NOTA VAN INLICHTINGEN

Europese aanbesteding
Inrichting en monitoring MDR
Zaaknummer 3555275 / TenderNed: 506319

Ref. Nr.	Vragenronde	Perceel	Individueel	Onderwerp	Vraag	Antwoord
1	1	Inrichting en monitoring MDR	Nee	Referentieformulier bijlage B	In de leidraad wordt om vier referenties gevraagd. Het referentieformulier heeft enkel ruimte voor 3 referenties. Kunt u hier een nieuw formulier voor toesturen ?	Akkoord. Zie bijlage B.
2	1	Inrichting en monitoring MDR	Nee	Bijlage G Opdrachtbeschrijving Scope / Omgeving gemeente Katwijk	Wat is het aantal Entra ID-identities (o.a. user accounts, admin accounts, service accounts, system accounts, gedeelde mailboxen, vergaderruimtes), exclusief guest-accounts? Zijn alle 950 E5-licenties toegewezen? En zijn er firewalls binnen het netwerk die ontsloten dienen te worden — zo ja, van welke provider(s)?	Er zijn 1577 EntraID Identities (exclusief guest accounts). Van de 980 E5 licenties zijn er 960 toegewezen. Er dienen geen firewalls te worden ontsloten.
3	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.2 Kwaliteitsborging	Welke certificering dient Gegadigde aan te leveren als bewijs voor BIO norm en Nis2? Hiervoor zijn geen bedrijfsmatige certificaten te behalen op bedrijfs- of individueelniveau.	De Gegadigde dient aantoonbaar te maken dat wordt voldaan aan deze kaders, bijvoorbeeld via ISO/IEC 27001 en onderliggende maatregelen en documentatie. Gelijkwaardige bewijsmiddelen zijn toegestaan.
4	1	Inrichting en monitoring MDR	Nee		§2.4 bepaalt dat de voertaal tijdens de uitvoering van de opdracht Nederlands is. Een 24×7 MDR/SOC-dienst wordt in de markt geleverd door internationale analistenteams die buiten reguliere kantooruren (avond, nacht, weekend) volledig Engelstalig werken; dit geldt zowel voor de interne analyse als voor de operationele communicatie in die uren. De Nederlandstalige dienstverlening — accountmanagement, formele incidentrapportages, escalatieoverleggen, periodieke rapportages en alle schriftelijke deliverables — wordt tijdens kantooruren verzorgd. Kunt u bevestigen dat: a) de operationele SOC-dienstverlening buiten kantooruren in het Engels mag plaatsvinden, mits alle formele communicatie en rapportage richting Katwijk (incidentrapportages, escalaties, overleggen en schriftelijke deliverables) in het Nederlands wordt aangeleverd; b) de eis van Nederlands als voertaal ziet op de formele communicatie- en rapportagelaag richting Katwijk, en niet op de operationele taal van het analistenteam buiten kantooruren?	Voertaal 24x7 Nederlands voor operationele communicatie.
5	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 Bandbreedte werkplekken (KC1)	KC1 vraagt een overheidsreferentie met een hybride infrastructuur in de bandbreedte van 500 tot maximaal 600 werkplekken. Kunt u bevestigen dat referenties van overheidsomgevingen met méér dan 600 werkplekken eveneens kwalificeren, mits aan de overige eisen wordt voldaan? Een bovengrens op het aantal werkplekken sluit aantoonbaar geschikte, zwaardere referenties uit en lijkt daarmee disproportioneel; wij verzoeken u de bovengrens te laten vervallen.	Akkoord

6	1	Inrichting en monitoring MDR	Nee	Bijlage G Opdrachtbeschrijving Azure-ingestie- en retentiekosten	Wie draagt de Azure-/Sentinel-verbruikskosten (data-ingestie, analytics-/auxiliary-tiers, langetermijnretentie)? Vallen deze binnen het budget van Katwijk en buiten de opdrachtsom van de opdrachtnemer, of dient de Inschrijver deze in zijn prijs op te nemen? Kunt u, ten behoeve van een realistische raming, het huidige gemiddelde dagelijkse ingestievolume (GB/dag) en de gewenste retentietermijn per logbron aangeven?	De Azure / Sentiel gebruikskosten draagt de gemeente Katwijk
7	1	Inrichting en monitoring MDR	Nee	Bijlage G Opdrachtbeschrijving Sentinel-tenant en data-eigenaarschap	De logbronnen zijn aangesloten op Microsoft Sentinel. Kunt u bevestigen dat de Sentinel-instance zich in de eigen Microsoft-tenant van Katwijk bevindt en dat de workspace, retentie en data-eigenaarschap bij Katwijk blijven? Levert de opdrachtnemer de dienst dus binnen úw tenant, of wordt een SOC-tenant van de leverancier verwacht?	Dat kunnen we bevestigen. De opdrachtnemer levert de dienst binnen de Tenant van de opdrachtgever
8	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 Definitie 'eigen SOC' (KC2)	KC2 vereist dat de SOC-werkzaamheden worden uitgevoerd vanuit een "eigen SOC" en uitdrukkelijk "niet via een derde partij". Deze formulering lijkt op gespannen voet te staan met de in §3.3 geboden mogelijkheid een beroep te doen op derden. Kunt u bevestigen dat aan KC2 wordt voldaan wanneer de Gegadigde de SOC-dienstverlening zelf levert vanuit een eigen (Microsoft-native) operating model, ook indien specifieke deelaspecten — zoals OT-monitoring of red teaming — door een gekwalificeerde partner worden ingevuld?	"Onder een “eigen SOC” wordt verstaan dat de opdrachtnemer zelf verantwoordelijk is voor de uitvoering van de SOC-dienstverlening. Het is toegestaan om voor specifieke specialistische onderdelen, waaronder OT-monitoring, red teaming en penetratietesten, gebruik te maken van gekwalificeerde partners, mits de opdrachtnemer eindverantwoordelijk blijft en de SOC-dienstverlening niet volledig aan derden wordt uitbesteed. Indien voor het voldoen aan Kerncompetentie 3 een beroep wordt gedaan op een derde, zijn tevens de voorwaarden uit het antwoord op vraag 11 van toepassing."
9	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §4 Red teaming / pentesten via derde (S2)	Selectiecriterium S2 waardeert ervaring met red teaming en penetratietesten, inclusief de doorvertaling naar detectieregels. Kunt u bevestigen dat ervaring die door een onderaannemer of derde wordt ingebracht voor S2 meetelt en dat de betreffende referentie als eigen referentie van de Gegadigde wordt gewaardeerd?	Akkoord
10	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 Hybride versus cloud-native referentie (KC1)	KC1 vereist ervaring met een hybride infrastructuur (zowel on-premise als cloud), terwijl de te bewaken omgeving blijkens Bijlage G volledig cloud-native is (geen on-premise servers). Kunt u bevestigen dat een volwaardige cloud-native referentie (Azure/Microsoft Sentinel, onder BIO en NIS2) als gelijkwaardig wordt aanvaard, nu deze de feitelijke opdracht beter weerspiegelt dan een hybride referentie?	Akkoord
11	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 OT-eis (KC3)	Indien KC3 gehandhaafd blijft: kunt u bevestigen dat aan deze eis mag worden voldaan via een beroep op de bekwaamheid van een derde (§3.3), waarbij diens referentie als eigen referentie geldt, en dat ervaring met cloud-/IoT-bewaking of gemeentelijke OT (bijv. gemalen, verkeersregelinstallaties, gebouwbeheersystemen) kwalificeert?	Gegadigde mag voor Kerncompetentie 3 overeenkomstig paragraaf 3.3 een beroep doen op de technische bekwaamheid van een derde. Gegadigde dient daarbij aan te tonen dat hij daadwerkelijk kan beschikken over de kennis en capaciteit van deze derde en dat deze derde de relevante werkzaamheden zal uitvoeren voor zover deze binnen de opdracht aan de orde zijn. Een referentie kwalificeert wanneer daaruit duidelijk en ondubbelzinnig blijkt dat gedurende minimaal twaalf maanden ervaring is opgedaan met het bewaken van netwerkaangesloten operationele of technische systemen binnen SIEM-/SOC-dienstverlening, inclusief gegevensbeveiliging. Ervaring met gemeentelijke OT, zoals gemalen, verkeersregelinstallaties, gebouwbeheersystemen, parkeersystemen of vergelijkbare operationele IoT-omgevingen, kan kwalificeren. Algemene cloudmonitoring of reguliere IT-monitoring zonder aantoonbare OT- of operationele IoT-component kwalificeert niet zelfstandig voor KC3.

12	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 OT-eis (KC3)	Indien er geen OT-systemen in scope zijn: verzoeken wij u KC3 te laten vervallen of te verplaatsen naar een wens/gunningscriterium in de offertefase, aangezien een geschiktheidseis op grond van art. 2.93 lid 1 Aanbestedingswet verband moet houden met en in verhouding moet staan tot het voorwerp van de opdracht. Een knock-out-eis voor een capaciteit die niet wordt afgenomen, is disproportioneel (art. 1.10 Aw, Gids Proportionaliteit).	Niet akkoord. Aanbestedende Dienst handhaaft Kerncompetentie 3 als geschiktheidseis. De gevraagde dienstverlening omvat netwerkdetectie op relevante technische en operationele netwerkzones en, voor zover aanwezig, OT-/IoT-zones. Hieronder valt in ieder geval de technische netwerkomgeving van de parkeergarage. Aanbestedende Dienst acht ervaring met het veilig monitoren van dergelijke omgevingen noodzakelijk voor een beheerste uitvoering van de opdracht. De eis blijft beperkt tot minimaal twaalf maanden ervaring in de afgelopen vijf jaar. Voor het voldoen aan de eis kan overeenkomstig paragraaf 3.3 een beroep worden gedaan op een derde. KC3 wordt niet verplaatst naar een wens of gunningscriterium.
13	1	Inrichting en monitoring MDR	Nee	Selectieleidraad §3.2.3.1 OT-eis (KC3)	Bijlage G beschrijft een volledig cloud-/Microsoft-gebaseerde IT-omgeving en vermeldt geen OT-, ICS- of SCADA-systemen. Kunt u bevestigen of er feitelijk OT-systemen binnen de scope van deze opdracht vallen? Zo ja, verzoeken wij u deze concreet te benoemen (type systemen, protocollen, aantal, locaties).	Aanbestedende Dienst verduidelijkt dat geen sprake is van een omvangrijke industriële productieomgeving met klassieke ICS- of SCADA-systemen. Binnen de huidige scope valt in ieder geval de technische netwerkomgeving van de parkeergarage. Het netwerk bestaat uit verschillende VLAN's en is via een firewall met het internet verbonden. De exacte aangesloten technische componenten, protocollen en netwerkverbindingen zijn op dit moment nog niet volledig geïnventariseerd. Hierdoor kan nog niet voor ieder afzonderlijk component worden vastgesteld of dit als OT of IoT moet worden aangemerkt. De exacte omstandigheden, netwerkzones, aansluitmogelijkheden en geschikte plaatsing van sensoren worden tijdens de implementatiefase gezamenlijk vastgesteld. Een materiële uitbreiding van de beschreven omgeving wordt niet zonder nadere afstemming aan de opdrachtnemer opgedragen.
14	1	Inrichting en monitoring MDR	Nee	Selectieleidraad , par 3.2.3.1: OT-eis (KC3)	Kunt u bevestigen dat Kerncompetentie 3 (12 maanden ervaring met OT-monitoring onder SIEM-SOC) een geschiktheidseis betreft, waarvan het niet aantonen leidt tot uitsluiting van deelneming?	Ja. Kerncompetentie 3 betreft een minimumeis op het gebied van technische en beroepsbekwaamheid. Wanneer Gegadigde niet aantoont aan deze kerncompetentie te voldoen, leidt dit tot uitsluiting van verdere deelname aan de aanbestedingsprocedure. Gegadigde kan overeenkomstig paragraaf 3.3 een beroep doen op de bekwaamheid van een derde, onder de voorwaarden zoals verduidelijkt in het antwoord op vraag 11.
15	1	Inrichting en monitoring MDR	Nee	Bijlage G, Pagina 2	Is Microsoft Sentinel reeds ingericht of dient dit nog te gebeuren?	Microsoft Sentinel is reeds ingericht binnen de huidige omgeving. De Opdrachtgever sluit echter niet uit dat (delen van) de inrichting in het kader van deze opdracht worden herzien of opnieuw opgebouwd.
16	1	Inrichting en monitoring MDR	Nee	Bijlage G, Pagina 2	Kunt u toelichten welke logbronnen reeds zijn aangesloten?	De aangesloten logbronnen omvatten Entra ID (identity), Microsoft 365/cloud, servers, endpoints en Defender XDR. Deze leveren logging voor identity, devices en cloudactiviteiten binnen de Sentinel-omgeving.
17	1	Inrichting en monitoring MDR	Nee	Bijlage G, Pagina 2	Is Topdesk integratie reeds beschikbaar of dient deze gerealiseerd te worden?	Dient nog gerealiseerd te worden.
18	1	Inrichting en monitoring MDR	Nee	Selectieleidraad , Paragraaf 4, Pagina 22	Wat wordt verstaan onder "actieve detectie use-cases"?	Actieve detectie use-cases zijn in het SIEM ingerichte en draaiende detectieregels die automatisch afwijkend of dreigend gedrag signaleren en alerts of incidenten genereren op basis van logdata.
19	1	Inrichting en monitoring MDR	Nee	Selectieleidraad , Paragraaf 4, Pagina 22	Worden standaard use-cases (bijv. Microsoft) meegenomen?	Standaard use-cases mogen worden meegenomen, mits deze actief zijn geïmplementeerd, operationeel zijn en daadwerkelijk alerts genereren binnen het SIEM-platform.
20	1	Inrichting en monitoring MDR	Nee	Selectieleidraad , Paragraaf 4, Pagina 22	Hoe wordt "doorvertaling van red teaming naar detectie" beoordeeld?	Beoordeling ligt bij de CISO en de Pricavy Officer

21	1	Inrichting en monitoring MDR	Nee	Selectieleidraad, Paragraaf 4, Pagina 22	Wordt uitsluitend gemeentelijke ervaring geaccepteerd of bredere overheid?	Voorkeur gemeentelijk,
22	1	Inrichting en monitoring MDR	Nee	Selectieleidraad, Paragraaf 1.2.1, Pagina 6	Kunt u toelichten hoe de wachtkamerovereenkomst wordt toegepast?	Met de partij die de op één na beste inschrijving heeft gedaan wordt een wachtkamerovereenkomst gesloten. Deze partij moet er rekening mee houden dat ze de wachtkamerovereenkomst moet accepteren als ze tweede eindigen. Dit betekent dat deze partij de gestanddoeningstermijn van de inschrijving verlengt met de duur van de wachtkamerovereenkomst. Het accepteren van de wachtkamerovereenkomst houdt in dat deze partij voor een periode van X maanden na ingangsdatum van de overeenkomst gehouden is een overeenkomst te accepteren in het geval deze door ons, bij het wegvallen van de gegunde partij, wordt aangeboden. De wachtkamerovereenkomst treedt in werking op xx.xx en heeft een looptijd tot en met xx.xx
23	1	Inrichting en monitoring MDR	Nee	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?	Akkoord
24	1	Inrichting en monitoring MDR	Nee	32.5 GIBIT 2025	Bent u bereid deze verplichting te beperken voor zover het de ICT prestatie betreft? Gaat u hiermee akkoord? Zo niet, kunt u dit nader toelichten hoe u dit ziet?	Akkoord
25	1	Inrichting en monitoring MDR	Nee	29.4 GIBIT 2025	Leverancier acht het reëel dat tijdens het simuleren of daadwerkelijk verrichten van (delen) van het exit plan 1) de overeengekomen service levels niet van toepassing verklaard worden (louter op het simuleren van het exit-plan of daadwerkelijk verrichten van de in het plan beschreven werkzaamheden en dus niet op de primaire dienstverlening) 2) de verplichtingen van leverancier aangemerkt worden als inspanningsverplichtingen. Bent u bereid deze uitzonderingen op te nemen? Zo nee, waarom niet?	Akkoord
26	1	Inrichting en monitoring MDR	Nee	27.15 (nieuw) GIBIT 2025	Tekstvoorstel (toe te voegen aan artikel): "Indien Opdrachtgever op het moment van de ontbinding reeds prestaties ter uitvoering van de Overeenkomst heeft ontvangen, zullen deze prestaties en de daarmee samenhangende betalingsverplichtingen geen voorwerp van ongedaanmaking zijn. Bedragen die Leverancier vóór de ontbinding heeft gefactureerd in verband met hetgeen hij ter uitvoering van de overeenkomst reeds heeft verricht of geleverd, blijven onverminderd verschuldigd en worden op het moment van de ontbinding direct opeisbaar." Kunt u hiermee akkoord gaan? Zo nee, waarom niet?	Akkoord. Idd werkzaamheden/diensten die zijn verricht dan wel geleverd worden betaald.
27	1	Inrichting en monitoring MDR	Nee	27 lid 11 sub v GIBIT 2025	Kan Opdrachtgever ermee akkoord gaan om dit artikel uit te sluiten aangezien een verandering van zeggenschap geen invloed hoeft te hebben op het leveren van de afgesproken diensten? Zo nee, waarom niet?	Niet akkoord. Wij behouden ons het recht voor om de overeenkomst te ontbinden, indien een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming in onze optiek een onwenselijke uitwerking heeft op de uitvoering van de opdracht en/of er andere beletselen bestaan. Wij zullen van deze bevoegdheid geen gebruik maken als de wijziging onze belangen niet raakt.

28	1	Inrichting en monitoring MDR	Nee	27.2 GIBIT 2025	Kan Opdrachtgever ermee instemmen om de opzegtermijn van 3 maanden ook voor Leverancier te laten gelden? Zo nee, waarom niet?	Niet akkoord. Opdrachtgeven heeft voldoende tijd nodig om een nieuwe leverancier te selecteren. 18 maanden is misschien wat lang. 12 maanden zou voldoende zijn.
29	1	Inrichting en monitoring MDR	Nee	24.2 GIBIT 2025	Bent u bereid aan dit artikel toe te voegen: "indien Leverancier geen geschikt vervangend Personeel heeft binnen de onderneming van Leverancier en de kosten voor de inhuur van de vervanger wezenlijk hoger zijn, treden partijen in overleg."	Niet akkoord
30	1	Inrichting en monitoring MDR	Nee	24.1 GIBIT 2025	Bent u bereid aan dit artikel toe te voegen: "mits opdrachtgever daarbij schriftelijk gemotiveerd onderbouwt en kenbaar maakt aan Leverancier waarom deze persoon niet voldoet aan de overeengekomen kwalificaties" En kan Opdrachtgever toelichten wat zij bedoelt met de zinsnede 'om redenen in de persoon gelegen'?	Niet akkoord met aanpassing. Dit staat er al voldoende duidelijk. Met deze zinsnede wordt bedoeld dat Opdrachtgever niet tevreden is met inzet, kwaliteit of instelling van de persoon.
31	1	Inrichting en monitoring MDR	Nee	22.1 GIBIT 2025	Leverancier stelt voor de volgende zin aan dit artikel toe te voegen: "Deze verplichting ziet uitsluitend op de eigen gegevens van Opdrachtgever en niet op de onderliggende programmatuur, datamodellen, configuraties, algoritmes of overige knowhow van Leverancier." Kan Opdrachtgever daarmee akkoord gaan? Zo nee, waarom niet?	Niet akkoord, de GIBIT voorwaarden zijn paritair in samenwerking met marktpartijen door de VNG opgesteld. Wij zien geen aanleiding om deze aanvulling toe te voegen.
32	1	Inrichting en monitoring MDR	Nee	21.4 GIBIT 2025	Leverancier stelt voor om de volgende zin aan dit artikel toe te voegen: "Leverancier is gerechtigd generieke bouwstenen, componenten, algoritmes en methodieken die in het kader van de ontwikkeling zijn toegepast of ontstaan, te hergebruiken en te exploiteren ten behoeve van andere opdrachten en klanten." Kan Opdrachtgever daarmee akkood gaan? Zo nee, waarom niet?	Zolang voldoet aan regel- wetgeving en privacy, JP. Check GJ (gjt) Vóóraf niet akkoord. het betreft maatwerk, dus intelectueel eigendom van Opdrachtgever. Het staat Leverancier vrij hiertoe een verzoek in te dienen bij Opdrachtgever.
33	1	Inrichting en monitoring MDR	Nee	20.2 GIBIT 2025	Leverancier stelt voor deze bepaling aan te passen en alleen stakingen van Personeel niet onder de overmachtsgrond te laten vallen en verlate aanlevering uit het artikel te schrappen. Kan Opdrachtgever daarmee akkoord gaan? Zo nee, waarom niet?	Niet akkoord. Staking van personeel van Leverancier is géén overmacht. Evenals verlate aanlevering.
34	1	Inrichting en monitoring MDR	Nee	19.4 GIBIT 2025	Leverancier geeft er de voorkeur aan om vooraf om toestemming te worden gevraagd voor het delen van de inhoud van de Overeenkomst met de in dit artikel genoemde partijen. Kan Opdrachtgever ermee akkoord gaan dat dit artikel dienovereenkomstig wordt aangepast? Zo nee, waarom niet?	Niet akkoord. Opdrachtgever werkt veel samen met andere gemeenten. transparantie onderling is een basis hierbij.

35	1	Inrichting en monitoring MDR	Nee	14.3 GIBIT 2025	Dit artikel druist in tegen art. 25 AI-verordening. Een toezichthouder zal uitgaan van de feiten en niet van de contractuele kwalificatie (aanbieder, gerbuiksverantwoordelijke) die partijen zijn overeengekomen. Als Opdrachtgever het systeem wezenlijk wijzigt, herlabelt of voor een ander (hoog-risico) doel inzet, wordt hij naar de letter van de verordening aanbieder — ongeacht wat partijen afspraken. Daarnaast heeft Leverancier, in dit artikel, de plicht bepaalde handelingen van Opdrachtgever te voorkomen die Opdrachtgever als 'aanbieder' zouden kunnen kwalificeren. Die verantwoordelijkheid ligt primair bij Opdachtgever zelf, niet bij Leverancier. Leverancier kan in sommige gevallen misschien waarschuwen, maar de verantwoordelijkheid voor het herclassificeren van een AI-systeem door Opdrachtegever kan niet bij Leverancier worden gelegd. Bent u bereid dit artikel aan te passen als volgt: "De rolverdeling volgt de feitelijke taakverdeling en artikel 25 van Verordening (EU) 2024/1689. Indien Opdrachtgever door eigen handelen — waaronder wezenlijke wijziging, het aanbrengen van zijn naam of merk, of wijziging van het beoogde doel — als aanbieder kwalificeert, komt dit voor rekening en risico van Opdrachtgever. De zorgplicht van Leverancier strekt zich uit tot het verstrekken van adequate gebruiksaanwijzingen en waarschuwingen, en niet tot het voorkomen van handelingen van Opdrachtgever of de juridische gevolgen daarvan."	Opdrachtgever erkent dat de kwalificatie van partijen onder de AI-verordening wordt bepaald door de feitelijke omstandigheden en de toepasselijke wet- en regelgeving. Contractuele bepalingen kunnen deze wettelijke kwalificatie niet opzijzetten. Opdrachtgever acht het echter redelijk dat Leverancier, vanuit zijn expertise en kennis van het AI-systeem, Opdrachtgever tijdig informeert wanneer voorgenomen wijzigingen of gebruikswijzen mogelijk gevolgen hebben voor de kwalificatie van partijen onder de AI-verordening. De bepaling wordt daarom niet geschrapt. Wel verduidelijkt Opdrachtgever dat Leverancier niet verantwoordelijk wordt gehouden voor zelfstandige keuzes van Opdrachtgever die leiden tot een gewijzigde juridische kwalificatie onder de AI-verordening.
36	1	Inrichting en monitoring MDR	Nee	14.1-14.2/14/6 GIBIT 2025	De leden 1,2 en 6 van dit artikel differentieren niet naar risiconiveau van het AI-systeem. De zware verplichtingen die op grond van de AI-verordening (nauwkeurigheid/robuustheid art. 15, logging art. 12, , risicobeheer art. 9) gelden voor hoog-risico AI-systemen, bestrijken nu ook AI-systemen met een beperkt- en minimaal risico. Bent u bereid om deze differentiatie naar risiconiveau van het geleverde AI-systeem te maken in dit artikel en eerdergenoemde verplichtingen niet van toepassing te verklaren op AI-systemen met een beperkt- of minimaal risico? Zo nee, waarom niet?	Opdrachtgever begrijpt de opmerking van Inschrijver over de differentiatie naar risiconiveau binnen de AI-verordening. De betreffende bepalingen zijn echter bewust opgenomen om voldoende transparantie, controleerbaarheid, betrouwbaarheid en informatiebeveiliging te waarborgen binnen de dienstverlening. Deze bepalingen zijn daarom niet uitsluitend gekoppeld aan de kwalificatie "hoog-risico AI-systeem" onder de AI-verordening, maar vormen tevens contractuele kwaliteitseisen die Opdrachtgever noodzakelijk acht voor de uitvoering van de opdracht. Opdrachtgever handhaaft de bepalingen derhalve ongewijzigd.
37	1	Inrichting en monitoring MDR	Nee	13.3-13.5 GIBIT 2025	Leverancier stelt voor om een extra lid 6 aan dit artikel toe te voegen waarin het volgende wordt ogpenomen: "Informatieverstrekking zoals genoemd in bovenstaande leden 1 tot en met 5 vindt uitsluitend plaats voor zover dit commercieel en technisch verantwoord is en zonder dat daarmee intellectueel eigendom van Leverancier in gevaar wordt gebracht. Derden die toegang krijgen tot deze algoritmische informatie via Opdrachtgever zullen een geheimhoudingsplicht inachtenemen die tenminste even ver strekt als die van Opdrachtgever." Kan Opdrachtgever hiermee akkoord gaan? Zo nee, waarom niet?	Akkoord

38	1	Inrichting en monitoring MDR	Nee	13.1 GIBIT 2025	Leverancier is van mening dat de garanties over bias, nauwkeurigheid en rechtmatigheid begrijpelijk zijn vanuit ethisch oogpunt, maar strikte en potentieel onbeheersbare eisen opleggen aan de Leverancier. Bovendien is “nauwkeurigheid” moeilijk objectief te kwantificeren bij complexe AI- of data-analyses. Ook “rechtmatige verwerking” kan buiten de controle van de Leverancier vallen als data door Opdrachtgever wordt aangeleverd. Kan Opdrachtgever ermee akkoord gaan dat de volgende zinsnede aan dit artikel wordt toegevoegd: "....voor zover dit binnen de invloedssfeer van Leverancier ligt"? Zo nee, waarom niet?	Akkoord
39	1	Inrichting en monitoring MDR	Nee	11.2 GIBIT 2025	Deze bepaling omschrijft dat 30% van de kosten voor de implementatie pas na integrale Acceptatie in rekening gebracht kan worden. Voor de reste rende 70% van de eenmalige en periodieke vergoedingen worden in de Overeenkomst afspraken gemaakt. Leverancier stelt voor om vooraf duidelijke afspraken te maken over het gehele facturatieschema en stelt het volgende voor: - 35% bij opdrachtverlening (ondertekening van de overeenkomsten) - 35% na installatie - 30% na acceptatie of in gebruik name. Kunt u hiermee akkoord gaan? Zo nee, waarom niet?	Voor eenmalige kosten akkoord. Voor structurele kosten 100% vooruitbetaling per kalenderjaar en facturatie in het betreffende jaar.
40	1	Inrichting en monitoring MDR	Nee	4.1 GIBIT 2025	Tekstvoorstel: Leverancier zou graag volgende toevoegen:" In alle gevallen, derhalve ook indien partijen schriftelijk en uitdrukkelijk een vaste of fatale termijn zijn overeengekomen, komt Leverancier wegens tijdsoverschrijding eerst in verzuim nadat Opdrachtgever hem schriftelijk in gebreke heeft gesteld. " Bent u hiertoe bereid? Zo nee, waarom niet?	Niet akkoord. een fatale termijn is duidelijk.
41	1	Inrichting en monitoring MDR	Nee	Par 3.5 Better performance	De door u in dit kader gedeelde link vermeldt weinig over de in itiatiefnemers, de gebruikers of de voorwaarden van gebruik van deze kennisbank. Kunt u ingaan op deze vragen. Kunt u daarnaast aangeven hoe u borgt dat de procedures die leiden tot het opnemen van een vermelding eerlijk en objectief verlopen? Kunt u tenslotte aangeven gedurende welke termijn deze beoordelingen in deze database beschikbaar blijven en of u vindt dat de lokale overheid aangewezen / gerechtigd is om haar oordeel over leveranciers met een markt te delen.	Better Performance is hierbij n.v.t. en uit de leidraad verwijderd.
42	1	Inrichting en monitoring MDR	Nee	Par 3.5 Better performance	Uw toelichting geeft aan dat de werkelijke beoordeling van de opdrachtnemer, het invullen van het formulier en het opnemen van het ingevulde formulier in de database, pas aan de orde is na oplevering van de opdracht. Bedoelt u gezien de duur van de opdracht dus pas na 4, 6 of 8 jaar?	Zie antwoord vraag 41.
43	1	Inrichting en monitoring MDR	Nee	par 3.2.3.2 Kwaliteitsborging	Het is wat betreft Nis2 mogelijk om het geëiste te lezen als zou u Nis2 certificering vragen. We denken dat u bedoeld kennis van de NIs2 (aanstaande) wetgeving., Kunt u verduidelijken wat u op dit punt precies verlangt?	De Gegadigde dient aantoonbaar te maken dat wordt voldaan aan deze kaders, bijvoorbeeld via ISO/IEC 27001 en onderliggende maatregelen en documentatie. Gelijkwaardige bewijsmiddelen zijn toegestaan.
44	1	Inrichting en monitoring MDR	Nee	Par 3.2.2.2 Geconsolideerde jaarrekening	Gegadigde maakt deel uit van een groep met een geconsolideerde jaarrekening. We zullen derhalve de geconsolideerde jaarrekening met u delen en de garantstellingsverklaring invullen. Kunt u in dit kader aangeven of u in dit beschouwd als het doen van een beroep op de draagkracht van een derde en daarom ook een UEA veracht van het moederbedrijf?	Geen UEA wel een concernverklaring. Zie bijlage A. Vanuit de KvK zien wij hoe de structuur verloopt en in welke organisatievorm u inschrijft. Maakt u deel uit van een holding dan is een concernverklaring noodzakelijk.

45	1	Inrichting en monitoring MDR	Nee	Par 3.2.2.1 Beroeps/ bedrijfsaansprakelijkheidsverzekering	De gevraagde verzekering van gegadigde dekt 2,5 miljoen per gebeurtenis en 5 miljoen per jaar. Deze verzekerde bedragen zijn ruim voldoende voor alle aanbestedingen waar we aan deelnemen. Dit zijn met regelmaat grotere partijen dan de gemeente Katwijk. U vraagt een hogere dekking. Wij vragen u de verzekerde bedragen te verlagen tot 2 miljoen per gebeurtenis en 4 miljoen per jaar. Dit zijn meer proportionele bedragen.	Inschrijver dekt 1.250.000 per gebeurtenis van een maximaal tot 2 gebeurtenissen per jaar.
46	1	Inrichting en monitoring MDR	Nee	Subgunningscriteria	Indien u bijzonder hecht aan ervaring binnen de gemeentelijke overheid dan heeft u in de door u gevolgde procedure middels de door u te bepalen selectiecriteria in zekere mate de mogelijkheid om gegadigden te selecteren die deze ervaring hebben. Daarnaast kunt u dit opnemen in de gevraagde kerncompetenties. Uit de leidraad maken wij echter op dat dit soort ervaring onderdeel gaat zijn van de subgunningscriteria. Dit is ongebruikelijk en wij vinden deze noemer ook ongeschikt als subgunningscriterium. Hoewel wij het exacte subgunningscriterium in deze fase nog niet kennen denken wij dat het gevaar dreigt dat er een disproportionele kwaliteit wordt toegekend aan dienstverlening aan een specifiek deel van de overheid. Kunt u uw keuze voor een dergelijk subgunningscriterium toelichten met daarbij uitleg waarom de twee andere mogelijkheden die in deze vraag zijn genoemd voor u niet volstaan.	In de selectiefase zijn we op zoek naar partijen met ervaring binnen de gemeentelijke overheid en in de gunningsfase willen wij graag zien op welke manier de ervaring van de gemeentelijke overheid bijdraagt aan de uitvoering van deze opdracht.
47	1	Inrichting en monitoring MDR	Nee	Voorbehoud in de inleiding	De zin "Wij moeten eerst goedkeuring krijgen van een eindverantwoordelijke voordat de opdracht definitief kan worden gegund." staat hier enigszins onverwacht. Is er enige specifieke situatie waarom de door u bedoelde eindverantwoordelijke de uitkomst van de gevolgde procedure niet zou goedkeuren?	Dit is een Interne procedure en tekenbevoegdheid. Geen specifieke uitkomst. Mandaat van dergelijke bedragen ligt bij burgemeester en dergelijke aanbesteding dient voorngelegd te worden ter goedkeuring.
48	1	Inrichting en monitoring MDR	Nee	Netwerkmonitoring	De opdrachtbeschrijving (Bijlage G) definieert de scope van de dienstverlening als: "24/7 bewaking van endpoints, identiteiten, accounts en cloudomgeving". Netwerkdetectie wordt hierin niet genoemd. Het Programma van Eisen (Bijlage H, sectie 4) introduceert echter veertien uitgebreide eisen op het gebied van netwerkdetectie, inclusief fysieke sensorplaatsing op locatie. Kan worden bevestigd dat netwerkdetectie onderdeel uitmaakt van de opdracht, en zo ja, waarom is dit niet opgenomen in de opdrachtbeschrijving?	Ja, netwerkdetectie maakt onderdeel uit van de aanbesteding, staat in het PVE. Opdrachtomschrijving is een beknopte weergave.
49	1	Inrichting en monitoring MDR	Nee	Netwerkmonitoring	De opdrachtbeschrijving (Bijlage G) definieert de scope van de dienstverlening als: "24/7 bewaking van endpoints, identiteiten, accounts en cloudomgeving". Netwerkdetectie wordt hierin niet genoemd. Het Programma van Eisen (Bijlage H, sectie 4) introduceert echter veertien uitgebreide eisen op het gebied van netwerkdetectie, inclusief fysieke sensorplaatsing op locatie. Kan worden bevestigd dat netwerkdetectie onderdeel uitmaakt van de opdracht, en zo ja, waarom is dit niet opgenomen in de opdrachtbeschrijving?	Zie het antwoord op vraag 48. Dit ivm evt. verschuiving van regels of volgorde.
50	1	Inrichting en monitoring MDR	Nee	Eis 3.1, 3.2 en 3.3	Deze eisen gaan over auditlogging en accountbeheer, maar specificeren niet op welke systemen deze eisen van toepassing zijn. Hebben deze eisen betrekking op de MDR-tooling en het portaal van de opdrachtnemer, op de Microsoft Sentinel omgeving, of op alle systemen binnen de scope van de dienstverlening?	De eisen met betrekking tot auditlogging en accountbeheer (3.1 t/m 3.3) zijn van toepassing op alle systemen en componenten binnen de scope van de MDR-dienstverlening, voor zover deze worden ingezet ten behoeve van monitoring, detectie en response. Hieronder vallen in ieder geval de SIEM-omgeving (Microsoft Sentinel), relevante bron-systemen en de tooling en eventuele portalen van de opdrachtnemer.

51	1	Inrichting en monitoring MDR	Nee	GBIT2023 of 2025	Eis 2.7 van het Programma van Eisen (Bijlage H) verwijst naar GIBIT 2023, terwijl de selectieleidraad en de concept-overeenkomst (Bijlage E) verwijzen naar GIBIT 2025. Welke versie van de GIBIT is van toepassing op deze opdracht?	Het betreft de GIBIT 2025. Administratieve fout.
52	1	Inrichting en monitoring MDR	Nee	SRoI	Paragraaf 2.12 stelt dat de SRoI-verplichting van 1% wordt berekend over de totale opdrachtsom inclusief eventuele verlengingen. Aangezien de verlengingsopties (2x2 jaar) op het moment van inschrijving nog niet vaststaan, is de totale grondslag voor de berekening onbekend. Op basis van welk bedrag en op welk moment wordt de SRoI-verplichting vastgesteld?	De SRoI-verplichting wordt bij aanvang van de opdracht vastgesteld op basis van de opdrachtsom behorende bij de initiële contractduur van vier (4) jaar. Aangezien eventuele verlengingen op het moment van inschrijving nog niet zijn gegarandeerd, worden deze niet meegenomen in de initiële vaststelling van de SRoI-verplichting. Indien de opdrachtgever gebruikmaakt van één of meer verlengingsopties, wordt de SRoI-verplichting gedurende de looptijd van de overeenkomst naar rato verhoogd op basis van de omzet die voortvloeit uit de betreffende verlengingsperiode(n). De aanvullende SRoI-verplichting wordt vastgesteld op hetzelfde percentage als opgenomen in de aanbestedingsstukken en berekend over de gerealiseerde omzet van de verlenging(en).
53	1	Inrichting en monitoring MDR	Nee	Kerncompetentie 3	Kerncompetentie 3 vereist aantoonbare ervaring met het bewaken van Operationele Technologie (OT). Gemeente Katwijk beschrijft echter een volledig cloudgebaseerde omgeving met als voornaamste componenten Microsoft Azure, Microsoft 365 E5, Windows 365 en mobiele endpoints. Er worden geen OT-systemen zoals SCADA, ICS of andere industriële besturingsinfrastructuur vermeld in de opdrachtbeschrijving of andere documenten. Het komt ons daarom vreemd en niet-proportioneel voor dat OT vervolgens wel als eis wordt gesteld in de kerncompetentie. Kunt u het OT-deel van deze eis laten vervallen? Indien dat niet mogelijk is, kunt u dan toelichten welke specifieke OT-componenten of -omgevingen binnen de scope van deze opdracht vallen en wat u in deze context onder "Operationele Technologie" verstaat?	Niet akkoord. Aanbestedende Dienst handhaaft Kerncompetentie 3. Onder Operationele Technologie verstaat Aanbestedende Dienst in deze aanbesteding netwerkaangesloten technische systemen die fysieke processen, installaties of operationele voorzieningen bewaken, aansturen of ondersteunen. Referenties met betrekking tot bijvoorbeeld gebouwgebonden installaties, parkeersystemen, gemalen, verkeersregelinstallaties of vergelijkbare gemeentelijke technische of operationele IoT-omgevingen kunnen kwalificeren. Deze voorbeelden betreffen mogelijke referentieomgevingen en betekenen niet dat al deze systemen binnen de huidige opdracht aanwezig of in scope zijn. Er wordt geen ervaring met een specifieke industriële sector, een specifiek protocol of een omvangrijke SCADA-omgeving verlangd. De referentie hoeft niet betrekking te hebben op exact dezelfde technische omgeving als die van Aanbestedende Dienst. Uit de referentie moet duidelijk blijken dat gedurende minimaal twaalf maanden ervaring is opgedaan met het bewaken van operationele of technische systemen binnen SIEM-/SOC-dienstverlening, inclusief gegevensbeveiliging. Reguliere IT- of cloudmonitoring zonder aantoonbare OT- of operationele IoT-component is hiervoor onvoldoende. Voor het voldoen aan KC3 mag overeenkomstig paragraaf 3.3 een beroep worden gedaan op de bekwaamheid van een derde.
54	1	Inrichting en monitoring MDR	Nee	Art 32.5 GIBIT 2025	Deze bepaling bevat een RTO en RPO voor data. Inschrijver acht deze bepaling echter niet van toepassing omdat niet sprake is van een gewone SaaS-dienst waarbij de back-up verantwoordelijkheid bij leverancier ligt. Inschrijver stelt derhalve voor om dee bepaling buiten toepassing te verklaren. In het geval Aanbestedende Dienst van oordeel is dat deze bepaling wel degelijk van toepassing is, is het verzoek om dan toe te lichten op welke data en systemen deze bepaling van toepassing is.	Niet akkoord, artikel blijft van toepassing en heeft betrekking op alle verzamelde data.
55	1	Inrichting en monitoring MDR	Nee	Artikel 28 GIBIT 2025	Inschrijver zou graag willen voorstellen de volgende nadere inkadering voor audits op te nemen: a) maximaal 1 audit per jaar, die b) tenminste 60 dagen van tevoren wordt aangekondigd, tenzij een toezichthouder een kortere termijn vereist, en c) dat auditors geheimhoudingsverplichtingen ondertekenen met Inschrijver die ten minste gelijkwaardig zijn aan art. 19 GIBIT, en (d) tot slot voor zover de audit daarop ziet dat deze uitsluitend plaatsvindt in een daarvoor bestemde testomgeving en niet in de productieomgeving van het SOC van Inschrijver, om verstoring van dienstverlening aan overige klanten te voorkomen. Kan Aanbestedende Dienst daarmee instemmen?	Aanbestedende Dienst kan niet instemmen met het voorstel en handhaaft artikel 28 GIBIT onverkort. Het auditrecht is essentieel voor informatiebeveiliging en compliance; generieke beperkingen op frequentie, aankondiging of scope worden niet aanvaard. Audits moeten te allen tijde mogelijk zijn, indien nodig ook in de productieomgeving. Uiteraard wordt dit recht redelijk en in overleg toegepast.

56	1	Inrichting en monitoring MDR	Nee	Art. 25 GIBIT 2025	Kan Aanbestedende Dienst verduidelijken op welke wijze Inschrijver een Software bill of materials moet aanleveren, op welk moment, en op welk deel van de ICT prestatie dit dan moet zien?	Kan vervallen.
57	1	Inrichting en monitoring MDR	Nee	Art. 20.2 GIBIT 2025	Inschrijver verzoekt Aanbestedende Dienst om te verduidelijken dat een cyberaanval op de eigen infrastructuur van inschrijver (bijv. een supply-chain-aanval op Tesorions SOC-platform) eveneens als overmacht kwalificeert. Kunt u dit bevestigen?	Aanbestedende Dienst kan hier niet op voorhand mee instemmen. Of sprake is van overmacht dient per geval te worden beoordeeld op basis van artikel 20 GIBIT. Een cyberaanval op de infrastructuur van de opdrachtnemer kwalificeert niet automatisch als overmacht, mede gelet op de verantwoordelijkheid van opdrachtnemer voor passende beveiligingsmaatregelen.
58	1	Inrichting en monitoring MDR	Nee	Art. 19.3 GIBIT 2025	Inschrijver vindt een contractuele boete niet passend binnen de samenwerking die partijen beogen. Is Aanbestendende Dienst bereid deze buiten toepassing te verklaren?	Artikel 19.3 gaat over geheimhouding en niet over een boete
59	1	Inrichting en monitoring MDR	Nee	Art. 17.5 Gibit 2025	(a) Inschrijver verzoekt Aanbestedende Dienst om te verduidelijken dat art. 17.5 sub iv (doorwerking van toezichthoudersboetes) uitsluitend van toepassing is als de boete opgelegd aan de Aanbestedende Dienst rechtstreeks verband houdt met een aantoonbare tekortkoming van Tesorion, en niet geldt als de Aanbestedende Dienst door haar eigen handelen als verwerkingsverantwoordelijke een boete ontvangt waaraan Tesorion geen of slechts deels verwijt treft. (b)Voorts verzoekt inschrijver Aanbestedende Dienst om te bevestigen dat de aansprakelijkheidslimieten van art. 17.3 en 17.4 ook van toepassing zijn op schade die voortvloeit uit een beveiligingsincident waarbij Tesorion als SOC-dienstverlener niet tijdig heeft gedetecteerd, zodat het commercieel risico voor inscrhijver proportioneel is ten opzichte van de overeengekomen vergoeding (dit betreffen immers situaties die onder de reguliere dienstverlening vallen en derhalve ook in aanmerking dienen te komen voor de aansprakelijkheidsbeperking, zodat inschrijver zich ook daartegen kan verzekeren.	Wij kunnen bevestigen dat het boetes dienen te betreffen die te wijten zijn aan leverancier. De aansprakelijkheidsbeperkingen zijn niet van toepassing indien er sprake is van 1 van de gevallen zoals genoemd in artikel 17.5 Gibit.
60	1	Inrichting en monitoring MDR	Nee	Art. 17.3 en 17.4 GIBIT 2025	Inschrijver wijst erop dat het budget voor de aanbesteding relatief beperkt is en dat de totale aansprakelijkheid per jaar voor zaakschade en overige schade daarmee in disproportionele verhouding staat tot de jaarvergoeding. In dat kader wijst Inschrijver erop dat Aanbestedende Dienst op grond van de gids proportionaliteit ook is gehouden om rekening te houden met de risico's die de aanbestedende dienst daadwerkelijk loopt en de gebruikelijke aansprakelijkheidseis in de betreffende branche of voor de betreffende opdracht naar aard en omvang. In dat kader is van belang dat een gangbare aansprakelijkheidsbeperking in de IT-markt 1x ACV per contractjaar betreft, alsmede dat indirecte schade, gederfde winst en omzetverlies, vertragingsschade en gevolgschade volledig zijn aangesloten. In dat kader kan Inschrijver als middenweg Art. 17.4 GIBIT 2025 accepteren, maar stelt zij voor om het begrip zaakschade uit 17.3 te verwijderen (en deze bepaling dus enkel op persoonsschade te laten zien) en daarnaast om een aanvullende bepaling op te nemen waarmee indirecte schade, gevolgschade, gederfde winst en verlies van omzet, alsmede vertragingsschade volledig is uitgesloten. Kan Aanbestedende Dienst daarmee instemmen? Zo nee, waarom niet?	Niet akkoord, betreft geen disproportionele dan wel onbeperkte aansprakelijkheid. Daarnaast blijven de bepalingen van het Burgerlijk Wetboek (zoals Boek 6 over schadevergoeding) onverkort van toepassing .

61	1	Inrichting en monitoring MDR	Nee	Art 14.8 GIBIT 2025	Inschrijver stelt voor om de bijstandsplicht nader in te kaderen door op te nemen dat inschrijver gehouden is om "redelijke medewerking" te verlenen. Kan Aanbestedende Dienst dit toevoegen?	Akkoord
62	1	Inrichting en monitoring MDR	Nee	Art 14.4 GIBIT 2025	Inschrijver stelt voorop dat de interpretatie van de AI-verordening nog in ontwikkeling is (er is nog nauwelijks jurisprudentie). Op basis van eigen beoordelingen komt Inschrijver tot de conclusie dat door haar gehanteerde AI-systemen geen hoog risico zijn. Deze conclusie kan echter in de toekomst veranderen op basis van gewijzigde inzichten en ontwikkelingen in wetgeving en jurisprudentie. Kan daarom worden toegevoegd dat een gewijzigde classificatie achteraf binnen redelijke termijn door Leverancier moet worden gemeld?	Akkoord
63	1	Inrichting en monitoring MDR	Nee	Art 14.1 GIBIT 2025	Inschrijver stelt voor dat "menselijk toezicht" voor geautomatiseerde response-acties gezien de aard van de dienstverlening wordt ingevuld als (i) mogelijkheid tot achteraf-audit van elke geautomatiseerde actie, (ii) configureerbare drempelwaarden voor autonome actie overeengekomen in de SLA, en (iii) een eventuele escalatieprocedure. De praktijk van de MDR/SOC-dienstverlening is namelijk dat er binnen vooraf afgestemde kaders steeds meer zal worden toegewerkt naar geautomatiseerde response (bijv. automatische isolatie van een endpoint door SOAR). Menselijk toezicht vóóraf is dan operationeel onhaalbaar. Kan Aanbestedende DIenst hiermee instemmen?	Niet akkoord, artikel geeft aan dat menstelijk toezicht mogelijk moet zijn.
64	1	Inrichting en monitoring MDR	Nee	Art. 13.3 GIBIT 2025	Inschrijver wijst erop dat Detectie-algoritmen in productie (ML-gebaseerde anomaly detection, behavioral analytics) vaak niet volledig explaineerbaar zijn op individueel niveau. Daarnaast kan Inschrijver niet toezeggen dat een specifieke detectiegebeurtenis volledig wordt geanalyseerd door middel van een forensische constructie zonder dat dit extra kosten geeft. Immers, dit is normaliter onderdeel van aanvullende Cert-dienstverlening die Aanbestedende Dienst in dat geval kan afnemen. Inschrijver stelt derhalve voor dat de individuele uitlegplicht beperkt is tot gevallen waarbij de algoritmische toepassing direct ten grondslag heeft gelegen aan een beslissing die de Opdrachtgever heeft genomen met rechtsgevolgen voor derden. Is dit akkoord voor Aanbestedende Dienst?	Niet akkoord. triggert om extra dienstverlening af te nemen. dit willen we juist niet.
65	1	Inrichting en monitoring MDR	Nee	Art. 13.2 GIBIT 2025	De aard van de dienstverlening kan met zich meebrengen dat specifieke treath intel informatie gedeeld moet worden met o.a. NCSC en andere partijen die lid zijn van het Cyclotronprogramma als onderdeel van het nationale programma om onze nationale cyberveiligheid te bevorderen . Deze intel kan niet gepseudo- of anonimiseerd worden, omdat het nu juist gaat om de intel zelf. Daarmee is het ook niet mogelijk om volledig uit te sluiten dat deze informatie tot gemeente Amsterdam te herleiden valt. Wel kan zij deze toezegging doen voor zover het persoonsgegevens betreft van gemeente Katwijk. Kan Aanbestedende Dienst bevestigen dat dit in het kader van deze bepaling voldoende is?	Voor verplicht verstrekken van informatie aan o.a. NCSC of rechtbank vervalt de verplichting voor het niet herleidbaar zijn. Voor eigen gebruik van Levancier blijft de verplichting wel in stand.

66	1	Inrichting en monitoring MDR	Nee	Art. 13.1 GIBIT 2025	De garantie in artikel 13.1 kan niet onbeperkt van aard zijn. Deze is immers ook in grote mate afhankelijk van de kwaliteit van data die van Aanbestedende Dienst wordt verkregen via de relevante koppelingen. Nauwkeurigheid is daarmee onhoudbaar als resultaatsverbintenis. Bovendien is deze bij de te leveren dienstverlening in feite al gekoppeld aan de Service Levels die partijen zullen afspreken in de SLA. Kan derhalve worden toegevoegd dat deze nauwkeurigheid wordt bepaald aan de hand van de nader overeen te komen Service Levels en dat het een inspanningsverbintenis betreft voor zover het gaat om factoren die van invleod kunnen zijn maar buiten de invloedssfeer van inschrijver liggen?	Akkoord
67	1	Inrichting en monitoring MDR	Nee	GIBIT 2025, art. 10.11	Inschrijver stelt voor om op te nemen dat van meerdere malen van overschrijding van hetzelfde Service Level als genoemd in dit artikel sprake is bij 3 achtereenvolgende overschrijdingen. Daarnaast stelt inschrijver voor om gezein de aard van de dienstverlening op te nemen dat artikel 10.11 uitsluitend ziet op incidenten die als p1 of p2 kwalificeren (en dus serieuze dreiging vormen). Kan Aanbestedende Dienst hiermee instemmen?	Niet akkoord. Dit geldt voor alle Service Levels
68	1	Inrichting en monitoring MDR	Nee	GIBIT 2025, art. 7	Kunt u bevestigen dat deze coördinatieverplichting en verantwoordelijkheid zich uitsluitend uitstrekt tot derde partijen die door Inschrijver zelf worden ingeschakeld bij de levering van de diensten?	Akkoord
69	1	Inrichting en monitoring MDR	Nee	GIBIT 2025, art. 4.3	Inschrijver verzoekt Aanbestedende Dienst om te bevestigen dat de fatale termijn van art. 4.3 in de context van NIS2-implementatie (Cyberbeveiligingswet) en de AI Act uitsluitend geldt voor de specifieke onderdelen van de ICT Prestatie die rechtstreeks worden geraakt door de nieuwe wetgeving, en niet voor de gehele SOC/MDR-dienstverlening, alsmede dat Inschrijver recht heeft op redelijke aanpassingstermijn indien de bevoegde toezichthouder nadere guidance uitvaardigt. De Cyberbeveiligingswet (implementatie NIS2) en de AI Act bevatten verplichtingen die geleidelijk in werking treden en waarover toezichthouders (NCSC, Rijksinspectie Digitale Infrastructuur, AP) nog nadere invulling geven. Als de fatale termijn van art. 4.3 breed wordt uitgelegd, kan iedere wetswijziging op het snijvlak van cybersecurity en AI een automatische fatale deadline voor Inschrijver creëren, ook als de concrete verplichting door toezichthouders nog niet is geconcretiseerd. Inschrijver stelt voor om voor zover van belang na gunning te definiëren welke onderdelen van de ICT-prestatie mogelijk worden geraakt door veranderende wet- en regelgeving. Kunt u hiermee akkoord gaan?	Aanbestedende Dienst stemt deels in. Art. 4.3 geldt alleen voor onderdelen die direct door wetgeving worden geraakt; bij nadere invulling door toezichthouders wordt een redelijke implementatietermijn gehanteerd. Generiek uitsluiten of uitstellen wordt niet geaccepteerd.
70	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 10.4	Kan Aanbestedende Dienst bevestigen dat de softwareproviders voor de dienst op afstand (zoals MS of andere softwareaanbieders) in dit kader niet vallen onder de definitie van ingeschakelde derden?	Aanbestedende Dienst bevestigt dat standaard softwareproviders (zoals Microsoft) in beginsel niet worden aangemerkt als door opdrachtnemer ingeschakelde derden in de zin van deze bepaling, voor zover zij generieke (SaaS-)diensten leveren en geen directe rol hebben in de uitvoering van de dienstverlening. Indien dergelijke partijen echter specifiek door opdrachtnemer worden ingezet voor de uitvoering van de dienstverlening, kunnen zij wél als ingeschakelde derden worden beschouwd.
71	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 9.4	In de conceptovereenkomst artikel 3.4 hanteert u geen termijn van 3 maanden na start implementatie, maar een fatale datum. Dit betreffen daarmee twee verschillende parameters en deze kunnen ook gaan schuiven. Kan Aanbestedende Dienst aangeven welke voor haar leidend is en die als uitsluitende fatale termijn opnemen?	3 maanden na startdatum.

72	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 7.23	Inschrijver hanteert beleid dat van klanten met wie het contract eindigt, de eventuele incidentdata nog maximaal een jaar beschikbaar blijft. Het kan namelijk zijn dat een ex-klant op een later moment nog vragen heeft omdat dergelijke incidenten soms ook achteraf relevant kunnen zijn. Kan Aanbestedende Dienst de eis aanpassen en bevestigen dat deze werkwijze voor haar akkoord is?	Eis 7.23 bestaat niet. Inschrijver bedoelt waarschijnlijk eis 7.3. Eis 7.3 wordt aangepast voor de termijn van 1 jaar ná einde overeenkomst. Dit dient in het exitplan te worden opgenomen.
73	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 6.22	Inschrijver wil binnen afzienbare termijn false positives volledig met AI afhandelen (uiteraard binnen bepaalde voorafgestelde kaders en met controlemogelijkheid achteraf). Dit komt de effectiviteit en kwaliteit van de dienstverlening ten goede omdat onze analisten daardoor niet meer handmatig false positives hoeven af te handelen. Kunt u bevestigen dat deze werkwijze acceptabel is binnen de gestelde eis? Kunt u daarbij bevestigen dat dergelijke modellen (en alle daaraan gerelateerde IE-rechten volledig aan inschrijver toebehoren?	Aanbestedende Dienst kan gedeeltelijk instemmen. Het verder automatiseren van de afhandeling van false positives met AI is toegestaan, mits wordt voldaan aan de gestelde randvoorwaarden, waaronder menselijke controle waar nodig, transparantie en aantoonbare kwaliteit van de dienstverlening. Ten aanzien van intellectuele eigendomsrechten geldt dat deze in beginsel bij de inschrijver kunnen blijven, voor zover geen sprake is van specifiek voor Aanbestedende Dienst ontwikkelde onderdelen of afwijkende afspraken in de overeenkomst.
74	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 2.7	In de conceptovereenkomst wordt de GIBIT 2025 van toepassing verklaart. Inschrijver stelt voor om 1 regime van inkoopvoorwaarden van toepassing te laten zijn en in dat kader aan te sluiten bij de GIBIT 2025. Is dit akkoord?	Het moet GIBIT 2025 zijn. Eis 2.7 wordt hierop aangepast
75	1	Inrichting en monitoring MDR	Nee	bijlage H, eis 1.4	In deze eis lijkt sprake te zijn van een verschrijving met de verwijzing naar SOC2 bij ISO 27001. Dit betreffen namelijk verschillende certificeringen. Kan Aanbestedende Dienst deze eis verduidelijken? In het geval dat ook een SOC2 verklaring is vereist, gaat Inschrijver er vanuit dat ook een gelijkwaardige verklaring akkoord is. Kunt u dit bevestigen?	Aanbestedende Dienst verduidelijkt dat het ISO/IEC 27001-certificaat de primaire eis betreft. De verwijzing naar SOC2 of TPM heeft betrekking op aanvullende assurance. Indien een SOC2-verklaring wordt overgelegd, wordt een gelijkwaardige (derden)verklaring eveneens geaccepteerd, mits deze aantoonbaar een vergelijkbaar niveau van assurance biedt.
76	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 10.2	De Oplossing die inschrijver wenst aan te bieden maakt het mogelijk dat data in beginsel binnen de tenant van de Aanbestedende Dienst zal blijven. Derhalve is het voor inschrijver onduidelijk wat Aanbestedende Dienst bedoelt met het maken van een back-up van de Data. Inschrijver stelt voor dat Aanbestedende Dienst een nadere definitie van het begrip Data geeft dat passend is voor deze Aanbesteding.	Aanbestedende Dienst verduidelijkt dat onder “Data” wordt verstaan: alle gegevens die in het kader van de dienstverlening worden verwerkt, waaronder logdata, detectie- en incidentgegevens en configuratiegegevens. Ook indien data primair binnen de tenant van Aanbestedende Dienst blijft, kan het maken van back-ups of het waarborgen van recoverability onderdeel zijn van de dienstverlening. Een nadere uitwerking hiervan kan in overleg worden vastgesteld.
77	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 8.6	Inschrijver acht het redelijk dat bij eventuele afstemming van Service Credits deze dan ook in mindering worden gebracht op een eventuele schadevergoeding waarop Aanbestedende Dienst in een bepaald geval recht heeft. Kan Aanbestedende Dienst dit toevoegen?	Akkoord
78	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 7.2	Kan Aanbestedende Dienst toelichten wat zij precies bedoelt met een test/acceptatieomgeving? In de regel wordt de acceptatie namelijk uitgevoerd op de geïmplementeerde en reeds geactiveerde dienst op afstand.	Aanbestedende Dienst verduidelijkt dat met een test-/acceptatieomgeving wordt bedoeld een situatie waarin de dienstverlening zodanig kan worden beoordeeld dat de werking aantoonbaar kan worden vastgesteld. Indien een separate test-/acceptatieomgeving niet beschikbaar is, kan acceptatie plaatsvinden op de (geactiveerde) productieomgeving, mits dit op zorgvuldige wijze gebeurt en geen onaanvaardbare verstoring van de dienstverlening veroorzaakt. Wij zullen geen gebruik maken van een test/acceptatieomgeving.

79	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 6.1-6.2	Kan Aanbestedende Dienst aangeven welke onderdelen van de Gemeentelijke Kwaliteitsnormen zoals in deze artikelen opgenomen specifiek moeten worden nagekomen? En hoe gaat Aanbestedende Dienst om met verschillen tussen eisen vanuit de kwaliteitsnormen en het PVE? In rangorde prevaleren immers de kwaliteitsnormen met opname ervan in de overeenkomst.	Aanbestedende Dienst bevestigt dat de relevante Gemeentelijke Kwaliteitsnormen van toepassing zijn voor zover deze van toepassing zijn op de aard van de ICT-prestatie. Bij eventuele tegenstrijdigheden tussen het PvE en de kwaliteitsnormen prevaleert de meest specifieke en voor de dienstverlening zwaarstwegende bepaling, waarbij uitgangspunt is dat aan beide kaders in samenhang wordt voldaan.
80	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 3.4	Inschrijver wijst erop dat het behalen van een fatale termijn in belangrijke mate ook afhankelijk is van de medewerking door Aanbestedende Dienst. Inschrijver komt regelmatig tegen dat er na gunning van de aanbesteding soms zelfs nog geen projectorganisatie is ingericht door de Aanbestedende Dienst, of dat er geen capaciteit is en dus onbekend is wanneer de Aanbestedende Dienst aan haar zijde kan starten. Inschrijver wenst derhalve graag op te nemen in deze bepaling dat iedere vertraging aan de zijde van Aanbestedende Dienst niet aan opdrachtnemer kan worden toegerekend en naar rato bij de fatale termijn dient te worden opgeteld. Kan Aanbestedende Dienst daarmee instemmen?	Akkoord
81	1	Inrichting en monitoring MDR	Nee	Bijlage E Concept Gibit overeenkomst, Art 1.5	Inschrijver kan een deel van de rangorde tussen de documenten begrijpen en stemt daar ook mee in. Inschrijver wijst er echter op dat antwoorden in de NVI's in beginsel dienen te prevaleren boven o.a. de standaardvoorwaarden en het PVE. Inschrijver stelt derhalve voor om de volgende rangorde te hanteren: A. De Service Level Agreement (SLA); B. de Verwerkersovereenkomst; C. het Exit-plan; D. de Overeenkomst; E. de Nota van Inlichtingen (NvI) d.d. 1 juni 2026; F. het ingevulde Programma van Eisen (PvE); G. het Bestek; H. de offerte/inschrijving (<>); I. de Inkoopvoorwaarden; J. Verslag verificatiegesprek. Kan Aanbestedende Dienst daarmee instemmen?	Niet akkoord. De volgorde dient echter wel aangepast te worden in: A. het Verslag verificatiegesprek B. de Service Level Agreement (SLA); C. de Verwerkersovereenkomst; D. het Exit-plan; E. de Overeenkomst; F. de Nota(s) van Inlichtingen; G. het ingevulde Programma van Eisen (PvE); H. het Bestek; I. de GIBIT 2025 voorwaarden; J. de Offerte/inschrijving;
82	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 6.16 wordt gesteld dat de Opdrachtnemer de Opdrachtgever binnen één dag informeert over nieuwe kwetsbaarheden in hard- en software die bij de gemeente in gebruik zijn. Gegadigde merkt op dat het kunnen voldoen aan deze eis veronderstelt dat er een volledig en actueel overzicht (bijvoorbeeld een CMDB) beschikbaar is van de ICT-omgeving van de Opdrachtgever. Dergelijke activiteiten maken in de praktijk veelal onderdeel uit van een Vulnerability Management-dienstverlening. Kan de Aanbestedende Dienst bevestigen of een dergelijke dienstverlening (inclusief het beschikken over een volledig en actueel omgevingsinzicht) onderdeel is van de scope van de opdracht?	Aanbestedende Dienst bevestigt dat geen volledige vulnerability management-dienstverlening wordt verlangd. Opdrachtnemer wordt geacht relevante kwetsbaarheden te signaleren op basis van de overeengekomen scope en beschikbare informatie over de omgeving, zonder dat een volledige en actuele CMDB wordt vereist.

83	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	Gegadigde gaat ervan uit dat de Aanbestedende Dienst gelijkwaardige invullingen van de gestelde eisen toestaat, waarbij verschillende technische benaderingen – zoals deep packet inspection en AI-gebaseerde gedragsanalyse – als functioneel equivalent kunnen worden beschouwd. Kan de Aanbestedende Dienst bevestigen dat dergelijke alternatieve technische oplossingen zijn toegestaan, mits de gevraagde use-cases aantoonbaar en effectief worden gedetecteerd?	Aanbestedende Dienst bevestigt dat alternatieve technische oplossingen zijn toegestaan, mits de gevraagde functionaliteit en use-cases aantoonbaar en effectief worden gerealiseerd en voldoen aan de gestelde eisen.
84	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.1 worden eisen gesteld ten aanzien van OT/IoT-detectie. Gegadigde gaat ervan uit dat het doel van deze eis is om afwijkingen en risico's binnen OT/IoT-omgevingen effectief te detecteren, ongeacht de onderliggende techniek. Kan de Aanbestedende Dienst bevestigen dat deze detectie gerealiseerd mag worden via passieve netwerkobservatie en gedragsanalyse, zonder dat deep protocol inspection van alle industriële protocollen vereist is, mits afwijkingen en risico's aantoonbaar worden gedetecteerd?	Aanbestedende Dienst bevestigt dat eis 4.1 functioneel moet worden geïnterpreteerd. Passieve netwerkobservatie, flow- of metadata-analyse en gedragsanalyse zijn toegestaan. Deep protocol inspection van alle mogelijke industriële protocollen wordt niet voorgeschreven. De gekozen oplossing moet risico's en afwijkingen binnen de in scope zijnde technische en operationele netwerkzones en, voor zover aanwezig, OT-/IoT-zones aantoonbaar effectief kunnen detecteren, zonder onaanvaardbare verstoring of performance-impact. De exacte detectiemethode wordt tijdens de implementatiefase afgestemd op de daadwerkelijk aanwezige componenten en netwerkarchitectuur.
85	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.11 wordt gesteld dat de netwerkdetectie geen performance-impact mag hebben op de omgeving van de Opdrachtgever. Gegadigde gaat ervan uit dat het doel van deze eis is om verstoring van de operationele netwerkprestaties te voorkomen. Kan de Aanbestedende Dienst bevestigen dat oplossingen die zonder inline inspectie functioneren, bijvoorbeeld op basis van metadata-analyse en virtuele sensoren, en daarmee geen directe impact op het netwerkverkeer veroorzaken, als passend worden beschouwd binnen deze eis?	Aanbestedende Dienst bevestigt dat oplossingen zonder inline inspectie (zoals metadata-analyse en virtuele sensoren) zijn toegestaan, mits geen negatieve impact op het netwerk ontstaat en de gevraagde detectie aantoonbaar wordt gerealiseerd.
86	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.2 en 4.13 worden vereisten gesteld ten aanzien van detectie van onder andere laterale beweging en misbruik van accounts. Gegadigde merkt op dat de effectiviteit van dergelijke detecties kan worden vergroot door de combinatie van netwerkdetectie met identity-context (bijvoorbeeld integratie met Entra ID/Active Directory). Kan de Aanbestedende Dienst bevestigen dat oplossingen waarin netwerkdetectie wordt gecombineerd met identity-context als een passende invulling van de gevraagde NDR-functionaliteit worden beschouwd en als meerwaarde worden gezien?	Aanbestedende Dienst bevestigt dat het combineren van netwerkdetectie met identity-context (zoals Entra ID/Active Directory) wordt beschouwd als een passende en waardevolle invulling van de gevraagde functionaliteit, mits de gevraagde detecties aantoonbaar effectief worden gerealiseerd.
87	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.5 worden zowel flow-based data (zoals NetFlow/IPFIX) als deep packet analyse genoemd. Gegadigde gaat ervan uit dat het doel van deze eis is om adequate detectiecapaciteit te waarborgen, ongeacht de onderliggende techniek. Kan de Aanbestedende Dienst bevestigen dat een oplossing die primair gebruikmaakt van flow- en metadata-analyse, aangevuld met contextuele verrijking (zoals identity- en cloudinformatie), als gelijkwaardig wordt beschouwd aan oplossingen gebaseerd op full packet capture?	Aanbestedende Dienst bevestigt dat oplossingen gebaseerd op flow- en metadata-analyse, eventueel aangevuld met contextuele verrijking, als gelijkwaardig worden beschouwd aan full packet capture, mits de gevraagde detectiecapaciteit aantoonbaar effectief wordt gerealiseerd

88	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.3 worden meerdere vereisten gesteld met betrekking tot het detecteren van afwijkend gedrag, zoals C2-beaconing, laterale beweging en data-exfiltratie. Gegadigde merkt op dat dergelijke detecties in de praktijk op verschillende wijzen kunnen worden gerealiseerd. Kan de Aanbestedende Dienst bevestigen dat deze detecties ook mogen worden ingevuld door middel van AI- en machine learning-gebaseerde gedragsanalyse, en niet uitsluitend via signature-based of deep packet inspection-technieken?	Aanbestedende Dienst bevestigt dat AI- en machine learning-gebaseerde gedragsanalyse is toegestaan, mits de gevraagde detecties aantoonbaar en effectief worden gerealiseerd. Gebruik van uitsluitend signature-based of deep packet inspection-technieken is niet vereist.
89	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.3 wordt gevraagd naar detectie van versleuteld verkeer, onder meer via technieken zoals JA3/JA3S en metadata-analyse. Gegadigde gaat ervan uit dat een oplossing die zonder decryptie, op basis van metadata, machine learning en gedragsanalyse afwijkingen in versleuteld verkeer detecteert, eveneens voldoet aan het doel van deze eis. Kan de Aanbestedende Dienst bevestigen dat deze interpretatie juist is?	Aanbestedende Dienst bevestigt dat detectie van versleuteld verkeer zonder decryptie, op basis van metadata, machine learning en gedragsanalyse, is toegestaan, mits afwijkingen en risico's aantoonbaar effectief worden gedetecteerd.
90	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.5 wordt gesproken over "minimal PCAP capture" bij verdachte netwerkflows. Kan de Aanbestedende Dienst bevestigen dat dit wordt bedoeld als een optionele functionaliteit die wordt ingezet op basis van specifieke detectietriggers? Gegadigde gaat ervan uit dat een oplossing die primair gebruikmaakt van netwerkmetadata en flow-gebaseerde analyse (zoals IPFIX/NetFlow), in combinatie met gedragsanalyse, eveneens voldoet aan deze eis. Kan de Aanbestedende Dienst bevestigen dat deze interpretatie juist is?	Aanbestedende Dienst bevestigt dat "minimal PCAP capture" wordt bedoeld als gerichte functionaliteit op basis van detectietriggers. Een oplossing die primair gebruikmaakt van flow- en metadata-analyse voldoet, mits de gevraagde detectiecapaciteit aantoonbaar effectief wordt gerealiseerd.
91	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 4.1 wordt gevraagd om netwerkdetectie over alle relevante zones, waaruit Gegadigde afleidt dat Network Detection & Response (NDR) onderdeel is van de gevraagde dienstverlening. Voor het kunnen opstellen van een adequate en onderbouwde prijsstelling constateert Gegadigde dat nadere informatie ontbreekt. Kan de Aanbestedende Dienst inzicht geven in: - het aantal actieve IP-adressen dat binnen de scope van de NDR-dienstverlening valt; - het aantal fysieke locaties dat binnen de scope van de NDR-dienstverlening valt? Gegadigde verzoekt de Aanbestedende Dienst deze gegevens te verstrekken.	Aanbestedende Dienst bevestigt dat netwerkdetectie onderdeel uitmaakt van de gevraagde dienstverlening. Het exacte aantal gelijktijdig actieve IP-adressen is niet bekend en kan fluctueren, onder andere door het gebruik van mobiele apparatuur, dynamische IP-adressering en wijzigingen in de infrastructuur. Aanbestedende Dienst kan daarom geen betrouwbare aantallen verstrekken. Voor de fysieke inrichting dient Gegadigde rekening te houden met de centrale on-premises netwerkomgeving en de parkeergarage. Daarnaast valt de Azure-omgeving binnen de scope van de dienstverlening. Azure wordt hierbij niet als fysieke locatie aangemerkt. Gegadigde dient voor de prijsstelling uit te gaan van de in de aanbestedingsstukken beschreven ICT-omgeving en van netwerkdetectie op alle relevante netwerkzones. De exacte netwerkzones, aansluitmogelijkheden en geschikte plaatsing van fysieke of virtuele sensoren worden tijdens de implementatiefase gezamenlijk vastgesteld.
92	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 5.1 wordt een minimumaantal use-cases voorgeschreven. Gegadigde merkt op dat het aantal use-cases op zichzelf onvoldoende inzicht geeft in de kwaliteit en effectiviteit van de detectiecapaciteit en de daadwerkelijke dekking van de dienstverlening. Gegadigde adviseert daarom om inschrijvers te verzoeken een onderbouwde weergave van de detectiedekking aan te leveren, bijvoorbeeld in de vorm van een heatmap gebaseerd op het MITRE ATT&CK-framework, afgestemd op de feitelijke monitoring-scope van de Opdrachtgever. Kan de Aanbestedende Dienst toelichten of zij bereid is deze beoordelingswijze (deels) te hanteren, dan wel motiveren waarom wordt vastgehouden aan het criterium van een minimumaantal use-cases?	Aanbestedende Dienst handhaaft het vereiste minimumaantal use-cases en verlangt geen aanvullende onderbouwing of afzonderlijke weergave van detectiedekking.

93	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE, Eis 2.2	Kan de Aanbestedende Dienst aangeven wat het aantal accounts binnen de omgeving bedraagt, exclusief gastaccounts?	Er zijn 1577 EntraID Identities
94	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 8.2 wordt een beperking gesteld aan hostingpartijen met een vestiging in de Verenigde Staten in verband met toepasselijke wetgeving, zoals de USA Freedom Act. Gegadigde merkt op dat de Aanbestedende Dienst zelf gebruik lijkt te maken van Microsoft-diensten, waarbij Microsoft als leverancier eveneens onder Amerikaanse wetgeving valt. Gegadigde verzoekt de Aanbestedende Dienst toe te lichten hoe deze eis zich, mede in het licht van het proportionaliteitsbeginsel, verhoudt tot het gebruik van Microsoft-diensten door de Aanbestedende Dienst. Kan de Aanbestedende Dienst dit nader toelichten?	Aanbestedende Dienst verduidelijkt dat eis 8.2 ziet op aanvullende opslag buiten de eigen tenant van Opdrachtgever. In dat geval worden beperkingen gesteld aan locatie en jurisdictie van de hostingpartij. Het gebruik van Microsoft-diensten binnen de eigen tenant van Opdrachtgever valt hierbuiten, aangezien deze onderdeel vormen van de bestaande ICT-omgeving. De eis beoogt te voorkomen dat aanvullende opslag of verwerking bij derden leidt tot ongewenste blootstelling aan buitenlandse wetgeving, en wordt proportioneel toegepast binnen de context van de opdracht.
95	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 8.2 wordt gesteld dat gegevens fysiek dienen te worden opgeslagen binnen de Europese Economische Ruimte en dat de hostingpartij geen vestiging in de Verenigde Staten mag hebben, dan wel dat de data niet opgevraagd kan worden onder de USA Freedom Act. Gegadigde gaat ervan uit dat, indien de tooling en opslag volledig door de Inschrijver zelf worden gehost en beheerd, voldaan wordt aan deze eis, ook in het geval dat een eventuele onderliggende datacenterleverancier een vestiging in de Verenigde Staten heeft. Kan de Aanbestedende Dienst bevestigen dat deze interpretatie juist is? Indien dit niet het geval is, kan de Aanbestedende Dienst toelichten om welke reden deze situatie niet als conform de eis wordt beschouwd?	Aanbestedende Dienst kan deze interpretatie niet bevestigen. De eis ziet erop dat data buiten de tenant uitsluitend wordt opgeslagen bij een partij die voldoet aan de gestelde vereisten ten aanzien van locatie en jurisdictie. Indien een onderliggende datacenterleverancier een vestiging in de Verenigde Staten heeft, dient aantoonbaar te worden gemaakt dat data niet onder Amerikaanse wetgeving, zoals de USA Freedom Act, kan worden opgevraagd. Zonder deze waarborg wordt niet zonder meer voldaan aan de eis.
96	1	Inrichting en monitoring MDR	Nee	Bijlage H PvE	In eis 7.4 en eis 6.5 is opgenomen dat alle configuraties, documentatie, use-cases en detectieregels overdraagbaar dan wel volledig toegankelijk dienen te zijn voor de Opdrachtgever. Gegadigde merkt op dat een dergelijke verplichting, waarbij tevens toegang wordt gevraagd tot generieke use-cases en detectielogica, niet gebruikelijk is binnen de markt voor managed security dienstverlening en bovendien kan raken aan het intellectueel eigendom en bedrijfsdebiet van de Opdrachtnemer. In de praktijk worden dergelijke componenten veelal generiek ontwikkeld en ingezet voor meerdere klanten. Gelet hierop acht Gegadigde deze eis niet proportioneel. Kan de Aanbestedende Dienst bevestigen dat deze verplichting uitsluitend betrekking heeft op configuraties, documentatie, use-cases en detectieregels die specifiek voor de Opdrachtgever zijn ontwikkeld, en niet op generieke of herbruikbare methodieken, use-cases en detectielogica van de Opdrachtnemer?	Aanbestedende Dienst bevestigt dat deze verplichting ziet op configuraties, documentatie, use-cases en detectieregels voor zover deze door of voor Opdrachtgever worden ingezet binnen de dienstverlening. Generieke of herbruikbare methodieken en detectielogica van opdrachtnemer vallen hier buiten, mits de werking en resultaten daarvan voor Opdrachtgever voldoende inzichtelijk en toetsbaar zijn.
97	1	Inrichting en monitoring MDR	Nee	Selectieleidraad Inrichting en Monitoring MDR, 3.2.3.2 Kwaliteitsborging	In paragraaf 3.2.3.2 wordt vereist dat Gegadigde aantoonbaar voldoet aan de BIO-norm en de NIS2-richtlijn. Gegadigde verzoekt de Aanbestedende Dienst te specificeren op welke wijze deze eis dient te worden aangetoond. Kan de Aanbestedende Dienst aangeven welke bewijsmiddelen of documentatie hiervoor verlangd worden?	Zie het antwoord op vraag 43

98	1	Inrichting en monitoring MDR	Nee	Selectieleidraad Inrichting en Monitoring MDR, 3.2.3.2 Kwaliteitsborging	Gegadigde gaat ervan uit dat met “Microsoft Security Partner” wordt gedoeld op de certificering “Microsoft Solutions Partner for Security”. Kan de Aanbestedende Dienst bevestigen dat deze aanname juist is?	Ja. Dit is correct.
99	1	Inrichting en monitoring MDR	Nee	Selectieleidraad Inrichting en Monitoring MDR, 2.5 Planning	De Inschrijver constateert dat de planning van de offertefase, en in het bijzonder de termijn voor het indienen van vragen, gedeeltelijk samenvalt met de zomervakantieperiode. Dit kan de beschikbaarheid van relevante deskundigen beïnvloeden en daarmee mogelijk de zorgvuldigheid en kwaliteit van de inschrijvingen beperken. Gelet op het belang van een zorgvuldig en kwalitatief hoogwaardig inschrijvingsproces, verzoekt Inschrijver de Aanbestedende Dienst de planning zodanig aan te passen dat de termijn voor het stellen van vragen buiten de zomervakantieperiode valt, dan wel deze termijn te verruimen.	Zie nieuwe planning in leidraad en Tenderned.
100	1	Inrichting en monitoring MDR	Nee	"""Bijlage G Opdrachtbeschrijving Managed Detection & Response (MDR).pdf"" bij ""Gewenst Resultaat"" "	"Er staat ""De opdrachtnemer dient de bestaande Sentinel inrichting te gaan beheren "" Onze Managed Detection and Response (MDR) dienst is gebaseerd op eigen ontwikkelde detectieregels en use cases en wij gebruiken Microsoft Sentinel als basis SIEM-platform. Deze technieken zijn intellectueel eigendom van Northwave en worden ingezet voor onze klanten om de dienst tot uitvoering te brengen. De detectieregels zijn per klant opgeslagen in onze eigen Microsoft Sentinel omgeving (EU located) en maken middels Microsoft Lighthouse connectie met de Sentinel omgeving (Log Analytics workspace) van de klant om de daar beschikbare events (van de daarop aangesloten logbronnen) te raadplegen. Een en ander is in het schema hiernaast, weergegeven. Implementatie (aansluiten van logbronnen in uw eigen omgeving, activeren,testen,tunen van use cases, afstemmen escalatieprocessen, etc, etc,) gebeurt in nauwe samenwerking en in projectvorm waarbij Opdrachtnemer de gemeente technisch ondersteunt middels handleidingen en wekelijkse overleggen. Tijdens de run-fase (operatie) monitort Opdrachtnemer ondermeer de correcte werking van de diverse logbronnen maar voert verder geen beheer uit op de omgeving van de gemeente. Vraag: Is dit voor de gemeente een acceptabele opzet / rolverdeling?"	Aanbestedende Dienst kan niet instemmen met de voorgestelde rolverdeling zoals beschreven. De opdrachtnemer wordt geacht de bestaande Microsoft Sentinel-inrichting te beheren en de SOC-dienstverlening daarop te leveren.
101	1	Inrichting en monitoring MDR	Nee	PvE (8.2)	De gemeente eist van de aanbieder een dienstverlening gebaseerd op Microsoft technologie (MS Security partner, MS Sentinel). Daarmee kan onmogelijk volledig aan deze eis worden voldaan. Is de gemeente geneigd deze eis te herzien?	Eis 8.2 gaat over opslag van data. De vraag van inschrijver correspondeert niet met deze eis.
102	1	Inrichting en monitoring MDR	Nee	PvE (6.16)	Deze eis wijst in de richting van Kwetsbaarheden beheer en minder op een eis mbt Managed Detection & Response. Daarbij is de vraag hoe het overzicht van "hard- en softwareproducten die bij de gemeente in gebruik zijn" up-to-date wordt gehouden en hoe deze softwarematig (geautomatiseerd) beschikbaar is voor Aanbieder. Is de gemeente geneigd deze eis te schrappen c.q. verder uit te werken?	Verder uitwerken

103	1	Inrichting en monitoring MDR	Nee	PvE (6.5 en 7.4)	De detectieregels zijn door aanbieder ontwikkeld en behoren tot het intellectueel eigendom van aanbieder. Voor Detectieregels die in nauwe samenwerking met de gemeente zijn ontwikkeld (zgn Custom Use Cases) kunnen in overleg uitzonderingen gemaakt worden mbt het eigendomschap. Is dit een besprekbare aanpak?	Ja
104	1	Inrichting en monitoring MDR	Nee	PvE (4.14)	"Wat wordt bedoeld met een Jaarlijkse verplichting voor validatie van C2, laterale beweging, exfiltratie use-cases? "	Met de jaarlijkse validatie wordt bedoeld dat opdrachtnemer minimaal éénmaal per jaar aantoonbaar toetst of de ingerichte detectie use-cases voor Command & Control (C2), laterale beweging en data-exfiltratie daadwerkelijk effectief functioneren in de praktijk. Deze validatie kan plaatsvinden door middel van gesimuleerde aanvalsscenario's (bijvoorbeeld purple teaming of MITRE ATT&CK gebaseerde tests) en resulteert in een rapportage met bevindingen en eventueel doorgevoerde verbeteringen.
105	1	Inrichting en monitoring MDR	Nee	PvE (4.14)	De hoe vindt de verrekening plaats van de jaarlijkse purple teaming sessie?	Nacalculatie.
106	1	Inrichting en monitoring MDR	Nee	PvE (4.12)	Wat wordt bedoeld met 'integreren" "voor:" "Threat Intel correlatie"?	Met "integreren voor threat intelligence correlatie" wordt bedoeld dat gegevens uit verschillende beveiligingscomponenten worden gekoppeld en gecombineerd met dreigingsinformatie, zodat deze gezamenlijk geanalyseerd kunnen worden en leiden tot effectievere detectie van beveiligingsincidenten.
107	1	Inrichting en monitoring MDR	Nee	PvE (4.9)	Kan de gemeente de condities van de Parkeergarage beschrijven?	De parkeergarage geldt als een relevante technische netwerkzone binnen de scope. Het netwerk bestaat uit verschillende VLAN's en is via een firewall met het internet verbonden. De exacte aangesloten technische componenten, omstandigheden, aansluitmogelijkheden en geschikte locatie voor een sensor worden tijdens de implementatiefase gezamenlijk vastgesteld.
108	1	Inrichting en monitoring MDR	Nee	PvE	"Een aanbieding dat op alle eisen uit het PVE ""JA"" heeft geantwoord lijkt ons een ""Silver Bullet"". Aanbieders met hier en daar een ""Nee, want..."" maar met misschien andere invulling vallen daarmee buiten beeld. De vraag is of de gemeente op zoek is naar een dergelijke 'perfecte oplossing' EN of de bijbehorende dienstverlening voor de gemeente uiteindelijk de beste match geeft. Is de gemeente geneigd om de wijze van beantwoording van het PVE te heroverwegen?"	Nee.

109	1	Inrichting en monitoring MDR	Nee	PvE	"De PVE moet worden beantwoord (kolom C) met 2 opties: Ja of Nee. Optie Nee leidt tot uitsluiting. Echter in diverse eisen zijn meerdere onderdelen genoemd die ook niet altijd zijn uitgewerkt (bv met ""etc""). Ook zijn er alternatieven te bedenken die mogelijk beter zijn. Bijvoorbeeld een snellere responsetijd of betere detecties. Hoe moeten deze Eisen worden beantwoord? "	Gegadigde dient iedere eis met “Ja” of “Nee” te beantwoorden. Gegadigde mag uitsluitend “Ja” antwoorden indien onvoorwaardelijk aan alle onderdelen van de betreffende eis wordt voldaan. Wanneer een eis uit meerdere onderdelen bestaat, geldt het antwoord “Ja” voor de eis als geheel. Het beter presteren op een ander onderdeel, zoals een snellere responstijd of aanvullende detectiemogelijkheden, compenseert niet voor het niet voldoen aan een minimumeis. Voor zover een eis functioneel is geformuleerd, is een technisch andere of gelijkwaardige invulling toegestaan, mits daarmee aantoonbaar volledig hetzelfde of een beter functioneel resultaat wordt bereikt. Gegadigde dient een dergelijke invulling duidelijk toe te lichten. Deze toelichting mag geen voorbehoud of beperking ten opzichte van de eis bevatten. Formuleringen zoals “bijvoorbeeld”, “denk aan” en “et cetera” zijn illustratief en dienen ter verduidelijking van de betreffende eis. Hieruit volgen geen aanvullende, niet nader omschreven verplichtingen buiten het expliciet gevraagde functionele resultaat. Indien Gegadigde niet of niet volledig aan een eis kan voldoen, dient de eis met “Nee” te worden beantwoord. Overeenkomstig de toelichting bij het Programma van Eisen leidt dit tot uitsluiting.
110	1	Inrichting en monitoring MDR	Nee	GIBIT voorwaarden (artikel 21.4)	Is de gemeente bereid hier een uitzondering te maken voor maatwerk use-cases? Als wij deze elders kunnen inzetten dan zouden wij dat graag doen. Vice versa profiteert u van maatwerk use-cases van andere klanten.	Ja
111	1	Inrichting en monitoring MDR	Nee	GIBIT voorwaarden (artikel 17)	Is de gemeente bereid indirecte schade, gevolgschade, gederfde winst en gemiste besparingen expliciet uit te sluiten van vergoeding?	Niet akkoord.
112	1	Inrichting en monitoring MDR	Nee	GIBIT voorwaarden (artikel 17)	In artikel 17.4 wordt de aansprakelijkheid voor overige schade gemaximeerd op tweemaal de Jaarvergoeding per gebeurtenis en viermaal de Jaarvergoeding per jaar. Gezien de omvang en het risicoprofiel van de opdracht verzoeken wij deze aansprakelijkheid te beperken tot eenmaal de Jaarvergoeding per gebeurtenis en eenmaal de Jaarvergoeding per contractjaar. Is Opdrachtgever hiertoe bereid?	Niet akkoord, zie ook beantwoording vraag 60.
113	1	Inrichting en monitoring MDR	Nee	GIBIT voorwaarden (artikel 12)	Wij zouden graag verduidelijken dat onze dienstverlening niet kan garanderen dat Opdrachtgever ten alle tijde vrij zal blijven van een Security Incident. Bent u hiermee akkoord?	Ja
114	1	Inrichting en monitoring MDR	Nee	"Bijlage G Opdrachtbeschrijving Managed Detection & Response (MDR).pdf" bij "Scope / Omgeving gemeente Katwijk"	Er staat "De gemeente Katwijk is in bezit van 950 Microsoft 365 E5 licenties." Hoeveel van deze E5 licenties zijn daadwerkelijk toegewezen c.q. in gebruik?	980 E5 licenties waarvan er 960 zijn toegewezen.
115	1	Inrichting en monitoring MDR	Nee	Huidige situatie	Zie vorige vraag m.b.t omvang team (aantal medewerkers) die de huidige SIEM meldingen afhandelt; is dit team (in noodgeval) 24/7 beschikbaar?	Nee

116	1	Inrichting en monitoring MDR	Nee	Huidige situatie	Hoe groot (aantal medewerkers) is het team dat de huidige SIEM meldingen afhandelt?	4
117	1	Inrichting en monitoring MDR	Nee	Huidige situatie	Hoeveel medewerkers heeft de gemeente?	960 medewerkers