Programma van Eisen - Aanbesteding Managed Detectie en Respons (MDR) Dienstverlening		
	Toelichting eisen: In kolom B staan de eisen geformuleerd ten aanzien van de Dienstverlening waarmee inschrijver de Opdracht invult. Het niet kunnen voldoen aan (een van) deze eisen is een knock-out criterium. Inschrijver kan in kolom C van de corresponderende rij kiezen uit 2 opties: 1- Ja 2- Nee Inschrijver wordt derhalve verzocht alle lichtblauwe cellen een van de opties te kiezen. De keuze voor optie 2 leidt tot uitsluiting van de aanbesteding. Dit formulier dient zowel digitaal te worden ingevuld en geretourneerd, alswel geprint, getekend en ingescand en geretourneerd als onderdeel van de inschrijving. In dit concept verdienen de eerste 2 onderdelen (Selectiecriteria en Uitvoeringseisen) speciale aandacht, omdat deze eisen naar onze mening onderscheidend zijn; het is daarom dat deze apart gepresenteerd zijn.	
Nr	**1 Selectiecriteria**	**Gegadigde voldoet Ja/Nee**
1.1	Opdrachtnemer is IBD-CERT verbonden.	
1.2	Opdrachtnemer is Microsoft Security Partner	
1.3	Opdrachtnemer kan tenminste 2 referenties aandragen van Opdrachtgevers die een Nederlandse gemeente zijn.	

1.4	De deelnemer stelt jaarlijks een verklaring van een onafhankelijke nationale of Europese IT-auditor (zoals NOREA, ISACA of vergelijkbaar) beschikbaar waaruit blijkt dat aan de eisen voor informatieveiligheid wordt voldaan. De dienstverlening valt binnen de scope van het managementsysteem voor informatiebeveiliging (ISO 27001 en eventuele vergelijkbare kwaliteitssystemen voor informatiebeveiliging) waarover de opdrachtnemer beschikt. Op verzoek stelt de opdrachtnemer een verklaring van een onafhankelijke derde beschikbaar waaruit blijkt dat de informatieveiligheid van de ICT-oplossing in lijn is met de eisen van de gemeente en dat de maatregelen gedurende het gehele jaar goed hebben gefunctioneerd. Dit kan door middel van verklaringen zoals een SOC 2-rapport, een ISAE 3000-verklaring of een vergelijkbaar document.	
Nr	**2 Uitvoeringseisen**	**Gegadigde voldoet Ja/Nee**
2.1	Opdrachtnemer biedt 24x7 dienstverlening o.b.v. "eyes on the screen" aan.	
2.2	Opdrachtnemer ondersteunt het gebruik van Microsoft Sentinel in de tenant van Opdrachtgever.	
2.3	Opdrachtnemer en alle medewerkers die contact onderhouden met Opdrachtgever zijn in staat in de Nederlandse taal te communiceren, zowel in spraak als geschrift.	
2.4	Alle medewerkers die in aanraking komen met de data van Opdrachtgever zijn gescreend en beschikken over een VOG die bij indiensttreding van Opdrachtnemer niet ouder is dan 3 maanden.	
2.5	Opdrachtnemer kan buiten kantooruren autonoom ingrijpen in geval van incidenten met een bepaalde urgentie. De voorwaarden wanneer Opdrachtnemer dient in te grijpen, worden na het sluiten van de Overeenkomst afgestemd, denk bij ingrijpen aan het blokkeren van een useraccount of het downbrengen of isoleren van een bepaalde server.	
2.6	Bij de hoogste classificatie (prio 1) moet het mitigatieadvies binnen 30 minuten na melding van het event worden gemaakt en zowel telefonisch als digitaal beschikbaar gesteld. Bij de een-na-hoogste classificatie (prio 2) moet het mitigatieadvies binnen één werkdag na melding van het event worden gemaakt en beschikbaar gesteld.	
2.7	Opdrachtnemer gebruikt Copilot for Security om correlatie tussen events te kunnen detecteren.	
2.8	Opdrachtnemer gaat akkoord met de GIBIT 2023 (overeenkomst wordt nog gebouwd).	
Nr	**3 Auditing**	**Gegadigde voldoet Ja/Nee**
3.1	De auditlog moet zodanig worden ingericht dat gebruikers van het systeem deze niet kunnen wijzigen.	
3.2	Alle activiteiten van gebruikers en beheerders worden gelogd en zijn inzichtelijk voor Opdrachtgever wanneer daar om gevraagd wordt.	

3.3	Alle accounts zijn herleidbaar naar een persoon, het delen van accounts is niet toegestaan.	
Nr	**4 Detectie**	**Gegadigde voldoet Ja/Nee**
4.1	De set van Use Cases moet een breed scala van relevante en detecteerbare aanvalstechnieken uit het MITRE ATT&CK-framework dekken, met prioriteit voor technieken die aansluiten bij de specifieke dreigingen en risico's binnen de infrastructuur van gemeente Katwijk.	
4.2	De ruleset voor netwerkdetectie moet actueel zijn en minimaal in staat zijn om dagelijks de relevante updates te krijgen. De ruleset moet geavanceerde detectie van bestaande en opkomende bedreigingen in het netwerkverkeer mogelijk maken. Daarnaast wordt van de Opdrachtnemer verwacht dat hij zelf de actualiteit in de gaten houdt en de ruleset aanvult bij opkomende bedreigingen.	
4.3	De correlatieregels op basis van use-cases en policies moeten toepasbaar zijn op zowel real-time als historische data en events.	
4.4	De aangeboden oplossing moet in staat zijn om ongewenste software en websites te detecteren die een bedreiging kunnen vormen, zoals remote control applicaties, phishing- en malwaresites, en sites met hacktools.	
4.5	De oplossing moet events van verschillende bronnen en apparaten kunnen correleren, zodat misbruik nauwkeuriger gedetecteerd kan worden.	
4.6	De verwerking van de loginformatie gebeurt vrijwel realtime, met een maximale vertraging van 10 minuten. Wanneer een cloud dienst de data echter later aanlevert, kan deze uiteraard niet realtime worden verwerkt.	
4.7	De oplossing maakt gebruik van een set standaard Use Cases die door de Opdrachtnemer worden geleverd en onderhouden. Deze Use Cases worden regelmatig bijgewerkt door de opdrachtnemer om de effectiviteit en actualiteit te waarborgen.	
4.8	De Opdrachtnemer heeft de mogelijkheid om in de loop van de tijd nieuwe Use Cases toe te voegen op basis van nieuwe technische mogelijkheden, veranderende beveiligingsbehoeften, of marktontwikkelingen.	
Nr	**5 Dienstverlening**	**Gegadigde voldoet Ja/Nee**
5.1	De Opdrachtnemer dient MS Sentinel zo in te richten dat incidenten geprioriteerd worden. Bij een incident moet er een handeling volgen conform de gemaakte afspraken, wat kan zijn (niet uitputtend): - Opdrachtnemer doet verder onderzoek en analyse op de situatie. - Opdrachtnemer onderneemt (al dan niet geautomatiseerd) directe risico beperkende actie en informeert Opdrachtgever. - Opdrachtnemer neemt telefonisch contact met Opdrachtgever. - Opdrachtnemer maakt in het ticket systeem van Opdrachtgever een ticket aan (bij prio 2 of lager).	

5.2	Bij de hoogste classificatie (prio 1) moet binnen 30 minuten de vervolgactie plaatsvinden, d.w.z. handeling conform gemaakte afspraken wordt uitgevoerd. Bij lagere prio (2 of lager) wordt het ticket binnen 1 werkdag aangemaakt inclusief mitigatieadvies.	
5.3	Het moet eenvoudig zijn om de dienst op of af te schalen bij een verandering in het aantal logbronnen die worden verwerkt.	
5.4	De opdrachtnemer stelt een vaste contactpersoon (en vervanger) aan voor alle communicatie tussen de gemeente Lelystad en de opdrachtnemer gedurende de gehele periode van de implementatie en de operationele fase van de dienstverlening. Deze contactpersoon is verantwoordelijk voor de communicatie en afhandeling van alle meldingen en vragen met betrekking tot de dienstverlening en fungeert als primair aanspreekpunt voor de opdrachtgever. De contactpersoon moet: - Beschikbaar zijn voor het bespreken en afhandelen van gemelde problemen, incidenten en vragen in relatie tot de dienstverlening. - Proactief opvolging geven aan lopende problemen en incidenten. - Direct bereikbaar zijn via Microsoft Teams, telefoon of e-mail voor ad-hoc vragen en urgente situaties. - Regelmatig rapporteren aan Opdrachtgever over de voortgang van openstaande issues en verbeterpunten. - Advies bieden zonder extra kosten wanneer Opdrachtgever vragen heeft over de dienstverlening. - Optreden als sparringpartner bij het bespreken van nieuwe technologieën en ontwikkelingen in het vakgebied. Het hebben van een vast aanspreekpunt bevordert de efficiëntie en transparantie in het afhandelingsproces, zorgt voor een nauwe samenwerking tussen opdrachtgever en opdrachtnemer, en ondersteunt de gemeente bij strategische en operationele vragen. De gemeente stelt eveneens een vast contactpersoon (en vervanger) aan.	
5.5	Voor de opdrachtgever is inzichtelijk welke bronnen zijn aangesloten op MS Sentinel, welke use-cases worden gebruikt, op welke IoC's wordt gecontroleerd en wat de specifieke instellingen zijn (bijvoorbeeld welke drempelwaarden zijn ingesteld).	

5.6	Om de uitvoering van de opdracht door de opdrachtnemer continu te verbeteren, is een operationele evaluatie onderdeel van een maandelijks gesprek. Op basis van deze operationele evaluatie kunnen schriftelijke afspraken worden gemaakt over geconstateerde tekortkomingen, aandachtspunten en verbeteringen/maatregelen, zoals het verminderen van false positives. Deze afspraken zijn bindend, tenzij ze in strijd zijn met de overeenkomst of tenzij anders overeengekomen.	
5.7	Bij foutmeldingen, zoals het niet meer ontvangen van loginformatie, neemt de opdrachtnemer binnen 1 uur contact op met de opdrachtgever.	
5.8	De dienst wordt geleverd vanuit een Operation Center (of vergelijkbaar) binnen de Europese Economische Ruimte (EER)	
5.9	De Opdrachtnemer bespreekt de Dienstverlening periodiek (maandelijks) in een operationeel overleg met de gemeente Katwijk en draagt verbetervoorstellen voor.	
5.10	Indien de opdrachtnemer werkt met onderaannemers, is hij verantwoordelijk voor het naleven van de contract- en SLA-afspraken door deze onderaannemers, zoals opgesteld tussen de opdrachtgever en opdrachtnemer.	
5.11	De mate en vorm van communicatie wordt vastgelegd in een OLA of SLA. Deze dient vanuit inschrijver opgeleverd te worden. Een concept/voorbeeld aanleveren als bijlage aan uw inschrijving is een vereiste.	
5.12	De opdrachtnemer biedt een deskundige Nederlandstalige helpdesk aan voor zowel technische als functionele ondersteuning. Deze helpdesk is bereikbaar via telefoon, e-mail en/of een webportaal. De helpdesk fungeert als centraal punt voor het melden van incidenten, het stellen van vragen, en het indienen van wijzigingsvoorstellen. Tevens verstrekt de helpdesk informatie en inzicht in de voortgang en afhandeling van deze meldingen.	
5.13	De Service Level Agreement (SLA) vormt de basis voor deze samenwerking. De SLA omvat duidelijke afspraken, prestatie-indicatoren en kwaliteitseisen met betrekking tot de oplossing en de bijbehorende dienstverlening. De definitieve SLA wordt vastgesteld bij gunning en overeengekomen tussen Partijen.	
5.14	Dienstverlener voert een triage en analyse uit op alerts vanuit Microsoft Sentinel, zodat de aanbestedende dienst alleen meldingen ontvangt, waarbij acties nodig zijn, bijvoorbeeld door systeem- en/of netwerkbeheerders.	
5.15	Opdrachtnemer isoleert assets en plaatst deze in quarantaine om een aanval of inbreuk te dwarsbomen en/of in te dammen. Na gunning wordt afgestemd: - Communicatie en beslisprotocol met bevoegdheden van de Opdrachtnemer - Werkwijze per assettype afhankelijk van de functionaliteit van EDR en de toewijzing van bevoegdheden aan de Opdrachtnmer. Het gaat daarbij om containment, zodra een inbreuk is geconstateerd.	

5.16	Opdrachtnemer adviseert in het incident response proces in afstemming met management en/of beheerders van de aanbestedende dienst die door Opdrachtnemer geconsulteerd zullen worden en die acties uitvoeren waartoe zij wel en Opdrachtnemer niet geautoriseerd is.	
5.17	De Opdrachtnemer voorziet de aanbestedende dienst van advies over communicatie- en handelingsplannen bij inbreuken.	
5.18	De inschrijver informeert de gemeente binnen 1 dag na bekendmaking (bijv. toewijzing CVE-nummer) over nieuwe kwetsbaarheden vanuit IBD-CERT in hard- en softwareproducten die bij de gemeente in gebruik zijn.	
5.19	Opdrachtgever kan verlangen dat technische details van een incident en de Oplossing worden gedeeld met Opdrachtgever of met een derde partij teneinde deze te analyseren en/of vast te kunnen stellen of herhaling aannemelijk is. Dit ontslaat Opdrachtnemer niet van haar verplichting tot eigen analyse.	
5.20	Opdrachtnemer neemt de verantwoordelijkheid om passende connectoren te bieden om componenten die niet "out-of-the-box" kunnen worden aangesloten op de producten die Opdrachtnemer gebruikt in de Oplossing, alsnog aan te kunnen sluiten op de aangeboden Oplossing.	
5.21	Opdrachtgever kan via een cloudportal inzicht krijgen in dashboards over de dienstverlening. Dit mag een geconfigureerde dashboards en/of portal zijn in de eigen tenant. Opdrachtnemer zorgt in afstemming voor de configuratie hiervan. De dashboards handelen omtrent actuele (live) data.	
5.22	Informatie die Opdrachtgever verwacht omtrent de dienstverlening: - Verrichtte requests/aanvragen van de aanbestedende dienst en status - Aantallen events/alerts, meldingen aan de gemeente en incidenten naar classificatie, zoals informational, low, medium, high, critical - Beschikbaarheid van dienstverlening - Evaluatie en aanbevelingen - Klachten en klachtafhandeling	
Nr	**6 Beëindiging overeenkomst en retransitie**	**Gegadigde voldoet Ja/Nee**
6.1	Bij het eerste verzoek stelt de opdrachtnemer binnen 10 werkdagen een gedetailleerd exitplan op, conform de GIBIT/artikel 5.3.	
6.2	Tijdens de periode van retransitie moet de opdrachtnemer alle dienstverlening voortzetten volgens de overeengekomen voorwaarden.	

6.3	De opdrachtnemer zal aan het einde van de overeenkomst of de retransitie alle vertrouwelijke informatie vernietigen of (indien van toepassing) retourneren zonder een kopie te behouden, tenzij anders overeengekomen op basis van een (wettelijke) eis of verplichting, of aanvullende afspraken. Als het langer bewaren van een kopie van vertrouwelijke informatie wettelijk verplicht is, zal deze informatie worden vernietigd zodra de bewaartermijn is verstreken.	
Nr	**7 Gegevensbeveiliging**	**Gegadigde voldoet Ja/Nee**
7.1	De gegevens (logbronnen, incidenten) worden binnen de tenant van Opdrachtgever opgeslagen, tenzij dat onmogelijk is. Alle gegevens die noodzakelijk daarbuiten moeten worden opgeslagen, moeten beveiligd worden opgeslagen, zowel tijdens transport als tijdens opslag.	
7.2	Indien het noodzakelijk is gegevens buiten de tenant van Opdrachtgever op te slaan, dienen gegevens tenminste fysiek te worden opgeslagen binnen de Europese Economische Ruimte en bij een hostingpartij/datacenter zonder vestiging in de Verenigde Staten, vanwege de USA Freedom Act. Als alternatief kan de opdrachtnemer garanderen dat de data niet opgevraagd kan worden onder de USA Freedom Act.	
7.3	Indien Opdrachtnemer gebruik maakt van een multi-tenant oplossing (zoals bijvoorbeeld Lighthouse) moet er een strikte logische scheiding zijn tussen de klanten van de Opdrachtnemer.	
Nr	**8 Implementatie**	**Gegadigde voldoet Ja/Nee**
8.1	Na definitieve gunning en vóór de start van het implementatietraject levert de opdrachtnemer een functioneel en technisch ontwerp aan. Dit ontwerp, gepresenteerd in Microsoft Visio, brengt de nieuwe situatie in kaart en beschrijft de voorzieningen, koppelingen en afhankelijkheden met andere informatievoorzieningen. Het ontwerp wordt afgestemd met de contactpersoon van de Opdrachtgever en wordt actueel gehouden. Opdrachtgever dient goedkeuring te geven op wijzigingen op het ontwerp. Bij wijzigingen vanuit de Opdrachtgever die impact hebben op het ontwerp, wordt Opdrachtnemer betrokken.	
8.2	Vanaf start van de overeenkomst dient zo spoedig als mogelijk overgegaan te worden tot implementatie, echter uiterlijk binnen 3 weken. De kosten van de dienstverlening worden in rekening gebracht vanaf oplevering en acceptatie van deze diensten.	

8.3	Acceptatie vindt plaats op basis van de volgende criteria: - de Dienstverlening is geïmplementeerd voor de aanbestedende dienst en ingericht voor en afgestemd op de omgeving van de aanbestedende dienst, waarbij kinderziektes, false-positives etc. zijn herkend en opgelost. - Alle log-bronnen in scope zijn aangesloten op Microsoft Sentinel. - De opslag van verzamelde (log-)informatie is ingericht, inclusief kostenoptimalisatie. - De werking van de initiële response door isolatie van gecompromitteerde (hier voor een test aangewezen) assets is aangetoond voor de verschillende asset-typen - Het interface met Topdesk is gerealiseerd en functioneel - Werkafspraken tussen Opdrachtgever en Opdrachtnemer zijn gemaakt, onder andere over de communicatiematrix en escalatie afspraken (in SLA / OLA / DAP) en afspraken omtrent respons / actie in voorkomende gevallen. - De dienstverlening is ingericht en operationeel voor de aanbestedende dienst en eerste meldingen zijn gedaan - Er is voldaan aan de overige eisen uit het beschrijvend document en het pakket van eisen Indien optionele dienstverlening wordt afgenomen: - NDR is geïmplementeerd, passend ingericht en aangesloten op Microsoft Sentinel - Honeypots zijn geïmplementeerd, passend ingericht en aangesloten op Microsoft Sentinel - Threat intelligence is geïmplementeerd en passend ingericht en eerste meldingen zijn gedaan - Threat hunting is geïmplementeerd en heeft eerste resultaten opgeleverd	
8.4	Vanaf de start van de implementatie dient de dienstverlening binnen 3 maanden operationeel te zijn, inclusief acceptatie. Dit geldt voor de logbronnen die in scope zijn benoemd. Dit geldt niet voor aansluiten van logging van SAAS applicaties die niet voorzien in een standaard interface voor logging Wel in scope is de logging van toegang tot applicaties indien die verloopt via Microsoft Entra, denk aan logging omtrent geslaagde en niet-geslaagde inlogpogingen.	
8.5	De Opdrachtnemer rapporteert tijdens de implementatie wekelijks over de voortang van de implementatie in relatie tot de planning (conform Plan van Aanpak)	
8.6	De inschrijving en alle bijbehorende contractuele documentatie is in de Nederlandse taal opgesteld	
8.7	De Opdrachtnemer verzorgt de aansluiting en configuratie van log-bronnen, daar waar dit niet mogelijk is voorziet Opdrachtnemer de Opdrachtgever van aanwijzingen om de log-bronnen aan te sluiten en te configureren.	
Nr	**9 Kwaliteitsborging**	**Gegadigde voldoet Ja/Nee**

9.1	Medewerkers van de opdrachtnemer die toegang hebben tot de gegevens van Opdrachtgever, zijn gescreend op integriteit. De minimale eis is dat zij bij indiensttreding bij Opdrachtnemer een voor de functie geldende Verklaring omtrent Gedrag (VOG) hebben overlegd die op dat moment niet ouder was dan drie maanden.	
9.2	De opdrachtnemer moet de privacy en bescherming van de verzamelde gegevens waarborgen in overeenstemming met relevante wet- en regelgeving, zoals de AVG.	
9.3	De opdrachtnemer moet een geldig kwaliteitscertificaat kunnen overleggen dat gebaseerd is op de ISO 9001-standaard voor kwaliteitsmanagement.	
9.4	De opdrachtnemer garandeert dat hij en eventuele door hem ingeschakelde derden voldoen en blijven voldoen aan alle wettelijke bepalingen en voorschriften, en dat zij beschikken en blijven beschikken over alle vereiste vergunningen, beschikkingen en verklaringen voor de dienstverlening en het ondernemerschap.	
9.5	De opdrachtgever is te allen tijde gerechtigd om de uitvoering van de overeenkomst te controleren. De kosten van deze controles worden gedragen door de opdrachtgever, tenzij blijkt dat de opdrachtnemer zijn verplichtingen niet is nagekomen. In dat geval worden de kosten door de opdrachtnemer gedragen. De opdrachtnemer is slechts verplicht tot vergoeding van kosten voor zover deze aantoonbaar en redelijkerwijs zijn gemaakt.	
Nr	**10 Notificatie**	**Gegadigde voldoet Ja/Nee**
10.1	De dienst moet notificaties voor meldingen via telefoon en e-mail kunnen leveren.	
10.2	Opdrachtgever en opdrachtnemer moeten specifieke afspraken kunnen maken over de situaties waarin notificaties volgen en hoe deze worden verzonden.	
10.3	Bij een telefonische notificatie moeten bij geen gehoor meerdere personen gebeld kunnen worden via een bel-lijst.	
10.4	Bij een incident moet de dienst conform afspraken automatisch een melding kunnen maken in het incidentmanagementsysteem van de gemeente Katwijk (Topdesk).	
Nr	**11 Retentie**	**Gegadigde voldoet Ja/Nee**
11.1	Retentietijden van audit-, log- en eventdata worden in overleg bepaald en worden door Opdrachtnemer ingesteld, binnen de wettelijke vereisten en mogelijkheden.	
11.2	De loginformatie wordt standaard 13 maanden bewaard. Daarna worden de log-gegevens (semi-)automatisch verwijderd.	
Nr	**12 Eisen aan de NDR dienstverlening**	**Gegadigde voldoet Ja/Nee**
12.1	NDR voorziet Microsoft Sentinel van loginformatie over alle netwerkactiviteiten door informatie van SPAN ports van netwerkcomponenten te verwerken.	

12.2	NDR bewaakt zowel het externe verkeer als het interne verkeer.	
	13 Eisen aan de Honeypots	**Gegadigde voldoet Ja/Nee**
13.1	De honeypots worden geïnstalleerd op een virtual machine in het interne netwerk of DMZ, die door de Opdrachtgever ter beschikking worden gesteld.	
13.2	De honeypots zijn voor een indringer niet te onderscheiden van productiesystemen	
13.3	De honeypots dekken een brede functionaliteit af, in ieder geval webserver, databaseserver, storage en rdp.	
13.4	De honeypots melden alle activiteiten aan Microsoft Sentinel	
13.5	De inschrijver adviseert over de effectieve inzet van honeypots	
E67A	**14 Eisen aan de Threat Intelligence dienstverlening**	**Gegadigde voldoet Ja/Nee**
14.1	Het SOC voert Threat Intelligence uit: het inwinnen en analyseren van informatie over ontwikkelingen van dreigingen en aanvallen en het vertalen daarvan naar aanvullende maatregelen, ter ondersteuning van de overige dienstverlening van het SOC	
14.2	De inschrijver maakt gebruik van erkende threat intelligence feeds en eigen analyses. NB Het gaat om generieke threat intelligence, niet specifiek op de aanbestedende dienst gerichte bedreigingen.	
14.3	Voor Threat Intelligence worden toekomstbestendige mainstream feeds/diensten uit de markt ingezet met minimaal maatwerk.	
E70A	**15 Eisen aan de Threat Hunting dienstverlening**	**Gegadigde voldoet Ja/Nee**
15.1	Dienstverlener voert Threat hunting uit: Een pro-actieve aanpak om nog niet bekende beveiligingsissues binnen het netwerk en de systemen van de aanbestedende dienst op te sporen	
	Namens Inschrijver voor akkoord:	

Naam:

Functie:

Handtekening:

Datum: