



gemeente

Zoetermeer

NOTA VAN INLICHTINGEN (Correctie)

Marktconsultatie MDR en XDR

2024-175523

Auteursrecht

Alle rechten voorbehouden aan de Gemeente Zoetermeer

Nota van Inlichtingen

In dit document zijn de vragen inclusief antwoorden weergegeven die betrekking hebben op de Marktconsultatie MDR en XDR ten behoeve van Gemeente Zoetermeer. Indien in deze Nota van Inlichtingen wijzigingen, correcties dan wel aanvullende gegevens zijn opgenomen, zijn deze van toepassing het marktconsultatiedocument. Deze Nota van Inlichtingen maakt onlosmakelijk deel uit van de marktconsultatiedocumenten.

Vragen en Antwoorden

#	Onderwerp	Vraag	Antwoord
1.	E-5 licentie	Wij zouden u willen vragen of Gemeente Zoetermeer een E5-licentie heeft. Zo ja, of de Defender producten die in de E5 licentie zitten volledig zijn ingericht?	Zoetermeer heeft E5 licenties voor alle medewerkers. Defender voor E5 is volledige ingericht, Defender voor Cloud is inclusief updatemanager ingericht. Zoetermeer sluit niet uit dat ondanks de inrichting, optimalisatie kan plaatsvinden.
2.	-	Hoeveel gebruikers heeft de Gemeente Zoetermeer in haar IT-omgeving?	Op 21-01-2025 zijn er 1775 M365 E5 account actief.
3.	-	Zijn er specifieke eisen van toepassing v.w.b. de levering van deze dienstverlening (bijv. offshore toegestaan, nearshore (binnen EU/EER), of anderszids?)	Binnen de EU/EER.
4.	-	Hoeveel pagina's wenst u te hanteren voor de beantwoording?	Dit betreft een vormvrije marktverkenning zonder beperking op het aantal pagina's. Wel willen wij u vragen om niet onnodig veel pagina's aan te bieden om het leesbaar te houden.
5.	-	Kunnen jullie inzicht geven in de huidige monitoringstrategie van jullie interne SOC op het gebied van strategie, visie en ambities?	Onze huidige strategie richt zich voornamelijk op Microsoft-oplossingen. Wij streven ernaar om binnenkort meer inzicht te kunnen geven in onze monitoringstrategie, inclusief onze langetermijnvisie en ambities. Deze zijn nog in ontwikkeling of moeten nog ontwikkeld worden.
6.	1.2 Aanleiding en doel, 24/7	Wil de gemeente (1) volledig uitbesteden of (2) alleen buiten kantooruren? Indien (2), wat is de huidige bezetting van het team?	Het eerste beeld is dat het zowel gaat om volledige uitbesteding als om monitoring buiten kantooruren. Onze geadviseerde mitigatie is hierbij ons uitgangspunt. Momenteel zijn er 5 medewerkers die actief alerts oppakken. Deze medewerkers doen dit niet als hun kerntaak, maar naast hun reguliere werkzaamheden. Hun functies variëren van security specialisten tot netwerkbeheerders.
7.	1.2 Aanleiding en doel, XDR	Geïntegreerde analyse vereist informatie (loggegevens) van alle componenten. In paragraaf 1.3 geeft u aan dat het monitoren van firewalls en switches is uitbesteed aan externe	Het standaard beschikbaar stellen van third party logging is een kostbare oplossing. Echter, indien logging incidenteel noodzakelijk is, kunnen wij dit wel realiseren. Zoetermeer laat zich graag

#	Onderwerp	Vraag	Antwoord
		partijen. Worden de loggegevens ook beschikbaar gesteld aan de XDR-leverancier?	adviseren over dit onderwerp en gaat graag het gesprek aan met de markt.
8.	1.2 Aanleiding en doel, (Geautomatiseerde) Mitigatie	De uitwerking van zowel geadviseerde mitigatie (voorbereid door het SOC, maar uit te voeren door beheerders van de infrastructuur) als geautomatiseerde mitigatie (via playbooks) vereist inzicht in de resultaten van de BIA's en dus in het belang van de te bewaken assets. Zijn deze resultaten beschikbaar?	Zoetermeer begrijpt de vraag als volgt: Zal de opdrachtnemer inzicht verkrijgen in de resultaten van de business impactanalyse na de implementatie van het advies? Het logische antwoord hierop is ja. Het is aan de opdrachtnemer en Zoetermeer om dit gezamenlijk te realiseren.
9.		Wat is de dagelijkse log ingest voor MS Sentinel?	Gemiddeld 15,5 GB per dag.
10.		Op hoeveel van de vermelde 250 servers heeft Gemeente Zoetermeer MS Defender for Server Plan 1/2 geïnstalleerd?	110 servers zijn voorzien van MS Defender for Server Plan 2. Dit aantal zal komende jaren oplopen.
11.		Hoeveel E5 licenties heeft Gemeente Zoetermeer op de ingangsdatum van de M(X)DR dienst?	Op moment van beantwoording zijn er 1775 E5 licenties actief. Bij de ingangsdatum van de XDR/MDR dienst zal dat aantal tussen de 1700-1800 liggen.
12.		Vulnerability Management en Extended Attack Surface Management worden niet benoemd in de doelen, richtlijnen of vragen. Is dit ook een vereiste vanuit de gemeente?	Nee, dit is geen onderdeel van de marktconsultatie.
13.		Kan de gemeente toelichten hoe diens huidige Managed dienstverlening partners kijken naar het samenwerken met andere dienstverleners kijkt en welke eisen/voorwaarden de huidige Managed dienstverlening partners stellen aan de samenwerkingsverbanden?	Zoetermeer kan hier op dit moment nog geen definitief antwoord op geven. Er is vooraf geen contact geweest met onze partners over een mogelijke samenwerking met een MDR/XDR-partner. In het huidige landschap is samenwerking tussen partijen essentieel om de huidige dienstverlening te waarborgen. Zoetermeer neemt in deze situaties de regievoering op zich. Indien de opdrachtnemer specifieke randvoorwaarden heeft voor de samenwerking, nodig ik u uit om deze kenbaar te maken. Zo kan Zoetermeer hier rekening mee houden bij een eventuele aanbesteding.
14.	Pagina 4	In ronde 2 vinden 1 op 1 gesprekken plaats in week 7/8. Op basis van de schriftelijke reacties selecteert de Gemeente Zoetermeer een aantal partijen voor verdiepende één-op-één gesprekken. Impliceert dit dat niet alle deelnemende partijen worden uitgenodigd voor de 2e ronde? Hoeveel partijen worden uitgenodigd en op basis van welke criteria wordt er een selectie gemaakt?"	Uw aanname is correct. Indien de situatie zich voordoet dat Zoetermeer veel reacties ontvangt, zal Zoetermeer enkel de meest interessante antwoorden selecteren voor een één-op-één sessie. Dit betekent niet dat de overige antwoorden niet van belang zijn. Alle antwoorden dragen bij aan het totale beeld dat Zoetermeer kan opmaken. Helaas hebben wij op dit moment geen concrete criteria op basis waarvan de selectie wordt gemaakt.

#	Onderwerp	Vraag	Antwoord
15.	Marktconsultatie document - MDR XDR	Wat doet de gemeente Zoetermeer nu aan MDR? Ligt dit volledig bij de gemeente of zijn er externe partijen bij betrokken die dus ook een rol hebben bij migratie/onboarding naar de externe MDR-dienstverlener.	De opvolging van Sentinel-alerts wordt uitgevoerd door de security specialisten van de Gemeente Zoetermeer. De geadviseerde mitigatie vanuit onze firewallpartner wordt gezamenlijk opgepakt, afhankelijk van de ernst van de situatie.
16.	Marktconsultatie document - MDR XDR	Maakt de gemeente Zoetermeer gebruik van een externe partij voor Incident Response?	Er zijn afspraken gemaakt met een van onze leveranciers voor IR ondersteuning. Dit betreft geen CERT retainer.
17.	Marktconsultatie document - MDR XDR	Hoe schat de gemeente Zoetermeer op dit moment de eigen volwassenheid op het gebied van security monitoring in?	Vanuit gemeentelijk perspectief is het volwassenheidsniveau goed.
18.	Marktconsultatie document - MDR XDR	Kunt u specificeren welke Microsoft E5 features momenteel actief gebruikt worden en welke nog niet?	Dit zijn de belangrijkste features binnen de E5 licentie welke worden gebruikt: - Exchange online Plan 1 - Microsoft 365 Copilot (hier doet GZ een pilot mee) - Microsoft Fabric - Microsoft Power Apps Plan 2 Trial - Microsoft Power Automate - Microsoft Stream Trial - Teams Rooms Basis - Teams Rooms Pro - Planner and Project Plan 3 - Power Apps Premium - Visio Plan 2 - Entra ID - Intune - Purview - Defender for Endpoint - Defender for Cloud - Defender for Servers - Microsoft Sentinel - Conditional Access - Risk detection - Power Platform Deze lijst is niet volledig maar geeft een goed beeld welke features binnen de gemeente worden gebruikt.

#	Onderwerp	Vraag	Antwoord
19.	Marktconsultatie document - MDR XDR	Kunt u meer details geven over de "geplande migratie naar de cloud in de komende jaren"?	Veel leveranciers van de gemeente Zoetermeer stappen over naar SaaS. Hierdoor worden bestaande on-premise oplossingen naar de cloud gemigreerd, waardoor naar verwachting onze kritieke applicaties binnen 3 jaar naar de cloud verhuizen.
20.	-	Maakt de gemeente Zoetermeer gebruik van webapplicaties voor externen en zijn deze buiten scope of dient hier rekening mee te worden gehouden in een eventuele aanbidding? Reden voor deze vraag is om er zeker van te zijn dat ook de 'niet Microsoft gerelateerde' oplossingen onder de dienstverlening kunnen worden ondergebracht.	Binnen de scope vallen alleen (web)applicaties die de productiviteit van onze medewerkers ondersteunen of zorgen voor connectiviteit met onze systemen. (Web)applicaties voor inwoners of (web)applicaties verbonden aan SaaS dienstverlening vallen buiten de scope van de uitvraag.
21.	-	Welke eisen stelt Gemeente Zoetermeer aan de gewenste incident response?	In deze marktconsultatie stellen we nog geen eisen. We willen graag uitvinden wat de markt biedt.
22.	-	Hoe ziet de bestaande infrastructuur van Gemeente Zoetermeer er nu en in de nabije toekomst uit?	Zie hiervoor de beschrijving van onze infra die we hebben meegegeven. In eventueel gesprek kunnen we hier dieper op in gaan, maar een openbare marktconsultatie is niet de plek om hier in detail op in te gaan.
23.	-	Is de mogelijkheid aanwezig om te koppelen met de oplossingen van derde partijen (firewallbeheerder/netwerkbeheerder) om de dienstverlening zo compleet mogelijk te kunnen verzorgen?	Dit moet binnen de mogelijkheden liggen en Zoetermeer staat hiervoor open.
24.	-	Verwacht Gemeente Zoetermeer ook een behoefte aan monitoring van haar externe aanvalsvlak? Denk hierbij aan darkweb monitoring, data- en credential leakage, phishing etc..	De genoemde opties vallen niet binnen de scope van deze marktconsultatie.
25.	-	Kan Gemeente Zoetermeer aangeven hoe zij tot de telling van het aantal endpoints uitgekomen is? Bijvoorbeeld: Niet alle Wifi access points dienen te worden beschouwd als een separate asset indien deze centraal gemanaged kunnen worden. Ditzelfde geldt voor printers, switches, toegangssystemen, IoT devices etc.	U kunt aannemen dat de telling zorgvuldig en representatief is voor de omgeving van Zoetermeer.