Bijlage 4 - RVICTO 26 Marktraadpleging | concept Programma van Eisen SOC-diensten

Specifieke eisen monitoring & detectie en/of kwetsbaarheden scanning & reporting

In de kolommen is per eis aangegeven waarop de eis van toepassing is.

	Basiseisen *Dit gedeelte omvat eisen van algemene aard en hebben veelal betrekking op organisatorische en personele aspecten.*	***M&D***	***KS&R***
B4.1	Opdrachtnemer levert op verzoek van Deelnemer het basispakket Monitoring & Detectie op de assets van de organisatie van Deelnemer. Deelnemers leveren tijdens de minicompetitie een specificatie van de ICT-assets die het betreft.	√	
B4.2	Indien Opdrachtnemer het startpakket Monitoring & Detectie levert, levert Opdrachtnemer op verzoek van Deelnemer ook de extra opties voor Monitoring & Detectie	√	
B4.3	Opdrachtnemer levert op verzoek van Deelnemer diensten voor Kwetsbaarheden Scanning & Reporting op assets van de organisatie van Deelnemer.		√
B4.4	Opdrachtnemer zorgt ervoor dat Informatie van Deelnemer uitsluitend toegankelijk is voor Personeel dat betrokken is bij de uitvoering van de Nadere Overeenkomst en voor zover toegang tot informatie in het kader uit te voeren werkzaamheden nodig is (need-to-know principe). Opdrachtnemer neemt maatregelen om ongeautoriseerde toegang tot informatie van Deelnemer te voorkomen.	√	√
B4.5	De Opdrachtnemer behoort een informatiebeveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de Opdrachtnemer en die aantoonbaar de informatieveiligheid ondersteunt.	√	√
B4.6	De Opdrachtnemer behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van dienstverlening te hebben opgezet en onderhouden.	√	√
B4.7	De Opdrachtnemer dient ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie. Opdrachtnemer toont dit aan bij Opdrachtgever door middel van een jaarlijks auditrapport.	√	√
B4.8	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	√	√
B4.9	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketens.	√	√
B4.10	Opdrachtnemer gaat ermee akkoord dat Deelnemer testen op de Dienstverlening uitvoert of uit laat voeren. Als voorbeeld kan gedacht worden aan o.a. penetratietesten en red teaming testen. Deelnemer	√	√

	bepaalt per geval of hij Opdrachtnemer al dan niet vooraf in kennis stelt van dergelijke testen.		
B4.11	Deelnemer kan beschikken over licenties, zoals bijvoorbeeld Microsoft E5. Dergelijke licenties omvatten componenten die voor monitoring en detectie ingezet kunnen worden. In de Nadere Overeenkomst bepaalt Deelnemer aan of het Opdrachtnemer toegestaan is om hier gebruik van te maken.	√	
B4.12	Opdrachtnemer gaat ermee akkoord dat alle documentatie, data, administratie, methoden en technieken die gedurende het uitvoeren van de Prestatie worden opgebouwd of zijn ingebracht door Deelnemer, eigendom zijn van Deelnemer. Bij beëindiging van de Overeenkomst wordt dit op eerste verzoek van Opdrachtgever binnen 14 dagen en zonder kosten overgedragen aan Opdrachtgever, of aan een door Opdrachtgever aangewezen derde partij. De overdracht van gegevens vindt plaats in een gestructureerde, gangbare en machine-leesbare vorm. Na deze overdracht worden alle gegevens vernietigd met uitzondering van gegevens waarvoor Opdrachtnemer een wettelijke grondslag heeft om deze te bewaren. Deelnemers kunnen in de Nadere Overeenkomst aanvullende afspraken over de overdracht vastleggen.	√	√
	Samenwerking & Beheer *Dit gedeelte omvat eisen die betrekking hebben op de wijze waarop de Opdrachtnemer en Deelnemer in de uitvoering samenwerken. Denk hierbij aan eisen met betrekking tot het vastleggen van werkafspraken, afstemming, het afhandelen van storingen en wijzigingsverzoeken, overlegstructuren, etc.*	***M&D***	***KS&R***
B4.13	Opdrachtnemer stelt een Servicemanager (of iemand in vergelijkbare functie) met voldoende mandaat aan. De Servicemanager is voor Deelnemer het centrale aanspreekpunt en coördineert de Prestatie voor Deelnemer, draagt zorg voor (toezicht op) naleving van de Nadere 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.	√	√
B4.14	Alle operationele afspraken voor de uitvoering van een Nadere Overeenkomst worden vastgelegd in de [NOK bijlage - 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 Nadere Overeenkomst. De inhoud van het DAP wordt altijd afgestemd met Deelnemer. Opdrachtnemer start de afstemming over het DAP direct na gunning van de Nadere Overeenkomst en zal het DAP gedurende de duur van de Nadere Overeenkomst actueel houden.	√	√
B4.15	Alle interactie tussen Deelnemer 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 het DAP een escalatiemodel opgenomen waarin de escalatieprocedure, -niveaus en contactpersonen c.q. rollen zijn beschreven. Opdrachtnemer zal de communicatiematrix en het escalatiemodel opstellen en onderhouden.		
B4.16	Opdrachtnemer biedt een SOC aan dat functioneert als één centraal aanspreekpunt voor Deelnemer ten aanzien van Security Operations gerelateerde zaken. Opdrachtnemer biedt tenminste de volgende mogelijkheden om contact te leggen met het SOC: • Telefonisch • Per email • Voorziening om veilig informatie uit te wisselen (zie eis B4.26) Incidenten en dreigingen met hoge prioriteit wordt altijd telefonisch gemeld aan de Deelnemer tenzij dit in de SLA anders is vastgelegd. De vereiste responsetijden zijn in de [NOK bijlage - Service Level Agreement (SLA)] vastgelegd.	√	√
B4.17	Opdrachtnemer biedt één centraal aanspreekpunt (servicedesk) voor Deelnemer ten aanzien van niet Security Operations gerelateerde vraagstukken. Het betreft onder andere 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 zoals vastgelegd in [NOK bijlage – SLA] geborgd is. Opdrachtnemer biedt tenminste de volgende mogelijkheden om met dit aanmeldpunt contact op te nemen: • Telefonisch • Per email De vereiste responsetijden zijn het in [NOK bijlage – SLA] vastgelegd.	√	√
B4.18	Opdrachtnemer dient Storingen binnen de in het Service Level Agreement vastgelegde normtijden te melden aan Deelnemer. Daarnaast is Opdrachtnemer 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 Deelnemer - delen van relevante informatie, ondersteunen bij testen, het verlenen van toegang tot benodigde systemen en gegevens, en het actief bijdragen aan herstel- en verbeterwerkzaamheden.	√	√
B4.19	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 Deelnemer in bedrijf zijn gesteld. Het onderhoud is zodanig ingericht dat de Prestatie voor de volledige duur van de Nadere Overeenkomst voldoet aan hetgeen in de Nadere Overeenkomst is vastgelegd.	√	√
B4.20	Opdrachtnemer zal wijzigingen en onderhoudswerkzaamheden op de eigen systemen, componenten en applicaties zodanig organiseren dat	√	√

	de impact voor Deelnemer zo klein mogelijk is. Opdrachtnemer kondigt het onderhoud aan volgens procedure en normen die in [NOK bijlage – DAP] en [NOK bijlage – SLA] zijn vastgelegd.		
B4.21	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.	√	√
B4.22	Opdrachtnemer initieert periodiek een operationeel overleg tussen Deelnemer en Opdrachtnemer over de uitvoering van de Nadere Overeenkomst waarin de rapportages en Prestatie op operationeel niveau worden geëvalueerd en potentiële verbeteringen worden besproken. Nadere afspraken over dit overleg worden als onderdeel van de Nadere Overeenkomst in [NOK bijlage – DAP] vastgelegd.	√	√
B4.23	Opdrachtnemer initieert periodiek een tactisch overleg tussen Deelnemer en Opdrachtnemer over de uitvoering van de Nadere Overeenkomst. Dit overleg heeft als doel om te evalueren of de Prestatie en rapportages nog voldoende aansluiten bij behoefte van partijen en om 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 [NOK bijlage – DAP] vastgelegd.	√	√
B4.24	Periodiek initieert Opdrachtnemer een strategisch overleg tussen Deelnemer en Opdrachtnemer over de uitvoering van de Nadere Overeenkomst. Doelstelling van dit overleg is de relatie en samenwerking tussen Deelnemer en Opdrachtnemer te evalueren en optimaliseren. Tevens wordt dit overleg gebruikt om te evalueren of de Nadere Overeenkomst en Prestatie nog voldoende aansluit bij de doelstellingen van Deelnemer. Nadere afspraken over dit overleg zijn in [NOK bijlage – DAP] vastgelegd.	√	√
B4.25	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 Deelnemer. Na goedkeuring door Deelnemer wordt het verslag vastgesteld.	√	√
B4.26	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 aan de Deelnemer en onderhoud deze gedurende de contractperiode van de Nadere Overeenkomst. Indien Deelnemer over een eigen systeem beschikt voor het uitwisselen van gevoelige en vertrouwelijke informatie dan wordt dit opgenomen in de Aanvraag en zal Opdrachtnemer voor het uitwisselen van gevoelige en vertrouwelijke informatie met Deelnemer gebruik maken van het systeem dat door Deelnemer beschikbaar wordt gesteld.	√	√
B4.27	Indien er forensisch onderzoek uitgevoerd moet worden, is het noodzakelijk bewijsmateriaal te verzamelen. Hoewel het forensisch	√	√

	onderzoek zelf geen onderdeel is van deze Raamovereenomst, zal een partij die een dergelijk onderzoek uitvoert bewijsmateriaal verzamelen zodanig dat het bewijsmateriaal juridisch geldig is. Voor het verzamelen van bewijsmateriaal is het waarschijnlijk dat er een beroep op het SOC wordt gedaan. Het verzamelen van bewijsmateriaal, geschikt voor forensisch onderzoek, is specialistisch werk en stelt specifieke eisen aan het verzamelen en vastleggen van bewijsmateriaal. In dergelijke situaties zal de partij die het forensisch onderzoek uitvoert de regie voeren over het verzamelen van bewijsmateriaal. In deze situatie kan er afgeweken worden van de in de Raamovereenkomst vastgelegde voorzieningen, processen en werkwijzen om dit bewijsmateriaal te verzamelen. Opdrachtnemer gaat hiermee akkoord en verleent in dergelijke situaties haar medewerking.		
B4.28	ICT-omgevingen zijn niet statisch. Wijzigingen in de ICT-omgeving van Deelnemer 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. Deelnemer 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.	√	√
Dienstverlening *Dit gedeelte 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.*		***M&D***	***KS&R***
B4.29	De SOC-diensten en alle onderdelen ervan voldoen aan de algemene verwachtingen die Deelnemer, 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.	√	√
B4.30	Opdrachtnemer is verantwoordelijk voor de kwaliteit, beschikbaarheid en continuïteit van de Prestatie zoals opgenomen in de Nadere Overeenkomst. In de [NOK bijlage - SLA] zijn de Dienstenniveaus, inclusief bijbehorende normen en de wijze van meten, beschreven. Opdrachtnemer zal voldoen aan de opgegeven specificaties en Dienstenniveaus zoals vastgelegd in [NOK bijlage – SLA].	√	√
B4.31	De medewerkers die bij het SOC werkzaam zijn bieden eerste lijns ondersteuning aan de Deelnemer en beschikken over de nodige kennis	√	√

	en vaardigheden om de Deelnemer adequaat te ondersteunen binnen de specifieke context van de dienstverlening.		
B4.32	Opdrachtnemer beschikt over specialisten en zet deze in voor Deelnemer bij meer complexe zaken die het kennisniveau van de eerste lijn ondersteuning van het SOC overstijgen. Deelnemer heeft toegang tot deze specialisten. In de communicatiematrix is vastgelegd welke personen hiervoor mandaat hebben.	√	
B4.33	Alvorens Opdrachtnemer bij Deelnemer melding maakt van een (potentieel) beveiligingsincident voert Opdrachtnemer triage uit. Doel van deze triage is het maken van onderscheid tussen echte dreigingen (true positives) en valse meldingen (false positives). Tevens wordt dit proces gebruikt om, op basis van de overeengekomen Inschalingsmatrix, prioriteit aan meldingen toe te kennen (zie ook eis B4.51). Opdrachtnemer meldt (potentiële) beveiligingsincidenten die volgens de Inschalingsmatrix als prioriteit 1 zijn ingeschaald altijd telefonisch bij Opdrachtgever. Opdrachtnemer voert periodieke kwaliteitscontroles op basis van uitgevoerde triages. Ervaringen en leerpunten uit deze triages worden verwerkt om de kwaliteit van het triageproces te behouden en zo nodig verder te optimaliseren.	√	
B4.34	Opdrachtnemer zorgt ervoor dat meldingen van een (potentieel) beveiligingsincident of dreiging op een gestandaardiseerde wijze worden gecommuniceerd met Deelnemer. Tevens zijn dergelijke meldingen ten alle tijden vergezeld van Handelingsperspectief. Opdrachtnemer stemt de afspraken hierover af met Deelnemer en legt deze vast in [NOK bijlage – DAP].	√	
B4.35	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 de [NOK bijlage – SLA] vastgelegd. Deelnemer kan in de Nadere Overeenkomst aanvullende eisen vastleggen met betrekking tot vooraf informeren, afstemmen en goedkeuren van dit onderhoud met/door Deelnemer.	√	
B4.36	Deelnemer kan verzoeken om specifieke Use Cases in het monitoringsysteem op te nemen. Specifieke Use Cases betreffen detectieregels die specifiek zijn voor een bepaalde situatie en/of voor de organisatie van Deelnemer. Opdrachtnemer zal een dergelijk verzoek honoreren en implementeren in zijn monitoringsystemen mits dat redelijkerwijs mogelijk is. Indien het verzoek niet uitvoerbaar is, dient Opdrachtnemer dit schriftelijk onderbouwd te motiveren en te bespreken met Deelnemer.	√	
B4.37	Deelnemer kan verzoeken om dreigingsanalyses uit te voeren en dreigingsbeelden te maken voor zijn organisatie.	√	
B4.28	Het NCSC stelt aan organisaties die tot de Rijksoverheid behoren zogenaamde CTI-feeds beschikbaar. Opdrachtnemer is in staat en bereid om deze door NCSC beschikbaar gestelde CTI-feed(s) in haar Prestatie voor de Nadere Overeenkomst op te nemen conform de aansluitvoorwaarden zoals gespecificeerd in [bijlage – NCSC aansluitvoorwaarden CTI-feeds]. Opdrachtnemer realiseert de	√	

	aansluiting binnen vier weken na gunning van de Nadere Overeenkomst. Deze CTI-feeds bevatten zogenaamde Indicators of Compromise (IoC's). Bij de implementatiefase van de Nadere Overeenkomst worden afspraken gemaakt om deze CTI-feed(s) efficiënt en effectief gebruiken en afspraken hierover worden vastgelegd in [NOK bijlage – DAP].		
B4.39	Tenzij Deelnemer anders verzoekt, zal Opdrachtnemer zogenaamde Sightings op basis van de door NCSC beschikbaar gestelde CTI-feed(s) terugmelden met het NCSC. Terugmelden vindt plaats via de aansluiting en aansluitvoorwaarden zoals beschreven in [bijlage – NCSC aansluitvoorwaarden CTI-feeds]. Als onderdeel van de implementatiefase van de Nadere Overeenkomst worden afspraken gemaakt om het terugmelden efficiënt en effectief te realiseren en deze worden vastgelegd in [NOK bijlage – DAP].	√	
B4.40	Opdrachtnemer voert jaarlijks op verzoek van Deelnemer een self-assessment uit waarin hij de Prestatie voor de Nadere Overeenkomst op basis van eigen inzichten evalueert ("hoe vindt u zelf dat het gaat") en rapporteert hierover aan Deelnemer. 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 Deelnemer. Deelnemer zal aangedragen verbeterpunten die op zijn organisatie betrekking hebben evalueren op kosten, baten, haalbaarheid en wenselijkheid. Op basis van deze evaluatie zal Deelnemer 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.	√	√
B4.41	Opdrachtnemer zal het 'need to know' principe en efficiëntie toe passen. Dat wil zeggen dat Opdrachtnemer niet om meer informatie en logging zal vragen dan strikt noodzakelijk om de gevraagde Prestatie voor de Nadere Overeenkomst te leveren. Daarnaast neemt Opdrachtnemer maatregelen om systemen van Deelnemer niet meer te belasten dan strikt noodzakelijk voor het uitvoeren van de Prestatie. De aangeboden dienstverlening is zodanig dat de reguliere werking van de ICT-componenten bij Opdrachtgever niet verstoort raakt. 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.	√	√
	Logdatabeheer *In dit gedeelte zijn eisen beschreven die betrekking hebben op het verzamelen van logdata en de wijze waarop deze logdata van Deelnemer aan Opdrachtnemer wordt overgedragen. Denk aan eisen die betrekking hebben op het verzamelen, overdragen en verwerken van loginformatie, beveiliging van deze logdata, etc.*	***M&D***	***KS&R***
B4.42	Opdrachtnemer is verantwoordelijk voor het verwerken van Logdata uit alle assets zoals gespecificeerd in [NOK bijlage – Assetoverzicht]. Naast componenten in het assetoverzicht, geldt dit ook voor de componenten die in het kader van de dienstverlening worden toegevoegd, bijvoorbeeld netwerkverbindingen. In dit assetoverzicht is voor elke asset gespecificeerd waar het demarcatiepunt ligt. De tarieven van dienstverlening worden éénmaal per kwartaal bijgesteld o.b.v. het actuele assetoverzicht.	√	

	Op het moment dat het assetoverzicht voor meer dan 5% afwijkt ten opzichte van de te factureren assets, wordt de prijs op de eerste dag van de daaropvolgende maand aangepast, of eerder indien Deelnemer en Opdrachtnemer hierover afwijkende afspraken hebben gemaakt. In het DAP wordt vastgelegd hoe het assetoverzicht gedurende de uitvoering van de overeenkomst actueel wordt gehouden en voor beide partijen inzichtelijk wordt gemaakt.		
B4.43	Logdatabeheer omvat het verzamelen, aggregeren en analyseren van Logdata uit diverse bronnen. Opdrachtnemer specificeert in zijn Offerte wat er van Deelnemer nodig is om de Prestatie te leveren ten aanzien van logdatabeheer. Denk bijvoorbeeld aan eisen die aan logbronnen worden gesteld, zoals: • het detailniveau van Logdata; • de wijze waarop Logdata vanuit Deelnemer bij Opdrachtnemer komt; • software en componenten die in de IT-infrastructuur van Opdrachtgever geplaatst worden; • etc.	√	
B4.44	Opdrachtnemer richt op locatie van een centraal verzamelpunt van logdata in. De koppeling tussen systemen van Opdrachtnemer en Deelnemer verloopt via het centraal verzamelpunt. Om te koppelen met logbronnen van Deelnemer, ondersteunt dit verzamelpunt verschillende gangbare methoden en protocollen zoals Syslog, NCSA, Common Event Format (CEF), JSON, REST APIs, Windows Event Forwarding, etc.	√	
B4.45	Opdrachtnemer beheert Logdata (assets, logs, detecties, informatie, 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 het domein, zoals systemen of configuraties, van Deelnemer bevindt, zal Opdrachtnemer hiervan tijdig melding maken bij Deelnemer zodat Deelnemer passende herstelmaatregelen kan nemen.	√	
B4.45	Opdrachtnemer zorgt ervoor dat Deelnemer ten alle tijde inzicht kan krijgen in de Logdata die in het kader van de Prestatie is vastgelegd. Opdrachtnemer zal aan een dergelijk verzoek hieromtrent van Deelnemer onvoorwaardelijk meewerken.	√	
B4.47	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.	√	
B4.48	Deelnemer zorgt ervoor dat Logdata, detectieregels, informatie, metadata, etc. goed overdraagbaar zijn. Opdrachtnemer zal op eerste verzoek van Deelnemer deze gegevens onvoorwaardelijk en uiterlijk binnen 14 dagen aan Deelnemer beschikbaar stellen in een gangbaar elektronisch open formaat, zodanig dat deze informatie in geautomatiseerde systemen kan worden ingelezen. Afspraken, processen en procedures hieromtrent worden vastgelegd in de afspraken voor kennisoverdracht zoals beschreven onder eis A11.	√	

		M&D	KS&R
	Implementatie & Onboarding *Dit gedeelte beschrijft 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.*		
B4.49	Opdrachtnemer stelt direct na gunning van de Nadere Overeenkomst de [NOK bijlage - Implementatie- en onboardingsplan] op: • Het implementatieplan beschrijft alle activiteiten, afspraken, processen, doorlooptijden, benodigde randvoorwaarden, milestones, oplevermomenten, etc. die nodig zijn voor implementatie van de Dienstverlening en is voorzien van een acceptatieprocedure voor iedere (deel)Oplevering; • Het onboardingsplan beschrijft hetzelfde maar is gericht op het technisch aansluiten van de assets en het technisch inrichten en operationaliseren van de dienst. Daar waar activiteiten impact hebben op Deelnemer, worden deze vooraf afgestemd met Deelnemer. Het implementatie- en onboardingsplan worden ter kennisgeving aan Deelnemer beschikbaar gesteld.	√	√
B4.50	Opdrachtnemer beschrijft in het implementatie- en onboardingsplan aanvullend op eis IO-01 duidelijk en concreet: • De acties en inspanningen die van Deelnemer worden verwacht. Denk bijvoorbeeld aan het aanleveren van bepaalde informatie, betrokkenheid bij testen, etc. Opdrachtnemer streeft daarbij naar het minimaliseren van de inspanningen door Deelnemer. Dit minimaliseren van inspanningen is erop gericht de Deelnemer te ontlasten, maar mag geen afbreuk doet aan de samenwerking en kwaliteit van de Prestatie; • Op welke momenten inspanningen van Deelnemer nodig zijn, wat er van Deelnemer verwacht wordt en een raming van het aantal uren dat voor deze inspanningen worden voorzien.	√	√
B4.51	Als onderdeel van de implementatie stelt Opdrachtnemer, in overleg met Deelnemer, [NOK bijlage – Inschalingsmatrix] op. Deze Inschalingsmatrix is het referentiekader om te bepalen welke prioriteit er aan meldingen van (potentiële) securityincidenten worden toegekend. Opdrachtnemer zal deze Inschalingsmatrix jaarlijks met Deelnemer evalueren en zo nodig actualiseren. Indien Deelnemer zelf een Inschalingsmatrix beschikbaar stelt in de Aanvraag dan is deze opgenomen in [NOK bijlage - SLA] en implementeert Opdrachtnemer de door Deelnemer gespecificeerde Inschalingsmatrix zodat meldingen uit het monitoringssysteem prioriteren conform de Inschalingsmatrix. Deelnemer zal de Inschalingsmatrix jaarlijks evalueren en zo nodig actualiseren. Opdrachtnemer zorgt ervoor dat de Prestatie gebaseerd is op de meest actuele versie van de Inschalingsmatrix die Deelnemer aan Opdrachtnemer beschikbaar heeft gesteld.	√	
B4.52	Indien Deelnemer al over een SOC beschikt dan zorgt Opdrachtnemer voor de transitie vanuit de bestaande situatie bij Deelnemer naar de nieuwe situatie conform de Nadere Overeenkomst. Alle activiteiten die nodig zijn om deze transitie te realiseren, worden door Opdrachtnemer in het implementatie- en onboardingsplan opgenomen. De transitie is zodanig georganiseerd dat de overlast en onderbreking van Dienstverlening zo beperkt mogelijk wordt gehouden.	√	

B4.53	De implementatie wordt door Opdrachtnemer volledig afgerond op basis van de overeengekomen acceptatieprocedure per (deel)Oplevering voordat de onboarding van start gaat.	√	√
B4.54	Opdrachtnemer dient ervoor te zorgen dat Deelnemer gedurende de gehele implementatie- en onboardingfases geïnformeerd is over de voortgang. Opdrachtnemer verstrekt tenminste eenmaal per twee weken een voortgangsrapportage aan Deelnemer. De voortgangsrapportages zijn erop gericht om Deelnemer tijdig inzicht te geven in tenminste: - behaalde resultaten in voorliggende periode, - voortgang ten opzichte van planning, - te behalen resultaten in voorliggende periode, - identificatie van eventuele afwijkingen, - identificatie van eventuele knelpunten. Met betrekking tot voortgangsrapportages kan Deelnemer in een Nadere Overeenkomst aanvullende of afwijkende afspraken maken.	√	√
B4.55	Opdrachtnemer dient een projectmanager aan te stellen die verantwoordelijk is voor de realisatie van de gehele fase implementatie- en onboardingfases bij een Deelnemer. Gedurende de gehele fase van implementatie en onboarding is deze projectmanager als eerste aanspreekpunt voor Deelnemer beschikbaar.	√	√
B4.56	De Onboarding wordt door Opdrachtnemer volledig afgerond op basis van de overeengekomen acceptatieprocedure per deel(Oplevering) voordat Opdrachtnemer aanvangt met monitoring en detectie en/of kwetsbaarheden scanning & reporting.	√	
B4.57	Voor elke (deel)Oplevering tijdens implementatie en Onboarding stelt Opdrachtnemer een Protocol van Oplevering op: • Het Protocol van Oplevering is zodanig opgesteld dat tijdens de acceptatieprocedure onomstotelijk wordt aangetoond dat de (deel)Oplevering voldoet aan de overeengekomen specificaties en afspraken; • Het Protocol van Oplevering wordt voor aanvang van de acceptatieprocedure met Deelnemer afgestemd; • Direct na de (deel)Oplevering wordt het Protocol van Oplevering ter goedkeuring aan Deelnemer aangeboden;	√	√
B4.58	Nadat een Protocol van Oplevering aan Deelnemer beschikbaar is gesteld voor Acceptatie, zal Deelnemer conform de opgenomen termijn in de acceptatieprocedure het Protocol van Oplevering accepteren of met onderbouwing afwijzen. Indien het Protocol van Oplevering volgens overeengekomen afspraken aan Deelnemer is verstrekt en binnen de overeengekomen termijn een reactie van Deelnemer uitblijft, mag Opdrachtnemer dit als een Acceptatie beschouwen.	√	√
B4.59	Indien de Opdrachtnemer een levering verricht die niet voldoet aan de overeengekomen eisen, specificaties of kwaliteit, wordt Opdrachtnemer in de gelegenheid gesteld om deze gebreken binnen redelijke termijn kosteloos te herstellen of de levering te vervangen zonder dat hierdoor de overeengekomen planning in gevaar komt. Indien zich echter herhaaldelijk gebrekkige leveringen voordoen, behoudt de Deelnemer zich het recht voor om aanvullende maatregelen te treffen, waaronder het ontbinden van de Nadere Overeenkomst.	√	√

B4.60	Er kunnen zich situaties voordoen dat er met spoed een onboarding noodzakelijk is. Dit kan bijvoorbeeld het geval zijn tijdens een security incident waarbij er met spoed onboarding van data nodig is. Een dergelijke spoed-onboarding wordt als wijziging uitgevoerd en niet projectmatig zoals een reguliere onboarding. Opdrachtnemer zorgt ervoor dat de dienstverlening voorziet in een procedure om in dergelijke gevallen met spoed een onboarding uit te voeren. De normen en werkwijze van deze spoed-onboarding worden in respectievelijk het SLA en DAP vastgelegd.	√	√
B4.61	Indien een (deel)Oplevering niet kan plaatsvinden als gevolg van omstandigheden bij de Deelnemer, 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 (deel)Oplevering niet kan plaatsvinden omdat Deelnemer niet voldaan heeft aan zijn verplichtingen uit de Nadere Overeenkomst. De kosten kunnen nooit hoger zijn dan de in [NOK bijlage – Prijzenblad] gespecificeerde kosten voor betreffende Prestatie.	√	√
	Rapportage NOK & Kwaliteitsborging	***M&D***	***KS&R***
	Dit gedeelte 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 gedeelte eisen die gebruikt kunnen worden om het niveau van de Prestatie op peil te houden en waar nodig bij te sturen.		
B4.62	Dienstenniveaus geven Deelnemer en Opdrachtnemer inzicht in het functioneren van de Prestatie(s). Opdrachtnemer rapporteert over de behaalde dienstenniveaus aan Deelnemer. De opzet van de rapportage en de frequentie waarin Opdrachtnemer rapporteert aan Deelnemer voldoet aan de rapportage-eisen zoals opgenomen in [NOK bijlage - SLA].	√	√
B4.63	Opdrachtnemer is verantwoordelijk voor het bijhouden van de informatie die in de rapportages moeten worden opgenomen.	√	√
B4.64	Bij constatering van foutieve informatie in de rapportages of het vermoeden daarvan door Deelnemer levert Opdrachtnemer aanvullend bewijs dan wel corrigeert de foutieve informatie op eerste verzoek per direct en levert een herziene rapportage aan.	√	√
B4.	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 aan Deelnemer.	√	√
B4.	Indien op basis van de rapportages 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 en stemt hierover met Deelnemer.	√	√

Hoofdletterwoorden	Definitie
Storing	Een storing is een defect of fout in een ICT-component of dienst die leidt tot, of kan leiden tot, een onderbreking of verslechtering van de dienstverlening.
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.
Oplevering	Zie Arbit
Prestatie	Zie Arbit
Deelnemer	EA doc
Opdrachtnemer	EA doc
Nadere overeenkomst	EA doc
Personeel	Zie Arbit
Service Manager	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.
Security Operations	De integrale benadering van (ICT) beveiliging waarmee beveiligings- en IT-operationele teams samenwerken om een organisatie effectief te beschermen.
Inschalingsmatrix	Referentiekader om te bepalen welke prioriteit er aan meldingen van (potentiële) securityincidenten worden toegekend
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.
Use Cases	Een beschrijving van een gedrag van een systeem dat reageert op een verzoek of situatie dat van buiten het systeem afkomstig is.
CTI	Cyber Threat Intelligence: Verzamelde, verrijkte en geanalyseerde informatie over dreigingen in het digitale domein, die als doel heeft deze dreigingen tijdig te identificeren en de weerbaarheid van de ontvangers te verhogen.
IoC's	Indicators of Compromise: Een aanwijzing die het mogelijk maakt de aanwezigheid van een specifieke dreiging binnen een computernetwerk/ICT-systeem op te sporen.
Acceptatie	Zie Arbit
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.
Offerte	EA doc

Niet opgenomen hoofdletterwoorden	Definitie
Triage	Het proces van het snel en efficiënt beoordelen, prioriteren en classificeren van meldingen uit de monitoring & detectiesystemen van het Security Operations Center.
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.