# Begeleidend document marktconsultatie

Inventarisatie van mogelijkheden inzake:

## Security Operations Center (SOC)

Interprovinciaal Overleg
van, voor en door provincies

BIJ12

Status : Definitief
Versie : 250514-1
Datum : 14-05-2025

# Inhoudsopgave

# 1 Inleiding

Deze marktconsultatie wordt gehouden voorafgaand aan een mogelijke aanbesteding, maar maakt daar geen deel van uit. De provincies en gelieerde organisatie hebben zich verenigd met als doel om gezamenlijk de SOC-dienstverlening aan te besteden. Hiervoor is een projectorganisatie opgezet welke verder wordt aangeduid als de "Aanbestedende dienst".

Een aantal provincies hebben reeds een aanbestedingsprocedure voor het inkopen van SOC-diensten doorlopen (Provincies Noord-Brabant, Gelderland, Noord-Holland en Zuid-Holland). De provincies die reeds SOC-diensten hebben ingekocht worden betrokken in dit traject om eventueel aanvullende SOC-dienst te kunnen inkopen, geleerde lessen mee te nemen en om eventuele verdere deelnemer overstijgende samenwerking vorm te geven.

**IPO en BIJ12**
Steeds meer taken die in het verleden door de rijksoverheid gedaan werden, worden nu gedecentraliseerd naar provincies en gemeenten, zoals natuurbeleid naar provincies. Voor de twaalf provincies betekent dit een uitbreiding van taken, vooral op het gebied van natuur en informatiesystemen. Om dat werk goed, en in veel gevallen ook samen, uit te voeren, ontstond vanuit de provincies de behoefte aan een aparte uitvoeringsorganisatie. Zo werd vanuit het Interprovinciaal Overleg (IPO), waar de samenwerkende provincies in zijn verenigd, BIJ12 opgericht. In het kader van de mogelijke aanbesteding zal IPO/BIJ12 optreden als de opdrachtgevende partij.

**Provincies**
De provincie staat als overheidsorgaan tussen de rijksoverheid en de lokale overheden als gemeenten in. Zij vormt een belangrijke schakel op een groot aantal terreinen. De verantwoordelijkheden van provincies kunnen kernachtig, als volgt worden samengevat:

- Regulerend en controlerend
  Gebiedsindeling en beheer, openbare orde en veiligheid, gemeenten, openbare voorzieningen, wegen, documenten etc.
- Beleidsvormend en initiërend
  Behoud en ontwikkeling van landschap, landbouw, economie, wegen, zorg, cultuur etc. Interactieve benadering, richtinggevend, acteur in vaak tegengestelde belangen. De provincie heeft de intentie op relevante terreinen een voorbeeldfunctie te vervullen.
- Betrouwbaar en dienstverlenend
  Van een provincie mag men verwachten dat men zorgvuldig met zaken omgaat. Zij heeft een "zorgplicht" in producten, procedures enz. (om deze redenen wordt er extra waarde gehecht aan kwaliteit van af te nemen middelen zodat aan deze zorgplicht zoveel als mogelijk voldaan kan worden.

Nadere informatie over de potentieel deelnemende provinciale organisaties, hun taken en werkzaamheden zijn te vinden op de volgende websites:

- www.bij12.nl
- www.brabant.nl
- www.flevoland.nl
- www.fryslan.frl
- www.gelderland.nl
- www.ipo.nl
- www.limburg.nl
- www.noord-holland.nl
- www.overijssel.nl
- www.provinciegroningen.nl
- www.provincie-utrecht.nl
- www.zeeland.nl
- www.zuid-holland.nl

## *1.1 Aanleiding marktconsultatie*

De provinciale bestuurslaag heeft op basis van de Network and Information Security (NIS2) Richtlijn en de nationale uitvoeringswet, de Cyberbeveiligingswet (Cbw), de wettelijke plicht tot het aansluiten bij een sectoraal Computer Security Incident Response Team (CSIRT) en het inrichten van monitoringsdiensten door een Security Operations Center (SOC).

Deze marktconsultatie wordt gehouden voorafgaand aan een mogelijke aanbesteding, maar maakt daar geen deel van uit. IPO/BIJ12 wenst te inventariseren welke mogelijkheden er in de markt voorhanden zijn op gebied van Security Operations Center (SOC) diensten.

De doelstelling van de mogelijke aanbesteding is het contracteren van één of meerdere partijen die Security Operations Center (SOC) diensten leveren voor een nadere te bepalen contractperiode.

Het doel van deze marktconsultatie is te onderzoeken of er partijen zijn die willen en kunnen meedoen met een dergelijke aanbesteding, welke informatie minimaal nodig is om een goede aanbieding te kunnen doen, wat de kosten zijn van SOC-diensten.

Alle ondernemingen worden hierbij van harte uitgenodigd om mee te denken. Aan deelneming of bijdragen in deze marktconsultatie kunnen geen rechten worden ontleend.

## *1.2 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 beschrijft het project waar het om draait.
- In hoofdstuk 4 zijn de vragen die de aanbestedende dienst wenst voor te leggen uitgewerkt.

## *1.3 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. |
| ADV | Aanbestedingswet op defensie- en veiligheidsgebied |
| AED | Aanbieders van Essentiële Diensten |
| CBW | Cyberbeveiligingswet |
| CIBO | Centraal Informatiebeveiliging Overleg |
| CISO | Chief Information Security Officer |
| CSIRT | Computer Security Incident Response Teams |
| CSIR | CyberSecurity ImplementatieRichtlijn |
| DSP | Digitale dienstverleners |
| ETL | Extract, Transform and Load |
| Findo | Financiën Decentrale Overheden (Data financiën Decentrale Overheden) |
| IPO | Interprovinciaal Overleg |
| IT | Informatie Technologie (ook wel kantoorautomatisering of KA genoemd) |
| KPI | Key Performance Indicator |
| NCSC | Nationaal Cyber Security Centrum |
| NIS2 | Network and Information Security (NIS2) richtlijn |

| | |
|---|---|
| OT | Operationele Technologie (ook wel procesautomatisering of PA genoemd) (verkeersregelings-installaties en bedieningssoftware voor bruggen, sluizen en gemalen e.d.) |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information and Event Management |
| SOC | Security Operations Center |
| UEBA | User and entity behavior analytics |
| VRI | VerkeersRegelInstallaties |
| Wbni | Wet beveiliging netwerk- en informatiesystemen |

# 2 Doel, opzet, planning en voorwaarden

## *2.1 Doel marktconsultatie*

Deze marktconsultatie wordt gehouden voorafgaand aan een mogelijke aanbesteding, maar maakt daar geen deel van uit. IPO/BIJ12 wenst te inventariseren welke mogelijkheden er in de markt voorhanden zijn op gebied van Security Operations Center (SOC) diensten,

De informatie die met deze marktconsultatie vergaard wordt, kan worden gebruikt bij de nadere besluitvorming inzake de aanbesteding.

Het doel van deze marktconsultatie is tweeledig, namelijk:

1. IPO/BIJ12 wil voorafgaande aan het aanbestedingstraject marktpartijen informeren over de behoefte van de provincies en gelieerde organisaties aan SOC-diensten.
2. Daarnaast wenst IPO/BIJ12 inzicht te krijgen in de kansen en potenties van het project en mogelijke optimalisaties in de scope en randvoorwaarden van het project die de interesse van marktpartijen in het project kunnen vergroten.

## *2.2 Opzet marktconsultatie*

De consultatie bestaat uit een schriftelijk deel en een mogelijk mondeling deel (consultatiegesprekken). Geïnteresseerde partijen kunnen zich aan de hand van dit document een beeld vormen.

IPO/BIJ12 heeft een aantal vragen geformuleerd. Deze vragen zijn opgenomen in hoofdstuk 4 van dit document.

## *2.3 Eventuele individuele consultatiegesprekken*

De Aanbestedende Dienst heeft de mogelijkheid om individuele gesprekken te voeren met Ondernemers.

De Aanbestedende Dienst maakt op basis van de gegeven antwoorden een afweging of zij toegevoegde waarde ziet in het voeren van individuele gesprekken. Wanneer de Aanbestedende Dienst daar de toegevoegde waarde van inziet, dan selecteert zij een aantal Ondernemers om hieraan deel te nemen. De Ondernemer kan het individuele gesprek zien als een toelichtend gesprek. Indien de Aanbestedende Dienst aanvullende vragen heeft naar aanleiding van de ontvangen reacties, dan komen deze aan de orde in het gesprek.

IPO/BIJ12 waardeert elke inspanning van geïnteresseerde partijen om aan een eventuele mondeling consultatiedeel deel te nemen, maar kan zich op voorhand niet verplichten om op individuele basis op elke reactie te reageren.

## *2.4 Doelgroep marktconsultatie*

Iedere belangstellende Ondernemer mag deelnemen aan deze Marktconsultatie. Met deze marktconsultatie richt IPO/BIJ12 zich direct tot marktpartijen die in de uitvoering van het project zijn geïnteresseerd.

## 2.5 Planning marktconsultatie

| Activiteit | Datum en tijd (CET) |
|---|---|
| Aankondiging marktconsultatie en beschikbaarstellingmarktconsultatiedocument op TenderNed | Woensdag 14 mei 2025 |
| Indienen antwoorden door partijen (via de berichtenmodule in TenderNed) | Woensdag 4 juni 2025 12:00 uur |
| Publicatie eindverslag marktconsultatie | Week 25- 26 |

## 2.6 Eindverslag marktconsultatie

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

## 2.7 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.

## 2.8 Contactgegevens marktconsultatie

IPO/BIJ12 begeleidt de marktconsultatie. Als contactpersoon treedt de heer Artjan Wouters (inkoper) (inkoop@bij12.nl) 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.

## *2.9 TenderNed*

Alle correspondentie verloopt via TenderNed o.v.v. marktconsultatie "Security Operations Center (SOC)". Dit betekent onder meer dat:

a) Alle documenten kosteloos en digitaal ter beschikking worden gesteld via TenderNed;
b) Het stellen van vragen plaatsvindt via de vraag & antwoordfunctie 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.

## *2.10 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

# 3 Waar zijn wij naar opzoek

In het kader de Europese Network and Information Security (NIS2) worden de provincies als essentiële entiteiten aangewezen. Dit levert een aantal verplichtingen op, zoals de zorgplicht en de meldplicht. Een verplichte maatregel is het beschikken over een sectoraal Computer Security Incident Response Team (CSIRT). In dit kader nam in 2023 het IPO-bestuur het principebesluit om de provinciale bestuurslaag aan te sluiten op het CSIRT van het Nationaal Cyber Security Centrum (NCSC). Dit principebesluit werd bekrachtigd in het IPO-bestuur op 14 december 2023, in aanwezigheid van de toenmalige Staatsecretaris voor Koninkrijksrelaties en Digitalisering.

Het aansluitingsproces bij het NCSC is in 2024 gestart In aanvulling op de dienstverlening van het NCSC zal de provinciale bestuurslaag maatregelen nemen om zowel de IT- als de OT-infrastructuur te monitoren. Hiervoor wordt middels een aanbestedingsprocedure SOC-dienstverlening ingericht.

## *3.1 De inkoopbehoefte*

### *3.1.1 SOC of the future: breed dienstenpakket*

Zowel een SOC als een CSIRT leveren operationele security-diensten voor een organisatie. De afbakening in de taken van een SOC en een CSIRT zijn vaak context gebonden en afhankelijk van de organisatie of omgeving waarin het SOC of de CSIRT opereert. In algemene zin zijn de diensten van een SOC gericht op monitoren en detectie en worden eenvoudige informatiebeveiligingsincidenten (IB-incidenten) direct afgehandeld. Meer complexe, grootschalige IB-incidenten worden dan overgedragen aan het CSIRT. SOC's en CSIRT raken meer geïntegreerd, waardoor het dienstenpakket meer verweven raakt. In afstemming met de CISO's van de provinciale bestuurslaag wordt voor de scope van de dienstverlening van het SOC uitgegaan van een dienstenpakket, waarbij sprake zal zijn van een groeimodel. Deelnemende organisaties hebben de keuze voor optionele diensten en voor het moment van deelname. De achterliggende reden voor latere deelname is dat een aantal provincies reeds SOC-diensten hebben ingekocht [1].

### *3.1.2 De scope van de diensten*

Provincies maken voor het uitvoeren van hun taken gebruik van informatietechnologie (IT) en van procesautomatisering, ook wel Operational Technology (OT). Voorbeelden van OT zijn verkeersregelinstallaties (VRI's), de automatisering voor de bediening van bruggen en sluizen en het gebruik van tunnels. De dienstverlening van het SOC dient gericht te zijn om beide gebieden te beschermen: IT en OT.

Het moderne IT-landschap is een mix van on-premise en cloud-based infrastructure, met een enorme keuze aan softwarepakketten. Het beoogde dienstenpakket richt zich op beide expertise gebieden en toepassingen. De afhankelijkheden en wisselwerking tussen beide gebieden en de (vaak) organisatorische en fysieke scheiding tussen beide toepassingen en de hierbij betrokken leveranciers is een complicerende factor in het project.

Daarnaast is het dienstenpakket breder dan de klassieke SOC-taken: het monitoren en detecteren. Het dienstenpakket is geënt op de ontwikkelingen van de SOC-dienstverlening en richt zich ook op vulnerability management door het alerteren op basis van relevante dreigingen en kwetsbaarheden, geclassificeerd, met handelingsperspectief. Ook valt information security incident management binnen de scope: de advisering, triage, coördinatie en afhandeling van informatiebeveiligingsincidenten.

[1] Het dienstenpakket is gebaseerd op de beschrijving van het dienstenpakket van FIRST. Zie https://www.first.org/standards/frameworks/csirts/FIRST-services-framework-team-types-v1.1.pdf Hiermee wordt ook aangesloten bij de beschrijving van de " SOC of the future" Blueprint for a Security Operations Center 2023 SOC of the future, TNO 2023 R11803. February 27th 2024.

Het SOC zal naast de provincies en IPO/BIJ12, ook samenwerken met de leveranciers die diensten en technologie leveren op het gebied van IT en OT, omdat de deelnemende organisaties services op het gebied van IT en OT hebben ingekocht bij externe leveranciers.

### *3.1.3 Het dienstenpakket*

Het gewenste provinciale dienstenpakket voor het SOC is in samenspraak met de CISO's van de provincies en IPO samengesteld. Het dienstenpakket bevat het hele spectrum van CSIRT-taken: diensten om incidenten te voorkomen, te detecteren en te herstellen. Dit dienstenpakket zal input zijn voor het programma van eisen. Het SOC zal in ieder geval diensten leveren op het gebied van:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability management
- Situational Awareness

Activiteiten op het gebied van Awareness Building, zoals awareness trainingen en het opstellen van white papers vallen buiten de scope van het gewenste dienstenpakket. Deze werkzaamheden en eventuele samenwerking wordt op andere platforms, zoals het CIBO (interprovinciale vakgroep van alle CISO's), besproken.

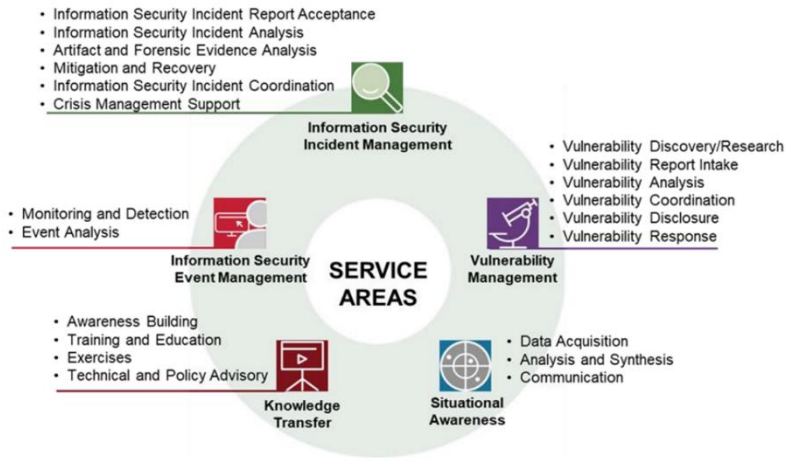


Figure 2: The five Service Areas and Their Associated Services of the CSIRT Services Framework v2.1 (source: (FIRST, 2019))

Een randvoorwaarde voor de implementatie zal zijn dat de diensten die het SOC zal leveren geprioriteerd en gefaseerd bij de provincies en IPO/BIJ12 geïmplementeerd worden. De prioritering ligt dan bij de klassieke SOC-diensten: monitoren en detectie (Information security event management) en incident response (Information security incident management).

### *3.1.4 Service windows sectoraal SOC*

Het sectoraal SOC zal de diensten 24/7 verlenen. Dit betekent dat het verwerken van geconstateerde kwetsbaarheden, dreigingen en incidenten, conform de classificatie, afgehandeld worden. Dit vraagt om passende afspraken met het SOC over classificatie, prioritering en mandaat. Een voorbeeld is het zogenaamde stekkermandaat, de bevoegdheid van het SOC om in bepaalde omstandigheden actief in te grijpen door het nemen van maatregelen. Deze werkwijze zal ook een impact hebben op de deelnemende organisaties en de afspraken met de betrokken leveranciers.


### *3.1.5 IT en OT landschappen*

Het IT-landschap van de provincies en gelieerde organisaties is een mix van on-premise en cloud-based infrastructuur, met een enorme keuze aan softwarepakketten. Tevens wordt er veel gebruik gemaakt van Microsoft (O365, E3/E5 licenties, Azure). In toenemende mate wordt gebruik gemaakt voor (bedrijfs)applicaties van SaaS-oplossingen. Het beoogde dienstenpakket richt zich op beide expertise gebieden en toepassingen (IT & OT). De afhankelijkheden en wisselwerking tussen beide gebieden en de (vaak) organisatorische scheiding tussen beide toepassingen en de hierbij betrokken leveranciers is een complicerende factor in het project.

# 4 Vragen marktconsultatie

De Aanbestedende dienst heeft verschillende vragen. De beantwoording hiervan vraagt de nodige tijdsinspanning van u, maar deze stellen we echter zeer op prijs. Als de marktconsultatie leidt tot een aanbesteding, verwachten we dat de aanbesteding beter aansluit op de markt.

Om de beoogde doelen van deze marktconsultatie te kunnen realiseren ontvangt de Aanbestedende dienst graag antwoord op de volgende vragen.

Wij verzoeken u om, na kennisneming van de aan u verstrekte stukken, oma op basis van dit document antwoord te geven op de gestelde vragen. Uw antwoorden op deze vragen kunnen, conform de planning weergegeven in par. 2.4 via de berichtenmodule in TenderNed indienen. In de berichtenmodule kunt u uw antwoorden in het Word bestand(dus niet in pdf) uploaden.

Uw opmerkingen en/of aanvullingen mogen van diverse aard zijn, en kunnen dus betrekking hebben op alle aspecten van de opdracht, zoals financiële, organisatorische, praktische, technische, juridische aspecten en planningsaspecten als doorlooptijd en volgordelijkheid.

*SOC-ondersteuning IT en OT*
De benodigde SOC-diensten zijn zowel voor het beschermen van de informatie-infrastructuur op het gebied van Operationele Technologie (OT, ook wel procesautomatisering of PA genoemd) als de Informatietechnologie (IT, ook wel kantoorautomatisering genoemd). Het projectteam heeft de indruk dat de op de markt beschikbare kennis en ervaring met het leveren van SOC-dienstverlening op gebied van Operationele technologie (OT) beperkt is.

1. Deelt u de inschatting van de aanbestedend dienst dat er nog weinig organisaties zijn die kennis en ervaring hebben met het leveren van SOC-dienstverlening op gebied van OT-oplossing? Graag uw antwoord motiveren/toelichten.
2. Welke kennis en ervaring heeft u als organisatie met het leveren van SOC-dienstverlening op gebied van OT?

*Operationele technologie (OT)*
Op gebied van het beveiliging van de operationele technologie (OT) zullen de provincies ook moeten investeren in het inrichten van monitoring van circa 1500 objecten zoals verkeersregelinstallatie, kleine bruggen, gemalen, sluizen et cetera. Dit kunnen objecten zijn van minimale of aanzienlijke omvang, in gebieden/locaties met minimale of volledige infrastructurele voorziening.

3. Welke adviezen kunt geven met betrekking tot het inrichten van SOC monitoring op gebied van de operationele technologie (OT)?

Het verzoek is om in uw antwoord in te gaan op de volgende aspecten:
   a. Welke doelmatige oplossingen adviseert u voor de diversiteit aan te monitoren objecten variërend van groot tot klein?
   b. Hoe houdt u rekening bij het selecteren van oplossingen indien het te monitoren object klein is en beschikt beperkte ruimte en of onder invloed staan van omgevingsinvloeden vocht temperatuur, pekel etc.) zoals verkeersregelinstallaties (VRI's) en kleine bruggen?
   c. Op welk niveau/laag adviseert u te monitoren?
   d. Implementatie en met name het voorkomen van verstoringen.
   e. Welke framework(s) adviseert u om toe te passen?
   f. Heeft u nog aanvullende adviezen met betrekking tot OT?
   g. Welke oplossing(en) adviseert u in het geval een vaste (internet) verbinding ontbreekt?

*Diversiteit deelnemers*
Een aantal provincies hebben reeds SOC-diensten verworven middels een aanbestedingsprocedure. Daarbij verschillende de provincies en gelieerde organisaties van elkaar, zowel organisatorisch, in volwassenheid en de gebruikte IT en OT oplossing.

4. Hoe kijkt u aan tegen het gezamenlijk aanbesteden van SOC-dienstverlening? Ziet u dat als een voordeel of een nadeel? Kunt u dat toelichten?
5. In hoeverre schat u in dat het integreren van verschillende ticketsystemen (Topdesk/ Jira/ Servicenow etc) dilemma's met zich meebrengen (zowel technisch als mede de verschillen in serviceprocessen tussen deelnemers)?

*Samenwerking derden*
De deelnemers hebben het beheer aan hun IT en OT-systemen uitbesteed aan verschillende marktpartijen (derden).

6. Hoe kijkt u aan tegen samenwerken met derden en welke adviezen kunt u ons meegeven?
7. Hoe kijkt u aan tegen het moeten werken met verschillende informatiesystemen op het gebied van security- en eventmanagement en monitoring (SIEM, MDR)?
8. Hoe kijkt u aan tegen het delen van data en voorziet u nog complicaties?

*Modulair dienstenpakket*
Een aantal provincies hebben reeds een aanbestedingsprocedure voor SOC-diensten doorlopen. Ook met deze provincies wordt gesproken over deelname aan dit aanbestedingstraject voor SOC-diensten. Mogelijk willen provincies gebruik maken van dienstverlening in aanvulling op de SOC-diensten die zij reeds ingekocht hebben. Dit zou betekenen dat het dienstenpakket modulair ingekocht worden, zoals een menukaart (cafetariamodel).

9. Hoe kijkt u aan tegen het modulaire opbouw van het diensten pakket en welke onderdelen zijn volgens u geschikt om optioneel aan te bieden aan de provincies die reeds over een SOC-dienstverlener beschikken?

*Onboaring*
Onder onboarding wordt verstaan de overgang van de bestaande situaties bij de verschillende deelnemers naar de SOC-dienstverlening van de te selecteren SOC-dienstverlener. De aanbestedende dienst wil graag inzicht hebben in hoe onboarding het best kan worden vormgegeven en wil graag inzicht aspecten zoals planning, tempo, volgorde, effecten van eventuele opdeling van de opdracht.

10. Welke adviezen kunt u gegeven om het onboardings-proces zo optimaal te laten verlopen?

*Gezamenlijk aanbesteden*
De Aanbestedende dienst is voornemens voor de provincies en gelieerde organisatie gezamenlijk aan te besteden omdat aangetoond is dat het gezamenlijk aanbesteden van ICT grote voordelen biedt. Door gezamenlijk aan te besteden wordt allereerst fors bespaard op de aanbestedingskosten. Daarnaast is gebleken dat door bundeling van inkoopvolume een aanzienlijk voordeel kan worden behaald door lagere inkoopprijzen en betere contractvoorwaarden. Bij de uitvoering ontstaan daarnaast efficiencyvoordelen omdat gezamenlijk aanbesteden leidt tot uniforme processen, efficiënter contractbeheer en efficiënter beheer.

11. Hoe kijkt u aan tegen het gezamenlijk aanbesteden van SOC-diensten? Ziet u dat als een voordeel of een nadeel? Kunt u dat toelichten?
12. Hoe kijkt u aan tegen het gezamenlijk aanbesteden van OT en IT versus afzonderlijk aanbesteden van OT en IT?

*Aanbesteding o.b.v. de Wet Aanschaffingen Defensie en Veiligheid (wet ADV).*
De ADV wet is bedoeld voor militaire en veiligheidsopdrachten. De ADV kan worden toegepast als er sprake is van gevoelig materiaal, diensten of werken, die bestemd zijn voor veiligheidsdoeleinden. De ADV is ook van toepassing op niet-militaire aanbestedingen, zolang deze vergelijkbare veiligheidsaspecten hebben. De aanbestedingen moeten een veiligheidsdoel hebben en op enige manier informatie bevatten die beschermd dient te worden ten behoeve van dat veiligheidsdoel. Ook decentrale overheden, speciale sector bedrijven of andere niet-Defensie gerelateerde aanbestedende diensten kunnen dus onder bepaalde voorwaarden gebruik maken van de ADV. Diverse OT objecten worden als vitale infrastructuur aangemerkt. Middels de ADV kan de

aanbestedende dienst één of meerdere geschikte marktpartijen uitsluitend te selecteren met het verzoek een offerte uit te brengen.

13. Hoe kijkt u aan tegen het verwerven van gevraagde dienstverlening op basis van de ADV wet?

*On-premise, cloud, SaaS*
De IT landschappen van de provincies zijn divers en bestaan uit on-premise, Cloud en SaaS oplossingen. Tevens wordt er veel gebruik gemaakt van Microsoft (O365, E3/E5 licenties, Azure). In toenemende mate wordt gebruik gemaakt voor (bedrijfs)applicaties van SaaS-oplossingen.

14. Hoe kijkt u aan tegen het om gaan met de verschillende oplossingen in het kader van de geschetste SOC-dienstverlening, monitoring en triage van meldingen en in het bijzonder in relatie tot SaaS-oplossingen?

*Marktontwikkelingen*
15. Wat is de toekomstvisie van uw organisatie op het gebied SOC-dienstverlening?

Het verzoek is om in uw antwoord minimaal in te gaan op de volgende punten:
a. Welke ontwikkelingen ziet u in de markt van SOC-dienstverlening met betrekking tot IT, OT, NIS2, CSIRT et cetera ?
b. Zijn er nog andere relevante ontwikkeling in de markt met betrekking tot SOC-dienstverlening die voor inkopende aanbestedende diensten relevant zijn?

*Artificial Intelligence (AI)*
Artificial Intelligence (AI) is een technologie die de laatste jaren steeds meer in opkomst is.

16. Ziet u nog relevante ontwikkelingen op gebied van inzet van AI in relatie tot de SOC-dienstverlening, bijvoorbeeld op gebied van machine learning, UEBA, etc?

*Door ontwikkelen SOC-dienstverlening*
Gezien de aard van de gevraagde dienstverlening is de noodzaak de dienstverlening door te ontwikkelen na het afsluiten van de overeenkomst evident.

17. Welke adviezen kunt u geven met betrekking tot het door ontwikkeling van de SOC dienstverlening?

Het verzoek is om in uw antwoord minimaal in te gaan de volgende aspecten:
a. Hoe de samenwerking op gebied doorontwikkeling van SOC-dienstverlening vorm te geven tussen opdrachtnemer, hoofopdrachtgever (contracteigenaar) en provincies en gelieerde organisaties.
b. Beschouwt u doorontwikkeling als integraal onderdeel van uw dienstverlening of adviseert u doorontwikkeling afzonderlijk te beprijzen?

*Kosten bepalende factoren*
Voor een redelijke , eerlijke en haalbare prijsstelling is het van belang inzicht te hebben wat de kostenbepalende factoren zijn voor SOC-dienstverlening. Onder kostenbepalende factoren verstaat de aanbestedende dienst bijvoorbeeld implementatiekosten, kosten per medewerker, KA-bron of OT-bron et cetera.

18. Welke kosten bepalende factoren onderkent u en hoe adviseert u deze te beprijzen?

Het verzoek is om in uw antwoord per door uw onderkende kostenfactor in te gaan op de volgende aspecten:
- Eenmalige, maandelijkse, jaarlijkse tarieven
- Opslag- en kortingspercentages
- Prijs per eenheid
- Toepassen van eventuele staffels

*Nederlands als voertaal*
In beginsel is de voertaal bij de Deelnemers zowel schriftelijk als mondeling de Nederlandse taal. De behoefte aan de Nederlandse taal spits zich met name toe op de mondelinge (telefonische) communicatie tussen deelnemer en opdrachtnemer waarbij één of meerder betrokkenen niet hun moedertaal spreken, terwijl op dat momenten heldere en snelle interactie (communicatie) vereist is (bv nachtelijke telefonische afstemming, over een incident op gebied van OT, vanaf een afgelegen locatie).

19. In hoeverre schat in dat het eisen van de Nederlandse taal als voertaal een beperking is voor de gevraagde dienstverlening en mogelijk marktpartijen weerhoudt om aan te bieden?

*Normeringen*
Op het gebied van informatiebeveiliging dienen de provincies en gelieerde organisaties zich te houden aan vastgestelde regels voor de overheid. De regels op het gebied van informatiebeveiliging die gelden voor de overheid zijn gebaseerd op de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 normen. Met betrekking de beoogde SOC-dienstverlening op het gebied van informatietechnologie (IT) en van procesautomatisering, ook wel Operational Technology (OT) zijn meerdere normen relevant.

De IEC 62443 is een set normen gericht op de Operationele Technologie (OT) en is een aanvulling op ISO 27001. Deze norm focust op de continuïteit en de digitale weerbaarheid van de 'Industrial Automation & Control Systems' (IACS).

20. Hoe gaat u om als organisatie rekening met normen zoals de IEC 62443 en CSIR en in het bijzonder voor Operationele Technology (OT)?

Het verzoek is om in uw antwoord minimaal in te gaan op de volgende aspecten:

a. Het omgaan met normeringen in relatie tot de diversiteit aan objecten zoals verkeersregelsystemen, kleine bruggen en sluizen en betrekking tot hun specifieke omgevingsinvloeden .

21. Welke relevante normeringen onderkent u op het gebied van SOC-dienstverlening en specifiek op het gebied van IT en OT?

*Kritieke Prestatie Indicatoren (KPI's)*
Om de wederzijdse verwachtingen te managen is het raadzaam kwantitatieve maatstaven af te spreken in de vorm van KPI's (Kritieke Prestatie Indicatoren).

22. Welke KPI's adviseert u met betrekking tot de gevraagde SOC-dienstverlening?

*Maatschappelijk Verantwoordelijk Opdrachtgeverschap en Inkopen (MVOI)*
De provincies en gelieerde organisatie willen met hun handelen economische, ecologische en sociale waarde toevoegen aan de maatschappij en aan de eigen organisatie. Dat begint bij goed opdrachtgeverschap en een professionele inkoop. De provincies en gelieerde organisatie zetten dan ook actief in op inkopen met impact op MVOI.

De MVOI maatschappelijke vraagstukken zijn onderverdeeld in zes MVOI-thema's; milieu (inclusief biodiversiteit), klimaat, circulair, internationale sociale voorwaarden (ketenverantwoordelijkheid), diversiteit en inclusie. Zie ook Praktijk & tools MVI | PIANOo - Expertisecentrum Aanbesteden.

23. Welke adviezen kunt u geven met het toepassen MVOI waarmee SOC-leveranciers zich kunnen onderscheiden tot de geschetste SOC-dienstverlening?

*Aanbevelingen*
24. Heeft u naast de door ons gestelde vragen nog aanbevelingen die u met ons wil delen?