TLP:GREEN

IMPLEMENTATIE EN ONBOARDING

Monitoring & Detectie – HAVIK

Handreiking versie 1.1

Complexiteit document
Gemiddeld

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht een veelheid aan loggegevens en andere (meta-) datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Monitoring- en detectiediensten kunnen binnen een organisatie worden ingericht in de vorm van een Security Operations Center (SOC). Het zelf inrichten van een SOC is, echter, niet voor elke organisatie opportuun. In dergelijke gevallen is het goed mogelijk om SOC-diensten bij externe, gespecialiseerde partijen, in te kopen.

Een belangrijk onderdeel van SOC-dienstverlening is de inrichting van de dienstverlening. Dit document is opgesteld om u op weg te helpen voor aanbestedingen van SOC-diensten. Dit document geeft diverse handvatten om de implementatie en onboarding van SOC-diensten in aanbestedingsstukken te beschrijven. Ook worden er overwegingen gegeven die u helpen om bepaalde keuzes te maken. Tot slot biedt het document diverse voorbeeldteksten die u kunt gebruiken als basis in een aanbesteding of minicompetitie.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set documenten om Rijksoverheidsorganisaties te ondersteunen bij het aanbesteden van SOC-diensten. In paragraaf 2.1 is een overzicht van deze documenten weergegeven.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor personen die werken aan het onder de aanbestedingswet inkopen van SOC-diensten. Primair is dit document bedoelde voor personen die de gunningsleidraad van een aanbesteding opstellen.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	18-12-2025	Initiële versie
V1.1	09-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
SOC Strategische Aanbevelingen	https://www.ncsc.nl/soc/het-vertrekpunt-voor-een-soc#:~:text=SOC%20Readiness%20Assistance
HAVIK Kennisdocumenten	VSSR kennisdocumenten voor het aanbesteden van monitoring- en detectiediensten
VSSR-kennisdocumenten	VSSR (https://www.ncsc.nl/vssr)

1.3 Definities

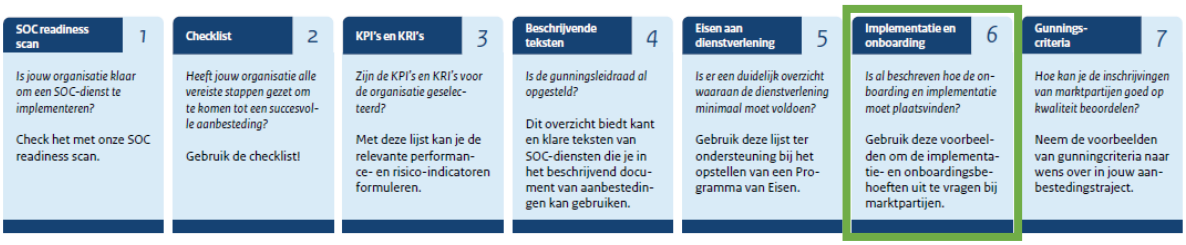
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er in Bijlage II - Afkortingen en definities" een overzicht van gebruikte afkortingen en definities opgenomen.

2 Inleiding

Organisaties van de Rijksoverheid die SOC-diensten bij een Managed Security Service Provider (MSSP) willen inkopen, stellen veelal vergelijkbare eisen aan dergelijke diensten. VSSR heeft een set hulpmiddelen ontwikkeld die ondersteuning bieden bij het inkopen van SOC-diensten. Deze hulpmiddelen zijn gebundeld in de "Handige Aanpak Voor Inkoop Kwalitatieve SOC-diensten", kortweg HAVIK-toolbox.

2.1 Context

Dit document, "*Implementatie en onboarding*", maakt onderdeel uit van de HAVIK-toolbox. Alle kennisproducten uit de HAVIK-toolbox zijn op het VSSR portaal[1] te vinden.



Figuur 1 - Positie van dit product in HAVIK-toolbox

Wij raden aan om voorafgaand aan het inkopen van SOC-diensten in elk geval de SOC-Readiness scan uit te voeren en de checklist door te nemen.

2.2 Doel van dit document

Voor succesvolle SOC-dienstverlening is het van belang dat de SOC-diensten goed aansluiten op de organisatie van opdrachtgever. Dit document is opgesteld met als doel handvatten te bieden die helpen om de inrichting van SOC-dienstverlening goed in aanbestedingen op te nemen.

Het inrichten (operationaliseren) van SOC-dienstverlening valt uiteen in twee onderdelen, te weten implementatie en onboarding. In dit document worden beide onderdelen beschreven.

2.3 Toepassing en reikwijdte

Dit kennisdocument richt zich op de ondersteuning bij het specificeren van de implementatie en onboarding van SOC-diensten.

Dit document kan gebruikt worden bij zowel het uitvoeren van een volledige aanbesteding als bij het inkopen onder bestaande mantelovereenkomsten. Dit document richt zich primair op het inkopen van SOC-Dienstverlening en is minder geschikt voor het inkopen van SOC-producten of vormen van hybride SOC-diensten.

In dit document wordt als uitgangspunt gehanteerd dat het geven van opvolging aan incidenten geen onderdeel uitmaakt van de SOC-dienstverlening. De overweging hierbij is dat opvolging vaak leidt tot wijzigingen in bestaande ICT-infrastructuur en dat hiervoor de staande beheerorganisatie verantwoordelijk is. Daarnaast is een dienstverlener die goed is in het leveren van monitoringdiensten, niet per definitie de meest geschikte dienstverlener voor beheer. Het staat een opdrachtgever uiteraard vrij om andere keuzes te maken. In dat geval zal opdrachtgever de te leveren incident response dienstverlening moeten beschrijven en toevoegen aan de aanbestedingsstukken

[1] HAVIK kennisdocumenten voor het aanbesteden van monitoring- en detectiediensten

3 Leeswijzer

Dit document is een hulpmiddel om de implementatie en onboarding van SOC-Dienstverlening in een aanbestedingsleidraad te specificeren.

Na deze leeswijzer treft u de volgende drie hoofdstukken:

4 - Inrichten dienstverlening

5 - Implementatie en onboarding in een aanbesteding

Bijlage I - Voorbeeldteksten

Bijlage II – Afkortingen en definities

In hoofdstuk 4 wordt beschreven wat er nodig is om SOC-dienstverlening in te richten en hoe dit de positioneren in een aanbestedingscontext. In dit hoofdstuk wordt ook beschreven wat onder implementatie wordt verstaan, wat onder onboarding en waarom het aanbrengen van dit onderscheid nuttig is.

Vervolgens wordt in hoofdstuk 5 nader ingegaan op de mogelijkheden, aandachtpunten en overwegingen om implementatie en onboarding in een aanbesteding voor SOC-diensten op te nemen. In dit hoofdstuk wordt ook inzicht gegeven in de informatie die een aanbestedende dienst moet verstrekken om het voor inschrijvers mogelijk te maken een succesvol voorstel voor implementatie en onboarding te doen.

Om vlot aan de slag te kunnen, worden in Bijlage I een aantal uitgewerkte en concrete voorbeeldteksten gegeven die als basis kunnen dienen in aanbestedingsstukken. Gebruikte afkortingen en definities zijn in bijlage II opgenomen. Vergeet niet om bij het gebruik van de tekstblokken uit bijlage I, ook de bijbehorende definities uit bijlage II over te nemen in uw aanbestedingsdocument.

4 Inrichten dienstverlening

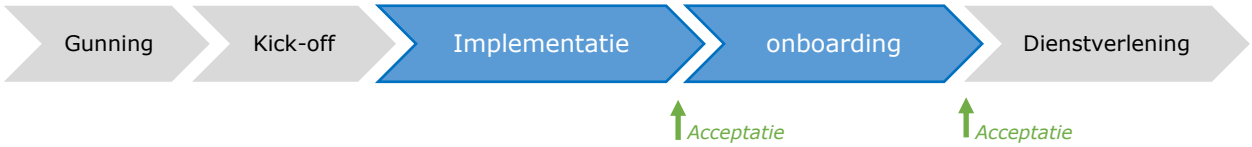
Binnen het inrichten van SOC-diensteverlening kan onderscheid gemaakt worden tussen:

- Implementatie
- Onboarding

Implementeren richt zich vooral op het inrichten van processen, (werk)afspraken en generieke technisch/functionele middelen om de diensten te kunnen leveren. Onboarden richt zich op het technisch aansluiten van de ICT-omgevingen en ICT-assets die bewaakt moeten worden. Verderop in dit document wordt hier dieper op ingegaan.

Reden om dit onderscheid te maken is dat implementatie een meer eenmalig karakter kent waarbij het zwaartepunt bij aanvang van de dienstverlening ligt. Voor onboarding is dat anders. Naast het initieel aansluiten van assets (onboarden) zullen er ook gedurende de looptijd van de overeenkomst nieuwe assets aangesloten worden (onboarding) en oude assets of anderszins niet langer gebruikte assets afgekoppeld moeten worden (offboarding). Daarnaast is het noodzakelijk dat de implementatie volledig is afgerond voordat diensten geleverd kunnen worden, terwijl het aansluiten van assets gefaseerd plaats kan vinden. Met name bij grotere omgevingen kan het wenselijk zijn om de assets gefaseerd in de monitoring op te nemen.

In de meest elementaire vorm ziet de inrichting er als volgt uit:

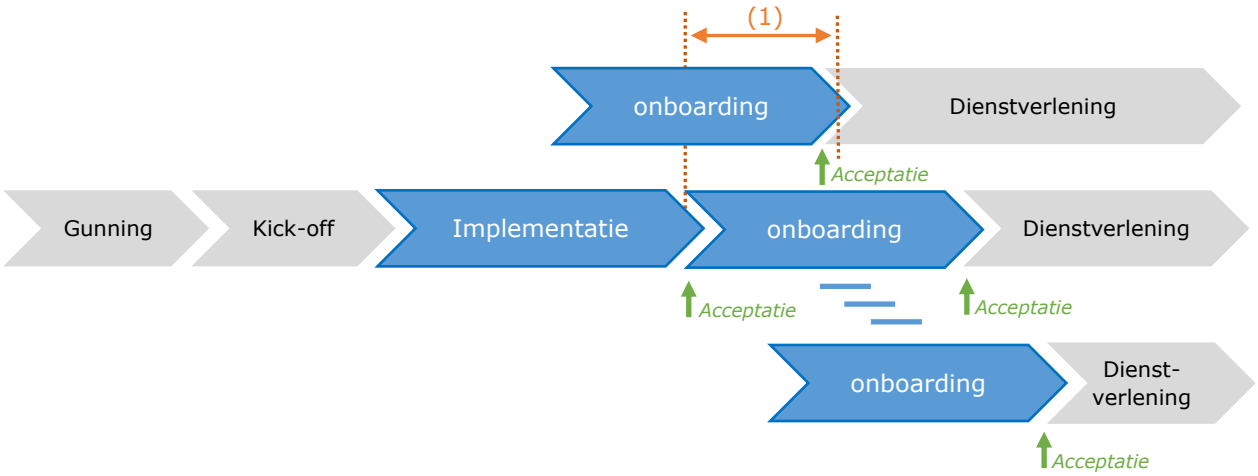


Figuur 2 - Model implementatieaanpak

In de meest elementaire vorm vindt de implementatie en onboarding achter elkaar plaats. Gebruikelijk is om na gunning van een aanbesteding eerst een kick-off overleg te houden. Het kick-off overleg is een eerste overleg na gunning waarin nadere afspraken gemaakt worden over de projectrealisatie. Na de kick-off start de implementatie van de dienstverlening en vervolgens de onboarding.

Het is aan te raden om zowel bij afronding van de implementatie als bij afronding van de onboarding een acceptatie uit te voeren. Hoewel de acceptatie zelf bij oplevering plaatsvindt, is het aan te bevelen om direct bij aanvang van het project een Protocol van Oplevering (PvO) op te stellen. Het PvO beschrijft de wijze van oplevering, criteria waaraan het opgeleverde moet voldoen en de wijze van testen. De afspraken uit de aanbesteding zijn de basis voor het PvO. Het PvO is vooral een nadere uitwerking van de wijze waarop acceptatie plaatsvindt. Door het PvO bij start op te stellen, wordt al voor realisatie en met voldoende detail duidelijk waaraan het eindproduct moet voldoen. Hiermee vermijdt men interpretatieverschillen die kunnen leiden tot herstel of meerwerk.

Grote organisaties, bijvoorbeeld organisaties met meerdere vestigingen, kunnen voor een aanpak kiezen waarbij onboarding en implementatie deels parallel worden uitgevoerd. Denk bijvoorbeeld aan situaties waar organisaties met meerdere locaties een aanpak hanteren waarbij deze locaties in deelprojecten worden aangesloten.



Figuur 3 - Model van meer complexe implementatieaanpak

De onboarding kan (deels) gelijktijdig met de implementatie worden uitgevoerd. Binnen de onboarding zijn de nodige voorbereidende werkzaamheden nodig die ook uitgevoerd kunnen worden als de implementatie nog niet is afgerond.

Wat ***niet*** kan, is de onboarding afronden als de implementatie nog niet is afgerond. Een afgeronde – en geaccepteerde - implementatie is immers een randvoorwaarde om de dienstverlening te starten. De oplevering van de eerste onboarding zal daarom altijd na het afronden van de implementatie liggen (1).

4.1 Implementatie

De implementatie draait om het bouwen van de fundamentele infrastructuur en het inrichten van de basisprocessen. De implementatiefase omvat een aantal voorbereidende werkzaamheden en alle werkzaamheden die nodig zijn om de diensten te kunnen leveren, met uitzondering van het technisch aansluiten van de te bewaken ICT-omgevingen en assets.

4.1.1 Voorbereidende activiteiten

Opdrachtgever dient in zijn aanbestedingsstukken duidelijkheid te geven over een aantal organisatorische uitgangspunten en kaders die essentieel zijn in de context van SOC-diensten. Dit is een niet te onderschatten inspanning die, voorafgaand aan een aanbesteding voor SOC-diensten, door opdrachtgever zelf gedaan moet worden.

Inschrijvers hebben dit inzicht nodig om een passende inschrijving te kunnen doen. Meer specifiek dient in elk geval over de volgende onderwerpen informatie in de aanbestedingsstukken te worden verstrekt:

- **Strategie & doelstellingen:**
  Opdrachtgever dient in een aanbesteding kenbaar te maken wat het SOC moet beschermen en kunnen (scope), de strategische doelstellingen[2] die een organisatie heeft en op welke wijze de organisatie invulling aan deze doelstellingen geeft. Deze informatie is voor inschrijvers relevant zodat het mogelijk is de aangeboden dienstverlening te laten aansluiten op de strategie en doelstellingen van Opdrachtgever.
- ***Governance & compliance:***
  Stel vast en maak in aanbestedingstukken kenbaar aan welk beleid, wet- en regelgeving de dienstverlening moet voldoen. Veelal zal dit een combinatie van specifiek organisatorisch beleid en generieke wet- en regelgeving zijn. Denk aan normenkaders als AVG, BIO, ISO 27001 of NIS2/Cbw. Voor zover dit geen openbare stukken zijn, moet deze informatie met

[2] De VSSR SOC-Readiness Quickscan is een hulpmiddel om o.a. strategische doelstellingen, in de context van een SOC, in kaart te brengen.

inschrijvers van een aanbesteding gedeeld worden. Neem in de acceptatieprocedure criteria op die hierop toetsen zodat er zeker gesteld kan worden dat de dienstverlening compliant is alvorens operationeel te gaan.

4.1.2 Implementatie-activiteiten

- **Architectuur & tooling:**
  Als onderdeel van de implementatie zorgt opdrachtnemer voor selectie en operationaliseren van de tools die nodig zijn om monitoring uit te voeren. Denk hierbij aan zaken zoals bijvoorbeeld:
  - SIEM
  - EDR/XDR
  - SOAR
  - Log management, ticketing, threat intelligence feeds, etc.
  - Ticketing systemen en/of koppelingen

  Indien het een dienstenopdracht betreft, blijft de invulling van dit onderdeel voor de opdrachtgever grotendeels een blackbox. Opdrachtnemer voert deze werkzaamheden, voor zover deze binnen het domein van opdrachtnemer liggen, zelfstandig en naar eigen inzicht uit. Opdrachtnemer is verantwoordelijk dat:
  1) de inrichting zodanig is dat aan alle verplichtingen uit de overeenkomst wordt voldaan en;
  2) dat de dienstverlening aansluit op de ICT-omgeving van opdrachtgever.

  Bij opdrachten waarbij SOC-diensten als dienstverlening worden ingekocht, is het belangrijk om deze verantwoordelijkheden nadrukkelijk bij opdrachtnemer te leggen. Dat wil zeggen dat je als opdrachtgever alleen aangeeft **"dat"** opdrachtnemer dit moet uitvoeren, maar dat u niet voorschrijft **"hoe"** opdrachtnemer hier invulling aan geeft. Het "hoe" beperkt zich hoogstens tot de beschrijving van de koppelvlakken van opdrachtgever waarop de SOC-dienstverlener moet aansluiten. Deze koppelvlakken zijn immers een gegeven.

- **Procesinrichting en procedures:**
  Een essentieel onderdeel van implementatie is het inrichten van de benodigde processen en procedures. Denk hierbij aan processen zoals het triageproces, meldproces*, [indien van toepassing*[3]: incident response-proces], escalatiepaden, playbooks, etc. Daarnaast worden er procedures opgesteld zoals een communicatiematrix, een inschalingsmatrix voor prioritering en het doen van meldingen met verschillende prioriteit.

  Naast de nieuwe processen, dienen bestaande beheerprocessen aangepast te worden op de SOC-dienstverlening. Bij toekomstige aanpassingen in de ICT-infrastructuur dient er rekening mee gehouden te worden dat de SOC-monitoring wordt meegenomen in zowel ontwerp, bouw, test als acceptatie. Organisaties die werken met een Change Advisory Board (CAB), doen er goed aan om deze controle onderdeel van de CAB-toets te maken. Wijzigingen kunnen leiden tot het opnemen van nieuwe ICT-assets in (onboarding), evenals het verwijderen van ICT-assets uit (offboarding) de SOC-dienstverlening.

  Verder moeten er procedures gemaakt worden die aansluiten op bestaande incidentprocessen. De SOC-dienstverlener moet immers een mogelijkheid hebben om incidenten, bijvoorbeeld het wegvallen van toegang tot logdata, te melden bij de verantwoordelijke beheersorganisatie. Ook moeten er afspraken gemaakt worden over tijdig herstel die in lijn zijn met de service levels

[3] Het is een keuze om incidentresponse al dan niet onderdeel te maken van SOC-dienstverlening. Veelal wordt incidentresponse bij de staande beheerorganisatie ondergebracht. Een SOC is niet altijd goed uitgerust voor operationeel incidentresponse.

voor de SOC-dienstverlening. Andersom moet de bestaande beheerorganisatie toegang krijgen tot de SOC-dienstverlener om storingen te melden die ontstaan door SOC-monitoring. Naast concreet incidentherstel is deze samenwerking ook vereist bij onderzoek naar incidenten waarvan de oorzaak nog niet duidelijk is.

Aansluiting op bestaande problem processen en capaciteitsbeheerprocessen zijn ook nodig. Dit omdat bij onderzoek vanuit het problem proces medewerking en inspanningen van opdrachtnemer nodig kunnen zijn. Capaciteitsbeheer is nodig zodat partijen wederzijds van elkaar op de hoogte zijn van veranderingen die substantiële impact op benodigde systeemcapaciteit kunnen hebben.

- **Samenwerking, personeel & rollen:**
  Opdrachtnemer zorgt voor de medewerkers die benodigd zijn om de dienstverlening zoals overeengekomen te leveren. Denk bijvoorbeeld aan werving en training van SOC-analisten, engineers, threat hunters en SOC-leads de verantwoordelijkheid voor de te leveren diensten.

  Ook bij het uitbesteden van SOC-diensten, blijven een aantal taken over het algemeen bij de opdrachtgever. Dit zijn vooral de onderdelen waar een organisatie verantwoordelijkheid moet afleggen aan derden. Denk aan het melden bij toezichthouders, informeren van bedrijven en burgers, informeren van de politiek en pers. Ook beslissingen met grote organisatorische impact zal een opdrachtgever zelf willen nemen, denk aan het al dan niet preventief uitschakelen van productiesystemen om verdere schade te voorkomen.

  Het aanbrengen van wijzigingen in de ICT-infrastructuur van opdrachtgever blijft de verantwoordelijkheid van opdrachtgever en eventuele door haar gecontracteerde toeleveranciers en/of dienstverleners. Een SOC kan wel ondersteunen met handelingsperspectief. Het opstellen van procedures om dergelijke ondersteuning te leveren maakt daarom ook onderdeel uit van de implementatie.

  Tijdens de implementatie wordt in detail vastgelegd wie wat doet en waar taken, verantwoordelijkheden en bevoegdheden zijn belegd. Ook wordt vastgelegd wie elkaars aanspreekpunten zijn en hoe escalatiestructuren ingericht zijn.

- **Use case development:**
  Use cases, ook wel detectieregels, zijn algoritmen die gebruikt worden om verdachte situaties in ICT-systemen te detecteren, denk aan brute-force login pogingen, data exfiltration, etc.. Het definiëren van use cases wordt gedaan op basis van risico's. Detectieregels zijn niet statisch en moeten continue onderhouden worden op basis omstandigheden die gedurende te tijd veranderen. Dit is specialistisch werk dat bij de SOC-dienstverlener wordt ondergebracht. Het beschikken over een proces voor onderhoud en beheer van use cases is onderdeel van de implementatie. Een nuttige toevoeging kan zijn dat de opdrachtgever het recht heeft om opdrachtnemer op te dragen specifieke situaties te bewaken. Opdrachtnemer ontwikkelt aan de hand van de gegeven situatie de use case en implementeert deze in de dienstverlening.

- **Communicatie:**
  Communicatie is essentieel voor de dienstverlening. In de aanbesteding moeten duidelijke kaders worden opgenomen over de gewenste rolverdeling zodat opdrachtnemer de implementatie hierop kan laten aansluiten. Houdt hierbij rekening dat de communicatie gedurende normale (rustige) periodes wezenlijk anders kan zijn dan gedurende (ernstige) incidenten. Bij ernstige incidenten kunnen er gevolgen voor burgers en bedrijven zijn, moeten bestuurders, toezichthouders en pers geïnformeerd worden. Overweeg om al tijdens het schrijven van een aanbesteding op dit onderwerp de communicatieafdeling te betrekken. Het inrichten van de communicatie afspraken en procedures is onderdeel van de implementatie en het is raadzaam om dit in het protocol van oplevering op te nemen.

- **Rapportage:**
  Rapportages zijn een belangrijk onderdeel om de SOC-dienstverlening te bewaken en zo nodig te optimaliseren. Rapportages geven op een gestructureerde wijze en met een passend detailniveau inzicht in zowel de prestaties van de dienstverlening alsmede inzicht in (potentiële) issues en risico's op het gebied van cyberweerbaarheid van de onderhavige ICT-assets.

  De rapportages omvatten niet alleen de door de opdrachtnemer geleverde dienstverlening, maar ook factoren die de informatiebeveiliging negatief beïnvloeden, zelfs als de opdrachtnemer hiervoor niet verantwoordelijk is. Denk bijvoorbeeld aan meldingen van het SOC over kwetsbaarheden die opgelost moeten worden. Hoewel het niet de verantwoordelijkheid van de SOC-dienstverlener is om deze kwetsbaarheden daadwerkelijk te verhelpen, wil de opdrachtgever wel inzicht in de mate waarin deze meldingen worden opgevolgd. De rapportages geven hiermee niet alleen inzicht in de kwaliteit van de SOC-dienstverlening, maar ook in de mate waarop de organisatie adequaat omgaat met meldingen en gesignaleerde risico's.

  Rapportages bevatten een weergave van de maand waarop de rapportage betrekking heeft en geeft een historisch inzicht over de twaalf voorliggende maanden (totaal 13 maanden). Dit maakt het mogelijk om trendanalyses te doen en jaar-op-jaar vergelijkingen.

  Het opzetten van dit rapportagesysteem is onderdeel van de implementatie en houdt in dat, binnen de kaders van de overeenkomst, processen en procedures worden ingericht en dat detailafspraken worden vastgelegd zodat er periodiek gerapporteerd wordt.

- **Playbooks:**
  Playbooks zijn stappenplannen waarin vastligt hoe SOC-analisten moeten reageren op specifieke beveiligingsincidenten of dreigingen. Doel van deze playbooks is om sneller te handelen, fouten te beperken en consistentie te waarborgen in het meldproces richting de verantwoordelijke voor incident response. In beginsel bepaalt opdrachtnemer zelf voor welke scenario's playbooks nodig zijn en zorgt dat voor deze scenario's playbooks zijn opgesteld. Indien opdrachtgever aanleiding ziet om voor bepaalde scenario's een playbook op te stellen, dan mag opdrachtgever hiervoor een verzoek bij opdrachtnemer indienen. Opdrachtnemer zal hieraan uitvoering geven, mits het verzoek uitvoerbaar, redelijk en billijk is. Behalve het opzetten van deze playbooks, is het raadzaam om deze te testen met echte gegevens.

  Belangrijk is dat Opdrachtgever zich realiseert dat de playbooks zoals hier bedoeld de scenario's voor het SOC beschrijven. Denk aan scenario's over melden, adviezen over eventueel isoleren, mitigerende maatregelen, etc. Het daadwerkelijk uitvoeren van wijzigingen in ICT-systemen blijft een verantwoordelijkheid voor Opdrachtgever en de door deze aangestelde of gecontracteerde beheerorganisaties. Deze playbooks geven geen invulling aan de gehele keten van incidentresponse.

4.2 Onboarding

De onboarding richt zich op het aansluiten van ICT-omgevingen en ICT-assets die door de opdrachtnemer bewaakt moeten worden. Onboarding bevat op hoofdlijnen de volgende onderdelen:

- **Inrichten connectiviteit:**

  Het realiseren van de dataverbindingen die nodig zijn om opdrachtnemer toegang te verschaffen tot de te bewaken ICT-assets**.** Het gaat om de volledige keten tussen de monitoringsystemen van opdrachtnemer en de te bewaken assets van opdrachtgever. Connectiviteit omvat het interne netwerk (LAN) alsmede de verbindingen naar buiten (WAN).

- **Aansluiten van assets:**

  Het daadwerkelijk aansluiten van de assets op de monitoringsystemen. Veelal omvat dit het installeren van clients en/of het aanpassen van configuraties zodat de betreffende asset zijn logdata beschikbaar stelt voor monitoring. Belangrijk is ook dat bestaande procedures voor beheer en life cycle management van de assets, en (netwerk)infrastructuur, zodanig worden aangepast dat de monitoringvoorziening ook blijft werken na aanpassingen en updates van assets en/of (netwerk)infrastructuur.

- **Log onboarding:**

  Zodra de connectiviteit gereed is en de assets hun logdata beschikbaar stellen, is integratie van logbronnen (firewalls, endpoints, servers, AD, cloudplatforms) nodig. Deze activiteit voorziet dat de logdata die van de assets afkomstig is, ook correct door de monitoringsystemen worden ingelezen.

  Een belangrijk aspect van de log onboarding is ervoor zorgdragen dat de logdata efficiënt en effectief wordt getransporteerd en verwerkt. Het is noodzaak om te voorkomen dat logdata onnodig naar monitoringsystemen wordt gestuurd. Enerzijds omdat het verwerken van overbodige logdata tot onnodige belasting van systeemcomponenten leidt, anderzijds om te voldoen aan wet en regelgeving. Bepaalde logdata, bijvoorbeeld persoonsgegevens, is onderhevig aan wet en regelgeving. Tijdens de log onboarding dienen maatregelen genomen te worden dat de verwerking van loginformatie binnen de geldende kaders, wet- en regelgeving plaatsvindt.

- **Baseline:**

  Nadat de technische koppeling met de ICT-assets is gerealiseerd en de relevante logdata binnenkomt, moet het 'normale' beeld van de omgeving worden vastgesteld. Zonder dit referentiepunt is het onmogelijk om afwijkingen betrouwbaar te signaleren.

  Het vaststellen van dit normale gedragspatroon wordt het opstellen van een baseline genoemd. Dit gebeurt door de verzamelde logdata over een representatieve periode te analyseren. Typische patronen die hierbij naar voren komen zijn bijvoorbeeld:

  - het gemiddelde aantal authenticatiepogingen per uur
  - de gebruikelijke inlogtijden en -locaties van gebruikers
  - het normale dataverkeer buiten kantoortijden
  - veelvoorkomende processen en commando's

  Met een goed gedefinieerde baseline kunnen detectieregels zodanig worden ingesteld dat zij een alert genereren wanneer het gedrag significant afwijkt van dit patroon.

- **Tuning:**

  Tuning is het vervolgproces dat ervoor zorgt dat de detectie zowel effectief als efficiënt blijft. Doel van tuning is om alleen de juiste dingen te zien en zo min mogelijk ruis of privacygevoelige gegevens te verwerken. Tuning omvat onder andere:

  - Het finetunen van de drempelwaarden en voorwaarden van detectieregels om onnodige meldingen (false positives) te verminderen.
  - Het bewust beperken van de hoeveelheid en het type logdata die wordt verzameld en verwerkt, zodat alleen de voor monitoring noodzakelijke informatie wordt ingelezen (data minimalisation / privacy by design).

Tuning is iets dat als onderdeel van onboarding uitgevoerd moet worden, maar heeft ook onderhoud nodig. Ook nadat onboarding heeft plaatsgevonden is het belangrijk om periodiek baseline en regels te herijken. Hiermee anticipeert de monitoring op veranderingen van de omgeving, bijvoorbeeld door nieuwe systemen, gewijzigde werkpatronen, seizoensinvloeden, etc.

5 Implementatie en onboarding in een aanbesteding

In het vorige hoofdstuk zijn de belangrijkste onderdelen voor implementatie en onboarding beschreven. In dit hoofdstuk wordt nader ingegaan op de mogelijkheden, aandachtpunten en overwegingen om implementatie en onboarding in een aanbesteding voor SOC-diensten op te nemen.

Dit hoofdstuk geeft ook inzicht in de informatie die Opdrachtgever als onderdeel van de aanbestedingsdocumenten moet verstrekken om het voor inschrijvers mogelijk te maken een succesvol voorstel voor implantatie en onboarding te doen.

5.1 Eis of (sub)gunningscriterium

Als eerste zal een keuze moeten worden gemaakt of de implementatie en onboarding als eis wordt opgenomen of als (sub)gunningscriterium. Het belangrijkste verschil is dat een eis een voorschrijvend karakter heeft: een aanbieder voldoet wel of niet aan de eis. Er is geen sprake van gradaties.
Een subgunningscriterium daarentegen is een onderdeel waaraan het beoordelingsteam een waarde kan toekennen. Hiermee is het mogelijk om kwaliteitsverschillen tussen inschrijvers mee te nemen in de beoordeling.

5.1.1 Afwegingen Implementatie en onboarding als eis

In deze paragraaf gaan we in op de voor- en nadelen van het **als eis** opnemen van de implementatie en onboarding in een aanbesteding.

Wanneer implementatie en onboarding als eis worden opgenomen, betreft dit een zogenoemd knock-out criterium. Dit betekent dat een aanbieder volledig aan alle onderdelen van de eis moet voldoen om voor gunning in aanmerking te komen.

Door het binaire karakter van een eis, mag aanbestedingsrechtelijk de opdrachtgever uitsluitend beoordelen of aan de eis is voldaan. Er is geen ruimte om kwalitatieve verschillen te waarderen. Een inschrijver met een uitgebreider of beter antwoord wordt daarmee gelijk beoordeeld aan een inschrijver die precies het minimum levert, zolang beide aan de eis voldoen. In de praktijk zullen inschrijvers daarom doorgaans niet meer aanbieden dan het minimaal gevraagde.

Voor- en nadelen van het opnemen van implementatie en onboarding als eis in een aanbesteding zijn als volgt:

Voordelen:

- Inschrijvers ontvangen een duidelijke omschrijving wat er geleverd moet worden;
- Uniformiteit: Meer aanbieden dan gevraagd levert geen voordeel op en zal zelfs negatief uitpakken als dit prijsopdrijvend is. Dit leidt tot meer gelijksoortige inschrijvingen en daarmee tot meer uniformiteit;
- Eenvoudig te beoordelen, geen subjectieve elementen in beoordeling;
- Meer zekerheid over naleving.

Nadelen:

- Inschrijvers hoeven alleen aan te tonen dat ze aan de eis voldoen, niet hoe goed ze het doen;

- Geen concurrentie op kwaliteit: Het heeft voor inschrijvers geen zin zich te onderscheiden met hogere kwaliteit of extra's;
- De aanbestedende dienst heeft veel inhoudelijke kennis van SOC-diensten nodig omdat implementatie- en onboarding in detail moet worden voorgeschreven;
- Minder ruimte voor innovatie of maatwerk: Het heeft voor inschrijvers geen zin om zich te onderscheiden met betere passende oplossingen;
- Risico's op uitsluiting: Inschrijvers met een inhoudelijk sterk plan dat op één klein detail niet aan de eis voldoet, moeten worden uitgesloten;
- Te strenge eisen kunnen een belemmering zijn voor marktpartijen om aan de aanbesteding deel te nemen;
- (Te) strenge eisen hebben een (onnodig) prijsopdrijvend effect. Vaak is het voor aanbestedende diensten lastig om de financiële gevolgen van eisen te overzien;
- Meer risico op meerwerk achteraf: Alle aspecten die niet in de eis zijn opgenomen en later alsnog toegevoegd moeten worden, is in beginsel meerwerk.

5.1.2 Afwegingen implementatie en onboarding als (sub)gunningscriterium

In deze paragraaf gaan we in op de voor- en nadelen van het als subgunningscirterium, ook wel 'wens' genoemd, opnemen van de implementatie en onboarding in een aanbesteding.

Wanneer implementatie en onboarding als subgunningscriterium worden opgenomen, ontstaat ruimte om voorstellen op kwalitatieve aspecten te beoordelen. In tegenstelling tot een eis kan het beoordelingsteam hierbij verschillen in kwaliteit waarderen. Een inschrijver met een beter uitgewerkt of ambitieuzer voorstel kan hierdoor een hogere score behalen dan een inschrijver met een minder sterk voorstel.

In de praktijk wordt een subgunningscriterium veelal gecombineerd met één of meerdere eisen. De eis borgt een minimaal kwaliteitsniveau waaraan alle inschrijvers moeten voldoen. Binnen deze kaders kunnen inschrijvers zich vervolgens onderscheiden door meerwaarde te bieden boven het gestelde minimum.

Een voorbeeld hiervan is een eis dat de implementatie uiterlijk binnen drie maanden na gunning moet zijn afgerond. Binnen een subgunningscriterium kan vervolgens een kortere implementatiedoorlooptijd worden aangeboden en beoordeeld. Aan deze verkorte doorlooptijd kan een hogere waardering worden toegekend. Op deze wijze wordt onderscheid tussen inschrijvers mogelijk gemaakt, terwijl tegelijkertijd een minimaal kwaliteitsniveau is gewaarborgd.

Voordelen

- Je kunt inschrijvers laten concurreren op *hoe goed* ze iets doen, niet alleen *of* ze het doen;
- Leveranciers krijgen ruimte om creatieve of geavanceerde oplossingen aan te dragen;
- Je kunt kwaliteit belonen in de gunningssystematiek waardoor beoordeling niet alleen op laagste prijs is, maar ook kwalitatieve aspecten worden meegewogen;
- Kleine afwijkingen leiden niet automatisch tot uitsluiting, zolang de meerwaarde overtuigt;
- Sturing op optimale prijs/kwaliteitsverhouding. Inschrijvers zullen een zorgvuldige afweging maken tussen de extra kwaliteit die geboden wordt en de financiële consequenties daarvan;
- Opdrachtgever heeft minder kennis van de materie nodig omdat Inschrijver verantwoordelijk wordt voor het opstellen van een goed plan.

Nadelen

- Het beoordelen van kwalitatieve teksten of plannen vraagt tijd, deskundigheid en objectiviteit;
- Meer risico dat leveranciers bezwaar maken tegen (vermeend) subjectieve scores;
- Vergt meer voorbereiding in de aanbestedingsfase omdat er beoordelingsmethodieken, scoringsmodellen en beoordelingsverslagen nodig zijn;
- Beloftes in een door inschrijver ingediend plan van aanpak zijn niet altijd even afdwingbaar als een harde eis.

5.2 Opnemen in een aanbesteding

In de volgende paragrafen doen we een handreiking om implementatie en onboarding in een aanbesteding op te nemen. We geven inzicht in de informatie die u aan inschrijvers dient te verstrekken zodat inschrijvers in staat zijn een passende inschrijving te doen. Ook worden een aantal varianten met overwegingen gegeven om het onderdeel implementatie en onboarding in een aanbesteding op te nemen.

5.2.1 Omvang van de dienstverlening

Om goede inschrijvingen op een aanbesteding te ontvangen is het essentieel dat inschrijvers een goed inzicht krijgen in de omvang van de dienstverlening die geleverd moet worden. Het inschrijven met SOC-diensten kan immers alleen als inschrijvers zicht hebben op wat de te bewaken ICT-assets zijn. Als aanbestedende dienst hebt u een verantwoordelijkheid om deze informatie met de aanbestedingsstukken aan te leveren.

Het gaat om de volgende informatie[4]:

- Aantal aan te sluiten assets, uitgesplitst naar:
  - Werkstations uitgesplitst naar operating system;
  - Servers uitgesplitst naar operating system;
  - Security appliances, merk en type per device;
  - IoT apparaten met relevante informatie zoals merk en type
  - Overige (bijzondere) apparatuur;
  - Aantal gebruikers accounts (incl. mail-adressen);
  - Aantal geprivilegieerd accounts (b.v. beheerders accounts).
- Globale netwerkarchitectuur, inclusief inzicht in:
  - Logische en fysieke locaties;
  - Zonering;
  - Koppelvlakken met andere netwerken;
  - Datavolumes die verwerkt worden;
- Aantal en type te monitoren accounts (in verband met identiteit monitoring);
- Beschrijving van de bewaking die geleverd moet worden;
- Vereiste service levels.

Al deze aspecten hebben invloed op de implementatie en onboarding die de dienstverlener moet uitvoeren. Zonder deze gegevens mag niet verwacht worden dan een inschrijver een goede aanbieding kan doen. Bij deze informatie dient ook steeds aangegeven te worden of er bijzonder omstandigheden zijn zoals dat bepaalde assets door een (andere) externe ICT-leverancier worden beheerd of dat er mogelijke restricties zijn betreft rechten of het wel/niet installeren van software (zoals log-agents).

Als het niet goed mogelijk is om deze gegevens inzichtelijk te maken, kunt u ervoor kiezen om kleiner te beginnen. Zo is het denkbaar dat u start met alleen het bewaken van de werkstations, servers en het e-mail verkeer. De aan te leveren gegevens zijn dan aanmerkelijk beperkter en eenvoudiger. Vanuit een dergelijke basisdienst kan, indien gewenst, op een later tijdstip verder worden uitgebouwd.

5.2.2 Samenwerking

Het implementeren en onboarden van SOC-diensten vereist altijd een nauwe samenwerking tussen opdrachtgever en opdrachtnemer, inclusief eventuele onderaannemers van opdrachtgever en opdrachtnemer. Een goede en constructieve samenwerking tussen alle partijen is essentieel om succesvol SOC-diensten in te richten. Zorg dat u als opdrachtgever, voor zover van toepassing, al **voor publicatie** van de aanbesteding betrokken leveranciers/dienstverleners in kennis stelt van het voornemen om SOC-dienstverlening in te kopen. Maak ook afspraken over medewerking van

[4] Het is niet wenselijk dat deze informatie publiekelijk beschikbaar wordt gesteld. Voor SOC-diensten is om deze reden vrijwel altijd een niet-openbare aanbestedingsprocedure de beste keuze.

deze partijen. Niets is zo vervelend om na publicatie, of zelfs na gunning, op weerstand bij deze essentiële partijen te ondervinden.

Aangezien samenwerking een belangrijke succesfactor voor de SOC-dienstverlening is, is het noodzakelijk om al in de aanbesteding criteria voor samenwerking op te nemen. Verder is het raadzaam om samenwerking als een beoordelingsaspect in de aanbesteding op te nemen. Dit kan als los subgunningscriterium, of als onderdeel van een implementatie- en onboardingsplan.

5.2.3 Implementatie en onboarding als eis

Indien u ervoor kiest om implementatie en onboarding als eis op te nemen, is het noodzakelijk om de implementatie en onboarding in de aanbesteding volledig uit te werken. Het is bij deze vorm belangrijk om geen onderdelen te vergeten, omdat die later tot meerwerk zullen leiden. Paragrafen 4.1 en 4.2 geven een aantal handvatten om de implementatie en onboarding uit te werken.

De inschrijver hoeft in zijn Inschrijving alleen akkoord te geven op het realiseren volgens de voorgeschreven aanpak.

Met deze aanpak zullen de inschrijvingen van verschillende marktpartijen weinig onderling verschil hebben. Omdat er aan eisen geen waarde wordt toegekend, is in deze vorm de prijs doorslaggevend voor de gunning.

Deze aanpak is vooral zinvol als de opdrachtgever exact weet wat hij wil en over zeer veel expertise beschikt om dit op voorhand volledig en in detail voor te schrijven. Het stuurt op laagste prijs, maar trekt gelijktijdig risico's van meerwerk naar opdrachtgever toe.

5.2.4 Implementatie en onboarding als wens (subgunningscriterium)

In veel gevallen zal de keuze voor onboarding als wens (subgunningscriterium) een meer logische keuze zijn. Bij deze vorm hoeft opdrachtgever alleen vast te stellen wat de minimale kwaliteitseisen zijn die u nodig zijn. Leg deze minimale kwaliteitseisen vast in de aanbestedingsdocumenten, bijvoorbeeld in een programma van eisen (PvE). Vervolgens dienen inschrijvers voorstellen voor implementatie en onboarding in. Indien de wens goed is beschreven, dan is het aan de inschrijvers om ervoor te zorgen dat men alle aspecten die nodig zijn voor implementatie en onboarding opneemt. De verantwoordelijkheid voor een volledige implementatie en onboarding ligt hiermee bij opdrachtnemer. In paragraaf 5.1.2 is dit met meer detail beschreven.

Het is van belang om de volgende onderdelen in uw aanbesteding op te nemen:

- **Beschrijving van de doelstelling:**
  Beschrijft zorgvuldig, volledig en duidelijk wat de doelstelling van de implementatie en onboarding is. De doelstelling omvat meer dan enkel het opleveren van een werkende dienst. Denk aan zaken als:
  - het voeren van regie;
  - het beperken van overlast bij de organisatie van opdrachtgever en haar leveranciers en dienstverleners;
  - het ontzorgen van opdrachtgever;
  - het zorgdragen dat alle belanghebbende goed geïnformeerd zijn en uiteraard;
  - het opleveren van een werkende dienst die voldoet aan de eisen en gehonoreerde wensen uit de aanbesteding.

  Belangrijk is om als aanbestedende dienst zo min mogelijk te beschrijven 'hoe' de aanbieder zijn werk moet uitvoeren. De kracht van het koppelen aan de doelstelling, is dat de aanbieder bepaald – en daarmee verantwoordelijk is – hoe de werkzaamheden gedaan moeten worden. Deze keuze is vrijwel altijd de beste keuze, omdat de aanbieders meer ervaring hebben met het leveren van deze diensten dan de opdrachtgever zelf.

- **Laat inschrijvers een (concept) implementatie- en onboardingsplan indienen**
  Laat inschrijvers een (concept) implementatie- en onboardingsplan indienen waarmee de hiervoor bedoelde doelstelling wordt ingevuld. Beschrijf op hoofdlijnen wat u van de implementatie verwacht. De aspecten die in paragraaf 4.1 en 4.2 van dit document zijn beschreven, bieden een goede basis voor een dergelijke beschrijving.

  Aanbestedingsrechtelijk moet u vermelden waarop u dit plan gaat beoordelen. U hebt veel vrijheid om dit in te vullen. Inventariseer welke aspecten voor uw organisatie belangrijk zijn en raadpleeg een inkoper of aanbestedingsexpert om u te begeleiden bij het opstellen van de beoordelingsaspecten.

  Ter inspiratie noemen we hier een aantal voorbeelden van **beoordelingsaspecten**:
  - Leesbaarheid van het implementatie- en onboardingplan;
  - Geven van inzicht in de aanpak en doorlooptijden van de implementatie;
  - Geven van inzicht in de aanpak en eventuele fasering van de onboarding;
  - Geven van inzicht in tijdslijnen, milestones en opleverprocessen;
  - Geven van inzicht wat er in de ICT-infrastructuur van opdrachtgever geplaatst en/of aangepast moet worden om logbronnen aan te sluiten;
  - Geven van inzicht in de inspanningen die van opdrachtgever worden verwacht en maatregelen om deze inspanningen zo beperkt mogelijk te houden;
  - Geven van inzicht in maatregelen die genomen worden om de continuïteit van de implementatie en onboarding te borgen;
  - De mate dat processen van opdrachtgever en opdrachtnemer op elkaar aansluiten;
  - De mate waarin de aanpak aansluit op de behoeftes van opdrachtgever;
  - Op welke wijze de voorgestelde aanpak invulling geeft aan de doelstellingen van opdrachtgever.
  - De wijze waarop inschrijver de impact en overlast van de implementatie en onboarding voor opdrachtgever en andere betrokkenen beperkt worden;
  - Hoe inschrijver ervoor zorgt dat de gekozen aanpak leidt tot een hoge planbetrouwbaarheid;
  - De mate waarin de gekozen aanpak haalbaar en realistisch is;
  - Geven van inzicht in de wijze waarop de samenwerking is georganiseerd met tenminste aandacht voor:
    - Waarom de aanpak efficiënt en effectief is;
    - Inlevingsvermogen in en rekening houden met belangen van andere betrokken partijen;
    - De wijze en mate van afstemming met opdrachtgever over planning, voorbereiding, realisatie, communicatie, etc.;
    - Hoe de afstemming met andere betrokkene wordt gerealiseerd;
    - Inzicht in expertise en rollen die opdrachtgever beschikbaar moet stellen;
    - Regie en coördinatie om de ICT-omgeving geschikt te maken om de benodigde logdata op een passend niveau te verzamelen;
  - De aandachtpunten die inschrijver voor opdrachtgever heeft om tot een succesvolle implementatie en onboarding te komen;
  - Hoe is risicobeheersing gedurende de realisatie ingericht en welke initiële risico's zijn voorzien.

  <u>Beoordelingskader</u>
  Naast de aspecten waarop u gaat beoordelen, moet u ook kenbaar maken hoe u gaat beoordelen. Dat wil zeggen dat u beschrijft wanneer een antwoord goed, slecht of iets er tussenin is. Dit noemt men het **beoordelingskader**.

  Voor een implementatie- en onboardingsplan is het zogenaamde **VCRRE** beoordelingskader vaak zeer geschikt. Dit staat voor **V**olledig, **C**oncreet, **R**ealistisch, **R**elevant en **E**ffectief. Bij dit beoordelingskader beoordeeld u de plannen op de beoordelingsaspecten en kijkt u in welke mate deze VCRRE zijn beschreven. Eventueel kunt u hier ook nog de aspecten Effectief en Toetsbaar aan toevoegen.

  Het voordeel van dit beoordelingskader is dat het weinig sturend is waardoor inschrijvers meer ruimte hebben voor creatieve en innovatieve voorstellen. Gelijktijdig biedt dit beoordelingskader de mogelijkheid om voorstellen die niet realistisch of relevant zijn, als minder goed te beoordelen. Ook "wollige" verhalen kunnen door gebrek aan concreetheid als minder goed worden beoordeeld.

Bespreek de beoordelingsaspecten en beoordelingskaders met uw inkoper of aanbestedingsexpert. Zij kunnen u ondersteunen om dit op de juiste wijze in de gunningsleidraad te verwerken.

Omvang van concept implementatie- en onboardigsplan
Gebruikelijk is om aan inschrijvers een maximum aantal pagina's op te geven dat voor een (concept) plan mag worden gebruikt. Wat de meest geschikte omvang is, hangt sterk samen met enerzijds de gevraagde omvang en complexiteit van de dienstverlening en anderzijds het aantal beoordelingsaspecten dat u opneemt.

Voor een eenvoudig plan zullen maximaal acht tot tien pagina's A4, excl. titelblad en inhoudsopgave, volstaan. Bij toenemende complexiteit of veel beoordelingsaspecten neemt de omvang toe. Het is aan te bevelen om niet meer dan twintig pagina's toe te staan. Het compact plan forceert inschrijvers om zich te beperken tot hoofdzaken en voorkomt dat er veel weinig of niet relevante beschrijvingen in het plan worden opgenomen. Dit helpt het beoordelingsproces dat later in de aanbesteding moet plaatsvinden.

- **Eis dat het ingediende plan aan de doelstelling voldoet**
  Neem in de aanbesteding een eis op dat het in te dienen (concept) implementatie- en onboardingsplan zodanig is uitgewerkt dat het invulling geeft aan de doelstelling. Daarmee wordt de inschrijver verantwoordelijk om te bepalen welke middelen en werkzaamheden er nodig zijn om de doelstelling te bereiken en dit in het implementatie- en onboardingsplan op te nemen. Met deze eis voorkomt u dat inschrijvers, al dan niet om strategische redenen, onvolledige voorstellen indienen. Feitelijk voorkomt u op deze manier meerwerk (binnen de gegeven scope).

- **Omzetten concept naar definitief implementatie- en onboardingsplan (na gunning)**
  Neem ook een eis op dat opdrachtnemer binnen een bepaalde periode na gunning, bijvoorbeeld drie weken, in samenspraak met opdrachtgever het concept implementatieplan zal omzetten naar een definitief implementatieplan. Het ingediende concept implementatieplan is de basis voor het definitieve implementatieplan. Eventuele toezeggingen die in het concept implementatieplan zijn gedaan, worden opgenomen in het definitieve implementatieplan.

Bijlage I - Voorbeeldteksten

In deze bijlage vindt u voorbeeldteksten die u kunt gebruiken als basis voor het opstellen van een aanbesteding voor SOC-diensten. De teksten zijn zo geformuleerd dat ze direct inzetbaar zijn voor een aanbestedingsdocument. Daarom vertonen ze veel overeenkomsten met de beschrijvende teksten uit de eerdere hoofdstukken, maar zijn ze in deze bijlage eenduidiger en meer directief geformuleerd.

De teksten in dit document zo universeel als mogelijk opgesteld. Dat laat onverlet dat het noodzakelijk is om de teksten goed door te nemen en te valideren of ze in uw specifieke geval ook van toepassing zijn. Definities zijn met een hoofdletter geschreven en treft u in Bijlage II, afkortingen en definities.

Opmerking: *Groene teksten in dit hoofdstuk betreffen placeholders. In aanbestedingsstukken moeten deze placeholders vervangen worden door teksten die specifiek voor de organisatie van Opdrachtgever van toepassing zijn.*

SOC-dienst

Het voor deze Dienstverlening benodigde Security Operatons Center (SOC) wordt door Opdrachtnemer beschikbaar gesteld. Het SOC dat Opdrachtnemer beschikbaar stelt is zodanig ingericht dat Opdrachtnemer aan alle eisen uit de onderhavige aanbesteding zal voldoen. Dit houdt in dat Opdrachtnemer zorgt dat het SOC over voldoende capaciteit (in kwaliteit en kwantiteit) beschikt om de diensten te leveren. Ook zorgt Opdrachtnemer dat de betrokken medewerkers voldoende kennis hebben van de omgeving van Opdrachtgever om werkzaamheden zoals Triage en inschaling uit te kunnen voeren.

Implementatie

Opdrachtnemer is verantwoordelijk voor het uitvoeren van de Implementatie van de Dienstverlening. De Implementatie draait om het bouwen van de fundamentele infrastructuur en het inrichten van de basisprocessen. De Implementatiefase omvat alle werkzaamheden die nodig zijn om de diensten te kunnen leveren, met uitzondering van het technisch aansluiten van de te bewaken ICT-omgevingen en Assets. Dit technisch aansluiten rekenen we tot Onboarding en is verderop beschreven.

Belangrijke onderdelen Implementatiefase:

- **Strategie & doelstellingen:** [In de aanbestedingsstukken moet Opdrachtgever beschrijven wat het SOC moet beschermen en kunnen (scope), wat de strategische doelstellingen zijn en de wijze waarop de organisatie invulling geeft aan deze doelstellingen. Deze Informatie is voor een Opdrachtnemer relevant omdat hij hierdoor de aangeboden Dienstverlening kan afstemmen op de strategie en doelstellingen van Opdrachtgever. Meer Informatie hierover vindt u in het VSSR kennisproduct "SOC Strategische Aanbevelingen"]
- **Governance & compliance:** [Beschrijf hier hoe Opdrachtgever en Opdrachtnemer de samenwerking organiseren en hoe de aansturing plaatsvindt. Beschrijf wie welke verantwoordelijkheden heeft, de bevoegdheden die daarbij horen, hoe besluitvorming

plaatsvindt, en de rapportage- en escalatielijnen die er zijn. Verder moet vastgelegd zijn aan welk beleid, wet- en regelgeving de Dienstverlening moet voldoen. Denk aan normenkaders als AVG, BIO, ISO 27001 of NIS2/Cbw.]

- **Architectuur & tooling:** Opdrachtnemer levert en richt alle voorzieningen in die nodig zijn om de SOC-Dienstverlening te leveren. Denk hierbij aan zaken zoals een SIEM, EDR/XDR, SOAR, Log management, ticketing, threat intelligence feeds, etc.

  Omdat het een dienstenopdracht betreft, blijft de invulling van dit onderdeel voor de Opdrachtgever grotendeels een blackbox. Opdrachtnemer voert deze werkzaamheden, voor zover deze binnen het domein van Opdrachtnemer liggen, zelfstandig en naar eigen inzicht uit. Opdrachtnemer zorgt ervoor dat de inrichting zodanig is dat aan alle verplichtingen uit de Overeenkomst worden voldaan en dat de dienstverlening aansluit op de ICT-omgeving van Opdrachtgever.

- **Inrichting processen en procedures:** Als onderdeel van de Implementatie richt Opdrachtnemer alle processen en procedures in die nodig zijn om de diensten te leveren. Operationele werkafspraken tussen Opdrachtgever en Opdrachtnemer zal Opdrachtnemer vastleggen in een Dossier Afspraken en Procedures (DAP).

  Tenminste de volgende processen worden ingericht:

  - **Triage, inschaling- en meldproces:** Dit omvat processen en procedures die nodig zijn om meldingen van de monitoringsystemen te beoordelen op geldigheid en te filteren (true-positive), vervolgens een prioriteit aan deze meldingen toe te kennen en te melden bij Opdrachtgever, of door Opdrachtgever aangewezen derden, te melden.
  - **Inschalingsmatrix:** In de Inschalingsmatrix zijn de criteria vastgelegd op basis waarvan meldingen geprioriteerd worden. Opdrachtnemer is in staat om op basis van zijn professionaliteit een Inschalingsmatrix op te stellen. Hij legt een concept Inschalingsmatrix voor en stemt deze met Opdrachtgever af. Opdrachtgever geeft akkoord op de Inschalingsmatrix.

    Situaties en dreigingen zijn niet statisch. Hierdoor kan de situatie ontstaan dat de Inschalingsmatrix bijgewerkt moet worden. Opdrachtnemer zorgt ervoor dat er een onderhoudsproces is ingericht zodat er aanpassingen in de Inschalingsmatrix gemaakt kunnen worden. Minimaal jaarlijks vindt een evaluatie van de Inschalingsmatrix plaats.
  - **Onboarding en offboarding van te monitoren Assets:** Gedurende de Dienstverlening zullen er aanpassingen in de te monitoren ICT-infrastructuur plaatsvinden. Als gevolg hiervan zullen er nieuwe Assets aan de monitoring moeten worden toegevoegd en bestaande Assets uit de monitoring genomen moeten worden. Opdrachtnemer zorgt ervoor dat als onderdeel van de Dienstverlening on- en offboarding van Assets mogelijk is
  - **Escalatieproces:** Als standaardprocedures niet functioneren of als er andere redenen zijn waardoor management-aandacht vereist is, dan dienen er processen en procedures te zijn om gecontroleerd op te schalen. Opdrachtnemer zorgt dat deze processen en procedures met Opdrachtgever worden afgestemd en vervolgens worden ingericht.
  - **Playbooks:** Playbooks zijn stappenplannen waarin vastligt hoe SOC-analisten moeten reageren op specifieke beveiligingsincidenten of dreigingen. Doel van deze playbooks is om sneller te handelen, fouten te beperken en consistentie te waarborgen in het meldproces richting de verantwoordelijke voor Incident Response. In beginsel bepaalt Opdrachtnemer zelf voor welke scenario's playbooks nodig zijn en zorgt dat voor deze scenario's playbooks zijn opgesteld. Indien Opdrachtgever aanleiding ziet om voor bepaalde scenario's een playbook op te stellen, dan mag

Opdrachtgever hiervoor een verzoek bij Opdrachtnemer indienen. Opdrachtnemer zal hieraan uitvoering geven, mits het verzoek uitvoerbaar, redelijk en billijk is.

- **Rapportageproces:** Opdrachtnemer zorgt ervoor dat de processen die nodig zijn om aan de rapportageverplichtingen worden ingericht.
- **Communicatiematrix:** Er wordt vastgelegd wie bij Opdrachtgever en Opdrachtnemer elkaars aanspreekpunten zijn, de contactgegevens en indien van toepassing, vervangers.

- **Aansluiten op bestaande procedures:** Naast het inrichten van nieuwe processen en procedures, is het ook noodzakelijk dat de SOC-Dienstverlening aansluit op bestaande processen van Opdrachtgever aan te sluiten. Aanpassingen in bestaande processen van Opdrachtgever of toeleveranciers van Opdrachtgever zullen worden doorgevoerd door de proceseigenaren van of namens Opdrachtgever. Opdrachtnemer zal haar medewerking verlenen, bijvoorbeeld met het aanleveren van Informatie die nodig is om deze processen aan te passen op de nieuwe SOC-Dienstverlening. Procesinrichting aan de zijde van Opdrachtnemer is uiteraard de verantwoordelijkheid van Opdrachtnemer.

  - **Incident Response-proces:** Opdrachtgever stelt een centraal aanspreekpunt voor de incidentprocessen beschikbaar aan Opdrachtnemer. Dit centrale aanspreekpunt fungeert als Single Point Of Contact (SPOC). Opdrachtnemer zorgt ervoor dat meldingen van het SOC via dit SPOC worden gedaan en zijn Dienstverlening aansluit op bestaande incidentprocessen van Opdrachtgever. Deze aansluiting is niet alleen nodig om meldingen vanaf het SOC in de organisatie van Opdrachtgever op te volgen, maar ook nodig zodat Opdrachtgever incidenten, bijvoorbeeld het wegvallen van toegang tot Logdata, kan aanmelden bij de verantwoordelijke beheersorganisatie. Ook moeten er afspraken gemaakt worden over tijdig herstel die in lijn zijn met de Service Levels voor de SOC-Dienstverlening. Andersom moet de bestaande beheerorganisatie van Opdrachtgever toegang krijgen tot een centraal aanspreekpunt van de SOC-dienstverlener om storingen te melden die ontstaan door SOC-monitoring. Naast concreet incidentherstel is deze samenwerking ook vereist bij onderzoek naar incidenten waarvan de oorzaak nog niet duidelijk is.
  - **Change proces:** Het aansluiten op het changeproces is tweeledig. Enerzijds kunnen er naar aanleiding van SOC-meldingen wijzigingen nodig zijn, bijvoorbeeld om dreigingen te mitigeren. Opdrachtgever stelt aan Opdrachtnemer een centraal aanspreekpunt aan dat als Single Point of Contact fungeert en dergelijke meldingen aanneemt en zorgt voor de verdere afhandeling binnen de organisatie van Opdrachtnemer en eventueel betrokken derden.

    Daarnaast is het noodzakelijk dat toekomstige aanpassingen in de ICT-infrastructuur bij Opdrachtgever zodanig worden uitgevoerd dat de SOC-diensten ook na de wijzigingen ongestoord blijven functioneren. Dit geldt voor zowel uitbreidingen van de te monitoren Assets (on-boarding), aanpassingen aan bestaande Assets alsmede voor het afschakelen/ontmantelen van te monitoren Assets (off-boarding). Voor zover er aanpassingen aan bestaande processen en procedures van Opdrachtgever nodig zijn, zal Opdrachtgever deze realiseren. Opdrachtnemer stelt de benodigde Informatie beschikbaar om deze aanpassingen uit te voeren.
  - **Problem proces:** Bij complexe incidenten/storingen kan diepgravend onderzoek nodig zijn, bijvoorbeeld voor een zogenaamde root-cause analyse. Monitoringdiensten kunnen betrokken raken in het problem proces en bijbehorende

root-cause analyse. Opdrachtnemer zorgt ervoor dat de SOC-Dienstverlening aansluit op de bestaande problem processen van Opdrachtgever en voert de benodigde inspanningen uit die nodig zijn om het problem proces adequaat te laten functioneren. Dit geldt nadrukkelijk ook voor inspanningen die nodig zijn terwijl op voorhand niet duidelijk is of de SOC-Dienstverlening wel of geen oorzaak is.

- **Capaciteitsbeheer:** Opdrachtgever en Opdrachtnemer moeten van elkaars plannen op de hoogte zijn als deze van substantiële invloed zijn op de capaciteit van de ICT-infrastructuur en/of de SOC-monitoringdiensten. Opdrachtnemer zorgt ervoor dat er een aansluiting is op het bestaande capaciteitsbeheer en voert de benodigde inspanningen uit die nodig zijn om capaciteitsbeheer adequaat te laten functioneren.

Indien er naast de hierboven beschreven processen en procedures nog andere processen en/of procedures nodig zij om SOC-diensten conform Overeenkomst te leveren, dan maakt dat onderdeel uit van de Overeenkomst en zal Opdrachtnemer deze als onderdeel van de Implementatie (binnen scope) inrichten. Opdrachtnemer legt operationele werkafspraken tussen Opdrachtgever en Opdrachtnemer vast in een Dossier Afspraken en Procedures (DAP).

- **Samenwerking, Personeel & rollen**: Opdrachtnemer zorgt voor gekwalificeerde medewerkers die benodigd zijn om de Dienstverlening zoals overeengekomen te leveren. Ook zorgt Opdrachtnemer voor passende maatregelen zodat medewerkers alleen op een need-to-know basis toegang hebben tot Gegevens en Informatie van Opdrachtgever en wordt voldaan aan de veiligheidseisen die in de Overeenkomst zijn gesteld.

  Een aantal taken en verantwoordelijkheden blijven nadrukkelijk bij Opdrachtgever. Dit zijn, naast het incident-response, vooral de onderdelen waar een organisatie verantwoordelijkheid moet afleggen aan derden. Denk aan het melden bij toezichthouders, informeren van bedrijven en burgers, informeren van de politiek en pers. Ook beslissingen met grote organisatorische impact zal Opdrachtgever zelf nemen, denk aan het al dan niet preventief uitschakelen van productiesystemen om verdere schade te voorkomen. Tijdens de Implementatiefase worden deze afspraken meer concreet uitgewerkt en door Opdrachtnemer vastgelegd in een Dossier Afspraken en Procedures (DAP).

- **Use case development:** Use cases, ook wel Detectieregels, zijn algoritmen die gebruikt worden om verdachte situaties in ICT-systemen te detecteren, denk aan brute-force login pogingen, data exfiltration, etc.. Het definiëren van use cases wordt gedaan op basis van risico's. Opdrachtnemer zorgt voor het aanmaken en onderhouden van de use-cases. Opdrachtgever behoudt het recht om specifieke scenario's aan te dragen en aan Opdrachtnemer te verzoeken hier een use case voor uit te werken. Opdrachtgever zal op basis van een dergelijk scenario een use case en Detectieregels uitwerken en implementeren. Dit kan bijvoorbeeld aan de orde zijn als dreigingen en/of specifieke aanvallen gericht op de organisatie van Opdrachtgever verwacht worden.

- **Communicatie:** Communicatie is essentieel voor de Dienstverlening. Als onderdeel van de Implementatie worden, in overleg met Opdrachtgever, de processen en werkafspraken met betrekking tot communicatie door Opdrachtnemer ingericht. [In de aanbesteding moeten duidelijke kaders worden opgenomen over de gewenste rolverdeling zodat Opdrachtnemer de Implementatie hierop kan laten aansluiten. Houdt hierbij rekening dat de communicatie gedurende normale (rustige) periodes wezenlijk anders kan zijn dan gedurende (ernstige) incidenten. Bij ernstige incidenten kunnen er gevolgen voor burgers en bedrijven zijn, moeten bestuurders, toezichthouders en pers geïnformeerd worden. Overweeg om al tijdens het schrijven van een aanbesteding op dit onderwerp de communicatieafdeling te betrekken.

Het inrichten van de communicatie afspraken en procedures is onderdeel van de Implementatie en het is raadzaam om in het Protocol van Oplevering.]

Onboarding

Onboarding richt zich op het aansluiten van ICT-omgevingen en ICT-Assets die bewaakt moeten worden. Na het uitvoeren van Onboarding zijn de Assets die in het Assetoverzicht zijn opgenomen daadwerkelijke aangesloten, geconfigureerd en ingeregeld en vindt monitoring door het SOC plaats.

Onboarding is niet alleen nodig bij de initiële inrichting van de Dienstverlening, maar ook gedurende de looptijd van de Overeenkomst zullen er Assets aan de Dienstverlening worden toegevoegd en andere Assets uit de Dienstverlening worden verwijderd (off-boarding).

Onboarding is een proces dat in samenwerking tussen Opdrachtnemer, Opdrachtgever en eventuele onderaannemers gerealiseerd wordt. Opdrachtnemer bereidt de Onboarding voor en voert de regie over de uitvoering. Opdrachtnemer stelt een vast contactpersoon aan die als eerste aanspreekpunt voor Opdrachtgever dient.

Indien voortgang achterblijft, zal Opdrachtnemer eerst zelf initiatief nemen om de voortgang te herstellen. Indien dit, buiten de schuld van Opdrachtnemer, niet tot het gewenste resultaat leidt, zal Opdrachtnemer volgens de overeengekomen procedures escaleren.

In deze Opdracht omvat Onboarding alles dat nodig is om de te monitoren Assets aan te sluiten op de SOC-dienst en het operationaliseren van de monitoring. Opdrachtgever voorziet op hoofdlijnen de volgende onderdelen:

- **Inrichten connectiviteit:** Het realiseren van de dataverbindingen die nodig zijn om opdrachtnemer toegang te verschaffen tot de te bewaken ICT-Assets. Het gaat om de volledige keten tussen de monitoringsystemen van opdrachtnemer en de te bewaken Assets van Opdrachtgever. Connectiviteit omvat het interne netwerk (LAN) alsmede de verbindingen naar buiten (WAN). Opdrachtnemer brengt in kaart welke connectiviteit benodigd is en welk change processen hiervoor gevolgd moeten worden. Vervolgens werkt Opdrachtgever de benodigde changeverzoeken uit en dient deze in bij de betreffende beheerorganisaties. Opdrachtnemer maakt ook een testplan en zorgt dat het testplan wordt uitgevoerd om de geleverde connectiviteit op werking te controleren.

- **Aansluiten van Assets:** Het daadwerkelijk aansluiten van de Assets op de monitoringsystemen. Opdrachtnemer brengt in kaart wat er nodig is om de Assets op de monitoringsystemen aan te sluiten, stelt eventuele wijzigingsverzoeken op en dient deze in. Wijzigingen aan Assets worden door de verantwoordelijke beheerorganisaties van of namens Opdrachtgever uitgevoerd. Opdrachtnemer zal de bestaande wijzigingsprocessen volgen om de benodigde wijzigingen aan te vragen en uit te laten voeren.

  Opdrachtnemer controleert dat de doorgevoerde wijzigingen correct en effectief zijn uitgevoerd, bijvoorbeeld door het opstellen en uitvoeren van een testplan. Opdrachtgever zorgt ervoor dat bestaande procedures voor beheer en life cycle management van Assets zodanig zijn aangepast dat Opdrachtnemer geïnformeerd wordt over relevante aanpassingen. Opdrachtnemer zorgt dat de monitoringvoorziening ook blijven werken na updates van Assets of andersoortige wijzigingen waarover hij is geïnformeerd.
- **Log Onboarding:** Zodra de connectiviteit gereed is en de Assets hun Logdata beschikbaar stellen, is integratie van logbronnen (firewalls, endpoints, servers, AD, cloudplatforms) nodig.

Deze activiteit voorziet dat de Logdata die van de Assets afkomstig is, ook correct door de monitoringsystemen worden ingelezen.

Opdrachtnemer draagt er zorg voor dat de Logdata efficiënt en effectief wordt getransporteerd en verwerkt in het monitoringsysteem. Met efficiënt en effectief wordt bedoeld dat alleen relevante Logdata naar monitoringsystemen wordt gestuurd. Enerzijds omdat het verwerken van overbodige Logdata tot onnodige belasting van systeemcomponenten leidt, anderzijds om te voldoen aan wet- en regelgeving. Bepaalde Logdata, bijvoorbeeld persoonsgegevens, is onderhevig aan wet- en regelgeving. Opdrachtnemer zorgt ervoor dat de inrichting zodanig is dat wordt voldaan aan de geldende kaders, wet- en regelgeving. Deze activiteiten vinden plaats binnen het domein van Opdrachtnemer en zijn daarmee de verantwoordelijkheid van Opdrachtnemer.

- **Baseline:** Nadat de technische koppeling met de ICT-Assets is gerealiseerd en de relevante Logdata binnenkomt, zal Opdrachtnemer het 'normale' beeld van de omgeving vaststellen. Dit referentiepunt is nodig om afwijkingen betrouwbaar te kunnen signaleren.

  Het vaststellen van dit normale gedragspatroon wordt het opstellen van een baseline genoemd. Opdrachtnemer voert dit uit door de verzamelde Logdata over een representatieve periode te analyseren. Typische patronen die hierbij naar voren komen, zijn bijvoorbeeld:

  - het gemiddelde aantal authenticatiepogingen per uur
  - de gebruikelijke inlogtijden en -locaties van gebruikers
  - het normale dataverkeer buiten kantoortijden
  - veelvoorkomende processen en commando's

  Deze lijst is niet limitatief. Opdrachtnemer zorgt ervoor dat alle elementen die nodig zijn om de Dienstverlening conform specificaties te leveren, zijn opgenomen in de baseline. Met een goed gedefinieerde baseline kan Opdrachtnemer de Detectieregels zodanig instellen dat zij een alert genereren wanneer het gedrag in bepaalde mate afwijkt van dit patroon.

- **Tuning:**

  Als onderdeel van Onboarding voert Opdrachtnemer tuning (optimalisatie) uit zodat de detectie zowel effectief als efficiënt wordt uitgevoerd. Met efficiënt wordt bedoeld dat alleen Gegevens en Informatie wordt verwerkt die nodig is om de juiste dingen te zien. Met effectief wordt bedoeld dat de overeengekomen doelstellingen worden behaald.

  In andere woorden, door het toepassen van tuning wordt er zo min mogelijk niet relevante Gegevens (ruis) of privacygevoelige Gegevens te verwerkt. Tuning omvat onder andere:

  - Het finetunen van de drempelwaarden en voorwaarden van Detectieregels om onnodige meldingen (False Positives) te verminderen.
  - Het bewust beperken van de hoeveelheid en het type Logdata die wordt verzameld en verwerkt, zodat alleen de voor monitoring noodzakelijke Gegevens en Informatie wordt ingelezen (data minimalisation / privacy by design).

  Deze lijst is niet limitatief. Opdrachtnemer zorgt ervoor dat alle elementen die nodig zijn voor een optimale tuning worden meegenomen in de realisatie.

  Ook nadat Onboarding heeft plaatsgevonden is het belangrijk om periodiek baseline en regels te herijken. Hiermee anticipeert de monitoring op veranderingen van de omgeving, bijvoorbeeld door nieuwe systemen, gewijzigde werkpatronen, seizoensinvloeden, etc. Opdrachtnemer zorg ervoor dat er een proces is ingericht dat hierin voorziet. Deze activiteiten vinden volledig plaats binnen het domein van Opdrachtnemer en zijn daarmee de volledige verantwoordelijkheid van Opdrachtnemer.

Concept implementatie- en onboardingsplan

Wij verzoeken u bij uw inschrijving een concept implementatie- en onboardingsplan in te dienen waarin u beschrijft hoe u de Implementatie en Onboarding in het kader van deze Opdracht uitvoert. Dit ingediende concept implementatie- en onboardingsplan is een Subgunningscriterium en toezeggingen die u doet en verwachtingen die u schept zijn bindend. Het ingediende conceptplan is de basis voor het definitieve implementatie- en onboardingsplan dat Opdrachtnemer na Gunning opstelt.

De omvang van het in te dienen concept implementatie- en onboardingsplan mag maximaal 12 zijdes A4 zijn, exclusief titelblad en inhoudsopgave.

Bij het beoordelen van het implementatieplan wordt in het bijzonder gelet op de volgende aspecten:

- De mate waarin het conceptplan leesbaar is en de mate waarin het plan een duidelijk, realistisch en logisch samenhangend voorstel voor Implementatie en Onboarding beschrijft;
- De mate waarin u laat zien dat uw aanpak volledig is en aansluit bij de behoefte en doelstellingen van Opdrachtgever;
- Op welke wijze u ervoor zorgt dat processen van Opdrachtgever en Opdrachtnemer goed op elkaar aansluiten;
- De mate waarin uw plan duidelijk inzicht geeft in tijdslijnen, te behalen (tussentijdse) mijlpalen, wijze van Oplevering inclusief oplever- en acceptatieprocessen.
- De mate waarin effectieve maatregelen genomen worden om de inspanningen die van Opdrachtgever worden verwacht zo beperkt mogelijk te houden;
- De mate waarin u concreet inzicht geeft in de expertise c.q. rollen die Opdrachtgever beschikbaar moet stellen gedurende Implementatie en Onboarding. Maak hierbij ook een inschatting van de benodigde hoeveelheid inspanning per rol/expertisegebied;
- De mate waarin u inzicht geeft in effectieve maatregelen voor risicobeheersing en welke initiële risico’s u voorziet.
- Op welke wijze en met welke inspanningen begeleid u Opdrachtgever bij het inrichten/aanpassen zijn ICT-omgeving zodat deze geschikt zijn voor verzamelen van de benodigde Logdata op een passend niveau en het aansluiten op de SOC-Dienstverlening;
- De mate waarin effectieve maatregelen worden genomen om overlast door implementatie en Onboarding bij Opdrachtgever te beperken;
- Het plan inzicht geeft in er eventueel in de ICT-infrastructuur van Opdrachtgever geplaatst en/of aangepast moet worden om de SOC-dienst aan te sluiten;
- Samenwerking: De wijze waarop u de samenwerking tussen Opdrachtnemer, Opdrachtgever en eventuele derden vormgeeft, de mate u rekening houdt met de belangen van andere betrokkenen en de wijze waarop u zorgt dat belanghebbende goed geïnformeerd worden.

Beoordeling

Om het Subgunningscriterium concept onboardings- en implementatieplan te beoordelen, wordt gelet op de mate waarin u de onderwerpen in het concept implementatie- en onboardingplan Volledig, Concreet, Realistisch, Relevant en Effectief (VCRRE) hebt uitwerkt.

Beoordelings- en waarderingsaspecten

Deze tabel benoemt de aspecten waarop uw concept implementatie- en onboardingsplan wordt beoordeeld en gewaardeerd. De waardering van uw antwoord door Aanbestedende dienst is gebaseerd op de beoordeling op het samenstel van deze aspecten. Uw antwoord voldoet aan de volgende beoordelingsaspecten:

Volledig	Het concept implementatie- en onboardingsplan beschrijft alle benoemde elementen. Er zijn geen onderdelen van Implementatie en onboarding onbeantwoord gebleven.
Concreet	Het concept plan is eenduidig, niet voor meerdere uitleg vatbaar en niet afhankelijk van aannames of interpretaties van de lezer: de lezer behoeft geen betekenis 'in te lezen' om zeker te weten wat hij/zij uit het concept plan mag begrijpen. Alle elementen van het concept plan sluiten logisch op elkaar aan. Er zijn geen 'open gaten' in redeneringen of in de presentatie van de aanpak.
Relevant	Uw concept plan is een gerichte uitwerking van de Implementatie en onboardingsaspecten. Het concept plan bevat zo min mogelijk Informatie die er voor de Implementatie en Onboarding eigenlijk niet toe doet. Het antwoord is van toegevoegde waarde voor Opdrachtgever.
Realistisch	Het concept implementatie- en onboardingsplan is praktisch uitvoerbaar, geloofwaardig en haalbaar binnen de context, randvoorwaarden en ambities van de Opdracht en is op geloofwaardige wijze onderbouwd met relevante kennis, ervaring of praktijkvoorbeelden. Het concept plan geeft blijk van inzicht in mogelijke belemmeringen, risico's of afhankelijkheden en laat zien hoe hier realistisch mee wordt omgegaan.
Effectief	Het antwoord maakt door onderbouwing inzichtelijk en begrijpelijk dat de gepresenteerde aanpak van Implementatie en Onboarding daadwerkelijk resulteert in de beoogde doelstellingen.

Tabel 1: Beoordelings- en waarderingsaspecten

Onderstaande tabel geeft een opsomming weer van de puntenwaardering die toekeend wordt aan het concept implementatie- en onboardingsplan. Deze opsomming is uitputtend – uitsluitend deze genoemde punten kunnen per wens worden toegekend.

Score	Omschrijving	Aantal punten
Uitstekend	Alle onderdelen van Implementatie en Onboarding zijn uitgewerkt. Het concept plan is **zeer duidelijk** uitgewerkt en overtuigd beoordelaars dat het zeer goed aansluit op de vraag- en doelstelling. Het geheel is zeer volledig, realistisch, relevant, concreet, effectief en logisch samenhangend uitgewerkt. Bovendien biedt de voorgestelde aanpak **positieve, verrassende en/of vernieuwende elementen**.	[invullen]
Goed	Alle onderdelen van Implementatie en Onboarding zijn uitgewerkt. Het concept plan is **duidelijk uitgewerkt** en overtuigd beoordelaars dat het goed aansluit op de vraag- en doelstelling. Het geheel is volledig, realistisch, relevant, concreet, effectief en logisch samenhangend uitgewerkt.	[invullen]
Voldoende	De onderdelen van Implementatie en Onboarding zijn grotendeels volledig uitgewerkt. Het concept plan is **voldoende duidelijk** uitgewerkt en overtuigd beoordelaars dat het voldoende aansluit op de vraag- en doelstelling. Het geheel is in voldoende mate volledig, realistisch, relevant, concreet, effectief en logisch samenhangend uitgewerkt.	[invullen]
Matig	**Niet alle onderdelen** van Implementatie en Onboarding zijn volledig uitgewerkt. En/of het concept plan geeft redelijk beeld, maar sluit niet volledig aan op de vraag- en doelstelling. En/of het geheel is niet volledig, realistisch, relevant, concreet, effectief en logisch samenhangend uitgewerkt.	[invullen]
Slecht	**Diverse onderdelen** van Implementatie en Onboarding zijn **onvoldoende of niet uitgewerkt**. En/of het concept plan geeft onvoldoende beeld, en/of sluit niet aan op de vraag- en doelstelling. En/of het geheel is weinig, realistisch, relevant, concreet, effectief en logisch samenhangend uitgewerkt.	[invullen; eventueel knock-out]

Tabel 1: Beoordelingstabel

Bijlage II - Afkortingen en definities

In dit document zijn afkortingen en definities gebruikt. Hieronder treft u het overzicht van gebruikte afkortingen en definities die in dit document zijn gebruikt.

Afkorting	Betekenis	Beschrijving
	Accepteren	De Acceptatie van een Oplevering
	Acceptatie	De goedkeuring door de Opdrachtgever van (onderdelen) van de Prestatie.
	Asset	In dit document wordt met Asset een ICT-Asset bedoeld; zie de definitie ICT-Asset in dit overzicht.
	Assetoverzicht	Een lijst waarin alle ICT-Assets zijn opgenomen die relevant zijn voor de levering van de Prestatie.
AVG	Algemene Verordening Gegevensbescherming	Europese verordening (EU 2026/679) inzake de bescherming van natuurlijke personen en die eisen stelt aan de verwerking en bescherming van persoonsgegevens.
BIO	Baseline Informatiebeveiliging Overheid	Het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen).
Cbw	Cyberbeveiligingswet	De Nederlandse wet die de minimale eisen stelt aan cyberbeveiliging van vitale en belangrijke organisaties. De Cbw is de Nederlandse implementatie van de Europese NIS2-richtlijn.
	Data	Data: De Engelse term voor Gegevens; zie definitie Gegevens in dit document. Opmerking: In de Nederlandse taal wordt data ook gebruikt als het meervoud van datum. Het is mogelijk dat in de aanbestedingsdocumenten 'data' ook in deze betekenis wordt gebruikt.
	Detectieregels	Logica in monitoring en detectiesystemen die als basis dienen om bepaalde patronen, afwijkingen of situaties te herkennen.
DAP	Dossier Afspraken en Procedures	Het document waarin de werkafspraken tussen Opdrachtnemer en Opdrachtgever zijn vastgelegd met betrekking tot de uitvoering van de Opdracht.
	Dienstverlening	Ingerichte en operationele SOC-diensten die aan Opdrachtgever geleverd worden (de Prestatie) of reeds bij Opdrachtgever aanwezig zijn. Dienstverlening kan ook betrekking hebben op toekomstige dienstverlening na beëindiging van de Overeenkomst.
EDR	Endpoint Detection and Response	Een technologie die continue eindpunten zoals werkstations, laptops, servers en mobiele apparaten monitort en analyseert om cyberdreigingen en verdachte activiteiten te detecteren.
	False Positive	Een waarschuwing of uitslag van het monitorsysteem die ten onrechte is afgegeven.
	Gegevens	Feitelijke, vastgelegde waarden of waarnemingen die op zichzelf nog geen betekenis hebben en die door interpretatie en plaatsing in een context kunnen worden omgezet in informatie.
	Gunning	De laatste fase van een aanbesteding waarin de Opdrachtgever schriftelijk aan alle inschrijvers de Gunningsbeslissing kenbaar maakt.
	Gunningscriterium	Een criterium, vastgesteld door de Opdrachtgever en vooraf kenbaar gemaakt, wat wordt gebruikt voor de beoordeling en rangschikking van geldige inschrijvingen teneinde de economisch meest voordelige inschrijving te bepalen.
	Gunningsbeslissing	De keuze van de aanbestedende dienst voor de Ondernemer met wie hij voornemens is de Overeenkomst waarop de aanbesteding betrekking had, te sluiten, waaronder mede wordt verstaan de keuze om geen Overeenkomst te sluiten.
HAVIK	Handige Aanbestedingshulpmiddelen Voor Inkoop Kwalitatieve SOC-diensten	Een set kennisproducten dat door het programma Versterken SOC Stelsel Rijk is ontwikkeld om Rijksorganisaties te ondersteunen bij het opstellen van aanbestedingen van SOC-diensten.
	Handelingsperspectief	Een of meerdere handvat(ten) voor actie. Het geeft Opdrachtgever Informatie over hoe deze in een bepaalde situatie kan handelen om tot een gewenst resultaat te komen.
	ICT-Infrastructuur	Het samenhangende geheel van alle ICT-Assets dat in zijn totaliteit een (of meerdere) operationeel functionerend geheel is/zijn.

Afkorting	Betekenis	Beschrijving
	Implementatie	Het geheel van handelingen en maatregelen die nodig zijn om de organisatie van Opdrachtgever, inclusief eventuele onderaannemers, geschikt te maken voor het overeengekomen gebruik van de Prestatie.
	Implementatiefase	De periode binnen de looptijd van de overeenkomst waarin Opdrachtnemer het geheel van handelingen en maatregelen uitvoert die noodzakelijk zijn om de implementatie, zoals gedefinieerd in deze aanbesteding, volledig en aantoonbaar te realiseren, eindigend bij formele Accceptatie door Opdrachtgever.
	Informatie	De betekenis die mensen geven aan gegevens in een context.
ICT	Informatie en Communicatie Technologie	Verwijzing naar de technologieën die worden gebruikt om op elektronische wijze te communiceren en gegevens te verwerken en uit te wisselen.
	ICT-Asset	Elk individueel component of systeem dat onderdeel uitmaakt van een ICT-infrastructuur. Een ICT-Asset kan uit zowel hardware als software of een mix van beide omvatten.
	Inschalingsmatrix	Een referentiekader waarin criteria zijn vastgelegd die worden gebruikt voor de beoordeling, classificatie en prioritering van meldingen over (potentiële) informatiebeveiligingsincidenten.
	Logdata	Logdata betreft automatisch geproduceerde en van een tijdstempel voorziene documentatie van gebeurtenissen die relevant zijn voor analyse van de werking en beveiliging van informatiesystemen.
MSSP	Managed Security Service Provider	Gespecialiseerd bedrijf dat ICT-beveiligingsdiensten levert aan een klant. Bijvoorbeeld managed firewalls, managed endpoint protection, etc.
NCSC	Nationaal Cyber Security Center	Organisatieonderdeel van het Ministerie van Justitie en Veiligheid. Het Nationaal Cyber Security Centrum (NCSC) werkt aan een digitaal veilig Nederland.
NIS2	Nerwork and Information Security directive 2	Een Europese richtlijn (EU 2022/2555) die de minimale eisen voor beveiliging van netwerk- en informatiesystemen voor essentiële en belangrijke organisaties binnen de EU beschrijft, teneinde de cyberveiligheid en incidentresponse te versterken.
	Onboarding	Het geheel van handelingen en maatregelen dat nodig is om de Prestatie voor de betreffende Assets te leveren. Denk hierbij aan zaken zoals administreren, realiseren van koppelvlakken, lijnverbindingen, routeringen, aansluiten, configureren en het technisch/functioneel inregelen en optimaliseren van de Prestatie voor de betreffende Assets.
	Opdrachtgever	Organisatie die de Opdracht verstrekt
	Opdrachtnemer	De Inschrijver aan wie de Opdracht in het kader van de betreffende aanbesteding wordt gegund en met wie Opdrachtgever de Overeenkomst zal aangaan.
	Opdracht	Op basis van de inschrijvingsleidraad en hieraan gelieerde documenten te verrichten leveringen, diensten of werken.
	Oplevering	Het aanbieden door de Opdrachtnemer van (onderdelen van) de Prestatie ter Acceptatie.
	Overeenkomst	De schriftelijk vastgelegde verbintenis tussen Opdrachtgever en Opdrachtnemer die voortvloeit uit het resultaat van de aanbesteding.
	Personeel	De door Opdrachtnemer voor de uitvoering van de Overeenkomst in te schakelen personeelsleden of hulppersonen.
	Prestatie	Alle te leveren producten, diensten, werkzaamheden, etc. die via de Overeenkomst zijn overeengekomen. De Prestatie omvat ook alle verplichtingen die Opdrachtnemer vanuit de Overeenkomst heeft richting Opdrachtgever.
PvO	Protocol van Oplevering	Een document dat de wijze van de Oplevering beschrijft en dat de Acceptatie door Opdrachtgever vastlegt of indien Opdrachtgever niet tot Acceptatie wenst over te gaan, ruimte biedt om dit middels een motivatie te onderbouwen.
	Rijksoverheid	De landelijke overheid die bestaat uit ministeries, uitvoerende diensten, inspecties, de Hoge Colleges van Staat en adviescolleges. Meer Informatie vind u hier: https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/organisatie-rijksoverheid
	Service Levels	In de Overeenkomst opgenomen kwantiteits- en kwaliteitseisen ten aanzien van de te leveren Prestatie.

Afkorting	Betekenis	Beschrijving
SIEM	Security Information and Event Management	Een SIEM-systeem verzamelt, correleert, analyseert en bewaakt log- en eventgegevens uit diverse ICT-Assets zoals IT-systemen, netwerken en applicaties. Het doel is detecteren van (potenitiële) beveiligingsincidenten, het genereren van meldingen en het ondersteunen van de SOC-dienstverlening.
SOAR	Security Orchestration, Automation and Response	SOAR verwijst naar technologieën en processen die SOC-teams helpen bij het automatiseren, orkestreren en afhandelen van beveiligingsincidenten.
SOC	Security Operations Center	Een afdeling, team of dienst dat digitale systemen en/of identiteiten controleert en/of bewaakt en soms ook afhandelt.
	SOC-diensten	Een reeks beveiligingsdiensten gericht op het realtime monitoren, detecteren, analyseren en reageren op beveiligingsincidenten en -dreigingen.
	Subgunningscriterium	Een nader uitgewerkt onderdeel van een Gunningscriterium op basis waarvan inschrijvingen door de Opdrachtgever inhoudelijk worden beoordeeld en gewaardeerd.
	Triage	Het proces van het snel en efficiënt beoordelen, prioriteren en classificeren van meldingen uit de monitoring & detectiesystemen van het Security Operations Center.
UC	Use Case	Een beschrijving van een gedrag van een systeem dat reageert op een verzoek of situatie dat van buiten het systeem afkomstig is.
TLP	Traffic Light Protocol	Een methodiek om op simpele en intuïtieve manier aan te duiden wanneer en op welke wijze gegevens en Informatie mogen worden verspreid. Voor meer Informatie, zie: https://www.ncsc.nl/aansluiten-en-samenwerken/traffic-light-protocol-tlp
XDR	Extended Detection and Response	Een geïntegreerd beveiligingssysteem dat gegevens van meerdere bronnen, zoals endpoints; netwerken; servers en cloudomgevingen, verzamelt, correleert en analyseert om continue ICT-assets zoals werkstations, laptops, servers en mobiele apparaten te bewaken. Het voert analyses uit om cyberdreigingen en verdachte activiteiten te detecteren in is in staat om geautomatiseerd te reageren op cyberdreigingen.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

December 2025