TLP:GREEN

EISEN AAN DIENSTVERLENING

Monitoring & Detectie – HAVIK

Handreiking versie 1.1

Complexiteit document
Gemiddeld

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord 3
Achtergrond 3
Doelgroep 3

1. Documentgegevens 4
2. Inleiding 5
2.1 Context 5
2.2 Toepassing en reikwijdte 5
3. Leeswijzer 6
3.1 Indeling categorieën 6
3.2 Uitvoeringseisen 7
3.3 Samenhang met andere documenten 7
3.3.1 Inschalingsmatrix 7
3.4 Gebruik van de eisen 8
4 Algemene eisen 9
5 Eisen aan samenwerking en beheer 12
6 Eisen aan Dienstverlening 16
7. Eisen aan Logdatabeheer 18
8. Eisen aan Implementatie en Onboarding 20
9. Eisen aan Rapportages en kwaliteitsborging 23

Bijlage I - Samenhangende documenten 24
Bijlage II - Afkortingen en definities 25

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.

Een belangrijk onderdeel voor organinisaties om zich te beschermen tegen dergelijke dreigingen zijn Security Operations Centers (SOCs). SOC's beschikken over monitoring- en detectiediensten die gericht zijn op het verzamelen, analyseren, aggregeren en correleren van een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie. Monitoring en detectiesystemen van een SOC kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Overheidsorganisaties die dergelijke SOC-diensten willen inkopen zijn genoodzaakt om dit binnen aanbestedingsrechtelijke kaders te doe. Om dit inkopen te ondersteunen, is er een toolkit ontwikkelt. Met Handige Aanbestedingshulpmiddelen Voor Inkoop Kwalitiatieve SOC-diensten (HAVIK) krijgen organisaties hulpmiddelen om dit proces te ondersteunen.

Dit document is onderdeel van de HAVIK toolkit en richt zich op het opstellen van een programma van eisen voor de inkoop van SOC-diensten. Het omvat van een basisset technische en functionele eisen waaruit een organisatie kan putten bij het opstellen van een aanbesteding voor SOC-diensten.

Achtergrond

VSSR levert diverse kennisproducten die organisaties kunnen gebruiken bij het inrichten van Security Operations Centers (SOC's). Deze handreiking is opgesteld voor Rijksorganisaties die voornemens zijn om SOC-diensten extern in te kopen.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor personen die betrokken zijn bij het opstellen van een aanbesteding voor SOC-diensten zoals behoeftestellers, inkopers en operationeel management.

1. Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	08-04-2025	Initiële versie
V1.1	09-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
HAVIK Kennisdocumenten	VSSR kennisdocumenten voor het aanbesteden van monitoring- en detectiediensten
VSSR Kennisdocumenten	VSSR (ncsc.nl)
PIANOo	https://www.pianoo.nl/nl
Rijksoverheid	https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/organisatie-rijksoverheid
Traffic Light Protocol	https://www.ncsc.nl/aansluiten-en-samenwerken/traffic-light-protocol-tlp

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. In dit document zijn definities met een hoofdletter geschreven.

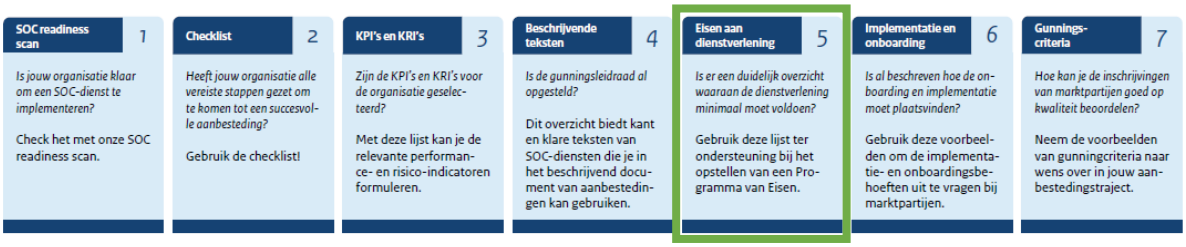
2. Inleiding

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, "*Eisen aan Dienstverlening*", maakt onderdeel uit van de HAVIK-toolbox. Alle kennisproducten uit de HAVIK-toolbox zijn op het VSSR portaal[1] te vinden.

Wij raden aan om voorafgaand aan gebruik van dit product in elk geval de SOC-Readiness scan uit te voeren en de checklist door te nemen. Verder wordt in dit document verwezen naar een Service Level Agreement (SLA). Het hulpmiddel "KPI's & KRI's" kunt u gebruiken ter ondersteuning bij het opstellen van het SLA.



Figuur 1 - Positie van dit product in HAVIK toolbox

2.2 Toepassing en reikwijdte

Dit kennisdocument richt zich op de ondersteuning bij het specificeren van minimale eisen voor SOC-diensten. Hiertoe bevat dit document een set aan basiseisen die als bron kunnen dienen bij het opstellen van een aanbesteding voor SOC-diensten. Dit document is opgesteld met het oog op organisaties die tot de Rijksoverheid behoren.

Dit document kan gebruikt worden bij zowel het uitvoeren van een volledige aanbesteding als bij het inkopen onder bestaande mantelovereenkomsten. In dit laatste geval zal een deel van de eisen die in dit document worden beschreven reeds in de betreffende mantelovereenkomst zijn vastgelegd. Voorkom tegenstrijdigheden en neem geen eisen over indien deze al in een mantelovereenkomst zijn vastgelegd.

Dit document richt zich op de technische, functionele en operationele aspecten van SOC-Dienstverlening. Andere eisen, bijvoorbeeld van aanbestedingsrechtelijke aard, zijn niet in dit document opgenomen. Dit document is opgesteld met als uitgangspunt dat er bij het gebruik en opstellen van aanbestedingsstukken ondersteuning is door professionals met kennis van inkopen en aanbesteden in generieke zin. Verder publiceert het Expertisecentrum Aanbesteden (PIANOo) van het ministerie van Economische Zaken nuttige Informatie over aanbesteden in algemene zin.

De eisen in dit document zijn gericht op het inkopen van SOC-Dienstverlening en minder geschikt voor het inkopen van SOC-producten.

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

3. Leeswijzer

3.1 Indeling categorieën

In de hoofdstukken 4 tot 9 zijn verschillende eisen uitgewerkt die in algemene zin voor organisaties die tot de Rijksoverheid behoren van toepassing zijn. In dit document is ervoor gekozen om de eisen in de volgende samenhangende categorieën onder te brengen:

- **Algemene eisen**
  Dit omvat eisen van algemene aard. Veelal zijn dit eisen die betrekking hebben op de organisatie van Opdrachtnemer, bijvoorbeeld eisen aan Personeel en vertrouwelijkheid van gegevens.

- **Eisen aan samenwerking en beheer**
  Deze categorie omvat eisen die betrekking hebben op de wijze waarop de Opdrachtnemer en Opdrachtgever in de uitvoering samenwerken. Denk hierbij aan eisen met betrekking tot het vastleggen van werkafspraken, het afhandelen van storingen en wijzigingsverzoeken, overlegstructuren, etc.

- **Eisen aan de Dienstverlening**
  De eisen in deze categorie gaan hebben specifiek betrekking op de SOC-Dienstverlening. Denk bijvoorbeeld aan eisen voor Triage, meldingen van security incidenten, gebruik van CTI, etc.

- **Eisen aan logdatabeheer**
  Deze categorie gaat in op de eisen die betrekking hebben op het verzamelen van Logdata en de wijze waarop deze Logdata van Opdrachtgever aan Opdrachtnemer wordt overgedragen. Eisen in deze categorie hebben betrekking op de wijze waarop Logdata wordt verzameld, demarcatiepunten, omvang van de te verzamelen Logdata, beveiligen van deze Logdata, maatregelen om continuïteit van het verzamelen te borgen, etc.

- **Eisen aan Implementatie en Onboarding**
  In het hoofdstuk Implementatie en Onboarding zijn de eisen beschreven die betrekking hebben op hetgeen nodig is om levering van de Dienstverlening mogelijk te maken. Er wordt onderscheid gemaakt tussen Implementatie en Onboarding. Implementatie richt zich primair op organisatorische en procesmatige aspecten die nodig zijn om de Dienstverlening te leveren. Denk hierbij aan het inrichten van processen, het maken van operationele afspraken, inrichten van communicatie- en escalatieafspraken, etc.
  Onboarding omvat de zaken die nodig zijn om de Assets die onderdeel van de Dienstverlening zijn aan te sluiten en technisch/functioneel in te regelen.
  Omdat Implementatie en Onboarding zijn op vele vlakken onlosmakelijk met elkaar verbonden en zijn daarom in één categorie opgenomen.

- **Eisen aan rapportages en kwaliteitsborging**
  In deze categorie zijn de minimale criteria beschreven die nodig zijn om als Opdrachtgever zicht te houden op de kwantiteit en kwaliteit van geleverde Prestatie en of de geleverde Prestatie voldoet aan de overeengekomen afspraken. Tevens zijn in deze categorie minimale criteria gespecificeerd die nodig zijn om de kwaliteit van de Prestatie op peil te houden en waar nodig bij te sturen.

U kunt deze of een soortgelijke onderverdeling in uw aanbesteding overnemen. De reden van dit onderverdelen is tweeledig. Enerzijds verhoogt een logische samenhang de leesbaarheid. Anderzijds zullen marktpartijen de werkzaamheden van een inschrijving veelal verdelen over experts binnen een organisatie. Deze indeling maakt het voor marktpartijen eenvoudiger om het werk binnen de organisatie te verdelen. Het staat u uiteraard vrij om in een aanbesteding een andere of geen onderverdeling aan te brengen.

3.2 Uitvoeringseisen

In aanbestedingen kan onderscheid gemaakt worden tussen zogenaamde uitvoeringseisen en geschiktheidseisen. Een geschiktheidseis betreft een eis waaraan een Inschrijver moet voldoen op het moment dat de Inschrijving wordt ingediend. Een uitvoeringseis is een eis waaraan een Inschrijver tijdens de uitvoering van de opdracht aan moet voldoen.

De eisen in dit document zijn uitvoeringseisen.

3.3 Samenhang met andere documenten

In dit document zijn een aantal eisen opgenomen die verwijzen naar andere aanbestedingsdocumenten. Een deel van deze documenten moet gelijktijdig met de aanbesteding worden gepubliceerd omdat de Inschrijver Informatie uit betreffende document nodig heeft om een Inschrijving te kunnen doen.

In onderstaande overzicht is weergegeven welke documenten bij publicatie van de aanbesteding beschikbaar gesteld moeten worden. De overige documenten worden na Gunning (door Opdrachtnemer) opgesteld.

Document	Beschikbaar bij publicatie
Service Level Agreement (SLA)	Ja
Dossier Afspraken en Procedures (DAP)	Nee
Protocol van Oplevering (PvO)	Nee
Inschalingsmatrix	Afhankelijk van de eis
Aansluitvoorwaarden NCSC CTI-feed	Ja
Assetoverzicht	Ja
Implementatie- en onboardingsplan	Nee
Kennisoverdrachtdocument	Nee

2.3.1 Inschalingsmatrix

Voor de Inschalingsmatrix kan ervoor gekozen worden deze vooraf kenbaar te maken, maar ook om deze na Gunning in overleg tussen de Opdrachtgever en Opdrachtnemer uit te werken.
Het op voorhand voorschrijven van de Inschalingsmatrix kan bijvoorbeeld aan de orde zijn als de aanbestedende dienst reeds over een SOC-dienst beschikt en de nieuwe overeenkomst als doel heeft deze dienst te continueren. Bij het op voorhand voorschrijven van een Inschalingsmatrix dient Opdrachtgever over voldoende expertise te beschikken om security incidenten te classificeren. Indien u de Inschalingsmatrix voorschrijft, dient u deze bij publicatie kenbaar te maken.

In andere gevallen kunt u ervoor kiezen om na Gunning in overleg tussen Opdrachtgever en Opdrachtnemer de Inschalingsmatrix op te stellen. In dit geval is er uiteraard geen sprake van publicatie van een Inschalingsmatrix ten tijde van een aanbesteding.

Verder is in de bijlage van dit document een overzicht opgenomen met eisen die naar documenten verwijzen en de onderwerpen die voor de betreffende eis in deze documenten beschreven moeten zijn c.q. worden.

3.4 Gebruik van de eisen

Bij elke eis zijn drie onderdelen gespecificeerd, te weten:

Ref: Referentienummer van de eis. Dit referentienummer kan gebruikt worden bij communicatie met het programma Versterken SOC-stelsel Rijk (VSSR).

Beschrijving: Beschrijving van de eis; dit is de basistekst die u kan overnemen in uw aanbesteding.

Toelichting: Een toelichting op de eis; dit is voor intern gebruik in uw organisatie.

- Elementen die in dit document <blauw> zijn gemarkeerd betreffen keuzes of specificaties die u als Opdrachtgever moet maken c.q. invullen.
- Afkortingen en termen die met een hoofdletter zijn geschreven, zijn in een lijst van definities en afkoringen opgenomen.

U dient zelf te bepalen in hoeverre de eisen die in dit document zijn geformuleerd voor uw organisatie c.q. aanbesteding van toepassing zijn. Betreffende eisen kunt u integraal overnemen, maar uiteraard ook in aangepaste vorm zodat ze specifieker aansluiten op de behoefte of omstandigheden van uw organisatie.

4 Algemene eisen

Dit hoofdstuk omvat eisen van algemene aard. De eisen in dit hoofdstuk hebben veelal betrekking op organisatorische en personele aspecten.

Ref	Beschrijving	Toelichting
A-01	Opdrachtnemer heeft voorafgaand aan de uitvoering van de Opdracht zich ervan vergewist en garandeert dat door hem in te zetten Personeel en/of hulppersonen geen integriteitsrisico's met zich meebrengen.	
A-02	Voor het Personeel dat Opdrachtnemer voornemens is deze bij de uitvoering van de opdracht te betrekken, stelt Opdrachtnemer stelt de identiteit van dit Personeel vast – ook op het aspect van de persoonsverwisseling – aan de hand van een geldig authentiek identiteitsbewijs. Indien van toepassing stelt Opdrachtnemer ook vast dat betrokken Personeel over een geldige verblijfs- of tewerkstellingsvergunning beschikt. De bij de Opdrachtgever ingezette professional(s) moet(en) zichzelf op verzoek van de Opdrachtgever kunnen identificeren (bij werkzaamheden op locatie van de Opdrachtgever).	
A-03	Opdrachtnemer zorgt ervoor dat Personeel dat voor deze opdracht wordt ingezet beschikt over een verklaring omtrent gedrag (VOG) of een vergelijkbare verklaring uit het land van herkomst voor Personeel met buitenlandse nationaliteit. De VOG dient betrekking te hebben op de volgende screeningsprofielen: <invullen>. De VOG mag maximaal <één jaar> oud zijn. Opdrachtnemer voert een administratie en zorgt voor tijdige vernieuwing.	Meer Informatie over screeningsprofielen vind u hier: https://justis.nl/producten/verklaring-omtrent-het-gedrag/vog-voor-werkgevers-en-organisaties/screeningsprofielen Een VOG kent geen geldigheidsduur, het is enkel een weergave situatie op het moment van afgifte. Het is verstandig om als Opdrachtgever een norm te stellen aan maximale ouderdom en vernieuwen van de VOG.
A-04	Indien met betrekking tot de uitvoering van de Opdracht sprake is van (potentiële) toegang tot vertrouwelijke gegevens, of dat Opdrachtgever het om andere redenen nodig vindt om een veiligheidsonderzoek uit te laten voeren, kan van het in te zetten Personeel een Verklaring van Geen Bezwaar (VGB) worden verlangd. Opdrachtnemer gaat hiermee akkoord.	
A-05	Opdrachtnemer draagt er zorg voor dat Personeel die locaties van Opdrachtnemer bezoekt, de VOG c.q. VGB altijd bij zich dragen en deze op eerste verzoek onverwijld overleggen aan een functionaris van Opdrachtgever.	
A-06	Opdrachtnemer zorgt ervoor dat gegevens van Opdrachtgever uitsluitend toegankelijk is voor Personeel dat betrokken is bij de uitvoering van de Overeenkomst en voor zover toegang tot gegevens in het kader uit te voeren werkzaamheden nodig is (need-to-know principe). Opdrachtnemer neemt maatregelen om ongeautoriseerde toegang tot gegevens van Opdrachtgever te voorkomen.	
A-07	Opdrachtgever hanteert een aantal ICT-/IV-kaders, waaraan Opdrachtnemer zich dient te conformeren. Opdrachtnemer is bereid om de Prestatie af te stemmen op de (referentie)architecturen, technologie standaarden, principes en bouwstenen binnen het ICT-/IV-domein van de Opdrachtgever, alsmede mogelijke wijzigingen daarin, om de Prestatie goed in te kunnen passen binnen de ICT-/IV-kaders. Het betreft de volgende kaders en standaarden, inclusief hun opvolgers:	

Ref	Beschrijving	Toelichting
	a. NORA (www.noraonline.nl en www.digitaleoverheid.nl/onderwerpen/nora) b. Beveiligingsvoorschrift Rijksdienst (BVR) 2013, het Besluit voorschrift informatiebeveiliging rijksdienst (VIR) 2007, het Besluit voorschrift informatiebeveiliging Rijksoverheid – bijzondere informatie (VIRBI) 2013, de Baseline Informatiebeveiliging Overheid (BIO) c. Cyberbeveiligingswet (NIS2) https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/nis2-wbni2 d. Traffic Light Protocol (TLP): https://www.ncsc.nl/aansluiten-en-samenwerken/traffic-light-protocol-tlp	Neem in dit overzicht de bronnen en standaarden op die relevant zijn voor uitvoering van de opdracht.
A-08	In het geval van een vermoedelijk of geconstateerd incident, waarin bij de uitvoering van een Overeenkomst niet voldaan wordt aan de daarvoor geldende ICT/IV-kaders of wetgeving, dient Opdrachtnemer dit onverwijld te melden aan Opdrachtgever.	
A-09	Opdrachtnemer zorgt voor actuele kennis van ontwikkelingen in het vakgebied die relevant zijn binnen het domein van Dienstverlening die Opdrachtnemer uitvoert voor Opdrachtgever. Deze kennis is aanwezig binnen de organisatie van Opdrachtnemer en wordt actief overgedragen aan het Personeel van partijen en andere betrokkenen die als zodanig worden aangewezen door de Opdrachtgever.	
A-10	Alle voor de Overeenkomst benodigde data die door of namens Opdrachtgever wordt verwerkt buiten de omgevingen van Opdrachtgever, dient binnen het grondgebied waarop de Europese regelgeving van toepassing is, opgeslagen en verwerkt te worden.	
A-11	Opdrachtnemer zal als onderdeel van de Prestatie die activiteiten verrichten die beschreven zijn in de Overeenkomst (dus inclusief de bijlagen, waaronder aanbestedingsdocumenten, Nota's van Inlichtingen, Prijsopgaven et cetera). Dit omvat ook activiteiten en voorzieningen die daaruit volgen of noodzakelijk zijn om de Prestatie conform de Overeenkomst te verrichten, ook als die activiteiten of voorzieningen niet expliciet zijn beschreven.	
A-12	Opdrachtnemer maakt binnen <periode> na aanvang van de Opdracht afspraken met Opdrachtgever omtrent benodigde maatregelen voor kennisoverdracht en borging van de continuïteit van de Dienstverlening na beëindiging van de Opdracht. Opdrachtnemer valideert deze afspraken tenminste jaarlijks met Opdrachtgever en Opdrachtnemer werkt proactief aan tussentijdse kennisoverdracht aan Opdrachtgever. Vóór het eindigen van de Overeenkomst (inclusief eventuele verlengingen) draagt Opdrachtnemer alle relevante gegevens die zijn verzameld en/of ontwikkeld tijdens diens inzet over aan de Opdrachtgever. Na deze overdracht wordt alle gegevens vernietigd met uitzondering van gegevens waarvoor een wettelijke grondslag bestaat om deze te bewaren.	Optioneel kan deze jaarlijkse validatie worden opgenomen. Kan worden weggelaten als dit als een te grote last wordt gezien of onvoldoende toegevoegde waarde biedt.
A-13	Opdrachtnemer gaat ermee akkoord dat Opdrachtgever testen op de Dienstverlening uitvoert of uit laat voeren. Als voorbeeld kan gedacht worden aan o.a. penetratietesten en redteam testen. Opdrachtgever bepaalt per geval of hij Opdrachtnemer al dan niet vooraf in kennis stelt van dergelijke testen.	Het gaat om uitvoeren van dergelijke testen op systemen van Opdrachtgever zelf. Met dergelijke testen kan onderzocht worden of de SOC-dienstverlener dergelijke testen/aanvallen op systemen van Opdrachtgever detecteert.

Ref	Beschrijving	Toelichting
A-14	<Eisen aan Facturering> Beschrijf de basis waarop de kosten worden gebaseerd? Bijvoorbeeld: prijzenblad Inschrijving (P) * assetoverzicht (Q) Om fluctuaties in kosten te beperken kan overwogen worden om de te factureren kosten éénmaal per kwartaal bij te stellen obv het actuele assetoverzicht, tenzij er wijzigingen zijn die leiden tot een kostenafwijking die groter is dan 5%. In dat geval kan de wijziging in de eerstvolgende kalendermaand worden verwerkt.	Beschrijf de eisen hoe kosten gespecificeerd moeten worden en waaraan facturen moeten voldoen om betaalbaar gesteld te worden. Beschrijf ook het proces dat gevolgd wordt indien een factuur niet betaalbaar gesteld kan worden. Tevens zijn hier enkele overwegingen opgenomen die u kunt meenemen in deze eis.
A-15	Opdrachtgever beschikt over <specificatie> licenties. Deze licenties omvatten componenten die voor monitoring en detectie ingezet kunnen worden. Het is Opdrachtnemer <WEL/NIET> toegestaan om hier gebruik van deze licenties maken.	Optioneel: Mogelijk beschikt uw organisatie over licenties waarin Monitoring en Detectie/SIEM functionaliteit is opgenomen, zoals bijvoorbeeld Microsoft E5 licenties. Bedenk vooraf wat de voor- en nadelen zijn om dergelijke licenties te gebruiken. Indien u het gebruik van bestaande licenties toestaat, zal er minder onderscheid zijn in het aanbod. Oplossingen met andere producten (waar licenties voor nodig zijn), zijn dan immers o.b.v. prijs niet kansrijk. Daarnaast zal een aantal marktpartijen afvallen omdat niet elke marktpartij Dienstverlening op deze wijze kan of wil leveren. De constructie met het gebruik van door Opdrachtgever aangeschafte licenties kan in situaties met een hybride SOC van nut zijn, omdat op deze wijze de tooling van Opdrachtgever is en zowel de dienstverlener als de eigen organisatie hier gebruik van kan maken zonder dat dit conflicten met andere klanten van de SOC-dienstverlener oplevert.
A-16	Opdrachtnemer gaat ermee akkoord dat alle documentatie, data, administratie, methoden en technieken die gedurende het uitvoeren van de Prestatie worden opgebouwd of door Opdrachtgever zijn ingebracht, eigendom zijn van Opdrachtgever. Bij beëindiging van de Overeenkomst worden deze zonder kosten, in elektronische vorm en in een gangbaar bewerkbaar formaat, overgedragen aan (een derde partij aan te wijzen door) Opdrachtgever.	Het gaat hier over kennis die gedurende de uitvoering door Opdrachtgever wordt ingebracht of o.b.v. van geleverde Prestatie wordt opgebouwd. Denk bijvoorbeeld aan organisatie-specifieke Use Cases/Detectieregels.

5 Eisen aan samenwerking en beheer

Dit hoofdstuk omvat eisen die betrekking hebben op de wijze waarop de Opdrachtnemer en Opdrachtgever in de uitvoering samenwerken. Denk hierbij aan eisen met betrekking tot het vastleggen van werkafspraken, afstemming, het afhandelen van storingen en wijzigingsverzoeken, overlegstructuren, etc.

Ref	Beschrijving	Toelichting
SB-01	Opdrachtnemer stelt een Servicemanager (of iemand in vergelijkbare functie) met voldoende mandaat aan. Deze Servicemanager is voor Opdrachtgever het centrale aanspreekpunt en coördineert de Prestatie voor Opdrachtgever, draagt zorg voor (toezicht op) naleving van de Overeenkomst en houdt toezicht op de kwaliteit van de totale Prestatie van Opdrachtnemer. Deze persoon dient telefonisch en per e-mail goed bereikbaar te zijn. Opdrachtnemer zorgt voor gemandateerde en minstens gelijkwaardige vervanging bij afwezigheid van de vaste contactpersoon, hetgeen tijdig kenbaar wordt gemaakt.	
SB-02	Alle operationele afspraken worden vastgelegd in een Dossier Afspraken en Procedures (DAP). Het DAP bevat tenminste de beschrijving van taken, verantwoordelijkheden, processen, procedures en contactgegevens. De afspraken in het DAP dienen te voldoen aan hetgeen is vastgelegd in de Overeenkomst. Opdrachtnemer zal binnen <periode> na Gunning het DAP opstellen en deze met Opdrachtgever delen. Opdrachtnemer zal het DAP gedurende de duur van de Overeenkomst actueel houden. De inhoud van de DAP wordt altijd afgestemd met Opdrachtgever.	
SB-03	Opdrachtnemer levert alle documenten in de Nederlandse taal. Alleen indien Opdrachtgever op voorhand schriftelijke toestemming heeft verstrekt mag hiervan worden afgeweken.	Overweeg om specialistische technische documentatie en Informatie in het Engels toe te staan.
SB-04	Het door Opdrachtnemer in te zetten Personeel - voor zover zij betrokken zijn in de communicatie met Opdrachtgever – beheerst de Nederlandse taal. Alleen indien vooraf expliciet anders is overeengekomen mag hiervan worden afgeweken. Opdrachtnemer verzekert zich hier zo nodig van voorafgaande aan het uitbrengen van een Offerte en uitvoeren van werkzaamheden. Opdrachtnemer gaat ermee akkoord dat Opdrachtgever de inzet van Personeel dat de Nederlandse taal onvoldoende beheerst mag weigeren als hij hiermee risico's of knelpunten in de uitvoering van de Overeenkomst of bruikbaarheid van de Prestatie voorziet.	
SB-05	Alle interactie tussen Opdrachtgever en Opdrachtnemer verloopt via personen die hiertoe gemandateerd zijn. Opdrachtnemer ziet er op toe dat alleen met gemandateerde contactpersonen wordt gecommuniceerd. In het DAP wordt een communicatiematrix opgenomen waarin de contactpersonen, rol en mandaat zijn vastgelegd. Tevens is er in de DAP een escalatiemodel opgenomen waarin de escalatieprocedure, -niveaus en contactpersonen cq rollen zijn beschreven. Opdrachtnemer zal deze communicatiematrix en escalatiemodel opstellen en onderhouden.	

Ref	Beschrijving	Toelichting
SB-06	Opdrachtnemer biedt een SOC aan dat functioneert als één centraal aanspreekpunt voor Security Operations gerelateerde zaken. Opdrachtnemer biedt tenminste de volgende mogelijkheden om contact te leggen met het SOC: • Telefonisch; • Per mail. • Voorziening om veilig gegevens uit te wisselen (zie eis SB-16) De vereiste responsetijden zijn in het Service Level Agreement vastgelegd. Opdrachtnemer dient Opdrachtgever directe (online) toegang te bieden tot de gegevens van Opdrachtgever die in of via de monitoringsystemen beschikbaar zijn. Deze gegevens omvatten minimaal de Logdata. Het doel hiervan is dat Opdrachtgever deze gegevens kan doorzoeken (queries uitvoeren). Het doel hiervan is het ondersteunen van Opdrachtgever bij het uitvoeren van werkzaamheden zoals bijvoorbeeld incident response en threat hunting.	
SB-07	Opdrachtnemer biedt één centraal aanspreekpunt (servicedesk) voor niet Security Operations gerelateerde vraagstukken. Denk storingen, informatieverzoeken, offerteaanvragen, onderhoudsvragen, wijzigingsverzoeken en andere verzoeken m.b.t. de Prestatie. Deze servicedesk hanteert een gestandaardiseerde werkwijze, voert administratie over de serviceprocessen en draagt zorg voor de processturing. De processturing is zodanig dat de overeengekomen kwaliteit conform SLA geborgd is. Opdrachtnemer biedt tenminste de volgende mogelijkheden om met dit aanmeldpunt contact op te nemen: • Telefonisch; • Per mail; • Een portaal. De vereiste responsetijden zijn het in het Service Level Agreement vastgelegd.	
SB-08	Opdrachtnemer is verplicht om bij storingen, maar ook tijdens reguliere operationele activiteiten, samen te werken met relevante partijen om een optimaal functioneren van de Prestatie te waarborgen. Deze samenwerking omvat het – met toestemming van Opdrachtgever - delen van relevante Informatie, ondersteunen bij testen, het verlenen van toegang tot benodigde systemen en gegevens, en het actief bijdragen aan herstel- en verbeterwerkzaamheden.	
SB-09	Opdrachtnemer dient als onderdeel van de Prestatie onderhoud uit te voeren op alle systemen, componenten, applicatie(s), etc. die ten behoeve van het leveren van de Prestatie worden ingezet. Dit omvat ook systemen, componenten en applicaties die door Opdrachtnemer bij Opdrachtgever in bedrijf zijn gesteld. Het onderhoud is zodanig ingericht dat de Prestatie voor de volledige duur van de Overeenkomst voldoet aan hetgeen in de Overeenkomst is vastgelegd.	
SB-10	Opdrachtnemer zal wijzigingen en onderhoudswerkzaamheden op de eigen systemen, componenten en applicaties zodanig organiseren dat de impact voor Opdrachtgever zo klein mogelijk is. Opdrachtnemer kondigt het onderhoud aan volgens procedure en normen die in de DAP en SLA zijn vastgelegd.	

Ref	Beschrijving	Toelichting
SB-11	Opdrachtnemer is verantwoordelijk voor de operationele continuïteit en veiligheid van systemen en componenten die voor het leveren van de Prestatie worden ingezet. Opdrachtnemer heeft passende maatregelen ingericht om deze verantwoordelijkheid adequaat in te vullen.	Opdrachtnemer krijgt voor het uitvoeren van de dienst toegang tot veel cruciale gegevens van Opdrachtgever. Dat maakt het noodzakelijk dat ook het monitorsysteem (en andere componenten) die voor de Prestatie worden ingezet ook zelf worden gemonitord, gepatched, etc. Passende maatregelen beperken zich niet enkel tot techniek. Zo is bijvoorbeeld het hebben van achtervang ook een maatregel voor continuïteit en een goed wachtwoordenbeleid relevant voor informatiebeveiliging.
SB-12	Opdrachtnemer initieert periodiek een operationeel overleg tussen Opdrachtgever en Opdrachtnemer waarin de rapportages en Prestatie op operationeel niveau wordt geëvalueerd en potentiële verbeteringen worden besproken. Nadere afspraken over dit overleg zijn in het DAP vastgelegd.	Leg in de DAP vast met welke frequentie het operationeel overleg moet plaatsvinden en eventueel andere criteria waaraan het operationeel overleg moet voldoen, bijvoorbeeld te bespreken onderwerpen.
SB-13	Opdrachtnemer initieert periodiek een tactisch overleg tussen Opdrachtgever en Opdrachtnemer. Dit overleg heeft als doel om te evalueren of de Prestatie en rapportages nog voldoende aansluiten bij behoefte van partijen en eventuele verbeterpunten te identificeren. Op basis van de resultaten uit dit evaluatie-overleg zal Opdrachtnemer - indien van toepassing - optimalisaties doorvoeren. Nadere afspraken over dit overleg zijn in het DAP vastgelegd.	Leg in de DAP vast met welke frequentie het tactisch overleg moet plaatsvinden en eventueel andere criteria waaraan het tactisch overleg moet voldoen, bijvoorbeeld te bespreken onderwerpen.
SB-14	Periodiek initieert Opdrachtnemer een strategisch overleg tussen Opdrachtgever en Opdrachtnemer. Doelstelling van dit overleg is de relatie en samenwerking tussen Opdrachtgever en Opdrachtnemer te evalueren en optimaliseren. Tevens wordt dit overleg gebruikt om te evalueren of de overeenkomst en Prestatie nog voldoende aansluit bij de doelstellingen van Opdrachtgever. Nadere afspraken over dit overleg zijn in het DAP vastgelegd.	Leg in de DAP vast met welke frequentie het tactisch overleg moet plaatsvinden en eventueel andere criteria waaraan het strategisch overleg moet voldoen.
SB-15	Van elk overleg maakt Opdrachtnemer binnen drie (3) Werkdagen een conceptverslag waarin besproken punten en actiepunten worden vastgelegd. Opdrachtnemer legt conceptverslag per e-mail voor aan Opdrachtgever. Na goedkeuring door Opdrachtgever wordt het verslag vastgesteld.	Als alternatief kan je als Opdrachtgever zelf verslag te maken. Dit is een extra inspanning, maar zorgt dat je zelf meer 'in control' bent.
SB-16	Opdrachtnemer biedt een voorziening om op elektronische wijze veilig bestanden (zoals Word/LibreOffice, pdf, logbestanden, zip-bestanden) uit te wisselen. Deze voorziening hanteert het zogenaamde need-to-know principe. Dit wil onder andere zeggen dat er met persoonlijke accounts wordt gewerkt. Het systeem omvat Logging zodat de uitwisseling van bestanden ook achteraf herleidbaar is. De Logging wordt tenminste voor twee jaar bewaard. Opdrachtnemer stelt een gebruikershandleiding en relevante processen ter ondersteuning beschikbaar en onderhoud deze gedurende de contractperiode. --- <of> --- Opdrachtnemer zal voor het uitwisselen van gevoelige en vertrouwelijke gegevens met Opdrachtgever gebruik maken van <systeemnaam> dat door Opdrachtgever beschikbaar wordt gesteld.	Gedurende de uitvoering van de overeenkomst zal er gevoelige en vertrouwelijke gegevens uitgewisseld worden waarvoor standaard voorzieningen zoals e-mail niet volstaan. Maak hier een keuze tussen een dergelijke systeem als onderdeel dan de Prestatie laten aanbieden of voorschrijven dat een systeem dat Opdrachtgever beschikbaar stelt wordt gebruikt.

Ref	Beschrijving	Toelichting
SB-17	ICT-omgevingen zijn niet statisch. Wijzigingen in de ICT-omgeving van Opdrachtgever kunnen impact hebben op de Prestatie. Denk aan uitbreiden, uitfaseren en migraties van ICT-systemen, transitie van en naar cloud, het verwerven of afstoten van locaties, etc. Opdrachtgever zal dergelijke wijzigingen aan Opdrachtnemer kenbaar maken. Opdrachtnemer neemt passende maatregelen zodat de Prestatie, ook na dergelijke wijzigingen, gecontinueerd wordt. Opdrachtnemer neemt hiervoor in het DAP een wijzigingsproces op waarin beschreven is op welke wijze wijzigingen gecontroleerd worden verwerkt in de Prestatie. Hierbij wordt in elk geval onderscheid gemaakt tussen standaard wijzigingen (bijvoorbeeld een asset toevoegen of verwijderen) en grootschalige of complexe wijzigingen die een projectmatige aanpak vergen. Opdrachtnemer zorgt er tevens voor dat na Oplevering de facturering conform afspraken aangepast wordt aan de gewijzigde situatie.	Aanpassingen in de ICT-infrastructuur van Opdrachtgever kunnen leiden dat de monitoring niet langer goed of volledig werkt. Daarom is het noodzakelijk om (relevante) changes in de infrastructuur aan Opdrachtnemer kenbaar te maken.

6 Eisen aan Dienstverlening

Dit hoofdstuk beschrijft eisen die specifiek betrekking hebben op de SOC-Dienstverlening zelf. Denk bijvoorbeeld aan eisen voor Triage, meldingen van security incidenten, gebruik van CTI, etc.

Ref	Beschrijving	Toelichting
DV-01	De SOC-diensten en alle onderdelen ervan voldoen aan de algemene verwachtingen die opdrachtgever, gezien wat gangbaar is voor dit soort SOC-diensten, gezien de betreffende markt en gezien andere vergelijkbare SOC-diensten, aan SOC-diensten mag hebben. Dit in ieder geval ook voor wat betreft de Prestatie waaronder maar niet beperkt tot: Implementatie, Onboarding, training, informatiebeveiliging, logdatabeheer, vakkundigheid, degelijkheid, betrouwbaarheid, onderhoud, functionaliteit, logdatabeheer, klanttevredenheid, gebruikservaring, Total Cost of Ownership, innovaties, marktontwikkelingen, etc.	
DV-02	Opdrachtnemer is verantwoordelijk voor de kwaliteit, beschikbaarheid en continuïteit van de Prestatie. In het Service Level Agreement zijn de Dienstenniveaus, inclusief bijbehorende normen en de wijze van meten, beschreven. Opdrachtnemer zal voldoen aan de opgegeven specificaties en Dienstenniveaus zoals vastgelegd in het Service Level Agreement.	Voeg een concept SLA aan de aanbestedingsstukken toe. VSSR heeft een KPI/KRI document waarin potentiële Key Performance en Risico Indicatoren geïdentificeerd zijn. Dit document kan als ondersteuning worden gebruikt bij het opstellen van een concept-SLA.
DV-03	De medewerkers die bij het SOC werkzaam zijn beschikken over de nodige kennis en vaardigheden om de Opdrachtnemer te ondersteunen binnen de specifieke context van de Dienstverlening.	
DV-04	Opdrachtnemer beschikt over specialisten en zet deze in bij meer complexe zaken die het kennisniveau van de eerste lijn medewerkers van Opdrachtnemer overstijgen. Opdrachtgever heeft toegang tot deze specialisten. In de communicatiematrix is vastgelegd welke personen hiervoor mandaat hebben.	
DV-05	Alvorens Opdrachtnemer bij Opdrachtgever melding maakt van een (potentieel) beveiligingsincident voert Opdrachtnemer Triage uit. Onderdeel van deze Triage is het uitfilteren van zogenaamde False Positives en het toekennen van de juiste prioriteit op basis van de overeengekomen Inschalingsmatrix. Opdrachtnemer meldt (potentiële) beveiligingsincidenten die volgens de Inschalingsmatrix als prioriteit 1 zijn ingeschaald altijd telefonisch bij Opdrachtgever.	Zie IO-03 voor Inschalingsmatrix Houdt er rekening mee dat bij 24/7 dienstverlening, Opdrachtgever ook 24/7 bereikbaar moet zijn tenzij hierover moeten afwijkende afspraken zijn gemaakt.
DV-06	Opdrachtnemer zorgt ervoor dat meldingen van een (potentieel) beveiligingsincident of dreiging op een gestandaardiseerde wijze worden gecommuniceerd. Tevens zijn dergelijke meldingen ten alle tijden vergezeld van Handelingsperspectief. Opdrachtnemer stemt de afspraken hierover af met Opdrachtgever en legt deze vast in het DAP.	

Ref	Beschrijving	Toelichting
DV-07	Opdrachtnemer dient Use Cases (Detectieregels/logica) te onderhouden. Denk hierbij aan het periodiek actualiseren, toevoegen van nieuwe Use Cases en het opruimen van oude niet meer in gebruik zijnde Use Cases. Ook bewaakt opdrachtnemer of alle randvoorwaarden, bijvoorbeeld actuele parameters en logbronnen, nog aanwezig zijn zodat de Use Cases getriggerd kunnen worden. De normen die hierop van toepassing zijn, zijn in het SLA vastgelegd.	
DV-08	Gedurende de uitvoering van de overeenkomst kan Opdrachtgever aan Opdrachtnemer verzoeken om de Dienstverlening af te stemmen op actuele en specifieke dreigingsbeelden. Optioneel kan een dergelijk voorzien zijn van specifieke Use Cases. Specifieke Use Cases betreffen Detectieregels die specifiek zijn voor een bepaalde situatie en/of voor de organisatie van Opdrachtgever. Opdrachtnemer zal een dergelijk verzoek honoreren en implementeren in zijn monitoringsystemen mits dat redelijkerwijs mogelijk is. Indien het verzoek niet uitvoerbaar is, dient Opdrachtgever dit schriftelijk onderbouwd te motiveren.	Neem in het prijzenblad de mogelijkheid op om kosten hiervoor in rekening te laten brengen.
DV-09	Het NCSC stelt aan organisaties die tot de Rijksoverheid behoren CTI-feeds beschikbaar. Deze CTI-feeds bevatten Indicators of Compromise (IoC's). In bijlage X zijn de aansluitvoorwaarden van deze CTI-feed beschreven. Opdrachtgever kan bij of na Gunning verzoeken om deze CTI-feed in de door Opdrachtnemer te leveren Prestatie op te nemen. Dat wil zeggen dat Opdrachtnemer de monitoringsystemen voor de Prestatie zo inricht dat deze (relevante) IoC's signaleert. Deze signaleringen worden ook wel Sightings genoemd. Opdrachtnemer zal een dergelijk verzoek honoreren en binnen vier weken na verzoek realiseren.	Voeg de aansluitvoorwaarden van het NCSC toe.
DV-10	Indien gebruik wordt gemaakt van de CTI-feed zoals beschreven in DV-09 en Opdrachtgever dit wenst, zal Opdrachtnemer Sightings op basis van de door NCSC beschikbaar gestelde CTI-feed(s) terugmelden aan het NCSC. Terugmelden vindt plaats via de aansluiting en aansluitvoorwaarden zoals in eis DV-09 is beschreven. Uitgangspunt is dat het terugmelden van Sightings geautomatiseerd plaatsvindt en dat Opdrachtnemer geen handmatige inspanningen hoeft te verrichten voor bijvoorbeeld Triage van terugmeldingen.	
DV-11	Opdrachtnemer voert jaarlijks een self-assessment uit waarin hij de Prestatie op basis van eigen inzichten evalueert ("hoe vindt u zelf dat het gaat") en rapporteert hierover aan Opdrachtgever. Deze rapportage mag Opdrachtnemer geheel naar eigen inzicht opstellen. Voor dit self-assessment is Opdrachtnemer vrij om onderwerpen te beschrijven. Onderwerpen hoeven niet enkel betrekking te hebben op eigen verantwoordelijkheid, maar kunnen ook gaan over de samenwerking met of pijnpunten bij/door Opdrachtgever. Opdrachtgever zal aangedragen verbeterpunten die op zijn organisatie betrekking hebben evalueren op kosten, baten, haalbaarheid en wenselijkheid. Op basis van deze evaluatie zal Opdrachtgever dergelijke verbeterpunten wel, niet of gedeeltelijk doorvoeren. Het al dan niet implementeren van voorgestelde verbeterpunten ontslaat Opdrachtnemer niet van haar verplichtingen met betrekking tot de te leveren Prestatie.	Dit is een volledig free format rapportage waarin Opdrachtgever zijn inzichten over de Prestatie met Opdrachtgever kan delen. Doelstelling hiervan is inzichten te krijgen die via reguliere rapportages niet zichtbaar worden en op die wijze de Prestatie en samenwerking te optimaliseren.

7. Eisen aan Logdatabeheer

In dit hoofdstuk zijn eisen beschreven die betrekking hebben op het verzamelen van Logdata en de wijze waarop deze Logdata van Opdrachtgever aan Opdrachtnemer wordt overgedragen. Denk aan eisen die betrekking hebben op het verzamelen, overdragen en verwerken van Logdata, beveiliging van deze Logdata, etc.

Ref	Beschrijving	Toelichting
LDB-01	Opdrachtnemer is verantwoordelijk voor het verwerken van Logdata uit alle Assets zoals gespecificeerd in bijlage <Bijlage XX (Assetoverzicht)>. In dit Assetoverzicht is voor elke asset gespecificeerd waar het demarcatiepunt ligt.	Als onderdeel van de aanbesteding moet gespecificeerd zijn welke ICT-componenten gemonitord moeten worden. Neem hiervoor een Assetoverzicht in de aanbesteding op.
LDB-02	Opdrachtnemer specificeert in zijn Inschrijving wat er van Opdrachtgever nodig is om de Prestatie te leveren. Denk bijvoorbeeld aan eisen die aan logbronnen worden gesteld, zoals het detailniveau van Logging; de wijze waarop Logdata vanuit Opdrachtgever bij Opdrachtnemer komt; software en componenten die in de IT-infrastructuur van Opdrachtgever geplaatst worden, etc. Opdrachtnemer zal het 'need to know' principe en efficiëntie toe passen. Dat wil zeggen dat Opdrachtnemer niet om meer gegevens en Logging zal vragen dan strikt noodzakelijk om de gevraagde Prestatie te leveren. Daarnaast neemt Opdrachtnemer maatregelen om de werking van systemen van Opdrachtgever niet te verstoren en de systemen niet meer te belasten dan strikt noodzakelijk voor het uitvoeren van de Prestatie. Indien er geen sprake is van een beveiligingsincidenten, zal de werking van de te monitoring Assets niet merkbaar verslechteren door de aangeboden Prestatie. De aangeboden oplossing is in staat om een teveel aan Logdata te filteren (in zowel volume als frequentie) alvorens de Logdata in monitoringsystemen verwerkt wordt.	
LDB-03	Opdrachtnemer richt op locatie van Opdrachtgever een centraal verzamelpunt van Logdata in. De koppeling tussen systemen van Opdrachtnemer en Opdrachtgever verlopen via deze koppeling. Om te koppelen met logbronnen van Opdrachtgever, ondersteunt dit verzamelpunt verschillende gangbare methoden en protocollen zoals Syslog, NCSA, Common Event Format (CEF), JSON, REST APIs, Windows Event Forwarding, etc.	
LDB-04	Opdrachtnemer beheert Logdata (Assets, logs, detecties, gegevens, etc.) en bewaakt pro-actief de geleverde Prestatie. Bij storingen neemt Opdrachtnemer direct corrigerende maatregelen. Opdrachtnemer rapporteert tijdig over de voortgang en herstelacties en neemt preventieve maatregelen om herhaling te voorkomen. Indien de oorzaak zich in systemen van Opdrachtgever bevindt, zal Opdrachtnemer hiervan melding maken bij Opdrachtgever.	
LDB-05	Opdrachtnemer zorgt ervoor dat Opdrachtgever ten alle tijde inzicht kan krijgen in de Logdata die in het kader van de Prestatie is vastgelegd. Opdrachtnemer zal aan een dergelijk verzoek onvoorwaardelijk meewerken.	Dit kan bijvoorbeeld noodzakelijk zijn als Opdrachtgever onderzoek wenst uit te voeren naar incidenten of voor trouble shooting-doeleinden.
LDB-06	Opdrachtnemer zorgt ervoor dat de integriteit van Logdata onomstotelijk vaststaat. Dit kan bijvoorbeeld nodig zijn voor forensisch onderzoek bij een incident. Deze verantwoordelijkheid start vanaf het demarcatiepunt waar de Logdata is overgedragen aan Opdrachtnemer.	

Ref	Beschrijving	Toelichting
LDB-07	Opdrachtgever zorgt dat Logdata, Detectieregels, gegevens, etc. goed overdraagbaar zijn. Opdrachtnemer zal op eerste verzoek van Opdrachtgever deze gegevens onvoorwaardelijk en uiterlijk binnen 14 dagen aan Opdrachtgever beschikbaar stellen in een gangbaar elektronisch open formaat, zodanig dat deze gegevens in geautomatiseerde systemen kan worden ingelezen. Afspraken, processen en procedures hieromtrent worden vastgelegd in de afspraken voor kennisoverdracht zoals beschreven onder eis A13.	

8. Eisen aan Implementatie en Onboarding

Dit hoofdstuk beschrijft een aantal eisen die aan onboarding en implementatie gesteld kunnen worden. Implementatie richt zich meer op de organisatorische en procesmatige aspecten die nodig zijn om de Dienstverlening in te richten. Onboarding richt zich op het technisch/functioneel aansluiten en inregelen van de Dienstverlening.

Ref	Beschrijving	Toelichting
IO-01	Opdrachtnemer dient direct na Gunning een implementatie- en onboardingsplan op te stellen. Het implementatieplan beschrijft alle activiteiten, afspraken, processen, doorlooptijden, benodigde randvoorwaarden, milestones, oplevermomenten, acceptatieprocedures, etc. die nodig zijn voor Implementatie van de Dienstverleningsprocessen. Het onboardingsplan beschrijft hetzelfde maar is gericht op het technisch aansluiten van Assets en het technisch inrichten en operationaliseren van de dienst. Daar waar activiteiten impact hebben op Opdrachtgever, worden deze vooraf afgestemd met Opdrachtgever. Het implementatie- en onboardingsplan worden ter kennisgeving aan Opdrachtgever beschikbaar gesteld.	Er kan voor gekozen worden om in plaats van deze eis als Subgunningscriterium een concept implementatie- en onboardingsplan bij de inschrijving te laten indienen. En/of Een verificatiefase in de aanbesteding opnemen waarbij ruimte ontstaat om het implementatie- en onboardignsplan te bespreken voorafgaand aan Gunning. Hiermee zijn vervelende verrassingen gedurende implementatiefase te voorkomen.
IO-02	Opdrachtnemer beschrijft in het implementatie- en onboardingsplan duidelijk en concreet de acties en inspanningen die van Opdrachtgever worden verwacht. Denk bijvoorbeeld aan het aanleveren van bepaalde Informatie, betrokkenheid bij testen, etc. Opdrachtnemer streeft naar het minimaliseren van de inspanningen door Opdrachtgever. Dit minimaliseren van inspanningen is erop gericht de Opdrachtgever te ontlasten, maar mag geen afbreuk doet aan de samenwerking en kwaliteit van de Prestatie. Opdrachtnemer beschrijft op welke momenten inspanningen van Opdrachtgever nodig zijn, wat er van Opdrachtgever verwacht wordt en een raming van het aantal uren dat voor deze inspanningen worden voorzien.	Deze eis beperkt zich tot het specificeren. Er kan op basis van deze eis geen onderscheid gemaakt worden tussen inschrijvers die veel en weinig inspanningen van Opdrachtgever vragen. Overweeg daarom om in de aanbesteding ook een Subgunningscriterium op te nemen waarbij een inschrijving positiever wordt beoordeeld naarmate er minder inspanningen van Opdrachtgever worden gevraagd.
IO-03	Als onderdeel van de implementatiefase zal Opdrachtnemer, in overleg met Opdrachtgever, een Inschalingsmatrix opstellen. Deze Inschalingsmatrix is het referentiekader om te bepalen welke prioriteit er aan meldingen van (potentiële) securityincidenten worden toegekend. Opdrachtnemer zal deze Inschalingsmatrix jaarlijks met Opdrachtgever evalueren en zo nodig actualiseren.	Maak een keuze om de Inschalingsmatrix na Gunning in door leverancier op te laten stellen of om zelf een Inschalingsmatrix aan te leveren. Opstellen door leverancier: Om een Inschalingsmatrix op te stellen is kennis van het primaire proces nodig. Daarom moet Opdrachtgever bij dit proces betrokken zijn.

Ref	Beschrijving	Toelichting
	<of> Opdrachtnemer zal de in <hoofdstuk X van de SLA> gespecificeerde Inschalingsmatrix implementeren zodat meldingen uit het monitoringsysteem prioriteren volgens deze Inschalingsmatrix worden geprioriteerd. Opdrachtgever zal de inschalingsmatrix jaarlijks evalueren en zo nodig actualiseren. Opdrachtnemer zorg ervoor dat de Prestatie gebaseerd is op de meest actuele versie van de Inschalingsmatrix die Opdrachtgever aan Opdrachtnemer beschikbaar heeft gesteld.	<of> Aanleveren door Opdrachtgever Opdrachtgever beschikt over de benodigde expertise om zelf een Inschalingsmatrix op te stellen en met de aanbestedingsstukken aan te leveren. In deze situatie is Opdrachtgever beheerder van dit document en het onderhoudsproces. Het initiatief voor evaluatie ligt in deze situatie bij Opdrachtgever.
IO-04	Alvorens de Prestatie te starten, zorgt Opdrachtnemer dat de Implementatie is afgerond. De Implementatie is afgerond zodra alle processen zijn ingericht, formele documenten zoals bijvoorbeeld SLA en DAP zijn vastgesteld en de acceptatieprocedure voor de implementatiefase succesvol is afgerond. Na de afgeronde implementatiefase is alles gereed om tot Onboarding over te gaan.	
IO-05	Opdrachtnemer gaat ermee akkoord dat Onboarding is afgerond zodra via een Protocol van Oplevering is aangetoond dat de Prestatie conform specificaties op betreffende Assets wordt uitgevoerd.	Zie ook LDB-01.
IO-06	Voor elke (deel)Oplevering zal Opdrachtnemer een Protocol van Oplevering opstellen. Het Protocol van Oplevering is zodanig opgesteld dat bij Oplevering van diensten en/of producten onomstotelijk wordt aangetoond dat de opgeleverde diensten/producten voldoet aan de overeengekomen specificaties en afspraken. Het protocol van Oplevering wordt voor aanvang van de werkzaamheden met Opdrachtgever afgestemd. Direct na Oplevering wordt het Protocol van Oplevering ter goedkeuring aan Opdrachtgever aangeboden.	
IO-07	Nadat een Protocol van Oplevering (PvO) aan Opdrachtgever beschikbaar is gesteld, zal Opdrachtgever de Oplevering binnen <aantal> werkdagen Accepteren of met onderbouwing afwijzen. Na Acceptatie start de vergoeding voor de Prestatie waarop het PvO betrekking heeft. Indien Opdrachtgever de Oplevering niet kan Accepteren, krijgt Opdrachtnemer éénmalig een redelijke termijn voor herstel. Indien daarna wederom niet tot Acceptatie kan worden overgegaan, zal er escalatie plaatsvinden en kan dit aanleiding zijn voor een ingebrekestelling. Indien het PvO volgens overeengekomen afspraken aan Opdrachtgever is verstrekt en binnen de gestelde termijn een reactie van Opdrachtgever uitblijft, mag Opdrachtnemer dit als een akkoord beschouwen. Indien Oplevering niet kan plaatsvinden omdat Opdrachtgever verzaakt, worden er afspraken gemaakt over het doorbelasten van kosten. Het uitgangspunt van deze afspraken is dat Opdrachtnemer schadeloos wordt gesteld voor kosten die hij moet maken, terwijl de dienst niet geleverd kan worden omdat Opdrachtgever niet voldaan heeft aan zijn verplichtingen die bij opdrachtverstrekking zijn overeengekomen. De kosten kunnen nooit hoger zijn dan de in het prijzenblad gespecificeerde kosten voor betreffende Prestatie.	Een Opdrachtnemer wil zicht hebben op de duur van de acceptatieprocedure. Immers, pas na acceptatie kan Opdrachtnemer voor de Prestatie factureren. Om het risico voor trage acceptatie door Opdrachtgever te mitigeren, mag Opdrachtnemer de levering als geaccepteerd beschouwen als er binnen de acceptatietermijn geen antwoord is gegeven.

Ref	Beschrijving	Toelichting
IO-08	Opdrachtnemer zorgt voor de transitie vanuit de bestaande situatie bij Opdrachtgever naar de nieuwe situatie conform de overeengekomen Prestatie. De transitie is zodanig georganiseerd dat de overlast en onderbreking van Dienstverlening zo beperkt mogelijk wordt gehouden. Alle activiteiten die nodig zijn om deze transitie te realiseren, worden door Opdrachtnemer in de implementatie- en onboardingsplannen opgenomen.	Transitie is alleen van toepassing als de organisatie reeds over een SOC beschikt.

9. Eisen aan Rapportages en kwaliteitsborging

Dit hoofdstuk omvat de eisen die betrekking hebben om zicht te houden op de mate waarin de geleverde diensten aan de afspraken voldoen. Het gaat hierbij om zowel kwantiteit en kwaliteit van geleverde diensten. Tevens omvat dit hoofdstuk eisen die gebruikt kunnen worden om het niveau van de Prestatie op peil te houden en waar nodig bij te sturen.

Ref	Beschrijving	Toelichting
RK-01	Dienstenniveaus geven Opdrachtgever en Opdrachtnemer inzicht in het functioneren van de Prestatie(s). Opdrachtnemer rapporteert over de behaalde dienstenniveaus aan Opdrachtgever. Opdrachtnemer dient ervoor te zorgen dat de rapportages voldoen aan de rapportage-eisen zoals in het Service Level Agreement zijn vastgelegd.	Voeg een concept-SLA bij de aanbestedingsstukken toe. Deze concept-SLA bevat de Service Levels waaraan de Prestatie moet voldoen en is daarmee normstellend voor de aanbesteding.
RK-02	Opdrachtnemer is verantwoordelijk voor het bijhouden van de gegevens die in rapportages moeten worden opgenomen.	
RK-03	Bij constatering van foutieve gegevens in de rapportages of het vermoeden daarvan door Opdrachtgever levert Opdrachtnemer aanvullend bewijs dan wel corrigeert de foutieve gegevens op eerste verzoek per direct en levert een herziene rapportage aan.	
RK-04	Opdrachtnemer heeft de kosten voor het opstellen van (maatwerk)rapportages opgenomen in de tarieven van de Prestatie en worden niet apart door Opdrachtnemer in rekening gebracht.	
RK-05	Indien blijkt dat de Prestatie afwijkt van de overeengekomen afspraken en normen, neemt Opdrachtnemer maatregelen om dit te herstellen en afwijkingen in de toekomst te vermijden.	

Bijlage I - Samenhangende documenten

Een aantal eisen refereert naar documenten. In deze bijlage wordt een overzicht gegeven van eisen waarin dergelijke verwijzingen in zijn opgenomen en welke onderwerpen in betreffende documenten opgenomen moeten zijn c.q. worden.

Eis	Document	Wanneer	Onderwerp
A-12	Kennisoverdracht	Na Gunning	Afspraken over kennisoverdracht bij beëindiging van de overeenkomst.
SB-02	DAP	Na Gunning	Operationele afspraken
SB-05	DAP	Na Gunning	Communicatiematrix
SB-06	SLA	Bij publicatie	Responsetijden SOC
SB-07	SLA	Bij publicatie	Responsetijden Servicedesk
SB-10	SLA	Bij publicatie	Normtijden onderhoudsmeldingen
	DAP	Na Gunning	Procesbeschrijving onderhoudsmeldingen
SB-12	DAP	Na Gunning	Afspraken m.b.t. operationeel overleg
SB-13	DAP	Na Gunning	Afspraken m.b.t. tactisch overleg
SB-14	DAP	Na Gunning	Afspraken m.b.t. strategisch overleg
DV-02	SLA	Bij publicatie	Normen m.b.t. de (SOC-)Dienstverlening
DV-06	DAP	Na Gunning	Afspraken over gestandaardiseerde manier van melden.
DV-07	SLA	Bij publicatie	Frequentie waarmee Use Cases c.q. Detectieregels onderhouden moeten worden.
DV-09	Aansluitvoorwaarden	Bij publicatie	Aansluitvoorwaarden NCSC CTI-feed
DV-10			
LDB-01	Assetoverzicht	Bij publicatie	Overzicht van alle Assets die Opdrachtnemer moet monitoren
IO-01	Implementatie- en onboardingsplan	Voor of na Gunning	Zie IO-01
IO-02			Inspanningen die Opdrachtgever zelf moet doen om de SOC-dienst te operationaliseren.
IO-03	Inschalingsmatrix	Bij publicatie óf Na Gunning	Criteria om prioriteiten aan security-incidenten toe te wijzen.
IO-05	PvO	Na Gunning	Acceptatieprocedures en -criteria
IO-06			
IO-07			
RK-01	SLA	Bij publicatie	Normen voor rapportages (frequentie en inhoudelijke criteria)

Bijlage II - Afkortingen en definities

In dit document zijn afkortingen en definities gebruikt. Definities zijn met een hoofdletter geschreven. 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.
	Assetoverzicht	Een lijst waarin alle ICT-Assets zijn opgenomen die relevant zijn voor de levering van de Prestatie.
BIO	Baseline Informatiebeveiliging Overheid	Het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen).
CTI	Cyber Threat Intelligence	Verzamelde, verrijkte en geanalyseerde gegevens over dreigingen in het digitale domein, die als doel heeft deze dreigingen tijdig te identificeren en de weerbaarheid van de ontvangers te verhogen.
	CTI-feed	Een bron die continu CTI levert en die geautomatiseerd kan worden verwerkt in systemen voor monitoring en detectie. Een CTI-feed bestrijkt belangrijke aanvalsvectoren zoals kwaadaardige URL's, phishing-URL's, spam, bot-IP's, sociale media en websites.
	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.
	False Positive	Een waarschuwing of uitslag van het monitorsysteem die ten onrechte is afgegeven.
	Gunning	De laatste fase van een aanbesteding waarin de Opdrachtgever schriftelijk aan alle inschrijvers de Gunningsbeslissing kenbaar maakt.
	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-Asset	Een 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.
	ICT-Infrastructuur	Het samenhangende geheel van alle ICT-Assets dat in zijn totaliteit een (of meerdere) operationeel functionerend geheel is/zijn.
	Implementatie	Het geheel van handelingen en maatregelen dat nodig is om de organisatie van Opdrachtgever geschikt te maken voor het overeengekomen gebruik van de Prestatie.
IoC	Indicator of Compromise	Een aanwijzing die het mogelijk maakt de aanwezigheid van een specifieke dreiging binnen een computernetwerk/ICT-systeem op te sporen.
	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.

Afkorting	Betekenis	Beschrijving
IV	Informatievoorziening	Het geheel van voorzieningen waarmee een gebruiker in zijn informatiebehoefte kan voorzien.
	Inschalingsmatrix	Referentiekader om te bepalen welke prioriteit er aan meldingen van (potentiële) securityincidenten worden toegekend
KPI	Key Performance Indicator	Een objectief meetbare waarde waarmee de kwaliteit van de door Opdrachtnemer geleverde Prestatie, of een specifiek deel hiervan, wordt bepaald.
KRI	Key Risico Indicator	Statistiek en/of meetbare waarde die (vroegtijdig) inzicht verschaft in de mate waarin een organisatie een bepaald risico loopt.
	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.
	Logging	Logging is een geautomatiseerde registratie van gegevens om bij te houden welke gebeurtenissen en handelingen binnen een systeem hebben plaatsgevonden.
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 Justiie en Veiligheid. Het Nationaal Cyber Security Centrum (NCSC) werkt aan een digitaal veilig Nederland.
NvI	Nota van Inlichtingen	Één of meerdere door de Opdrachtgever beantwoorde vragenlijst(en) over de opdracht.
	Offerte	Een aanbieding door de Opdrachtnemer tot het leveren van producten en/of diensten binnen de scope van de Overeenkomst.
	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 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.
SLA	Service Level Agreement	Het deel van de Overeenkomst waarin afspraken over het niveau van Dienstverlening (service levels) zijn vastgelegd.
	Security Operations	De integrale benadering van (ICT) beveiliging waarmee beveiligings- en IT-operationele teams samenwerken om een organisatie effectief te beschermen.
SOC	Security Operations Center	Een afdeling, team of dienst dat digitale systemen en/of identiteiten controleert en/of bewaakt en soms ook afhandelt.

Afkorting	Betekenis	Beschrijving
	Sighting	Het waarnemen of detecteren van een gebeurtenis, activiteit of object dat mogelijk verband houdt met een beveiligingsdreiging of incident.
	Servicemanager	Een persoon die verantwoordelijk is voor het leveren van de diensten conform Overeenkomst en stuurt op het voldoen aan de overeengekomen dienstenniveaus. De Servicemanager zorgt ervoor dat de Dienstverlening voldoen aan de behoefte van Opdrachtgever.
	SOC-diensten	Een reeks beveiligingsdiensten gericht op het realtime monitoren, detecteren, analyseren en reageren op beveiligingsincidenten en -dreigingen.
	Subgunningscriterium	Een criterium dat verband houdt met het voorwerp van de Opdracht, die door de Aanbestedende dienst wordt gehanteerd bij de toepassing van het gehanteerde gunningscriterium.
TCO	Total Cost of Ownership	De volledige kosten die gepaard gaan met het bezit en gebruik van een product of dienst gedurende de gehele levenscyclus.
	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
VIR	Voorschrift Informatiebeveiliging Rijksdienst	Ministeriële regeling met een aantal basisregels over de informatiebeveiliging. Het voorschrift is bindend voor de ministeries en de daaronder ressorterende 'diensten, bedrijven en instellingen'
VIRBI	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie	Ministeriële regeling met aanvullende eisen voor de beveiliging van staatsgeheimen en andere bijzondere gegevens en Informatie. Het voorschrift is bindend voor de ministeries en de daaronder ressorterende 'diensten, bedrijven en instellingen'.

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)

April 2025