdocumentatie
A.108	Opdrachtnemer levert per activatie een formele CSIRT-activatiebevestiging, inclusief het tijdstip van melding, het moment van daadwerkelijke activatie, betrokken responsteamleden en toegewezen rollen.
A.109	Opdrachtnemer levert een initiële incidentbeoordeling binnen de overeengekomen responstijd, met een eerste inschatting van aard, ernst, potentiële impact en voorgestelde vervolgstappen.

	Voortgang en uitvoering
A.110	Opdrachtnemer verstrekt een actierapportage per CSIRT-activatie, waarin alle uitgevoerde handelingen, beslismomenten, escalaties en communicatieacties aantoonbaar zijn vastgelegd.
A.111	Opdrachtnemer levert een periodieke voortgangsrapportage gedurende de inzet, waarin status, risico-inschatting, openstaande acties en afhankelijkheden zijn beschreven.
A.112	Opdrachtnemer documenteert alle interacties met interne en externe stakeholders, waaronder Deelnemers, ketenpartners, leveranciers en nationale cybersecurityorganisaties, inclusief gedeelde informatie en verkregen adviezen. Opdrachtnemer waarborgt dat alle documentatie, waaronder incidentgegevens, analyse-informatie, communicatie-uitingen en besluitvorming in het kader van CSIRT-activaties, gedurende minimaal drie (3) jaar wordt bewaard, conform BIO2-overheidsmaatregel 5.28.01, en op verzoek volledig en herleidbaar beschikbaar wordt gesteld aan Opdrachtgever en/of bevoegde instanties.
	Afronding en evaluatie
A.113	Opdrachtnemer levert een eindrapportage per CSIRT-activatie, inclusief volledige tijdlijn, root-cause-analyse, impactanalyse, uitgevoerde mitigerende maatregelen en aanbevelingen voor structurele verbeteringen.
A.114	Opdrachtnemer levert een audit-trail van alle relevante communicatie, besluitvorming en loggebeurtenissen die onderdeel waren van de CSIRT-activatie.
A.115	Opdrachtnemer levert een voorstel voor verbeteracties, gericht op optimalisatie van incidentresponsprocessen, tooling en samenwerking met Deelnemers.
	Governance & borging
A.116	Opdrachtnemer levert jaarlijks een geaggregeerde analyse van alle CSIRT-activaties, inclusief trends, patronen in responstijden, terugkerende kwetsbaarheden en aanbevelingen voor procesverbetering.

3.3 Basis - Threat intelligence

3 Threat intelligence

Doel: Het analyseren en duiden van dreigingen en aanvalspatronen, en het vertalen hiervan naar prioriteiten, detectievereisten en handelingsperspectieven voor de organisatie.

Karakter: Primair richtinggevend, voorspellend en contextueel.

Wat valt hieronder?

- Verzamelen en analyseren van externe en interne dreigingsinformatie (IoC's, TTP's, campagnes, kwetsbaarheden)
- Opstellen van dreigingsbeelden en prioritering op basis van sector, dreigingsactoren en organisatiecontext
- Vertalen van dreigingsinformatie naar:

- detectievereisten en use-cases
- risico-inschattingen en impactanalyses
- aanbevelingen voor monitoring, patching en mitigatie
- Verrijken van incidenten met dreigingscontext (actor, campagne, motief)
- Signaleren van trends en emerging threats
- Adviseren over aanpassingen in detectie- en responsstrategie

Expliciete afbakening: Threat Intelligence voert geen structurele, operationele detectie of actieve zoekacties uit binnen de SIEM-data; deze activiteiten vallen onder Threat Hunting.

Kernvraag: *Welke dreigingen zijn relevant voor de organisatie en hoe moet de detectie- en beveiligingsstrategie hierop worden aangepast?*

Resultaat: Dreigingsgestuurde prioriteiten en concrete input voor detectie, hunting en respons.

Eisen	
	Doel, scope en dienstverlening
A.117	Opdrachtnemer levert de dienst Threat Intelligence, gericht op het verkrijgen, analyseren, verrijken en distribueren van actuele en potentiële dreigingsinformatie, met als doel het SOC in staat te stellen proactief en effectief dreigingen te detecteren, te voorkomen en hierop te reageren.
A.118	De geleverde Threat Intelligence omvat niet uitsluitend dataverzameling, maar het omzetten van dreigingsdata naar bruikbare, contextuele en actiegerichte informatie voor detectie-, preventie- en responsdoeleinden.
	Dreigingsbronnen en dataverzameling
A.119	Opdrachtnemer verzamelt, analyseert en deelt dreigingsinformatie op basis van externe bronnen, waaronder in ieder geval ISAC's, CERT's, commerciële TI-feeds en relevante Beveiligingsincidentdata van decentrale overheden en provincies.
A.120	Opdrachtnemer verzamelt en levert sectorspecifieke dreigingsinformatie, gericht op decentrale overheden en provincies, inclusief relevante trends, actoren en TTP's.
	Analyse, verrijking en duiding
A.121	Opdrachtnemer verrijkt dreigingsinformatie met relevante context, waaronder TTP's, MITRE ATT&CK-mapping, indicatoren, dreigingsactorprofielen en risicoduiding.
A.122	Opdrachtnemer koppelt de dreigingsinformatie aan de infrastructuur, systemen en IT-assets van de Deelnemer, zodat gericht inzicht ontstaat in mogelijke impact en kwetsbaarheden.
A.123	Opdrachtnemer duidt welke dreigingen relevant zijn voor de Deelnemer, inclusief prioritering op basis van risico, impact en waarschijnlijkheid.
A.124	Opdrachtnemer correleert dreigingsinformatie automatisch met beschikbare SIEM-data, Beveiligingsincidentmeldingen en detectiesignalen, ten behoeve van verrijkte detectie en versneld Beveiligingsincidentonderzoek.
A.125	Opdrachtnemer adviseert proactief over geïdentificeerde dreigingen, inclusief aanbevelingen voor preventieve, mitigatieve en detective maatregelen.

	Integratie in SOC-processen
A.126	De door Opdrachtnemer geleverde Threat Intelligence is integraal onderdeel van de detectie-, analyse- en responsprocessen van het SOC van de Deelnemer.
A.127	Opdrachtnemer ondersteunt automatische verwerking van TI-data binnen de SOC-tooling van de Deelnemer, waaronder SIEM-, SOAR- en CMDB-systemen.
	Technische interoperabiliteit en standaarden
A.128	Threat Intelligence voldoet aan gangbare interoperabiliteitsstandaarden, waaronder STIX en TAXII.
A.129	De door Opdrachtnemer geleverde dreigingsinformatie is machine leesbaar en geschikt voor geautomatiseerde verwerking binnen de keten van detectie- en responsmiddelen.
A.130	Opdrachtnemer levert volledige en actuele documentatie en API-koppelingen voor ontsluiting van TI-data naar systemen van de Deelnemer.
	Beveiliging, toegang en vertrouwelijkheid
A.131	Opdrachtnemer slaat alle dreigingsinformatie versleuteld op en verzendt deze versleuteld, conform door de Deelnemer goedgekeurde methoden. Opdrachtnemer waarborgt dat dreigingsinformatie, inclusief onderliggende analyse, verrijking en broninformatie, gedurende minimaal drie (3) jaar wordt bewaard, conform BIO2-overheidsmaatregel 5.28.01, en op verzoek volledig en herleidbaar beschikbaar wordt gesteld aan Opdrachtgever en/of bevoegde instanties.
A.132	Alleen geautoriseerde gebruikers krijgen toegang tot dreigingsinformatie en onderliggende artefacten, waarbij Opdrachtnemer passende authenticatie- en autorisatiemaatregelen hanteert.
	Organisatorische eisen en samenwerking
A.133	Opdrachtnemer beschikt over een team van Threat Intelligence-analisten met aantoonbare ervaring in cyberdreigingsanalyse, sectorspecifieke dreigingen en TTP-duiding.
A.134	Opdrachtnemer neemt actief deel aan relevante samenwerkingsverbanden, waaronder in ieder geval NCSC, ISAC's en sectorale CERT's.
A.135	Deelname aan informatie-uitwisseling met andere overheden (formeel en operationeel) is vereist.
SLA-paramaters	
A.136	Beschikbaarheid van dreigingsinformatiefeeds
	SLA: Opdrachtnemer garandeert dat machine leesbare dreigingsinformatiefeeds (STIX/TAXII) minimaal 99,5% van de tijd per maand beschikbaar zijn, exclusief vooraf geplande onderhoudsvensters.
	Doel: Continu gebruik van actuele dreigingsinformatie in SOC-detectie- en preventieprocessen.

A.137	Frequentie periodieke dreigingsrapportages
	SLA: Opdrachtnemer levert periodieke dreigingsrapportages met een minimale frequentie van één keer per maand, conform overeengekomen format en inhoud.
	Doel: Tijdige beschikbaarheid van contextuele dreigingsinformatie voor besluitvorming en risicobeheersing.
A.138	Ad-hoc waarschuwingen bij urgente dreigingen
	SLA: Opdrachtnemer verstrekt ad-hoc waarschuwingen binnen 2 uur na identificatie van kritieke of urgente dreigingen die impact kunnen hebben op Deelnemers.
	Doel: Snelle detectie en escalatie ter ondersteuning van SOC-acties.
A.139	Volledigheid en bruikbaarheid van dreigingsinformatie
	SLA: Alle geleverde Threat Intelligence bevat minimaal de volgende elementen: TTP's (MITRE ATT&CK mapping), assetrelevantie, risicobeoordeling en herkomst van informatie.
	Doel: Contextuele en bruikbare informatie voor effectieve detectie, preventie en respons.
A.140	Integratie met SOC-detectieprocessen
	SLA: Dreigingsinformatie wordt geïntegreerd in de detectie-, analyse- en responsprocessen van het SOC binnen 1 Werkdag na levering, voor zover deze technisch compatibel is met de SOC-tooling en prioriteit heeft op basis van risico-inschatting.
	Doel: Directe toepasbaarheid van Threat Intelligence voor operationele security monitoring.
A.141	Documentatie van bronnen en certificeringen
	SLA: Opdrachtnemer documenteert alle gebruikte bronnen, hun betrouwbaarheid en certificeringen, en werkt deze documentatie minimaal één keer per kwartaal bij.
	Doel: Transparantie, auditability en naleving van compliance-eisen.
A.142	Toegankelijkheid en beveiliging
	SLA: Alleen geautoriseerde gebruikers hebben toegang tot dreigingsinformatie, waarbij data versleuteld wordt opgeslagen en verzonden.
	Doel: Bescherming van gevoelige informatie en naleving van security policies.
Deliverables	
A.143	Wekelijkse dreigingsupdates
	Opdrachtnemer levert wekelijks updates over nieuwe dreigingen die relevant zijn voor provincies en het overheidsdomein, inclusief context en mogelijke impact op de infrastructuur van Deelnemers. Deze mogen in het Engels worden verstrekt.
A.144	Periodieke dreigingsrapportages

	Opdrachtnemer verstrekt periodieke dreigingsrapportages met een minimale frequentie van één keer per maand, inclusief analyse van trends, potentiële risico's en aanbevelingen voor preventieve maatregelen. Deze mogen in het Engels worden verstrekt.
A.145	Ad-hoc urgente dreigingswaarschuwingen Opdrachtnemer verstrekt onverwijld ad-hoc waarschuwingen bij het constateren van nieuwe of kritieke dreigingen die directe impact kunnen hebben op de Deelnemers. Deze mogen in het Engels worden verstrekt.
A.146	Machineleesbare dreigingsfeeds Opdrachtnemer levert dreigingsinformatie aan Deelnemers in machineleesbare vorm, conform standaarden zoals STIX en TAXII, geschikt voor automatische verwerking en integratie in SOC-platformen.
A.147	Bronvermelding en certificering Opdrachtnemer documenteert alle gebruikte dreigingsbronnen, inclusief certificeringen en herkomst, en verstrekt deze informatie op verzoek aan Deelnemers.

3.4 Basis - Rapportage & dashboards

4 Rapportage en dashboarding

Doel: Het creëren en ontsluiten van inzichtelijke, betrouwbare en tijdige rapportages en dashboards die de beveiligingsstatus, trends, prestaties en risico's van de organisatie duidelijk maken.

Wat valt hieronder?

- Opstellen, beheeren en verbeteren van periodieke SOC-rapportages, zoals maandrapportages, kwartaalrapportages en SLA/KPI-overzichten.
- Ontwikkelen en onderhouden van dashboards voor real-time inzicht in Events, Beveiligingsincidenten, trends, logvolledigheid, SOC-prestaties en dreigingsniveaus.
- Visualiseren van operationele en strategische KPI's, waaronder MTBD, MTTA, logvolledigheid, Eventvolumes en Beveiligingsincidenttrends.
- Rapporteren over naleving van wet- en regelgeving en normenkaders, zoals de Cbw, ISO 27001/2 en BIO.
- Analyseren van data om structurele trends, patronen of afwijkingen te identificeren (bijv. pieken in aanvallen, toename in bronuitval, herhaalde Beveiligingsincidenttypen).
- Leveren van managementinformatie en verbeteradviezen op basis van monitoring- en Beveiligingsincidentdata.
- Bewaken van datakwaliteit zodat rapportages en dashboards accuraat, volledig en eenduidig zijn.
- Afstemmen van rapportageformaten met verschillende stakeholders, zoals CISO, IT-beheer, directie en auditors.

Kernvraag: Is relevante, betrouwbare en actuele informatie beschikbaar voor besluitvorming, verbetering en verantwoording?

Resultaat: Heldere, gestructureerde en actiegerichte rapportages en dashboards die per Deelnemer en overall inzicht geven in de beveiligingspositie en prestaties van het SOC en die bijdragen aan continue verbetering van securityprocessen.

Eisen	
	Kaders en verantwoordelijkheden
A.148	Rapportages en dashboards voldoen minimaal aan de vereisten uit de BIO, Cbw en AVG.
A.149	Opdrachtnemer is verantwoordelijk voor de juistheid, volledigheid, tijdigheid en continuïteit van alle data die wordt gebruikt voor rapportages, dashboards en prestatie-informatie, voor zover deze data correct, volledig en tijdig wordt aangeleverd door de Deelnemer en beschikbaar is binnen het onderliggende platform.
A.150	Opdrachtnemer draagt zorg voor het volledig en actueel bijhouden van alle informatie die aan rapportages en dashboards ten grondslag ligt.
A.151	Informatie uit rapportages en dashboards zijn nadrukkelijk ondersteunend van aard en bedoeld om de Deelnemer in staat te stellen geïnformeerde beslissingen te nemen. De Opdrachtnemer is niet verantwoordelijk voor het integraal vaststellen van het securitybeeld, risicobereidheid of prioriteiten van de Deelnemer.
	Inhoud en kwaliteit van rapportages
A.152	Opdrachtnemer levert rapportages en dashboards per Deelnemer en overall die inzicht en transparantie bieden in de beveiligingsstatus, gedetecteerde dreigingen, Beveiligingsincidenttrends en de operationele prestaties van het SOC.
A.153	De rapportages ondersteunen besluitvorming, risicosturing en continue verbetering, en zijn afgestemd op de informatiebehoefte van de relevante doelgroepen (operationeel, tactisch en strategisch).
	Toegankelijkheid van data
A.154	Alle onderliggende data van rapportages, dashboards en prestatie-informatie zijn voor Deelnemers en Opdrachtgever respectievelijk regieorganisatie toegankelijk via een beveiligde interface, inclusief mogelijkheden voor dataportabiliteit en export ten behoeve van eigen analyses.
	Periodieke rapportageverplichtingen
A.155	Dienstenniveaus geven inzicht in het functioneren van de geleverde Prestatie(s). Opdrachtnemer rapporteert periodiek aan Deelnemer en Opdrachtgever conform de rapportage-eisen en frequentie zoals vastgelegd in de SLA.
A.156	Periodieke rapportages bevatten ten minste afwijkingen, root-cause analyses, genomen corrigerende maatregelen en de impact op de overeengekomen dienstenniveaus.
	Correcties, afwijkingen en herstelmaatregelen
A.157	Indien sprake is van foutieve of vermoedelijk foutieve informatie in rapportages of dashboards, levert Opdrachtnemer op eerste verzoek aanvullend bewijs, corrigeert de informatie onverwijld en verstrekt een gecorrigeerde rapportage met toelichting op de oorzaak.

A.158	Indien rapportages aantonen dat de geleverde Prestatie afwijkt van de overeengekomen afspraken of normen, neemt Opdrachtnemer direct herstel- en preventieve maatregelen. Deze maatregelen worden afgestemd met Deelnemer en vastgelegd in de eerstvolgende rapportagecyclus.
	Kosten
A.159	Alle kosten voor het opstellen, onderhouden en opleveren van rapportages en dashboards, inclusief maatwerkrapportages, zijn inbegrepen in de tarieven van de Prestatie en worden niet afzonderlijk in rekening gebracht.
SLA-paramaters	
A.160	Beschikbaarheid van dashboards
	SLA: Opdrachtnemer garandeert dat dashboards minimaal 99,5% van de tijd per maand beschikbaar zijn, exclusief vooraf geplande onderhoudsvensters, voor zover de beschikbaarheid van onderliggende platformen en diensten van derden dit toelaat.
	Doel: Continu inzicht in actuele dreigingen, incidentstatussen en beveiligingsindicatoren.
A.161	Levering van periodieke rapportages
	SLA: Opdrachtnemer levert alle afgesproken periodieke rapportages (bijv. maandelijks, kwartaal) binnen 5 Werkdagen na afloop van de rapportageperiode.
	Doel: Tijdige beschikbaarheid van actuele informatie voor besluitvorming en compliance.
A.162	Volledigheid van rapportages
	SLA: Rapportages bevatten minimaal alle overeengekomen KPI's, KSI's, SLA-indicatoren en trends zoals vastgelegd in het DAP of contract.
	Doel: Consistente en volledige informatie voor monitoring en evaluatie.
A.163	Ad-hoc rapportages en alerts
	SLA: Opdrachtnemer levert ad-hoc rapportages of waarschuwingen binnen 24 uur na verzoek of detectie van urgente dreigingen of afwijkingen.
	Doel: Snelle escalatie en ondersteuning bij incidentafhandeling.
A.164	Integriteit en betrouwbaarheid van data
	SLA: Alle rapportages en dashboards tonen actuele en gevalideerde data, waarbij $\geq 98\%$ van de logbronnen zichtbaar en correct verwerkt zijn, rekening houdend met de latency van logaanlevering en verwerking binnen het SOC-platform.
	Doel: Verzekering van betrouwbare besluitvorming en compliance.
A.165	Toegankelijkheid en gebruikersbeheer
	SLA: Dashboards en rapportages zijn toegankelijk voor geautoriseerde gebruikers, met ondersteuning voor federated identity (SAML/OpenID Connect) en MFA.

	Doel: Bescherming van gevoelige informatie en naleving van security policies.
A.166	Documentatie van wijzigingen
	SLA: Opdrachtnemer documenteert wijzigingen in dashboards, datastromen en rapportages binnen 7 Werkdagen na implementatie.
	Doel: Transparantie en auditability van informatievoorziening.
Deliverables	
A.167	Periodieke prestatie- en voortgangsrapportages
	Opdrachtnemer levert periodieke rapportages conform de overeengekomen prestatie-indicatoren (KPI's, KSI's en SLA's). Deze rapportages vormen een formele prestatieverklaring en bevatten minimaal alle afgesproken indicatoren, afwijkingen, root-cause analyses en corrigerende maatregelen.
A.168	Standaard dashboards
	Opdrachtnemer levert alle standaard dashboards die onderdeel zijn van de dienstverlening proactief en zonder aanvullende kosten aan Deelnemers en Hoofopdrachtgever. De dashboards bieden inzicht in actuele beveiligingsstatus, incidenten, dreigingen, logvolledigheid en prestatie-indicatoren.
A.169	Ad-hoc rapportages op verzoek
	Opdrachtnemer verstrekt op verzoek van Deelnemers of Hoofopdrachtgever aanvullende ad-hoc rapportages over specifieke gebeurtenissen, trends, incidentanalyses of compliance-gerelateerde onderwerpen.
A.170	Historische data en trendanalyses
	Opdrachtnemer maakt historische data en trendanalyses beschikbaar in de dashboards en rapportages, zodat ontwikkeling van dreigingen, incidenten en operationele prestaties over tijd inzichtelijk wordt.
A.171	Toegankelijkheid en exportmogelijkheden
	Opdrachtnemer stelt alle dashboards en rapportages beschikbaar via een beveiligd platform, inclusief exportmogelijkheden voor eigen analyse door de Deelnemers.
A.172	Rapportagedocumentatie
	Opdrachtnemer documenteert de methodiek, gebruikte bronnen en definities van alle indicatoren in de rapportages en dashboards, zodat consistentie en reproduceerbaarheid gewaarborgd zijn.

3.5 Basis - Use case management

5 Use case management

Doel: Het ontwikkelen, onderhouden en optimaliseren van detectie-use-cases die zorgen voor effectieve, actuele en risicogebaseerde signalering van beveiligingsdreigingen binnen de monitoringomgeving.

De invulling van Use Case Management vindt plaats conform en in samenhang met Bijlage 4 – SOC Use Case Roadmap. Deze roadmap beschrijft de gefaseerde opbouw, prioritering en standaardisatie van use cases en is leidend voor zowel de initiële inrichting als de doorontwikkeling van de SOC-dienstverlening.

Wat valt hieronder?

- Inventariseren van risico's, dreigingen en bedrijfsprocessen om te bepalen welke use-cases noodzakelijk zijn voor adequate monitoring.
- Ontwerpen, bouwen en configureren van use-cases en detectieregels binnen SIEM-, UEBA-, EDR/XDR- en andere monitoringplatforms.
- Afstemmen van use-cases op relevante normenkaders en compliance-eisen (zoals de Cbw, ISO 27001/2, BIO).
- Valideren en testen van use-cases op effectiviteit, detectiekwaliteit, performance en false positive/false negative ratio's.
- Periodieke evaluatie en actualisatie van bestaande use-cases op basis van nieuwe dreigingen, threat intelligence, Beveiligingsincidenttrends en wijzigingen in de IT/OT-omgeving.
- Versiebeheer en levenscyclusbeheer van use-cases, inclusief documentatie, wijzigingshistorie en rationale achter detectiologica.
- Adviseren over aanvullende logs, telemetry of technische aanpassingen die nodig zijn voor effectieve detectie.
- Samenwerken met security monitoring- en Beveiligingsincidentmanagementteams om detectiegaten te identificeren en prioriteiten bij te stellen.

Kernvraag: *Zijn de juiste detecties ingericht en worden dreigingen effectief, tijdig en relevantesignaleerd?*

Resultaat:

Een set geoptimaliseerde, gevalideerde en actuele use-cases die:

- aansluiten op de SOC Use Case Roadmap;
- uniform en herbruikbaar zijn voor meerdere Deelnemers;
- integraal onderdeel vormen van het security monitoringproces.

Eisen	
	Doel en scope
A.173	Opdrachtnemer levert de dienst Use Case Management, gericht op het gestructureerd, efficiënt en risicogericht uitvoeren van beveiligingsmonitoring en Beveiligingsincidentrespons. Use Case Management omvat ten minste het definiëren, beheren, evalueren en optimaliseren van detectiescenario's die door het SOC worden gebruikt om dreigingen tijdig te identificeren en hierop te reageren, conform de fasering en prioritering zoals opgenomen in Bijlage 3 – SOC Use Case Roadmap.
	Proces en lifecycle
A.174	Opdrachtnemer hanteert een aantoonbaar gestructureerd proces voor het definiëren, implementeren, testen, onderhouden en uitfaseren van SOC-use cases, waarbij ontwikkeling en prioritering aantoonbaar plaatsvinden conform de SOC Use Case Roadmap.

A.175	Opdrachtnemer beheert use cases volgens een volledige lifecycle, bestaande uit minimaal: creatie, validatie, onderhoud, periodieke review, optimalisatie en afbouw.
A.176	Opdrachtnemer onderhoudt een volledige audit-trail van alle wijzigingen, beslissingen en versies in de use case-documentatie.
	Risico-, compliance- en businessalignment
A.177	Use cases sluiten aan op de risico's, kritieke processen en businessdoelstellingen van de Deelnemer, inclusief expliciete dekking van alle kritieke processen.
A.178	Use cases voldoen aan relevante wet- en regelgeving en normen, waaronder maar niet beperkt tot BIO, Cbw en sectorale richtlijnen.
A.179	Opdrachtnemer adviseert Deelnemer over prioritering van use cases op basis van risicobeoordeling, actuele dreigingsinformatie en het sectorspecifieke dreigingslandschap.
	Kwaliteitsborging en periodieke evaluatie
A.180	Opdrachtnemer voert minimaal jaarlijks een volledige review uit op alle actieve use cases, gericht op relevantie, effectiviteit, kwaliteit en performance.
A.181	Opdrachtnemer organiseert jaarlijks gezamenlijke evaluatie- en optimalisatiesessies met Deelnemers om verbeteringen, prioritering en wijzigingen af te stemmen.
	Methodieken, frameworks en tooling
A.182	Opdrachtnemer maakt bij de ontwikkeling en beoordeling van use cases gebruik van erkende frameworks, waaronder ten minste MITRE ATT&CK en MaGMA UCF.
A.183	Alle detectie use-cases worden geclassificeerd conform het MITRE ATT&CK-framework (Enterprise en/of ICS). Per use-case wordt minimaal gespecificeerd: gedekte Tactic(s), Technique(s), prioriteit op basis van dreigingsprofiel Deelnemer, en detectie-effectiviteit. Opdrachtnemer rapporteert kwartaalijks over MITRE ATT&CK-coverage
A.184	Opdrachtnemer integreert alle use cases in de SIEM- en SOAR-platformen van de Deelnemer, inclusief benodigde triggers, logics, correlatieregels en automatiseringen.
	Organisatie en samenwerking
A.185	Opdrachtnemer beschikt over een dedicated team voor Use Case Management, bestaande uit gekwalificeerde specialisten met aantoonbare ervaring in SOC-detectieontwikkeling, dreigingsanalyse en risicogestuurde monitoring.
A.186	Deelnemers hebben structureel inspraak in de ontwikkeling, prioritering en uitfasering van use cases, conform vooraf overeengekomen governance- en besluitvormingsprocessen.

A.187	Opdrachtnemer neemt actief deel aan Deelnemer-overstijgend Use Case Management, waarbij: • de SOC Use Case Roadmap als gemeenschappelijk referentiekader wordt gehanteerd; • use cases primair collectief worden ontwikkeld en gestandaardiseerd; • hergebruik tussen Deelnemers het uitgangspunt is, tenzij aantoonbaar en gemotiveerd niet mogelijk.
A.188	Opdrachtnemer past hergebruik toe van bestaande use cases, detectieregels en automatiseringen die binnen de opdracht voor andere Deelnemers zijn ontwikkeld, tenzij aantoonbaar en gemotiveerd niet mogelijk. Afwijkingen worden onderbouwd en afgestemd met de regieorganisatie.
SLA-paramaters	
A.189	Implementatie van nieuwe kritieke use cases
	SLA: Opdrachtnemer implementeert nieuwe kritieke use cases binnen maximaal tien (10) Werkdagen nadat de Deelnemer de betreffende use case heeft goedgekeurd.
	Doel: Tijdige beschikbaarheid van nieuwe detectieregels en monitoringlogica zodat relevante dreigingen en risico's binnen de omgeving van de Deelnemer adequaat kunnen worden gedetecteerd.
A.190	Implementatie van updates en optimalisaties van use cases
	SLA: Opdrachtnemer implementeert overeengekomen updates en optimalisaties van bestaande use cases binnen maximaal vijf (5) Werkdagen na ontvangst van een wijzigingsverzoek of goedkeuring van de wijziging door de Deelnemer.
	Doel: Continu verbeteren van de detectiekwaliteit en het actueel houden van use cases in relatie tot veranderende dreigingen, systemen en processen.
A.191	Update en actualisatie van use-cases
	SLA: Opdrachtnemer evalueert en actualiseert alle actieve use-cases minimaal één keer per maand, inclusief effectiviteit, false positives en aansluiting op het actuele dreigingsbeeld.
	Doel: Continu verbeteren van detectie en triage.
A.192	Lifecycle management van use-cases
	SLA: Opdrachtnemer documenteert alle stappen in de lifecycle van use-cases (creatie, validatie, onderhoud, afbouw) en rapporteert wijzigingen binnen 7 dagen na implementatie.
	Doel: Transparante en toetsbare use-case administratie.
A.193	Prioritering en risicogebaseerde afstemming
	SLA: Opdrachtnemer prioriteert use-cases op basis van risicobeoordeling en kritieke processen van Deelnemer en rapporteert periodiek (minimaal maandelijks) over de prioritering en dekking.

	Doel: Use-cases sluiten aan op bedrijfsrisico's en kritieke processen.
A.194	Integratie in SOC-detectieplatformen
	SLA: Opdrachtnemer zorgt dat alle use-cases binnen 15 Werkdagen na creatie of wijziging volledig geïntegreerd zijn in SIEM- en SOAR-platformen van Deelnemer.
	Doel: Directe operationele inzet van nieuwe of aangepaste detectieregels.
A.195	Periodieke rapportage over status en effectiviteit
	SLA: Opdrachtnemer levert minimaal één keer per kwartaal een rapport per Deelnemer met status, effectiviteit, wijzigingen en aanbevelingen voor optimalisatie van use-cases.
	Doel: Transparantie en continue verbetering.
A.196	Deelnemer-inspraak en evaluatie
	SLA: Opdrachtnemer organiseert jaarlijks een gezamenlijke sessie met Deelnemers voor evaluatie van de use-cases en verwerkt leerpunten binnen 30 dagen in het use-case plan.
	Doel: Afstemming met Deelnemer en borging van procesverbeteringen.
A.197	Beschikbaarheid van dedicated team
	SLA: Opdrachtnemer stelt een dedicated team beschikbaar voor use-case management, bereikbaar tijdens kantooruren, met back-up contactpersoon binnen 2 uur.
	Doel: Continuïteit en expertiseborging.
Deliverables	
A.198	Maandelijkse use-case statusrapportage
	Opdrachtnemer levert maandelijks per Deelnemer een rapportage over de actuele status, effectiviteit, wijzigingen en prioritering van alle actieve use-cases. De rapportage bevat ook aanbevelingen voor optimalisatie en eventuele uitfasering van use-cases.
A.199	Jaarlijkse use-case review
	Opdrachtnemer rapporteert jaarlijks over de review van alle actieve use-cases, inclusief beoordeling van relevantie, effectiviteit, dekking van kritieke processen en aansluiting op actuele dreigingsinformatie.
A.200	Use-case catalogus
	Opdrachtnemer levert een actuele en volledig gedocumenteerde use-case catalogus, inclusief classificatie (bijvoorbeeld MITRE ATT&CK), versiebeheer, dekking per logbron, lifecycle-status en criticiteit. Alle wijzigingen worden aantoonbaar gedocumenteerd en beschikbaar gesteld aan Deelnemer.
A.201	Use-case ontwikkel- en wijzigingsrapportages

	Opdrachtnemer rapporteert periodiek over nieuw ontwikkelde, geoptimaliseerde of uit gefaseerde use-cases. De rapportages bevatten de motivatie voor wijziging, effectbeoordeling, prioriteitstelling en aansluiting op actuele dreigingsinformatie en risicobeoordeling.
A.202	Audit-trail en documentatie
	Opdrachtnemer waarborgt een volledige audit-trail van alle wijzigingen, inclusief verantwoordelijken, besluitvorming, datum en inhoud van wijziging. Alle documentatie wordt beschikbaar gesteld via het SOC-detectieplatform en kennisportaal van Deelnemer.
A.203	Integratie in SOC-detectieplatformen
	Opdrachtnemer verzorgt de implementatie en onderhoud van use-cases binnen de SOC-detectieplatformen (SIEM, SOAR, EDR/XDR) van Deelnemer, zodat geautomatiseerde detectie, alerting en analyse correct functioneert.
A.204	Optimalisatie- en verbeteradvies
	Opdrachtnemer levert periodieke adviezen ter optimalisatie van de use-cases, inclusief identificatie van hiaten, redundante detecties en aanbevelingen voor betere aansluiting op dreigingsinformatie en kritieke processen.

3.6 Basis - Knowledge transfer

6 Knowledge transfer

Doel: Zorgen dat kennis, expertise en leerpunten structureel worden overgedragen aan de Deelnemer, zodat de organisatie zelfstandig beter in staat is om securityrisico's te begrijpen, beheersen en verbeteren.

Wat valt hieronder?

- Reguliere kennisoverdracht-sessies, zoals maandelijkse of kwartaalreviews over detecties, Beveiligingsincidenten, trends en verbetermaatregelen.
- Training en begeleiding voor interne medewerkers, zoals:
 - Uitleg over SOC-processen
 - Gebruik van dashboards en rapportages
 - Interpretatie van alerts en detecties
 - Basis threat hunting en analyse
- Documentatievoorziening, waaronder:
 - Handleidingen voor tooling en workflows
 - Beveiligingsincident response playbooks
 - Use-case catalogus en detectieregel-documentatie
 - Architectuuroverzichten en datastromen
- Overdracht van lessons learned, bijvoorbeeld:
 - Post-Beveiligingsincident reviews
 - Trendanalyses
 - Analyse van false positives / false negatives
 - Aanbevelingen voor proces- en technologieverbeteringen
- Samenwerking en kennisdeling tussen SOC-analisten van opdrachtnemer en securitymedewerkers van de Deelnemer.
- Kennisborging, zodat informatie niet afhankelijk is van individuele analisten of leveranciers.

- Ad-hoc kennislevering bij wijzigingen in dreigingslandschap, nieuwe technologieën of belangrijke kwetsbaarheden (bijv. zero-days).

Kernvraag: *Bezit de Deelnemer voldoende kennis om securityprocessen effectief te begrijpen, beoordelen en verbeteren?*

Resultaat: Een beter geïnformeerde en capabelere organisatie, met actuele kennis, duidelijk gedocumenteerde processen en verbeterde security maturity.

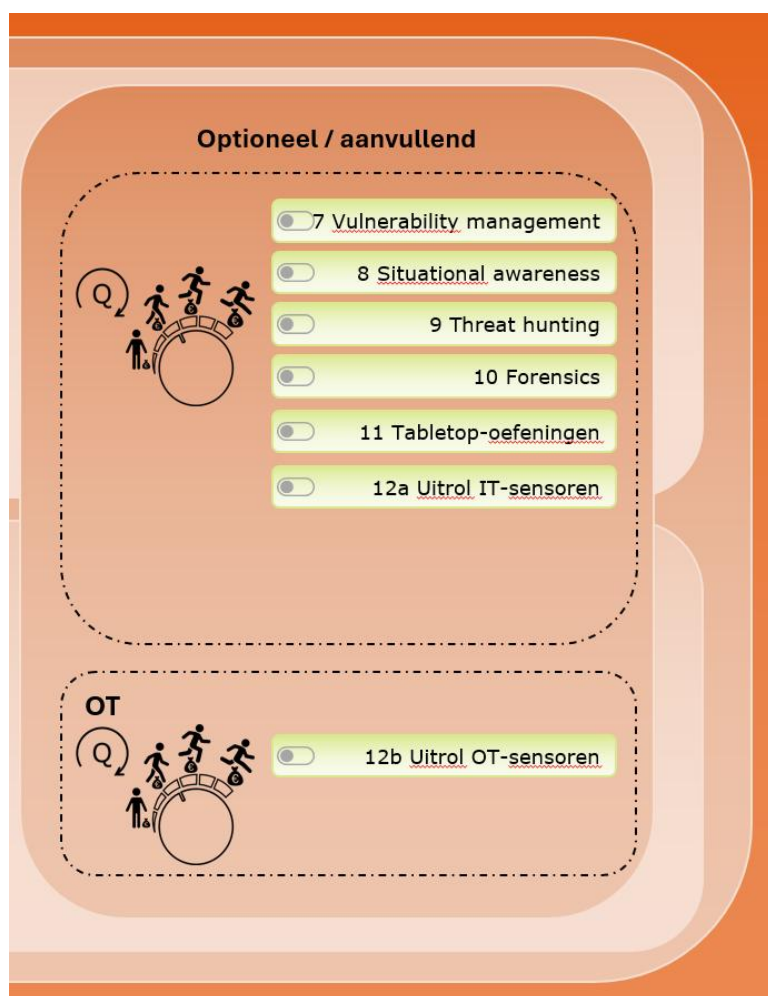
Eisen	
	Doel en scope
A.205	Opdrachtnemer levert structurele en continue kennisoverdracht, gericht op het versterken van de expertise van Deelnemers op het gebied van beveiligingsdreigingen, SOC-processen, Beveiligingsincidentafhandeling, detectie, threat intelligence, toolinggebruik en oplossingsrichtingen. De kennisoverdracht is integraal onderdeel van de dienstverlening.
	Kennisoverdrachtsplan
A.206	Opdrachtnemer stelt met de Deelnemer een gedetailleerd kennisoverdrachtsplan op en voert dit uit. Het plan bevat minimaal: • doelstellingen • onderwerpen • werkvormen • tijdslijnen • verantwoordelijkheden • benodigde middelen • evaluatiemomenten
A.207	Het kennisoverdrachtsplan omvat in ieder geval onderwerpen op het gebied van SOC-processen, Beveiligingsincidentrespons, threat intelligence, use case-ontwikkeling, analysevaardigheden, en het gebruik van SIEM-, SOAR- en overige securitytooling.
A.208	Kennisoverdracht wordt afgestemd op erkende frameworks, waaronder ten minste NIST CSF, NIST 800-61, MITRE ATT&CK, OWASP SAMM en ISO 27001/27002.
	Documentatie & kennisportaal
A.209	Opdrachtnemer documenteert alle SOC-processen, configuraties, operationele procedures en werkafspraken in duidelijke, actuele en doelgroepgerichte documentatie.
A.210	Documentatie en trainingsmateriaal worden digitaal ontsloten via een door Opdrachtnemer te leveren kennisportaal, zijn beschikbaar in het Nederlands en worden structureel bijgewerkt.
A.211	Alle documentatie en werkwijzen voldoen aan relevante wet- en regelgeving, waaronder BIO, AVG, Archiefwet en eventuele Deelnemer-specifieke normen.
	Trainingen, workshops en praktische kennisoverdracht

A.212	Opdrachtnemer organiseert op verzoek van de Deelnemer minimaal jaarlijks trainingen en kennissessies voor security officers, IT-beheerders en overige relevante doelgroepen, gericht op SOC-processen, nieuwe dreigingen, trends en best practices.
A.213	Opdrachtnemer verzorgt workshops met hands-on praktijktraining voor het gebruik, beheer en de interpretatie van SIEM-, SOAR- en overige relevante securitytools.
A.214	Opdrachtnemer verzorgt bij de start van iedere Nadere Overeenkomst een gestructureerd onboarding-programma, waarin processen, rollen, escalatieprocedures, documentatie en tooling worden toegelicht.
	Organisatie & samenwerking met Deelnemers
A.215	Opdrachtnemer wijst vaste contactpersonen aan die verantwoordelijk zijn voor coördinatie van kennisoverdracht, planning, escalaties en ondersteuning.
A.216	Deelnemers hebben inspraak in de planning, onderwerpen en werkvormen van trainingen, workshops en overige kennisoverdracht, zodat deze optimaal aansluiten op de behoefte.
SLA-paramaters	
A.217	Planning en uitvoering van kennisoverdracht
	SLA: Opdrachtnemer stelt een gedetailleerd kennisoverdrachtsplan op en voert dit uit conform de overeengekomen tijdlijnen, minimaal één keer per kwartaal bij reguliere updates en direct bij proces- of toolingwijzigingen.
	Doel: Tijdige en gestructureerde overdracht van SOC-kennis.
A.218	Beschikbaarheid en bereikbaarheid van kenniscoördinatoren
	SLA: Opdrachtnemer wijst vaste contactpersonen toe voor coördinatie van kennisoverdracht, bereikbaar tijdens kantoortijden en voor urgente kwesties binnen 24 uur.
	Doel: Direct aanspreekpunt voor Deelnemer voor alle kennisoverdrachtactiviteiten.
A.219	Documentatie van processen en procedures
	SLA: Alle relevante SOC-processen, configuraties, operationele procedures en werkafspraken worden gedocumenteerd, actueel en digitaal ontsloten, inclusief versiebeheer, minimaal één update per kwartaal.
	Doel: Transparante en toetsbare kennisbasis voor Deelnemers.
A.220	Trainings- en workshopfrequentie
	SLA: Op verzoek van Deelnemer organiseert opdrachtnemer minimaal één training of workshop per jaar voor security officers, IT-beheerders en andere relevante doelgroepen; aanvullende sessies worden binnen 30 dagen gepland op verzoek van Deelnemer.
	Doel: Praktische versterking van expertise van Deelnemers.
A.221	Evaluatie van kennisoverdracht

	SLA: Opdrachtnemer evalueert jaarlijks de kennisoverdrachtsactiviteiten en rapporteert bevindingen en verbeterpunten binnen 30 dagen na evaluatie, inclusief aanbevelingen voor aanpassing van het plan.
	Doel: Continue verbetering van kennisoverdracht.
A.222	Toegankelijkheid van kennisportaal
	SLA: Het door opdrachtnemer beschikbaar gestelde kennisportaal is minimaal 99,5% van de tijd beschikbaar voor geautoriseerde gebruikers, exclusief gepland onderhoud.
	Doel: Betrouwbare toegang tot documentatie en trainingsmateriaal.
Deliverables	
A.223	Kennisoverdrachtsplan
	Opdrachtnemer stelt bij aanvang van de overeenkomst een gedetailleerd kennisoverdrachtsplan op en legt dit ter goedkeuring voor aan de Deelnemer. Het plan bevat minimaal: doelstellingen, onderwerpen, werkvormen, tijdlijnen, verantwoordelijkheden, benodigde middelen en evaluatiemomenten.
A.224	Documentatie SOC-processen en procedures
	Opdrachtnemer documenteert alle SOC-processen, operationele procedures, werkafspraken en configuraties van tools (SIEM, SOAR, EDR/XDR) in een actuele en voor de doelgroep begrijpelijke vorm. De documentatie wordt digitaal beschikbaar gesteld via een kennisportaal van Deelnemer.
A.225	Trainingsmateriaal en workshops
	Opdrachtnemer levert trainingsmateriaal en verzorgt op verzoek van de Deelnemer minimaal jaarlijks trainingen en workshops voor security officers, IT-beheerders en andere relevante doelgroepen. Onderwerpen omvatten SOC-processen, incidentrespons, threat intelligence, use-case ontwikkeling, detectie en analysetechnieken, toolinggebruik en relevante security-standaarden.
A.226	Onboarding-programma
	Op verzoek van de Deelnemer verzorgt Opdrachtnemer bij de start van iedere nieuwe overeenkomst een gestructureerd onboarding-programma, waarin rollen, processen, tooling, escalatieprocedures en documentatie worden toegelicht.
A.227	Jaarlijkse evaluatie en optimalisatie
	Opdrachtnemer organiseert jaarlijks gezamenlijke sessies met de Deelnemer voor evaluatie van de kennisoverdracht. Leerpunten worden verwerkt in een verbeterplan, inclusief aanpassingen aan trainingsmateriaal, documentatie en werkprocessen.
A.228	Toegangsbeheer en coördinatie

	Opdrachtnemer wijst vaste contactpersonen aan die verantwoordelijk zijn voor coördinatie van kennisoverdracht, planning van trainingen, escalaties en ondersteuning. Deelnemers hebben inspraak in planning, onderwerpen en werkvormen zodat deze aansluiten op de behoefte.
	Kennisoverdracht conform frameworks en normen
A.229	Opdrachtnemer borgt dat alle kennisoverdracht aansluit op erkende frameworks zoals NIST CSF, NIST 800-61, MITRE ATT&CK, OWASP SAMM en ISO 27001/27002, en voldoet aan relevante wet- en regelgeving, waaronder BIO, AVG en Deelnemer-specifieke normen.

4 Optionele / aanvullende diensten



Figuur 2. Optionele diensten

Opdrachtnemer levert op verzoek van de Deelnemer optionele SOC-diensten die de Basis SOC-dienst uitbreiden en verdiepen, gericht op het vergroten van het proactieve detectievermogen, situational awareness en responscapaciteit binnen IT- en OT-omgevingen. Het doel van de optionele diensten is om aanvullende risico's te identificeren, kwetsbaarheden te mitigeren, incidenten diepgaand te onderzoeken en organisatiebreed bewustzijn en paraatheid te versterken.

De optionele SOC-dienstverlening bestaat uit de volgende kerncomponenten:

7. Vulnerability Management

- Periodieke en continue identificatie, analyse en prioritering van kwetsbaarheden in IT- en OT-assets.
- Rapportages en adviezen voor mitigatie, patching en risicobeheersing.
- Ondersteuning bij het opstellen en bijwerken van risicoprofielen en prioriteringsmatrices.

8. Situational Awareness

- Real-time en near-real-time inzicht in dreigingen, incidenten en relevante trends.
- Integratie van interne detectie, externe threat intelligence en contextinformatie om een actueel totaalbeeld van de beveiligingspositie van de Deelnemer te verschaffen.
- Ondersteuning bij besluitvorming en prioritering van mitigatiemaatregelen.

9. Threat Hunting

- Proactief zoeken naar tekenen van verborgen aanvallen, geavanceerde dreigingen en afwijkend gedrag in IT- en OT-omgevingen.
- Hypothese-gedreven analyses en periodieke hunting-cycli, inclusief rapportages met bevindingen, risicoanalyse en mitigatie-aanbevelingen.
- Integratie van resultaten in detectieplatformen en SOC-processen.

10. Forensics

- Verzamelen, analyseren en veiligstellen van digitale bewijsmaterialen bij Beveiligingsincidenten.
- Root cause analysis, chain-of-custody documentatie en integriteitsbewijzen van digitale data.
- Ondersteuning bij forensisch-verantwoorde incidentanalyse en juridische compliance.

11. Tabletop

- Gestructureerde simulaties en scenario-oefeningen voor testen en verbeteren van incidentresponsprocessen.
- Beoordeling van rollen, verantwoordelijkheden, procedures en communicatie.
- Documentatie van lessons learned, verbeteracties en implementatiestatus.

12. Uitrol van IT- en OT-sensoren

- Implementatie en configuratie van sensoren in IT- en OT-omgevingen om betrouwbare datastromen voor detectie en analyse te waarborgen.
- Integratie met het SOC-detectieplatform en onderhoud van sensorconfiguraties.
- Eigendom en overdraagbaarheid van sensoren worden gewaarborgd volgens afspraken met Deelnemer.

4.1 Optioneel - Vulnerability Management

Doel: Het systematisch identificeren, analyseren en beheersbaar maken van kwetsbaarheden binnen de IT- en OT-omgeving van de Deelnemer, zodat risico's tijdig inzichtelijk zijn en effectief kunnen worden gereduceerd, met behoud van duidelijke rolverdeling tussen Opdrachtnemer en Deelnemer.

Wat valt hieronder?

- Periodieke en/of continue kwetsbaarheidsscans op IT- en OT-assets binnen de overeengekomen scope.
- Toepassing van gangbare scanmethoden (authenticated, unauthenticated, agent-based waar passend).
- Classificatie en technische prioritering van kwetsbaarheden op basis van o.a. CVSS, exploitability en threat intelligence.
- Verrijking van bevindingen met assetcontext en dreigingsinformatie.
- Opstellen en onderhouden van een actueel vulnerability-register.
- Advisering over mitigerende maatregelen, patching en prioriteiten.
- Monitoring van opvolging op basis van beschikbare informatie (bijv. ITSM), inclusief signalering van overschrijdingen en risico's.
- Integratie met ITSM- en changeprocessen voor registratie en opvolging.
- Rapportage over trends, risico's en voortgang (o.a. aantallen, doorlooptijden, aging, exposure).
- Afhandeling van kritieke kwetsbaarheden en zero-days met tijdige signalering en advies.
- Afstemming met SOC-processen voor verrijking van detectie en incidentanalyse.
- Voor OT-omgevingen: uitsluitend passieve, niet-verstorende monitoring, proportioneel ingericht in afstemming met de Deelnemer.

Kernvraag: *Zijn kwetsbaarheden binnen de overeengekomen scope tijdig en volledig geïdentificeerd, adequaat geanalyseerd en zodanig inzichtelijk gemaakt dat de Deelnemer effectief kan sturen op prioritering en opvolging?*

Resultaat: Een actueel en aantoonbaar beheerst kwetsbaarhedenbeeld binnen de overeengekomen scope, met:

- volledig en actueel inzicht in kwetsbaarheden en risico's;
- onderbouwde prioritering en handelingsperspectief;
- transparantie over voortgang en opvolging;
- duidelijke scheiding van verantwoordelijkheden tussen Opdrachtnemer (signaleren, analyseren, adviseren) en Deelnemer (prioriteren, besluiten en uitvoeren);
- ondersteuning van compliance, auditability en continue verbetering van de beveiligingshouding.

Eisen	
	Doel en algemene verplichting
A.230	Opdrachtnemer levert, op verzoek van de Deelnemer, vulnerability-managementdiensten gericht op het proactief identificeren, analyseren, prioriteren en mitigeren van kwetsbaarheden binnen de IT- en/of OT-omgevingen van de Deelnemers, met als doel het reduceren van risico's op succesvolle cyberaanvallen en het versterken van de beveiligingshouding.
	Scopebepaling
A.231	De Deelnemer bepaalt welke IT- en/of OT-assets worden opgenomen of uitgesloten in de scope van de scans.
A.232	Opdrachtnemer voert kwetsbaarheidsscans uit op alle door de Deelnemer aangewezen infrastructuurcomponenten, zowel on-premises als in cloud- en hybride omgevingen.
A.233	Opdrachtnemer voert minimaal, maar niet uitsluitend, scans uit op: • servers, • werkplekken en endpoints, • netwerkcomponenten, • cloudservices (IaaS/PaaS/SaaS), • containers, • webapplicaties, • OT-systemen, voor zover deze binnen de door de Deelnemer vastgestelde scope vallen.
A.234	De omvang van de vulnerability-managementdienst wordt per Deelnemer vastgelegd in het DAP en omvat ten minste: • het aantal en type assets binnen scope (bijv. endpoints, servers, OT-assets); • de scanfrequentie per assetcategorie; • het verwachte scanvolume (bijv. aantal scans per maand); • het aantal integraties (bijv. ITSM, CMDB); • eventuele aanvullende diensten (bijv. webapp scanning, container scanning). Wijzigingen in scope kunnen leiden tot aanpassing van de dienstverlening en bijbehorende kosten.

A.235	De vulnerability-managementdienst omvat niet: • het zelfstandig uitvoeren van patching of changes in productieomgevingen; • verantwoordelijkheid voor het behalen van patch- of compliancedoelstellingen; • volledige dekking van alle assets buiten de overeengekomen scope.
	Rol en verantwoordelijkheden
A.236	Opdrachtnemer is verantwoordelijk voor het identificeren, analyseren, prioriteren en rapporteren van kwetsbaarheden en het adviseren over mitigatiemaatregelen. De Deelnemer blijft eindverantwoordelijk voor: • besluitvorming over risicoacceptatie; • uitvoering van patching en mitigatiemaatregelen; • change- en releaseprocessen. Opdrachtnemer vervult een signalerende, adviserende en monitorende rol en ondersteunt de Deelnemer bij de opvolging van kwetsbaarheden.
	Ondersteuning bij mitigatie
A.237	Op verzoek van de Deelnemer levert Opdrachtnemer ondersteuning bij mitigatie- en patchmaatregelen. Deze ondersteuning is adviserend en/of coördinerend van aard, tenzij expliciet anders overeengekomen in het DAP.
	Scanfrequentie en monitoring
A.238	Opdrachtnemer ondersteunt zowel periodieke scans (bijv. wekelijks of maandelijks) als continue monitoring van kwetsbaarheden.
A.239	Opdrachtnemer levert real-time signalering bij kritieke kwetsbaarheden en zero-day vulnerabilities.
A.240	Opdrachtnemer voert op verzoek van de Deelnemer periodieke kwetsbaarheidsscans uit en verstrekt opvolgend advies met mogelijke mitigatie- en patchmaatregelen.
	Analyse, classificatie en prioritering
A.241	Opdrachtnemer classificeert kwetsbaarheden op basis van impact en exploitability, waaronder toepassing van gangbare standaarden zoals CVSS.
A.242	Opdrachtnemer prioriteert bevindingen op basis van: • de classificatie en kritikaliteit van de processen van de Deelnemer, en • de risicobeoordeling van de gedetecteerde kwetsbaarheden.
A.243	Opdrachtnemer adviseert de Deelnemer over passende mitigatie- en patchstrategieën.
	Ondersteuning
A.244	Op verzoek van de Deelnemer levert Opdrachtnemer ondersteuning bij patching en/of het treffen van aanvullende technische maatregelen ter mitigatie van kwetsbaarheden.
A.245	Opdrachtnemer stelt een real-time vulnerability dashboard beschikbaar met inzicht in het vulnerability management van alle Deelnemers.

SLA-paramaters	
A.246	Frequentie van kwetsbaarheidsscans
	SLA: Opdrachtnemer voert periodieke kwetsbaarheidsscans uit volgens de in het DAP overeengekomen frequentie, minimaal maandelijks, en bij kritieke kwetsbaarheden onmiddellijk na detectie.
	Doel: Tijdige identificatie van kwetsbaarheden om risico's te minimaliseren.
A.247	Tijdigheid van rapportage van kritieke kwetsbaarheden
	SLA: Bevindingen van critical en high kwetsbaarheden worden binnen 24 uur na detectie gerapporteerd aan Deelnemer, inclusief mitigatie- en patchadvies.
	Doel: Snelle opvolging en mitigatie van risico's.
A.248	Log- en scanvolledigheid
	SLA: $\geq 98\%$ van alle overeengekomen IT- en OT-assets worden volledig gescand; uitval of afwijkingen worden binnen 15 minuten gemeld aan Deelnemer.
	Doel: Compleet inzicht in kwetsbaarheden van alle relevante systemen.
A.249	Rapportage en risicoprioritering
	SLA: Opdrachtnemer levert minimaal maandelijks rapportages met een overzicht van gedetecteerde kwetsbaarheden, risicoclassificatie (incl. CVSS), trends, herhaalde kwetsbaarheden, aging-informatie en concrete aanbevelingen voor beheersmaatregelen.
	Doel: Ondersteuning van prioritering, mitigatie en patchmanagement.
A.250	Ondersteuning bij mitigatie en patching
	SLA: Op verzoek van Deelnemer levert opdrachtnemer technische ondersteuning bij mitigatie- en patchmaatregelen binnen de door Deelnemer gestelde planning.
	Doel: Effectieve reductie van risico's en versterking van de beveiligingshouding.
A.251	Integriteit van scandata en documentatie
	SLA: Alle scandata, logboeken en rapportages worden veilig opgeslagen en zijn overdraagbaar aan Deelnemer of opvolgende opdrachtnemer.
	Doel: Waarborging van audittrail, compliance en bewijsvoering.

Deliverables	
A.252	Kwetsbaarhedenrapportage
	Opdrachtnemer levert volgens de in het Dienstverlenings- en Afspraakplan (DAP) vastgelegde frequentie een volledig kwetsbaarhedenrapport per Deelnemer. Het rapport bevat ten minste: overzicht van alle gedetecteerde kwetsbaarheden, risicoclassificatie (inclusief CVSS-scores), trends, herhaalde kwetsbaarheden, aging-informatie en concrete aanbevelingen voor beheersmaatregelen.
A.253	Risicoprofiel per Deelnemer
	Opdrachtnemer stelt een gedetailleerd risicoprofiel op per Deelnemer, inclusief prioritering van assets op basis van impact, exploitability en kritichiteit. Dit risicoprofiel wordt periodiek bijgewerkt volgens de in het DAP overeengekomen frequentie.
A.254	Periodieke scanrapportages
	Opdrachtnemer levert maandelijkse of periodieke scanrapportages met daarin: resultaten van uitgevoerde kwetsbaarheidsscans, detectie van nieuwe en herhaalde kwetsbaarheden, en informatie over de scope van de scans (servers, endpoints, netwerkcomponenten, cloudservices, containers, webapplicaties en OT-systemen).
A.255	Risico- en prioriteringsmatrix
	Opdrachtnemer levert per asset een overzichtelijke risico- en prioriteringsmatrix, waarmee Deelnemer inzicht krijgt in welke kwetsbaarheden eerst moeten worden aangepakt op basis van hun risico-impact.
A.256	Adviesrapporten voor mitigatie en patching
	Opdrachtnemer verstrekt periodiek adviesrapporten waarin concrete mitigatie- en patchstrategieën worden aanbevolen, inclusief technische maatregelen en planning voor implementatie.
A.257	Logboeken en audit-trail van scans
	Opdrachtnemer onderhoudt volledige logboeken van alle uitgevoerde kwetsbaarheidsscans, inclusief opvolging van bevindingen, status van mitigatiemaatregelen en audit-trail van wijzigingen. Deze logboeken worden periodiek beschikbaar gesteld aan Deelnemer.

4.2 Optioneel - Situational awareness

Doel: Het verkrijgen en continu actueel houden van een integraal beeld van de beveiligingsstatus, dreigingen, kwetsbaarheden en afwijkingen binnen de IT- en OT-omgeving van de Deelnemer, om tijdige en gefundeerde besluitvorming mogelijk te maken.

Wat valt hieronder?

- Continu inzicht in actuele dreigingen op basis van interne signalen (alerts, Beveiligingsincidenten, logdata) en externe bronnen (threat intelligence, sectorinformatie, overheidswaarschuwingen).
- Realtime zicht op de status van monitoring, detectie en Eventverwerking, inclusief logvolledigheid, sensorstatus, platformbeschikbaarheid en openstaande alerts.

- Overzicht van openstaande kwetsbaarheden, inclusief risicoclassificatie, exploit availability en voortgang van mitigerende acties.
- Contextualisering van securitygebeurtenissen, waarbij informatie uit verschillende bronnen wordt gecombineerd tot één coherent beeld (SOC-situatiebeeld).
- Duidelijk inzicht in trends, zoals toename in aanvalspatronen, herhaalde dreigingen, structurele monitoringgaten of terugkerende kwetsbaarheden.
- Inrichting van periodieke beveiligingsbriefings, zoals weekly SOC updates, monthly security summaries of quarterly risk assessments.
- Ondersteuning bij besluitvorming door het leveren van handelingsperspectief, prioriteitsanalyse en impactduiding op basis van actuele situatie.
- Visualisatie van actuele securitystatus via dashboards, rapportages en geautomatiseerde statusoverzichten.
- Samenvoegen van IT-, OT- en cloudinformatie tot één integraal securitybeeld.
- Escalaties bij afwijkingen ten opzichte van afgesproken normsituaties, zoals uitval van kritieke logbronnen, ernstige kwetsbaarheden of dreigingspieken.

Kernvraag: *Begrijpen we op elk moment wat de actuele beveiligingssituatie is en kunnen we hier effectief op sturen?*

Resultaat: Een actueel, geïntegreerd en betrouwbaar situatiebeeld dat tijdige besluitvorming, prioritering en effectieve respons ondersteunt.

Eisen	
	Doel en algemene verplichting
A.258	Opdrachtnemer levert, op verzoek van de Deelnemer, de dienst Situational Awareness, gericht op het tijdig en proactief identificeren, duiden en mitigeren van dreigingen.
A.259	De dienst omvat minimaal het verzamelen, verwerken, analyseren en interpreteren van dreigingsinformatie uit interne en externe bronnen, teneinde een actueel, volledig en integraal beeld van de beveiligingspositie van de Deelnemer te verschaffen.
	Dashboards en informatievoorziening
A.260	Opdrachtnemer levert een continu beschikbaar, near-real-time dashboard dat inzicht biedt in: • actuele dreigingen, • dreigingstrends, • Beveiligingsincidentstatussen, • kwetsbaarheden, • relevante security-indicatoren.
A.261	Het dashboard presenteert geïntegreerde informatie uit interne detectie- en monitoringssystemen, threat-intelligencebronnen en relevante externe bronnen, waaronder minimaal het NCSC, informatieknooppunten en sectorale ISAC's.
A.262	Opdrachtnemer verrijkt alle meldingen, alerts en bevindingen met relevante context, waaronder impactanalyse, waarschijnlijkheid, urgentie, relaties met processen van de Deelnemer en ketenafhankelijkheden.
A.263	De dienst bevat functionaliteit voor historische analyses en trendrapportages (bijv. dreigingsontwikkelingen, terugkerende patronen, seizoensinvloeden).

	Gebruik van erkende standaarden en frameworks
A.264	Opdrachtnemer duidt dreigingen en tactieken, technieken en procedures (TTP's) conform internationaal erkende frameworks, waaronder MITRE ATT&CK, en past deze eenduidig toe in dashboarding, analyses en rapportages.
A.265	De dienst ondersteunt ten minste de standaarden STIX en TAXII voor het ontvangen, uitwisselen en distribueren van dreigingsinformatie.
	Integraties en interoperabiliteit
A.266	Opdrachtnemer levert Situational Awareness volledig geïntegreerd met de SIEM-, SOAR- en CMDB-voorzieningen van de Deelnemer, conform gestandaardiseerde API's en interoperabiliteitsstandaarden.
A.267	Situational Awareness koppelt automatisch aan lopende Beveiligingsincidenten in het SOC-proces en ondersteunt SOAR-workflows.
A.268	De dienst moet bevindingen uit Red-team- en Blue-teamactiviteiten kunnen integreren ter verrijking van het dreigingsbeeld.
	Analyse, correlatie en prioritering
A.269	Opdrachtnemer correleert interne en externe dreigingsinformatie automatisch om relevante patronen, trends en risico's te identificeren en prioriteren.
A.270	Opdrachtnemer past risicogebaseerde prioritering toe (bijv. CVSS of eigen risk-scoringmodel) zodat de Deelnemer direct inzicht heeft in dreigingen die als eerste actie vereisen.
A.271	Opdrachtnemer past mechanismen toe om ruis te beperken, waaronder deduplicatie, filtering van false positives en machine-learninggebaseerde classificatie.
A.272	Opdrachtnemer hanteert heldere criteria voor escalatie van dreigingen naar de Deelnemer, bijvoorbeeld bij high-severitybevindingen of directe impact op kritieke dienstverlening.
	Toegangsbeveiliging en logging
A.273	Toegang tot dashboards, rapportages en onderliggende data is uitsluitend toegestaan voor geauthenticeerde en geautoriseerde gebruikers, met ondersteuning voor federated identity (SAML / OpenID Connect) en multi-factor authentication (MFA).
A.274	Alle toegang, configuratiewijzigingen en handelingen binnen de dienst worden gelogd en minimaal 12 maanden bewaard.
	Scope en toepassingsgebieden
A.275	Indien van toepassing op de Deelnemer ondersteunt de dienst ook monitoring en dreigingsinformatie voor: • cloudomgevingen, • IoT-apparaten, • OT-netwerken.

	Transparantie over bronnen
A.276	Opdrachtnemer maakt inzichtelijk welke externe threat-intelligenceleveranciers worden gebruikt, inclusief hun certificeringen, datakwaliteit en herkomst.
SLA-paramaters	
	Beschikbaarheid dashboards en informatie
A.277	SLA: Opdrachtnemer garandeert dat de near-real-time situational awareness dashboards minimaal 99,8% per kalendermaand beschikbaar zijn, exclusief gepland onderhoud.
	Doel: Continu inzicht in dreigingen, incidentstatussen, kwetsbaarheden en relevante security-indicatoren.
	Tijdigheid van dreigingsinformatie
A.278	SLA: Opdrachtnemer verwerkt en presenteert nieuwe relevante dreigingsinformatie binnen 15 minuten na ontvangst of detectie, inclusief correlatie met lopende incidenten.
	Doel: Snelle detectie van trends, nieuwe dreigingen en potentiële incidenten.
	Updatefrequentie threat-intelligence feeds
A.279	SLA: Opdrachtnemer levert dreigingsinformatie uit alle overeengekomen threat-intelligence feeds met een gegarandeerde updatefrequentie van minimaal elke 15 minuten.
	Doel: Continu actuele dreigingsinformatie beschikbaar voor vroegtijdige detectie en preventie.
	Integratie met lopende Beveiligingsincidenten SOC-processen
A.280	SLA: Opdrachtnemer koppelt relevante bevindingen automatisch aan lopende SOC-incidenten en SOAR-workflows binnen 30 minuten na identificatie.
	Doel: Efficiënte respons en preventie van escalatie naar beveiligingsincident.
	Kwaliteit en volledigheid van data
A.281	SLA: $\geq 98\%$ van alle overeengekomen bronnen (intern en extern) levert continu bruikbare data aan het SA-platform; uitval of afwijkingen worden binnen 15 minuten gemeld aan Deelnemer.
	Doel: Compleet en betrouwbaar beeld van de dreigingsomgeving.

A.282	Periodieke rapportages en trendanalyse
	SLA: Opdrachtnemer levert minimaal maandelijks situational awareness-rapportages met gecontextualiseerde dreigingsinformatie (TTP's, MITRE ATT&CK mapping) en trendanalyses.
	Doel: Ondersteuning van strategische besluitvorming, risico-evaluatie en verbeteracties.
A.283	Toegangsbeheer en beveiliging
	SLA: Alleen geautoriseerde gebruikers hebben toegang tot dashboards, rapportages en onderliggende data; toegang wordt beveiligd via MFA en federated identity (SAML / OpenID Connect).
	Doel: Bescherming van gevoelige dreigingsinformatie en compliance met wet- en regelgeving.
Deliverables	
A.284	Maandelijks dreigingsrapportages
	Opdrachtnemer levert per Deelnemer maandelijks een overzichtsrapport met daarin: actuele dreigingen, geregistreerde Beveiligingsincidenten, trends, en relevante ontwikkelingen. Het rapport bevat analyse en contextualisatie van de impact op de infrastructuur en kritieke processen van de Deelnemer.
A.285	Jaarlijkse evaluatie en verbeterplan
	Opdrachtnemer voert jaarlijks een evaluatie uit van de situational awareness-processen en -methodieken. De uitkomsten worden vastgelegd in een rapport met concrete aanbevelingen en verbeterpunten, inclusief voorgestelde aanpassingen in processen, dashboards of informatievoorziening.
A.286	Near-real-time situational awareness dashboards
	Opdrachtnemer levert dashboards die near-real-time inzicht geven in dreigingen, Beveiligingsincidenten, kwetsbaarheden en relevante security-indicatoren. De dashboards integreren interne detectie- en monitoringsystemen, threat intelligence feeds en externe bronnen zoals NCSC en sectorale ISAC's.
A.287	Periodieke dreigings- en trendrapportages
	Opdrachtnemer levert periodiek (minimaal maandelijks) gedetailleerde rapportages met analyse van dreigingstrends, terugkerende patronen en potentiële risico's. Deze rapportages worden afgestemd op de scope en criticiteit van de Deelnemer en zijn geschikt voor strategische besluitvorming.
A.288	Gecontextualiseerde dreigingsinformatie
	Opdrachtnemer verrijkt alle meldingen, alerts en bevindingen met relevante contextinformatie, zoals Tactics, Techniques and Procedures (TTP's), MITRE ATT&CK mapping, impactanalyse, waarschijnlijkheid en relaties met kritieke processen.

	Integratie met lopende Beveiligingsincidenten
A.289	Opdrachtnemer zorgt dat situational awareness volledig is geïntegreerd met lopende incidenten in het SOC, zodat alerts, analyses en dreigingsinformatie direct kunnen worden gebruikt binnen de incident response- en SOAR-workflows.

4.3 Optioneel - Threat hunting

Doel: Het proactief vaststellen of dreigingen of aanvalspatronen daadwerkelijk aanwezig zijn (of zijn geweest) binnen de IT- en OT-omgeving, ondanks bestaande detectiemaatregelen.

Karakter: Primair onderzoekend, hypothese-gedreven en validatief.

Wat valt hieronder?

- Uitvoeren van hypothese-gedreven onderzoeken gebaseerd op:
 - threat intelligence
 - bekende aanvalstechnieken (MITRE ATT&CK)
 - afwijkend gedrag
- Proactieve analyse van interne data (SIEM, EDR/XDR, netwerk, cloud, OT)
- Valideren of:
 - IoC's daadwerkelijk voorkomen in de omgeving
 - TTP's of aanvalspatronen zichtbaar zijn
 - aanvallers persistent aanwezig zijn zonder detectie
- Identificeren van:
 - detectiegaten
 - ontbrekende use-cases
 - onvoldoende correlatieregels
- Ontwikkelen van herhaalbare hunting-playbooks
- Doorvertalen van bevindingen naar:
 - verbeterde detectieregels
 - nieuwe use-cases
 - incident response

Expliciete afhankelijkheid: Threat Hunting maakt gebruik van input vanuit Threat Intelligence, maar voert zelfstandig onderzoek uit op basis van interne data.

Kernvraag: *Zijn er aanwijzingen dat een dreiging daadwerkelijk aanwezig is binnen de omgeving, ondanks bestaande detectie?*

Resultaat: Gevalideerde bevindingen over aanwezigheid van dreigingen en concrete verbeteringen in detectie en monitoring.

Eisen	
	Doel en algemene verplichting
A.290	Opdrachtnemer levert, op verzoek van de Deelnemer, de dienst Threat Hunting, gericht op het proactief opsporen van tekenen van kwaadaardige activiteiten, geavanceerde dreigingen, verborgen aanvallen en afwijkend gedrag in de IT- en/of OT-omgevingen van de Deelnemers, teneinde schade te voorkomen en aanvallen vroegtijdig te detecteren.
A.291	Threat Hunting is nadrukkelijk niet reactief van aard, maar gericht op preventie en vroegtijdige detectie, aanvullend op reguliere detectie- en Beveiligingsincidentresponsprocessen.
A.292	Opdrachtnemer meldt kritieke bevindingen per ommegaande bij de Deelnemer.
	Scope en uitvoering
A.293	Opdrachtnemer stemt de scope van de Threat-Huntingdienst vooraf af met de Deelnemer.

A.294	Alle in scope bepaalde IT- en OT-assets worden meegenomen in de uitvoering, waaronder minimaal: • endpoints, • servers, • netwerkcomponenten, • cloudomgevingen (IaaS/PaaS/SaaS), • OT-systemen.
A.295	Opdrachtnemer voert Threat Hunting uit op basis van: a) hypothese-gedreven onderzoek, en b) actuele dreigingsinformatie, en c) zowel indicatoren van compromise (IoC's) als gedragsanalyse.
A.296	Opdrachtnemer voert, indien de Deelnemer daarom verzoekt, minimaal één keer per kwartaal per Deelnemer een Threat Hunt uit, en voert aanvullend hunts uit bij urgente dreigingen of kritieke signalen.
	Personele eisen
A.297	Het personeel van Opdrachtnemer dat Threat Hunting uitvoert beschikt over aantoonbare relevante ervaring en over erkende certificeringen, zoals GCTI, CTIA, OSCP of gelijkwaardig.
	Overdracht en eigendom van data
A.298	Opdrachtnemer zorgt ervoor dat alle huntingdata, bevindingen en documentatie volledig overdraagbaar zijn.
A.299	Opdrachtnemer draagt, op verzoek van de Deelnemer, alle huntingdata en documentatie tijdig en volledig over aan de Deelnemer en/of een opvolgende Opdrachtnemer.
SLA-paramaters	
A.300	Scope en frequentie van hunting-activiteiten
	SLA: Opdrachtnemer voert threat-huntingcycli uit op alle overeengekomen IT- en OT-assets, minimaal één keer per kwartaal per Deelnemer en daarnaast ad-hoc bij urgente dreigingen.
	Doel: Proactief opsporen van verborgen aanvallen, geavanceerde dreigingen en afwijkend gedrag voordat deze schade veroorzaken.
A.301	Hypothese-gedreven onderzoek en use-case integratie
	SLA: Opdrachtnemer documenteert alle hypothesen, analyseprocessen en bevindingen binnen 48 uur na afronding van een threat-hunt.
	Doel: Transparantie van het onderzoeksproces en integratie met lopende use-cases en SOC-detectieplatformen.

A.302	Rapportage van bevindingen en risicobeoordeling
	SLA: Opdrachtnemer levert per hunting-cyclus een volledig rapport met geconstateerde afwijkingen, risicobeoordeling en mitigatie- of detectieaanbevelingen, uiterlijk binnen 5 Werkdagen na afronding van de hunting-cyclus.
	Doel: Snelle beschikbaarheid van inzichten voor Deelnemer, zodat mitigatie of vervolgstappen kunnen worden genomen.
A.303	Integratie met SOC- en incidentmanagement
	SLA: Bevindingen van threat-hunting worden binnen 24 uur na rapportage gekoppeld aan relevante SOC-detecties, use-cases en, indien van toepassing, incidentmanagementprocessen.
	Doel: Efficiënte opvolging van dreigingen en preventie van escalatie naar beveiligingsincidenten.
A.304	Beschikbaarheid en continuïteit van hunting-personeel
	SLA: Opdrachtnemer stelt continu beschikbaar gecertificeerd hunting-personeel ter beschikking gedurende de overeengekomen openingstijden, inclusief 24/7 ondersteuning bij urgente dreigingen.
	Doel: Ononderbroken proactieve detectie en snelle respons bij kritieke dreigingen.
A.305	Documentatie en overdraagbaarheid
	SLA: Alle huntingdata en documentatie worden op verzoek van Deelnemer binnen 5 Werkdagen volledig overgedragen, inclusief audit-trails, zodat continuïteit bij opvolgende analyses of door een andere opdrachtnemer gegarandeerd is.
	Doel: Borging van kennis en herbruikbaarheid van onderzoeksdata, inclusief compliance met interne en externe regelgeving.
Deliverables	
A.306	Hunting-cyclus rapportages
	Opdrachtnemer levert per uitgevoerde hunting-cyclus een rapport aan de Deelnemer met daarin de uitgevoerde activiteiten, geïdentificeerde afwijkingen, geanalyseerde risico's en concrete aanbevelingen voor mitigatie en vervolgstappen.
A.307	Scope- en asset-specifieke hunting-rapportages
	Opdrachtnemer levert per Deelnemer en per overeengekomen scope of IT-/OT-asset een overzicht van de uitgevoerde threat hunting-activiteiten, inclusief relevante bevindingen, prioritering en impactanalyse.
A.308	Documentatie van hypothesen en analyse
	Opdrachtnemer documenteert alle gehanteerde hypothesen, toegepaste analysemethoden, correlaties en geconstateerde afwijkingen. Deze documentatie is aantoonbaar, volledig en overdraagbaar aan de Deelnemer of opvolgende opdrachtnemer.

A.309	Kwartaal- en urgentierapportages
	Opdrachtnemer levert minimaal per kwartaal een overzicht van uitgevoerde threat hunts, trends en leerpunten. Daarnaast verstrekt Opdrachtnemer ad-hoc urgentierapportages wanneer nieuwe of kritieke dreigingen worden geïdentificeerd die impact kunnen hebben op de Deelnemer.
A.310	Integratie met SOC-detectieplatformen
	Opdrachtnemer zorgt dat alle bevindingen en analyses uit de threat hunting-cycli worden geïntegreerd in de lopende SOC-detectie-, correlatie- en Beveiligingsincidentmanagementprocessen. Hierdoor kunnen alerts, use-cases en detectieregels direct worden geoptimaliseerd en toegepast binnen het SOC.

4.4 Optioneel – Forensics

Doel: Het op forensisch-verantwoorde wijze verzamelen, veiligstellen, analyseren en interpreteren van digitale sporen en bewijsmateriaal na (vermoede) beveiligingsincidenten, met als doel de oorzaak, impact, gebruikte aanvalstechnieken en gevolgschade vast te stellen en juridische houdbaarheid te borgen.

Wat valt hieronder?

- Veiligstellen van digitaal bewijsmateriaal (logbestanden, memory dumps, netwerkverkeer, artifacts, forensische images) conform chain-of-custody-principes.
- Forensische analyse gericht op reconstructie van aanvalsvector, TTP's, laterale beweging, persistence-mechanismen en impactbepaling.
- Gebruik van erkende forensische methoden en tooling zoals EnCase, FTK, Volatility, Autopsy en technieken conform ISO 27037.
- Herleidbaarheid en integriteitsborging via hashing, signing, beveiligde opslag en gedocumenteerde onderzoekshandelingen.
- Rapportage met bevindingen, conclusies, tijdlijnen, risico's, impactanalyse en aanbevelingen.
- Ondersteuning bij juridische of opsporingsprocedures inclusief overdracht van bewijsmateriaal aan externe partijen (bijv. politie, OM of CSIRT's).
- Afstemming met Beveiligingsincidentresponsprocessen inclusief root cause analysis (RCA) en hersteladvies.

Kernvraag: *Wat is er precies gebeurd, hoe heeft het kunnen gebeuren, welke systemen en data zijn geraakt en hoe kan dit aantoonbaar worden vastgesteld volgens forensische standaarden?*

Resultaat: Een forensisch onderbouwd onderzoeksrapport met juridisch houdbaar bewijs, een reconstructie van het Beveiligingsincidentverloop, vastgestelde impact, root cause, gebruikte technieken, gedetecteerde sporen en aanbevelingen voor herstel en preventie. Indien nodig omvat het resultaat tevens een beveiligde overdrachtsset met forensisch materiaal.

Eisen	
	Doel en algemene verplichting
A.311	Opdrachtnemer levert, op verzoek van de Deelnemer, de dienst Forensisch Onderzoek (Digital Forensics), gericht op het verzamelen, analyseren en veiligstellen van digitale sporen en bewijsmateriaal na Beveiligingsincidenten, teneinde root cause, aanvalsvector, gebruikte technieken en impact vast te stellen.

A.312	De forensische dienstverlening sluit aantoonbaar aan op de Beveiligingsincident-responseprocessen van de Deelnemer en vormt een integraal onderdeel van het SOC-proces.
	Forensische uitvoering en methodieken
A.313	Opdrachtnemer voert forensische analyses uit volgens forensisch-verantwoorde procedures, inclusief: • waarborging van chain of custody, • integriteit en authenticiteit van bewijs, • volledige en controleerbare audit trails.
A.314	Digitale bewijsmaterialen (zoals logbestanden, geheugendumps, schijfimages, netwerkverkeer en artefacten) worden verzameld, verwerkt en bewaard op een juridisch houdbare wijze, conform geldende normen.
A.315	De forensische analyses zijn gericht op het vaststellen van: • aanvalsvectoren, • gebruikte tactieken en technieken, • de technische en functionele impact op provinciale systemen en diensten, • de onderliggende root cause.
A.316	Opdrachtnemer gebruikt erkende forensische tools en methodieken, waaronder minimaal: • tools zoals EnCase, FTK, Volatility of gelijkwaardig, • methodieken conform ISO 27037 en relevante sectorale richtlijnen.
A.317	Opdrachtnemer past forensische procedures toe op zowel IT-omgevingen als, waar van toepassing, OT-omgevingen, met gebruik van tooling die hiervoor geschikt is.
	Beveiliging, bewaring en overdracht van forensische data
A.318	Opdrachtnemer versleutelt alle forensische data tijdens opslag en transport, tenzij anders schriftelijk overeengekomen met de Deelnemer.
A.319	Opdrachtnemer bewaart forensische data zodanig dat deze beschikbaar is voor detectie, analyse en forensisch onderzoek van beveiligingsincidenten. De standaard bewaartermijn voor forensische data bedraagt minimaal twaalf (12) maanden, tenzij: a. een door Deelnemer vastgestelde langere of kortere bewaartermijn geldt; of b. uit wettelijke verplichtingen, relevante normen of een door Deelnemer uitgevoerde risicoafweging een andere bewaartermijn voortvloeit. Opdrachtnemer dient bewaartermijnen te hanteren in overeenstemming met artikel 5, lid 1, sub e van de Algemene Verordening Gegevensbescherming (AVG), waarbij gegevens niet langer worden bewaard dan noodzakelijk is voor het beoogde doel. Opdrachtnemer maakt onderscheid tussen typen forensische data en past waar nodig gedifferentieerde bewaartermijnen toe, met inachtneming van proportionaliteit en dataminimalisatie.
A.320	Opdrachtnemer biedt de mogelijkheid tot veilige overdracht van forensische data en bevindingen aan externe partijen, waaronder CSIRTs en opsporingsinstanties, overeenkomstig vooraf overeengekomen procedures.

	Rapportages en compliance
A.321	Opdrachtnemer levert een gestructureerd forensisch onderzoeksrapport, waarin alle genomen stappen, bevindingen, gebruikte methoden en conclusies aantoonbaar zijn gedocumenteerd
A.322	Rapportages moeten voldoen aan relevante wet- en regelgeving en provinciale eisen, waaronder: • BIO, • AVG, • Cbw, • eventuele Deelnemer-specifieke normen.
A.323	Opdrachtnemer documenteert alle stappen en handelingen binnen het forensisch onderzoek in een volledige audit-trail die overdraagbaar en verifieerbaar is.
SLA-paramaters	
A.324	Forensisch bevindingen- en aanbevelingsrapport
	SLA: Binnen vijf (5) Werkdagen na afronding van het forensisch onderzoek levert de Opdrachtnemer een volledig rapport met bevindingen, conclusies en aanbevelingen aan de Deelnemer, tenzij anders schriftelijk overeengekomen.
	Doel: Tijdige en bruikbare informatie verschaffen voor incidentafhandeling, risicobeheersing en implementatie van preventieve maatregelen.
A.325	Respons en initiële forensische analyse
	SLA: Opdrachtnemer start forensische activiteiten binnen 2 uur na melding van een beveiligingsincident dat forensisch onderzoek vereist.
	Doel: Vroegtijdige veilige veiligstelling van digitale bewijsmaterialen en minimale kans op dataverlies.
A.326	Verzameling en veiligstelling van digitale bewijzen
	SLA: Opdrachtnemer verzamelt, beveiligt en documenteert alle relevante digitale bewijzen (logs, geheugen dumps, netwerkverkeer, etc.) conform chain-of-custody procedures en binnen de overeengekomen tijdslimiet (bijvoorbeeld binnen 24 uur na start onderzoek).
	Doel: Integriteit, authenticiteit en juridische houdbaarheid van bewijsmateriaal waarborgen.
A.327	Forensische analyse en rapportage
	SLA: Opdrachtnemer levert een volledig forensisch rapport inclusief root cause analysis binnen 10 Werkdagen na start van het onderzoek, tenzij anders afgesproken met de Deelnemer.
	Doel: Tijdige en bruikbare analyse voor incidentafhandeling en preventieve maatregelen.

A.328	Integriteit- en authenticiteitsbewijzen
	SLA: Opdrachtnemer documenteert alle stappen in het forensische proces, inclusief hash-waarden, audit-trails en wijzigingen, zodat de authenticiteit van alle digitale bewijzen aantoonbaar is.
	Doel: Juridisch en compliance-proof verantwoording van het onderzoek.
A.329	Overdracht en archivering
	SLA: Opdrachtnemer draagt alle verzamelde forensische data en documentatie op verzoek veilig en volledig over aan Deelnemer of opvolgende opdrachtnemer en archiveert de data minimaal 12 maanden, tenzij anders afgesproken.
	Doel: Borging van continuïteit, naleving van regelgeving (BIO, AVG, Cbw) en traceerbaarheid van bewijs.
Deliverables	
A.330	Forensische rapportages inclusief root cause analysis
	Opdrachtnemer levert forensische rapportages per incident, inclusief een gedetailleerde root cause analysis, vastgestelde aanvalsvectoren, gebruikte technieken en impact op systemen van de Deelnemer.
A.331	Chain-of-custody documentatie
	Opdrachtnemer levert volledige chain-of-custody documentatie voor alle digitale bewijsmaterialen, waarin de herkomst, overdracht, verwerking en opslag van data aantoonbaar wordt vastgelegd.
A.332	Bewijsverzameling
	Opdrachtnemer verzamelt, documenteert en levert digitale bewijzen, waaronder logbestanden, geheugen dumps en netwerkverkeer, op een juridisch verantwoorde wijze.
A.333	Integriteit- en authenticiteitsbewijzen van digitale data
	Opdrachtnemer levert bewijs van integriteit en authenticiteit van alle verzamelde digitale data, inclusief cryptografische hashes en verificatiestappen.
A.334	Documentatie van gebruikte forensische tooling en methodologie
	Opdrachtnemer documenteert alle gebruikte forensische tools, methodieken en procedures, inclusief certificeringen van tooling en naleving van internationale standaarden (zoals ISO 27037).
A.335	Versleutelde opslag van forensische data
	Opdrachtnemer levert alle forensische data in versleutelde vorm, tenzij anders schriftelijk overeengekomen met de Deelnemer, en borgt daarmee vertrouwelijkheid en compliance met wet- en regelgeving.

4.5 Optioneel – Tabletop

Doel: Het testen, oefenen en verbeteren van Beveiligingsincidentresponsprocessen, besluitvorming, samenwerking en communicatie binnen de organisatie, door middel van gesimuleerde Beveiligingsincident-scenario's in een gecontroleerde, niet-technische setting.

Wat valt hieronder?

- Voorbereiding en planning van tabletop-sessies, inclusief doelstellingen, Deelnemers, scenario-opzet, tijdslijnen en benodigde materialen.
- Ontwikkeling van realistische, actuele en organisatie-specifieke scenario's, gebaseerd op dreigingsbeeld, ketenafhankelijkheden en kritieke processen.
- Afstemming van scope, deelnemersrollen en scenario's met de Deelnemer voorafgaand aan de oefening.
- Uitvoering van de tabletop-oefening, waarbij alle relevante stakeholders deelnemen, zoals SOC-analisten, IT-beheer, security officers, OT-specialisten, management, communicatie en bestuur.
- Faciliteren van discussies, beslismomenten en injects (gebeurtenisprykkels) om respons, samenwerking en escalatiepaden te testen.
- Evaluatie van het optreden, inclusief sterke punten, knelpunten, beslismomenten, communicatiekwaliteit en naleving van procedures (bijv. CSIRT-proces, escalatiepaden, crisisstructuren).
- Oplevering van een after-action rapport, waarin bevindingen, risico's en verbeterpunten worden vastgelegd.
- Advisering over procesverbeteringen, waaronder aanpassingen in Beveiligingsincidentresponsplannen, communicatieprotocollen, technische maatregelen of governance.
- Herhaalbaarheid en continue verbetering, waarbij uitkomsten worden gebruikt om toekomstige tabletop-oefeningen te verfijnen.
- Optioneel: integratie met bredere crisioefeningen, zoals war gaming, red team-blue team scenario's of ketenoefeningen met externe partijen.

Kernvraag: *Kan de organisatie een Beveiligingsincident effectief herkennen, escaleren, beheersen en herstellen op basis van bestaande processen en besluitvorming?*

Resultaat: Een geteste en geëvalueerde responsketen, inclusief een rapport met bevindingen, aanbevelingen en verbetermaatregelen ter versterking van de weerbaarheid en samenwerking.

Eisen	
	Doel en algemene verplichting
A.336	Opdrachtnemer levert, op verzoek van de Deelnemer, de dienst Tabletop-oefeningen, gericht op het in een gecontroleerde, niet-technische setting testen en verbeteren van Beveiligingsincidentresponsprocessen, samenwerking, besluitvorming, communicatie en rollen bij Beveiligingsincident.
A.337	Een tabletop-oefening betreft een gesimuleerd scenario waarbij relevante betrokkenen (zoals SOC-analisten, IT-beheerders, security officers, management, communicatie en ketenpartners) gezamenlijk door een fictieve Beveiligingsincident-situatie worden geleid.
	Planning, afstemming en doelstelling
A.338	Opdrachtnemer voert een tabletop-oefening uit op verzoek van de Deelnemer.
A.339	Opdrachtnemer plant iedere tabletop-oefening vooraf in overleg met de Deelnemer en legt datum, tijd, Deelnemers, locatie en randvoorwaarden vast.

A.340	Opdrachtnemer bepaalt vooraf, in afstemming met de Deelnemer, de scope, reikwijdte en doelstellingen van de tabletop-oefening. De uiteindelijke scope wordt ter goedkeuring voorgelegd aan de Deelnemer.
A.341	Iedere tabletop-oefening heeft duidelijke, vooraf gedefinieerde leerdoelen (zoals testen van escalatieprocessen, besluitvorming, communicatie, ketensamenwerking of crisisteaminzet).
	Scenario-ontwikkeling
A.342	Opdrachtnemer ontwikkelt realistische en actuele scenario's, gebaseerd op: • dreigingen uit threat intelligence, • relevante sectorspecifieke risico's, • trends in Beveiligingsincidenten, • tactieken en technieken volgens erkende frameworks (bijv. MITRE ATT&CK).
A.343	De scenario's worden afgestemd op de processen, kritieke systemen, risico's en organisatorische context van de Deelnemer.
A.344	Scenario's bevatten voldoende detail en dynamiek om besluitvorming, samenwerking, rolverdeling en escalatiepaden effectief te toetsen.
	Uitvoering van de tabletop-oefening
A.345	Opdrachtnemer faciliteert en begeleidt de tabletop-oefening, inclusief moderatie, rollenspellen, injects en tijdsopbouw.
A.346	Opdrachtnemer bewaakt het behalen van de vooraf vastgestelde doelstellingen en stuurt de oefening zodanig dat alle relevante onderdelen worden doorlopen.
A.347	Opdrachtnemer zorgt voor een veilige omgeving waarin Deelnemers vrij kunnen oefenen, falen, reflecteren en leren.
	Evaluatie en rapportage
A.348	Opdrachtnemer voert direct na afloop een debriefing uit met de Deelnemers waarin observaties, knelpunten, verbeterpunten en succesfactoren worden besproken.
A.349	Opdrachtnemer levert een schriftelijke evaluatie binnen een vooraf overeengekomen termijn. De evaluatie bevat minimaal: • beschrijving van het scenario en de scope, • geobserveerde reacties en besluitvorming, • effectiviteit van processen en samenwerking, • gesignaleerde risico's en verbeterpunten, • concrete aanbevelingen voor verbetering van processen, procedures en communicatie, • eventuele vervolgacties.
A.350	Opdrachtnemer verwerkt de leerpunten uit de tabletop-oefening in een verbeterplan, indien de Deelnemer dit verlangt.

SLA-paramaters	
A.351	Oefenplanning en -afstemming
	SLA: Opdrachtnemer plant iedere tabletop-oefening minimaal 6 weken vooraf in overleg met Deelnemer en verstrekt een formeel oefenplan ter goedkeuring.
	Doel: Zekerstellen dat alle stakeholders voldoende tijd hebben voor voorbereiding en afstemming.
A.352	Scenario-ontwikkeling
	SLA: Opdrachtnemer levert scenario's die relevant zijn voor de kritieke processen van Deelnemer en gebaseerd zijn op actuele dreigingen minimaal 4 weken voor de oefening.
	Doel: Kwalitatief hoogwaardige, actuele en realistische scenario's waarborgen.
A.353	Oefenuitvoering
	SLA: Opdrachtnemer voert de tabletop-oefening uit op de afgesproken datum en tijd, met aanwezigheid van alle vooraf benoemde rollen en Deelnemers.
	Doel: Continuïteit en volledigheid van de oefening garanderen.
A.354	Rapportage en lessons learned
	SLA: Opdrachtnemer levert het observatierapport en overzicht van lessons learned binnen 10 Werkdagen na de oefening, inclusief voorgestelde verbeteracties, status en prioriteit.
	Doel: Tijdige terugkoppeling voor verbetering van processen, rollen en procedures.
A.355	Opvolging van verbeteracties
	SLA: Opdrachtnemer volgt periodiek (bijv. kwartaal) de implementatie van de voorgestelde verbeteracties en rapporteert de voortgang aan Deelnemer.
	Doel: Borging van continue verbetering van incidentresponsprocessen.
Deliverables	
4.5.21	Tabletop-scenario en oefenplan
	Opdrachtnemer levert voorafgaand aan elke tabletop-oefening een gedetailleerd scenario en oefenplan, inclusief doelstellingen, scope, betrokken rollen, verwachte acties en tijdsplanning. Het scenario sluit aan op actuele dreigingen, kritieke processen en systemen van de Deelnemer.
4.5.22	Observatierapporten en lessons learned
	Opdrachtnemer levert na afloop van de tabletop-oefening een rapport met observaties, bevindingen en lessons learned, waarmee inzicht wordt gegeven in prestaties van processen, besluitvorming en samenwerking tijdens de oefening.

4.5.23	Adviezen voor proces- en rolverbetering
	Opdrachtnemer verstrekt concrete aanbevelingen voor verbetering van incidentresponsprocessen, procedures en rolverdelingen, gebaseerd op de uitkomsten van de tabletop-oefening.
4.5.24	Documentatie van aanpassingen in procedures
	Opdrachtnemer documenteert alle voorgestelde en doorgevoerde wijzigingen in procedures, werkafspraken en protocollen die voortvloeien uit de tabletop-oefening, inclusief versiebeheer en audit-trail.

4.6 Optioneel - Uitrol sensoren

Uitgangspunt is dat Deelnemers in beginsel zelf verantwoordelijk zijn voor de aanschaf van sensoren die worden ingezet voor securitymonitoring. In geval van aanschaf door de Deelnemer blijft de Deelnemer eigenaar van de betreffende sensor(en).

Voor IT-omgevingen kan het voorkomen dat sensoren onderdeel uitmaken van reeds gebruikte IT-oplossingen of securityproducten. Indien aanvullende IT-sensoren moeten worden aangeschaft, kan dit gepaard gaan met softwarelicenties, abonnementen of andere contractuele verplichtingen die rechtstreeks tussen de Deelnemer en de betreffende leverancier worden afgesloten.

Voor OT-omgevingen geldt dat sensoren in veel gevallen gespecialiseerde oplossingen betreffen. Deelnemers behouden de mogelijkheid om dergelijke OT-sensoren zelfstandig en separaat aan te schaffen, bijvoorbeeld via bestaande leveranciers of specifieke OT-beveiligingsoplossingen.

Deze Raamovereenkomst sluit niet uit dat sensoren via de Opdrachtnemer kunnen worden afgenomen. Indien een Deelnemer ervoor kiest sensoren via de Opdrachtnemer te betrekken, vindt dit plaats als Speciaal Product en/of Speciale Dienst, conform de bepalingen van de Raamovereenkomst.

Ongeacht de wijze van aanschaf dienen sensoren zodanig te worden geïmplementeerd en geconfigureerd dat zij kunnen worden geïntegreerd met de SOC-dienstverlening en dat de Deelnemer bij beëindiging van de overeenkomst kan blijven beschikken over de sensoren en de bijbehorende configuratie.

Doel: Het implementeren, configureren en beheren van detectiesensoren op alle relevante IT-, OT- en cloud-assets van de Deelnemer, met als doel het creëren van een volledige, betrouwbare en actuele bron van security-data voor monitoring, analyse en Beveiligingsincidentrespons.

Wat valt hieronder?

- Inventarisatie en afstemming van de sensorscope met de Deelnemer, gebaseerd op de actuele CMDB, criticiteit, netwerksegmentatie en monitoringsbehoefte.
- Opstellen van een plan van aanpak, inclusief planning, aanpak, afhankelijkheden, testmomenten en overdrachtscriteria, ter goedkeuring door de Deelnemer.
- Implementatie en configuratie van detectiesensoren op alle door de Deelnemer aangewezen assets, waaronder:
 - endpoints en servers
 - netwerkkapapparaat
 - OT-systemen
 - industriële protocollen
 - cloud-diensten en workloads
- Configuratie van sensoren conform beveiligingsbeleid van de Deelnemer (o.a. loggingniveau, retentie, encryptie, privacyrichtlijnen, hardening).
- Afstemming van sensorplaatsing met de Deelnemer, inclusief segmentatie, kritieke locaties en afhankelijkheden.

- Testen van correcte werking, waaronder datastromen, Eventgeneratie, detectiekwaliteit en verbinding met SIEM/SOC-platform.
- Doorlopende monitoring van sensorstatus en datastromen, inclusief health checks, foutdetectie en optimalisatie.
- Documentatie van installatie, configuratie en beheermaatregelen, inclusief versies, locaties, instellingen en deviatieafspraken.
- Rapportage over voortgang van de uitrol, inclusief afwijkingen, risico's en afhankelijkheden.
- Overdracht van sensoren aan de Deelnemer, waarbij sensoren eigendom zijn van de Deelnemer en overdraagbaar zijn bij contractbeëindiging.
- Ondersteuning bij beheer en onderhoud, inclusief updates, patches, tuning en vervanging, op verzoek van de Deelnemer.
- Zorg voor veilige gegevensstromen, waaronder versleuteling en integriteitsborging tijdens transport.

Kernvraag: *Is de sensorinfrastructuur volledig, betrouwbaar en correct geconfigureerd om alle relevante security-Events en telemetry tijdig en volledig aan te leveren aan het SOC?*

Resultaat: Een volledig uitgerolde, gedocumenteerde en operationele sensorinfrastructuur die betrouwbare en actuele security-data levert voor monitoring, detectie en Beveiligingsincidentrespons.

Eisen	
	Doel en dienstverlening
A.356	Opdrachtnemer levert op verzoek van de Deelnemer de dienst uitrol van sensoren met als doel een volledige en betrouwbare bron van securitydata te creëren ten behoeve van detectie, analyse en respons.
	Planning en afstemming
A.357	Opdrachtnemer stelt voor de uitrol een plan van aanpak op, inclusief planning, fasering, afhankelijkheden en benodigde middelen.
A.358	Het plan van aanpak wordt vooraf ter goedkeuring aan de Deelnemer voorgelegd.
A.359	Opdrachtnemer rapporteert gedurende de uitvoering met de met de Deelnemer overeengekomen frequentie over de voortgang van de uitrol.
	Scopebepaling en betrokkenheid van de Deelnemer
A.360	De Deelnemer heeft inspraak in de plaatsing, scope en configuratie van de sensoren.
A.361	De uiteindelijke scope en configuratie worden vastgelegd in het door de Deelnemer goedgekeurde plan van aanpak.
	Implementatievereisten
A.362	Opdrachtnemer implementeert sensoren op alle door de Deelnemer aangewezen IT-assets, waaronder servers, endpoints, netwerkapparatuur, cloudomgevingen en, indien van toepassing, OT-systemen.
A.363	Opdrachtnemer configureert alle sensoren conform het securitybeleid en de richtlijnen van de Deelnemer.

A.364	Opdrachtnemer documenteert de installatie-, configuratie- en implementatiestappen op een controleerbare en reproduceerbare wijze.
	Beheer en overdraagbaarheid
A.365	Opdrachtnemer levert op verzoek van de Deelnemer ondersteuning bij sensorbeheer en monitoring.
SLA-paramaters	
A.366	Tijdige oplevering
	SLA: Opdrachtnemer voltooit de uitrol van de sensoren conform het goedgekeurde plan van aanpak binnen de afgesproken termijn (bijv. 90% van de sensoren binnen de planning).
	Doel: Waarborgen dat de Deelnemer tijdig over een volledig functionerende sensorinfrastructuur beschikt.
	Bewijsstuk: Opleverrapport met statussensoren en realisatiedatum per asset.
A.367	Operationele beschikbaarheid van sensoren
	SLA: Minimaal 95% van de sensoren is operationeel en levert correcte securitydata aan het SOC-/SIEM-platform gedurende de eerste maand na uitrol, tenzij anders overeengekomen.
	Doel: Zekerstellen dat de sensoren daadwerkelijk bruikbare en actuele data aanleveren.
	Bewijsstuk: Monitoringrapport sensorstatus, datastromen en Eventgeneratie.
A.368	Correcte configuratie
	SLA: Alle sensoren worden geïmplementeerd en geconfigureerd volgens het goedgekeurde plan, inclusief loggingniveau, retentie, encryptie en privacyrichtlijnen.
	Doel: Borging van compliance, veiligheid en betrouwbaarheid van data.
	Bewijsstuk: Configuratieoverzicht, testresultaten en validatierapport.
A.369	Test en verificatie
	SLA: Na uitrol voert de Opdrachtnemer tests uit op alle sensoren om datastromen, Eventgeneratie, detectiekwiteit en verbinding met het SOC-/SIEM-platform te verifiëren, met minimaal 90% van de tests succesvol.
	Doel: Valideren dat de sensorinfrastructuur daadwerkelijk functioneel is en securitydata correct aanlevert.
	Bewijsstuk: Testresultaten en validatierapport, inclusief openstaande issues en remediatieplan.

A.370	Overdraagbaarheid van sensoren
	SLA: Alle sensoren en configuraties zijn overdraagbaar aan de Deelnemer of een opvolgende opdrachtnemer bij beëindiging van de overeenkomst, zonder verlies van functionaliteit of historische configuratie-informatie.
	Doel: Vendor lock-in mitigatie en continuïteit van monitoringdiensten.
	Bewijsstuk: Export van configuraties, documentatie van sensorinstellingen en overdrachtsrapport.
Deliverables	
A.371	Geïmplementeerde sensoren
	Opdrachtnemer levert een operationele implementatie van detectiesensoren op de in het plan van aanpak en de sensorscope vastgelegde IT-, OT- en cloud-assets van de Deelnemer. De sensoren zijn correct geïnstalleerd, geconfigureerd en verbonden met het SOC-/SIEM-platform, zodat relevante security-Events en telemetry betrouwbaar worden verzameld en beschikbaar zijn voor monitoring, detectie en Beveiligingsincidentrespons.
A.372	Documentatie sensorinfrastructuur
	Opdrachtnemer levert volledige en actuele documentatie van de geïmplementeerde sensoren, inclusief locatie, type sensor, configuratie-instellingen, versies, afhankelijkheden, datastromen en beheerprocedures. De documentatie stelt de Deelnemer in staat de sensorinfrastructuur te begrijpen, te beheren en – indien nodig – over te dragen aan een andere dienstverlener.
A.373	Geteste sensorinfrastructuur
	Opdrachtnemer levert aantoonbaar geteste sensoren, waarbij de correcte werking is gevalideerd door middel van functionele tests, verificatie van datastromen naar het SOC-/SIEM-platform en controle op Eventgeneratie en detectiekwaliteit. De testresultaten tonen aan dat de sensoren operationeel zijn en betrouwbare securitydata leveren voor monitoring en incidentdetectie.
A.374	Acceptatie- en opleverrapport
	Opdrachtnemer levert na afronding van de sensoruitrol een opleverrapport waarin wordt bevestigd dat de sensoren conform het goedgekeurde plan van aanpak zijn geïmplementeerd. Het rapport bevat ten minste een overzicht van de uitgerolde sensoren, eventuele afwijkingen ten opzichte van de oorspronkelijke scope, openstaande punten en de bevestiging dat de sensoren operationeel zijn en data aanleveren aan het SOC-/SIEM-platform.
A.375	Overzicht sensorinfrastructuur
	Opdrachtnemer levert een actueel overzicht van de geïmplementeerde sensoren en de bijbehorende assets waarop deze zijn geplaatst. Dit overzicht bevat ten minste het type sensor, de gekoppelde asset of omgeving, locatie of netwerksegment, status van de sensor en de verbinding met het SOC-/SIEM-platform, zodat inzicht bestaat in de dekking van de sensorinfrastructuur.

A.376	Overdraagbare sensorconfiguratie
	Opdrachtnemer levert op verzoek van de Deelnemer de configuratie-instellingen van de geïmplementeerde sensoren in een reproduceerbaar en overdraagbaar formaat. Hierdoor kan de Deelnemer de sensorinfrastructuur zelfstandig beheren of overdragen aan een andere dienstverlener bij beëindiging van de overeenkomst of wijziging van dienstverlening.

5 Implementatie

De implementatie van SOC-diensten verloopt gefaseerd per Deelnemer en is gebaseerd op een gestandaardiseerde, herhaalbare en iteratieve aanpak. De implementatie omvat de volledige lifecycle van de dienstverlening, waaronder contractering, intake, data onboarding, inrichting van detectie en automatisering, validatie, operationele start en doorlopende optimalisatie.

De implementatie sluit aan op Bijlage 4 – SOC Use Case Roadmap en is gericht op het gefaseerd opbouwen en doorontwikkelen van detectiecapaciteit, in samenhang met databronnen, processen en organisatorische inbedding. Hierbij wordt onderscheid gemaakt in:

- Fase 1: basisdetectie;
- Fase 2: verdieping en correlatie;
- Fase 3: geavanceerde detectie en automatisering.

Per Deelnemer wordt Fase 1 binnen maximaal zes (6) maanden na start van de dienstverlening gerealiseerd. Voor alle Deelnemers gezamenlijk geldt dat Fase 1 binnen twaalf (12) maanden na aanvang van de Raamovereenkomst is geïmplementeerd. Verdere doorontwikkeling vindt plaats conform Fase 2 en Fase 3.

Use Case Management maakt integraal onderdeel uit van de Basis SOC-diensten en vormt het primaire mechanisme voor de inrichting en doorontwikkeling van detectie. In het basistarief is een jaarlijkse groei van het aantal use cases van 10% inbegrepen conform Bijlage 4. Aanvullende groei wordt afgerekend op basis van inzet (PxQ).

De implementatie vindt plaats volgens een centraal gecoördineerde, gefaseerde uitrolplanning, waarbij beheersbaarheid, kwaliteit en onderlinge samenhang tussen Deelnemers worden geborgd. Om deze reden starten maximaal twee Deelnemers per periode van zes weken.

De regieorganisatie is verantwoordelijk voor coördinatie, prioritering en voortgangsbewaking. De Opdrachtnemer draagt zorg voor een consistente uitvoering en borgt dat ontwikkelde componenten, waaronder use cases, datakoppelingen, playbooks en configuraties, maximaal worden hergebruikt tussen Deelnemers, tenzij aantoonbaar niet mogelijk.

De implementatie is gericht op uniforme inrichting, schaalbaarheid en continue verbetering. Optimalisaties en doorontwikkelingen worden, waar relevant, doorgevoerd bij alle aangesloten Deelnemers.

Stap 1: Ondertekening Nadere Overeenkomst	
A.377	De Deelnemer sluit een Nadere Overeenkomst (NOK) met de Opdrachtnemer voor de afname van de Basis SOC-diensten voor IT-omgevingen en – indien van toepassing – OT-omgevingen.
A.378	In de Nadere Overeenkomst worden ten minste afspraken vastgelegd over: – de omvang en scope van de dienstverlening (IT en optioneel OT); – de initiële set use cases conform Bijlage 4 (Fase 1); – servicetijden en toepasselijke SLA/OLA; – rapportages en dashboards; – communicatie-, escalatie- en governanceafspraken.
A.379	Doel: – Formeel kader creëren; – Scope en randvoorwaarden vastleggen.

Stap 2: Initiële kick-off en intake	
A.380	De Opdrachtnemer organiseert samen met de Deelnemer een gezamenlijke kick-off en intake.
A.381	Tijdens deze fase wordt ten minste geïnventariseerd: - IT- en OT-assets die gemonitord moeten worden; - de bestaande infrastructuur, logging- en detectiemogelijkheden; - relevante interne processen en contactpersonen; - prioritaire use cases voor de initiële fase (Fase 1 roadmap); - benodigde toegangsrechten en randvoorwaarden, waaronder: - o toegang tot cloudomgevingen (bijv. Azure); - o toegang tot security-oplossingen (bijv. Microsoft Defender, Entra ID); - o toegang tot netwerkcomponenten en logbronnen; - o benodigde rechten voor integratie met ITSM- en/of SOAR-oplossingen.
A.382	Doel: - Vaststellen van de uitgangssituatie en prioriteiten; - Borgen dat alle technische en organisatorische randvoorwaarden tijdig beschikbaar zijn.
Stap 3: Data onboarding en validatie	
A.383	De Opdrachtnemer sluit in overleg met de Deelnemer gefaseerd databronnen aan. Dit omvat onder andere: - Microsoft-bronnen (bijv. Entra ID, Microsoft 365, Defender, Azure logs); - netwerkcomponenten (bijv. firewalls, switches, syslog); - endpoints en servers; - cloud- en SaaS-applicaties; - OT-bronnen (indien van toepassing).
A.384	De Opdrachtnemer: - prioriteert databronnen op basis van risicowaarde en detectiewaarde; - richt parsing, normalisatie en correlatie van logdata in; - valideert datakwaliteit, volledigheid en consistentie; - stemt dataverzameling af op performance, kosten en detectiebehoefte.
A.385	Doel: - Realiseren van betrouwbare, volledige en kostenefficiënte datastromen als fundament voor effectieve detectie en monitoring.
Stap 4: Implementatie use cases en detectielogica	
A.386	Opdrachtnemer implementeert detectieregels, use cases en automatisering conform de SOC Use Case Roadmap (Bijlage 4). Dit omvat: - implementatie van out-of-the-box detecties; - aanvulling met maatwerk use cases; - toepassing van hergebruik tussen Deelnemers; - inrichting van SOAR/playbooks; - integratie van threat intelligence.

	Voor OT geldt: - overdracht en integratie van bestaande use cases (bijv. Flevoland); - gefaseerde uitbreiding naar andere Deelnemers.
A.387	Doel: - Opbouwen van effectieve en schaalbare detectiecapaciteit.
Stap 5: Validatie en acceptatie	
A.388	De Deelnemer en Opdrachtnemer voeren gezamenlijk validatie- en acceptatietests uit. Dit omvat ten minste: - controle op logintegriteit en datavolledigheid; - verificatie van de werking van use cases en detectieregels; - beoordeling van alertkwaliteit (false positives en false negatives); - validatie van dashboards, rapportages en escalatieprocedures; - aanvullende validatie van: - o datadekking en prioritering van databronnen; - o effectiviteit van threat intelligence-integraties; - o werking van automatisering en playbooks; - o datavolumes en kostenindicaties (indien van toepassing).
A.389	Doel: - Bevestigen dat de SOC-dienstverlening voldoet aan de overeengekomen kwaliteits- en prestatie-eisen; - Verifiëren dat zowel functionele, operationele als financiële uitgangspunten correct zijn ingericht.
Stap 6: Operationele start en monitoring	
A.390	Na acceptatie wordt de SOC-dienstverlening operationeel. De Opdrachtnemer: - voert monitoring, eventmanagement en rapportage uit conform de in de Nadere Overeenkomst overeengekomen servicetijden; - ondersteunt de Deelnemer bij de opvolging van alerts en beveiligingsincidenten; - evalueert periodiek de effectiviteit van use cases en detectiekwaliteit.
A.391	Doel: - Borgen van continu en betrouwbaar toezicht op IT- en OT-omgevingen.
Stap 7: Geleidelijke uitbreiding van diensten	
A.392	De Deelnemer kan in overleg met de Opdrachtnemer de dienstverlening uitbreiden. Dit omvat onder andere: - uitbreiding van het aantal use cases;

	- uitbreiding van databronnen; - uitbreiding van servicetijden tot 24/7; - afname van aanvullende SOC-diensten, zoals: - Threat Hunting; - o Forensics; - o Tabletop-oefeningen; - o Situational Awareness; - o Vulnerability Management.
A.393	Doel: - Opschalen van de SOC-dienstverlening in lijn met de volwassenheid en risicobehoeft van de Deelnemer.
Stap 8: Periodieke evaluatie en optimalisatie	
A.394	De Opdrachtnemer en Deelnemer voeren periodiek evaluaties uit (bijv. per kwartaal). Dit omvat ten minste: - evaluatie van eventmanagement- en incidentresponseprocessen; - beoordeling van de effectiviteit van use cases en detectieregels; - evaluatie van integratie met interne processen; - bespreking van rapportages, bevindingen en verbeteracties; - optimalisatie van: - o datagebruik en ingestiekosten; - o detectieregels en use cases; - o automatisering en responseprocessen; - o aansluiting op actuele dreigingen en threat intelligence.
A.395	Doel: - Continu verbeteren van effectiviteit, efficiëntie en toekomstbestendigheid van de SOC-dienstverlening.
Stap 9: Rapportage en kennisoverdracht	
A.396	De Opdrachtnemer levert periodiek rapportages en verzorgt kennisoverdracht. Dit omvat ten minste: - rapportages over alerts en beveiligingsincidenten; - inzicht in use case performance; - analyse van trends en eventkwaliteit; - overdracht van kennis naar interne SOC-, IT- en securityteams van de Deelnemer.
A.397	Doel: - Borgen van transparantie en compliance; - Versterken van de interne kennis en zelfredzaamheid van de Deelnemer.

Bijlage A - SLA-overzicht per dienst (SOC)

Monitoring & Detectie (3.1)		
SLA-paramater	KPI / Parameter	Norm
Beschikbaarheid platform	Uptime SOC-platform	≥ 99,95% per maand
Monitoring	Continuïteit monitoring	24/7/365
Logvolledigheid	Visibility rate	≥ 98%
Loguitval (kritiek)	Meldtijd	≤ 30 min
Loguitval (niet-kritiek)	Meldtijd	≤ 4 uur
Log latency	Max vertraging	≤ 60 sec
Eventnormalisatie	Verwerkingstijd	≤ 5 min
Eventcorrelatie	Verwerkingstijd	≤ 5 min
Detectietijd (MTTD)	Critical alerts	≤ 10 min
Detectietijd (MTTD)	High alerts	≤ 20 min
Detectieregels evaluatie	Frequentie	≥ 1x per kwartaal
Compliance	Cbw / BIO / ISO	Aantoonbaar compliant

Event Management (3.2.1)		
SLA-paramater	KPI / Parameter	Norm
MTTA (start triage)	Critical alerts	≤ 10 min
MTTA (start triage)	High alerts	≤ 30 min
Escalatie	Naar incidentmanagement	≤ 10 min
Documentatie	Audit trail compleet	≤ 24 uur
Beschikbaarheid team	Eventmanagement	24/7 (of conform service window)

Beveiligingsincident Management (3.2.2)		
Reactietijden (RTO)		
Prioriteit	80% norm	100% norm
P1 Critical	≤ 30 min	≤ 1 uur

P2 High	≤ 1 uur	≤ 4 uur
P3 Medium	≤ 4 uur	≤ 24 uur
Operationele KPI's		
SLA-paramater	KPI / Parameter	Norm
MTTC (containment)	Critical	≤ 4 uur
MTTC (containment)	High	≤ 8 uur
MTTI (analyse)	Critical (initieel / volledig)	≤ 2 uur / ≤ 24 uur
MTTI (analyse)	High (initieel / volledig)	≤ 4 uur / ≤ 48 uur
MTTR (oplossing)	Critical	≤ 48 uur
MTTR (oplossing)	High	≤ 72 uur
RCA	Oplevering	≤ 5 werkdagen
Communicatie & escalatie		
SLA-paramater	KPI / Parameter	Norm
Eerste melding	Na classificatie	≤ 15 min
Statusupdates	Critical	Elk uur
Statusupdates	High	Elke 4 uur
CSIRT escalatie	Critical incident	≤ 30 min
Melding sector-CSIRT	NCSC	≤ 24 uur
Forensics & compliance		
SLA-paramater	KPI / Parameter	Norm
Start forensics	Na verzoek	≤ 1 uur
Oplevering data	Forensisch pakket	≤ 48 uur
Meldplicht signalering	Incident	≤ 1 uur
Aanlevering melddata	Technische info	≤ 4 uur

CSIRT Activatie (3.2.3)		
SLA-paramater	KPI / Parameter	Norm
Beschikbaarheid	Incidentcoördinator	24h/7d
Reactietijd	Start coördinatie	≤ 15 min

Escalatie	Naar CSIRT	≤ 30 min
Datalevering	Logs & artefacten	≤ 1 uur
Communicatie	Beveiligde kanalen	Verplicht
Samenwerking	Real-time info	Verplicht
Evaluatie	CSIRT samenwerking	≥ 1 x per jaar