Nota van inlichtingen selectiefase

Europese aanbesteding SOC/MDR-diensten samenwerkende Veiligheidsregio's en NIPV

Betreft: Nota van Inlichtingen
Kenmerk: NIPV2026-EA-04749
Datum: 24-06-2026
Status: Definitief

In deze Nota van Inlichtingen geeft de Aanbestedende Dienst antwoord op de gestelde vragen en wijzigingsvoorstellen die in het kader van de Aanbesteding 'SOC/MDR-diensten' zijn geplaatst. De Nota van Inlichtingen maakt integraal onderdeel uit van de aanbestedingsdocumenten. Eventuele wijzigingen die zijn toegezegd aan het Programma van Eisen worden in de gunningsfase verwerkt in een nieuwe versie van het Programma van Eisen.

Vraagnr.	Paragraaf, Artikelnaam	Vraag	Antwoord
1	Paragraaf 2.2	Paragraaf 2.2 stelt dat M-EDR de baseline is en SIEM optioneel. Binnen het PVE en deze paragraaf staan echter veel meer eisen beschreven dan dat een standaard M-EDR zou leveren (denk aan use case beheer, logdata ontsluiting, training, etc). Betekent dit dat EDR als baseline het minimale is wat de deelnemers moeten kunnen aansluiten zodat monitoring kan plaatsvinden, of is M-EDR de dienst die aangeboden moet worden?	Managed EDR is de verplichte baseline (minimale afname per Deelnemer). De aangeboden dienst is de volledige managed MDR/SOC-dienstverlening conform Paragraaf 2.2, waarvan onderdelen als use case beheer, ontsluiting van logdata, detectie en respons integraal deel uitmaken. NDR en aanvullende SIEM-logbronnen zijn optionele uitbreidingen op de baseline.
2	Paragraaf 2.2, Eis 5.27 en Eis 5.28	Paragraaf 2.2 stelt dat NDR optioneel is, maar het PvE maakt in E5.27 en E5.28 een onderscheid tussen twee dingen: integreren met NDR-oplossingen (E5.27) en zelf NDR leveren (E5.28). Zijn dit twee aparte eisen die los van elkaar worden beoordeeld? En is E5.28 een knock-out voor alle inschrijvers, of alleen relevant als een deelnemer NDR wil afnemen?	Het zijn twee afzonderlijke eisen die zelfstandig worden beoordeeld. E5.27 betreft integratie van het SIEM met gangbare NDR-oplossingen, E5.28 het zelf kunnen leveren van NDR binnen de MDR-dienstverlening. Beide zijn eisen en gelden voor alle inschrijvers: de optionaliteit zit in de afname door de Deelnemer, niet in de capability die Opdrachtnemer moet kunnen bieden. E5.28 is dus een capability-eis, ook wanneer een Deelnemer geen NDR afneemt.
3	Eis 6.04	E6.04 stelt dat opdrachtnemer minimaal twee opslagmodellen ondersteunt. In de markt zien we echter een duidelijke verschuiving naar opslag binnen de eigen tenant van de klant, juist vanwege data-soevereiniteit, kostenbesparing en een eenvoudigere exitstrategie — de data blijft immers altijd bij de deelnemer zelf. Het verplicht aanbieden van Model B leidt tot onnodige extra kosten, terwijl deelnemers met een volwaardige Microsoft-tenant hier weinig toegevoegde waarde van zien. Is de aanbestedende dienst bereid deze eis aan te passen zodat één opslagmodel volstaat, mits beschikbaar voor alle deelnemers?	Nee. Beide opslagmodellen blijven bestaan en de Opdrachtnemer faciliteert ze beide. Uitsluitend Model A aanbieden zou Deelnemers zonder eigen geschikte omgeving uitsluiten, tenzij zij hun licentie- of opslagstructuur aanpassen, en dat mag niet worden afgedwongen. Model A kent twee varianten: variant 1, opslag binnen de eigen omgeving of infrastructuur van de Deelnemer (bijvoorbeeld Microsoft Sentinel in de Deelnemer-tenant of een equivalent zoals een eigen datalake), en variant 2, opslag binnen het door de Deelnemer gebruikte ecosysteem onder licentie of beheer van de Opdrachtnemer (bijvoorbeeld Microsoft Defender/Sentinel). Model B blijft beschikbaar voor wie daarvoor kiest. De keuze ligt per Deelnemer, wordt vastgelegd in de Nadere Overeenkomst en kent een afzonderlijk tarief in het Prijzenblad.

4	Eis 6.12	E6.12 vereist 48-uurs caching van logdata bij netwerkstoringen. Geldt deze verplichting ook bij Model A, waarbij de data in de klanttenant staat en opdrachtnemer geen eigen opslaglaag beheert om caching te realiseren?	Ja, E6.12 geldt voor beide opslagmodellen. De eis is uitkomstgericht: Opdrachtnemer borgt dat log- en eventdata bij (netwerk)verstoringen minimaal 48 uur behouden blijft en na herstel wordt nagestuurd. Onder Model A vindt deze buffering plaats op de collectie- of forwarderlaag in de omgeving van de Deelnemer; Opdrachtnemer is verantwoordelijk voor het zodanig dimensioneren van de buffercapaciteit dat de 48 uur ook bij het verwachte datavolume wordt gehaald.
5	Eis 7.04	E7.04 stelt proactief threat hunting als verplicht maar geeft geen frequentie of scope. Wat is de minimaal verwachte frequentie per Deelnemer, en geldt er een minimale rapportageverplichting voorafgaand aan de eerste afstemming in het Stand-van-Zaken Security-overleg?	E7.04 schrijft geen centraal vastgestelde minimumfrequentie voor. Threat hunting is een verplichte, doorlopende activiteit binnen de dienst; de focusgebieden, frequentie en rapportage worden per Deelnemer risicogebaseerd afgestemd in het Stand-van-Zaken Security-overleg (E7.04 in samenhang met E7.02). De wijze waarop Opdrachtnemer threat hunting invult, waaronder frequentie en rapportage, wordt als gunningscriterium beoordeeld. Er geldt geen aparte minimale rapportageverplichting vóór de eerste afstemming; juist die afstemming legt de kaders, frequentie en rapportagevorm vast.
6	Eis 3.03	In E3.03 wordt aangegeven dat de daadwerkelijke monitoring 24/7 moet zijn voor alle niveaus maar bij niveau 3 wordt "geen actieve monitoring buiten deze tijden" aangegeven. Bij Niveau 2 (buiten het piket voor P1/P2) en Niveau 3 (buiten kantoortijden) kan een incident gedurende een periode onopgevolgd blijven, met mogelijke gevolgschade tot gevolg. Kan de aanbestedende dienst bevestigen dat dit restrisico een bewuste en geaccepteerde keuze van de individuele deelnemer is, en dat de opdrachtnemer niet aansprakelijk of verantwoordelijk is voor de gevolgen van incidenten die zich buiten het gekozen servicevenster voordoen en daardoor niet of vertraagd worden opgevolgd? Heeft de aanbestedende dienst, gezien de aard van de veiligheidsregio's als vitale aanbieders, overwogen om 24/7 eyes-on-screen als minimale baseline te hanteren?	De daadwerkelijke monitoring is bij alle drie de niveaus 24/7: de detectie- en monitoringsystemen draaien continu door, inclusief collectie, detectie, alarmering en logging. Het onderscheid tussen de niveaus betreft de bemenste opvolging (eyes-on-screen en response), niet de monitoring zelf. Alarmen die buiten het bemenste venster ontstaan, worden gedetecteerd en vastgelegd en bij aanvang van het eerstvolgende bemenste venster opgevolgd; bij niveau 2 geldt daarbij 24x7 piket voor P1- en P2-alarmen. De keuze voor een niveau is een bewuste, risicogebaseerde keuze van de individuele Deelnemer, vastgelegd in de Nadere Overeenkomst. Opdrachtnemer levert conform het gekozen niveau; de aansprakelijkheidsverdeling volgt uit de overeenkomst. AD schrijft geen uniforme 24/7-baseline voor:

			niveau 1 is beschikbaar en elke Deelnemer kiest op basis van eigen risicomanagement.
7	Eis 7.10 en Eis 7.11	E7.10 en E7.11 stellen dat deelnemers onbeperkt use cases mogen inbrengen en dat opdrachtnemer actief ondersteunt bij het opstellen en uitwerken hiervan, zonder extra kosten. Wij ondersteunen dit principe, maar zonder enige beperking kan dit in de praktijk leiden tot een situatie waarbij deelnemers dagelijks nieuwe use cases inbrengen, wat een onevenredige belasting op de dienstverlening legt. Kan de aanbestedende dienst een redelijke grens stellen aan het aantal kosteloos te ontwikkelen use cases per periode, of aangeven wat onder "actieve ondersteuning" wordt verstaan in termen van maximale inspanning?	Ja. In plaats van een onbeperkt aantal hanteert de Aanbestedende Dienst een afgebakend en collectief georganiseerd model. De Opdrachtnemer levert een standaard pakket use cases dat doorlopend en kosteloos wordt onderhouden en uitgebreid (E7.09). Dit wordt aangevuld met maximaal 20 sectorspecifieke use cases, die de deelnemersgroep onderling organiseert en als collectief per kwartaal aandraagt ter afstemming met de Opdrachtnemer. Het maximum van 20 is leidend; hiervan wordt uitsluitend afgeweken met goedkeuring van de Opdrachtnemer. Incidenteel kunnen, waar nodig voor de veiligheid, buiten de kwartaalcyclus use cases worden toegevoegd in overleg met de Opdrachtnemer. "Actieve ondersteuning" is daarmee begrensd tot dit collectief afgestemde volume en de uit de toepasselijke kaders voortvloeiende use cases (E7.12); een ongelimiteerde, dagelijkse instroom is niet aan de orde.

8	Paragraaf 2.2	Paragraaf 2.2 noemt vulnerability management als optionele uitbreiding maar het PVE bevat geen eisen of wensen ten aanzien van deze dienst. Kan aangegeven worden welke minimale eisen er zijn aan deze optionele dienst?	Vulnerability management wordt in deze aanbesteding niet als gespecificeerde dienst uitgevraagd. Paragraaf 2.2 noemt het uitsluitend als mogelijke optionele uitbreiding; er zijn daarom geen minimale eisen opgenomen. Indien een Deelnemer hieraan behoefte heeft, kan dit in overleg via een Nadere Overeenkomst worden ingevuld.
9	Bijlage 10 Programma van Eisen, E 1.02	U vraagt tal van eisen die feitelijk pas goed beoordeeld kunnen worden in de gunningsfase op basis van de concrete uitvraag en aanbestedingsstukken die dan worden gedeeld. Kunt u derhalve toelichten wat u van inschrijver verwacht aan akkoordverklaring van alle stukken, bepalingen en voorbehouden voor zover die in deze selectiefase nog onbekend zijn maar die pas bij gunningsfase worden gepubliceerd?	In de selectiefase wordt geen volledig akkoord verlangd met nog niet gepubliceerde gunningsstukken. In de selectiefase wordt uitsluitend beoordeeld op uitsluitingsgronden, geschiktheidseisen en selectiecriteria (§3.8 Selectiedocument). Bijlage 10 betreft het Concept Programma van Eisen. Dit is bijgesloten met als doel een beeld te schetsen van welke eisen er in de gunningsfase worden gesteld. Het akkoord dat door het indienen van een Aanmelding wordt gegeven (§3.10) ziet toe op de aanbestedingsprocedure en de uitgangspunten, niet op een definitief en onvoorwaardelijk akkoord met de afzonderlijke eisen van het concept-PvE. Het bindende akkoord op het Programma van Eisen wordt gegeven bij Inschrijving in de gunningsfase, waarna twee vragenrondes beschikbaar zijn voor nadere verduidelijking of aanpassing (zie planning §3.3).
10	Bijlage 10 Programma van Eisen, E 1.04	Op grond van de gangbare decentrale inkoopvoorwaarden (zoals o.a. GIBIT 2025) is ontbinding pas mogelijk dat leverancier ingebreke is gesteld en hij ondanks een redelijke termijn de tekortkoming niet heeft hersteld. Daarnaast gelden er bijvoorbeeld specifieke ontbindingsgronden in de acceptatieprocedure, als dan aantoonbaar blijkt dat de leverancier de oplossing niet afdoende kan implementeren conform de eisen van de aanbesteding. Kunt u bevestigen dat deze eis ziet op acceptatie van dergelijke bepalingen en niet als separate ontbindingsgrond naast de ontbindingsgronden in de overeenkomst en inkoopvoorwaarden kwalificeert?	E1.04 is een aanvullende grond voor ontbinding en/of schadevergoeding voor de specifieke situatie dat Inschrijver onjuiste of onvolledige informatie heeft verstrekt, dan wel niet kan nakomen wat bij Inschrijving is aangeboden. E1.04 zet de gangbare systematiek van verzuim, ingebrekestelling en hersteltermijn dus niet opzij, maar geldt in aanvulling op de overige ontbindingsgronden uit de overeenkomst en de toepasselijke inkoopvoorwaarden

11	Bijlage 10 Programma van Eisen, E 1.05	Ook voor deze eis geldt dat inschrijver hier pas volledig akkoord op kan geven nadat alle stukken en informatie in de gunningfase met haar is gedeeld. Hoe moet inschrijver hier in de selectiefase mee omgaan?	Zie 9
12	Bijlage 10 Programma van Eisen, E 1.06	Op grond van de gangbare decentrale inkoopvoorwaarden (zoals o.a. GIBIT 2025) is ontbinding pas mogelijk dat leverancier ingebreke is gesteld en hij ondanks een redelijke termijn de tekortkoming niet heeft hersteld. Daarnaast gelden er bijvoorbeeld specifieke ontbindingsgronden in de acceptatieprocedure, als dan aantoonbaar blijkt dat de leverancier de oplossing niet afdoende kan implementeren conform de eisen van de aanbesteding. Kunt u bevestigen dat deze eis ziet op acceptatie van dergelijke bepalingen en niet als separate ontbindingsgrond naast de ontbindingsgronden in de overeenkomst en inkoopvoorwaarden kwalificeert? Dit geldt overigens eveneens voor aansprakelijkheid wat te doen gebruikelijk een vast onderdeel is van de overeenkomst en/of de inkoopvoorwaarden.	E1.06 betreft geen ontbindingsgrond, maar de verplichting dat Opdrachtnemer na gunning en ondertekening van het Contract geen nieuwe Onderaannemers inzet zonder voorafgaande schriftelijke toestemming van Opdrachtgever. Voor de systematiek van ontbinding en ingebrekestelling waar de vraag op ziet: zie het antwoord op vraag 10.

13	Bijlage 10 Programma van Eisen, E 1.11	Deze eis geeft aan dat bij een wijziging van de juridische zeggenschap de deelname van de onderneming aan de raamovereenkomst automatisch vervalt. Dit is op grond van het Nederlands privaatrecht uitsluitend mogelijk door opzegging of ontbinding. Vaak voorzien de gangbare inkoopvoorwaarden ook in een mogelijkheid voor opzegging of ontbinding bij de wijziging van de zeggenschap. Veelal wordt daaraan toegevoegd dat opzegging niet mogelijk is als de de overnemende partij de overeenkomst onverkort kan nakomen. Onduidelijk is waarom u derhalve deze eis heeft opgenomen omdat dit veel verder gaat dan gebruikelijk is. Inschrijver stelt voor dat Aanbestedende Dienst in de overeenkomst die in gunningsfase wordt gepubliceerd een opzeggingsclausule opneemt die voor haar voldoende ruimte laat om de overeenkomst op te zeggen in het geval zij of een van de deelnemende partijen door een wijziging in de zeggenschap aantoonbare en wezenlijke risico's loopt. Is Aanbestedende Dienst bereid om de eis middels een dergelijke bepaling nader in te vullen?	Aanbesteder begrijpt uw punt en heeft daar ook begrip voor. Aanbesteder zal in het concept van de overeenkomst een recht tot beëindiging opnemen in dergelijke situaties en dus niet een verplichting. Op basis van de omstandigheden van het geval kan de aanbesteder alsdan een beslissing nemen en deze ook dergelijke, geobjectiveerd, onderbouwen
14	Bijlage 10 Programma van Eisen, E 1.13	Moet Inschrijver deze eis als zodanig interpreteren dat zij pas na totstandkoming van de nadere overeenkomst met een van de deelnemers een recht op betaling verkrijgt? Daarnaast moet inschrijver er redelijkerwijs vanuit kunnen gaan dat aantallen van accounts/werkplekken/servers/licenties etc die een deelnemer in de NVI's als informatie deelt, wel degelijk juist en volledig is. Immers, inschrijver moet hier de aanbieding op baseren? Hoe moet inschrijver hier in het licht van deze eis mee omgaan?	De Raamovereenkomst kent geen afname- of omzetgarantie; alle in de aanbestedingsstukken genoemde bedragen en aantallen zijn indicatief en Opdrachtnemer kan hieraan geen rechten ontlenen (PvE E1.13). Het recht op betaling ontstaat op basis van daadwerkelijk afgenomen dienstverlening onder de per Deelnemer gesloten Deelovereenkomst. De in de aanbestedingsstukken verstrekte aantallen zijn indicatief maar worden te goeder trouw verstrekt en mogen door Inschrijver als uitgangspunt worden gehanteerd.
15	Bijlage 10 Programma van Eisen, E 2.02	Kan Aanbestedende Dienst de geheimhoudingsverklaring delen? Dan kan inschrijver beoordelen of zij daarmee akkoord kan gaan.	De (model-)geheimhoudingsverklaring (vgl. PvE E2.02) maakt onderdeel uit van de uitvoeringsdocumenten en wordt in de gunningsfase ter beschikking gesteld, zodat Inschrijver deze voorafgaand aan Inschrijving kan beoordelen.

16	Bijlage 10 Programma van Eisen, E 2.03	Op grond van de gangbare decentrale inkoopvoorwaarden (zoals o.a. GIBIT 2025) is ontbinding pas mogelijk dat leverancier ingebreke is gesteld en hij ondanks een redelijke termijn de tekortkoming niet heeft hersteld. Daarnaast kunnen er bijvoorbeeld specifieke ontbindingsgronden voor specifieke gevallen overeengekomen worden. Kunt u bevestigen dat deze eis ziet op acceptatie van dergelijke bepalingen en niet als separate ontbindingsgrond naast de ontbindingsgronden in de overeenkomst en inkoopvoorwaarden kwalificeert?	Zie 10
17	Bijlage 10 Programma van Eisen, E 2.08	Inschrijver stelt voor dat u de huisregels na eventuele gunning tijdig ter beschikking stelt zodat eventueel personeel dat op locatie moet verschijnen van tevoren redelijkerwijs daarvan kennis heeft kunnen nemen. Is dit akkoord?	Akkoord. Voor zover medewerkers van Opdrachtnemer fysiek op locatie van een Deelnemer komen, worden de geldende huisregels na gunning tijdig ter beschikking gesteld, zodat het betrokken personeel hiervan vooraf kennis kan nemen.
18	Bijlage 10 Programma van Eisen, E 2.09	Inschrijver wijst er graag op dat de WAADI niet zonder meer van toepassing is op deze vorm van dienstverlening, omdat het doel niet is het uitlenen van personeel, maar het leveren van een managed dienst. Er zal in de regel ook geen tewerkstelling van personeel bij Aanbestedende Dienst plaatsvinden. Voor zover er al personeel op een locatie aanwezig zal zijn, zal dit louter voor specifieke werkzaamheden en enkel op projectbasis zijn. De WAADI is enkel van toepassing als personeel onder leiding en toeizcht van de aanbestedende dienst werkzaamheden zal gaan verrichten. Dat zal bij deze vorm van dienstverlening echter niet het geval zijn, omdat de leverancier nu juist de deskundige partij is. Kortom: het risico waarop deze eis zit bestaat in feite niet. Bent u bereid om deze eis buiten toepassing te verklaren?	De eis legt vast dat ingezette werknemers gerechtigd zijn arbeid te verrichten in Nederland conform de WAADI en vrijwaart de Deelnemer voor boetes en sancties. De eis kwalificeert de WAADI niet als zonder meer van toepassing op de gehele managed dienstverlening; voor zover de WAADI feitelijk niet van toepassing is op deze dienstverlening heeft de eis voor Opdrachtnemer geen verzwarend effect. Deze eis is uitsluitend van toepassing indien en voor zover de WAADI daadwerkelijk van toepassing is. De eis wordt gehandhaafd.

19	Bijlage 10 Programma van Eisen, E 3.03	Eis E3.03 beschrijft de verschillende serviceniveaus van de SOC-dienstverlening, waarbij sprake is van klantgerichte dienstverlening richting de Deelnemers. Inschrijver verzoekt de Aanbestedende Dienst te verduidelijken in hoeverre er eisen worden gesteld aan de geografische locatie van het SOC en het daarin werkzame personeel. Inschrijver gaat ervan uit dat centralisatie van de SOC-dienstverlening, waarbij het SOC en de hierin werkzame medewerkers volledig vanuit Nederland opereren, voldoet aan de gestelde eisen en kan bijdragen aan kwaliteit, beheersbaarheid en governance van de dienstverlening. Kan de Aanbestedende Dienst bevestigen dat een dergelijke inrichting is toegestaan?	Ja, dat is toegestaan. Het PvE vereist dat het SOC, de gebruikte software en de datacenters binnen de EER gevestigd zijn (E8.01) en dat alle Deelnemer-data binnen de EER wordt verwerkt en opgeslagen, waarbij het SOC-team vanuit een vestiging binnen de EER werkt (E8.02). Een SOC dat met zijn medewerkers volledig vanuit Nederland opereert, valt binnen de EER en voldoet daarmee aan de locatie-eisen. Daarnaast gelden onder meer de eisen voor Nederlandstalige klant-facing communicatie (E2.12) en een actuele VOG (E8.22).
20	Bijlage 10 Programma van Eisen, E 4.01 t/m E 4.10	Kan de Aanbestedende Dienst verduidelijken: - of onboarding gefaseerd plaatsvindt per deelnemer; - en in hoeverre hierbij sprake is van prioritering of afhankelijkheden tussen deelnemers?	Ja, onboarding vindt gefaseerd per Deelnemer plaats; elke Deelnemer treedt op een eigen instapmoment toe via een Nadere Overeenkomst. De fasering volgt de indicatief gegeven planning van instapmomenten. Er zijn geen onderlinge afhankelijkheden tussen Deelnemers; Opdrachtnemer onboardt Deelnemers zelfstandig en zo nodig gelijktijdig.
21	Bijlage 10 Programma van Eisen, E 4.04	Eis E4.04 beschrijft de verplichtingen rondom de exit van de dienstverlening, waaronder de overdracht van data, documentatie en ondersteuning bij de overgang naar een andere opdrachtnemer. Inschrijver maakt uit deze eis op dat zij mogelijk bij exit ook het MDR-platform moet overdragen. Kan Aanbestedende Dienst bevestigen dat dit niet het geval is? De IE-rechten tbv de dienstverlening, op de detectierules en standaard usecases blijven immers toebehoren aan Inschrijver en zullen bij een exit niet worden overgedragen	Bevestigd. Bij exit worden de Deelnemer-specifieke data, configuraties en maatwerk-use-cases overgedragen. Het MDR-platform en de IE-rechten van Opdrachtnemer, waaronder generieke detectieregels, standaard use cases, playbooks, methodieken, tooling en knowhow, vallen buiten de overdracht. E4.04 verplicht tot medewerking aan een soepele overgang, niet tot overdracht van het platform of de generieke IE.

22	Bijlage 10 Programma van Eisen, E 8.05	Inschrijver begrijpt de betreffende eis en de achterliggende wens tot flexibiliteit voor de Aanbestedende Dienst. Tegelijkertijd geldt dat na totstandkoming van een Nadere Overeenkomst partijen in beginsel voor de overeengekomen looptijd gebonden zijn en dat opdrachtnemer investeringen doet en omzet afhankelijk is van deze looptijd. Inschrijver verzoekt de Aanbestedende Dienst te verduidelijken op welke wijze in de contractuele uitwerking rekening wordt gehouden met een evenwichtige verdeling van risico's bij tussentijdse beëindiging van de overeenkomst om andere redenen dan toerekenbaar tekortschieten aan de zijde van opdrachtnemer. Kan de Aanbestedende Dienst bevestigen dat in dergelijke gevallen voorzien wordt in een passende compensatieregeling dan wel dat hierover nadere bepalingen worden opgenomen in de gunningsfase?	De contractuele uitwerking van tussentijdse beëindiging, opzegging en een eventuele compensatieregeling wordt in de overeenkomst in de gunningsfase opgenomen, met inachtneming van een evenwichtige risicoverdeling. .
23	Bijlage 10 Programma van Eisen, E 8.13	Eis E8.13 betreft de medewerking aan verzoeken van betrokkenen in het kader van de AVG. Inschrijver gaat ervan uit dat de verantwoordelijkheid voor de afhandeling van verzoeken van betrokkenen primair bij de verwerkingsverantwoordelijke ligt en dat opdrachtnemer in de rol van verwerker een passende en redelijke mate van ondersteuning verleent, conform gebruikelijke verhoudingen onder de AVG en zoals nader vast te leggen in een verwerkersovereenkomst. Kan de Aanbestedende Dienst bevestigen dat deze rolverdeling wordt gehanteerd en dat de nadere uitwerking hiervan plaatsvindt in de verwerkersovereenkomst?	Bevestigd. De Deelnemer is verwerkingsverantwoordelijke; Opdrachtnemer treedt op als verwerker. Opdrachtnemer verleent een passende en redelijke mate van ondersteuning bij verzoeken van betrokkenen. De nadere uitwerking van deze rolverdeling vindt plaats in de verwerkersovereenkomst, die in de gunningsfase aan de orde komt.

24	Bijlage 10 Programma van Eisen, E 8.17	Aanbestedende Dienst vereist kostenloze medewerking aan een IAMA. Inschrijver kan niet goed plaatsen op grond waarvan een IAMA vereist zou zijn. Toepasselijke wet- en regelgeving lijkt dit niet te vereisen en daarmee is deze eis in beginsel disproportioneel nu dit verder gaat dan nodig is. Inschrijver is wel bereid om hieraan haar redelijke medewerking te verlenen tegen betaling van de kosten die inschrijver hiervoor maakt, nu het een maatregel betreft die verder gaat dan redelijkerwijs nodig is op basis van toepasselijke wet- en regelgeving. Is dit akkoord voor Aanbestedende Dienst?	De eis vraagt om medewerking in redelijke en gangbare mate, kosteloos, aan de IAMA die de Deelnemer uitvoert ten aanzien van de detectie-algoritmes en ML-componenten. Gelet op de inzet van AI/ML en de publieke context acht de Aanbestedende Dienst deze medewerkingsplicht proportioneel; de eis wordt gehandhaafd. De medewerking betreft het in redelijke mate leveren van informatie, niet het zelfstandig uitvoeren van de IAMA.
25	Bijlage 10 Programma van Eisen, E 8.18	Inschrijver verwerkt natuurlijk niet meer persoonsgegevens dan relevant is voor de uitvoering van de diensten. Tegelijkertijd kan de omgeving van een deelnemer zodanig zijn ingericht dat Inschrijver bijvoorbeeld wel toegang krijgt tot informatie over de MS-accounts van medewerkers van de klant omdat er toegang is verschaft tot de tenant van de deelnemer. Vanuit technisch oogpunt is het vooralsnog niet mogelijk om dit helemaal te beperken. Derhalve vraagt inschrijver Aanbestedende Dienst te bevestigen dat hiermee desondanks wordt voldaan aan deze eis.	E8.18 ziet op de feitelijke inzage en verwerking, niet op het volledig technisch uitsluiten van toegang. Dat Opdrachtnemer door tenant-toegang technisch meer zou kunnen inzien, vormt op zichzelf geen strijd met de eis. Aan E8.18 wordt voldaan zolang Opdrachtnemer feitelijk niet meer persoonsgegevens inziet of verwerkt dan noodzakelijk en de bijbehorende waarborgen naleeft: doelbinding op rolniveau (E8.28), gescheiden en beperkte toegang (E8.07) en logging van alle toegang en raadpleging (E8.30).
26	Bijlage 10 Programma van Eisen, E 8.28 en E 8.29	Eisen E8.28 en E8.29 zien op het beperken en borgen van toegang tot persoonsgegevens op basis van rollen en taken. Kan de Aanbestedende Dienst verduidelijken of deze bepalingen uitsluitend betrekking hebben op toegang door medewerkers van opdrachtnemer (inclusief diens eigen personeel), of tevens op toegang door eventuele subverwerkers en andere ingeschakelde derde partijen?	De bepalingen inzake doelbinding en beperkte toegang (PvE E8.07, E8.09, E8.28) gelden voor eenieder die in het kader van de dienstverlening toegang heeft tot of gegevens verwerkt van een Deelnemer: zowel medewerkers van Opdrachtnemer als ingeschakelde subverwerkers en andere door Opdrachtnemer gecontracteerde derde partijen, conform de in de eisen opgenomen zinsnede 'inclusief alle door Opdrachtnemer gecontracteerde derde partijen'.
27	Bijlage 10 Programma van Eisen, E 8.35	Aangezien Inschrijver zelf pentesters in dienst heeft en Inschrijver geen toegang wenst te verlenen tot haar systemen en netwerken is het voorstel van Inschrijver dat zij jaarlijks een eigen pentest kan doen. Deze verplichting is Inschrijver ook reeds met andere klanten overeengekomen. Daarnaast wijst Inschrijver erop dat eigen pentesten conform de standaard NIST SP800 115 uitvoert waarmee de onafhankelijkheid ook wordt gegarandeerd.	E8.35 vereist dat de jaarlijkse penetratietest wordt uitgevoerd door een externe, onafhankelijke partij. Eigen pentesters die bij Opdrachtnemer in dienst zijn voldoen daar niet aan; de eis ziet op organisatorische onafhankelijkheid, niet alleen op de methode, en NIST SP 800-115 doet daar niet aan af. Het staat Opdrachtnemer vrij daarnaast eigen pentesten uit te voeren, maar de in E8.35 bedoelde assurance-test blijft extern en onafhankelijk. De eis blijft ongewijzigd.

28	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 3 en VW 7	Beide veiligheidsregio's vereisen specifiek ISO 22301 tav business continuity. Voor inschrijver is onduidelijk waarom dit specifiek door deze partijen wordt vereist. Dit is namelijk geen gangbare eis bij aanbesteding van MDR-dienstverlening. Daarbij beperkt dit de marktwerking op significante wijze omdat maar een beperkt aantal partijen op deze norm zijn gecertificeerd. Tot slot kent ISO 22301 ook behoorlijke overlap met ISO 27001 in bv combinatie met ISAE 3402 type 2. Kan aanbestedende dienst derhalve deze specifieke certificering buiten toepassing laten?	De in Bijlage 11 opgenomen voorwaarden zijn aanvullende, deelnemer-specifieke voorwaarden. De betreffende deelnemers met voorwaarden kunnen zich hierop beroepen, maar zijn daartoe niet verplicht. ISO 22301 (VW3 en VW7) betreft zo'n aanvullende voorwaarde; deze geldt niet generiek voor de opdracht en wordt door de Aanbestedende Dienst niet centraal buiten toepassing verklaard. Of de voorwaarde daadwerkelijk van toepassing is, blijkt bij de betreffende Nadere Overeenkomst.
29	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 6	In Bijlage 11 (voorwaarde Veiligheidsregio Gooi en Vechtstreek / Flevoland) wordt voor de gezamenlijke scope – bestaande uit managed EDR, NDR en (eventuele) aanvullende SIEM-logbronnen – een maximumbudget van € 83.000 (incl. btw) per jaar gehanteerd, waarbij wordt uitgegaan van één gecombineerde te monitoren omgeving. Om de haalbaarheid en proportionaliteit van deze randvoorwaarde adequaat te kunnen beoordelen en een passende prijsopbouw te kunnen aanbieden, verzoekt inschrijver de Aanbestedende Dienst om nadere inzicht te geven in de omvang en inhoud van deze gezamenlijke scope, in het bijzonder: 1. Het aantal te monitoren gebruikers, endpoints en/of IP-adressen binnen de gecombineerde omgeving; 2. De verwachte (indicatieve) omvang en typen logbronnen die aangesloten dienen te worden (bijv. endpoints, netwerkcomponenten, cloud-omgevingen, security tooling); 3. Eventuele bandbreedtes of groeiverwachtingen gedurende de looptijd.	VW6 is een aanvullende, deelnemer-specifieke voorwaarde van de betreffende regio's. In Bijlage 11 is bij deze voorwaarde al globaal omschreven wat bij de regio's onder de scope valt. Nadere detaillering van scope, omvang en budgetafbakening komt aan de orde bij de betreffende Nadere Overeenkomst. De deelnemers met voorwaarden kunnen zich op de voorwaarde beroepen, maar zijn daartoe niet verplicht.

30	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 6	In Bijlage 11 bij voorwaarde 6, geven de gecombineerde Veiligheidsregio's Gooi en Vechtstreek en Flevoland als voorwaarde aan dat voor de gezamenlijke scope – bestaande uit managed EDR, NDR en aanvullende SIEM-logbronnen – een maximumbedrag van € 83.000 (incl. btw) per jaar wordt gehanteerd. Kan de Aanbestedende Dienst aangeven of deze gecombineerde organisatie momenteel reeds gebruikmaakt van een MDR-/SOC-dienstverlening waarin deze domeinen (EDR, NDR en/of SIEM) reeds zijn ingericht en worden afgedekt?	Zie het antwoord op vraag 29.
31	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 15	In Bijlage 11 bij voorwaarde 15, geeft Veiligheidsregio Zaanstreek-Waterland als voorwaarde aan dat voor de scope – bestaande uit managed EDR, NDR en aanvullende SIEM-logbronnen – een maximumbedrag van € 83.000 (excl. btw) per jaar wordt gehanteerd. Om de haalbaarheid van deze randvoorwaarde en de daarbij behorende prijsopbouw adequaat te kunnen beoordelen, verzoekt inschrijver de Aanbestedende Dienst om nadere inzicht te geven in de omvang en inhoud van deze scope, in het bijzonder: 1. Het aantal te monitoren gebruikers, endpoints en/of IP-adressen binnen de organisatie; 2. De verwachte (indicatieve) set en omvang van de aan te sluiten logbronnen (bijvoorbeeld endpoints, netwerkcomponenten, cloud-omgevingen en security tooling).	VW15 is een aanvullende, deelnemer-specifieke voorwaarde van de betreffende regio. In Bijlage 11 is bij deze voorwaarde al globaal omschreven wat bij de regio onder de scope valt. Nadere detaillering van scope, omvang en budgetafbakening komt aan de orde bij de betreffende Nadere Overeenkomst. De deelnemers met voorwaarden kunnen zich op de voorwaarde beroepen, maar zijn daartoe niet verplicht.
32	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 15	In Bijlage 11 bij voorwaarde 15, geeft Veiligheidsregio Zaanstreek-Waterland als voorwaarde aan dat voor de scope – bestaande uit managed EDR, NDR en aanvullende SIEM-logbronnen – een maximumbedrag van € 83.000 (excl. btw) per jaar wordt gehanteerd. Kan de Aanbestedende Dienst aangeven of Veiligheidsregio Zaanstreek-Waterland momenteel reeds gebruikmaakt van een MDR-/SOC-dienstverlening waarin deze domeinen (EDR, NDR en/of SIEM) (gedeeltelijk) zijn ingericht en worden afgedekt?	Zie het antwoord op vraag 31.

33	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 18	In Bijlage 11 bij voorwaarde 18, geeft Veiligheidsregio Fryslân als voorwaarde aan dat voor de scope – bestaande uit managed EDR, NDR en aanvullende SIEM-logbronnen – een maximumbedrag van € 96.000 (excl. btw) per jaar wordt gehanteerd. Om de haalbaarheid van deze randvoorwaarde en de daarbij behorende prijsopbouw adequaat te kunnen beoordelen, verzoekt inschrijver de Aanbestedende Dienst om nadere inzicht te geven in de omvang en inhoud van deze scope, in het bijzonder: 1. Het aantal te monitoren gebruikers, endpoints en/of IP-adressen binnen de organisatie; 2. De verwachte (indicatieve) set en omvang van de aan te sluiten logbronnen (bijvoorbeeld endpoints, netwerkcomponenten, cloudomgevingen en security tooling).	VW18 is een aanvullende, deelnemer-specifieke voorwaarde van de betreffende regio. In Bijlage 11 is bij deze voorwaarde al globaal omschreven wat bij de regio onder de scope valt. Nadere detaillering van scope, omvang en budgetafbakening komt aan de orde bij de betreffende Nadere Overeenkomst. De deelnemers met voorwaarden kunnen zich op de voorwaarde beroepen, maar zijn daartoe niet verplicht.
34	Bijlage 11 voorwaarden deelnemers met voorwaarden, VW 18	In Bijlage 11 bij voorwaarde 18, geeft Veiligheidsregio Fryslân als voorwaarde aan dat voor de scope – bestaande uit managed EDR, NDR en aanvullende SIEM-logbronnen – een maximumbedrag van € 96.000 (excl. btw) per jaar wordt gehanteerd. Kan de Aanbestedende Dienst aangeven of Veiligheidsregio Fryslân momenteel reeds gebruikmaakt van een MDR-/SOC-dienstverlening waarin deze domeinen (EDR, NDR en/of SIEM) (al dan niet gedeeltelijk) zijn ingericht en worden afgedekt?	Zie het antwoord op vraag 33.

35	Bijlage 10 Programma van Eisen, E 5.06	Eis E5.06 bepaalt dat preventief onderhoud uitsluitend wordt uitgevoerd binnen vooraf met de [Deelnemer] overeengekomen onderhoudsvensters, zoals vastgelegd in het DAP (zie E3.04). Inschrijver constateert dat bij individuele afstemming per deelnemer dit in de praktijk kan leiden tot een groot aantal verschillende onderhoudsvensters. In het kader van een efficiënte en beheersbare uitvoering van de dienstverlening stelt inschrijver voor om te werken met één uniform onderhoudsvenster voor alle deelnemende veiligheidsregio's, dan wel met een beperkt aantal (bijvoorbeeld 2 à 3) standaard onderhoudsvensters. Kan de Aanbestedende Dienst bevestigen of een dergelijke gestandaardiseerde inrichting van onderhoudsvensters is toegestaan?	Opdrachtnemer mag een uniform of een beperkt aantal standaard onderhoudsvensters voorstellen. E5.06 vereist dat het toe te passen venster per Deelnemer wordt overeengekomen en in het DAP wordt vastgelegd (E5.06 in samenhang met E3.04). De verwachting is dat de Deelnemers hierin zoveel mogelijk samen optrekken, zodat een gestandaardiseerde opzet goed mogelijk is; een Deelnemer behoudt het recht een afwijkend venster overeen te komen.
36	Selectiedocument SOC-MDR Versie 1.0, 3.1 Europese niet-openbare aanbestedingsprocedure	De Aanbestedende Dienst heeft voorafgaand aan de keuze voor de Europese niet-openbare procedure een marktconsultatie uitgevoerd. Inschrijver verzoekt de Aanbestedende Dienst om de verslaglegging, bevindingen en/of notulen van deze marktconsultatie ter beschikking te stellen aan de Inschrijvers.	De Aanbestedende Dienst stelt geen separaat marktconsultatieverslag ter beschikking. De relevante uitkomsten zijn verwerkt in de keuzes en onderbouwingen in de aanbestedingsstukken. De Aanbestedende Dienst is niet gehouden interne (aanbestedings)documenten bekend te maken (§3.15 Selectiedocument).
37	E2.04 & E8.22 (Screening & VOG)	Kan Opdrachtgever bevestigen dat een VOG of equivalente screening voor SOC-personeel voldoende is en dat er geen aanvullende AIVD- of veiligheidsonderzoeken per medewerker worden vereist?	Een VOG ziet uitsluitend op antecedenten en vormt op zichzelf geen volledige screening. Gezien de aard van de werkzaamheden voor de veiligheidsregio's wordt naast de VOG een aanvullende screening wenselijk geacht. De Aanbestedende Dienst werkt de vorm hiervan nader uit en verankert dit in de aanbestedingsstukken.

38	E7.05 & E7.09 (Use cases & IP)	Kan Opdrachtgever bevestigen dat alle standaard use cases, detectieregels en threat intelligence van Opdrachtnemer intellectueel eigendom blijven van Opdrachtnemer en dat Opdrachtgever hierop geen licentie of overdrachtsrechten verkrijgt?	Bevestigd. De exitverplichtingen (PvE E4.02, E4.04) zien op overdracht van Deelnemer-specifieke gegevens, documentatie en use cases, niet op overdracht van het MDR-platform zelf. Intellectuele eigendomsrechten op de generieke dienstverlening, standaard detectieregels en standaard use cases blijven bij Opdrachtnemer en worden bij exit niet overgedragen. De afbakening wordt vastgelegd in het Exit-plan.
39	E5.20 & E5.24 (SOAR & host isolation)	Kan Opdrachtgever bevestigen dat geautomatiseerde respons-acties (SOAR, host isolation) uitsluitend plaatsvinden binnen vooraf expliciet goedgekeurde playbooks en dat Opdrachtnemer niet aansprakelijk is voor schade als gevolg van door Opdrachtgever goedgekeurde geautomatiseerde acties?	Bevestigd voor het eerste deel: host isolation en netwerksegmentatie worden uitsluitend uitgevoerd na expliciete toestemming van de Deelnemer per incident, of binnen vooraf in playbooks vastgelegde scenario's (E5.24); geautomatiseerde respons blijft binnen de in het DAP afgesproken kaders (E7.20). Voor het tweede deel geeft de Aanbestedende Dienst geen blanco vrijwaring: dat acties binnen door de Deelnemer goedgekeurde playbooks plaatsvinden is relevant, maar de aansprakelijkheidsverdeling volgt uit de overeenkomst.
40	E4.04 & E4.07 (Exit & data-overdracht)	Kan Opdrachtgever bevestigen dat bij exit alleen de Opdrachtgever-specifieke data, configuraties en maatwerk-use-cases worden overgedragen en dat generieke detectieregels, playbooks, methodieken, knowhow en tooling van Opdrachtnemer buiten de overdracht vallen?	Zie het antwoord op vraag 21.
41	E7.05 / E4.04 – Use-cases	In het Programma van Eisen (E7.05 en E4.04) wordt bepaald dat use-cases overdraagbaar moeten zijn bij exit. Kan Opdrachtgever bevestigen dat dit uitsluitend geldt voor specifiek overeengekomen maatwerk-use-cases en dat standaarddienstverlening, generieke templates, methodieken en knowhow van Opdrachtnemer hier niet onder vallen?	Zie het antwoord op vraag 21.

42	E8.37 – ISO27001	In het Programma van Eisen (Eis E8.37) wordt vereist dat Opdrachtnemer gecertificeerd is conform ISO27001 met SOC-dienstverlening binnen scope. Kan Opdrachtgever bevestigen dat een geldige SOC 2 Type II-rapportage met een Verklaring van Toepasselijkheid (SoA) die de SOC/MDR-dienstverlening expliciet omvat, als gelijkwaardig bewijs wordt geaccepteerd?	Geschiktheidseis 7 staat naast het ISO/IEC 27001-certificaat uitdrukkelijk een gelijkwaardig certificaat of onafhankelijk beoordelingsrapport toe, mits ten minste dezelfde waarborgen worden geboden en de scope de uitgevraagde SOC/MDR-dienstverlening dekt. Een geldige SOC 2 Type II-rapportage met een Verklaring van Toepasselijkheid (SoA) die de dienstverlening expliciet omvat, kan als gelijkwaardig bewijs worden aanvaard, mits onderbouwd met een verklaring en bewijs van gelijkwaardigheid. De Aanbestedende Dienst behoudt zich het recht voor de reikwijdte en gelijkwaardigheid te beoordelen.
43	Paragraaf 6.6 (Geschiktheidseis 7) – informatiebeveiliging	In Geschiktheidseis 7 van het Selectiedocument en Eis E8.37 van het PvE wordt ISO27001 als eis gesteld. Kan Opdrachtgever, mede gelet op het proportionaliteits- en gelijkwaardigheidsbeginsel, bevestigen dat een geldige SOC 2 Type II-rapportage (die een zwaardere en diepgaandere toets op de werking van beheersmaatregelen over een referentieperiode betreft) als gelijkwaardig bewijs van aantoonbaar ingerichte en werkende informatiebeveiligingsmaatregelen wordt geaccepteerd? Zo nee, kunt u gemotiveerd toelichten waarom een zwaardere assurance niet als gelijkwaardig kan gelden?	Zie 42
44	Paragraaf 6.4 – Kerncompetentie 1 (Geschiktheidseis 4)	In paragraaf 6.4 van het Selectiedocument (Kerncompetentie 1) wordt als minimale ervaringseis 500 endpoints genoemd. Kan Opdrachtgever bevestigen dat dit het minimale aantal endpoints betreft dat in de referentieopdracht aanwezig moet zijn geweest en dat dit aantal endpoints als indicatie kan worden beschouwd van het aantal endpoints binnen de scope van Opdrachtgever?	De 500 endpoints betreffen het minimale aantal in de referentieopdracht om Kerncompetentie 1 aan te tonen. Dit is een drempelwaarde voor de referentie-eis en vormt geen indicatie van de omvang van de onderhavige opdracht.

45	Paragraaf 7.1 – Selectiecriteria	In het Selectiedocument wordt niet expliciet vermeld of de aanmelding of latere inschrijving in eigen format mag worden ingediend. Kan Opdrachtgever bevestigen dat inschrijvers de Aanmelding en eventuele bijlagen in eigen format mogen indienen, mits de gevraagde inhoud en structuur worden gerespecteerd?	Bevestigd, met inachtneming van het volgende. De bij de Aanmelding verplichte bijlagen (UEA, referentieformulier Bijlage 6, overige verklaringen uit de Checklist Aanmelding Bijlage 1) dienen in de voorgeschreven vorm te worden ingediend; vaste teksten mogen niet worden gewijzigd of aangevuld (§3.8). De visiedocumenten bij de selectiecriteria (SC1-3) mogen in een eigen format worden aangeleverd, mits binnen de paginalimiet van maximaal 2 A4 per criterium en met inachtneming van de gevraagde onderdelen (§7.2-7.4). Aanvullende bijlagen buiten de paginalimiet worden niet beoordeeld.
46	Geschiktheidseis 8 (Gegevensverwerking) - paragraaf 6.7 Selectiedocument	Geschiktheidseis 8 vereist dat alle verwerkte gegevens uitsluitend worden verwerkt en opgeslagen binnen de EU of EER, inclusief de infrastructuur van subverwerkers. Kan de Aanbestedende Dienst bevestigen dat een inschrijver aan deze eis voldoet wanneer alle [Deelnemer]-data uitsluitend in EU/EER-datacenters wordt verwerkt, doorgifte naar derde landen contractueel is uitgesloten via een verwerkersovereenkomst conform artikel 46 AVG met EU-standaardcontractbepalingen, en de inschrijver als NL-gevestigde verwerkingsverantwoordelijke de volledige juridische en operationele verantwoordelijkheid draagt - ook indien de ingezette technologieleverancier als rechtspersoon buiten de EU is gevestigd?	Geschiktheidseis 8 stelt een absoluut vereiste: alle verwerking en opslag van gegevens (logdata, detectiegegevens, incidentinformatie) vindt uitsluitend binnen de EU/EER plaats; doorgifte naar derde landen is niet toegestaan, inclusief de infrastructuur van subverwerkers (PvE E8.01/E8.02). Dit is bewust strenger dan de AVG-minimumnorm; doorgifte op basis van SCC's volstaat derhalve niet. De vestigingsplaats van een technologieleverancier buiten de EU staat hieraan op zichzelf niet in de weg, mits de feitelijke verwerking en opslag volledig binnen de EU/EER plaatsvinden (bijv. via EU Data Boundary-configuratie) en geen doorgifte naar of toegang vanuit een derde land plaatsvindt.
47	Paragraaf 2.2 / Selectiecriterium 1 / PvE E1.14	Paragraaf 2.2 beschrijft sterk uiteenlopende Microsoft-licentieniveaus bij de deelnemers. PvE E1.14 vereist een transparante staffelstructuur met voorbeeldcalculaties. Dient de inschrijver in zijn staffelstructuur en/of visie (Selectiecriterium 1) inzichtelijk te maken welke aanvullende kosten per Microsoft-licentietier zijn verbonden aan de dienstverlening - inclusief eventuele licentie-upgrades of aanvullende ingestiekosten - zodat de Aanbestedende Dienst	De selectiefase kent geen prijscomponent. Selectiecriterium 1 beoordeelt de organisatiebrede visie op het MDR-vakgebied, waaronder de visie op licentiediversiteit en de verhouding tussen bestaande functionaliteit en aanvullende tooling. De transparante staffel- en TCO-uitwerking wordt in de gunningsfase gevraagd via het Prijzenblad (PvE E1.14).

		een vergelijkbaar Total Cost of Ownership-overzicht kan opstellen?	
48	Paragraaf 2.1 (Globale aansluitingsplanning deelnemers)	De aansluitingsplanning toont dat naar verwachting acht vaste deelnemers in H1 2027 aansluiten. Kan de Aanbestedende Dienst een indicatie geven van het totale aantal endpoints dat deze acht deelnemers gezamenlijk inbrengen bij aanvang van de dienstverlening, zodat inschrijvers de technische en commerciele haalbaarheid in de opstartfase kunnen beoordelen en hun staffelstructuur met voorbeeldcalculaties hierop kunnen afstemmen?	Deze aanbesteding bevindt zich in de selectiefase; indicatieve omvang-informatie zoals het totale aantal endpoints van de aansluitende deelnemers wordt in deze fase niet verstrekt. In de gunningsfase ontvangen de geselecteerde inschrijvers de benodigde indicatieve aantallen, zodat zij hun prijs- en staffelstructuur daarop kunnen afstemmen.
49	Selectiecriterium 2 (Visie op CTI)	Ten aanzien van Selectiecriterium 2 (Visie op CTI): Waardeert de Aanbestedende Dienst inschrijvingen waarbij Threat Intelligence Management (TIM) native, geautomatiseerd en integraal onderdeel uitmaakt van de architectuur van het MDR-platform, hoger in de beoordeling dan oplossingen waarbij dit proces afhankelijk is van losse/externe platformen of handmatige handelingen?	Selectiecriterium 2 wordt beoordeeld op de visie op de rol van CTI binnen MDR-dienstverlening (§7.3), niet op een specifieke technische architectuurkeuze. Of TIM native, geautomatiseerd en integraal is ingericht kan onderdeel zijn van de onderbouwing, maar leidt niet op voorhand tot een hogere waardering. De beoordeling verloopt via de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%). Bepalend is de mate waarin het antwoord inhoudelijk relevant, concreet, toepasselijk, onderscheidend en innoverend is. Er wordt geen voorkeur toegekend aan een specifieke architectuur of oplossing. Beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet in de beoordeling betrokken.

50	Geschiktheidseis 5 en 9	In geschiktheidseis 5 en 9 wordt vereist dat het SOC-team aantoonbaar gescreend moet zijn en dat er geen relatie mag zijn met offensieve statelijke actoren. Kan de Aanbestedende Dienst bevestigen dat dit betekent dat het volledige operationele SOC-team (inclusief eventuele 'follow-the-sun' Tier 1/Tier 2 analisten in de nachtelijke uren) via deze specifieke Nederlandse normen (AIVD/NCTV) gescreend moet kunnen worden, en dat offshore SOC-locaties buiten de EU hiermee nagenoeg zijn uitgesloten?	Geschiktheidseis 5 vereist dat de integriteit van alle SOC-analisten die aan de Opdracht werken — inclusief eventuele follow-the-sun Tier 1/Tier 2-analisten in de nachtelijke uren — via een erkende screening is vastgesteld. Een VOG ziet uitsluitend op antecedenten en vormt op zichzelf geen volledige screening. Gezien de aard van de werkzaamheden voor de veiligheidsregio's wordt naast de VOG een aanvullende screening wenselijk geacht. De Aanbestedende Dienst werkt de vorm hiervan nader uit en verankert dit in de aanbestedingsstukken; een specifiek AIVD-veiligheidsonderzoek wordt daarbij niet op voorhand uitgesloten. Geschiktheidseis 9 / PvE E2.01 stelt aanvullend dat geen relatie of inmenging mag bestaan met door AIVD/NCTV als offensief geclassificeerde statelijke actoren. Het SOC-team werkt binnen de EER (PvE E8.02); SOC-locaties buiten de EER zijn niet toegestaan.
51	Paragraaf 4.4 (Onderaanneming) / Geschiktheidseis 9	Paragraaf 4.4 maakt onderscheid tussen onderaannemers ter voldoening aan geschiktheidseisen en onderaannemers voor feitelijke uitvoering. Geschiktheidseis 9 vereist screening op statelijke actoren. Kan de Aanbestedende Dienst bevestigen dat een leverancier van een standaard SaaS-beveiligingsplatform niet wordt aangemerkt als onderaannemer in de zin van paragraaf 4.4, en dat voor deze leverancier geen UEA, Verklaring Onderaanneming of screening conform Geschiktheidseis 9 is vereist, mits de inschrijver als hoofdaannemer de volledige operationele en contractuele verantwoordelijkheid voor de dienstverlening draagt?	Een leverancier van een standaard SaaS-/technologieplatform die geen deel van de Opdracht in onderaanneming uitvoert, wordt in beginsel niet aangemerkt als onderaannemer in de zin van §4.4. Opgave-, UEA- en Verklaring Onderaanneming-verplichtingen gelden dan niet, mits Inschrijver als hoofdaannemer de volledige operationele en contractuele verantwoordelijkheid draagt. Onverlet blijven Geschiktheidseis 8 (EU/EER, inclusief subverwerkers) en Geschiktheidseis 9 / PvE A1.18 (geen inmenging statelijke actoren), ook voor derde partijen die door Opdrachtnemer zijn gecontracteerd.

52	Selectiecriterium 3 (Research & Development en innovatie) - paragraaf 7.4 Selectiedocument	Selectiecriterium 3 vraagt naar R&D, innovatie en bijdragen aan platformgebonden ecosystemen vanuit de eigen organisatie. Mag de inschrijver bij Selectiecriterium 3 de AI-ontwikkelingen en R&D-investeringen van zijn strategische technologiepartner meewegen, mits aantoonbaar wordt beschreven hoe deze innovaties door de inschrijver zelf worden vertaald naar sectorspecifieke detectielogica voor de Nederlandse normenkaders BIO, Cyberbeveiligingswet/NIS2 en NEN7510?	Selectiecriterium 3 vraagt hoe R&D en innovatie structureel in de eigen organisatie zijn verankerd. R&D-ontwikkelingen van een strategische technologiepartner mogen worden betrokken, mits Inschrijver aantoonbaar beschrijft hoe deze door de eigen organisatie worden geabsorbeerd, vertaald naar eigen R&D en sectorspecifieke detectielogica, en teruggebracht naar de eigen dienstverlening. Een loutere verwijzing naar R&D van derden telt niet zelfstandig mee. De beoordeling verloopt via de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%). Bepalend is de mate waarin het antwoord inhoudelijk relevant, concreet, toepasselijk, onderscheidend en innoverend is. Er wordt geen voorkeur toegekend aan een specifieke architectuur of oplossing. Beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet in de beoordeling betrokken.
53	Selectiecriterium 1 (Visie op het MDR-vakgebied) / Paragraaf 2.2	Paragraaf 2.2 benoemt M-EDR als verplichte baseline en SIEM en NDR als optionele uitbreidingen. De markt kent zowel geintegreerde platformen als modulaire point-solution architecturen. Waardeert de Aanbestedende Dienst bij Selectiecriterium 1 een architectuur waarbij M-EDR, SIEM en NDR native zijn geintegreerd in een uniform platform aantoonbaar positiever dan een modulaire aanpak waarbij deze componenten als afzonderlijke oplossingen worden aangeboden en geintegreerd?	Selectiecriterium 1 wordt beoordeeld op de organisatiebrede visie (§7.2), niet op de keuze voor een geïntegreerde dan wel modulaire architectuur. De beoordeling verloopt via de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%). Bepalend is de mate waarin het antwoord inhoudelijk relevant, concreet, toepasselijk, onderscheidend en innoverend is. Er wordt geen voorkeur toegekend aan een specifieke architectuur of oplossing. Beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet in de beoordeling betrokken.

54	PvE E6.04 (Opslagmodellen logdata)	PvE E6.04 definieert Model A als opslag 'binnen de tenant of infrastructuur van [Deelnemer]' en noemt Microsoft Sentinel in de deelnemer-tenant als voorbeeld. Kwalificeert een architectuur waarbij iedere deelnemer een contractueel aan hem toegewezen, logisch gesoleerde cloudomgeving krijgt in een EU/EER-datacenter - waarbij eigendomsrecht en datacontrole bij de deelnemer berusten en de opdrachtnemer uitsluitend detectie verzorgt zonder data naar een centraal opdrachtnemer-platform te kopieren - als Model A in de zin van PvE E6.04?	De beschreven architectuur, een door de Opdrachtnemer toegewezen, logisch geïsoleerde en door de Opdrachtnemer beheerde cloudomgeving in een EU/EER-datacenter, is toegestaan, maar kwalificeert als Model B en niet als Model A. Bepalend voor het onderscheid is welke omgeving wordt gebruikt: blijft de data binnen de eigen omgeving van de Deelnemer of binnen het door de Deelnemer gebruikte ecosysteem (Model A), of wordt zij opgeslagen in een eigen, daarvan losstaande omgeving van de Opdrachtnemer (Model B). Dat eigendom en datacontrole bij de Deelnemer liggen en er geen kopie naar een gedeeld centraal platform plaatsvindt, onderscheidt de oplossing van een gedeeld datalake, maar maakt het geen Model A. Bij Model B zijn E6.05, E6.06 en E6.11 van toepassing.
55	PvE E7.08 en E9.03 (STIX/TAXII en MISP)	PvE E7.08 en E9.03 vereisen ondersteuning van STIX, TAXII en MISP, waarbij E9.03 een voorkeur voor automatisering uitdrukt. Is het zo dat de MISP-ondersteuning in PvE E7.08 en E9.03 uitsluitend kan worden ingevuld door een door de opdrachtnemer zelf gehoste MISP-instantie, en dat een geautomatiseerde bidirectionele koppeling via de MISP REST API of STIX/TAXII met een extern beheerde MISP-omgeving niet kwalificeert als gelijkwaardige invulling?	E7.08 en E9.03 vereisen ondersteuning van de standaarden en protocollen (STIX, TAXII, MISP), met voorkeur voor automatisering; zij schrijven geen door Opdrachtnemer zelf gehoste MISP-instantie voor. Een geautomatiseerde bidirectionele koppeling via de MISP REST API of via STIX/TAXII met een extern beheerde MISP-omgeving kwalificeert als gelijkwaardige invulling, mits de vereiste geautomatiseerde uitwisseling van dreigingsinformatie en IOC's wordt geborgd.
56	PvE E5.09 (AI/ML-componenten) in samenhang met E8.02-E8.05	PvE E5.09 vereist dat klantdata uitsluitend geanonimiseerd of geaggregeerd wordt verwerkt voor model-verbetering, met instemming van de deelnemer, en niet voor training van generieke modellen ten behoeve van derden. Is het zo dat een inschrijver niet voldoet aan PvE E5.09 wanneer AI/ML-verwerking uitsluitend in EU/EER-datacenters plaatsvindt, gebruik van klantdata voor model-training ten behoeve van derden contractueel is uitgesloten via een verwerkersovereenkomst, en de deelnemer het recht heeft verwerking te weigeren - uitsluitend omdat de	E5.09 beoordeelt de inzet van AI/ML op basis van waar de verwerking plaatsvindt en de waarborgen daaromheen: de verwerking vindt binnen de EU/EER plaats, klantdata wordt uitsluitend geanonimiseerd of geaggregeerd en met instemming gebruikt voor modelverbetering, en niet voor training van generieke modellen ten behoeve van derden (E5.09 in samenhang met E8.02 t/m E8.05). De vestigingsplaats van de technologieleverancier als rechtspersoon is voor E5.09 op zichzelf niet doorslaggevend, mits aan deze voorwaarden wordt voldaan. De bredere vraag over vestigingsplaats en doorgifte naar derde landen valt onder geschiktheidseis 8 en wordt in dat kader beoordeeld.

		technologieleverancier als rechtspersoon buiten de EU is gevestigd?	
57	Paragraaf 2.2 (M-EDR als verplichte baseline) / PvE E5.07 en E5.17	Paragraaf 2.2 benoemt M-EDR als verplichte baseline. Alle deelnemers beschikken over Microsoft E3/E5-licenties, een deel inclusief Microsoft Defender for Endpoint Plan 1 of Plan 2. PvE E5.01 vereist aansluiting op reeds aanwezige security capabilities. Wordt onder Managed EDR (M-EDR) verstaan dat de opdrachtnemer een eigen EDR-agent uitrolt op de endpoints van de deelnemer, of dat de opdrachtnemer de beheerde 24/7 SOC-monitoring en respons levert bovenop de reeds bij de deelnemer aanwezige endpoint-detectiecapabiliteiten - waaronder Defender for Endpoint Plan 1 of Plan 2 - zonder een eigen agent te installeren?	Onder Managed EDR wordt de beheerde 24/7 SOC-monitoring en respons op endpointniveau verstaan, niet per se een door Opdrachtnemer zelf uitgerolde agent. Opdrachtnemer mag voortbouwen op de reeds aanwezige endpoint-detectiecapaciteiten (zoals Defender for Endpoint P1/P2), conform de eis om aan te sluiten op de bestaande Microsoft-omgeving (E5.01, E5.07, E5.16), of een eigen dan wel gelijkwaardige marktconforme EDR-oplossing inzetten die aan de PvE-eisen voldoet (E5.18, mits beschreven). Een specifieke EDR-tooling is niet voorgeschreven, en een geïntegreerde aanpak waarbij de managed endpoint-detectie en -respons onderdeel is van het SOC voldoet aan de eis. Wel maakt de inschrijver, conform de overige eisen in het PvE, in de gunningsfase inzichtelijk welke impact de gekozen invulling heeft op het gedifferentieerde speelveld van de deelnemers.

58	PvE E1.14 (Tarieven en verdienmodel - facturatiegrondslag)	PvE E1.14 vereist facturatie over verbruik achteraf en een transparante staffelstructuur op basis van heldere grondslagen, met als voorbeelden endpoints, logbronnen, datavolume of een combinatie. Kan de Aanbestedende Dienst bevestigen dat een staffelstructuur op basis van het aantal gebruikers per maand, met maandelijkse facturatie achteraf, voldoet aan PvE E1.14, en dat de keuze van de verbruiksgrondslag vrij is aan de inschrijver mits onderbouwd met voorbeeldcalculaties die de financieele effecten van groei en krimp inzichtelijk maken?	E1.14 maakt onderdeel uit van het concept-Programma van Eisen (Bijlage 10) en blijft als eis van toepassing. De Aanbestedende Dienst zal de grondslag(en) voor de staffelstructuur (zoals aantal endpoints, logbronnen, datavolume, aantal gebruikers of een combinatie) zelf bepalen en in de gunningsfase opnemen in het door Inschrijver in te vullen Prijzenblad. Een door Inschrijver zelf voorgestelde grondslag, zoals een staffel op het aantal gebruikers per maand, wordt in deze fase niet op voorhand bevestigd of uitgesloten
59	PvE E1.14 (Staffelkortingen en collectieve afname) / Paragraaf 2.1	PvE E1.14 bepaalt dat staffelkortingen worden berekend over de gezamenlijke afname van alle deelnemers met een actieve dienstverlening. De aansluitingsplanning toont gefaseerde aansluiting van H1 2027 tot en met 2029. Is het zo dat deelnemers die later dan H1 2027 aansluiten niet automatisch profiteren van het op dat moment geldende collectieve kortingsniveau, en dat voor latere deelnemers een afwijkend kortingsniveau geldt ten opzichte van eerder aangesloten deelnemers?	Staffelkortingen worden bepaald over de gezamenlijke (collectieve) afname van alle actieve Deelnemers; alle Deelnemers profiteren gelijk van de behaalde schaalvoordelen (PvE-verdienmodel). Er geldt geen permanent afwijkend kortingsniveau voor later aangesloten Deelnemers; het op enig moment geldende collectieve niveau is voor alle actieve Deelnemers gelijk. De nadere uitwerking volgt in de gunningsfase.
60	PvE E5.29 (MFA en Privileged Access Management - toepassingsbereik)	PvE E5.29 vereist PAM voor geprivilegieerde toegang, met just-in-time-toegang, sessie-logging en periodieke review. Geldt de PAM-verplichting van PvE E5.29 ook voor geautomatiseerde service-to-service API-verbindingen die technisch noodzakelijk zijn voor het functioneren van de dienstverlening, of uitsluitend voor menselijke beheerders die handmatig directe toegang hebben tot klantdata en -configuraties?	E5.29 ziet op gebruikersinterfaces en geprivilegieerde (menselijke) administratieve toegang; de PAM-onderdelen just-in-time, sessie-logging en periodieke review gelden voor menselijke beheerders met toegang tot het platform, ruwe logdata en configuratie. Geautomatiseerde service-to-service API-verbindingen vallen niet onder de menselijke MFA- en just-in-time-vorm, maar moeten wel passend worden beveiligd met sterke machine-authenticatie en secrets management, least privilege, en logging en periodieke review van de service-accounts (in samenhang met E5.03, E8.25 en E8.30).

61	PvE E8.30 (Logging toegangsrechten - WORM-vereiste)	PvE E8.30 vereist beveiliging van logbestanden via een append-only of equivalent WORM-mechanisme, ook niet-wijzigbaar door beheerders van de opdrachtnemer. Kwalificeert cloudgebaseerde immutable object storage in een EU/EER-datacenter - waarbij schrijfbescherming voor opname van de data is geconfigureerd en wijziging technisch onmogelijk is inclusief voor beheerders van de opdrachtnemer - als equivalent WORM-mechanisme in de zin van PvE E8.30?	Ja. E8.30 is uitkomstgericht: logbestanden moeten append-only of via een vergelijkbaar WORM-mechanisme zijn beveiligd en niet wijzigbaar zijn, ook niet door beheerders van Opdrachtnemer. Cloudgebaseerde immutable object storage in een EU/EER-datacenter waarbij schrijfbescherming vóór opname is geconfigureerd en wijziging technisch onmogelijk is, inclusief voor beheerders van Opdrachtnemer, kwalificeert als een gelijkwaardig WORM-mechanisme, mits de onveranderlijkheid de vereiste bewaartermijn dekt.
62	PvE E6.03 (Retentietijden logdata - 3-jaars bewaarplicht incidentdata)	PvE E6.03 bepaalt dat de kosten voor de minimale basisretentie van 6 maanden zijn inbegrepen in het basistarief. BIO2 artikel 5.28.01 stelt aanvullend een 3-jaars bewaarplicht voor incidentgerelateerde data. Omvat de verplichting om retentiekosten in het basistarief op te nemen uitsluitend de 6-maands basisretentie, of ook de 3-jaars bewaarplicht voor incidentdata? En mag de inschrijver voor de 3-jaars bewaarplicht een transparante, apart geprijsde optie in het Prijzenblad opnemen?	PvE E6.03 blijft als eis van toepassing en verplicht opname van de kosten voor de minimale basisretentie van 6 maanden in het basistarief. De aanvullende bewaarplicht van minimaal 3 jaar voor log- en eventdata die betrekking heeft op een geconstateerd (vermoedelijk) informatiebeveiligingsincident is, conform BIO2 (versie 1.3), een verplichting (zie ook het antwoord op vraag 203). Op welke wijze de kosten hiervoor in het Prijzenblad worden verwerkt — al dan niet als afzonderlijke post — bepaalt de Aanbestedende Dienst zelf; dit wordt in de gunningsfase aan Inschrijver voorgelegd
63	Selectiecriterium 1, onderdeel digitale soevereiniteit - paragraaf 7.2 / Paragraaf 2.2	Selectiecriterium 1 bevraagt de visie op digitale soevereiniteit en de risico's van toepasselijkheid van niet-EU-wetgeving. Paragraaf 2.2 signaleert dat deelnemers op termijn alternatieven voor Amerikaanse producten kunnen inzetten. Is het zo dat een inschrijver het onderdeel digitale soevereiniteit van Selectiecriterium 1 niet als 'Goed' of 'Uitstekend' kan worden beoordeeld uitsluitend vanwege de vestigingsplaats buiten de EU van de ingezette technologieleverancier, ongeacht contractuele EER-garanties, de positie van de inschrijver als NL-gevestigde verwerkingsverantwoordelijke en een beschreven retransitieaanpak conform PvE E8.05?	Het onderdeel digitale soevereiniteit van Selectiecriterium 1 wordt beoordeeld op de kwaliteit van de organisatiebrede visie, niet uitsluitend op de vestigingsplaats van een ingezette technologieleverancier. Een aanmelding kan als 'Goed' of 'Uitstekend' worden beoordeeld ondanks een niet-EU-gevestigde technologieleverancier, mits de visie en geboden waarborgen daartoe aanleiding geven en aan Geschiktheidseis 8 wordt voldaan. De beoordeling verloopt via de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%). Bepalend is de mate waarin het antwoord inhoudelijk relevant, concreet, toepasselijk, onderscheidend en innoverend is. Er wordt geen voorkeur toegekend aan een specifieke architectuur of oplossing. Beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet in de beoordeling betrokken.

64	PvE E1.09 (Uitvoeringsverplichtingen uit selectiecriteria-antwoorden)	PvE E1.09 bepaalt dat antwoorden op kwalitatieve sub-gunningcriteria automatisch deel uitmaken van de uitvoeringsverplichtingen. Het bewijsmiddel bij de selectiecriteria stelt dat beschrijvingen betrekking hebben op de 'eigen organisatie en werkwijze' en dat antwoorden over de 'voorgenomen aanpak voor de opdracht' niet worden beoordeeld. Omvat de uitvoeringseis van PvE E1.09 uitsluitend de beschreven methoden en werkwijzen van de inschrijver, of ook specifieke technische implementatiekeuzes die als praktijkvoorbeeld uit bestaande klantomgevingen worden vermeld in de visie?	PvE E1.09 bepaalt dat antwoorden op kwalitatieve sub-gunningcriteria (gunningsfase) automatisch deel uitmaken van de uitvoeringsverplichtingen. In de selectiefase vraagt het bewijsmiddel bij de selectiecriteria om een beschrijving van de eigen organisatie en werkwijze; beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet beoordeeld (§7.2-7.4). De uitvoeringseis in de gunningsfase ziet op de beschreven methoden en werkwijzen; de Aanbestedende Dienst zal in de gunningsfase verduidelijken welke elementen uitvoeringsverplichting worden.
65	PvE E8.04 (ABRO-toepasselijkheid) / Paragraaf 2.1	PvE E8.04 bepaalt dat de dienstverlening geheel of gedeeltelijk onder de ABRO kan vallen. De Veiligheidsregio's zijn publiekrechtelijke samenwerkingsverbanden van gemeenten als decentrale overheden. De ABRO geldt formeel voor Rijksoverheidsopdrachten. Voor welke specifieke deelnemers is de ABRO formeel van toepassing, en welke concrete verplichtingen gelden voor de opdrachtnemer per betrokken deelnemer bij aanvang van de dienstverlening?	Zie 201
66	PvE E7.15 (Time-to-notify definitie - P1 = 10 minuten)	PvE E7.15 definieert time-to-notify als 'de tijd tussen het automatisch genereren van een alarm en de melding van een mogelijk incident bij de desbetreffende Deelnemer.' Het begrip 'melding' is niet nader gedefinieerd. Kwalificeert het automatisch beschikbaar komen van een alarm in het SOC-portaal van de deelnemer via de SSO-toegang als bedoeld in PvE E5.22 als de 'melding' in de zin van PvE E7.15, of vereist de eis een actieve notificatie via een aanvullend kanaal als afzonderlijke handeling?	De 'melding' in E7.15 is een actieve melding van het (mogelijke) incident aan de Deelnemer, niet uitsluitend het passief beschikbaar komen van het alarm in het SOC-portaal. Het portaal (E5.22, E7.21) biedt inzage, maar voldoet op zichzelf niet aan de time-to-notify. Voor incidenten, in het bijzonder P1 en P2, is een actieve notificatie via een in het DAP afgesproken kanaal vereist (zie ook E7.20, alarmeren bij P1/P2 conform E7.15).

67	PvE E8.35 (Penetratietest - scope bij SaaS-platform)	PvE E8.35 omschrijft de pentestscope als: 'de SIEM-, SOAR- en monitoringplatforms binnen het beheer van Opdrachtnemer.' Omvat 'binnen het beheer van Opdrachtnemer' uitsluitend de door de opdrachtnemer geconfigureerde lagen - connectoren, detectielogica en aansluitvoorzieningen - of ook de onderliggende cloudinfrastructuur van een SaaS-technologieleverancier waarover de opdrachtnemer geen eigenstandig testmandaat heeft?	"Binnen het beheer van Opdrachtnemer" omvat de lagen die Opdrachtnemer zelf configureert en beheert: connectoren, detectielogica, aansluitvoorzieningen en de configuratie van en toegang tot de SIEM-, SOAR- en monitoringplatforms. De onderliggende cloudinfrastructuur van een SaaS-technologieleverancier waarover Opdrachtnemer geen eigenstandig testmandaat heeft, valt niet onder de pentestscope; die wordt afgedekt door de eigen assurance en certificering van die leverancier.
68	PvE E6.09 (Logdata-ontsluiting - Microsoft-first als verplichting of voorkeur)	PvE E6.09 bepaalt dat 'waar mogelijk' gebruik wordt gemaakt van bestaande capabilities binnen de Microsoft-stack van de deelnemer, om beheer- en netwerklast te beperken. Is deze bepaling een verplicht architectuurprincipe waarbij de opdrachtnemer bij deelnemers met een actieve Defender XDR- of Sentinel-omgeving verplicht is deze Microsoft-native connectoren als primair ontsluitingsmechanisme te hanteren, of is het een voorkeur waarvan de opdrachtnemer gemotiveerd kan afwijken?	"Waar mogelijk" maakt E6.09 een uitgangspunt met voorkeur, geen absolute verplichting. Bij deelnemers met een actieve Defender XDR- of Sentinel-omgeving hanteert Opdrachtnemer bij voorkeur de Microsoft-native capabilities als ontsluitingsmechanisme, om beheer- en netwerklast te beperken. Opdrachtnemer kan hiervan gemotiveerd afwijken wanneer een alternatieve ontsluiting aantoonbaar passender is, mits de volledigheid van de logdata en de overige PvE-eisen, waaronder data-soevereiniteit, geborgd blijven.
69	Selectiecriteria 1, 2 en 3 - paragraaf 7.2, 7.3, 7.4 Selectiedocument (bewijsmiddel)	Het bewijsmiddel bij Selectiecriteria 1, 2 en 3 vereist 'concrete voorbeelden uit de praktijk' over de 'eigen organisatie en werkwijze.' Er wordt niet gespecificeerd uit welke sector deze voorbeelden afkomstig moeten zijn. Mogen als concrete praktijkvoorbeelden ook opdrachten bij commerciele of internationale klanten worden aangehaald, of verwacht de Aanbestedende Dienst uitsluitend voorbeelden uit de sector publieke veiligheid, overheid of zorg?	Er is geen beperking tot een specifieke sector. Praktijkvoorbeelden uit commerciële of internationale opdrachten zijn toegestaan, mits zij de gevraagde visie en gerealiseerde kwaliteit/uitkomsten onderbouwen. Voorbeelden uit de sectoren publieke veiligheid, overheid of zorg zijn niet verplicht.

70	Selectiecriterium 2, onderdeel verhouding bestaande capabilities / aanvullende tooling - paragraaf 7.3 Selectiedocument	Selectiecriterium 2 vraagt naar de visie op 'de verhouding tussen bestaande beveiligingscapabiliteiten en aanvullende tooling' als leidend principe. Paragraaf 2.2 beschrijft dat meerdere deelnemers beschikken over bestaande SIEM-omgevingen zoals Microsoft Sentinel. Waardeert de Aanbestedende Dienst bij de beoordeling van Selectiecriterium 2 een aanpak waarbij de inschrijver zijn dienstverlening positioneert als aanvulling op bestaande Microsoft-security-investeringen aantoonbaar positiever dan een aanpak waarbij de inschrijver een functioneel superieure vervanging aanbiedt van de bestaande SIEM-omgeving?	Selectiecriterium 2 vraagt onder meer naar de visie op de verhouding tussen bestaande capabilities en aanvullende tooling, waarbij het als uitgangspunt nemen van bestaande capabilities een leidend principe is (§7.3). Een aanpak die bestaande investeringen als uitgangspunt neemt sluit hierop aan. Een 'aanvulling' op of een 'vervanging' van bestaande SIEM-omgevingen wordt niet op voorhand positiever gewaardeerd; bepalend is de kwaliteit van de onderbouwde visie. De beoordeling verloopt via de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%). Bepalend is de mate waarin het antwoord inhoudelijk relevant, concreet, toepasselijk, onderscheidend en innoverend is. Er wordt geen voorkeur toegekend aan een specifieke architectuur of oplossing. Beschrijvingen die primair ingaan op de voorgenomen aanpak voor deze opdracht worden niet in de beoordeling betrokken.
71	PvE E1.11 (All-in tarieven) in samenhang met E4.01 en E4.08 (Onboarding en implementatie)	PvE E1.11 vereist all-in tarieven, inclusief kosten voor apparatuur, software en hardware die nodig zijn bij het oplossen van een informatieveiligheidsincident. PvE E4.01 en E4.08 vereisen implementatieondersteuning en een vaste projectleider per deelnemer bij onboarding. Dienen eenmalige implementatie- en onboardingkosten per deelnemer - waaronder tenant-inrichting, agent-uitrol, data-source onboarding en configuratie van detectielogica - onderdeel te zijn van het all-in basistarief conform E1.11, of mogen deze als transparante eenmalige projectkosten per Nadere Overeenkomst worden opgenomen in het Prijzenblad?	De Aanbestedende Dienst zal de opbouw van het Prijzenblad, waaronder de vraag of eenmalige implementatie- en onboardingkosten als afzonderlijke post dan wel verdisconteerd in het basistarief worden uitgevraagd, zelf bepalen en in de gunningsfase aan Inschrijver voorleggen. Een door Inschrijver zelf voorgestelde opsplitsing van kostencomponenten wordt in deze fase niet op voorhand bevestigd of uitgesloten.

72	PvE E1.14 (Staffelstructuur - minimum afname per individuele deelnemer)	PvE E1.14 beschrijft staffelkortingen over de gezamenlijke afname van alle deelnemers, maar noemt geen minimum afname per individuele deelnemer. Geldt er een minimale afname per individuele deelnemer - uitgedrukt in endpoints, gebruikers of een andere eenheid - om gebruik te mogen maken van de raamovereenkomst, en zo ja, wat is dat minimum?	De Raamovereenkomst kent geen afname- of omzetgarantie; alle in de aanbestedingsstukken genoemde bedragen en aantallen zijn indicatief en Opdrachtnemer kan hieraan geen rechten ontlenen (PvE E1.13). Er geldt geen voorgeschreven minimale afname per individuele Deelnemer om gebruik te maken van de Raamovereenkomst; de Raamovereenkomst kan meegroeien of krimpen naar gebruik (PvE E1.14). Voor zover Inschrijver in zijn verdienmodel met staffelgrenzen werkt, wordt dit transparant in het Prijzenblad onderbouwd (gunningsfase).
73	PvE E7.06 en E7.07 (Dreigingsinformatiebronnen - Connect2Trust en Z-CERT)	PvE E7.06 vereist dreigingsinformatie van Connect2Trust en vergelijkbare sectorale trust-netwerken, alsmede Z-CERT voor deelnemers met zorggerelateerde processen. PvE E7.07 vereist dat de opdrachtnemer partnerships en informatiedelingsafspraken heeft met de bronnen uit E7.06. Dient de opdrachtnemer bij aanmelding of uiterlijk bij gunning te beschikken over een actief lidmaatschap van of informatiedelingsafspraak met Connect2Trust en - voor zover van toepassing - Z-CERT, of volstaat het aantonen van de bereidheid en het vermogen om deze aansluitingen bij aanvang van de dienstverlening per deelnemer te realiseren?	Het is niet vereist dat de inschrijver bij inschrijving of gunning reeds over een actief lidmaatschap of informatiedelingsafspraak met Connect2Trust en, voor zover van toepassing, Z-CERT beschikt. Bij gunning toont de inschrijver de bereidheid en het vermogen aan, met een concreet plan, om deze aansluitingen te realiseren. De partnerships en informatiedelingsafspraken (E7.07) zijn operationeel uiterlijk bij aanvang van de dienstverlening, per Deelnemer en voor zover van toepassing (Z-CERT uitsluitend voor deelnemers met zorggerelateerde processen). De enige uitzondering is de situatie waarin Z-CERT de aansluiting afwijst; in dat geval vervalt die verplichting voor zover het Z-CERT betreft.

74	Bijlage 6 / Geschiktheidseis 4 - Kerncompetentie 2 - paragraaf 6.4 Selectiedocument	Bijlage 6 vereist bij kerncompetentie 2 opgave van het exacte gefactureerde bedrag in euros exclusief btw. Het openbaar maken van exacte contractbedragen is in de zakelijke markt standaard vertrouwelijk en maakt doorgaans onderdeel uit van contractuele geheimhoudingsbepalingen met opdrachtgevers. Het verplicht stellen van prijsopgave in een openbaar aanmeldingsdossier stelt gegadigden voor de keuze tussen contractbreuk richting bestaande klanten of uitsluiting van de aanbestedingsprocedure. Dit is disproportioneel en niet noodzakelijk om te beoordelen of aan de minimumdrempel van 200.000 euro is voldaan. Is de Aanbestedende Dienst bereid Bijlage 6 te wijzigen zodat voor kerncompetentie 2 volstaat met een ondertekende verklaring van de referentopdrachtgever dat het gefactureerde bedrag de minimumdrempel van 200.000 euro overschrijdt, zonder opgave van het exacte bedrag, zodat geen inbreuk wordt gemaakt op commercieel vertrouwelijke prijsafspraken?	Ja, wij passen dit aan. De Aanbestedende Dienst past Bijlage 6 aan: voor kerncompetentie 2 volstaat een verklaring dat het gefactureerde bedrag voor de betreffende opdracht minimaal € 200.000 excl. btw bedraagt, zonder opgave van het exacte bedrag. De aangepaste Bijlage 6 wordt gepubliceerd op TenderNed.
75	Bijlage 6 / Geschiktheidseis 4 - Kerncompetentie 2 - paragraaf 6.4 Selectiedocument	Kerncompetentie 2 stelt als eis een opdracht met een minimale omvang van 200.000 euro. Het Selectiedocument specificeert niet of dit het totale gefactureerde bedrag over de gehele (minimaal 3-jarige) looptijd betreft, of het jaarlijks gefactureerde bedrag. Betreft de minimale omvang van 200.000 euro het totale gefactureerde bedrag over de volledige looptijd van de referentieopdracht, of dient dit bedrag jaarlijks gefactureerd te zijn?	De minimale omvang van € 200.000 (excl. btw) bij Kerncompetentie 2 betreft het totale gefactureerde bedrag over de (minimaal 3-jarige) referentieopdracht, niet een jaarlijks gefactureerd bedrag.

76	Bijlage 6 / Geschiktheidseis 4 - Kerncompetentie 2 - paragraaf 6.4 Selectiedocument	Kerncompetentie 2 vereist IT-dienstverlening met de BIO als normenkader. In de praktijk worden BIO-gerelateerde diensten vaak geleverd als onderdeel van een bredere opdracht, waarbij meerdere diensten (zoals firewall management, security monitoring en advies) gezamenlijk worden gefactureerd. Mag het totale gefactureerde bedrag van de gehele opdracht worden opgegeven in Bijlage 6, ook als de opdracht meerdere diensten omvat waarvan niet alle diensten expliciet onder de BIO vallen, of dient het opgegeven bedrag uitsluitend betrekking te hebben op het aantoonbaar BIO-gerelateerde deel van de dienstverlening?	Bij Kerncompetentie 2 dient de referentieopdracht IT-dienstverlening te betreffen waarbij de BIO als normenkader is gehanteerd. Indien BIO-gerelateerde dienstverlening onderdeel uitmaakt van een bredere opdracht, mag het totale bedrag worden opgegeven voor zover de gehele opdracht onder het BIO-normenkader is uitgevoerd; voor het overige dient het opgegeven bedrag betrekking te hebben op het aantoonbaar BIO-gerelateerde deel.
77	Bijlage 6 / Geschiktheidseis 4 - Kerncompetentie 2 - paragraaf 6.4 Selectiedocument	Kerncompetentie 2 staat toe dat nog lopende referentieopdrachten worden opgegeven, mits voldaan aan de minimaal geëiste looptijd van 3 jaar. Bij lopende opdrachten is het totale gefactureerde bedrag op de datum van aanmelding lager dan de uiteindelijke opdrachtwaarde. Mag voor een nog lopende referentieopdracht het tot de datum van aanmelding gefactureerde bedrag worden opgegeven als bewijsmiddel voor de minimale omvang van 200.000 euro, ook als dit bedrag op de peildatum nog niet volledig is bereikt maar de verwachte totale opdrachtwaarde de drempel op jaarbasis ruimschoots overschrijdt?	De referentieopdracht moet in de drie jaar vóór de datum van Aanmelding zijn verricht. Zowel afgeronde als nog lopende opdrachten kwalificeren, mits aan de minimale looptijd van 3 jaar is voldaan. Een opdracht die voor deze driejaarsperiode is aangevangen kwalificeert, mits zij binnen de driejaarsperiode nog in uitvoering was of is afgerond. Voor een nog lopende referentieopdracht is het tot de datum van Aanmelding gefactureerde bedrag bepalend; dit dient ten minste € 200.000 (excl. btw) te bedragen.
78	Hoofdstuk 6 Geschiktheidseisen	Accepteert de Aanbestedende Dienst, in het geval de inschrijver geen eigen jaarrekening opstelt, een geconsolideerde jaarrekening van de moedermaatschappij in combinatie met een gedeponeerde 403-verklaring als invulling van deze eis, zonder dat een beroep wordt gedaan op de draagkracht van de moedermaatschappij en zonder separate UEA voor de moedermaatschappij?	Een geconsolideerde jaarrekening van de moedermaatschappij in combinatie met een gedeponeerde 403-verklaring kan worden aanvaard als invulling van Geschiktheidseis 2, mits hieruit blijkt dat aan de eis wordt voldaan. Wanneer geen beroep wordt gedaan op de draagkracht van de moeder als 'derde' in de zin van §4.5, is een separaat UEA van de moedermaatschappij niet vereist.

79	Hoofdstuk 4.5 Beroep op derden & Bijlage 5 Verklaring middelen derde	Dient de “Verklaring middelen derde” te worden ondertekend door zowel de inschrijver als de betreffende derde partij, of uitsluitend door de inschrijver?	De 'Verklaring middelen derde' (Bijlage 5) dient door zowel de Gegadigde als de betreffende derde te worden ingevuld en rechtsgeldig ondertekend (§4.5.1). De verklaring wordt overgelegd door de Gegadigde aan wie de Aanbestedende Dienst de Opdracht beoogt te gunnen.
80	Hoofdstuk 1 Begrippenlijst	Kunt u toelichten op welke wijze Deelovereenkomsten tot stand komen onder de Raamovereenkomst?	Op basis van de Raamovereenkomst met één Opdrachtnemer sluit iedere Deelnemer een Deelovereenkomst (Nadere Overeenkomst), waarin de specifieke dienstverlening nader wordt uitgewerkt (zie Begrippenlijst). De Deelovereenkomst komt tot stand bij aansluiting van de betreffende Deelnemer, waarbij een keuze wordt gemaakt uit serviceniveaus en optionele diensten en een specifieke SLA en DAP worden opgesteld (PvE E3.04).
81	Hoofdstuk 1 Begrippenlijst	Kunt u aangeven op welke wijze prijsvorming binnen Deelovereenkomsten plaatsvindt en in welke mate deze af kan wijken van de Raamovereenkomst?	De prijsvorming binnen Deelovereenkomsten vindt plaats op basis van de tarieven die zijn vastgelegd in het Prijzenblad, dat als onderdeel van de Raamovereenkomst in de gunningsfase wordt opgesteld. Afwijking van deze tarieven binnen een Deelovereenkomst is niet toegestaan. De opbouw van het verdienmodel, waaronder eventuele staffeling, bepaalt de Aanbestedende Dienst zelf en wordt in de gunningsfase nader uitgewerkt.
82	Hoofdstuk 1 Begrippenlijst	Kunt u aangeven of het proces en de voorwaarden voor Deelovereenkomsten verder worden uitgewerkt in de gunningsfase?	Bevestigd. Het proces en de voorwaarden voor de Deelovereenkomsten worden nader uitgewerkt in de gunningsfase (beschrijvend document, concept-Raamovereenkomst en concept-Deelovereenkomst).

83	Hoofdstuk 3 Aanbestedingsprocedure - Paragraaf 3.8 Proces beoordeling aanmeldingen	Kunt u aangeven: 1. Of het gebruik van voorgeschreven formats/templates verplicht is voor de Aanmelding (naast de voorgeschreven bijlagen), en 2. Welke structuur en volgorde wordt verwacht voor de Aanmelding en de visiedocumenten, 3. Of er beperkingen gelden voor aanvullende bijlagen naast de genoemde paginalimieten?	Zie het antwoord op vraag 45 voor de voorgeschreven bijlagen en de beperkingen voor aanvullende bijlagen. Aanvullend hierop: de visiedocumenten dienen qua structuur de in §7.2-7.4 gevraagde onderdelen te volgen; een vaste volgorde daarbuiten is niet voorgeschreven.
84	Hoofdstuk 3.8 Proces beoordeling Aanmeldingen	Kunt u bevestigen dat geschiktheidseisen uitsluitend als knock-out criteria worden gehanteerd en geen onderdeel vormen van de onderlinge ranking? Kunt u daarnaast toelichten op welke wijze de ranking tussen gegadigden tot stand komt binnen de selectiecriteria?	Bevestigd. Geschiktheidseisen worden als knock-out gehanteerd (stap 4, §3.8): een Gegadigde die niet voldoet wordt terzijde gelegd. Geschiktheidseisen maken geen onderdeel uit van de onderlinge ranking. De ranking komt uitsluitend tot stand op basis van de score op de selectiecriteria (stap 5): SC1 = 40 punten, SC2 = 35 punten, SC3 = 25 punten. De 5 hoogst scorende Gegadigden worden uitgenodigd; bij een gelijke 5e plaats geldt voorrang op SC1.
85	Hoofdstuk 7 Selectiecriteria - Paragraaf 7.1 t/m 7.4	Er wordt gevraagd om visies (MDR, CTI, R&D), de beoordelingsmethodiek is globaal en er zijn geen concrete criteria of scoringsrubrieken. Kunt u nader specificeren op basis van welke beoordelingsaspecten (bijv. diepgang, concreetheid, toepasbaarheid, meetbare resultaten) de visiedocumenten worden beoordeeld, en hoe onderscheid wordt gemaakt tussen inschrijvingen die op hoofdlijnen vergelijkbaar zijn?	De visiedocumenten worden beoordeeld aan de hand van de schaal in §7.1 (Uitstekend 100% / Goed 80% / Voldoende 50% / Matig 20% / Onvoldoende 0%) op de mate van inhoudelijke relevantie, concreetheid, toepasselijkheid, onderscheidend vermogen en innovatie voor ieder van de in §7.2-7.4 opgenomen onderdelen. Er worden geen separate sub-scores per onderdeel toegekend; de algehele kwaliteit van de visie is bepalend.

86	Hoofdstuk 3.8 Proces beoordeling Aanmeldingen	Kunt u aangeven uit welke functionele rollen de beoordelingscommissie bestaat (bijv. inkoop, inhoudelijke experts, security-specialisten) en of sprake is van een multidisciplinair beoordelingsteam?	De beoordelingscommissie is multidisciplinair samengesteld en bestaat uit functionarissen met expertise op het gebied van inkoop/aanbesteding, informatiebeveiliging/cybersecurity en inhoudelijke kennis van SOC/MDR-dienstverlening. De precieze samenstelling en functies van de commissieleden worden niet nader bekendgemaakt.
87	Bijlage 10, Programma van Eisen, E2.01	Kan de Aanbestedende Dienst nader toelichten: a) op welke wijze wordt bepaald of sprake is van een “relatie of inmenging met statelijke actoren” en welke toetsingscriteria en beoordelingsmethodiek daarbij worden gehanteerd; en b) hoe het begrip “relatie of inmenging met statelijke actoren” concreet wordt gedefinieerd, in het bijzonder welke situaties en vormen van betrokkenheid hieronder worden begrepen (zoals onder meer aandeelhouderschap, hosting en afhankelijkheden in de supply chain)?	De classificatie volgt de actuele AIVD- en NCTV-dreigingsanalyse (Cybersecuritybeeld Nederland en AIVD-jaarverslag), jaarlijks getoetst (E2.01). "Relatie of inmenging" omvat betrokkenheid waardoor zo'n actor invloed, toegang of zeggenschap kan krijgen op Opdrachtnemer of de dienstverlening, waaronder zeggenschap of aandeelhouderschap, hosting of dataverwerking en supply chain-afhankelijkheden. De wijze van aantonen valt onder de geschiktheidseisen.
88	Bijlage 10, Programma van Eisen, E7.15	Hoe wordt omgegaan met time-to-notify buiten bemensingsuren bij gekozen servicelevel?	De time-to-notify (P1 10 minuten, P2 30 minuten, P3 4 uur) geldt binnen het overeengekomen serviceniveau (E3.03). Buiten de bemensingsuren gelden deze tijden voor zover redelijkerwijs haalbaar binnen het bij dat niveau passende mechanisme: bij niveau 1 continu (eyes-on-screen 24/7), bij niveau 2 voor P1 en P2 via de 24x7 piketregeling, en bij niveau 3 geen actieve melding buiten de bemensingsuren, waarbij alarmen wel worden gedetecteerd en vastgelegd en bij aanvang van het eerstvolgende bemenste venster worden opgevolgd. De systemen monitoren in alle gevallen 24/7 door.
89	Bijlage 10, Programma van Eisen, E1.14	Is het verplicht om alle prijscomponenten volledig transparant uit te werken inclusief groeiscenario’s?	de prijscomponenten en de staffelstructuur, inclusief de financiële effecten van groei en krimp, dienen transparant inzichtelijk te zijn. Dit wordt geborgd doordat Inschrijver het door de Aanbestedende Dienst opgestelde Prijzenblad invult; de Aanbestedende Dienst bepaalt zelf de exacte opzet waarmee deze transparantie wordt uitgevraagd. Het Prijzenblad wordt in de gunningsfase verstrekt.

90	Bijlage 10, Programma van Eisen, E1.11	Dienen alle kosten (incl. tooling, personeel, IR etc.) volledig inbegrepen te zijn zonder additionele kostenposten?	Ja. E1.11 vereist dat de aangeboden tarieven all-in zijn, dat wil zeggen inclusief (niet-limitatief) salariskosten, overheadkosten, kosten voor gebruik van apparatuur/software/hardware en de overige in E1.11 genoemde kostencomponenten. Aanvullende kostenposten naast het aangeboden tarief voor de in E1.11 bedoelde componenten zijn niet toegestaan. De wijze waarop dit tarief in het Prijzenblad wordt opgebouwd en uitgesplitst, wordt in de gunningsfase nader bepaald.
91	Bijlage 11 voorwaarden deelnemers met voorwaarden	Leidt overschrijding van regionale budgetten automatisch tot opt-out of is heronderhandeling mogelijk?	Overschrijding van een in Bijlage 11 opgenomen regionaal budgetplafond leidt er automatisch toe dat de betreffende 'Deelnemer met voorwaarden' niet aan de Raamovereenkomst deelneemt (opt-out); dit heeft geen gevolgen voor de overige Deelnemers. Bijlage 11 bevat geen harde eisen voor de gunning en maakt geen onderdeel uit van het PvE.
92	Bijlage 11 voorwaarden deelnemers met voorwaarden	Kan de Aanbestedende Dienst verduidelijken of van de Opdrachtnemer wordt verwacht dat de MDR-dienstverlening wordt ingericht volgens één uniform model voor zowel het IT-domein als de zorggerelateerde domeinen (zoals GGD, ambulancezorg en GHOR), dan wel dat differentiatie per domein is toegestaan of vereist?	De MDR-dienstverlening kent één uniform dienstmodel als basis. De concrete inrichting wordt per Deelnemer, en waar relevant per domein (IT en zorggerelateerde domeinen zoals GGD, ambulancezorg en GHOR), risicogebaseerd afgestemd via de Nadere Overeenkomst. Differentiatie per domein is toegestaan binnen het uniforme model; de inschrijver licht de gekozen inrichting toe tijdens de gunningsfase.
93	Bijlage 10, Programma van Eisen, E8.01–E8.03	Hoe wordt omgegaan met oplossingen gebaseerd op non-EU technologie (bijv. Microsoft/cloudproviders) binnen deze eis?	Zie 46.

94	Bijlage 10, Programma van Eisen, E2.01	Hoe wordt “relatie of inmenging met statelijke actoren” concreet gedefinieerd en beoordeeld (bijv. aandeelhouderschap, hosting, supply chain)?	Onder 'relatie of inmenging met statelijke actoren' wordt verstaan een band met of beïnvloeding door statelijke actoren die door de AIVD of NCTV als offensieve dreigingsactor tegenover Nederlandse vitale belangen zijn geclassificeerd (Geschiktheidseis 9 / PvE E2.01). De geldende lijst wordt jaarlijks getoetst aan het Cybersecuritybeeld Nederland (NCTV) en het AIVD-jaarverslag. De eis omvat relevante vormen van betrokkenheid zoals zeggenschap/aandeelhouderschap, hosting en afhankelijkheden in de toeleveringsketen.
95	Bijlage 10, Programma van Eisen, E5.20	Moet SOAR direct operationeel ingezet worden of is het voldoende dat deze capability beschikbaar is voor toekomstige inzet?	De SOAR-capability moet bij aanvang beschikbaar zijn; dit is een toekomstbestendigheidsvereiste (E5.20). Directe, volledige operationele inzet is niet vereist: ook bij beperkte geautomatiseerde respons bij aanvang moet de capability beschikbaar zijn voor groei tijdens de looptijd. De daadwerkelijke inzet wordt per Deelnemer risicogebaseerd en gefaseerd ingericht binnen de in playbooks en het DAP afgesproken kaders (E5.24, E3.04). De eis betreft dus de beschikbaarheid van de capability, niet een verplichte directe integratie; omzetting naar een wens is daarom niet nodig.
96	Bijlage 10, Programma van Eisen, E7.15	Hoe worden SLA’s (time-to-notify) beoordeeld buiten bemenste uren bij lagere servicelevels?	Zie het antwoord op vraag 88.
97	Bijlage 10, Programma van Eisen, E1.11	Dienen de aangeboden tarieven volledig all-in te zijn of mogen aanvullende kostencomponenten worden toegevoegd?	Ja. E1.11 vereist dat de aangeboden tarieven all-in zijn, dat wil zeggen inclusief (niet-limitatief) salariskosten, overheadkosten, kosten voor gebruik van apparatuur/software/hardware en de overige in E1.11 genoemde kostencomponenten. Aanvullende kostenposten naast het aangeboden tarief voor de in E1.11 bedoelde componenten zijn niet toegestaan. De wijze waarop dit tarief in het Prijzenblad wordt opgebouwd en uitgesplitst, wordt in de gunningsfase nader bepaald.

98	Bijlage 10, Programma van Eisen, E1.14	Is het verplicht om een volledige staffelstructuur met groeiscenario's en voorbeeldcalculaties op te nemen?	Zie 89.
99	Bijlage 10, Programma van Eisen, E1.14	Hoe wordt omgegaan met prijsverschillen per deelnemer (bijv. verschillende volumes/licenties)?	E1.14 maakt onderdeel uit van het concept-Programma van Eisen (Bijlage 10). Verschillen in afname per Deelnemer (volume, licenties, serviceniveau, scope) leiden tot een verschillend factuurbedrag per Deelnemer; het gestaffelde tariefniveau wordt over het collectieve volume bepaald. De wijze waarop deze verschillen inzichtelijk worden gemaakt, bepaalt de Aanbestedende Dienst zelf en wordt opgenomen in het door Inschrijver in te vullen Prijzenblad, dat in de gunningsfase wordt verstrekt
100	Algemeen	Bent u bereid om, na gunning en succesvolle uitvoering van de opdracht, op verzoek van de Opdrachtnemer als referent op te treden voor toekomstige (aanbestedings)trajecten, bijvoorbeeld door middel van het verstrekken van een referentieverklaring of het fungeren als contactreferentie?	De Aanbestedende Dienst staat in beginsel open voor het fungeren als referent na gunning en succesvolle uitvoering van de opdracht, voor zover toepasselijke regels en de vertrouwelijkheidsverplichting (§3.15 Selectiedocument) dit toestaan. Definitieve afspraken hierover kunnen in de gunningsfase of na contractsluiting worden gemaakt.
101	Bijlage 11 voorwaarden deelnemers met voorwaarden	In Bijlage 11 ("voorwaarden deelnemers met voorwaarden") wordt voor een aantal Veiligheidsregio's expliciet verwezen naar toepassing van de BIO-normering. Kan de aanbestedende dienst verduidelijken of wordt verwacht dat alle deelnemende Veiligheidsregio's gedurende de looptijd van de raamovereenkomst deze normering (volledig) zullen hanteren of implementeren?	De dienstverlening sluit aan op de BIO: zo geldt de retentie conform BIO2 (E6.03) en de auditlog conform BIO/NEN7510 (E8.36), en ondersteunt Opdrachtnemer de Deelnemers conform de voor hen toepasselijke kaders (E7.12, E2.05). De mate en het tempo waarin een individuele Deelnemer de BIO zelf implementeert, is de verantwoordelijkheid van die Deelnemer en wordt in deze aanbesteding niet centraal voor alle deelnemers afgedwongen of gegarandeerd. Waar een Deelnemer de BIO expliciet als aanvullende voorwaarde in Bijlage 11 noemt, kan die zich daarop beroepen.

102	Selectiedocument SOC-MDR Versie 1.0, Paragraaf 6.4	Conform (Technische bekwaamheid en beroepsbekwaamheid), kerncompetentie 2, dient de Gegadigde aantoonbare ervaring te hebben met IT-dienstverlening waarbij de Baseline Informatiebeveiliging Overheid (BIO) als normenkader is gehanteerd. Kan de aanbestedende dienst bevestigen of een referentie die is gebaseerd op ISO/IEC 27001 (ISO27001 Annex A) en ISO/IEC 27002, en waarbij aantoonbaar sprake is van vergelijkbare informatiebeveiligingsmaatregelen, als gelijkwaardig wordt geaccepteerd?	Een referentie gebaseerd op ISO/IEC 27001 (Annex A) en ISO/IEC 27002 kan als gelijkwaardig aan het BIO-normenkader worden aanvaard, mits aantoonbaar is dat vergelijkbare informatiebeveiligingsmaatregelen zijn gehanteerd. De Gegadigde onderbouwt de gelijkwaardigheid in het referentieformulier; de Aanbestedende Dienst beoordeelt dit.
103	Selectiedocument SOC-MDR Versie 1.0	2.6 Doel Aanbestedingsprocedure. De periode van de Raamovereenkomst is 4 jaar met opties tot verlengingen tot maximaal 12 jaar. Kan aanbestedende dienst aangeven wat de mogelijkheden zijn om overeengekomen tarieven aan te passen bij verlenging? Inschrijver gebruikt o.a. technologieen van 3e partijen welke kosten met zich mee brengen. Eventuele jaarlijkse indexatie van de tarieven is mogelijk niet toereikend bij stijging van deze materiaalkosten.	De wijze van (eventuele) jaarlijkse indexatie of tariefaanpassing wordt in de gunningsfase geregeld in het beschrijvend document en de (concept-)Raamovereenkomst. Deze vraag valt buiten de selectiefase.
104	Selectiedocument SOC-MDR Versie 1.0	3.3 Beoogde planning. Inschrijver overweegt deel te nemen aan de selectiefase. Hiervoor moet inschrijver o.a. het PvE met 161 eisen doornemen. De 5 werkdagen tussen publicatie en deadline indien vragen is hiervoor niet toereikend. Kan aanbestedende dienst een tweede vragen ronde opnemen in de planning?	De beoogde planning (§3.3 Selectiedocument) bevat één vragenronde in de selectiefase, met uiterste datum 15 juni 2026. De planning voorziet in twee vragenrondes in de gunningsfase (augustus en september 2026). Een tweede vragenronde in de selectiefase is niet voorzien en wordt niet toegevoegd aan de huidige planning. Vragen over het PvE zijn voorzien in de gunningsfase.
105	Bijlage 10 Programma van Eisen	Inschrijver merkt op dat het PvE 161 eisen bevat en acht dat het aantal marktpartijen die aan alle eisen kunnen voldoen beperkt zeer beperkt zal zijn. Is het mogelijk dat punten uit deze bijlage als wens worden opgenomen met een wegingsfactor?	Het PvE bevat een uitgebreide set eisen die voortkomt uit de aard, complexiteit en het risicoprofiel van de gevraagde SOC/MDR-dienstverlening voor vitale publieke organisaties. De Aanbestedende Dienst is niet bereid eisen om te zetten naar wensen; de eisen worden gehandhaafd. Mogelijke verbeteringen of aanpassingen kunnen via de vragenrondes in de gunningsfase worden besproken, zolang er geen sprake is van wezenlijke wijzigingen.

106	Bijlage 10 Programma van Eisen	Deze eis beschrijft flexibel gebruik met groei of krimp. Inschrijver dienst voor de contractperiode te investeren in materiaal. Opschalen is mogelijk echter afschalen niet. Dit kan bij krimp resulteren in niet kostendekkende dienstverlener voor Inschrijver. Inschrijver stelt voor dat krimp mogelijk is per verlenging van de contractperiode. Kan aanbestedende dienst beschrijven wat hierin de mogelijkheden zijn?	De Raamovereenkomst kan meegroeien of krimpen naar gebruik; facturatie over verbruik vindt achteraf plaats (PvE E1.14). De wijze waarop afschaling in het verdienmodel wordt verwerkt, wordt transparant in het Prijzenblad onderbouwd. De mogelijkheden voor afschaling worden in de gunningsfase nader uitgewerkt; uitgangspunt is een flexibel, verbruiksgebaseerd model.
107	Bijlage 10 Programma van Eisen	Inschrijver adviseerd niveau 3 te laten vervallen. SOC dienstverlening heeft als doel tijdig in te grijpen op gedetecteerde en bevestigde security incidenten. Niet opvolgen buiten 10x5/12x5 past niet in het doel van een SOC dienst.	Zie het antwoord op vraag 6.
108	Bijlage 10 Programma van Eisen	Inschrijver gaat ervan uit dat met 'ondersteuning' bedoeld wordt dat de security event logging van genoemde partijen als informatiebron gebruikt kan worden in de geboden dienstverlening, is dit correct?	Ja, dat is correct. E5.01 vraagt dat Opdrachtnemer aansluit op de bij de Deelnemer in gebruik zijnde marktconforme security capabilities, zodat de security event logging van die oplossingen als logbron wordt ontsloten en gebruikt in de detectie en monitoring. De genoemde partijen zijn voorbeelden en niet-limitatief. Indien de inschrijver hiervan afwijkt, bijvoorbeeld door een gangbare capability niet of niet standaard te ondersteunen, onderbouwt de inschrijver waarom en welke implicaties dit heeft voor de Deelnemer en de dienstverlening.
109	Bijlage 10 Programma van Eisen	Voor automated response is een verregaande en veilige integratie benodigd tussen de infrastructuur van deelnemer en dienstverlener. Kan aanbestedende dienst deze eis omzetten in een wens?	Zie het antwoord op vraag 95.

110	Bijlage 10 Programma van Eisen	Bij opslag model A is de inzet van centrale SOC tooling (zoals SIEM & SOAR) niet mogelijk aangezien de loginformatie binnen de infrastructuur van deelnemer moet blijven. Dit betekend dat inschrijver gebruik moet maken van de SOC tooling van de deelnemer, inclusief functioneel gebruik en beheer. Dit is mogelijk een diversiteit aan tools van verschillende fabrikanten. Inschrijver kan niet de benodigde kennis borgen om hiermee een kwalitatieve dienst te bieden. Kan aanbestedend dienst deze eis laten vervallen?	De eis vervalt niet, en de premisse dat Model A centrale SOC-tooling onmogelijk maakt, delen wij niet. Onder Model A blijft de log- en eventdata binnen de eigen omgeving van de Deelnemer of binnen het door de Deelnemer gebruikte ecosysteem. De Opdrachtnemer hoeft daarvoor niet de diverse tooling van de Deelnemer te gebruiken; hij sluit zijn eigen detectie-, correlatie- en responsinrichting aan op die omgeving. Het is de opgave van de Opdrachtnemer de dienst kwalitatief in te richten voor zowel Sentinel- als niet-Sentinel-situaties en in de aanbieding te beschrijven hoe hij dit doet en welke consequenties dit heeft voor inrichting en kosten.
111	Bijlage 10 Programma van Eisen	Is het mogelijk dit aan te passen naar een wens voor optionele dienst?	Nee. De eisen E7.01, E7.06, E7.07 en E7.08 worden niet omgezet naar een optionele wens. Dreigingsinformatie is een integraal onderdeel van de managed SOC/MDR-dienstverlening: zonder het opnemen en verwerken van dreigingsinformatie (E7.01), continue monitoring van interne en externe bronnen (E7.06), informatiedelingsafspraken (E7.07) en gestandaardiseerde uitwisseling via STIX, TAXII en MISP (E7.08) kan de detectie niet aansluiten op het actuele dreigingsbeeld. De ondersteuning van deze protocollen is bovendien nodig voor de aansluiting op het Nationaal Detectie Netwerk van het NCSC. De gevraagde flexibiliteit zit al in de eisen als afbakening per Deelnemer en niet als optionaliteit: Z-CERT geldt uitsluitend voor Deelnemers met zorggerelateerde processen (E7.06), en een extern beheerde MISP-omgeving via STIX/TAXII of de MISP REST API kwalificeert als gelijkwaardige invulling van E7.08. De capability blijft verplicht; de concrete invulling, waaronder de partnerships en de wijze van uitwisseling, varieert per Deelnemer en wordt waar relevant als gunningscriterium meegewogen.
112	Bijlage 10 Programma van Eisen	Is het mogelijk dit aan te passen naar een wens voor optionele dienst?	E7.04 (threat hunting) blijft een eis en wordt niet omgezet naar een optionele wens; threat hunting is een integraal onderdeel van de managed dienstverlening. De wijze van invulling, waaronder frequentie en rapportage, wordt als gunningscriterium meegewogen (zie ook vraag 5).

113	Bijlage 10 Programma van Eisen	Inschrijver acht het implementeren en bijhouden van use-cases als intergaal onderdeel van de dienstverlening. Het aantal use cases met bijbehorende complexiteit en tijdsinspanning is door inschrijver vooraf onvoldoende accuraat in te schatten. Inschrijver verzoekt deze eis aan te passen dat wijzigingen van use cases als 'niet standaard wijziging' kunnen worden doorbelast. Dit voorkomt dat deelnemers onnodig hoge kosten krijgen door risico opslagen voor onvoorzienne werkzaamheden. Onbeperkte use cases is voor inschrijver niet werkbaar gezien het risico op niet kostendekkende dienstverlening.	De eis blijft niet onbeperkt. Het aantal kosteloos te ontwikkelen use cases wordt begrensd en voorspelbaar gemaakt: een standaard pakket van de Opdrachtnemer (E7.09), aangevuld met maximaal 20 sectorspecifieke use cases die de deelnemersgroep collectief en per kwartaal aandraagt en met de Opdrachtnemer afstemt, plus de uit de toepasselijke kaders voortvloeiende use cases (E7.12). Het maximum van 20 is leidend en wordt alleen met goedkeuring van de Opdrachtnemer overschreden. Doordat het volume collectief is begrensd en in een vast kwartaalritme wordt afgestemd, is de inspanning voor de Opdrachtnemer vooraf in te schatten en vervalt het risico op niet-kostendekkende dienstverlening dat aan een onbeperkt model kleeft. Een separate doorbelasting van use-case-wijzigingen als niet-standaard wijziging is binnen dit begrensde model niet aan de orde. De eisen E7.10 en E7.11 worden op dit model aangepast.
114	Bijlage 10 Programma van Eisen	Inschrijver is voornemens te gaan voldoen aan de nieuwe ABRO beveiligingseisen. Voor de uitvoering van de dienstverlening wordt deels gebruik gemaakt van een externe partij welke voldoet aan alle gangbare informatiebeveiligingseisen. Inschrijver kan echter niet garanderen dat deze partij kan voldoen aan specifieke ABRO eisen. Inschrijver gaat ervan uit dat de relevante beveiligingseisen per nadere overeenkomst overeengekomen kunnen worden. kan aanbestedende dienst dit bevestigen?	PvE E8.04 (ABRO) bepaalt dat de dienstverlening geheel of gedeeltelijk onder de ABRO kan vallen. De relevante ABRO-beveiligingseisen worden per Deelnemer bij de totstandkoming van de Nadere Overeenkomst bepaald. Bevestigd dat de concrete ABRO-vereisten per Nadere Overeenkomst kunnen worden overeengekomen, voor zover de ABRO op die specifieke Deelnemer van toepassing is.
115	Programma van Eisen	Er worden drie verschillende service niveaus gevraagd. Welke verdeling van service niveaus verwacht opdrachgever van de deelnemende veiligheidsregio's?	De Aanbestedende Dienst schrijft geen vaste verdeling van serviceniveaus voor; de keuze is per Deelnemer risicogebaseerd en wordt vastgelegd in de Nadere Overeenkomst (E3.03). Qua scope is de verwachting dat deelnemers doorgaans een mix afnemen van de basis (managed EDR), NDR en additionele SIEM-logbronnen, in wisselende samenstelling.

116	Algemeen	Is het mogelijk om tijdens een later moment deze eerste fase juridische vragen toe te voegen om te stellen?	Het stellen van vragen is uitsluitend mogelijk via de in §3.5 Selectiedocument voorziene vragenronde, met uiterste indieningsdatum 15 juni 2026 via TenderNed. Vragen die na deze termijn worden ontvangen, worden niet in behandeling genomen. Een aanvullende vragenronde in de selectiefase is niet voorzien; wel zijn er twee vragenrondes in de gunningsfase.
117	6.4	Bij Kerncompetentie 2 wordt gevraagd naar ervaring met het leveren van IT-dienstverlening. De uitvraag betreft SOC/MDR diensten. Als cyber security dienstverlener leveren wij deze uitgevraagde dienstverlening, echter wij zijn geen IT-dienstverlener. Bent u akkoord dat IT dienstverlening gelezen wordt als MDR dienstverlening?	Kerncompetentie 2 ziet bewust op bredere IT-dienstverlening met de BIO als normenkader, niet uitsluitend op SOC/MDR. SOC/MDR-dienstverlening die met de BIO als normenkader is geleverd kwalificeert eveneens voor Kerncompetentie 2, mits aan alle overige criteria (€ 200.000, minimaal 3 jaar) is voldaan.
118	6.4	Bij Kerncompetentie 2 wordt gevraagd naar ervaring met het leveren van IT-dienstverlening met de BIO als normenkader. Onze ervaring leert dat het aantonen van het ISO-27001 certificaat voldoende wordt geacht. Is dat bij deze ook akkoord?	Zie 102
119	7.2	Kunt u toelichten wat u met complexe omgevingen bedoeld?	Met "complexe omgevingen" worden omgevingen bedoeld die zich kenmerken door bijvoorbeeld een groot of divers aantal logbronnen, een heterogeen IT-landschap, meerdere organisatieonderdelen of domeinen, koppelingen met externe partijen, en verhoogde beschikbaarheids- en beveiligingseisen, zoals bij organisaties met vitale of maatschappelijk kritische processen.
120	7.3	Kunt u toelichten wat u met capabilities bedoeld?	Met 'capabilities' in Selectiecriterium 2 wordt bedoeld de bestaande beveiligingscapaciteiten en -functionaliteiten waarover een omgeving al beschikt, zoals de bij de Deelnemers aanwezige Microsoft-beveiligingsfunctionaliteit (vgl. PvE E5.01, E5.07). Selectiecriterium 2 vraagt naar de visie op de verhouding tussen het benutten van deze bestaande capabilities als uitgangspunt en het inzetten van aanvullende tooling.

121	3.12	Bepaalde gevraagde certificaten/polissen bewijsstukken zijn in het Engels. Is het akkoord dat deze stukken in het Engels aangeleverd worden?	Op grond van §3.12 Selectiedocument dienen alle correspondentie en in te dienen stukken in de Nederlandse taal te worden opgesteld, dan wel voorzien te worden van een Nederlandse vertaling (vgl. PvE E2.12/E2.13 voor de operationele dienstverlening). Stukken in een andere taal zonder Nederlandse vertaling worden niet in aanmerking genomen. Voor internationaal gestandaardiseerde certificaten en polisbladen (bijvoorbeeld ISO-certificaten, verzekeringspolissen) volstaat aanlevering in de taal van uitgifte, mits de relevante informatie voor de Aanbestedende Dienst voldoende begrijpelijk is; bij twijfel kan een vertaling worden gevraagd.
122	E1.13	Kunt u toelichten hoe leveranciers rekening kunnen houden met het ontbreken van een afnamegarantie, terwijl wel vooraf investeringen in capaciteit en infrastructuur nodig zijn? Is het mogelijk om meer transparantie te geven in de verwachte volumes of een minimale afname?	De Raamovereenkomst kent geen afname- of omzetgarantie; alle in de aanbestedingsstukken genoemde bedragen en aantallen zijn indicatief en Opdrachtnemer kan hieraan geen rechten ontlenen (PvE E1.13). Het verdienmodel is verbruiksgebaseerd (PvE E1.14); voor zover mogelijk worden indicatieve volumes in de gunningsfase verstrekt. Een minimale afname per Deelnemer wordt niet voorgeschreven.
123	E1.11	Hoe wordt omgegaan met situaties waarin de complexiteit van de dienstverlening hoger blijkt dan vooraf ingeschat, gezien het all-in prijsmodel? Is er ruimte om tijdens de looptijd bij te sturen bij aantoonbare afwijkingen?	De aangeboden tarieven zijn all-in conform PvE E1.11. Het verdienmodel is verbruiksgebaseerd: de dienstverlening kan meegroeien of krimpen naar gebruik, en bij wijzigingen in de omvang wordt het verbruik navenant aangepast. Een eenzijdige tariefsverhoging wegens achteraf hoger ingeschatte complexiteit binnen ongewijzigde scope is niet voorzien; Inschrijver baseert zijn tarieven op een realistische inschatting.

124	E3.03	Wat is de reden dat alle drie serviceniveaus verplicht moeten worden aangeboden, terwijl deelnemers er uiteindelijk één kiezen? Zou het mogelijk zijn deze verplichting te beperken, zodat de inzet beter aansluit bij de daadwerkelijke vraag (proportionaliteit)?	Alle drie serviceniveaus worden aangeboden zodat elke Deelnemer, op basis van eigen risicomanagement binnen het federatieve stelsel, het passende niveau kan kiezen en gedurende de looptijd zo nodig kan wisselen. Eén raamovereenkomst bedient meerdere deelnemers met uiteenlopende behoeften; daarom moet het volledige palet beschikbaar zijn. De verplichting wordt niet beperkt: een Deelnemer kiest weliswaar één niveau, maar de beschikbaarheid van alle drie is nodig om de keuzevrijheid en het federatieve karakter te borgen.
125		Kunt u verduidelijken in hoeverre verschillen tussen deelnemers (zoals volwassenheid en IT-omgeving) vooraf worden gestandaardiseerd? Hoe wordt hier transparantie over geboden richting opdrachtnemer om de impact op de uitvoering goed te kunnen inschatten?	Verschillen tussen deelnemers (volwassenheid, IT-omgeving) worden niet vooraf volledig gestandaardiseerd; elke Deelnemer brengt de eigen omgeving in. De impact wordt per Deelnemer inzichtelijk via het onboardingtraject: het ontwerpplan voor logdata (E4.06), de inleer- en baseliningperiode (E4.10) en de periodieke beoordeling van de logconfiguratie samen met de IT-afdeling (E6.02). In de selectiefase wordt geen gedetailleerde omgevings- of prijsinformatie per Deelnemer verstrekt; indicatieve omvang-informatie voor de prijs- en staffelopbouw volgt in de gunningsfase (zie vraag 48).
126	E6.04	Wat is de gedachte achter het ondersteunen van meerdere datamodellen binnen dezelfde dienstverlening? Kunt u meer transparantie geven in de verwachte toepassing hiervan (bijvoorbeeld verdeling of voorkeur)?	De gedachte achter meerdere opslagmodellen is het gedifferentieerde speelveld van de Deelnemers: een deel beschikt over een eigen geschikte omgeving (bijvoorbeeld E5/Sentinel), een deel niet (bijvoorbeeld E3 zonder Sentinel). Eén model zou een van beide groepen dwingen tot aanpassing van de eigen licentie- of opslagstructuur, wat niet wordt verlangd. De Aanbestedende Dienst schrijft geen vaste verdeling of voorkeur voor; de keuze ligt per Deelnemer. Microsoft Sentinel is in E6.04 als voorbeeld genoemd en niet als enige optie; ook een equivalente omgeving kan Model A zijn.

127	E2.04, E2.12	Kunt u toelichten voor welke rollen de combinatie van certificeringen en Nederlandse taalvaardigheid noodzakelijk is? Is het mogelijk hier onderscheid in te maken per rol, zodat de inzet van resources proportioneel blijft?	De eisen maken al onderscheid per rol. De SOC-relevante certificering (E2.04) geldt voor alle SOC-teamleden die op de dienstverlening worden ingezet. De Nederlandse taalvaardigheid op B2-niveau (E2.12) geldt uitsluitend voor klant-facing rollen: servicedesk, Service Delivery Manager, SOC-analisten die rechtstreeks met de Deelnemer schakelen, en andere medewerkers met direct klantcontact. SOC-analisten (L1/L2) zonder rechtstreeks klantcontact vallen niet onder de Nederlandse-taaleis; de combinatie is dus alleen vereist voor klant-facing analisten.
128		Hoe wordt de onboardinginspanning per deelnemer ingeschat, gezien de verschillende uitgangssituaties? Is er meer transparantie mogelijk in hoe deze verschillen worden meegenomen in het prijsmodel?	Zie het antwoord op vraag 125.
129	E1.08	Kunt u toelichten hoe wordt omgegaan met situaties waarin incidenten mede worden veroorzaakt door de inrichting of keuzes van de deelnemer? Hoe wordt hierbij geborgd dat verantwoordelijkheden en risico's proportioneel blijven?	De verantwoordelijkheidsverdeling bij incidenten die mede voortvloeien uit keuzes van de Deelnemer wordt vastgelegd in de Deelovereenkomst en het DAP (vgl. PvE E3.04). De nadere aansprakelijkheidsregeling volgt in de overeenkomst in de gunningsfase.
130	E7.15	Kunt u toelichten hoe de gestelde responstijden zich verhouden tot gangbare marktstandaarden voor SOC/MDR-dienstverlening? In hoeverre acht u deze eisen realistisch en proportioneel, met name in complexe situaties zoals een hack door een geavanceerde APT?	E7.15 betreft de time-to-notify: de tijd tussen het automatisch gegenereerde alarm en de melding van een (mogelijk) incident, niet de tijd voor volledige triage, analyse, mitigatieadvies of containment (geen MTTR). Naar aanleiding van de marktreacties is de P1 time-to-notify verruimd van 10 naar 15 minuten. Dit ligt binnen de gangbare marktrange voor detection-to-alert en escalatie van circa 13 tot 20 minuten voor kritieke incidenten en is haalbaar in een 24/7 SOC met geautomatiseerde detectie en alarmering, mede gelet op de SLO van 95% per maand. De tijden voor P2 (30 minuten) en P3 (4 uur) blijven ongewijzigd. De diepgaande analyse en respons bij complexe aanvallen, zoals een APT, kennen een eigen, langer tijdsbeloop en vallen onder de respons- en rapportageafspraken (E7.16, E7.17 en het DAP), niet onder de time-to-notify.

131	E3.06	Kunt u nader toelichten hoe de beschikbaarheidseis van 99,7% wordt gemeten en welke afhankelijkheden daarin worden meegenomen (bijvoorbeeld klantomgeving of onderliggende systemen)? Is het mogelijk om hierin meer transparantie te geven over de scope van deze meting?	De 99,7%-beschikbaarheid wordt per maand gemeten over de door Opdrachtnemer geleverde monitoring-, alarmerings-, rapportage- en SOC-portaalfuncties (E3.06). Geplande onderhoudsvensters tellen niet mee als onbeschikbaarheid (E5.06). Componenten in het netwerk van de Deelnemer (collectoren, sensoren, agents) en de bronsystemen waarmee Opdrachtnemer integreert vallen onder de gedeelde verantwoordelijkheid (E5.05) en worden niet eenzijdig aan Opdrachtnemer toegerekend. De concrete meetmethode, het meetinterval en de maandelijkse rapportage worden vastgelegd in het DAP, zodat de beschikbaarheid verifieerbaar is.
132	E5.01	Kunt u verduidelijken welke mate van integratie met bestaande tooling van deelnemers wordt verwacht en hoe breed deze scope is? Hoe wordt voorkomen dat de benodigde ondersteuning onevenredig groot wordt, zodat de inspanning proportioneel blijft?	De verwachte integratie betreft het aansluiten op de bij de Deelnemer in gebruik zijnde marktconforme security capabilities en het ontsluiten van de relevante logbronnen (E5.01). De scope is niet onbegrensd: deze wordt per Deelnemer risicogebaseerd bepaald in het ontwerpplan voor logdata (E4.06) en periodiek samen met de IT-afdeling beoordeeld op relevantie en proportionaliteit (E6.02), en vastgelegd in het DAP (E3.04). De inschrijver beschrijft daarnaast voor welke partijen ondersteuning standaard beschikbaar is en welke binnen redelijke termijn worden geaccommodeerd (E5.01), zodat de inspanning beheersbaar blijft.
133	E5.20	Kunt u toelichten welk volwassenheidsniveau van SOAR-functionaliteit wordt verwacht bij de start van de dienstverlening? Is het mogelijk om meer transparant te maken hoe deze capability zich gedurende de looptijd mag ontwikkelen?	Zie het antwoord op vraag 95.

134	E5.10	Kunt u verduidelijken hoe wordt vastgesteld dat de dienstverlening geen nadelige impact heeft op de prestaties van de omgeving van de deelnemer? Hoe wordt hierin een proportionele balans gevonden tussen detectiekwaliteit en systeemprestaties?	E5.10 stelt de uitkomst: de dienstverlening mag de prestaties van de te monitoren omgeving niet nadelig beïnvloeden. Vaststelling en balans verlopen in overleg met de Deelnemer: tijdens de inleer- en baseliningperiode (E4.10) wordt de impact beoordeeld, de logconfiguratie wordt periodiek samen met de IT-afdeling getoetst op onder meer resourcebeslag (E6.02), en waar mogelijk wordt voortgebouwd op bestaande capabilities om de belasting te beperken (E6.09). De afspraken hierover worden vastgelegd in het DAP; bij geconstateerde nadelige impact wordt de inrichting in overleg bijgesteld.
135	Bijlage 10 Programma van Eisen	Zijn er aanvullende nationale of organisatorische beperkingen op toegang tot systemen/data vanuit andere EU-landen?	Er gelden geen aanvullende nationale of organisatorische beperkingen op toegang vanuit andere EU/EER-landen, anders dan de reeds in de aanbestedingsstukken opgenomen vereisten (o.a. Geschiktheidseis 8: verwerking en opslag uitsluitend binnen EU/EER, PvE E8.01/E8.02). Toegang vanuit buiten de EER is niet toegestaan.
136	Bijlage 10 Programma van Eisen	Geldt de eis dat klantgerichte communicatie minimaal B2 Nederlands vereist is ook voor SOC-analisten (L1/L2), of alleen voor klant-facing rollen zoals SDM?	Zie het antwoord op vraag 127.
137	Bijlage 10 Programma van Eisen	Is Engels toegestaan voor operationele communicatie (bijv. incident coördinatie) buiten escalaties?	Nee, niet als algemene regel. Communicatie met de Deelnemer in klant-facing rollen is in het Nederlands op niveau B2 (E2.12). De uitzondering die E2.12 noemt: voor verdiepende technische escalaties of incidentcoördinatie waarbij specialistische kennis betrokken is en gezamenlijk overleg in het Engels efficiënter is, kan in overleg met de Deelnemer het Engels worden gebruikt. Paragraaf 3.12 van het selectiedocument betreft de aanbestedingsprocedure, niet de operationele dienstverlening.

138	Bijlage 10 Programma van Eisen	kan opdrachtgever bevestigen welke concrete use cases en logbronnen minimaal in scope moeten zijn bij start? Is er een bestaande use-case set (bijv. Sentinel) die moet worden overgenomen?	Er wordt verwacht dat de inschrijver bij aanvang start met een voor de deelnemers passende set use cases en adviseert over logische en passende logbronnen (ontwerpplan logdata, E4.06). Aanvullend worden sectorbreed nuttige use cases voor de deelnemersgroep toegevoegd in de reguliere overleggen (E7.02, E7.05), als onderdeel van de standaard set die Opdrachtnemer doorlopend onderhoudt en uitbreidt (E7.09). Er is geen verplicht over te nemen bestaande set; waar een Deelnemer al use-cases heeft (bijvoorbeeld in Sentinel), worden die in het onboardingtraject beoordeeld en waar passend meegenomen.
139	Bijlage 10 Programma van Eisen	mogen we geboden tarieven wel indexeren conform de CBS index	De wijze van jaarlijkse indexatie of tariefaanpassing wordt in de gunningsfase geregeld in het beschrijvend document en de (concept-)Raamovereenkomst. Deze vraag valt buiten de selectiefase.
140	Bijlage 10 Programma van Eisen	kunt u toelichten hoe de opdrachtgever de facturatie achteraf ziet, per week/maan/kwartaal?	Facturatie over verbruik vindt achteraf plaats per Deelnemer op basis van de afzonderlijke Deelovereenkomst. De facturatiefrequentie en nadere inrichting worden in de gunningsfase via het beschrijvend document en het Prijzenblad vastgelegd.
141	Bijlage 10 Programma van Eisen	kan de opdrachtgever inschatten hoeveel deelnemers er per niveau zijn? Het te verwachten totaal aantal deelnemers.	Zie het antwoord op vraag 115.
142	Bijlage 10 Programma van Eisen	welke doorlooptijd hanteert de opdrachtgever voor de ontwikkeling van de noodzakelijk passende additionele connectoren?	De Aanbestedende Dienst schrijft geen vaste doorlooptijd voor de ontwikkeling van aanvullende connectoren voor. De inschrijver beschrijft in de aanbieding voor welke partijen ondersteuning standaard beschikbaar is en welke binnen redelijke termijn kunnen worden geaccommodeerd (E5.01). De concrete doorlooptijd voor een specifieke aanvullende connector wordt per Deelnemer in onderling overleg bepaald en vastgelegd in het DAP (E3.04).

143	Bijlage 10 Programma van Eisen	Verwacht de opdrachtgever dat er deelnemers of de opdrachtgever zelf migreren van Microsoft of andere niet soevereine omgeving naar een soevereine omgeving binnen de EER?	Er wordt geen migratie van Microsoft of een andere omgeving naar een specifieke soevereine omgeving verwacht of vereist. De eis is dat het SOC, de gebruikte software en de data binnen de EER blijven (E8.01, E8.02); de bestaande, sterk Microsoft-georiënteerde omgevingen van de deelnemers blijven het uitgangspunt (E5.07, E5.16). Eventuele toekomstige keuzes rond datasoevereiniteit zijn aan de individuele Deelnemer.
144	Bijlage 10 Programma van Eisen	is het wenselijk om alle data van deelnemers in één datalake / analitics workspace te laten samenkomen voor analyse of moet er per deelnemer een eigen omgeving zijn?	Data van verschillende Deelnemers moet logisch gescheiden blijven; het ongescheiden samenbrengen van alle ruwe deelnemersdata in één gedeelde datalake of workspace is niet toegestaan. Elke Deelnemer is een eigen verwerkingsverantwoordelijke, met per Deelnemer gescheiden en doelgebonden toegang en verwerking (E8.07, E8.28). Een multi-tenant platform met strikte logische scheiding per Deelnemer is toegestaan, mits het gekozen opslagmodel (E6.04) en de datalocatie-eisen (E8.01, E8.02) worden gerespecteerd. Sectorbrede analyse vindt plaats via gedeelde dreigingsinformatie en geaggregeerde of geanonimiseerde inzichten (E7.06, E9.03), niet via het ongescheiden samenbrengen van ruwe data.
145	Bijlage 10 Programma van Eisen	voorziet Deelnemer of Opdrachtgever in een een gestandaardiseerde (TAXII / STIX) feed de dreigingsinformatie bronnen naar het platform van de Opdrachtnemer?	De Deelnemer voorziet in de toegang (feed-login) tot de betreffende dreigingsinformatiebronnen. De Opdrachtnemer moet in staat zijn de geboden oplossing daarop technisch te koppelen op basis van de standaarden STIX en TAXII (E7.08), en sluit daarnaast aan op de in E7.06 genoemde bronnen via de eigen partnerships en informatiedelingsafspraken (E7.07).

146	Bijlage 10 Programma van Eisen	Komt er van de Opdrachtgever of Deelnemers ook dreigingsinformatie met betrekking tot het externe landschap zoals bv misconfiguratie van web-sites, ge compromiteerde accounts op het dark-web enz?	De Opdrachtgever en Deelnemers leveren deze externe dreigingsinformatie niet aan als invoer. E7.06 vereist wel dat Opdrachtnemer interne en externe dreigingsinformatie continu monitort op relevantie voor de Deelnemer, met als minimale bronnen de in E7.06 genoemde (zoals NCSC, sectorale trust-netwerken en Z-CERT). Specifieke monitoring van het externe aanvalsoppervlak, zoals dark-web-monitoring, gecompromitteerde accounts, blootgestelde assets en kwetsbare internet-facing systemen, behoort niet tot de minimale basisscope; voor zover Opdrachtnemer dit binnen de eigen dienstverlening biedt wordt het benut, en het kan als aanvullende of optionele uitbreiding worden afgenomen.
147	Bijlage 10 Programma van Eisen	Verzoek om de time-to-notify voor de Critical (P1) events aan te passen naar 15 minuten.	De Aanbestedende Dienst neemt dit verzoek over. De time-to-notify voor Critical (P1) meldingen wordt verruimd van 10 naar 15 minuten. Daarmee blijft de norm binnen de gangbare marktrange voor detection-to-alert en escalatie (circa 13 tot 20 minuten) en blijft een haalbare en afdwingbare SLA gewaarborgd. De tijden voor High (P2: 30 minuten) en Medium (P3: 4 uur) blijven ongewijzigd. De time-to-notify betreft uitsluitend de melding van een (mogelijk) incident, niet de volledige triage, analyse of respons. E7.15 wordt hierop aangepast.
148	Bijlage 10 Programma van Eisen	de Opdrachtgever draagt zorg voor de uitwisseling van de alarmen met de Deelnemer?	Nee. De Opdrachtnemer draagt zorg voor de melding en alarmering richting de betreffende Deelnemer, rechtstreeks (E7.15, E7.20) en via het SOC-portaal (E7.21). De Aanbestedende Dienst (NIPV) is de centrale contractpartij en bemiddelt niet in de operationele uitwisseling van alarmen; die loopt tussen Opdrachtnemer en de Deelnemer, op basis van de in het DAP vastgelegde afspraken. Ter nuance: NIPV vervult een dubbele rol, als Aanbestedende Dienst en als Deelnemer; waar NIPV als Deelnemer optreedt, verloopt de uitwisseling van alarmen op gelijke wijze als bij de overige deelnemers.

149	Bijlage 10 Programma van Eisen	is het ook wenselijk dat de door Opdrachtnemer gebruikte tooling is ontwikkeld binnen de EER?	Nee, ontwikkeling binnen de EER is geen eis. Het beheer en de uitvoering van de dienst, waaronder het SOC, de softwareomgeving en de dataopslag, vinden wel binnen de EER plaats (E8.01, E8.02). De plaats waar de gebruikte tooling is ontwikkeld is geen voorwaarde; de herkomst van de oplossing wordt wel meegewogen in het kader van geschiktheidseis 8 en E2.01 (geen relatie met offensieve statelijke actoren).
150	Selectiedocument SOC-MDR Versie 1.0, §2.1 Deelnemers	Kan de opdrachtgever een indicatie geven van het verwachte aantal deelnemers per aansluitmoment, inclusief de verwachte verdeling tussen deelnemers die uitsluitend M-EDR afnemen en deelnemers die daarnaast SIEM en/of NDR zullen afnemen?	De deelnemers en de aansluitplanning zijn beschreven in paragraaf 2.1 van het selectiedocument. Een vooraf vastgestelde verdeling tussen deelnemers die uitsluitend M-EDR afnemen en deelnemers die daarnaast SIEM en/of NDR afnemen wordt niet gegeven; de scope is een risicogebaseerde keuze per Deelnemer (Nadere Overeenkomst), waarbij naar verwachting doorgaans een mix van managed EDR, NDR en additionele SIEM-logbronnen wordt afgenomen (zie vraag 115). Indicatieve omvang-informatie voor de prijs- en staffelopbouw volgt in de gunningsfase (zie vraag 48).
151	Selectiedocument SOC-MDR Versie 1.0, §2.1 Deelnemers	Wordt gedurende de looptijd van de raamovereenkomst verwacht dat aanvullende veiligheidsregio's, samenwerkingsverbanden of andere publieke organisaties kunnen toetreden tot de overeenkomst?	De Raamovereenkomst biedt de mogelijkheid dat gedurende de looptijd aanvullende veiligheidsregio's, samenwerkingsverbanden of andere publieke organisaties tot de Raamovereenkomst toetreden, voor zover dit aanbestedingsrechtelijk is toegestaan en de Raamovereenkomst hierin voorziet. De concrete bepalingen voor toetreding worden in de gunningsfase uitgewerkt in de (concept-)Raamovereenkomst.
152	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Kan opdrachtgever bevestigen welke concrete use-cases en logbronnen minimaal operationeel moeten zijn bij de initiële ingebruikname van de dienstverlening?	Zie het antwoord op vraag 138.

153	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Is er een bestaande set detectieregels, use-cases of content (bijvoorbeeld Microsoft Sentinel use-cases) aanwezig die door de opdrachtnemer dient te worden overgenomen of gemigreerd?	Zie het antwoord op vraag 138.
154	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Welke doorlooptijd acht opdrachtgever acceptabel voor het ontwikkelen, testen en implementeren van additionele connectoren die noodzakelijk blijken voor een deelnemer?	Zie het antwoord op vraag 142.
155	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Verwacht opdrachtgever dat deelnemers gedurende de looptijd migreren van Microsoft- of andere niet-soevereine omgevingen naar een soevereine omgeving binnen de Europese Economische Ruimte?	Zie het antwoord op vraag 143.

156	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Is het wenselijk dat securitydata van alle deelnemers wordt samengebracht in één centrale analytics workspace/datalake ten behoeve van sectorbrede analyse, of verwacht opdrachtgever een volledig gescheiden omgeving per deelnemer?	Zie het antwoord op vraag 144.
157	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Voorziet opdrachtgever of één van de deelnemers in gestandaardiseerde dreigingsinformatiefeeds (bijvoorbeeld STIX/TAXII) die beschikbaar worden gesteld aan de opdrachtnemer?	Zie het antwoord op vraag 145.
158	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Wordt verwacht dat de opdrachtnemer dreigingsinformatie levert over het externe landschap, zoals gecompromitteerde accounts, dark-web monitoring, blootgestelde assets en kwetsbare internet-facing systemen?	Zie het antwoord op vraag 146.

159	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Kan opdrachtgever verduidelijken of de uitwisseling van alarmen en meldingen richting de deelnemers centraal wordt gefaciliteerd door opdrachtgever of dat dit onderdeel is van de dienstverlening van opdrachtnemer?	Zie het antwoord op vraag 148.
160	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Zijn er aanvullende nationale of organisatorische beperkingen ten aanzien van toegang tot systemen en data vanuit andere lidstaten binnen de Europese Economische Ruimte?	Zie ook vraag 135. Er gelden geen aanvullende nationale of organisatorische beperkingen op toegang vanuit andere EU/EER-lidstaten, anders dan de in de aanbestedingsstukken opgenomen vereisten (EU/EER-verwerking, EER-locatie SOC, PvE E8.01/E8.02). Toegang vanuit buiten de EER is niet toegestaan.
161	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht	Is het wenselijk of vereist dat de door opdrachtnemer gebruikte security tooling zelf eveneens binnen de Europese Economische Ruimte is ontwikkeld en/of wordt beheerd?	Zie het antwoord op vraag 149.

162	Selectiedocument SOC-MDR Versie 1.0, §3.10 Toepasselijk recht en geschillenbeslechting / toekomstige overeenkomst	Kan opdrachtgever bevestigen dat tarieven gedurende de looptijd van de overeenkomst jaarlijks mogen worden geïndexeerd conform een objectieve CBS-index?	De wijze van jaarlijkse indexatie of tariefaanpassing wordt in de gunningsfase geregeld in het beschrijvend document en de (concept-)Raamovereenkomst. Deze vraag valt buiten de selectiefase.
163	Selectiedocument SOC-MDR Versie 1.0, §2.6 Doel aanbestedingsprocedure / toekomstige overeenkomst	Kan opdrachtgever toelichten hoe de facturatie wordt ingericht (per deelnemer of centraal) en welke facturatiefrequentie wordt gehanteerd (maandelijks, per kwartaal of anders)?	Facturatie over verbruik vindt achteraf plaats per Deelnemer op basis van de afzonderlijke Deelovereenkomst. De facturatiefrequentie en nadere inrichting worden in de gunningsfase via het beschrijvend document en het Prijzenblad vastgelegd.

164	Selectiedocument SOC-MDR Versie 1.0, §2.2 Voorwerp (scope) van de opdracht / SLA	Verzoek om de vereiste notificatietijd voor Critical (P1) meldingen vast te stellen op 15 minuten na detectie, passend bij operationele MDR-dienstverlening.	Zie het antwoord op vraag 147. De P1 time-to-notify wordt vastgesteld op 15 minuten, gemeten vanaf het (automatisch) genereren van het alarm conform de definitie in E7.15.
165	§Selectiedocument SOC-MDR Versie 1.0, 3.12 Taal	Geldt de eis dat klantgerichte communicatie minimaal op B2-niveau Nederlands dient plaats te vinden uitsluitend voor klantgerichte rollen (zoals Service Delivery Managers) of ook voor operationele SOC-rollen zoals L1- en L2-analisten?	Zie het antwoord op vraag 127.
166	Selectiedocument SOC-MDR Versie 1.0, §3.12 Taal	Is Engels toegestaan voor operationele communicatie, bijvoorbeeld tijdens incidentcoördinatie en technische afstemming, buiten formele escalaties richting deelnemers?	Zie het antwoord op vraag 137.

167	Selectiedocument - Paragraaf 2.2.	In het Selectiedocument wordt security analyse gepositioneerd als een optionele dienst. In de visie van de aanbestedende dienst is security analyse een integraal en onlosmakelijk onderdeel vormt van een volwaardige SOC-dienstverlening. Kunt u verduidelijken wat u precies verstaat onder de term "security analyse" en hoe deze dienst zich verhoudt tot de verplichte scope van de SOC-dienstverlening?	De operationele security-analyse die nodig is om alarmen te duiden, te onderzoeken en als (mogelijk) incident te classificeren, behoort tot de verplichte basisscope van de managed dienstverlening; analyse van detecties is inherent aan MDR (zie onder meer E7.13, E7.16 en E7.17). Voor zover het selectiedocument een dienst als optioneel positioneert, betreft dit een aanvullende of verdiepende vorm van security-analyse die bovenop de verplichte detectie, triage, analyse en respons kan worden afgenomen, niet de basisanalyse zelf.
168	Selectiedocument - Paragraaf 2.2.	In het Selectiedocument wordt Threat Intelligence gepresenteerd als een optionele dienst, terwijl de visie op Threat Intelligence tegelijkertijd één van de drie selectiecriteria vormt. Deze twee elementen lijken op het eerste gezicht tegenstrijdig. Kunt u de achterliggende rationale van deze benadering nader toe te lichten?	Er is geen tegenstrijdigheid. Threat Intelligence is als afzonderlijk afneembare optionele dienst benoemd (§2.2), terwijl de basisdienstverlening al het structureel monitoren en benutten van dreigingsinformatie omvat (PvE E7.06). Selectiecriterium 2 beoordeelt de organisatiebrede visie op de rol van CTI binnen MDR-dienstverlening en staat los van de vraag of een Deelnemer de afzonderlijke optionele dienst 'Threat Intelligence' afneemt.
169	Bijlage 10 - Programma van Eisen	Inschrijver neemt aan dat de kosten voor data-ingestie in de SIEM, data-opslag en licenties niet worden meegerekend in de definitie van de 'all-in' terieven, is dat correct?	E1.11 bepaalt dat de aangeboden tarieven all-in zijn voor de daarin genoemde kostencomponenten (waaronder salariskosten, overheadkosten en kosten voor gebruik van apparatuur/software/hardware). De aanname dat data-ingestie, data-opslag en licentiekosten hierbuiten vallen, wordt in deze fase niet bevestigd. De Aanbestedende Dienst bepaalt zelf welke kostencomponenten via het basistarief en welke via afzonderlijke posten worden uitgevraagd, en legt dit vast in het door Inschrijver in te vullen Prijzenblad, dat in de gunningsfase wordt verstrekt
170	Bijlage 10 - Programma van Eisen	In het geval van Microsoft worden de licentiekosten en de kosten voor data-ingestie en -opslag door de Deelnemer rechtstreeks aan Microsoft voldaan. Indien deze kosten dienen te worden opgenomen in het basistarief van de dienstverlening, dient de kostenberekening te worden gebaseerd op de kortingen die individuele Deelnemers bij Microsoft hebben bedongen. Dit betekent dat deze kortingen met de	Voor zover licentie- en data-ingestie-/opslagkosten rechtstreeks door de Deelnemer aan een derde (zoals Microsoft) worden voldaan, vallen deze buiten het door Opdrachtnemer aan te bieden tarief. De wijze waarop deze kosten transparant worden gemaakt, wordt in de gunningsfase via het Prijzenblad uitgewerkt. Het delen van door individuele Deelnemers bedongen kortingen is geen vereiste.

		opdrachtnemer gedeeld moeten worden. Kunt u bevestigen of de Aanbestedende Dienst met deze werkwijze akkoord gaat?	
171	Bijlage 10 - Programma van Eisen	Kunt u verduidelijken of communicatie in het Engels is toegestaan wanneer een Security Analyst een Deelnemer notificeert over een incident of responsacties met een Deelnemer bespreekt?	Zie het antwoord op vraag 137.
172	Bijlage 10 - Programma van Eisen	Kunt u te bevestigen of ondersteuning in het Engels buiten kantooruren is toegestaan?	Zie het antwoord op vraag 137.
173	Bijlage 10 - Programma van Eisen	Wij constateren dat de beschreven serviceniveaus 2 en 3 buiten kantooruren voorzien in respectievelijk een piketregeling en geen actieve monitoring. Vanuit ons dienstverleningsmodel hanteren wij als uitgangspunt dat effectieve SOC-dienstverlening te allen tijde een continue, actieve bewaking vereist, waarbij direct gekwalificeerd personeel beschikbaar is voor detectie en respons. Een piketregeling of het volledig ontbreken van actieve monitoring buiten kantooruren achten wij, gezien de huidige dreigingslandschap waarin cyberaanvallen veelvuldig buiten kantooruren plaatsvinden, ontoereikend voor vitale organisaties. Wij bieden daarom uitsluitend Niveau 1 (24x7 eyes-on-screen) aan als verantwoord serviceniveau. Kan de Aanbestedende Dienst bevestigen of inschrijving met uitsluitend Niveau 1 is toegestaan, dan wel of deelname aan de aanbesteding zonder invulling van Niveau 2 en Niveau 3 mogelijk is?	Zie het antwoord op vraag 6.

174	Bijlage 10 - Programma van Eisen	Sommige van de in E5.20 genoemde geautomatiseerde acties, zoals bijvoorbeeld het aanmaken van tickets, maken deel uit van de generieke functionaliteit van ons platform en zijn van toepassing op alle klanten. De klantspecifieke SOAR-acties, zoals account- en hostisolatie, IP-blokkades of vergelijkbare responsacties, vinden daarentegen altijd plaats binnen vooraf in playbooks vastgelegde scenario's en autorisatiegrenzen. Kunt u bevestigen of de Aanbestedende Dienst zich met deze werkwijze kan verenigen?	Zie het antwoord op vraag 39.
175	Bijlage 10 - Programma van Eisen	Binnen onze SOC-dienstverlening wordt er geen klantdata opgeslagen in onze systemen. Endpoint-data en overige Deelnemerdata blijven opgeslagen binnen de tenant van de betreffende Deelnemer (bijvoorbeeld de Defender XDR-tenant). Kunt u bevestigen of de Aanbestedende Dienst zich met deze werkwijze kan verenigen?	Ja, dat kan de Aanbestedende Dienst bevestigen. Een werkwijze waarbij geen klantdata in de eigen systemen van de Opdrachtnemer wordt opgeslagen en de data binnen het door de Deelnemer gebruikte Microsoft/Defender-ecosysteem blijft (bijvoorbeeld Defender XDR of Microsoft Sentinel), is een acceptabele invulling van Model A, variant 2. Deze omgeving hoeft niet de eigen tenant van de Deelnemer te zijn, mits de data binnen dat ecosysteem blijft. De Deelnemer mag niet worden verplicht zijn eigen licentiestructuur aan te passen. Het is de opgave van de Opdrachtnemer de oplossing passend te maken voor zowel bestaande E5/Sentinel-omgevingen als bestaande E3-omgevingen zonder Sentinel, en in de aanbieding te beschrijven hoe hij dit doet en welke consequenties dit heeft voor inrichting en kosten. De in E5.23 bedoelde opslag "bij de dienstverlener binnen de EER" wordt functioneel uitgelegd: de data bevindt zich binnen de EER, binnen de omgeving waarin Model A is ingericht, en is toegankelijk voor de Opdrachtnemer; een fysieke kopie naar een eigen, niet tot dat ecosysteem behorend platform is onder Model A niet vereist.

176	Bijlage 10 - Programma van Eisen	Kunt u de achterliggende rationale van het verplicht stellen van Model B als opslagmodel nader toe te lichten?	Model B wordt niet als voorkeur of standaard verplicht gesteld. Verplicht is dat de Opdrachtnemer beide opslagmodellen kan faciliteren, zodat elke Deelnemer kan kiezen wat bij de eigen omgeving past. Model A is er voor Deelnemers die hun data binnen de eigen omgeving of het door hen gebruikte ecosysteem willen houden (Microsoft Sentinel is daarvan een voorbeeld, niet de enige optie); Model B voor Deelnemers die hun data in een eigen, niet tot dat domein behorende omgeving van de Opdrachtnemer willen of moeten laten opslaan. Bepalend voor het onderscheid is dus welke omgeving wordt gebruikt, niet wie de licentie of het beheer heeft. De keuze ligt per Deelnemer.
177	Bijlage 10 - Programma van Eisen	Kan de Aanbestedende Dienst bevestigen of de kosteloze levering zoals benoemd in E7.10 zonder beperking op het aantal use cases uitsluitend betrekking heeft op de standaard use cases zoals bedoeld in E7.09, of eveneens op custom use cases en detecties die specifiek voor een Deelnemer worden ontwikkeld en uitsluitend binnen diens omgeving worden toegepast?	De kosteloze levering ziet niet op een onbeperkt aantal use cases. Kosteloos en inbegrepen in het basistarief zijn: het standaard pakket (E7.09), de collectief afgestemde sectorspecifieke set van maximaal 20 use cases, de uit de voor Deelnemer toepasselijke kaders voortvloeiende use cases (E7.12) en de actieve ondersteuning bij het opstellen daarvan (E7.11). Er is geen separaat, onbeperkt traject voor uitsluitend voor één Deelnemer ontwikkelde custom use cases; sectorspecifieke en organisatiespecifieke behoeften lopen via het collectieve kwartaalproces en worden, eenmaal afgestemd, voor de deelnemersgroep uitgerold. Het maximum van 20 sectorspecifieke use cases is leidend en wordt alleen met goedkeuring van de Opdrachtnemer overschreden.
178	Bijlage 10 - Programma van Eisen	Eis E7.11 stelt dat ondersteuning bij het opstellen van organisatiespecifieke use cases is opgenomen in de pricing. Wij constateren dat de behoefte hieraan per Deelnemer sterk verschilt, terwijl de kosten voor alle Deelnemers worden doorberekend. Kan de Aanbestedende Dienst bevestigen of het is toegestaan deze ondersteuning als optionele dienst op te nemen in het Prijzenblad, in plaats van als verplicht onderdeel van het basistarief?	Nee. De ondersteuning bij het opstellen van use cases blijft onderdeel van het basistarief en wordt niet als optionele, per Deelnemer af te nemen dienst in het Prijzenblad opgenomen. Het use-case-beheer is collectief georganiseerd, niet per Deelnemer, en wordt daarom niet per Deelnemer onderhandeld of afgerekend. De zorg over een per Deelnemer sterk wisselende behoefte wordt ondervangen doordat het volume nu collectief is begrensd en voorspelbaar: een standaard pakket plus maximaal 20 sectorspecifieke use cases,

			per kwartaal afgestemd, met overschrijding alleen na goedkeuring van de Opdrachtnemer.
179	Bijlage 10 - Programma van Eisen	De in E7.15 genoemde responstijden lijken, naar ons inzicht, lager te liggen dan wat binnen de markt gangbaar is voor vitale organisaties en crisisomgevingen. Uit breed gedragen inzichten binnen de cybersecuritysector blijkt dat te strak gedefinieerde responstijden kunnen leiden tot een hogere interne werklast (door een groter volume aan generieke, laagkwalitatieve meldingen), kwaliteitsverlies in de dienstverlening en hogere kosten, zonder dat dit een betere beveiliging garandeert. Kunt u bevestigen of de in E7.15 gestelde responstijden zijn gebaseerd op specifieke compliancevereisten of operationele behoeften, dan wel of er ruimte bestaat voor een heroverweging van deze eisen, teneinde een optimale balans te waarborgen tussen servicekwaliteit, uitvoerbaarheid en kostenbeheer?	Er is ruimte voor heroverweging gebleken: de P1 time-to-notify is verruimd van 10 naar 15 minuten, passend bij operationele MDR-dienstverlening en binnen de gangbare marktrange. De tijden voor P2 en P3 blijven ongewijzigd. Zie verder het antwoord op vraag 130.

180	Bijlage 10 - Programma van Eisen	Kunt u een aantal concrete voorbeelden geven van de foutmeldingen waarnaar in eis 7.22 wordt verwezen?	E7.22 ziet op foutmeldingen die in het SOC-portaal en de aansluitvoorzieningen aan beheerders van de Deelnemer worden getoond. Concrete voorbeelden zijn: een logbron of connector die geen data meer aanlevert ("verbinding met logbron X verbroken sinds [tijdstip]"); een mislukte aanmelding of verlopen token bij een gekoppelde bron ("authenticatie bij bron Y mislukt, controleer de feed-login"); een sensor, collector of agent die offline is ("sensor Z onbereikbaar sinds [tijdstip]"); een sterke daling of het stilvallen van het eventvolume van een bron; of een vertraagde of mislukte verwerking in de aanleverpijplijn. Conform E7.22 zijn deze meldingen informatief genoeg om de oorzaak te herleiden of een gerichte vraag te stellen, zonder gevoelige technische details zoals interne paden, stack traces, softwareversies of credentials.
181	Bijlage 11 - voorwaarde deelnemers met voorwaarden	Kunt u verduidelijken of het maximumbedrag van 83.000 euro per jaar inclusief btw all-in is bedoeld, inclusief EDR-licentiekosten, log data ingestion, opslag van logdata en alle diensten die voortvloeien uit de eisen in het Programma van Eisen? Kunt u eveneens een indicatie geven van het totaal aantal te monitoren endpoints en het geschatte volume aan log-ingestie per maand? Dit stelt ons in staat een volledige en kwalitatief verantwoorde afweging te doen of dienstverlening binnen het genoemde maximumbedrag realiseerbaar is.	De budgetplafonds in Bijlage 11 betreffen randvoorwaarden van de betreffende 'Deelnemer met voorwaarden' en geven een indicatie van de maximale jaarlijkse vergoeding inclusief alle gevraagde diensten. Of een plafond al dan niet all-in bedoeld is (inclusief licentiekosten, data-ingestie, opslag etc.) en welke scope van toepassing is, wordt per Deelnemer bij de totstandkoming van de Nadere Overeenkomst nader bepaald. Indicatieve informatie over omvang (endpoints, logvolume) van de betreffende Deelnemers wordt voor zover beschikbaar in de gunningsfase verstrekt.

182	Bijlage 11 - voorwaarde deelnemers met voorwaarden	Uit de vraagstelling onder Index 14 leiden wij af dat de scope in ieder geval managed EDR en SIEM omvat. Kunt u bevestigen of naast EDR en SIEM ook aanvullende XDR-componenten of NDR onderdeel uitmaken van de te onboarden scope? Daarnaast verzoeken wij om een indicatie van het totaal aantal te monitoren endpoints en het geschatte volume aan log-ingestie per maand, zodat wij kunnen beoordelen of de volledige implementatiescope binnen het maximumbedrag van € 15.000,- (ex btw) realiseerbaar is.	De basisscope omvat managed EDR (baseline per Deelnemer), aangevuld met NDR en additionele SIEM-logbronnen. NDR maakt dus deel uit van de mogelijke onboardingscope; XDR is geen afzonderlijke verplichte component, maar past binnen de geïntegreerde, Microsoft-georiënteerde aanpak (E5.07, E5.16). De concrete samenstelling per Deelnemer is een risicogebaseerde keuze. Een indicatie van het aantal endpoints en het log-ingestievolume wordt in de selectiefase niet verstrekt; deze indicatieve omvang-informatie volgt in de gunningsfase (zie vraag 48). Het onder Index 14 in Bijlage 11 genoemde bedrag betreft een aanvullende voorwaarde van de betreffende deelnemer; wat per regio onder de scope valt is in Bijlage 11 globaal omschreven.
183	Bijlage 11 - voorwaarde deelnemers met voorwaarden	Kunt u verduidelijken of het maximumbedrag van 83.000 euro per jaar (ex btw) all-in is bedoeld, inclusief EDR-licentiekosten, log data ingestion, opslag van logdata en alle diensten die voortvloeien uit de eisen in het Programma van Eisen? Kunt u een indicatie van het totaal aantal te monitoren endpoints en het geschatte volume aan log-ingestie per maand, zodat wij kunnen beoordelen of een volledige en kwalitatief verantwoorde dienstverlening binnen het genoemde maximumbedrag realiseerbaar is.	Zie het antwoord op vraag 31.
184	Bijlage 11 - voorwaarde deelnemers met voorwaarden	In Index 18 wordt vermeld dat VRF een maximumbedrag van € 96.000,- (ex btw) per jaar hanteert voor de combinatie van managed EDR en NDR. Kunt u bevestigen of dit maximumbedrag all-in is bedoeld, inclusief de ED-licentiekosten? Daarnaast leiden wij uit de omschrijving af dat een SIEM geen onderdeel uitmaakt van de scope voor VRF. Kunt u dit bevestigen?	Zie het antwoord op vraag 33.

185	Algemeen & Bijlage 11 - voorwaarde deelnemers met voorwaarden	Wij verzoeken de Aanbestedende Dienst te bevestigen of de in Bijlage 11 genoemde budgetindicaties representatief zijn voor de verwachte eenmalige en maandelijkse kosten van de vaste deelnemers. Indien de financiële kaders van de vaste deelnemers hier significant van afwijken, verzoeken wij om nadere indicatieve informatie, teneinde een realistische aanbieding mogelijk te maken.	De in Bijlage 11 genoemde budgetindicaties betreffen de aanvullende voorwaarden van de betreffende deelnemers en zijn niet bedoeld als representatief kader voor de gehele groep vaste deelnemers. De Aanbestedende Dienst verstrekt in de selectiefase geen centrale budget- of kostenkaders; indicatieve omvang-informatie ten behoeve van een realistische prijsstelling volgt in de gunningsfase (zie vraag 48).
186	Selectiedocument - Paragraaf 2.5	Op welke wijze wordt de 'beste prijs-kwaliteitverhouding' gewogen, en welke aspecten krijgen daarbij de meeste aandacht?	De gunningscriteria, waaronder de weging van prijs en kwaliteit binnen de 'beste prijs-kwaliteitverhouding', worden bekendgemaakt in het beschrijvend document (gunningsfase). In de selectiefase worden uitsluitend selectiecriteria beoordeeld (SC1-SC3, zie §7); de gunningscriteria en -weging zijn in deze fase nog niet aan de orde.
187	Selectiedocument - Paragraaf 3.3	Inschrijver stelt voor om een tweede Nota van Inlichtingen te introduceren voor nadere verduidelijking van de aangeleverde informatie én de antwoorden van de eerste Nota van Inlichtingen verder te verduidelijken, is dit akkoord?	De planning (§3.3) voorziet in één Nota van Inlichtingen in de selectiefase (publicatie 24 juni 2026) en twee Nota's van Inlichtingen in de gunningsfase. Een tweede Nota van Inlichtingen in de selectiefase is niet voorzien en wordt niet aan de planning toegevoegd. Voor inhoudelijke verduidelijking van de antwoorden in de eerste Nota van Inlichtingen kunnen Inschrijvers in de gunningsfase gebruik maken van de twee daarvoor beschikbare vragenrondes.
188	Selectiedocument - Paragraaf 6.4	Inschrijver neemt aan dat een referentie waarbij de dienstverlening langer dan 36 maanden geleden is aangevangen kan worden ingediend als referentie, is dat correct?	De referentieopdracht moet in de drie jaar vóór de datum van Aanmelding zijn verricht. Zowel afgeronde als nog lopende opdrachten kwalificeren, mits aan de minimale looptijd van 3 jaar is voldaan. Een opdracht die voor deze driejaarsperiode is aangevangen kwalificeert, mits zij binnen de driejaarsperiode nog in uitvoering was of is afgerond.

189	Selectiedocument - Paragraaf 6.4	Citaat: een opdracht met een minimale omvang van € 200.000. Inschrijver neemt aan dat dit bedrag per jaar wordt bedoeld, is dat correct	De minimale omvang van € 200.000 (excl. btw) bij Kerncompetentie 2 betreft het totale gefactureerde bedrag over de (minimaal 3-jarige) referentieopdracht, niet een jaarlijks gefactureerd bedrag.
190	Selectiedocument - Paragraaf 2.5	In het selectiedocument en met name Bijlage 10 wordt impliciet vermeld dat door inschrijving nu al een volledig akkoord wordt gegeven op Bijlage 10 (Programma van Eisen E1.02). Inschrijver neemt aan dat het indienen van de inschrijving nu nog niet wordt gezien als een volledig en bindend akkoord op Bijlage 10; het is een verklaring van bereidheid en het definitieve akkoord wordt pas gegeven door inschrijving in de gunningsfase , is dat correct ?	Bevestigd. Het indienen van een Aanmelding betreft een verzoek om toelating tot de procedure en geen volledig en bindend akkoord op Bijlage 10. In de selectiefase wordt uitsluitend beoordeeld op uitsluitingsgronden, geschiktheidseisen en selectiecriteria (§3.8 Selectiedocument). Bijlage 10 betreft het Concept Programma van Eisen. Het akkoord dat door het indienen van een Aanmelding wordt gegeven (§3.10) ziet op de aanbestedingsprocedure en de uitgangspunten, niet op een definitief en onvoorwaardelijk akkoord met de afzonderlijke eisen van het concept-PvE. Het bindende akkoord op het Programma van Eisen wordt gegeven bij Inschrijving in de gunningsfase, waarna twee vragenrondes beschikbaar zijn voor nadere verduidelijking of aanpassing (zie planning §3.3).
191	Selectiedocument - Paragraaf 2.5 & Bijlage 10	Op basis van de vorige vraag over de status van Bijlage 10 in deze fase neemt inschrijver aan dat in de volgende fase er ruimte is om verdere vragen te stellen over dit programma van eisen waarbij die vragen ook kunnen leiden tot verduidelijking en aanpassing van het programma van eisen, is dat correct? In de ogen van de inschrijver is het niet proportioneel om een zo uitgebreid en gedetailleerd programma van eisen met 1 vragenronde tijdens de selectiefase volledig te accorderen, deelt de aanbestedende dienst die visie ?	Bevestigd. In de gunningsfase is via twee vragenrondes ruimte om vragen te stellen over het PvE, die kunnen leiden tot verduidelijking en aanpassing. De Aanbestedende Dienst onderschrijft dat een omvangrijk PvE niet met één vragenronde volledig behoeft te worden geaccordeerd; de gunningsfase voorziet daarvoor in twee vragenrondes. In de selectiefase wordt uitsluitend beoordeeld op uitsluitingsgronden, geschiktheidseisen en selectiecriteria (§3.8 Selectiedocument). Bijlage 10 betreft het Concept Programma van Eisen. Het akkoord dat door het indienen van een Aanmelding wordt gegeven (§3.10) ziet op de aanbestedingsprocedure en de uitgangspunten, niet op een definitief en onvoorwaardelijk akkoord met de afzonderlijke eisen van het concept-PvE. Het bindende akkoord op het Programma van Eisen wordt gegeven bij Inschrijving in de

			gunningsfase, waarna twee vragenrondes beschikbaar zijn voor nadere verduidelijking of aanpassing (zie planning §3.3).
192	Selectiedocument - Paragraaf 2.5 & Bijlage 11	Op basis van de vraag over de status van Bijlage 10 in deze fase neemt inschrijver aan dat in de volgende fase er ruimte is om ook over Bijlage 11 verdere vragen te stellen over dit programma van eisen waarbij die vragen ook kunnen leiden tot verduidelijking en aanpassing van de voorwaarden van deelnemers met voorwaarden, is dat correct? In de ogen van de inschrijver is het niet proportioneel om een zo uitgebreid en gedetailleerd programma van eisen met 1 vragenronde tijdens de selectiefase volledig te accorderen, deelt de aanbestedende dienst die visie ?	Ja, wij bevestigen dit
193	Bijlage 2, 4. gefactureerd bedrag	Inschrijver neemt aan dat de informatie over het gefactureerde bedrag enkel voor kerncompetentie 2 dient te worden opgegeven, is dat correct?	Bevestigd. Het gefactureerde bedrag wordt uitsluitend gevraagd voor Kerncompetentie 2 (referentie-eis 2). Voor Kerncompetentie 1 wordt de hoeveelheid endpoints gevraagd, niet een gefactureerd bedrag (Bijlage 6, §6.4).

194	Bijlage 2, 4. Handtekening	Inschrijver neemt aan dat de handtekening van de inschrijver en niet de referent dient te zijn, is dat correct?	Bevestigd. Het referentieformulier (Bijlage 6) wordt door de Gegadigde/Inschrijver ondertekend; een handtekening van de referent is niet vereist. De Aanbestedende Dienst behoudt zich het recht voor ter verificatie rechtstreeks contact op te nemen met de opdrachtgever van de referentieopdracht (§6.4).
195	Bijlage 10 - Programma van Eisen	Geldt dit voor onderliggende algemene voorwaarden, geheimhouding, verwerkersovereenkomsten en dergelijke, of is dat nog niet aan de orde in deze fase?	Onderliggende algemene voorwaarden, geheimhouding en verwerkersovereenkomsten maken onderdeel uit van de uitvoeringsdocumenten en worden in de gunningsfase ter beschikking gesteld en aldaar aan de orde gesteld. In de selectiefase zijn deze nog niet aan de orde. In de selectiefase wordt uitsluitend beoordeeld op uitsluitingsgronden, geschiktheidseisen en selectiecriteria (§3.8 Selectiedocument). Bijlage 10 betreft het Concept Programma van Eisen. Het akkoord dat door het indienen van een Aanmelding wordt gegeven (§3.10) ziet op de aanbestedingsprocedure en de uitgangspunten, niet op een definitief en onvoorwaardelijk akkoord met de afzonderlijke eisen van het concept-PvE. Het bindende akkoord op het Programma van Eisen wordt gegeven bij Inschrijving in de gunningsfase, waarna twee vragenrondes beschikbaar zijn voor nadere verduidelijking of aanpassing (zie planning §3.3).
196	Bijlage 10 - Programma van Eisen	Wij verzoeken de Aanbestedende Partij te bevestigen dat de kosten voor dergelijke audit gedragen worden door Opdrachtnemer (collectief).	PvE E8.34 bepaalt dat de Deelnemer het recht heeft maximaal eenmaal per jaar een audit te laten uitvoeren door een externe onafhankelijke partij. De kosten van deze audit zijn voor rekening van de Deelnemer; het PvE schrijft geen verplichting tot kostenvrije medewerking namens Opdrachtnemer voor buiten de in het PvE opgenomen medewerkingsverplichtingen.
197	Bijlage 10, Eis E3.03 – Serviceniveaus	E3.03 beschrijft drie serviceniveaus (24x7 eyes-on-screen, 12x5 + piket, 12x5). Kan een Deelnemer gedurende de looptijd van de Nadere Overeenkomst wisselen van serviceniveau (bijv. van Niveau 3 naar Niveau 1)? Zijn aan dergelijke wijzigingen minimale contracttermijnen, opzegtermijnen of overstapkosten verbonden?	De keuze voor een serviceniveau (vgl. PvE E3.03) wordt vastgelegd in de Nadere Overeenkomst. Of en onder welke voorwaarden (opzegtermijnen, overstapkosten) een Deelnemer gedurende de looptijd van serviceniveau kan wisselen, wordt geregeld in de overeenkomst in de

			gunningsfase (beschrijvend document / concept-Raamovereenkomst).
198	Bijlage 10, Eis E6.04 – Opslagmodellen A en B	Wij verzoeken Aanbestedende Dienst te heroverwegen om in geval van Model A wel toe te staan om data over te nemen of structureel te dupliceren naar een door Opdrachtnemer beheerd platform omdat dit enerzijds enrom kostenbesparend zal werken voor de deelnemers omdat hierdoor opslag en verwerkingskosten in Azure wordt voorkomen alsmede in geval van een geopolitieke switch alle relevante en historische data en op maat gemaakte use cases niet meer beschikbaar zouden zijn.	Onder Model A blijft de data binnen de eigen omgeving van de Deelnemer of binnen het door de Deelnemer gebruikte ecosysteem; het opleggen van verplichte overname of verplaatsing naar een eigen, niet tot dat domein behorende omgeving van de Opdrachtnemer is onder Model A uitgesloten. Een Deelnemer die om redenen van kosten of continuïteit opslag in een eigen, door de Opdrachtnemer beheerde omgeving wenst, kiest daarvoor Model B; dat is dan een bewuste modelkeuze en geen verplichte voorwaarde onder A. De continuïteit en beschikbaarheid van historische data en use cases, ook bij een eventuele overstap, worden geborgd via de export- en exiteisen (onder meer E6.06), niet via gedwongen duplicatie onder Model A.
199	Bijlage 10, Eis E6.04 – Opslagmodellen A en B	E6.04 stelt dat Opdrachtnemer 'minimaal twee opslagmodellen' ondersteunt: Model A (opslag in Deelnemer-tenant) en Model B (opslag bij Opdrachtnemer). Geldt de verplichting om beide modellen te ondersteunen als harde eis, of kan Opdrachtnemer de aanbieding beperken tot uitsluitend Model B? Indien Model A verplicht is: hoe dient Opdrachtnemer de retentie van minimaal 6 maanden (E6.03) te borgen als de data is opgeslagen in de Deelnemer-eigen Microsoft Sentinel-tenant?	Deel 1: het ondersteunen van beide modellen is een harde eis; de aanbieding kan niet worden beperkt tot uitsluitend Model B. Beide modellen blijven bestaan en de Opdrachtnemer faciliteert ze beide. Deel 2: de Opdrachtnemer borgt de minimumretentie van E6.03 ook onder Model A, binnen dezelfde omgeving waarin de data al staat. De vereiste retentie en de aanvullende incident-bewaartermijn worden gerealiseerd via de retentie- en archieffunctionaliteit van die omgeving zelf, bijvoorbeeld de interactieve retentie en de archieflaag van een Sentinel-/Log Analytics-werkruimte, zo nodig aangevuld met holds. De data verlaat de omgeving waarin Model A is ingericht daarbij niet; de archieflaag is een tier binnen dezelfde omgeving en geen externe opslag. De verantwoordelijkheid voor het halen van de retentietermijn ligt bij de Opdrachtnemer, ongeacht

			het model; eventuele aanvullende kosten zijn inbegrepen in het baseline-tarief conform E6.03.
200	Bijlage 10, Eis E2.04 – Certificeringen SOC-teamleden	E2.04 stelt dat SOC-teamleden 'aantoonbaar over een actuele SOC-relevante certificering of over aantoonbare gelijkwaardige kennis en ervaring op SOC-analist-niveau' beschikken. Betreft dit een eis op individueel medewerkerniveau (elke analist die de dienstverlening uitvoert), of volstaat een representatief percentage van het team? Geldt de certificeringseis ook voor piket-functionarissen (Niveau 2) die incidenteel worden ingezet buiten de bemensingsuren?	E2.04 geldt op individueel niveau: elk SOC-teamlid dat voor de Deelnemer wordt ingezet, beschikt over een actuele SOC-relevante certificering of over aantoonbaar gelijkwaardige kennis en ervaring op SOC-analist-niveau. Een representatief percentage van het team volstaat niet; de eis kan per medewerker wel worden ingevuld via certificering of via gelijkwaardige kennis en ervaring. De eis geldt ook voor piket-functionarissen (Niveau 2) die buiten de bemensingsuren worden ingezet, omdat zij eveneens SOC-analistwerkzaamheden voor de Deelnemer verrichten.

201	Bijlage 10, Eis E8.04 – ABRO	E8.04 stelt dat de dienstverlening geheel of gedeeltelijk onder de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) kan vallen. Welke specifieke Deelnemers vallen naar verwachting onder ABRO? Is er een indicatieve lijst beschikbaar, of wordt dit pas per Nadere Overeenkomst bepaald? Kan Aanbestedende Dienst alvast aangeven welke ABRO-screeneisen (bijv. Verklaring van Geen Bezwaar) concreet van toepassing zullen zijn?	De ABRO is op dit moment uitsluitend van toepassing op het deel van de dienstverlening dat het NIPV betreft, in zijn hoedanigheid als zelfstandig bestuursorgaan binnen de Rijksoverheid. De Veiligheidsregio's zijn geen Rijksoverheid; voor hen is de ABRO op dit moment niet van toepassing. De formulering in E8.04 dat de ABRO geheel of gedeeltelijk van toepassing kan zijn, is een bewust voorbehoud: indien daartoe in de toekomst wordt besloten, kunnen ook Veiligheidsregio's hierop terugvallen. Opdrachtnemer werkt actief mee aan de uit de ABRO voortvloeiende verplichtingen voor zover en op het moment dat deze van toepassing zijn; de concrete invulling wordt per Deelnemer in de Nadere Overeenkomst bepaald.
202	Bijlage 10, Eis E5.15 – Open standaarden Forum Standaardisatie	E5.15 verplicht naleving van de open standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Geldt deze eis ook voor de intern gebruikte SIEM-, EDR- en SOAR-platforms van Opdrachtnemer (interne verwerking, niet klantgericht), of uitsluitend voor klantgerichte interfaces, communicatiekanalen en rapportages richting de Deelnemer? Mocht een platform een alternatief bieden voor een verplichte standaard, volstaat dan een 'leg uit' motivatie in de aanbieding?	E5.15 richt zich op de klantgerichte interfaces, communicatiekanalen, koppelvlakken en rapportages richting de Deelnemer en op de uitwisseling van gegevens; daarvoor geldt het 'pas toe of leg uit'-regime van het Forum Standaardisatie. De zuiver interne verwerking binnen de SIEM-, EDR- en SOAR-platforms, die niet klantgericht is en geen externe uitwisseling betreft, valt niet onder de eis, mits de klantgerichte koppelvlakken en de gegevensuitwisseling wel aan de standaarden voldoen. Indien een platform voor een verplichte standaard een alternatief biedt, kan in de aanbieding een 'leg uit'-motivatie worden opgenomen, conform het 'pas toe of leg uit'-principe.

203	Bijlage 10, Eis E6.03 – 3 jaar retentie incidentdata	E6.03 stelt een bewaartermijn van minimaal 3 jaar voor 'log- en eventdata die betrekking heeft op een geconstateerd security-incident'. Wat is de precieze definitie van 'geconstateerd security-incident' in dit kader: geldt de 3 jaar retentie voor alle gegenereerde alarmen, of uitsluitend voor alarmen die als True Positive zijn geclassificeerd? Wie draagt de eindverantwoordelijkheid voor de initiële classificatie (Opdrachtnemer of Deelnemer), en wat zijn de gevolgen als classificatie achteraf herzien wordt?	Conform BIO2 (versie 1.3, op 5 maart 2026 gepubliceerd in de Staatscourant) wordt de logging en alle informatie rondom een (vermoedelijk) informatiebeveiligingsincident, waaronder de analyse, de oplossing en het advies, minimaal drie jaar ongewijzigd bewaard. Voor de algemene logretentie hanteert BIO2 een risicogebaseerde benadering; E6.03 stelt hiervoor een minimum van zes maanden, in lijn met de door de IBD gehanteerde praktijknorm. De classificatie van alarmen en incidenten wordt operationeel uitgevoerd door Opdrachtnemer conform het alarmclassificatieschema (E7.13); de Deelnemer blijft als eigenaar van de eigen beveiliging eindverantwoordelijk voor de besluitvorming over de opvolging, conform de in het DAP vastgelegde afspraken. Wordt een alarm achteraf alsnog als (vermoedelijk) incident aangemerkt, dan gaat de driejaarstermijn voor de betreffende data gelden; de werkwijze rond herclassificatie en retentie wordt in het DAP vastgelegd.
204	Bijlage 10, Eis E7.15 – Time-to-notify	De gevraagde notificatie tijden (i.e. MTTR) acht gegadigde als niet-marktconform met name omdat structureel 10 minuten tijd bij een P1 incident voor pick-up time, triage, incident analyse, mitigatie advies formuleren en escalatie door een analist bijna ondoenlijk is zonder dat er van een significante uitbreiding van resources sprake zal zijn en daardoor enorm kosten en dus ook prijs verhogend werkt terwijl de praktijk uitwijst dat een langere notifciatie tijd geen onnodige risico's met zich meebrengt. Daarnaast zou 30 minuten voor een P2 incident evenzo onnodig kosten verhogend doorwerken. Gegadigde verzoekt derhalve om de notificatie tijden aan te passen naar P1: 30 minuten en P2: 1 uur.	De P1 time-to-notify wordt verruimd van 10 naar 15 minuten; het verzoek om 30 minuten voor P1 en 1 uur voor P2 wordt niet gevolgd. De time-to-notify betreft de melding van een (mogelijk) incident, niet de volledige triage en respons (geen MTTR); 15 minuten ligt binnen de gangbare marktrange en blijft haalbaar en afdwingbaar. De tijden voor P2 (30 minuten) en P3 (4 uur) blijven ongewijzigd. Zie verder het antwoord op vraag 130.

205	Bijlage 10, Eis E7.15 – Time-to-notify bij piket (Niveau 2)	Indien de Aanbestedende Dienst blijft vasthouden aan de gestelde notificatietijden:E3.03 beschrijft bij Niveau 2 een piket-mechanisme buiten de bemensingsuren. Geldt de P1 time-to-notify van 10 minuten ook voor een piket-functionaris buiten de bemensingsuren van Niveau 2 (08:00–18:00), of geldt voor piket-situaties een afwijkende reactietijd? Hoe worden de time-to-notify SLO's gemeten en gerapporteerd per Deelnemer en per maand?	Zie het antwoord op vraag 88.
206	Bijlage 10, Eis E8.01 / E8.02 – EER-eis voor back-up en DR	E8.01 en E8.02 vereisen dat het SOC, de gebruikte software (SIEM, EDR, NDR) en de datacenters binnen de EER zijn gevestigd, inclusief redundante systemen. Geldt deze eis ook voor tijdelijke datacaching, hot-standby back-up- en disaster-recoverysystemen van Opdrachtnemer? Mogen sub-verwerkers (bijv. cloud hostingproviders) worden ingezet buiten Nederland maar binnen de EER, en zo ja, op welke wijze dient de transparantie conform E8.03 te worden vormgegeven?	PvE E8.01 vereist dat het SOC, de gebruikte software (SIEM, EDR, NDR) en de datacenters - ook redundante systemen - binnen de EER zijn gevestigd. Dit omvat tijdelijke datacaching en hot-standby/disaster-recovery-systemen van Opdrachtnemer, voor zover deze binnen het beheer van Opdrachtnemer vallen. Subverwerkers (zoals cloud-hostingproviders) mogen buiten Nederland maar binnen de EER worden ingezet, mits voldaan aan Geschiktheidseis 8. Transparantie over de inzet van subverwerkers conform PvE E8.03 wordt in de Nadere Overeenkomst vastgelegd.
207	Bijlage 10, Eis E5.25 – Mobile EDR en platform-eenheid	E5.25 stelt dat mobile EDR 'geleverd wordt binnen hetzelfde EDR-platform dat ook voor werkplekken en servers wordt gebruikt (platform-eenheid)'. Geldt deze platform-eenheidseis als harde technische vereiste ook voor Deelnemers die geen mobile EDR afnemen, of is de eis uitsluitend van toepassing op het moment dat een Deelnemer de optionele mobile EDR-dienst activeert? Kan een aanbieder die een ander EDR-platform gebruikt voor mobiel (bijv. Microsoft Defender for Mobile) dan voor werkplekken toch voldoen aan E5.25?	E5.25 vraagt dat Opdrachtnemer de capability biedt om EDR op mobiele apparaten te leveren binnen hetzelfde EDR-platform als werkplekken en servers (platform-eenheid, E5.07). De capability moet door iedere inschrijver worden aangeboden; de daadwerkelijke afname van mobile EDR is optioneel per Deelnemer (Nadere Overeenkomst). Voor een Deelnemer die geen mobile EDR afneemt, is de levering niet aan de orde, maar de aangeboden oplossing moet de platform-eenheid wel ondersteunen. Een mobiele oplossing als Microsoft Defender for Mobile kan aan E5.25 voldoen, mits deze binnen hetzelfde EDR- of XDR-platform en dezelfde beheer- en correlatieomgeving valt als de EDR voor werkplekken en servers; een losstaand, niet-geïntegreerd mobiel EDR-platform voldoet niet aan de platform-eenheid.

208	Bijlage 10, Eis E4.03 / E4.04 – Kosten retransitieperiode	E4.03 verplicht Opdrachtnemer de dienstverlening op verzoek van Deelnemer maximaal 6 maanden voort te zetten na de einddatum (retransitie). Zijn de kosten van deze retransitieperiode inbegrepen in het all-in tarief (E1.11), of mogen hiervoor aanvullende kosten in rekening worden gebracht? Geldt de retransitieverplichting ook bij beëindiging van de overeenkomst wegens wanprestatie door Deelnemer, of uitsluitend bij contractsverloopdatum of reguliere opzegging?	PvE E4.03 bepaalt dat de retransitieperiode maximaal 6 maanden bedraagt, onder dezelfde condities, prijzen en tarieven, op verzoek van de Deelnemer. De vraag of de kosten hiervan in het all-in tarief zijn inbegrepen dan wel afzonderlijk in rekening mogen worden gebracht, en of de retransitieverplichting ook geldt bij beëindiging wegens wanprestatie van de Deelnemer, wordt geregeld in de overeenkomst in de gunningsfase.
209	§ 2.2 Voorwerp van de Opdracht	Het Selectiedocument vermeldt dat Deelnemers vanwege geopolitieke ontwikkelingen alternatieven kunnen inzetten voor Amerikaanse producten. Welke contractuele verplichtingen worden aan Opdrachtnemer gesteld om een dergelijke technologische transitie te ondersteunen? Binnen welke termijn en tegen welke (extra) kosten dient Opdrachtnemer een transitie van een Deelnemer naar alternatieve (niet-Amerikaanse) tooling te faciliteren?	Het Selectiedocument signaleert dat Deelnemers op termijn alternatieve (niet-Amerikaanse) producten kunnen overwegen (§2.2). PvE E8.05 bepaalt dat een Deelnemer de dienstverlening (geheel of gedeeltelijk) kan afbouwen of beëindigen indien gewijzigde nationale overheidsrichtlijnen of wettelijke kaders het gebruik van de onderliggende technologiestack niet langer toestaan, in welk geval de retransitieprocedure conform E4.03/E4.04 in werking treedt. De contractuele verplichtingen voor ondersteuning bij een dergelijke technologische transitie, de termijnen en de bijbehorende kosten worden in de gunningsfase verder uitgewerkt.
210	§ 2.2 Voorwerp van de Opdracht	Meerdere Deelnemers beschikken reeds over Microsoft Sentinel als SIEM-oplossing. Dient de Opdrachtnemer de MDR-dienstverlening te integreren met de bestaande Sentinel-instantie van die Deelnemer, of staat het Opdrachtnemer vrij een eigen SIEM-platform aan te bieden als vervanging? Hoe dient de Opdrachtnemer het prijsverschil tussen beide scenario's inzichtelijk te maken?	Het uitgangspunt is dat Opdrachtnemer zo goed mogelijk aansluit bij de bestaande omgevingen en applicaties van de Deelnemers. De inschrijver geeft aan hoe de oplossing omgaat met reeds gedane investeringen, zoals bestaande Microsoft Sentinel-instanties vanuit E5-licenties, en biedt tegelijkertijd passende oplossingen voor Deelnemers die daar niet over beschikken. De Opdrachtnemer moet dus kunnen omgaan met uiteenlopende uitgangspunten per Deelnemer. In de gunningsfase wordt aan de hand van casuïstiek en voorbeeldregio's de gelegenheid geboden om aan te geven hoe dit wordt geïntegreerd en geprijsd, en welke eventuele consequenties dit heeft voor de verschillende soorten Deelnemers.

211	§ 2.2 Voorwerp van de Opdracht	De M-EDR is verplichte afname voor alle Deelnemers. Dient de Opdrachtnemer een specifieke EDR-tooling te leveren (bijv. Microsoft Defender for Endpoint), of is Opdrachtnemer vrij om een gelijkwaardige, marktconforme EDR-oplossing in te zetten die aan de PvE-eisen voldoet, mits de functionaliteit aantoonbaar gelijkwaardig is?	Zie het antwoord op vraag 57.
212	§ 2.2 Voorwerp van de Opdracht	Kan Aanbestedende Dienst een indicatie geven van het verwachte totale aantal endpoints over alle (maximaal 15) Deelnemers bij volledige uitrol? Dit is voor Opdrachtnemer essentieel om een realistisch en transparant staffelmodel te kunnen opbouwen zoals gevraagd in PvE-eis E1.14.	Zie het antwoord op vraag 48.
213	§ 6.4 Technische bekwaamheid – Referentie-eis 2	Referentie-eis 2 stelt een minimale omvang van € 200.000. Betreft dit het totaal over de gehele looptijd van de referentieopdracht (minimaal 3 jaar), of dient het jaarlijks gefactureerde bedrag minimaal € 200.000 te bedragen?	De minimale omvang van € 200.000 (excl. btw) bij Kerncompetentie 2 betreft het totale gefactureerde bedrag over de (minimaal 3-jarige) referentieopdracht, niet een jaarlijks gefactureerd bedrag.
214	Bijlage 10, Eis E2.01	Eis E2.01 stelt dat er vanuit Opdrachtnemer geen relatie of inmenging mag zijn met statelijke actoren die als offensief worden geclassificeerd door AIVD/NCTV. Op welke wijze dient Opdrachtnemer aan te tonen dat aan deze eis wordt voldaan? Is een eigen verklaring (op erewoord) voldoende, of wordt een specifiek auditraport, keten-screening of andere objectieve verificatie verwacht?	Voor Geschiktheidseis 9 kan bij Aanmelding worden volstaan met het UEA (eigen verklaring). De Aanbestedende Dienst behoudt zich het recht voor nadere onderbouwing of toelichting te vragen; een specifiek auditrapport of keten-screening is bij Aanmelding niet vereist.
215	Bijlage 11 – Deelnemers met voorwaarden	Meerdere Deelnemers met voorwaarden hebben budgetplafonds benoemd. Dienen Inschrijvers in de gunningsfase een afzonderlijk prijsoverzicht per Deelnemer te verstrekken waaruit blijkt of aan het budgetplafond wordt voldaan? Op welke wijze dient de Opdrachtnemer rekening te houden met deze plafonds in het transparante staffelmodel (PvE E1.14)?	Budgetplafonds in Bijlage 11 zijn randvoorwaarden van de betreffende 'Deelnemer met voorwaarden'; overschrijding leidt tot opt-out van die Deelnemer. Inschrijvers hoeven in de selectiefase geen afzonderlijk prijsoverzicht per Deelnemer aan te leveren. In de gunningsfase wordt via het Prijzenblad en de voorbeeldcalculaties (PvE E1.14) inzichtelijk gemaakt of de aangeboden tarieven binnen de budgetplafonds vallen.

216	Bijlage 11 – VGGM / Z-CERT	VGGM (Veiligheids- en Gezondheidsregio Gelderland-Midden) stelt als voorwaarde aansluiting op het zorgdetectienetwerk via Z-CERT. Is deze Z-CERT-aansluiting een eis die uitsluitend voor VGGM als Deelnemer met voorwaarden geldt, of wordt verwacht dat de Opdrachtnemer voor alle Deelnemers de mogelijkheid van Z-CERT-integratie aanbiedt? Hoe dient dit in de aanbieding te worden verankerd?	Z-CERT-aansluiting is geen generieke eis voor alle Deelnemers. Z-CERT is relevant voor Deelnemers met zorggerelateerde processen (E7.06); Opdrachtnemer moet Z-CERT-integratie kunnen bieden waar dit van toepassing is. Voor VGGM is dit als aanvullende deelnemer-voorwaarde expliciet gemaakt, waarop VGGM zich kan beroepen.
217	§ 2.2 + Bijlage 10 PvE	Diverse Deelnemers hebben nog een lopende overeenkomst met een andere MDR/SIEM-leverancier en sluiten later aan (H2 2027 – 2029). Welke minimale beschikbaarheidsverplichtingen en SLA-vereisten gelden voor de Opdrachtnemer gedurende de periode vóór livegang van een specifieke Deelnemer? Dient de Opdrachtnemer de migratie en exit bij de vorige leverancier actief te ondersteunen, en zo ja, valt dit binnen de all-in prijs?	De SLA- en beschikbaarheidsverplichtingen (zoals E3.06 en E7.15) gelden per Deelnemer vanaf de livegang van de dienstverlening voor die Deelnemer, zoals vastgelegd in de betreffende Nadere Overeenkomst. Vóór livegang zijn er voor die Deelnemer geen operationele beschikbaarheids- of SLA-verplichtingen; in die periode gelden de afspraken rond onboarding en transitie (E4.06, E4.10). Opdrachtnemer ondersteunt actief de onboarding en de overname van de Deelnemer, waaronder het inrichten op basis van door de Deelnemer aangeleverde configuraties en use-cases; de exit bij de vorige leverancier is primair de verantwoordelijkheid van de Deelnemer en de vertrekkende leverancier, op basis van diens exit-verplichtingen. De onboarding- en transitie-activiteiten van Opdrachtnemer vallen binnen de afgesproken prijsstructuur; de kosten van de exit bij de vorige leverancier vallen daar niet onder.

218	2,2	In paragraaf 2.2 wordt Managed-EDR (M-EDR) aangemerkt als verplichte baseline voor alle Deelnemers, terwijl SIEM en NDR als optionele uitbreiding zijn bestempeld. In een Microsoft-georienteerd landschap zijn endpointdetectie en -response doorgaans geintegreerd, waarbij endpointsignalen worden gecorreleerd en opgevolgd binnen een SOC-operatie die mede gebruikmaakt van een SIEM. Kan de Aanbestedende Dienst bevestigen dat een geintegreerde aanpak, waarbij de managed endpoint-detectie en -response onderdeel uitmaakt van een SOC dat mede gebruikmaakt van een SIEM-component, voldoet aan de invulling van de baseline M-EDR-dienstverlening? Zo nee, kan de Aanbestedende Dienst verduidelijken welke specifieke capabilities zij als minimale invulling van de baseline M-EDR beschouwt, los van de optionele SIEM-uitbreiding?	Zie het antwoord op vraag 57.
219	6,3	Geschiktheidseis 3 vereist een beroepsaansprakelijkheidsverzekering met een minimale dekking van EUR 2.500.000 per aanspraak, gemaximeerd tot EUR 5.000.000 per verzekeringsjaar. In de markt van gespecialiseerde SOC/MDR-dienstverleners is een verzekerde som van EUR 2.500.000 per aanspraak en EUR 2.500.000 per verzekeringsjaar een gangbaar dekkingsniveau, terwijl een maximum van EUR 5.000.000 per verzekeringsjaar met name voor het MKB tot aanvullende premielasten leidt. Kan de Aanbestedende Dienst onderbouwen waarom een jaarmaximum van EUR 5.000.000 in verhouding tot de aard en het risicoprofiel van de Opdracht proportioneel wordt geacht, en is de Aanbestedende Dienst bereid het vereiste jaarmaximum bij te stellen naar EUR 2.500.000, dan wel naar een niveau dat aansluit bij hetgeen in deze markt gangbaar is? Indien de Aanbestedende Dienst de eis handhaaft: kan de Aanbestedende Dienst bevestigen dat het bij Aanmelding volstaat het UEA in te dienen, en dat een Gegadigde de vereiste dekking eerst hoeft aan te tonen voor aanvang van de Raamovereenkomst, waarbij een verklaring van de verzekeraar dat de dekking op eerste verzoek wordt verhoogd	Geschiktheidseis 3 vereist een beroepsaansprakelijkheidsverzekering met minimale dekking van € 2.500.000 per aanspraak, gemaximeerd tot € 5.000.000 per verzekeringsjaar. Gelet op de aard, omvang en het risicoprofiel van de meerjarige Raamovereenkomst voor vitale publieke organisaties acht de Aanbestedende Dienst dit proportioneel; de eis wordt gehandhaafd. Bij Aanmelding volstaat het UEA; de daadwerkelijke dekking hoeft pas aan te vangen op de dag dat de uitvoering van de Raamovereenkomst start. Een verklaring van de verzekeraar dat de dekking uiterlijk per die datum beschikbaar is, kan als toereikend bewijs worden aanvaard na selectie. Dit dient binnen 7 dagen na verzending voornemen tot selectie ingediend te worden als bewijs.

		naar EUR 2.500.000 per aanspraak / EUR 5.000.000 per verzekeringsjaar als toereikend bewijs wordt aanvaard?	
220	6,4	Kerncompetentie 1 spreekt van minimaal 500 endpoints, terwijl in paragraaf 2.2 (pagina 12) bij de 0-meting servers, werkplekken, mobile devices en netwerkcomponenten in scope worden genoemd. Kan de Aanbestedende Dienst verduidelijken welke typen devices als 'endpoint' meetellen voor het aantonen van Kerncompetentie 1, en of cloud-workloads hieronder vallen?	Voor Kerncompetentie 1 tellen de endpoints mee die in de referentieopdracht door de SOC/MDR-dienstverlening werden gemonitord. Hieronder vallen in elk geval servers, werkplekken, mobile devices en netwerkcomponenten (zie ook §2.2 voor de scope bij de 0-meting). Cloud-workloads kunnen meetellen voor zover deze als endpoint binnen de monitoring zijn opgenomen. De Gegadigde onderbouwt de aantallen en typen in het referentieformulier (Bijlage 6).
221	6,4	Geschiktheidseis 5 vereist dat de integriteit van alle SOC-analisten door middel van een erkende screening is vastgesteld. Kan de Aanbestedende Dienst verduidelijken welke vormen van screening als 'erkend' worden beschouwd (bijvoorbeeld VOG, AIVD-veiligheidsonderzoek, of een gelijkwaardige werkgeversscreening).	Zie het antwoord op vraag 37.

222	6,7	Geschiktheidseis 8 vereist dat alle in het kader van de opdracht verwerkte gegevens uitsluitend binnen de EU/EER worden verwerkt en opgeslagen, en dat geen doorgifte naar derde landen plaatsvindt. De Algemene Verordening Gegevensbescherming (AVG) staat doorgifte naar derde landen onder voorwaarden toe, onder meer op basis van de door de Europese Commissie vastgestelde modelcontractbepalingen (Standard Contractual Clauses, SCC's), aangevuld met passende aanvullende waarborgen. Kan de Aanbestedende Dienst verduidelijken of Geschiktheidseis 8 een absoluut vereiste van uitsluitend verwerking en opslag binnen de EU/EER betreft (strikter dan de AVG), of dat AVG-conforme doorgifte naar een derde land op basis van SCC's met passende aanvullende maatregelen eveneens als voldoend aan deze eis wordt aangemerkt? Indien sprake is van een absoluut EER-vereiste: geldt dit voor de volledige verwerkingsketen, inclusief eventuele toegang op afstand, ondersteuningsdiensten en subverwerkers?	Zie 46.
223	6,7	Geschiktheidseis 8 vereist dat alle in het kader van de opdracht verwerkte gegevens, waaronder logdata, detectiegegevens en incidentinformatie, uitsluitend binnen de EU/EER worden verwerkt en opgeslagen, zonder doorgifte naar derde landen. Kan de Aanbestedende Dienst verduidelijken hoe deze eis zich verhoudt tot het gebruik van clouddiensten van een leverancier met een onder niet-EU-recht vallende moederorganisatie, indien de verwerking en opslag van gegevens aantoonbaar binnen de EU/EER plaatsvindt (bijvoorbeeld via een EU-dataresidency- of EU Data Boundary-configuratie)? Beschouwt de Aanbestedende Dienst een dergelijke configuratie als voldoend aan Geschiktheidseis 8?	Zie 46.
224	6,4	Kan de Aanbestedende Dienst bevestigen dat een afgeronde referentieopdracht die voldoet aan de minimale looptijd van 3 jaar, maar die deels vóór de periode van 3 jaar voorafgaand aan de Aanmelding is uitgevoerd, kwalificeert, mits de opdracht binnen die 3-jaarsperiode nog in uitvoering was of is afgerond?	De referentieopdracht moet in de drie jaar vóór de datum van Aanmelding zijn verricht. Zowel afgeronde als nog lopende opdrachten kwalificeren, mits aan de minimale looptijd van 3 jaar is voldaan. Een opdracht die voor deze driejaarsperiode is aangevangen kwalificeert, mits zij binnen de driejaarsperiode nog in uitvoering was of is afgerond.

225	6,4	Kan de Aanbestedende Dienst bevestigen dat dienstverlening die aaneengesloten is geleverd onder opeenvolgende deelopdrachten of verlengingen binnen één raamovereenkomst, geldt als één aaneengesloten referentieopdracht van minimaal 3 jaar in de zin van Kerncompetentie 1?	Dienstverlening die aaneengesloten is geleverd onder opeenvolgende deelopdrachten of verlengingen binnen één raamovereenkomst, geldt als een aaneengesloten referentieopdracht van minimaal 3 jaar in de zin van Kerncompetentie 1, mits de continuïteit en de minimale looptijd aantoonbaar zijn.
226	3,12	Paragraaf 3.12 ziet op de taal van correspondentie en stukken binnen de aanbestedingsprocedure. Kan de Aanbestedende Dienst verduidelijken welke taaleisen gelden voor de operationele dienstverlening, in het bijzonder de communicatie met Deelnemers bij detectie, alarmering en incidentrapportage (waaronder buiten kantoortijden)? Wordt verwacht dat deze communicatie te allen tijde in het Nederlands plaatsvindt, of is Engelstalige operationele communicatie toegestaan voor bepaalde dienstonderdelen of tijdvensters, bijvoorbeeld tijdens 24/7-dekking?	Zie het antwoord op vraag 137.
227	2.2	In de aanbestedingsdocumentatie wordt aangegeven dat er Deelnemers zijn die “een ander merk SIEM inzetten (al dan niet met andere dienstverleners)” en dat van de inschrijver wordt verwacht dat zij met deze dynamiek binnen één raamovereenkomst kan omgaan. Kunt u nader toelichten wat hiermee precies wordt bedoeld? Wordt van inschrijver verwacht dat zij ook dienstverlening levert op, of integraties verzorgt met, deze bestaande niet-Microsoft SIEM-oplossingen? Of wordt uitsluitend verwacht dat inschrijver hiermee rekening houdt bij de onboarding, afstemming en eventuele migratie naar de gevraagde dienstverlening? Daarnaast ontvangen wij graag een indicatie van het aantal Deelnemers waarvoor dit geldt, welke SIEM-oplossingen momenteel worden gebruikt en in hoeverre bestaande dienstverleners gedurende de looptijd van de raamovereenkomst betrokken blijven.	Zie het antwoord op vraag 210.

228	E3.03	Voor een efficiënte SOC-dienstverlening is standardisatie van de operatie van groot belang. In deze eis lijkt echter gevraagd te worden drie verschillende invullingen van de dienst aan te bieden. Kunt u bevestigen dat het volstaat om aan te bieden op basis van drie verschillende invullingen van de SLA (bijvoorbeeld met aangepaste responstijden en/of tijden waarop contact kan worden genomen met Deelnemers voor incidentescalaties) met één invulling van de achterliggende dienstverlening (zijnde 24x7 eyes-on-screen)?	Zie het antwoord op vraag 6.