Verwijzing	Eis	Optie	Baseline	Optioneel	Pakket	Opmerkingen
A1.1	Inschrijver verklaart door Inschrijving zich te onthouden van gedragingen die de mededinging tussen de Inschrijvers kan beperken.		x		Dienstverlening	
A1.2	Voor het definiëren van dienstverlening, de benodigde security functies en gebruik van best practices hanteert deze uitvraag het NIST-CSF 2.0 model: - De gevraagde dienstverlening 'Monitoring & Alarmering wordt gedefinieerd conform de definitie van 'Detect en Respond' - Opdrachtnemer kan de dienstverlening formuleren en aanbieden conform het NIST-CSF model		x		Dienstverlening	
A1.3	Opdrachtnemer levert één (1) vast aanspreekpunt voor de contractmanager van [Deelnemer] voor de looptijd van de overeenkomst.		x		Dienstverlening	
A1.4	Opdrachtnemer verplicht zich vertrouwelijk om te gaan met de informatie die in het kader van de uitvoering van deze overeenkomst hem ter kennis komt. Het niet vertrouwelijk omgaan met deze informatie kan leiden tot een ontbinding van de overeenkomst.		x		Dienstverlening	
A1.5	[Deelnemer] heeft het recht om maximaal één (1) maal per jaar een audit te laten uitvoeren, door een externe onafhankelijke partij. Deze audit wordt in overleg met de Opdrachtnemer ingepland en omvat zowel bestaan als werking.		x		Dienstverlening	
A1.6	Opdrachtnemer biedt de dienstverlening aan conform de standaard verwerkersovereenkomst van [Deelnemer]		x		Dienstverlening	
A1.7	De Opdrachtnemer borgt aantoonbaar de integriteit van haar medewerkers door hen te laten screenen door een als Particulier Onderzoeksbureau gecertificeerde organisatie. In de screenings zijn minimaal de volgende onderdelen zijn opgenomen: financiële checks, social media onderzoek, verificatie strafblad en een persoonlijk interview.			x	Dienstverlening	
A1.8	Opdrachtnemer kan aantonen dat de dienstverlening compliant is met de minimale beveiligingseisen voor de relevante inkoop onderdelen uit de Inkoopeisen Cybersecurity Overheid (https://www.bio-overheid.nl/ico-wizard). Opdrachtnemer kan dit voor definitieve gunning van de opdracht aantonen. Minimaal zijn de volgende Inkoop-onderdelen in scope: - Algemeen Ketenpartners - Clouddiensten - Softwarepakketten - Toegangsbeveiliging		x		Dienstverlening	
A1.9	Na definitieve gunning wordt er samen met Opdrachtnemer een SLA document gemaakt en vastgesteld. In deze SLA komen minimaal de volgende onderwerpen terug: - Heldere dienstbeschrijving; - Communicatiematrix met de gegevens van de contactpersonen van Opdrachtgever en Opdrachtnemer met onderverdeling naar functies/ verantwoordelijkheden/escalatieniveau 's - Overlegmatrix - KPI's - Evaluaties/prestatiemeting		x		Dienstverlening	
A1.10	Opdrachtnemer gaat door Inschrijving akkoord met de inhoud van alle Aanbestedingsstukken, de beoordelings-en waarderingssystematiek, de gekozen Aanbestedingsprocedure en alle bepalingen en voorbehouden die hiermee samenhangen.		x		Dienstverlening	
A1.11	Inschrijver verklaart dat alle bij Inschrijving overlegde gegevens juist, volledig en naar waarheid zijn ingevuld en gestand worden gedaan gedurende de gehele looptijd van de overeenkomst inclusief eventuele verlengingen.		x		Dienstverlening	
A1.12	Opdrachtgever behoudt zich het recht voor op ontbinding van de overeenkomst en/of een schadevergoeding in geval van onjuiste en/of onvolledige informatie en/of het niet kunnen nakomen hetgeen bij Inschrijving aangeboden is.		x		Dienstverlening	
A1.13	Opdrachtnemer is in staat en bereid om de gevraagde dienstverlening ten behoeve van de Opdrachtgever, conform de in de Aanbestedingsstukken gestelde eisen te verzorgen.		x		Dienstverlening	
A1.14	Opdrachtnemer handelt (aantoonbaar) conform de (Uitvoeringswet) Algemene Verordening Gegevensbescherming ((U)AVG) en aanverwante wetgeving. De Opdrachtgever behandelt alle door Opdrachtnemer verstrekte persoonsgegevens eveneens conform de in Nederland geldende Wet- en regelgeving.		x		Dienstverlening	
A1.15	Mondelinge communicatie van de Opdrachtnemer naar de Opdrachtgever en Deelnemers vindt plaats in de Nederlandse taal (C1; zie ook https://detaalbrigade.nl/taalniveaus/).		x		Dienstverlening	
A1.16	(Technische) documentatie is opgesteld in de Nederlandse taal (C1; zie ook https://detaalbrigade.nl/taalniveaus/). Documentatie wordt continu up-to-date gehouden en de laatste versie wordt actief gedeeld met [Deelnemer]		x		Dienstverlening	
B2.1	Opdrachtnemer beschikt over een primair aanspreekpunt voor administratieve, - en contractzaken, dat op werkdagen beschikbaar is tussen 08.30 en 17.00 Nederlandse tijd.		x		Dienstverlening	
C3.1	De door Inschrijver aangeboden tarieven zijn 'all-in', dat wil zeggen inclusief (niet gelimiteerd) salariskosten, overheadkosten, kosten voor gebruik apparatuur/software/hardware (die nodig zijn bij het in het kaart brengen en oplossen van een informatieveiligheid incident), verzekeringen, reis- en verblijfskosten, reistijd, belasting, heffingen, administratieve kosten, kosten voor overleg etc.		x		Dienstverlening	
C3.2	Verlagingen van wettelijke heffingen zoals het btw-percentage dient Opdrachtnemer te allen tijde te melden en de tarieven dienen in een dergelijk geval verplicht te worden herzien.		x		Dienstverlening	
C3.3	Alle in de Aanbestedingsstukken en de daarbij behorende bijlagen genoemde bedragen en/of aantallen zijn indicatief. Opdrachtnemer kan aan deze bedragen en/of aantallen geen rechten in termen van (minimaal en maximaal) afzet/omzet ontlenen.		x		Dienstverlening	
D4.1	De Opdrachtnemer kan haar SOC-analisten classificeren volgens de marktdefinities voor SOC-Analisten niveau 1, niveau 2 of niveau 3.		x		Dienstverlening	
D4.2	De Opdrachtnemer levert SOC-dienstverlening. Het collecteren en opslaan van de vereiste logdata is verantwoordelijkheid van de Deelnemers. Opslag van de logdata vindt plaats binnen de netwerkgrenzen van iedere individuele Deelnemer. Ontsluiting van de data ten behoeve van de SOC-dienstverlening, m.a.w. de benodigde data voor security monitoring feitelijk kunnen benutten voor deze monitoring, is verantwoordelijkheid van de Opdrachtnemer. Deelnemers zorgen dat zij voldoen aan de overeengekomen aansluitcriteria ten aanzien van het beschikbaar stellen van logdata.		x		Dienstverlening	
D4.2.1	De Opdrachtnemer levert SOC-dienstverlening. Het collecteren en opslaan van de vereiste logdata is de verantwoordelijkheid van de Opdrachtnemer. Ontsluiting van de data ten behoeve van de SOC-dienstverlening, m.a.w. de benodigde data voor security monitoring feitelijk kunnen benutten voor deze monitoring, is verantwoordelijkheid van de Opdrachtnemer. Deelnemers zorgen dat zij voldoen aan de overeengekomen aansluitcriteria ten aanzien van het beschikbaar stellen van logdata.			x	Dienstverlening	Vervangt baseline D4.2. Gaat niet samen met D4.2.2
D4.2.2	De Opdrachtnemer levert SOC-dienstverlening. Het collecteren en opslaan van de vereiste logdata is een gedeelde verantwoordelijkheid tussen [Deelnemer] en Opdrachtnemer. Ontsluiting van de data ten behoeve van de SOC-dienstverlening, m.a.w. de benodigde data voor security monitoring feitelijk kunnen benutten voor deze monitoring, is verantwoordelijkheid van de Opdrachtnemer. Deelnemers zorgen dat zij voldoen aan de overeengekomen aansluitcriteria ten aanzien van het beschikbaar stellen van logdata.			x	Dienstverlening	Vervangt baseline D4.2 Gaat niet samen met D4.2.1
D4.2.3	De Opdrachtnemer realiseert een plan in samenwerking met [Deelnemer] voor de ideale wijze van collecteren en opslaan van logdata t.b.v. SOC-dienstverlening. Dit plan bevat minstens een HLD en LLD.			x	Dienstverlening	Deze optie wordt vereist als D4.2.1 of D4.2.2 wordt gekozen.
D4.3	Opdrachtnemer sluit aan op de bestaande security capabilities en bestaande log analytics omgeving van [Deelnemer].		x		EDR, NDR, SIEM, Dienstverlening	

D4.4	Opdrachtnemer houdt een overzicht bij waarop een mapping is gemaakt van de gebruikte use cases op een industriestandaard framework.		x		Dienstverlening	
D4.4.1	Opdrachtnemer houdt een overzicht bij waarop een mapping is gemaakt van de gebruikte use cases op het Mitre ATT&CK framework.	Optie 1		x	Dienstverlening	Vervangt baseline D4.4
D4.5	Opdrachtgever analyseert proactief op afwijkingen in gedrag op IT, naast de gedefinieerde use cases.		x		Dienstverlening	
D4.6	Opdrachtnemer implementeert, beheert en optimaliseert de te gebruiken security use cases en alle benodigde detectieregels. Indien [Deelnemer] over een lokale SIEM-oplossing beschikt, worden de use cases ook in dit lokale SIEM geimplementeerd. Operationalisatie van deze uitrol vindt plaats in overleg met de betreffende Deelnemer. De security use cases bestaan minimaal uit: -Bescherming tegen bekende generieke aanvallen -Bescherming tegen specifieke aanvallen op Deelnemers -Bescherming tegen aanvallen die gedetecteerd zijn bij andere klanten van Opdrachtnemer en relevant zijn voor de Deelnemers		x		SIEM	
D4.7	Interne en externe dreigingsinformatie wordt continue gemonitord op relevantie voor [Deelnemer]. Deze dreigingsinformatie voorziet minimaal in: -dreigingsinformatie specifiek voor de sector (Zowel Veiligheidsregio als GGD/Zorg) -dreigingsinformatie specifiek voor IT -dreigingsinformatie voor andere klanten van Opdrachtnemer die ook relevant zijn voor de Deelnemers -Opdrachtnemer gebruikt deze informatie om de detectie mogelijkheden van dreigingen te verbeteren		x		Dienstverlening	
D4.8	Opdrachtnemer heeft partnerships met diverse partijen om markt specifieke dreigingsinformatie te ontvangen, in ieder geval met het NCSC en een nog aan te wijzen VR-Knooppunt.				Dienstverlening	
D4.9	De Opdrachtnemer stelt op basis van de overeengekomen generieke SLA een dossier afspraken en procedures (DAP) op. In de specifieke SLA komen minimaal de volgende onderwerpen terug: -Overeengekomen dienstverlening en de status van deze dienstverlening - Het dreigingslandschap van de [Deelnemer] -KPI's -Evaluaties/prestatiemeting -Rapportages die geleverd worden In het DAP komen minimaal de volgende onderwerpen terug: -Communicatiematrix met de gegevens van de contactpersonen van Opdrachtnemer en [Deelnemer] met onderverdeling naar functies/ verantwoordelijkheden/escalatieniveau 's -Technische/ functionele ondersteuning over de dienstverlening -Procesafspraken t.a.v. het Incident-, Problem, Change en Configuratiemanagementproces		x		Dienstverlening	
D4.10	Opdrachtnemer draagt zorg voor de classificatie van alarmen en maakt hierbij tenminste onderscheid in: -True Positive -False Positive -Benign Positive -Vulnerability		x		Dienstverlening	
D4.11	Opdrachtnemer levert rapportages in een digitale vorm via een dashboard- of portalfunctie op basis van een (near) real time rapportage. Deze rapportage bevat minimaal de onderdelen: -Kwaliteit van de dienstverlening, inclusief te verwachten ontwikkelingen op korte termijn (1 kwartaal vooruit kijkend) -Incidenten - alle benodigde informatie voor sturing op incidenten (o.a. opgetreden, afgesloten en openstaand) -Waarschuwingen ter voorkoming van incidenten -Time to respond van incidenten en waarschuwingen -False positives - alle benodigde informatie voor sturing op reductie -Brondata - alle benodigde informatie voor optimalisatie van- en continuïteit in brondata aanlevering -Trends in de markt -Lifecycle Management t.a.v. use cases en detectiemechanismen -Dekkingsgraad van de security monitoring -Verbetermogelijkheden van de monitoring en response processen		x		Dienstverlening	
D4.12	Tijdelijk verwijderd		x		Dienstverlening	
D4.12.1	Tijdelijk verwijderd	Optie 1		x	Dienstverlening	Vervangt baseline D4.12
D4.12.2	Tijdelijk verwijderd	Optie 2		x	Dienstverlening	Vervangt baseline D4.12
D4.12.3	Tijdelijk verwijderd	Optie 3		x	Dienstverlening	Vervangt baseline D4.12
D4.13	Opdrachtnemer draagt zorg voor een tijdige prioritering van- en respons op- security incidenten door melding aan [Deelnemer]*. Hierbij voldoet Opdrachtnemer aan de volgende richtlijn: Time to respond: -Critical (P1). - 20 min -High (P2) - 1 uur -Medium (P3) - 4 uur -Low (P4). - 16 uur * En eventueel andere partijen zoals een nog aan te wijzen VR-Knooppunt. **onder time to respond wordt hier verstaan: de maximale tijd tussen het (automatisch) genereren van een alarm, en het melden van een (mogelijk) incident bij de desbetreffende Deelnemer.		x		Dienstverlening	
D4.14	De Opdrachtnemer laat minimaal één (1) maal per jaar de dienstverlening testen d.m.v. een penetratietest (PenTest), door een externe onafhankelijke partij.			x	Dienstverlening	
D4.15	Opdrachtnemer dient op verzoek [Deelnemer] te kunnen ondersteunen bij het aansluiten op de SOC-dienstverlening. Dit omvat zowel de configuratie van de lokale componenten van een [Deelnemer] binnen haar eigen netwerkgrenzen als het aansluiten op de converged SOC-dienstverlening.		x		Dienstverlening	
D4.16	De Opdrachtnemer verzorgt training/opleiding van (interne) medewerkers van [Deelnemer] voor het effectief gebruik van de dienstverlening.		x		Dienstverlening	
D4.17	Op eerste aangeven van [Deelnemer] stelt Opdrachtnemer, binnen 3 maanden, een Exit-plan op voor de Deelnemer. Het Exit-plan dient voor goedkeuring aan de verzoeker te worden voorgelegd.		x		Dienstverlening	
D4.18	De Opdrachtnemer zal op verzoek [Deelnemer] de uitvoering van de Nadere Overeenkomst onder dezelfde condities, prijzen en tarieven voortzetten na de einddatum daarvan tot het moment dat de continuïteit van de Diensten en de uitvoering van de overeenkomst door een andere opdrachtnemer wordt gewaarborgd (de "retransitie" periode) hetgeen uitsluitend door [Deelnemer] kan worden beoordeeld. De transitieperiode wordt gesteld op maximaal 6 (zes) maanden.		x		Dienstverlening	

D4.19	Bij beëindiging van de overeenkomst of beëindiging van de deelname door [Deelnemer] ongeacht de reden of wijze van beëindiging, zal Opdrachtnemer aan [Deelnemer] alle noodzakelijke medewerking verlenen zodat [Deelnemer] op een soepele wijze kan overstappen naar een andere opdrachtnemer. Opdrachtnemer zal gedurende de retransitie alle ter hand gestelde documenten, goederen en data van [Deelnemer] ter beschikking stellen aan een door [Deelnemer] aan te wijze derde, inclusief bijbehorende meta-data. Dit ter hand stellen dient te gebeuren in een gangbaar en voor [Deelnemer] bruikbaar en gedocumenteerd elektronisch formaat. [Deelnemer] zal de ontvangen gegevens controleren en verifiëren of de data in goede orde, dus leesbaar, bruikbaar, volledig en juist zijn. Indien de gegevens in goede orde zijn ontvangen, stuurt [Deelnemer] hiervan een bevestiging aan Opdrachtnemer.		x		Dienstverlening	
D4.19.1	Opdrachtnemer zorgt dat in transitieperiode gekwalificeerde (en zoveel mogelijk dezelfde)medewerkers betrokken zijn bij de uitvoering van de werkzaamheden en de transitie.		x		Dienstverlening	
D4.20	Na ontvangst van bevestiging als hiervoor (in D4.26) bedoeld zal Opdrachtnemer overgaan tot vernietiging van onder hem bevindende gegevens, waarbij de vernietigingshandelingen gedocumenteerd zullen worden en een rapportage hiervan aan [Deelnemer] ter hand gesteld zal worden. Een afwijkende afspraak kan worden gemaakt, indien daartoe aanleiding bestaat (bijv. in het kader van het eerbiedigen van een wettelijke bewaartermijn).		x		Dienstverlening	
D4.21	Eventuele voor de MDR dienstverlening benodigde specifieke hardware- en softwarecomponenten worden in abonnementsvorm geleverd.			x	Dienstverlening	
D4.22	Inschrijver houdt conform BIO/NEN7510 een auditlog bij die voor daartoe aangewezen medewerkers van Deelnemer continu in te zien is.		x		Dienstverlening	
D4.23	Het SOC, de door de Opdrachtnemer gebruikte software (SIEM) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).		x		Dienstverlening	
D4.23.1	Het SOC, de door de Opdrachtnemer gebruikte software (EDR) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).	Optie 1		x	Dienstverlening	Dit is geen vervanging maar een Add-on voor D4.23 Gaat niet samen met D4.23.2
D4.23.2	Het SOC, de door de Opdrachtnemer gebruikte software (NDR) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).	Optie 2		x	Dienstverlening	Dit is geen vervanging maar een Add-on voor D4.23 Gaat niet samen met D4.23.1
D4.24	Het SOC team is werkzaam en werkt binnen de EER.		x		Dienstverlening	
D4.25	Inzage van logdata is alleen mogelijk voor Deelnemer en bevoegde medewerkers bij Opdrachtnemer, tenzij vooraf uitdrukkelijk en schriftelijk toestemming is gegeven door Deelnemer of als de rechter daar opdracht toe geeft.		x		Dienstverlening	
D4.26	Bevoegde medewerkers: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot logdata, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.		x		Dienstverlening	
D4.27	Het SOC-team van de Opdrachtnemer bestaat minimaal uit niveau 1 en niveau 2 SOC analisten, waarbij het SOC-team gedurende de 24 uur per dag op elk moment bestaat uit minimaal 40% niveau 2 analisten.			x	Dienstverlening	Als D4.12.2 of D4.12.3 wordt gekozen is dit Baseline, anders optioneel. Bespreken of wij dit daadwerkelijk willen eisen.
D4.28	Het SOC-team bestaat gedurende de 24 uur per dag op elk moment uit minimaal 2 personen.			x	Dienstverlening	Als D4.12.2 of D4.12.3 wordt gekozen is dit Baseline, anders optioneel
G6.1	De SOC-teamleden van de Opdrachtnemer zijn aantoonbaar gecertificeerde SOC analisten via een marktconforme certificering (bijvoorbeeld CompTIA, SANS of ISACA, CEH, OSCP, CISSP).		x		Dienstverlening	
F5.1	Facturen dienen te voldoen aan de wettelijke vereisten (zie www.belastingdienst.nl). Een factuur bevat minimaal de volgende gegevens: Gegevens Opdrachtnemer · Bedrijfsnaam · Adres · Telefoonnummer · KvK-nummer · Btw-nummer · IBAN-rekeningnummer · Debiteurnummer Gegevens de Aanbestedende dienst · Organisatienaam · Adres · Contractnummer Factuur gegevens				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
F5.2	Een kostenoverzichten bevat minimaal de volgende gegevens: •Factuurdatum •Factuurnummer •Ordernummer •Periode waar de factuur/kostenoverzicht betrekking op heeft •Naam van de opdrachtverstrekker (indien van toepassing) •Prijs per onderdeel zoals opgenomen in het prijzenblad (of de offerte in het geval van aanvullende werkzaamheden) •Aantal per onderdeel zoals opgenomen in het prijzenblad (of de offerte in het geval van aanvullende werkzaamheden) •Totaal kosten (incl. en excl. btw) •In het geval van aanvullende werkzaamheden een kopie van de door de Deelnemer goedgekeurde offerte •Naam en telefoonnummer contactpersoon Opdrachtnemer				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
F5.3	Indien een factuur niet voldoet aan de in de Overeenkomst genoemde voorwaarden wordt de Opdrachtnemer hiervan binnen 30 kalenderdagen na ontvangst schriftelijk op de hoogte gebracht. De betreffende factuur wordt pas in behandeling genomen op het moment dat deze voldoet aan de in de Overeenkomstgenoemde voorwaarden.				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
F5.4	[Deelnemer] is gerechtigd om indien er sprake is van door Opdrachtnemer verschuldigde bedragen (crediteringen) deze te verrekenen met bedragen die Opdrachtnemer verschuldigd is aan de [Deelnemer].				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
F5.5	Indien [Deelnemer] niet tijdig betaalt en de vertraging niet te wijten is aan Opdrachtnemer, kan Opdrachtnemer aanspraak maken op de wettelijke rente van het bedrag, met de betaling waarvan [Deelnemer] in gebreke is, met ingang van de dag, volgend op die, waarop de betaling uiterlijk diende te geschieden. Rente van rente kan Opdrachtnemer niet vorderen.				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
F5.6	De kosten van het accountantsonderzoek komen voor rekening van de Opdrachtgever of [Deelnemer], tenzij uit het onderzoek van de accountant blijkt dat de factu(u)r(en) niet juist dan wel onvolledig is/zijn, in welk geval bedoelde kosten voor rekening van Opdrachtnemer komen.				Dienstverlening	Geen baseline of optioneel opgegeven aangezien (regionale)inkoop hier over moet beslissen
G6.2	De Opdrachtnemer heeft minimaal 3 jaar ervaring bij Opdrachtgevers met de Baseline Informatiebeveiliging Overheid (BIO).			x	Dienstverlening	
G6.3	De Opdrachtnemer is gecertificeerd conform ISO27001 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.		x		Dienstverlening	
G6.4	De Opdrachtnemer is gecertificeerd conform ISO27017 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.			x	Dienstverlening	
G6.5	De Opdrachtnemer is gecertificeerd conform ISO9001 (of gelijkwaardig), waarbij SOC-dienstverlening binnen het toepassingsbereik valt.		x		Dienstverlening	

G6.6	De Opdrachtnemer is in bezit van een ISEA3402 Type 2 verklaring, SOC2 verklaring of een ander gelijkwaardig certificaat, waarbij SOC-dienstverlening binnen het toepassingsbereik valt.			x	Dienstverlening	
J7.1	Opdrachtnemer brengt de contactpersoon van de Opdrachtgever, zodra Opdrachtnemer weet of behoort te weten dat de nakoming van de Diensten niet of niet tijdig of niet naar behoren plaatsvindt, onmiddellijk schriftelijk én telefonisch op de hoogte onder vermelding van de omstandigheden.		x		Dienstverlening	
J7.2	Indien de overeenkomst binnen de looptijd wordt ontbonden, om reden van een onjuiste calculatie, op grond van een onvoldoende prestatie of andere tekortkomingen die aan Opdrachtnemer kunnen worden toegerekend, is Opdrachtnemer verplicht tot vergoeding van de schade die door de annulering ontstaat. Onder schade wordt in dit verband mede verstaan het verschil tussen de met Opdrachtnemer overeengekomen prijs en de eventueel hogere prijs, verbonden aan het doen uitvoeren van de Diensten door een derde, zulks te berekenen over de nog resterende looptijd van de overeenkomst. Indirecte- en gevolgschade zoals bedrijfsstagnatie vallen hier niet onder.		x		Dienstverlening	
J7.3	Door het indienen van een Inschrijving maken de door Opdrachtnemer opgegeven antwoorden op de kwalitatieve sub-gunningcriteria automatisch en direct deel uit van de eisen die gesteld worden aan de uitvoering van de dienstverlening.		x		Dienstverlening	
P8.1	Opdrachtnemer beschikt over voldoende medewerkers om de Diensten conform de Aanbestedingsstukken uit te voeren.		x		Dienstverlening	
P8.2	Opdrachtnemer ziet erop toe dat de uitvoering van de Dienstverlening ongestoord voortgang vindt en conform de daaraan gestelde eisen wordt uitgevoerd. Opdrachtnemer draagt er zorg voor dat de voortgang niet door o.a. ziekte, vakantie of andere redenen van afwezigheid van haar medewerkers wordt onderbroken. Opdrachtnemer neemt in voorkomende gevallen onverwijld de nodige maatregelen tot het doen van de vereiste voorzieningen c.q. inzet van vervangend gelijkwaardig personeel (zowel qua werk- en denkniveau als aantoonbare relevante werkervaring).		x		Dienstverlening	
P8.3	Alle medewerkers van en namens Opdrachtnemer welke in een gebouw van [Deelnemer] komen houden zich aan de geldende huisregels en kunnen zich op verzoek legitimeren.		x		Dienstverlening	
P8.4	De Opdrachtgever kan nimmer aansprakelijk gesteld worden voor het inlenen van illegale werknemers. De door de overheid aan de Opdrachtgever opgelegde boetes zullen worden vergoed door Opdrachtnemer.		x		Dienstverlening	
P8.5	Indien de Opdrachtgever niet tevreden is over de inzet van een medewerker van Opdrachtnemer kan de Opdrachtgever verzoeken om vervanging van de desbetreffende medewerker. De Opdrachtgever zal tijdig Opdrachtnemer op de hoogte stellen en zal geen vervanging eisen op basis van ongegronde redenen.		x		Dienstverlening	
P8.6	Opdrachtnemer verklaart dat alle medewerkers welke gedurende de looptijd van de overeenkomst bij Opdrachtnemer in dienst zijn aan alle wettelijke voorschriften voldoen van het land (of de landen) waar de medewerker gecontracteerd en werkzaam is. Opdrachtnemer is volledig verantwoordelijk voor het naleven van de wet- en regelgeving met betrekking tot aanstelling, tewerkstelling, betrouwbaarheid, gedrag en andere relevante zaken met betrekking tot haar medewerkers.		x		Dienstverlening	
PR9.1	Opdrachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor die doeleinden gebruiken en niet voor enig ander doeleinde.		x		Dienstverlening	
PR9.2	Datalekken: De organisatie heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.		x		Dienstverlening	
PR9.3	Datalekken: Opdrachtnemer meldt het zo spoedig mogelijk maar in ieder geval binnen 24 uur na ontdekken van datalek aan [Deelnemer] dat er een datalek heeft plaatsgevonden waarbij (persoons)gegevens van [Deelnemer] betrokken zijn. Dit betreft datalekken vanuit de Opdrachtnemer. Datalekken die worden gedetecteerd vanuit de dienstverlening bij [Deelnemer] dienen ook zo spoedig mogelijk d.m.v. een Critical incident en in ieder geval binnen 24 uur na ontdekken van het datalek te worden gemeld bij [Deelnemer].		x		Dienstverlening	
PR9.4	Doelbinding op rolniveau: De Opdrachtnemer behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.		x		Dienstverlening	
PR9.5	Toegang op taakniveau: Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.		x		Dienstverlening	
PR9.6	Logging en monitoring uitgeven toegangsrechten: De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.		x		Dienstverlening	
PR9.7	Opdrachtnemer zal bij de uitvoering van de Diensten alle noodzakelijke zorg betrachten om te vermijden dat (nader) forensisch onderzoek niet goed meer kan worden uitgevoerd of de resultaten daarvan niet goed (meer) zouden kunnen worden vertrouwd.		x		Dienstverlening	
PR9.8	Indien de Dienst bestaat uit het uitvoeren van forensisch (digitaal) onderzoek, zal Opdrachtnemer zorgdragen voor het aantoonbaar maken van de bevindingen om als bewijsmateriaal te kunnen dienen in strafrechtelijke of civielrechtelijke rechtszaken en op een voor dat doeleinde deugdelijke en betrouwbare wijze bijhouden wie op ieder moment toegang had tot of beschikking had over het bewijsmateriaal ('chain of custody').			x	Dienstverlening	
PR9.9	Na afloop van een incident zal Opdrachtnemer alle gegevens over [Deelnemer], diens werknemers of overige relaties die Opdrachtnemer heeft verwerkt, vernietigen of terug leveren aan [Deelnemer], met uitzondering van gegevens die (a) Opdrachtnemer nodig heeft om zich gereed te houden om bij een volgend incident zo snel en effectief mogelijk op te treden en (b) Opdrachtnemer op grond van de wet verplicht is te bewaren. Op verzoek van [Deelnemer] verstrekt Opdrachtnemer inzage in de gegevens die Opdrachtnemer bewaart om zich gereed te houden om bij een volgend incident zo snel en effectief mogelijk op te treden. Voor zover Opdrachtnemer verplicht is om na afloop van de opdracht dergelijke gegevens te bewaren, zal Opdrachtnemer [Deelnemer] deugdelijk informeren over welke (categorieën) gegevens bewaard moeten worden en op grond van welke specifieke wettelijke verplichtingen.		x		Dienstverlening	
PR9.10	Opdrachtnemer dient aan te tonen dat hij passende technische en organisatorische beveiligingsmaatregelen heeft geïmplementeerd om persoonsgegevens en andere gevoelige gegevens van (medewerkers, klanten of andere relaties van) [Deelnemer] te kunnen verwerken.		x		Dienstverlening	
PR9.11	De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.		x		Dienstverlening	
PR9.12	Privacyverklaring: De organisatie heeft een privacyverklaring waarin is beschreven op welke wijze persoonsgegevens worden verwerkt en hoe een betrokkene, zijn of haar rechten kan uitoefenen.		x		Dienstverlening	
PR9.12.1	Opdrachtnemer werkt mee aan verzoeken van betrokkenen die hun rechten willen uitoefenen.		x		Dienstverlening	
PR9.13	Vertrouwelijkheid/Integriteit: Opdrachtnemer zal bij de uitvoering van de Diensten geen handelingen verrichten die de vertrouwelijkheid, integriteit en/of beschikbaarheid van de systemen van [Deelnemer] en/of de daarop verwerkte gegevens in gevaar kan brengen.		x		Dienstverlening	

PR9.14	DPIA (data protection impact assessment): Inschrijver kan een actuele DPIA overleggen op de SOC-dienst waarin: • Minimaal wordt beschreven welke risico's en kwetsbaarheden voor de vrijheden en rechten van betrokkenen bij de verwerking verwacht worden/ontstaan. • Welke maatregelen kunnen worden genomen om bovengenoemde risico's en kwetsbaarheden te mitigeren. • De DPIA dient minimaal 1 keer per jaar te worden her beoordeeld. De DPIA dient minimaal 1 keer per 3 jaar te worden herhaald.		x		Dienstverlening	
PR9.15	Inschrijver kan aantonen de maatregelen benoemd in de eigen DPIA te hebben geïmplementeerd.		x		Dienstverlening	
PR9.16	Inschrijver zal kosteloos meewerken aan de uit te voeren DPIA door [Deelnemer].		x		Dienstverlening	
PR9.17	Inschrijver zal kosteloos meewerken aan de uit te voeren IAMA door [Deelnemer].		x		Dienstverlening	
PR9.18	Opdrachtnemer draagt er zorg voor dat bij de uitvoering van de werkzaamheden niet meer persoonsgegevens of andere gevoelige gegevens worden ingezien of anderszins verwerkt dan werkelijk noodzakelijk voor het correct uitvoeren van de Opdracht.		x		Dienstverlening	
PR9.19	Privacybeleid: De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.		x		Dienstverlening	
PR9.20	Privacy-organisatie: De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld, inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.		x		Dienstverlening	
PR9.21	Privacy-bewustzijn: De organisatie waarborgt dat eenieder die de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.		x		Dienstverlening	
PR9.22	Formele vastlegging handelen verwerkingsverantwoordelijke: De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.		x		Dienstverlening	
PR9.23	Privacy in de levenscyclus: Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacy-risico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.		x		Dienstverlening	
PR9.24	Register van verwerkingsactiviteiten: De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.		x		Dienstverlening	
T10.1	De IT-infrastructuur van de [Deelnemer] is sterk Microsoft georiënteerd. Alle diensten die ingezet worden voor de dienstverlening Monitoring en Alarmering moet derhalve compatibel zijn met Microsoft producten en diensten.		x		Dienstverlening	
T10.2	Opdrachtnemer is verantwoordelijk voor het, in afstemming met Opdrachtgever, opleveren van Playbooks t.b.v. incidentafhandeling. Deze worden beschikbaar gesteld aan [Deelnemer]		x		Dienstverlening	
T10.3	Opdrachtnemer moet uitwisselingsprotocollen voor dreigingsinformatie ondersteunen (zoals STIX / TAXII). Hiermee moet Opdrachtnemer in staat zijn dreigingsinformatie met [Deelnemer] te delen, of van [Deelnemer] te ontvangen voor verdere analyse binnen de dienstverlening.		x		Dienstverlening	
T10.4	Opdrachtnemer sluit aan op het incident response proces van [Deelnemer] en een nog aan te wijzen VR-Knooppunt (bijvoorbeeld technische aansluiting op Topdesk, of een veilige email). Informatie-uitwisseling vindt op een veilige manier plaats.		x		Dienstverlening	
T10.5	Opdrachtnemer dient zorg te dragen voor een alarmeringsmechanisme dat is toegespitst op de impact van een melding (bijv. bellen bij een critical, mail bij een lagere prioriteit).		x		Dienstverlening	
T10.6	Toegang voor [Deelnemer] tot de oplossing en bijbehorende functionaliteit zoals dashboards of rapportages wordt ingericht volgens een Role Based Access Control Model (RBAC).		x		Dienstverlening	
T10.7	Toegang voor [Deelnemer] tot het monitoringsplatform geschiedt op basis van Single-SignOn, incl. MFA.		x		Dienstverlening	
T10.7.1	Toegang voor [Deelnemer] tot het monitoringsplatform heeft de mogelijkheid om in geval van calamiteiten en gemis aan centrale authenticatie mechanismes (LDAP, SSO, AD etc) te authenticeren met een lokaal account.			x	Dienstverlening	
T10.8	De interface van het aan te bieden dashboard dient te functioneren zonder noodzaak voor het installeren van plug-ins bij gebruikers en geheel op basis van gangbare veilige technologie.		x		Dienstverlening	
T10.9	Opdrachtnemer stelt na monitoring een baseline (=normaal gedrag van apps en netwerkverkeer) vast voor [Deelnemer]. Voor wijzigingen in infrastructuur en inrichting bij [Deelnemer], zal een change management proces gevolgd worden.		x		NDR, EDR, SIEM	
T10.10	Opdrachtnemer detecteert afwijkingen van de baseline en signaleert dit bij [Deelnemer] inclusief context en analyse.		x		NDR, EDR, SIEM	
T10.10.1	Opdrachtnemer detecteert afwijkingen van de baseline en signaleert dit bij [Deelnemer] inclusief context en analyse. minimaal, maar niet uitsluitend: - lateraal verkeer tussen endpoints - a-specifiek serververkeer (DNS request naar een niet DNS-server bijv.) - Scanactviteiten (bijv. nmap) - detectie op afwijkend aansturingsgedrag - detectie op toevoegen van machines	Optie 1		x	NDR, EDR, SIEM	Deze optie gaat wel uit van een NDR oplossing, vervangt T10.10 Gaat niet samen met T10.10.2 & T10.10.3
T10.10.2	Opdrachtnemer detecteert afwijkingen van de baseline en signaleert dit bij [Deelnemer] inclusief context en analyse. minimaal, maar niet uitsluitend: - lateraal verkeer tussen endpoints - a-specifiek serververkeer (DNS request naar een niet DNS-server bijv.) - Scanactviteiten (bijv. nmap) - detectie op afwijkend aansturingsgedrag - detectie op toevoegen van machines - detectie op internetverkeer (layer 0, 1 en 2 indien afwijkend van de baseline) - detectie op basis van configuratiehandelingen in (afwijkend van de baseline) zoals het uploaden en downloaden van configuraties of het aanmaken van admin accounts. Dit alles bij unencrypted communicatieverkeer.	Optie 2		x	NDR, EDR, SIEM	Deze optie gaat wel uit van een NDR oplossing, vervangt T10.10 Gaat niet samen met T10.10.1 & T10.10.3

T10.10.3	Opdrachtnemer detecteert afwijkingen van de baseline en signaleert dit bij [Deelnemer] inclusief context en analyse. minimaal, maar niet uitsluitend: - lateraal verkeer tussen endpoints - a-specifiek serververkeer (DNS request naar een niet DNS-server bijv.) - Scanactviteiten (bijv. nmap) - detectie op afwijkend aansturingsgedrag - detectie op toevoegen van machines - detectie op internetverkeer (layer 0, 1 en 2 indien afwijkend van de baseline) - detectie op basis van configuratiehandelingen (afwijkend van de baseline) zoals het uploaden en downloaden van configuraties of het aanmaken van admin accounts. Dit alles bij unencrypted communicatieverkeer. - detecteren & signaleren op onion exit (TOR) nodes - detectie van traffic flooding / DOS aanvallen	Optie 3		x	NDR, EDR, SIEM	Deze optie gaat wel uit van een NDR oplossing, vervangt T10.10 Gaat niet samen met T10.10.1 & T10.10.2
T10.11	Opdrachtnemer kan User & Entity Behavior Analythics (UEBA) capabilities leveren als onderdeel van de dienstverlening.			x	SIEM	
T10.12	Binnen de IT-infrastructuur van de [Deelnemer] wordt ook gebruik gemaakt van Linux systemen. Alle diensten die ingezet worden voor de dienstverlening Monitoring en Alarmering moet derhalve compatibel zijn met Linux producten en diensten.		x		Dienstverlening	
T10.13	Opdrachtnemer voert (waar gewenst) threat hunting uit op het digitale landschap van [Deelnemer] als onderdeel van de overeenkomst.			x	Dienstverlening	
T10.14	Opdrachtnemer adviseert Opdrachtgever continu over het toevoegen van security sensoren of het her-configureren van systemen in [Deelnemer] IT-infrastructuur om blinde vlekken in de security monitoring te adresseren.			x	Dienstverlening	Dit wordt vereist als aanbieder sensoren gaat aanbieden
T10.15	Opdrachtnemer heeft de mogelijkheid om eventuele output te gebruiken van vulnerability management, configuratie management en risk management processen van [Deelnemer] in de dienstverlening om de detectie mogelijkheden van dreigingen en incidenten te verbeteren.			x	Dienstverlening	Vereist van [Deelnemer] dat er een vulnerability oplossing aanwezig is.
T10.16	De SOC-dienst dienstverlening wordt door de Opdrachtgever flexibel aangeboden, dat wil zeggen: Uitbreidbaar wanneer het IT-landschap van de Opdrachtgever groeit of migreert (on-prem naar Cloud bijv) of wanneer er (nieuwe) bronnen bij komen of worden vervangen.		x		Dienstverlening	
T10.17	Opdrachtnemer geeft in de aanbieding aan in hoeverre zij de logdata, die wordt gegenereerd door producten en diensten in gebruik bij [Deelnemer], kunnen opnemen in de dienstverlening.		x		Logging	
T10.18	De standaard retentietijd van log- en eventdata en het auditlog is minimaal cf. wet- en regelgeving. Op basis van de BIO geldt een retentietijd van minimaal 6 maanden. Opdrachtnemer zorgt er ook voor dat informatie over security incidenten en betrokken data niet verloren gaan, hiertoe zijn aantoonbaar afdoende maatregelen genomen om verlies van informatie te voorkomen.		x		Logging	
T10.19	Indien [Deelnemer] gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, wordt deze zodanig opgeslagen dat de beschikbaarheid, integriteit en vertrouwelijkheid gegarandeerd is, deze gedeeld kan worden voor analyse van historische data (forensisch en post-mortem).		x		Logging	
T10.19.1	Indien [Deelnemer] gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, wordt deze zodanig opgeslagen dat de beschikbaarheid, integriteit en vertrouwelijkheid gegarandeerd is, deze gedeeld kan worden voor analyse van historische data (forensisch en post-mortem) en als bewijsmateriaal gebruikt kan worden in strafzaken.	Optie 1		x	Logging	
T10.20	Indien [Deelnemer] gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, dienen analyse danwel delen van de (eigen) log- en eventdata geëxporteerd te kunnen worden voor archivering buiten de systemen van de Opdrachtnemer.			x	Logging	
T10.21	De dienstverlening moet in staat zijn om de event tijd te corrigeren voor systemen met een onjuiste tijdaanduiding, bijvoorbeeld door een foutieve tijdzone instelling. De integriteit van de timestamp moet gegarandeerd blijven.		x		Logging	
T10.22	Log- en eventdata met een onjuiste tijdsaanduiding moet worden gesignaleerd als incident.		x		Logging	
T10.23	De Opdrachtnemer draagt zorg dat er geen hardware van de Opdrachtnemer geïnstalleerd hoeft te worden in de netwerken van [Deelnemer] om de SOC dienst te doen laten functioneren. [Deelnemer] is zelf verantwoordelijk voor het verzamelen van logdata en het ter beschikking stellen van die data aan de Opdrachtnemer. Indien additionele sensoren/ systemen benodigd zijn voor het ontsluiten van benodigde logdata dan zal [Deelnemer] deze aanschaffen, in gebruik nemen en beheren.	Optie 1		x	Logging	Als T10.23.1 of T10.23.2 word gekozen vervalt deze en vice versa
T10.23.1	[Deelnemer] is zelf verantwoordelijk voor het verzamelen van logdata en het ter beschikking stellen van die data aan de Opdrachtnemer. Indien additionele sensoren/ systemen benodigd zijn voor het ontsluiten van benodigde logdata dan zal [Deelnemer] deze aanschaffen, in gebruik nemen en beheren.	Optie 2		x	Logging	Als T10.23 of T10.23.2 word gekozen vervalt deze en vice versa
T10.23.2	Opdrachtnemer is verantwoordelijk voor het verzamelen van logdata. Indien additionele sensoren/ systemen benodigd zijn voor het ontsluiten van benodigde logdata dan zal Opdrachtnemer deze aanschaffen, in gebruik nemen en beheren.	Optie 3		x	Logging	Als T10.23 of T10.23.1 word gekozen vervalt deze en vice versa
T10.24	Normaliseren van de door [Deelnemer] aangeleverde logging aan de Opdrachtnemer, is een verantwoordelijkheid van de Opdrachtnemer.		x		Logging	
T10.25	Indien [Deelnemer] gebruik maakt van de optie om de log – en event data op te slaan bij Opdrachtnemer, dient deze op een veilige en versleutelde wijze verzonden te kunnen worden naar de Opdrachtnemer.		x		Logging	
T10.26	De Opdrachtnemer is in staat om een netwerkvisualisatie op te leveren op basis van de ontsloten logdata.			x	NDR	
T10.27	Opdrachtnemer zal als onderdeel van de dienstverlening op IT data Deep Packet Inspection (DPI) analyse uitvoeren.			x	NDR	Vereist een NDR oplossing
T10.28	Als het verdienmodel van de dienstverlening gebaseerd is op de hoeveelheid te verwerken data, moeten de maandelijkse dataverbruikskosten gebaseerd zijn op de daadwerkelijk noodzakelijke data om monitoring effectief en efficiënt te laten zijn. Opdrachtnemer adviseert periodiek of optimalisatie mogelijk is en neemt hierin ook proactief stappen.		x		Dienstverlening	
T10.29	De dienstverlening dient aantoonbaar 99,99% per maand beschikbaar te zijn.		x		Dienstverlening	
T10.30	Opdrachtnemer maakt gebruik van artificial intelligence (AI) en machine learning (een specifieke subset van AI) om onbekende bedreigingen en afwijkend gedrag op te sporen.		x		Dienstverlening	
T10.31	Opdrachtnemer dient een SOAR-platform (Security Orchestration, Automation and Respons) aan te bieden als aanvulling op de SIEM oplossing. Waarbij de randvoorwaarde geldt dat er enkel geautomatiseerd ingegrepen wordt in overeenstemming met expliciete toestemming van [Deelnemer]. Dit is een toekomstbestendigheidseis.			x	SIEM, SOAR	
T10.32	Het gebruik van de dienstverlening mag nagenoeg geen nadelige invloed hebben op de prestaties van de te monitoren omgeving.		x		NDR, EDR	
T10.33	Opdrachtnemer borgt dat endpointdata niet op de endpoints zelf wordt opgeslagen maar binnen de EER, in overeenstemming met de geldende eisen en conform overeengekomen beveiligingsmaatregelen.		x		EDR	
T10.34	Opdrachtnemer voorziet in de mogelijkheid om IoT-apparaten te monitoren met behulp van een EDR oplossing binnen de SOC-dienstverlening.			x	EDR	
T10.35	Opdrachtnemer faciliteert isolatie van systemen of onderdelen binnen het netwerk (bijvoorbeeld “Stekkermandaat”) wanneer daartoe aanleiding is in het kader van incidentrespons.			x	EDR	
T10.36	Opdrachtnemer biedt multiplatformondersteuning voor de monitorings- en detectietools, zodat de dienstverlening device- en platformonafhankelijk kan plaatsvinden.			x	EDR	
T10.37	De Opdrachtnemer draagt zorg voor het beschikbaar houden van logdata d.m.v. caching voor NDR voor een periode van minimaal 48 uur in het geval (netwerk)verstoringen.		x		NDR, Logging	
T10.38	De Opdrachtnemer draagt zorg voor het beschikbaar houden van logdata d.m.v. caching voor SIEM voor een periode van minimaal 48 uur in het geval (netwerk)verstoringen.		x		SIEM, Logging	

T10.39	Opdrachtnemer zorgt dat het SIEM integreert met de meest voorkomende NDR-oplossingen, zodat de gewenste functionaliteit voor [Deelnemer] kan worden geborgd.			x	NDR	Als [Deelnemer] beschikt over deze capabilities wordt dit een baseline
T10.40	Opdrachtnemer zorgt dat het SIEM integreert met de meest voorkomende EDR oplossingen, zodat de gewenste functionaliteit voor [Deelnemer] kan worden geborgd.			x	EDR	Als [Deelnemer] beschikt over deze capabilities wordt dit een baseline
T10.41	Opdrachtnemer waarborgt dat het SIEM importmogelijkheden biedt voor alle gangbare vormen van logging.		x		SIEM	
T10.42	Opdrachtnemer biedt toegang tot het SIEM via Single Sign-On (SSO). In geval van calamiteiten is lokaal inloggen mogelijk.		x		SIEM	
D4.29	Opdrachtnemer kan dreigingsinformatie afkomstig van [Deelnemer] opnemen en verwerken binnen de SOC-dienstverlening.		x		Dienstverlening	
D4.30	Opdrachtnemer faciliteert forensisch onderzoek dat voldoet aan de geldende normeringen en wet- en regelgeving (BIO, NIS2, NEN7510, “Gele Pas”, enz.).			x	Dienstverlening	
A1.18	Er mag vanuit de Opdrachtnemer geen enkele relatie of inmenging zijn met landen met een offensief cyberprogramma.		x		Dienstverlening	
T10.43	De Opdrachtnemer is in staat om zelf een NDR oplossing te bieden als onderdeel van de MDR dienstverlening			x	NDR	
A1.19	Opdrachtnemer ondertekent een geheimhoudingsverklaring en verplicht zich vertrouwelijk om te gaan met alle informatie die in het kader van de overeenkomst ter kennis komt.		x		Dienstverlening	
A1.20	Opdrachtnemer verklaart dat na gunning en ondertekening van het Contract geen nieuwe Onderaannemers worden ingezet, tenzij hiervoor voorafgaand schriftelijke toestemming is verleend door Opdrachtgever.		x		Dienstverlening	
D4.31	Opdrachtnemer levert gedurende de voorbereiding, implementatie, livegang en nazorg één vaste, integraal verantwoordelijke projectleider, die verantwoording aflegt aan [Later te bepalen onderdeel van deelnemer]		x		Dienstverlening	
T10.44	Opdrachtnemer specificeert indien externe (VPN) verbindingen benodigd zijn voor communicatie of beheer van de oplossing.		x		Dienstverlening	
D4.32	Opdrachtnemer werkt bij een security-incident indien noodzakelijk samen met bestaande (IT-)dienstverleners van Opdrachtgever en neemt hierin een (leidende) rol. Opdrachtnemer wordt gemandateerd om rechtstreeks te schakelen met deze dienstverleners voor het uitvragen van informatie en het voorbereiden van changeverzoeken. De uiteindelijke besluitvorming over het doorvoeren van mitigatiemaatregelen blijft de verantwoordelijkheid van Opdrachtgever.		x		Dienstverlening	
D4.33	Opdrachtnemer verstrekt op verzoek van Opdrachtgever technische details (RCA) van incidenten en de getroffen maatregelen. Opdrachtgever behoudt het recht deze informatie te delen met een derde partij voor verdere analyse of infrastructuuraanpassingen.		x		Dienstverlening	
T10.45	Opdrachtnemer implementeert een Network-Based Intrusion Detection System (IDS) en Intrusion Prevention System (IPS). Netwerksensoren worden zodanig aangesloten dat er geen dataterugvloeiing naar het netwerk kan plaatsvinden en geen ongeautoriseerde toegang tot het netwerk mogelijk is.			x	NDR	
D4.34	Opdrachtnemer ontwikkelt indien noodzakelijk passende connectoren voor componenten die niet standaard kunnen worden aangesloten op de gebruikte producten binnen de oplossing.		x		Dienstverlening	
D4.35	Opdrachtnemer licht op verzoek toe op welke wijze risicomanagement binnen de dienstverlening is ingericht.		x		Dienstverlening	
A1.21	Telefonische meldingen worden door Opdrachtnemer altijd schriftelijk bevestigd.		x		Dienstverlening	
D4.36	Opdrachtnemer levert periodiek, bijvoorbeeld wekelijks, een overzicht met relevante dreigingsinformatie, ontwikkelingen en nieuws op wereldwijd niveau.			x	Dienstverlening	
D4.37	Opdrachtnemer geeft zowel gevraagd als ongevraagd advies over welke security use cases geïmplementeerd dienen te worden.		x		Dienstverlening	
D4.38	Opdrachtnemer verschaft inzicht in de verbeteringscyclus van de monitoringdiensten, inclusief maatregelen om het aantal false positives te reduceren en de detectie van true positives te verbeteren.		x		Dienstverlening	
D4.39	Opdrachtnemer stelt een team van deskundigen beschikbaar tijdens cyberoefeningen en bij feitelijke cyberaanvallen.			x	Dienstverlening	
T10.46	Alle internetgebruikersinterfaces van de oplossing worden beveiligd met Multi-Factor Authentication.		x		Dienstverlening	
PR9.25	Opdrachtnemer waarborgt dat alle gegevensoverdracht end-to-end versleuteld, correct geverifieerd en beveiligd is. Opdrachtnemer specificeert het gebruikte encryptie-algoritme.		x		Dienstverlening	
D4.40	Het dashboard is aanpasbaar, zodat beheerders het kunnen configureren naar individuele behoeften. Het bevat een realtime samenvatting van beveiligingsincidenten.			x	Dienstverlening	
D4.41	De oplossing beschikt over een geïntegreerde Knowledge Base-functionaliteit waarmee systeem- en omgevingsspecifieke informatie wordt vastgelegd en toegankelijk is voor analisten.			x	Dienstverlening	
T10.47	Indien de oplossing webbased is, functioneert deze minimaal op de meest actuele versies van de veel gebruikte webbrowers.		x		Dienstverlening	
D4.42	Opdrachtnemer levert volledige en actuele documentatie van alle aangeboden API’s en webservices.			x	Dienstverlening	
D4.43	Foutmeldingen in de oplossing zijn zelfbeschrijvend en bevatten voldoende detail voor analyse. Foutmeldingen vormen geen beveiligingsrisico.		x		Dienstverlening	
D4.44	Nieuwe releases behouden alle eerder uitgevoerde wijzigingen en configuraties.		x		Dienstverlening	
D4.45	De oplossing ondersteunt organisatiestructuren, inclusief de indeling van gebruikers binnen interne en externe entiteiten.		x		Dienstverlening	
PR9.26	Opdrachtnemer waarborgt dat alle data van [Deelnemer] minimaal logisch gescheiden is van andere klanten en dat de security en performance niet worden beïnvloed door andere gebruikers van de dienst.		x		Dienstverlening	
D4.46	Opdrachtnemer stelt trainingsdocumentatie beschikbaar en stemt deze voorafgaand aan de livegang af met [Deelnemer].		x		Dienstverlening	
T10.48	Security-incidenten worden geregistreerd in het ticketsysteem van Opdrachtnemer en automatisch uitgewisseld met Opdrachtgever. De registratie bevat minimaal: - Uniek referentienummer - Type bedreiging (dreiging of daadwerkelijk incident) - Datum en tijdstip van detectie en registratie - Naam van betrokken medewerkers - Impact en bedreigingsniveau - Technische details, inclusief IP-adressen en poorten - Aanbevolen maatregelen		x		Logging	
D4.47	Opdrachtnemer is volledig verantwoordelijk voor het lifecyclemanagement, updates en upgrades van de componenten binnen de dienstverlening. Kosten hiervoor zijn inbegrepen in het prijsmodel.		x		Dienstverlening	
D4.48	Preventief onderhoud wordt uitsluitend uitgevoerd binnen vooraf overeengekomen onderhoudsvensters.		x		Dienstverlening	
D4.49	Opdrachtnemer beoordeelt periodiek de logconfiguratie, ondersteunt bij configuratie en bewaakt de correctheid van ontvangen loggegevens.		x		Dienstverlening	
VR11.1	Opdrachtnemer zal in loop der tijd aansluiten op het VR-knooppunt, dit zal zowel op technisch niveau en waar mogelijk ook op dienstverlening niveau mogelijk moeten zijn.		x		Dienstverlening	
VR11.2	Opdrachtnemer zal alle medewerking bieden die nodig is in het goed laten verlopen van de relatie tussen [Deelnemer], VR-Knooppunt & Opdrachtnemer.		x		Dienstverlening	
VR11.3	Communicatie tussen [Deelnemer], VR-Knooppunt & Opdrachtnemer is op allerlei manieren mogelijk middels (maar niet gelimiteerd tot): - Mail - Telefoon - Chat (bijv. MS Teams) - Ticketing systeem In alle zaken waarbij eerst verbaal contact is geweest wordt het naderhand en z.s.m. schriftelijk bevestigd		x		Dienstverlening	

VR11.4	Het delen informatie over dreigingen, incidenten en andere noemenswaardigheden is op allerei manieren mogelijk middels (maar niet gelimiteerd tot): - Mail - Telefoon - MISP - Ticketing systeem Waarbij de automatiseren de voorkeur geniet. In alle zaken waarbij eerst verbaal contact is geweest wordt het naderhand en z.s.m. schriftelijk bevestigd		x		Dienstverlening	
VR11.5	Technische informatie (IOC) wordt zo compleet mogelijk en zo snel mogelijk gedeeld met het VR-Knooppunt, waarbij informatie minimaal (en waar toepasselijk) bestaat uit (maar niet gelimiteerd tot): - IP adres - Hash (meerdere varianten mogelijk, MD5, SHA etc..) - URL - Domein namen - Payloads		x		Dienstverlening	
VR11.6	Opdrachtnemer stelt een vast aanspreekpunt aan voor het VR-Knooppunt, dit aanspreekpunt is op kantoordagen bereikbaar tussen 08:30 en 17:00.		x		Dienstverlening	
VR11.7	Opdrachtnemer stelt een vast aanspreekpunt aan voor het VR-Knooppunt, dit aanspreekpunt is 24/7 bereikbaar			x	Dienstverlening	
VR11.8	Opdrachtnemer is verantwoordelijk voor het aanleveren van de juiste contactgegevens voor het aanspreekpunt zoals aangegeven in VR6 of VR6.1. Ook in het geval van ziekte of vakantie.		x		Dienstverlening	