V2 Bijlage 4 Programma van Eisen – MXDR-Dienstverlening

Nummer	Programma van Eisen - Europees openbare aanbesteding MXDR gemeente Gooise Meren
	Toelichting eisen: Hieronder staan de eisen geformuleerd waar Opdrachtnemer aan dient te voldoen bij de uitvoering van de Opdracht. Het niet kunnen voldoen aan (een van) deze eisen is een knock-out criterium. Alle Eisen uit dit programma van Eisen dienen in de prijs van de maandelijkse Dienstverlening in te zijn begrepen. Dit geldt ook voor advieskosten. Indien er kosten aan bepaalde adviezen verbonden zijn in geval van consultancy uren (voor incidenten en niet standaard changes), vraagt Opdrachtnemer toestemming voor ureninzet. Zonder goedkeuring van Opdrachtgever kunnen deze uren niet gefactureerd worden. Eisen die gaan over onboarding, implementatie en offboarding dienen bij de prijs voor de onboarding, implementatie en offboarding in te zitten.
	Bronaansluitingen
1	Het toevoegen, verwijderen en wijzigen van databronnen dient in overleg met de Opdrachtgever te gebeuren. Indien nodig wordt dit projectmatig uitgevoerd, waarbij de Opdrachtnemer de documentatie bijwerkt.
2	Opdrachtnemer dient ervoor te zorgen dat de (data)connectoren in de lucht blijven. De beschikbaarheid van (data)connectoren wordt up-time gemonitord en Opdrachtgever wordt geïnformeerd indien er uitval is.
3	Vanaf de start van de implementatie, moet Opdrachtnemer binnen 1 maand technisch kunnen integreren, de Dienstverlening binnen 1 maand operationeel zijn, inclusief de SOC-dienst, op basis van de huidige inrichting Opdrachtgever van Microsoft Sentinel, Microsoft Defender en de overige securitymaatregelen die binnen de E5/M365-licenties vallen. *De huidige configuratie van de gemeente Gooise Meren kunt u opvragen via de berichtenmodule in TenderNed middels het indienen van de geheimhoudingsverklaring (dit kan op elk moment na publicatie van de Inschrijving tot moment indienen Inschrijving), zie bijlage 16.*
4	Opdrachtnemer moet in staat zijn een eigen security framework neer te zetten, waarbij Opdrachtnemer binnen 3 maanden functioneel moet kunnen integreren.
	Detectie
5	Compliancy- en securitypakketten (zoals baselines, use cases en threat intelligence) voor het SIEM worden door Opdrachtnemer standaard meegeleverd en onderhouden, zonder aanvullende kosten. Daarnaast wordt van de Opdrachtnemer verwacht dat hij zelf de actualiteit in de gaten houdt en de use cases/rule sets aanvult bij opkomende en actuele bedreigingen.

6	Opdrachtnemer moet in staat zijn ook te monitoren op Operationele Technologie (OT) en Internet of Things (IoT) binnen de bestaande Microsoft Sentinel-oplossing.
7	De logs van de firewall van gemeente Gooise Meren zijn geïntegreerd in Microsoft Sentinel. Opdrachtnemer moet in staat zijn een playbook op te stellen voor het monitoren van verdacht verkeer waargenomen via de firewall, zoals het downloaden van een hacktool, bezoeken van een malafide website en dergelijke.
8	Opdrachtnemer maakt gebruik van een algemeen geaccepteerd framework (zoals MITRE ATT&CK-framework of gelijkwaardig) voor het classificeren van aanvalstechnieken en kwetsbaarheden, met prioriteit voor (aanvals)technieken die aansluiten bij specifieke dreigingen en risico's binnen de infrastructuur van gemeente Gooise Meren.
9	Alleen door de CISO van de Opdrachtgever aangewezen medewerkers mogen wijzigingen indienen die betrekking hebben op het detectiebeleid en de respons, zoals het aanpassen van afspraken over wanneer contact wordt opgenomen bij bepaalde typen alerts of het whitelisten van specifiek verkeer.
	Dienstverlening
10	*Versie 2 eis 10:* Bij P1, P2 en P3 incidenten en escalaties die raken aan de Dienstverlening, moet Opdrachtnemer (bijvoorbeeld de servicelevelmanager en/of accountmanager) 24/7 in staat zijn om hierover zowel schriftelijk als mondeling afstemming te hebben met Opdrachtgever met de Nederlandse taal als voertaal.
11	Opdrachtnemer moet een fysieke locatie binnen de Europese Economische Ruimte (EER) hebben voor de uitvoering van de Opdracht, en data onderbrengen bij een hostingpartij/datacenter binnen de EER. Als alternatief moet de Opdrachtnemer garanderen dat de data niet opgevraagd kan worden onder de USA Freedom Act, CLOUD-Act en andere (Amerikaanse) wetgeving die ervoor kan zorgen dat data door een entiteit buiten de EER kan worden ingezien.
12	Een eventueel door Opdrachtnemer in te zetten Onderaannemer voldoet aantoonbaar aan dezelfde eisen als hoofdaannemer en werkt binnen de reguliere processen, techniek (devices) en organisatiestructuur van de hoofdaannemer. Indien Onderaannemers worden ingezet, dienen deze gebruik te maken van dezelfde technische omgeving en beveiligingsmaatregelen als de hoofdaannemer.
13	De MXDR-Dienstverlening is 24 uur per dag, 7 dagen per week, telefonisch bereikbaar voor de Opdrachtgever en biedt binnen 15 minuten contact met de medewerker (of een directe collega) die het security incident aan Opdrachtgever heeft gemeld.
14	De MXDR moet de events bekijken en incidenten prioriteren. Bij een incident moet er een handelingsperspectief zijn dat beschrijft hoe en met welke prioriteit het incident opgevolgd moet worden.
15	*Versie 2 eis 15:* De eerste triage moet binnen een half uur na detectie worden gemeld aan Opdrachtgever bij zowel prio 1 , 2 en 3. Prio 1: De totale tijd tot opleveren eerste mitigerende stappen vanaf triage incident is binnen 1 uur. Prio 2: De totale tijd tot opleveren eerste mitigerende stappen vanaf triage incident is 4 uur. Prio 3: De totale tijd tot opleveren van eerste mitigerende stappen vanaf triage incident is 8 uur.

16	Het moet mogelijk zijn om de Dienstverlening op of af te schalen bij een verandering in het aantal logbronnen (in Sentinel: connectors) of endpoints die verwerkt worden.
17	De Opdrachtnemer stelt een vast contactpersoon (en vervanger) aan voor alle communicatie tussen gemeente Gooise Meren en de Opdrachtnemer gedurende de gehele periode van de implementatie en de operationele fase van de Dienstverlening. Deze contactpersoon communiceert op minimaal B1-niveau zowel schriftelijk als mondeling in de Nederlandse taal. Deze contactpersoon is verantwoordelijk voor de communicatie en afhandeling van alle meldingen en vragen met betrekking tot de MXDR-Dienstverlening en fungeert als primair aanspreekpunt voor de Opdrachtgever. De gemeente stelt eveneens een vast contactpersoon (en vervanger) aan. De contactpersoon moet: • Beschikbaar zijn voor het bespreken en afhandelen van gemelde problemen, incidenten en vragen in relatie tot de MXDR-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 de gemeente Gooise Meren over de voortgang van openstaande issues en verbeterpunten, in relatie tot de planning. • Gevraagd en ongevraagd advies bieden over de MXDR-Dienstverlening. • Optreden als sparringpartner bij het bespreken van nieuwe technologieën en ontwikkelingen in het vakgebied. • Advies bieden over inrichting Sentinel, hardening Microsoft-producten, bijwerken playbooks. • In staat zijn (nieuwe) klantvragen te vertalen in een werkbaar en timeboxed plan van aanpak, waarin de randvoorwaarden, benodigde expertise en risico's in worden benoemd.
18	Om de uitvoering van de Opdracht door de Opdrachtnemer continu te verbeteren, evalueert de Opdrachtgever de Dienstverlening minimaal één keer per 6 weken. Deze evaluaties worden gezamenlijk uitgevoerd, zodat beide partijen de gelegenheid hebben om bevindingen en inzichten te delen. Op basis van deze 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.
19	Opdrachtnemer dient als onderdeel van de Dienstverlening (proactief) te adviseren over aanbevolen beveiligingsmeldingen vanuit de SIEM en deze te implementeren.
20	Opdrachtnemer monitort de beschikbaarheid van connectoren, waaronder de standaard Microsoft Azure dataconnectoren en aangesloten maatwerkconnectoren (bijvoorbeeld firewall) en informeert Opdrachtgever hierover. Afspraken hierover worden gemaakt en vastgesteld in de SLA.
	Gegevensbeveiliging

21	Opdrachtnemer maakt gebruik van huidige PIM-configuratie binnen de Azure tenant van Gooise Meren. *De huidige configuratie van de gemeente Gooise Meren kunt u opvragen via TenderNed middels het indienen van de geheimhoudingsverklaring (dit kan op elk moment na publicatie van de Inschrijving tot moment indienen Inschrijving), zie bijlage 16.*
22	Gegevens (ook van eventuele derde partijen) worden gehost binnen de Europese Economische Ruimte (EER). Gegevens worden niet (lokaal) opgeslagen op gegevensdragers buiten de EER.
23	Alle personen die vanuit Opdrachtnemer toegang hebben tot Azure/Sentinel voor de uitvoering van de Opdracht, hebben een eigen account dat herleidbaar is naar betreffende persoon.
24	Opdrachtnemer is verantwoordelijk voor het 24/7 monitoren van de SIEM van gemeente Gooise Meren. (Plaatselijke) connectiviteitsproblemen (zoals DDoS, stroomuitval) bij het SOC van Opdrachtnemer hebben geen invloed op kwaliteit en beschikbaarheid van de monitoring.
	Kwaliteitswaarborging
25	Medewerkers van de Opdrachtnemer die toegang hebben tot de verzamelde gegevens, zijn gescreend op integriteit op basis van screeningsprofiel 11, 12 en 13. De minimale eis is dat Nederlands personeel bij indiensttreding een voor de functie geldende Verklaring omtrent Gedrag (VOG) heeft overhandigd. Voor (eventueel) buitenlands personeel mag dit een vergelijkbaar document zijn.
26	Opdrachtgever kan periodiek vragen een nieuwe VOG (of vergelijkbaar) te overhandigen.
27	De Opdrachtnemer moet de privacy en bescherming van de verzamelde gegevens waarborgen in overeenstemming met relevante wet- en regelgeving, zoals de AVG, BIO en NIS2/Cbw.
28	Opdrachtnemer is in staat een actuele versie van het incident response-beleid aanleveren.
29	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 moet door middel van verklaringen zoals een SOC 2-rapport, een ISAE 3000-verklaring of een vergelijkbaar document. Een en ander conform eis 32.
30	Bij start van de uitvoering van de Opdracht en gedurende de gehele uitvoering van de Opdracht dient Opdrachtnemer Microsoft Partner te zijn voor de geleverde diensten bij het Sentinel product van Microsoft. Opdrachtnemer dient te beschikken over de status Microsoft Solutions Partner voor Security of gelijkwaardig en over de volgende door Microsoft geverifieerde specialisaties of gelijkwaardig: • Cloud Security • Threat Protection
31	Alle door Opdrachtnemer ingezette analisten beschikken over passende kennis en expertise over het gebruik van Microsoft-producten en de basispraktijk van security analyse binnen de Microsoft-omgeving. Hier wordt een minimaal certificeringsniveau van SC-200 of gelijkwaardig verwacht gedurende de looptijd van de Overeenkomst.
32	*Versie 2 eis 32:*

	Opdrachtnemer blijft gedurende de gehele looptijd van de Overeenkomst gecertificeerd voor 1. ISO 9001 of gelijkwaardig, 2. ISO 27001 of gelijkwaardig. Opdrachtnemer dient binnen 1 jaar na ingangsdatum van de Overeenkomst SOC-2 certificering of gelijkwaardig te hebben verkregen. Deze certificering dient Opdrachtnemer te behouden gedurende de resterende looptijd van de Overeenkomst.
33	De Opdrachtgever is te allen tijde gerechtigd om de uitvoering van de Overeenkomst te controleren, conform de GIBIT. 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.
	Notificatie
34	Opdrachtgever en Opdrachtnemer stemmen per meldingsprioriteit af hoe Opdrachtgever door Opdrachtnemer wordt geïnformeerd.
35	Opdrachtgever en Opdrachtnemer moeten specifieke afspraken kunnen maken over de situaties waarin notificaties volgen en hoe deze worden verzonden.
	Rapportage
36	Opdrachtnemer dient minimaal eens per 6 weken, de volgende service level rapportages te overhandigen: • Verrichte requests/aanvragen van de Opdrachtgever en status. • Aantallen events/alerts, meldingen aan de gemeente en incidenten naar classificatie, zoals informational, low, medium, high, critical. • Bevindingen worden gerelateerd aan gemaakte afspraken in de SLA/DAP. • Beschikbaarheid van diensten SOC en SIEM over de rapportageperiode. • Evaluatie en aanbevelingen. • Klachten en klachtafhandeling. • Een managementsamenvatting met daarin benoemd de dreigingen.
	Retransitie en beëindiging
37	Bij het eerste verzoek stelt de Opdrachtnemer binnen 10 werkdagen een gedetailleerd exitplan op, conform de GIBIT 2023, artikel 26.
38	Tijdens de periode van retransitie moet de Opdrachtnemer alle Dienstverlening voortzetten volgens de overeengekomen voorwaarden.
39	De Opdrachtnemer zal aan het einde van de Overeenkomst of van de retransitie alle vertrouwelijke informatie retourneren zonder een kopie te behouden, tenzij anders overeengekomen op basis van een (wettelijke) eis of verplichting, of op basis van aanvullende afspraken. Als het langer bewaren van een kopie van vertrouwelijke informatie verplicht is, zal deze informatie worden vernietigd zodra de bewaartermijn is verstreken.
	Contract en SLA, DAP
40	De mate en vorm van communicatie worden vastgelegd in een DAP en SLA.
41	Om de afgesproken kwaliteit te waarborgen, de dienstenniveaus te realiseren en verbeteringen door te voeren, is regelmatig overleg op verschillende organisatieniveaus noodzakelijk. De periodieke rapportages, zoals vermeld in eis 36 in deze bijlage, maken hier deel van uit. De Opdrachtnemer moet bij aanvang van de Opdracht in de SLA uitleggen hoe de communicatie met de Gemeente Gooise Meren wordt georganiseerd, inclusief frequentie, onderwerpen en betrokken niveaus. Daarnaast vindt er halfjaarlijks een evaluatie plaats, die zowel de communicatie als de naleving van de SLA betreft.
42	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 de Opdrachtnemer en Opdrachtgever.