Begeleidend document vervolgmarktconsultatie

Inventarisatie van mogelijkheden inzake:

Sectoraal Security Operations Center (SOC)

Interprovinciaal Overleg
van, voor en door provincies

BIJ12

Status : Voorlopig
Versie : 260506-1
Datum : 06-05-2022

Inhoudsopgave

1 Inleiding

IPO/BIJ12 heeft in 2025 een marktconsultatie uitgevoerd om informatie uit de markt op te halen. Het doel van deze consultatie was om, voorafgaand aan het opstellen van de aanbesteding, inzicht te verkrijgen in de beschikbare mogelijkheden op het gebied van Security Operations Center (SOC)-diensten. De marktconsultatie en het bijbehorende verslag zijn te raadplegen via de volgende link: Marktconsultatie Security Operations Center (SOC)

Aansluitend is IPO/BIJ12, samen met de provincies, gestart met de voorbereiding van de aanbesteding voor SOC-dienstverlening. In dit kader is de behoefte aan SOC-diensten bij de beoogde deelnemers geïnventariseerd en vastgelegd. Deze inventarisatie is inmiddels zodanig gevorderd dat een deel van de resultaten beschikbaar kan worden gesteld aan marktpartijen en deelnemers, in de vorm van een vervolgmarktconsultatie via TenderNed.

Dit document bevat een beschrijving van de gevraagde dienstverlening (hoofdstuk 3) en Bijlagen met de eisen en wensen die het projectteam voornemens is op te nemen in de aanbestedingsdocumenten voor het Sectoraal SOC. De nadruk ligt daarbij op de beschrijving van de prestatie, ook wel aangeduid als het Programma van Eisen.

Het doel van dit document is om potentiële marktpartijen, evenals partijen die reeds hebben deelgenomen aan de eerdere marktconsultatie, in een vroeg stadium te informeren over onderdelen van de voorgenomen aanbesteding. Hiermee wordt beoogd marktpartijen en deelnemers in de gelegenheid te stellen om, voorafgaand aan de officiële publicatie van de aanbesteding, feedback te geven op (onderdelen van) de gevraagde dienstverlening.

Lezers worden van harte uitgenodigd hun feedback in te dienen via de berichtenmodule van TenderNed. Het projectteam zal deze input zorgvuldig beoordelen en afwegen in hoeverre deze aanleiding geeft tot aanpassing van de gestelde eisen.

Alle in dit document opgenomen informatie dient te worden beschouwd als een momentopname en is derhalve onderhevig aan wijzigingen. Aan de inhoud van dit document kunnen geen rechten worden ontleend. Indien daartoe aanleiding bestaat op basis van nieuwe of gewijzigde inzichten, zal het projectteam geactualiseerde versies van dit document publiceren via TenderNed.

1.1 De opbouw van het marktconsultatiedocument

Dit document richt zich tot geïnteresseerde partijen. Het bevat uitleg over de marktconsultatie zelf en bevat een aantal vragen die IPO/BIJ12 aan geïnteresseerde partijen in de markt wenst voor te leggen.

- Hoofdstuk 2 gaat in op het doel, de procedure, de planning en de voorwaarden van de marktconsultatie.
- Hoofdstuk 3 Toelichting gevraagde SOC-dienstverlening
- Bijlage 1a - Specificatie van de Prestatie - Diensten
- Bijlage 1b - Specificatie van de Prestatie - Architectuur
- Bijlage 1b - Specificatie van de Prestatie – Kwaliteits- en Prestatie-eisen
- Bijlage 2 – Programma van Wensen

1.2 Afkortingen

In dit document worden afkortingen en begrippen gebruikt met de volgende betekenis.

Afkorting	Betekenis
Aanbestedende dienst	Opdrachtgever die voornemens is namens de provincies en gelieerde organisatie een aanbesteding uit te schrijven en middels dit document te voorbereiding informatie wenst te verzamelen.
Beveiligingsincident	Een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van netwerk- en informatiesystemen of de daarin opgeslagen, verzonden of verwerkte gegevens in gevaar brengt of aantast, dan wel een aanzienlijke verstoring van de dienstverlening

	kan veroorzaken. (Beveiligingsincident wordt ook wel aangeduid als Securityincident.
CBW	Cyberbeveiligingswet
CIBO	Centraal Informatiebeveiliging Overleg
CISO	Chief Information Security Officer
CSIR	CyberSecurity ImplementatieRichtlijn
CSIRT	Computer Security Incident Response Teams
Databron	Een systeem, applicatie, apparaat of platform dat relevante beveiligingsdata genereert of opslaat, en die door het SOC wordt gebruikt voor monitoring en analyse.
Deelnemer	Een overheidsorganisatie namens wie de Aanbesteding wordt uitgevoerd en de Raamovereenkomst wordt gesloten. Een limitatieve lijst van Deelnemers is opgenomen als Bijlage XX – Opgave Deelnemers aan de Raamovereenkomst. Tevens Opdrachtgever zoals bedoeld in artikel 1.22 ARBIT-2022.
Event	Een Event is een enkel, specifieke voorval of activiteit die plaatsvindt binnen de IT-infrastructuur van een organisatie en die mogelijk relevant is voor beveiliging.
Hoofdopdrachtgever	IPO/BIJ12 die namens de Deelnemers de Raamovereenkomst sluit. Tevens Opdrachtgever zoals bedoeld in artikel in artikel 1.22 ARBIT-2022.
IPO	Interprovinciaal Overleg
IT	Informatie Technologie (ook wel kantoorautomatisering of KA genoemd)
IT Databron	Een Databron in de IT infrastructuur.
KPI	Key Performance Indicator
MSP	Managed Service Provider (Een MSP levert netwerk-, applicatie-, database- en andere algemene IT-ondersteuning en diensten
MSSP	Managed Security Service Provider Richt zich uitsluitend op het leveren van cyberbeveiligingsdiensten.
MTTA	Mean Time To Acknowledge/Analyse
MTTD	Mean Time To Detect
NCSC	Nationaal Cyber Security Centrum
NIS2	Network and Information Security (NIS2) richtlijn
Opdrachtnemer	De leverancier (in geval van de levering van een Product en een gebruiksrecht) en/of opdrachtnemer (in geval van het uitvoeren van een Dienst) zoals bedoeld in artikel 1.23 ARBIT-2022.
OT	Operationele Technologie (ook wel procesautomatisering of PA genoemd) (verkeersregelings-installaties en bedieningssoftware voor bruggen, sluizen en gemalen e.d.)
OT Databron	Een Databron in de OT-infrastructuur.
Professioneel	In overeenstemming met de eisen die zijn gesteld aan de te leveren Prestatie, bekwaam, adequaat, vakkundig en volgens gebruikelijke standaarden, protocollen en gangbare kwaliteitsnormen van het betreffende vakgebied. Het beoordelen of het handelen professioneel is geweest in de zin van het bovenstaande, kan worden voorgelegd aan een onafhankelijke marktdeskundige of branche organisatie.
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOC-diensten	De door Opdrachtnemer geleverde diensten gericht op het continu monitoren, detecteren, analyseren en opvolgen van beveiligingsincidenten en -dreigingen binnen de IT- en OT-omgevingen van de Deelnemers, waaronder begrepen logmonitoring, alerting, incident triage, rapportage en advisering op het gebied van informatiebeveiliging.

2 Doel, opzet, planning en voorwaarden

2.1 Doel marktconsultatie

Deze vervolgmarktconsultatie wordt uitgevoerd in aanloop naar de voorgenomen aanbesteding voor sectorale SOC-dienstverlening en maakt geen onderdeel uit van de aanbestedingsprocedure zelf. De consultatie bouwt voort op de eerder in 2025 uitgevoerde marktconsultatie en de nadien uitgevoerde behoefte-inventarisatie onder de beoogde deelnemers.

Met deze vervolgmarktconsultatie beoogt IPO/BIJ12 marktpartijen in een vroegtijdig stadium te informeren over de voorgenomen richting van de aanbesteding, in het bijzonder de (concept)beschrijving van de gevraagde dienstverlening en het bijbehorende Specificatie van de Prestatie (Programma van Eisen).

De informatie die via deze consultatie wordt opgehaald, wordt gebruikt ter verdere aanscherping en validatie van de aanbestedingsdocumenten.

Het doel van deze vervolgmarktconsultatie is tweeledig:

1. IPO/BIJ12 stelt marktpartijen in staat kennis te nemen van de (voorlopige) scope, eisen en wensen met betrekking tot de SOC-dienstverlening, zoals deze op basis van de uitgevoerde inventarisatie zijn opgesteld.
2. IPO/BIJ12 wenst gerichte feedback te verkrijgen van marktpartijen op de voorgestelde dienstverlening, inclusief mogelijke optimalisaties, aandachtspunten en marktconformiteit van de gestelde eisen en randvoorwaarden, teneinde de kwaliteit en uitvoerbaarheid van de voorgenomen aanbesteding te verbeteren.

2.2 Opzet vervolgmarktconsultatie

De vervolgmarktconsultatie vindt primair schriftelijk plaats via TenderNed. Geïnteresseerde marktpartijen worden in de gelegenheid gesteld om op basis van dit document, inclusief de beschrijving van de gevraagde dienstverlening (hdst 3), de (concept) Specificaties van de Prestatie (PvE) en het Programma van Wensen, een goed beeld te vormen van de voorgenomen aanbesteding.

In plaats van een afzonderlijke vragenlijst worden marktpartijen expliciet uitgenodigd om een inhoudelijke review te geven op de opgenomen eisen en wensen, zoals nader toegelicht in paragraaf 2.10. Hierbij wordt in het bijzonder gevraagd aandacht te besteden aan onder meer de consistentie, proportionaliteit en haalbaarheid van de eisen, het prijs- en financieringsmodel, en de indeling van de dienstverlening.

Marktpartijen kunnen hun bevindingen, aandachtspunten en verbetervoorstellen indienen via de berichtenmodule van TenderNed. Deze input wordt door IPO/BIJ12 gebruikt ter verdere aanscherping en validatie van de aanbestedingsdocumenten.

Indien daartoe aanleiding bestaat, kan IPO/BIJ12 besluiten om – aanvullend op de schriftelijke consultatie – verdiepende consultatiegesprekken te voeren met (een selectie van) marktpartijen, teneinde verkregen inzichten nader te duiden.

2.3 Doelgroep marktconsultatie

Iedere belangstellende Ondernemer mag deelnemen aan deze vervolgmarktconsultatie. De deelnemers aan de eerste marktconsultatie zullen wij direct benaderen en attenderen op deze vervolgmarktconsultatie. Met deze marktconsultatie richt IPO/BIJ12 zich direct tot marktpartijen die in de uitvoering van het project zijn geïnteresseerd.

2.4 Planning marktconsultatie

Activiteit	Datum en tijd (CET)
Aankondiging marktconsultatie en beschikbaarstellingmarktconsultatiedocument op TenderNed	Donderdag 30 april 2026
Indienen antwoorden door partijen (via de berichtenmodule in TenderNed)	~~Woensdag 13 mei 2026 12:00 uur~~ Woensdag 20 mei 2026 12:00 uur
Publicatie verslag marktconsultatie	~~Week 22- 23~~ Week 23- 24

2.5 Verslag marktconsultatie

Na afloop van de vervolgmarktconsultatie zal IPO/BIJ12 een verslag opstellen en publiceren op TenderNed. Het verslag zal een geabstraheerde weergave op hoofdlijnen bevatten van de verkregen informatie en inzichten in de diverse onderdelen van het project. In het verslag van de marktconsultatie zal de door IPO/BIJ12 verkregen informatie uitsluitend geanonimiseerd worden weergegeven. Concurrentiegevoelige of geheime bedrijfsinformatie wordt niet gepubliceerd. Aan het verslag zal uit oogpunt van transparantie de lijst met deelnemers aan de marktconsultatie worden toegevoegd.

2.6 Voorwaarden voor de marktconsultatie

Op deze marktconsultatie zijn de volgende voorwaarden van toepassing:

1. De marktconsultatie is voor alle betrokkenen vrijblijvend.
2. Deelname aan de marktconsultatie brengt partijen ten opzichte van elkaar op geen enkele wijze in een bevoordeelde of benadeelde positie bij aanbesteding.
3. Partijen kunnen geen rechten ontlenen aan de informatie die ten behoeve van de marktconsultatie is verstrekt.
4. Claims over het gebruik van informatie, vertrouwelijkheid, of verzoeken om vergoedingen in verband hiermee worden niet gehonoreerd.
5. Verstrekte informatie in het kader van de marktconsultatie kan afwijken van in de aanbestedingsprocedure te verstrekken informatie.
6. IPO/BIJ12 is niet gebonden aan de uitkomsten van de marktconsultatie.
7. Er wordt geen vergoeding of compensatie in welke vorm dan ook toegekend aan de deelnemers van deze marktconsultatie.
8. Dit marktconsultatiedocument is uitsluitend geschreven in het kader van deze marktconsultatie.
9. Dit document, deelname of bijdrage aan de marktconsultatie geldt niet als uitnodiging tot inschrijving op de (Europese)aanbesteding(en) voor het onderhavige project, noch kunnen daaraan rechten worden ontleend.
10. IPO/BIJ12 behoudt zich het recht voor de in dit document opgenomen planningen tussentijds te wijzigen.
11. Deze marktconsultatie zal worden gevoerd in uitsluitend de Nederlandse taal.

Door deelname aan deze marktconsultatie geven partijen te kennen onvoorwaardelijk akkoord te gaan met deze voorwaarden.

2.7 Contactgegevens marktconsultatie

IPO/BIJ12 begeleidt de marktconsultatie. Als contactpersoon treedt de heer Artjan Wouters (Inkoopadviseur) of diens vervanger op. Het is niet toegestaan om IPO/BIJ12 rechtstreeks te benaderen. Acquisitie naar aanleiding van deze marktconsultatie wordt niet op prijs gesteld.

2.8 TenderNed

Alle correspondentie verloopt via TenderNed. Dit betekent onder meer dat:

a) Alle documenten kosteloos en digitaal ter beschikking worden gesteld via TenderNed.
b) Het stellen van vragen vindt plaats via de berichtenmodule van TenderNed.
c) Het indienen van de uw antwoorden van de marktconsultatie uitsluitend digitaal kunnen worden ingediend via de berichtenmodule.
d) Ook alle verdere correspondentie in beginsel plaatsvindt via de berichtenmodule van TenderNed.

Om optimaal gebruik te kunnen maken van de functionaliteit van TenderNed is het voor Inschrijvers van belang dat de organisatie juist is geregistreerd en onder andere de juiste personen voor de onderhavige aanbesteding de juiste machtiging gegeven wordt. Registratie dient eenmalig te geschieden en is kosteloos.

NB. Alleen als een onderneming in TenderNed op de groene knop "*Houd mij op de hoogte van deze aanbesteding"* heeft gedrukt, ontvangt deze bepaalde automatische berichten die de onderneming bijvoorbeeld attenderen op het feit dat aanbestedingsdocumenten zijn toegevoegd door de Aanbestedende dienst. Het sec downloaden van de aanbestedingsdocumenten is hiervoor dus niet voldoende.

Via www.TenderNed.nl/voor-ondernemingen/ondersteuning zijn tal van kennisbronnen te raadplegen. Indien Ondernemers technische problemen ervaren of vragen hebben over de werking van TenderNed, dan dient contact opgenomen te worden met de servicedesk van TenderNed zelf en niet met de Aanbestedende dienst. De servicedesk is bereikbaar op werkdagen van 08.30 tot 17.00 uur via 0800-TenderNed (0800-8363376) of servicedesk@TenderNed.nl.

2.9 CPV-codes

Bij deze Marktconsultatie gaat het in eerste instantie om diensten en/of leveringen met de volgende CPV-codes:

- 72000000-5 – IT diensten: adviezen, softwareontwikkeling, internet en ondersteuning
- 72212730-9 – Diensten voor ontwikkeling van beveiligingssoftware
- 48000000-8 – Software en informatiesystemen

2.10 Uitnodiging voor review van eisen en wensen

Met deze vervolgmarktconsultatie nodigen wij marktpartijen uit om een inhoudelijke review te geven op de geformuleerde eisen en wensen. We vragen daarbij specifiek aandacht voor:

- Tegenstrijdige, dubbele, te stringente of overbodige eisen (bijlagen).
- Eisen die mogelijk leiden tot een no-bid (bijlagen).
- Het prijs- en financieringsmodel (Hdst. 3.6).
- De indeling van basis- en optionele diensten (Hdst.3).
- Het Programma van Eisen en het Programma van Wensen (bijlagen).
- Mogelijke verbeteringen of alternatieve adviezen.

Daarnaast waarderen we opmerkingen over extra aspecten die de haalbaarheid, flexibiliteit en toekomstbestendigheid van de dienstverlening kunnen beïnvloeden, zoals: schaalbaarheid, interoperabiliteit met bestaande systemen, innovatiemogelijkheden en risico's in de uitvoering.

Uw feedback helpt ons om de aanbesteding zo realistisch, duidelijk en marktconform mogelijk te maken, zodat de uiteindelijke dienstverlening goed aansluit bij de behoeften van de deelnemers.

3 Toelichting gevraagde SOC-dienstverlening

De deelnemende organisaties binnen deze opdracht kenmerken zich door een uiteenlopende mate van volwassenheid op het gebied van informatiebeveiliging. Deze verschillen manifesteren zich zowel in de inrichting en volwassenheid van monitorings- en alarmeringsdiensten als in de bredere governance, processen en maatregelen rondom informatiebeveiliging. De gevraagde SOC-dienstverlening dient flexibel en schaalbaar te zijn, zodat deze optimaal aansluit bij de specifieke behoeften en het volwassenheidsniveau van de individuele Deelnemers.

Binnen de provinciale bestuurslaag vervult het Nationaal Cyber Security Centrum (NCSC) de rol van sectoraal CSIRT. Dit betekent dat beveiligingsincidenten niet alleen aan de betreffende Deelnemer moeten worden gemeld, maar tevens aan het NCSC. De SOC-dienstverlening dient deze meldstructuur te ondersteunen en te borgen.

Het eigenaarschap van systemen, maatregelen en opvolging van incidenten blijft nadrukkelijk belegd bij de individuele Deelnemers. De SOC-dienstverlener heeft hierin een signalerende, analyserende en adviserende rol, maar treedt niet in de verantwoordelijkheid van de Deelnemer.

De aansluiting van de Deelnemer op de SOC-dienstverlening zal gefaseerd plaatsvinden. Deelnemers bepalen binnen de vastgestelde aansluitperiode zelf het moment van onboarding. Ter ondersteuning hiervan wordt een implementatiekalender opgesteld, waarin inzicht wordt gegeven in de fasering, planning en betrokken Deelnemers.

Tot slot dient de SOC-dienstverlening toekomstbestendig te zijn. Dit houdt in dat zowel uitbreiding, verdieping als verbreding van de dienstverlening structureel mogelijk moet zijn. Innovaties uit de markt, waaronder toepassingen van kunstmatige intelligentie, maken integraal onderdeel uit van de doorontwikkeling van de dienst.

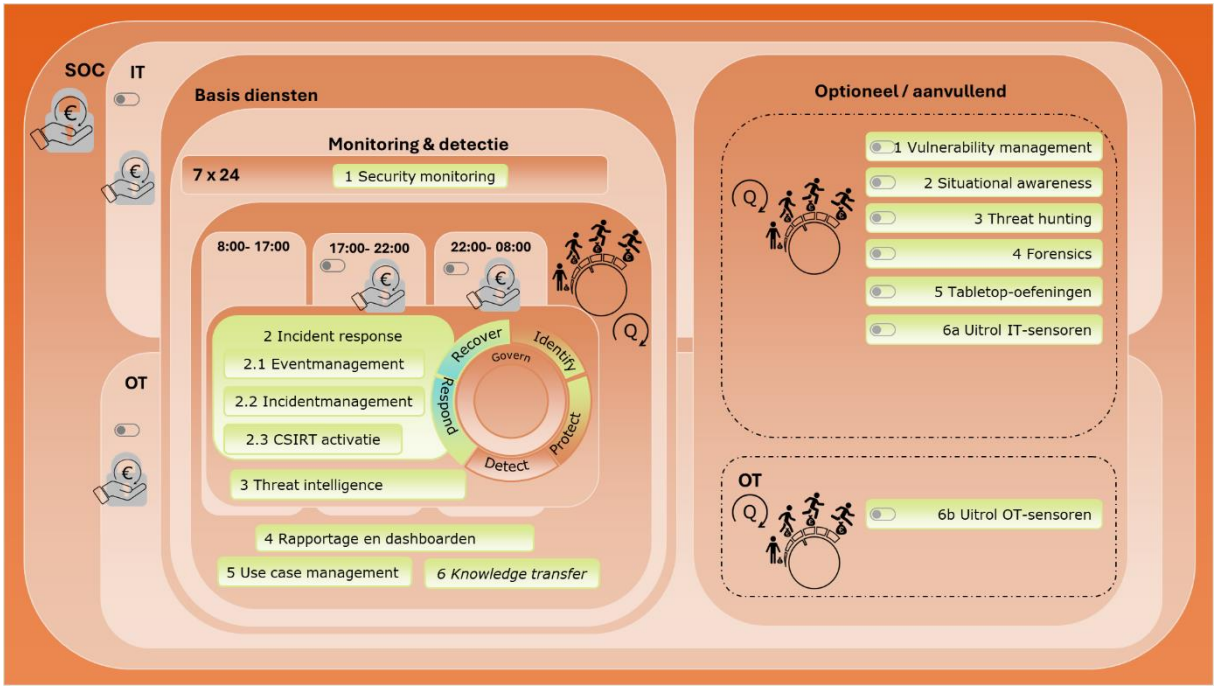
3.1 Centrale regie en samenwerking binnen de SOC-dienstverlening

Door gezamenlijk aan te besteden en uniforme SOC-dienstverlening af te nemen, ontstaan synergie- en efficiëntievoordelen, zoals kennisdeling, standaardisatie van architectuur, collectieve threat intelligence en gezamenlijke maturity-ontwikkeling. Tegelijkertijd brengt deze samenwerking deelnemeroverstijgende vraagstukken met zich mee, zoals coördinatie, contractbeheer en leveranciersmanagement, die actief moeten worden gemanaged en expliciet moeten worden geborgd in zowel de aanbesteding als de governance van de opdrachtgever en de Deelnemers.

Om deze voordelen te realiseren en de bijbehorende complexiteit beheerst te organiseren, wordt een centrale regiefunctie ingericht bij IPO/BIJ12. Deze regiefunctie coördineert, stuurt en bewaakt namens de gezamenlijke provincies de SOC-dienstverlening, met als doel de kwaliteit, samenhang en continuïteit te waarborgen, zonder zelf operationele taken uit te voeren. De functie combineert contract- en leveranciersmanagement met interprovinciale afstemming, waarbij zowel formele sturing (via 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.

3.2 SOC-diensten

De aan te besteden Raamovereenkomst biedt Deelnemers de mogelijkheid SOC-diensten af te nemen. De afname start altijd met de Basis SOC-diensten voor IT- en/of OT-omgevingen. Hiervoor sluit de Deelnemer een Nadere Overeenkomst met de Opdrachtnemer. Optionele SOC-diensten kunnen aanvullend worden afgenomen, maar maken geen deel uit van het verplichte basispakket.



Figuur 1. SOC-diensten

3.2.1 Basis SOC-diensten

De Basis SOC-diensten vormen het fundament voor detectie, analyse en opvolging van cyberdreigingen in IT- en OT-omgevingen. De dienstverlening biedt continu inzicht in beveiligingsrisico's, ondersteunt een snelle respons op beveiligingsincidenten en draagt bij aan bedrijfscontinuïteit en compliance. De basisdienst omvat de volgende kerncomponenten:

1. **Security Monitoring**
   - Real-time bewaking van IT- en OT-omgevingen via koppeling tussen de SIEM van de Opdrachtnemer en de Deelnemer.
   - Doorlopende detectie van afwijkingen en verdachte activiteiten.
   - Opvolging vindt plaats binnen Incident Response.
2. **Incident Response**
   - Analyse en behandeling van gedetecteerde events en Beveiligingsincidenten.
   - Inclusief eventmanagement, Incidentmanagement en CSIRT-activatie bij ernstige dreigingen.
   - Gericht op snelle mitigatie en herstel.
3. **Threat Intelligence**
   - Verrijking van detecties met actuele dreigingsinformatie.
   - Proactieve signalering van nieuwe aanvalstechnieken en trends.
4. **Rapportage en Dashboards**
   - Periodieke rapportages en interactieve dashboards met inzicht in status, trends en verbeterpunten.
   - Ondersteuning bij compliance en strategische besluitvorming.

5. **Use Case Management**
   - Ontwikkeling en onderhoud van detectiescenario's op basis van risico's en het actuele dreigingslandschap.
   - Continue optimalisatie om relevantie en effectiviteit te waarborgen.

6. **Knowledge Transfer**
   - Structurele kennisoverdracht aan de Deelnemer.
   - Gericht op het vergroten van interne expertise en samenwerking met het SOC.

3.2.2 Aanvullende diensten

De aanvullende SOC-diensten breiden de basisdienstverlening uit en versterken het proactieve detectievermogen, de situational awareness en de responscapaciteit van de Deelnemer. Deze optionele diensten richten zich op het identificeren en mitigeren van aanvullende risico's, het uitvoeren van diepgaande analyses en het vergroten van organisatiebrede paraatheid. De aanvullende dienstverlening bestaat uit de volgende componenten:

1. **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.

2. **Situational Awareness**
   - Real-time en near-real-time inzicht in dreigingen, incidenten en relevante trends.
   - Integratie van interne detectie, externe threat intelligence en contextinformatie voor een actueel totaalbeeld.
   - Ondersteuning bij besluitvorming en prioritering van maatregelen.

3. **Threat Hunting**
   - Proactief onderzoek naar verborgen aanvallen, geavanceerde dreigingen en afwijkend gedrag.
   - Hypothese-gedreven analyses en periodieke hunting-cycli, inclusief rapportages met bevindingen en aanbevelingen.
   - Integratie van resultaten in detectieplatformen en SOC-processen.

4. **Forensics**
   - Verzamelen, analyseren en veiligstellen van digitale bewijsmaterialen bij Beveiligingsincidenten.
   - Root-cause-analyse, chain-of-custody-documentatie en borging van dataintegriteit.
   - Ondersteuning bij forensisch-verantwoorde incidentanalyse en juridische compliance.

5. **Tabletop-oefeningen**
   - Gestructureerde simulaties en scenario-oefeningen ter beoordeling en verbetering van incidentresponsprocessen.
   - Toetsing van rollen, verantwoordelijkheden, procedures en communicatie.
   - Documentatie van bevindingen, verbeteracties en opvolging.

6. **Uitrol van sensoren en OT-sensoren**
   - Implementatie en configuratie van sensoren in IT- en OT-omgevingen voor betrouwbare datastromen.
   - Integratie met het SOC-detectieplatform en beheer van sensorconfiguraties.
   - Eigendom en overdraagbaarheid van sensoren worden geborgd conform de afspraken met de Deelnemer.

3.3 Implementatie

De implementatie van de SOC-dienstverlening verloopt gefaseerd per Deelnemer. De uitrol begint met een beperkte set use cases die volledig worden ingericht en gevalideerd voor dienstverlening tijdens kantoortijden. Vervolgens kan de dienstverlening stapsgewijs worden uitgebreid, zowel wat betreft servicetijden als het aantal te monitoren bronnen en use cases. De Deelnemer bepaalt in overleg met de Opdrachtnemer het tempo en de fasering, afgestemd op interne capaciteit en prioriteiten.

Stap 1: Ondertekening Nadere Overeenkomst

- Deelnemer sluit een Nadere Overeenkomst (NOK) met de Opdrachtnemer voor de afname van Basis SOC-diensten voor IT en/of OT.
- In deze overeenkomst worden afspraken vastgelegd over:
  - Omvang van de af te nemen diensten (IT/OT of beide)
  - Scope van initiële use cases
  - Openingstijden en servicelevel-afspraken (SLA/OLA)
  - Rapportages en dashboards
  - Communicatie- en escalatieprocedures
- *Doel:* Formeel kader creëren voor start SOC-dienstverlening en duidelijkheid over rechten, plichten en scope.

Stap 2: Initiële kick-off en intake

- Organiseer een gezamenlijke kick-off tussen Deelnemer en Opdrachtnemer.
- Inventariseer:
  - IT- en OT-assets die gemonitord moeten worden
  - Huidige infrastructuur, detectie- en loggingmogelijkheden
  - Interne processen en contactpersonen
  - Prioritaire use cases voor de initiële fase
- *Doel:* Uitgangssituatie en prioriteiten helder krijgen voor een succesvolle start.

Stap 3: Implementatie van Basis SOC-diensten

- Opdrachtnemer configureert monitoringplatformen, log-integraties, dashboards en alerts.
- Implementatie van een beperkte set initiële use cases in overleg met Deelnemer.
- Koppeling met ITSM/SOAR-processen en incidentmanagement wordt ingericht.
- Valideren van datastromen, eventnormalisatie en alertgeneratie.
- *Doel:* Basisdiensten operationeel maken en eerste detectiecapaciteit opbouwen.

Stap 4: Validatie en acceptatie

- Deelnemer en Opdrachtnemer voeren gezamenlijk tests uit op:
  - Logintegriteit en volledigheid
  - Correcte werking van use cases en detectieregels
  - Alertkwaliteit (false positives/negatives)
  - Dashboards, rapportages en escalatieprocedures
- *Doel:* Bevestigen dat de basis SOC-diensten voldoen aan afgesproken SLA's en kwaliteitsnormen.

Stap 5: Operationele start en monitoring

- Basis SOC-diensten gaan live (initieel vaak tijdens kantooruren).
- Opdrachtnemer voert 24/7 monitoring, eventmanagement en rapportage uit volgens SLA.
- Regelmatige evaluaties van use case-effectiviteit en detectiekwaliteit.
- *Doel:* Continu en betrouwbaar toezicht op IT/OT-assets.

Stap 6: Geleidelijke uitbreiding van diensten

- Deelnemer kan in overleg met Opdrachtnemer:
- Extra use cases implementeren
- Optionele SOC-diensten afnemen (Threat Hunting, Forensics, Tabletop, Situational Awareness, Vulnerability Management)

- Openingstijden en monitoringcapaciteit uitbreiden naar 24/7 indien gewenst
- *Doel:* SOC-dienstverlening opschalen op basis van organisatiecapaciteit en risicoprioriteiten.

Stap 7: Periodieke evaluatie en optimalisatie

- Periodieke evaluaties (bijv. kwartaalreviews) van:
  - Eventmanagement- en incidentresponseprocessen
  - Effectiviteit van detectieregels en use cases
  - Integratie met interne processen
  - Rapportages en lessons learned bespreken en verbeteracties implementeren.
- *Doel:* Continu verbeteren van SOC-diensten en aansluiten op veranderende dreigingsomgeving.

Stap 8: Rapportage en kennisoverdracht

- Opdrachtnemer levert periodiek rapportages over:
  - Alerts en incidenten
  - Use case performance
  - Eventkwaliteit en trends
  - Kennisoverdracht naar interne SOC- of IT-teams van Deelnemer waar nodig.
- *Doel:* Transparantie, naleving van compliance en versterking van interne capaciteit.

3.4 IT

Binnen de IT-omgeving is al veel functionaliteit beschikbaar om SOC-diensten te starten. De focus ligt op het inrichten van SOC-monitoring en het organiseren van opvolging van meldingen.

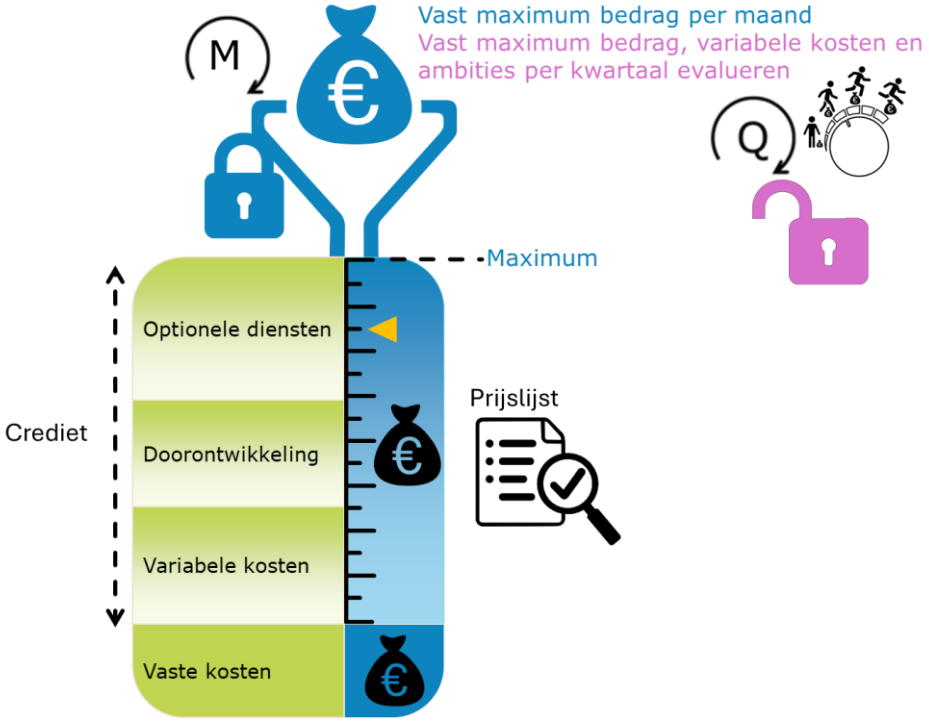
De implementatie van SOC-diensten binnen de IT-omgeving vindt gefaseerd en stapsgewijs plaats. Hierbij wordt ingeschat dat veelal gestart wordt met dienstverlening tijdens kantooruren, conform het eerder beschreven stappenplan, gericht op bijvoorbeeld eerst de basis SOC-diensten voor het netwerk van de Deelnemer te implementeren.

3.5 OT

Voor OT-omgevingen is het bewustzijn van monitoring nog beperkt. Momenteel zet vooral provincie Flevoland de eerste stappen op dit gebied. Monitoring van OT vereist de uitrol van specifieke sensoren.

De start van SOC-dienstverlening binnen OT gebeurt op basis van een beperkte set gelijksoortige OT-objecten. Het afnemen van aanvullende diensten wordt voor OT-omgevingen niet verwacht, met uitzondering van de implementatie van OT-sensoren.

3.6 Prijsstructuur



Figuur 2. Beoogde prijsstructuur

De beoogde prijsstructuur is opgebouwd uit vaste kosten, variabele kosten, doorontwikkelkosten en optionele diensten. Per kwartaal wordt per Deelnemer een maximaal totaalbedrag per maand vastgesteld, afgestemd op de verwachte variabele kosten, afspraken over doorontwikkeling en gewenste optionele diensten.

De afrekening vindt plaats op basis van daadwerkelijk geleverde diensten volgens een PxQ-model:

- P: de prijs zoals vastgelegd in de Prijslijst die via de Europese aanbesteding is overeengekomen.
- Q: de kwantiteit (Quantity), oftewel het aantal afgenomen diensten, bijvoorbeeld het aantal uren vermenigvuldigd met het tarief uit de prijslijst.

Deze opzet stelt de Deelnemer in staat het ambitieniveau van de SOC-dienstverlening te bepalen en tegelijkertijd beheersbare kosten te behouden. Voor de Opdrachtnemer zijn de kosten gedekt. Door variabele kosten, doorontwikkelkosten en optionele diensten als gezamenlijke kostenpost te behandelen, ontstaat bovendien een stimulans voor zowel de Deelnemer als de Opdrachtnemer om variabele kosten te beperken ten gunste van doorontwikkeling en uitbreiding van optionele diensten.