Verslag marktconsultatie

Inventarisatie van mogelijkheden inzake:

Security Operations Center (SOC)

Interprovinciaal Overleg
van, voor en door provincies

BIJ12

Status : Definitief
Versie : 250828-1
Datum : 28-08-2025

Inleiding

Op woensdag 14 mei 2025 is door IPO/BIJ12 een marktconsultatie gestart om informatie op te halen vanuit de markt. Doel van de marktconsultatie is om voorafgaand aan een mogelijke aanbesteding te inventariseren welke mogelijkheden er in de markt voorhanden zijn op gebied van Security Operations Center (SOC) diensten,

De deelnemers aan de marktconsultatie konden schriftelijke reageren. Dertien deelnemers aan de marktconsultatie hebben een reactie ingediend. De kwaliteit van de reacties is zeer hoog. De aanbestedende dienst kan zien dat de deelnemers veel tijd hebben gestoken in het beantwoorden van de vragen. De aanbestedende dienst stelt de geleverde inspanning en de geleverde adviezen zeer op prijs en wil de deelnemers aan de marktconsultatie daarvoor hartelijk danken.

Dit verslag zal de basis vormen voor de verdere besluitvorming van de strategie met betrekking tot de aanbesteding Security Operations Center (SOC), tevens vindt IPO/BIJ12 het van groot belang om de uitkomsten van de marktconsultatie met de markt te delen (transparantiebeginsel), waarmee op deze wijze een gelijk speelveld in de markt wordt geborgd (gelijkheidsbeginsel).

Het verslag is uitgewerkt aan de hand van de vragen die in het kader van het marktconsultatiedocument zijn gesteld. Dit verslag geeft een totaalbeeld van de antwoorden die zijn gegeven.

De Aanbestedende dienst heeft de volgende vragen gesteld in het kader van de marktconsultatie (originele vraag binnen een kader):

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?

De meeste partijen onderschrijven dat er relatief weinig organisaties zijn met aantoonbare specifieke OT SOC kennis en ervaring. Enkele partijen geven aan dit ten dele te onderkennen.

Diverse organisaties hebben verschillende oplossingen en leverancier specifieke aanpakken ontwikkeld voor OT. Slechts een beperkt aantal organisaties heeft een bewezen trackrecord op gebied van het leveren OT SOC oplossingen en diensten.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- aantal beschikbare technologieën/oplossingen voor OT SOC-dienstverlening nemen toe;
- breed scala OT expertise nodig;
- duidelijk omschrijven wat onder OT wordt verstaan;
- expliciet benoemen welke OT componenten "gescand" dienen te worden;
- fysieke proceskennis;
- industriële protocollen toepassen voor OT;
- IT volgt OSI-model en OT volgt Purdue-model;
- kennis en ervaring op gebied van ICS, SCADA;
- multidisciplinaire aanpak en daardoor breed personeelsbestand nodig;
- netwerksegmentatie in OT-omgevingen;
- OT is een kleinere markt dan IT en daardoor is minder geïnvesteerd in OT security oplossingen;
- OT SOC diensten niet verwarren/beperken tot het enkel inzetten van een firewall;
- OT-oplossingen zijn gebouwd voor een specifiek functie, IT-oplossingen zijn gebouwd voor data. Daardoor moelijker samen te brengen en dat is een potentiële kwetsbaarheid;
- OT-systemen zijn niet ontwikkeld en gestandaardiseerd met de huidige cybersecurity vereisten voor ogen;
- OT-systemen zijn ontwikkeld met een specifieke OT-functionaliteit voor ogen. Verwachting is dat dit niet op korte termijn verandert;
- SOC leverancier moeten aanvullend tooling en processen ontwikkelen om de OT omgevingen adequaat te kunnen monitoren;
- veel maatwerk op gebied van OT nodig;
- OT systemen aangeschaft voor de lange termijn daardoor veel verouderde OT-oplossing.

Operationele technologie (OT)
Op gebied van de 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 u 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?

a) Doelmatige oplossing voor te monitoren objecten
Uit de reacties is op te maken dat er verschillende oplossingen beschikbaar zijn, zowel fysiek als virtueel en van verschillende merken.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- bij grote OT-objecten sensoren implementeren;
- onderscheid maken tussen grote en kleine objecten;
- OT en IT logisch scheiden;
- passieve netwerkmonitoring;
- segmentatie VLAN's en firewalls;
- SIEM en Asset Discovery Tools;
- onderzoeken wat al mogelijk is binnen bestaande oplossingen.

b) Voor monitoren klein object waar beschikbare ruimte beperkt is en of onder invloed staat van omgevingsinvloeden worden de volgende aandachtpunten meegegeven:
- (Industriële) normen eisen (IP6x, EN 50155, IEC 60068, IEC 60068-2);
- laag energieverbruik;
- "ruggedized" hardware;
- virtuele en fysiek sensoren.

c) Lagen monitoring
Op hoofdlijnen is het advies gegeven op meerdere/alle lagen te monitoren en met enkel accent verschillen te focussen op laag 3 (netwerkniveau) en besturingsniveau (1-2).

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- alle lagen monitoren waardevol;
- netwerk niveau verkeer meten;
- onderscheid maken tussen grote en kleine objecten;
- Perdue-model gebruiken;
- proces gebaseerde benadering.

e) Frameworks
Op gebied van frameworks is als aandachtpunt meegeven een risico-gebaseerde modulaire aanpak.

De volgende frameworks zijn op hoofdlijnen geselecteerd uit de reacties:
- IP65 (industrieel gecertificeerd) IP67 of hoger;
- ISA/IEC 62443;
- ISA-99 en MITRE ATT&CK for ICS;
- ISO/IEC 27019;
- NIST 800-82 (optioneel);
- OT: NIST Cybersecurity Framework (CSF);
- Purdue Enterprise Reference Architecture (PERA).

d) Implementatie en voorkomen verstoringen
De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- gefaseerd;
- implementatie plannen buiten bedrijfstijd of in overleg met beheerteams;
- passief eerst;
- port mirroring;
- SPAN- of TAP -poorten of logreplicatie;
- test vooraf met digitale twins of in offline simulaties;
- voer altijd een non-intrusive implementatie uit;
- voorkom write-access of active polling.

f) Adviezen
De volgende aandachtpunten op gebied van adviezen zijn op hoofdlijnen geselecteerd uit de reacties:
- de systemen evalueren;
- groeipad;
- samenwerking leveranciers/belanghebbenden;

- logisch startpunt noord-zuidverkeer monitoren. Vervolgfase oost-westverkeer;
- regelmatig audits, assessments;
- secure by design;
- testen en onderhoud;
- training.

g) Adviezen in het geval een vaste (internet) verbinding ontbreekt
De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- air-gapped synchronisatie;
- edge-computing;
- fysieke data extractie;
- gebruik maken van lokale WAS infra;
- LoRaWAN;
- mesh-netwerken;
- mobiele netwerken 4G/5G/LTE i.c.m. VPN;
- NB-IoT;
- satellietcommunicatie;
- store-and-foreward architectuur.

Diversiteit deelnemers
Een aantal provincies hebben reeds SOC-diensten verworven middels een aanbestedingsprocedure. Daarbij verschillen 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)?

4) Gezamenlijk aanbesteden wordt overwegend als positief gezien. Positief door de kansen op gebied van: schaalvoordelen, kostenefficiëntie, kennisdeling, standaardisatie, verhogen professionaliteit van de sector en versterking van collectieve digitale weerbaarheid.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- datasegregatie;
- eigenaarschap;
- flexibiliteit;
- governance;
- informatiebeveiliging;
- inspelen op verschillen;
- verantwoordelijkheden.

5) De respondenten beogen veelal de gangbare ticketsystemen te kunnen integreren/koppelen middels API-koppelingen.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- API beperkingen;
- beveiliging en toegangscontrole;
- eigenaarschap en verantwoordelijkheden;
- gegevenscompatibiliteit;
- onderhoud;
- procesinrichting/-standaardisatie;
- schaalbaarheid;
- verschillende workflows bij 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?

6) Mening en adviezen samenwerken met derden
Samenwerken van SOC-leveranciers met derden is voor iedereen de norm en de dagelijkse praktijk. Het samenwerken met derden biedt een kans de kennisdeling tussen alle betrokkenen te verbeteren en te vergroten.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- beveiliging en compliance;
- demarcatie verantwoordelijkheden;
- driehoek samenwerking;
- expliciet benoemen verantwoordelijkheden van SOC, deelnemers en derden;
- governance;
- heldere rollen;
- interoperabiliteit in te zetten middelen;
- regie;
- service orkestratie;
- standaardiseren processen;
- vertrouwen en transparantie;
- werkwijzen en kaders.

7) Verschillende informatiesystemen
De respondenten reageren positief op het werken met verschillende informatiesystemen. Het wordt bijvoorbeeld gezien als kans en uitdaging om verschillende SIEM/MDR systemen te integreren.

Het belangrijkst aandachtspunt voor succes dat wordt meegeven is standaardisatie.

8) Complicaties bij delen van data
Het delen van data wordt door de respondenten als essentieel gezien.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- beveiliging;
- compliance;
- datasoevereiniteit;
- duidelijke richtlijnen en protocollen;
- gefaseerde implementatie;
- privacy;
- standaardisatie;
- terughoudendheid in delen van data;
- vertrouwen.

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?

Verschillende partijen geven aan een modulair dienstenpakket te kunnen en willen leveren. Wel wordt er gewaarschuwd dat niet alle dienstverleningsonderdelen geschikt zijn om modulair aan te bieden. Tevens uit een enkele respondent een kritische noot om de dienstverlening zoveel mogelijk in één hand te houden. Het is raadzaam essentiële onderdelen die verband houden zoveel mogelijk bij één partij te beleggen.

Onboarding
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?

De respondenten hebben vele adviezen gegeven met als kernboodschap de onboarding te faseren.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- commitment opdrachtgever;
- samenwerking met service providers.

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?

De respondenten beoordelen het voornemen om gezamenlijk aan te besteden als positief.

De voordelen die worden onderkend zijn: schaalvoordelen, efficiënter, gebruik maken van de collectieve intelligentie, kennisdeling, standaardisatie, kans om de kwaliteit te verhogen.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- bij deelnemers nagaan wat de behoefte is en omvang;
- change management;
- compliance;
- datasegregatie tussen provincies;
- eigenaarschap;
- elke deelnemer eigen tenant dus afzonderlijk onboarden;
- flexibiliteit versus standaardisatie;
- maatwerk per provincie;
- ontwikkelen gezamenlijke best practices;
- risicomanagement;
- terughouden zijn m.b.t. focus op lagere kosten;
- transparantie,
- uitvoeringsnelheid;
- vendor lock-in.

12) Advies gezamenlijk aanbesteden
De respondenten adviseren IT en OT gezamenlijk aan te besteden bij één opdrachtnemer. De praktijk is dat bedreigingen niet laten ophouden bij de grens tussen IT en OT. Tevens is OT en IT nauw met elkaar verbonden. Door vraagbundeling kunnen dienstverleningen en oplossingen op gebied van (de combinatie van) IT en OT sneller worden doorontwikkeld.

De voordelen die worden onderkend zijn:

- betere onderhandelingspositie voor bundeling OT- en IT-monitoring;
- efficiënter;
- convergentie;
- geïntegreerd beeld;
- potentiële bevordering integratie van veiligheidssystemen PLC-leveranciers;
- kans voor meer uniformiteit/standaardisatie;
- synergievoordelen;
- uniforme rapportages;
- verminderde complexiteit/fragmentatie.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- domein specifieke expertise;
- governance;
- integratietesten;
- modulaire opzet;
- OT vereist gespecialiseerde oplossingen;
- overschatting voordelen;
- scheiding versus samenwerking van detectie- en analyse teams en processen voor OT en IT;
- technische OT verschillen leiden waarschijnlijk tot sub optimalisaties;
- vendor management;
- verschillen SLA en responseprocedures per domein;
- verschillende risicoprofielen en prioriteiten.

Aanbesteding o.b.v. de Aanbestedingswet op defensie- en veiligheidsgebied (ADV).
De ADV 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 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?

De respondenten van de marktconsultatie zien het belang in en maken geen bezwaar tegen het toepassen van de ADV voor SOC-diensten voor de provincies. Het advies is dat indien de ADV wordt toegepast, de aanbestedende dienst het toepassen van de ADV deugdelijk motiveert.

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?

Het is de praktijk dat alle partijen ervaring hebben met een gemêleerd IT-landschap en ervaring hebben met oplossingen/leveranciers zoals MS Azure, AWS, Google en SaaS/PaaS/IaaS-oplossingen.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- SOC flexibel en technologisch agnostisch;
- gestandaardiseerde API's.

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?

De volgende marktontwikkelingen zijn op hoofdlijnen geselecteerd uit de reacties:
- AI, machine learning;
- groeiend belang CSIRT-functionaliteiten;
- toenemende uniformering;
- toename cloud;
- meer integratie van IT en OT;
- ontwikkelingen op basis van vigerende wet- en regelgeving;
- toepassen van zero-trust principes.

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?

Respondenten koppelen terug hun inschatting is dat er geen partijen zijn die niet met AI bezig zijn. De ontwikkelingen op AI-gebied gaan snel. Er is een verschil tussen leveranciers in hoeverre ze AI toepassen.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- AI is krachtig maar niet feilloos;
- AI mogelijkheid om afwijkingen automatisch te signaleren;
- dreigingsdetectie;
- grote hoeveelheden data analyseren;
- incidentrespons automatiseren en versnellen;
- kwetsbaarheidsanalyse;
- machine learning m.b.t. gedragsanalyse;
- verwachtingen managen.

Doorontwikkelen SOC-dienstverlening
Gezien de aard van de gevraagde dienstverlening is de noodzaak de dienstverlening door te ontwikkelen na het sluiten van de overeenkomst evident.
17. Welke adviezen kunt u geven met betrekking tot het doorontwikkeling 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?

Cyberdreigingen evolueren voortdurend en daarom is cybersecurity een dynamisch vakgebied. Doorontwikkelen van de dienstverlening is een essentieel onderdeel van de SOC-dienstverlening. Het afzonderlijk beprijzen van doorontwikkeling zorgt voor meer transparantie en flexibiliteit - echter doorontwikkeling als een integraal onderdeel van de dienstverlening te beschouwen - biedt meer continuïteit.

De volgende aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:
- focus op doorontwikkeling;
- gebruikersraad, klankbordgroep;
- inrichten van gestructureerde en nauwe samenwerking;
- regelmatige afstemming;
- roadmap;
- vast contactpersoon voor het verbeteren van de dienstverlening.

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 kostenbepalende 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

De respondenten hebben diverse suggesties gedaan en de volgende aandachtspunten meegegeven: voorspelbare kostenstructuur, maatwerk waar nodig tegen vooraf afgestemde tarieven, retentie-eisen, geen verborgen kosten, schaalbaarheid.

De volgende prijsitems en aandachtpunten zijn op hoofdlijnen geselecteerd uit de reacties:

- aantal end-points/users;
- aantal IT-bronnen;
- aantal logbronnen;
- aantal OT-objecten;
- all-in dienstverlening;
- compliancy kosten;
- detectie en triage capaciteit;
- eenmalige kosten;
- forensisch onderzoek;
- implementatiekosten;
- indexering;
- industrial security;
- licentiekosten;
- maandelijks kosten;
- opslag- en kortingspercentages;
- opslag en retentie;
- optionele kosten;
- prijs per eenheid;
- rapportages/dashboards;
- servicekosten;
- staffels toepassen;
- threat detection
- threat intelligence integratie;
- verwerking- en service kosten;
- volume kortingen.

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 u 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?

SOC-dienstverleners opereren internationaal en dan is Engels de standaard voertaal. Verschillende respondenten geven aan wel in de directe contacten primair Nederlands als voertaal te ondersteunen. Documentatie is veelal in het Engels.

Incidentafhandeling vereist heldere communicatie, lokale kennis en contextuele interpretatie is essentieel. Er is een schaarste wat betreft Nederlandssprekende securityspecialisten. Nederlands eisen is wel van invloed op de marktwerking. Door volledig Nederlandse taal te eisen sluit men waarschijnlijk partijen uit die inhoudelijk uitstekend zijn gekwalificeerd.

Het volgende aandachtpunt is meegegeven:

- Mogelijk onderscheid maken met betrekking tot voertaal tussen - kantoortijden en buitenkantoortijden - eerstelijns en tweedelijnsondersteuning.

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?

Algemene lijn van de reacties is dat de respondenten voldoen aan de meest voorkomende relevante normeringen voor IT en niet altijd voor specifieke OT normeringen.

De volgende normeringen zijn op hoofdlijnen genoemd in de reacties:
- ABDO
- Baseline Informatiebeveiliging Overheid (BIO)
- CSIRT-richtlijn
- CSIT+RT/CSIR
- Cybersecurity implementatierichtlijn objecten RWS (CSIR)
- IEC 62443
- IP65 – 67 en hoger
- ISA-99/IEC 62443
- ISAE 3402 Financiële verslaglegging of ICM SOC1/2
- ISO 45001
- ISO 9001
- ISO 15408
- ISO/IEC 27019
- ISO14001
- MITRE ATT&CK for ICS
- NEN7510 (Informatiebeveiliging zorg)
- NEN-ISO/IEC 27001 en 27002:
- NEN-ISO/IEC 62443
- NIS2-richtlijn
- NIST 800-82
- NIST-CSF
- SOC CMMI
- SOC Type 2
- FIRST CSIRT Service Framework

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?

De respondenten hebben een grote diversiteit aan mogelijke KPI's voorgesteld zoals KPI's met betrekking tot:
- aantal gedetecteerde bedreigingen;
- asset coverage;
- beschikbaarheid;
- beschikbaarheid op locatie;
- betrouwbaarheid;
- coverage;
- detectietijden;
- escalatie;
- false positive ratio;
- incidentafhandeling;
- klanttevredenheid;
- kostenbeheersing;
- logdekking;
- MTTD;
- MTTR;
- oplostijden;
- preventie incidenten;
- rapportage tijdigheid, frequentie en kwaliteit;
- reactietijden;
- SLA compliance;
- tijdigheid rapportages en adviezen;
- updates;
- uptime;
- voertaal.

De volgende aandachtpunten zijn meegeven met betrekking tot KPI's:

- effectiviteit en samenwerking binnen het SOC;
- kern-KPI's die inzicht geven in snelheid;
- mandaat SOC-dienstverlener;
- snelheid incident melden versus de tijd nemen voor de analyse.

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?

Door de respondenten zijn diverse adviezen gegeven zoals op met betrekking tot de volgende onderwerpen:

- apparatuur met lange levensduur;
- circulair;
- CO2 voetprint verkleinen;
- diversiteit en inclusie;
- duurzaam;
- energiezuinigheid;
- internationale sociale voorwaarden;
- ISO14001;
- ketenverantwoordelijkheid;
- lokale samenwerking;
- milieu en klimaat;
- MVO-beleid opdrachtnemer;
- ROI;
- social return;
- stimuleren digitale veiligheid et cetera;
- stimuleren wetenschap met maatschappelijke impact;
- transparantie.

Aanbevelingen

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

De respondenten hebben een groot aantal constructieve aanbevelingen meegegeven. De volgende aanbevelingen of aandachtpunten zijn als steekwoorden geselecteerd uit de reacties:

- aanbestedingsprocedure;
- aandacht op aanvalsvectoren;
- banden van dienstverlener met vijandelijke en mogelijk vijandelijke statelijke actoren;
- benodigde informatie om een goede aanbieding te doen;
- contractduur;
- controle dienstverlener op technologieën derden;
- CSIRT-SOC integratie voor nationale coherentie;
- cultuur;
- demarcatie en triage;
- denken vanuit aanvalsperspectief;
- detectie en response in één hand;
- duidelijke KPI's;
- één SOC-dienstverlener;
- end-point steeds belangrijker;
- fasering;
- flexibiliteit en stabiliteit
- focus detectie verbreden naar detectie en response;
- forensisch onderzoek;
- functioneel uitvragen;
- holistische benadering;
- impact MDR-dienstverlener bij ingrijpende technologie veranderingen;
- kennis, ervaring, training en kennisuitwisseling;
- kijken naar identiteit;
- leveranciersonafhankelijkheid (open standaarden & voorkomen vendor lock-in);
- locatie dataopslag en herkomst software;
- mogelijk aanbieders die nog geen ervaring hebben met provincies;
- nadruk op samenwerken en governance;
- niet te technisch of gedetailleerd;
- oefenscenario's;
- partner first strategie;
- praktijkgerichte voorbereiding;
- regionale clustering;
- ruimte voor dialoog in concretiseringsfase;
- sectorale dreigingsanalyses;
- speciale aandacht voor OT-systemen;
- threat hunting op klantniveau;

- geen minicompetities;
- gefaseerde invoering;
- gespecialiseerde partners;
- threat intelligence;
- volwassenheidsmetingen deelnemers;
- weging prijs in aanbesteding.