gemeente Schiedam

Marktconsultatie
MSSP-Diensten
met dossiernummer '-2.07.353.221/00063

Ontvangen vragen Marktconsultatie 24-11-2025

Ref. nr.	Onderwerp	Vraag	Antwoord
1	**De rol van automatisering versus 'ogen op het scherm'**	In uw document beschrijft u de wens voor 24/7 "ogen op het scherm" monitoring. Onze ervaring is dat een AI-gestuurde, geautomatiseerde monitoring en detectie niet alleen sneller en nauwkeuriger is in het identificeren van dreigingen, maar ook aanzienlijke kostenvoordelen biedt. In hoeverre staat de gemeente Schiedam open voor een aanpak waarbij automatisering de primaire monitoring uitvoert, met een 'human in the loop' voor complexe incidenten en analyses, in plaats van een traditionele, volledig mens-afhankelijke 'ogen op het scherm'-dienstverlening?	Uitgangspunt is dat er 24/7 real-time monitoring is waarbij waarschuwingen worden opgevolgd door een natuurlijke persoon met voldoende kennis (Tier 2 of Tier 3) om een beoordeling te maken en om verbanden te zien, te acteren en vervolgacties te nemen. U kunt in de marktconsultatie een toelichting geven op de wijze waarop invulling wordt gegeven aan het '24/7 monitoring door een natuurlijk persoon' mocht dit AI gestuurd zijn.
2	**Efficiëntie en schaalbaarheid bij gefaseerde uitrol**	U geeft aan te willen starten met een pilot op één systeem en dit gefaseerd uit te breiden. Een geautomatiseerd platform kan doorgaans zeer efficiënt en snel nieuwe systemen en logbronnen integreren, vaak met lagere incrementele kosten dan bij een op man-uren gebaseerde dienst. Hoe ziet u de ideale schaalbaarheid van de oplossing voor u, en welke rol speelt de efficiëntie van het toevoegen van nieuwe systemen in uw evaluatie van een MSSP-partner voor de lange termijn?	Voor de uitrol is het van belang dat de gemeente Schiedam het tempo bepaalt. Tijdens de uitvoering van de opdracht en het gefaseerd uitrollen verwacht de gemeente een efficiënte en adviserende rol van de leverancier.
3	**Toegevoegde waarde op de bestaande ELK-stack**	De gemeente is bezig met het opzetten van een centrale loggingomgeving op basis van een ELK-stack, die als primaire bron dient. Ons AI-platform kan direct op dergelijke databronnen aanhaken om geavanceerde correlatie en dreigingsdetectie uit te voeren, veel verder dan standaard rule-based monitoring. Welke verwachtingen heeft u van de MSSP met betrekking tot het verrijken van de data uit uw ELK-stack en het leveren van proactieve, voorspellende analyses in plaats van enkel reactieve alarmering?	De gemeente Schiedam beschikt over een centrale logging en zal, gefaseerd in uitrol, de logevents 1-op-1 zonder verlies doorsturen naar de MSSP. Het gaat dus altijd alleen om sturen, nooit om ontvangen. Het is niet mogelijk om data aan te passen of aan te vullen. Analyses worden bij de MSSP uitgevoerd.

Ref. nr.	Onderwerp	Vraag	Antwoord
4	**Kostenmodel en betaalbaarheid voor de publieke sector**	In de marktconsultatie (Annex 1, Vraag 4) vraagt u om een kostenindicatie. Onze oplossing is specifiek ontwikkeld om geavanceerde SIEM/SOC-diensten betaalbaar te maken voor middelgrote (publieke) organisaties, door manuele processen verregaand te automatiseren. Kunt u een indicatie geven van de budgettaire kaders waarbinnen u een oplossing zoekt, en in welke mate is de 'total cost of ownership' over een periode van bijvoorbeeld drie jaar een belangrijke factor in uw uiteindelijke keuze?	De gemeente Schiedam wil op basis van de marktconsultatie bepalen welke oplossing het best passend is, waarbij gekeken wordt naar de totale kosten om zo ook het benodigde budget te bepalen. Er is op dit moment nog geen budget vastgesteld.
5	**Geautomatiseerde incidentrespons**	U stelt in Vraag 3 de relevante vraag of een MSSP direct kan ingrijpen om escalatie te voorkomen. Geautomatiseerde respons (SOAR-functionaliteit) is een kernonderdeel van moderne beveiligingsplatforms en kan, op basis van vooraf gedefinieerde playbooks, direct en foutloos ingrijpen (bv. een account blokkeren of een IP-adres isoleren). In hoeverre bent u geïnteresseerd in een dienst die niet alleen detecteert, maar ook (in overleg en conform afspraak) geautomatiseerd kan reageren op incidenten om de responstijd significant te verkorten en de afhankelijkheid van directe menselijke interventie te verlagen?	De gemeente Schiedam wil 24/7 real-time monitoring door een natuurlijke persoon, voor de MSSP geldt dat er altijd een menselijke beoordeling gewenst is. De response naar de gemeente Schiedam komt niet vanuit een geautomatiseerd proces zonder beoordeling. Wij verwachten een toelichting op mogelijkheden die de MSSP biedt op dit gebied.
6	**Paragraaf 1.2 - De Opdracht**	De gemeente Schiedam is voornemens een Security Operations Center (SOC) en Security Information and Event Management (SIEM) in te richten om haar digitale infrastructuur proactief te monitoren en te beveiligen. In dit kader wil de gemeente een Managed Security Service Provider (MSSP) contracteren die 24/7 toezicht houdt op de systemen, met als doel proactief detectie van risico's en het (in overleg c.q. conform afspraak) nemen van passende maatregelen bij incidenten. **Betekent dit dat de MSSP dienst volledig wordt uitbesteed? Dus Tier 1 t/m tier 3? Of is dit deels en zo ja, welke Tier diensten wilt u afnemen?**	Gemeente Schiedam is voornemens Tier 1 t/m 3 af te nemen.
7	**Paragraaf 1.2 - De Opdracht**	Verder geeft u aan dat MSSP dienst 24/7 toezicht betreft en is dus gebaseerd op 'eyes on screen'. **Dient incident handeling door de MSSP service dienst (mitigerende, forensische werkzaamheden) ook buiten kantoortijden te worden uitgevoerd? Zo ja, is een IT/Security beheerder van Gem. Schiedam op die tijden ook beschikbaar?**	Incidentafhandeling binnen de MSSP-dienst dient wanneer nodig ook buiten kantoortijden te worden uitgevoerd. Forensische werkzaamheden vallen daar in principe niet standaard onder; deze worden alleen in uitzonderlijke gevallen en altijd in overleg met, en na beoordeling door, de opdrachtgever uitgevoerd. Voor reguliere mitigerende acties is er buiten kantoortijden een IT/Security-beheerder van Gemeente Schiedam beschikbaar, zodat we de opvolging goed kunnen coördineren.
8	**Paragraaf 1.2.2 - CPV code**	U benoemt een tweetal diensten met CPV code: 7231500-6 Beheer van datanetwerken en ondersteunende diensten & 72000000-5 IT-diensten: adviezen, softwareontwikkeling, internet en ondersteuning. Gaat u beide diensten inderbrengen in de MSSP dienst? Zo ja, volgt deze aanvraag ook een in de komende Europese aanbesteding?	Er is gekozen voor meerdere CPV codes om een groot bereik te genereren voor deze Marktconsultatie. Hetgeen wat wordt meegenomen in de aanbesteding volgt in de scope en zal openbaar worden gemaakt bij publicatie via TenderNed.

Ref. nr.	Onderwerp	Vraag	Antwoord
9	**Paragraaf 1.3 - Huidige situatie**	U geeft aan systemen on-premises draaien binnen de gemeentelijke infrastructuur, terwijl andere systemen als clouddienst worden afgenomen. **Bij welke cloud provider wordt deze cloud dienst afgenomen?**	Dit zijn verschillende Cloud Leveranciers, welke marktconform zijn binnen de overheid.
10	**Paragraaf 1.4 - Doelstelling en gewenste situatie**	De gemeente Schiedam is een decentrale overheidsorganisatie en dient te voldoen aan de wettelijke eisen ten aanzien van informatiebeveiliging, waaronder de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). **Wordt volgend jaar na de marktconsultatie NIS2 ook meegenomen in de Europese aanbesteding?**	Ja, wetgeving wordt gevolgd.
11	**Paragraaf 2.1 - Doel van de marktconsultatie**	U geeft aan dat Gem. Schiedam binnen 12 maanden na publicatie van het verslag overgaan tot het naar de markt brengen van MSSP-diensten, zal het verslag als bijlage met de aanbestedingsstukken worden toegevoegd. **Kunt u wat specifieker zijn in de planning? Wellicht in eerste half jaar? Dit om ervoor te zorgen dat (vanwege implementatie periode) u per 1-1-2027 een operationele MSSP dienst heeft**	Dit zal mede afhankelijk zijn van de oplossing en het te volgen inkooptraject. De planning kan om deze redenen nog niet worden vastgesteld.
12	**Annex 1 Vragen en antwoorden**	U heeft geen prijsindicatie gevraagd in de 6-tal vragen. Heeft u budget reeds vastgesteld? Zo niet, wenst u hier advies?	Er is geen budget vastgesteld. Doel is om dit op basis van de marktconsultatie te doen.

Ref. nr.	Onderwerp	Vraag	Antwoord
13	**Annex 1 Vragen en antwoorden**	De gemeente Schiedam wil in het de pilot fase slechts één systeem laten monitoren en daarna geleidelijk uitbreiden zodat we aan het einde van het jaar alle componenten hebben opgenomen. **Het is echter moet raadzaam om te beginnen met slechts één apparaat aan een SIEM-systeem toe te voegen, zelfs als dit alleen als een pilot zou worden beschouwd. Dit beperkt namelijk het vermogen om bedreigingen effectief te detecteren en ondermijnt de kernfunctionaliteit van het SIEM-systeem. De kracht van een SIEM ligt in het verzamelen en correleren van data uit diverse bronnen om een compleet overzicht van de beveiligingssituatie te krijgen. Bent u eens met dit advies? Zo niet, wat is uw doel met de pilotfase?**	Wij nemen uw advies niet over. De gemeente Schiedam wil in de pilotfase starten met het monitoren van één systeem en dit daarna stapsgewijs uitbreiden, zodat aan het einde van het jaar alle componenten zijn opgenomen.
14	**TenderApp MSSP-diensten pagina 1 Punt 1: 24/7 security monitoring (SOC) met actieve “eyes on screen”.**	MSSP heeft een reactietijd buiten kantooruren en op feestdagen van 15 minuten. Heeft u 24x7 medewerkers op locatie om de context van eventuele security dreigingen die wij vinden te kunnen beoordelen zodat wij direct een incident of aanval kunnen afwenden?	Voor reguliere mitigerende acties is er buiten kantoortijden een IT/Security-beheerder van Gemeente Schiedam beschikbaar, zodat we de opvolging goed kunnen coördineren.
15	**TenderApp MSSP-diensten pagina 2: Integratie met de centrale ELK-logging, waarbij de MSSP logdata ontvangt vanuit de gemeentelijke logcollector; de gemeente is voornemens loggegevens via een realtime, gestandaardiseerde connectie te pushen.**	Hoeveel ELK-logging kan MSSP per dag ontvangen?	Deze informatie is op dit moment nog niet bekend.
16	**TenderApp MSSP-diensten pagina 2: Integratie met de centrale ELK-logging, waarbij de MSSP logdata ontvangt vanuit de gemeentelijke logcollector; de gemeente is voornemens loggegevens via een realtime, gestandaardiseerde connectie te pushen.**	Tot hoeveel dagen terug kunnen we in uw ELK Logging platform de data terug vinden of zoeken?	Er is geen mogelijkheid historische data te raadplegen, omdat wij voornemens zijn de logging te verzenden. Het is wel mogelijk zelf historie te bewaren.

Ref. nr.	Onderwerp	Vraag	Antwoord
17	**TenderApp MSSP-diensten pagina 2: Integratie met de centrale ELK-logging, waarbij de MSSP logdata ontvangt vanuit de gemeentelijke logcollector; de gemeente is voornemens loggegevens via een realtime, gestandaardiseerde connectie te pushen.**	Uit welke systemen//bronnen ontvant uw ELK-Logging platform de data en welke niet?	Dit is benoemd in beschrijving op globaal niveau. Specifieke system worden uit veiligheidsoverweging niet nader genoemd.
18	**Marktconsultatie MSSP-diensten: Pagina 6 paragraaf 1.3; Werkplekken vallen (op dit moment) buiten de scope van deze opdracht. De MSSP gaat alleen de kritieke componenten controleren**	Waarom heeft u de wens om uw werkplekken buiten scope te houden? Dit zijn voor ons als MSSP cruciale loggegevens. Wij zien bij onze huidige klanten dat hier een XDR oplossing is geimplementeerd en ons advies is om dit ook voor u te implementeren. Hierdoor hebben wij veel meer inzicht en kunnen we snleer acteren en missen we geen cruciale aanvalsvectoren.	De prioriteit ligt op dit moment niet bij de werkplekken en zijn daarom in deze fase buiten de scope gehouden. De werkplekken zijn daarmee zeker niet uitgesloten.
19	**Secuirty monitoring van endpoints en servers wordt door de markt als primair en meest essentieel gezien**	Kunt toelichten waarom Gemeente Schiedam voornemens is dit pas na de pilot fase te realiseren?	De gemeente Schiedam wil in de pilotfase starten met het monitoren van één systeem en dit daarna stapsgewijs uitbreiden, zodat aan het einde van het jaar alle componenten zijn opgenomen.
20	**werkplekken**	Wat zijn de overwegingen van de gemeente om werkplekken vooralsnog buiten de scope van de MSSP te houden?	De prioriteit ligt op dit moment niet bij de werkplekken en zijn daarom in deze fase buiten de scope gehouden. De werkplekken zijn daarmee zeker niet uitgesloten.
21	**Cloudomgevingen en SaaS-applicaties**	Verwacht de gemeente ook logging te (gaan) ontvangen vanuit Cloudomgevingen en SaaS-applicaties?	Ja, deze verwachting heeft de gemeente.
22	**De gemeente wenst initieel één systeem onder toezicht te plaatsen.**	A) Klopt de aanname dat dit systeem de ELK-stack betreft waarin van diverse omgevingen de loginformatie wordt verzameld? B) Zo ja, om wat voor soort bronnen gaat het? C) Zit hier ook logdata bij afkomstig van Vitale Objecten (OT-omgeving)? D) Hoeveel data komt er binnen in de ELK-stack? E) Hoeveel data wordt aan de MSSP beschikbaar gesteld?	A. Ja, deze aanname klopt. B. Diverse bronnen, zoals benoemd in 1.2.1. C. Initieel zit hier geen logdata bij. D. De hoeveelheid is nog onbekend. E. de hoeveleelheid is nog onbekend.

Ref. nr.	Onderwerp	Vraag	Antwoord
23	**24 7 security**	Gemeente heeft het over 24x7 eyes on screen. Wij zien deze “eis” zelden binnen de lokale overheid voorbij komen daar de noodzaak er niet voor is, opdrachtgever zelf niet over 24x7 continue beschikbaarheid beschikt maar op basis van standby/consignatiedienst acteert. Derhalve is 24x7 actieve Monitoring op basis van strakke SLA en directe acties op P1 en P2 op basis van standby dienst voldoende. En betaalbaar. Kan de gemeente Schiedam daar ook mee uit de voeten?	Voor de gemeente is direct actie in voorkomende situaties uiterst belangrijk. Een wekdienst zou daarbij mogelijk een te lange doorlooptijd hebben. De gemeente kan hiermee dus niet uit de voeten.
24	**Annex 1 vraag 3**	Bij vraag 3 van Annex 1 heeft u het over ingrijpen. Dat is een breed begrip en laat veel ruimte over voor interpretatie. Kunt u aangeven wat uw beeld is bij ingrijpen?	“Ingrijpen” door een MSSP betekent dat een analist — dus altijd een mens en geen automatische actie — een gedetecteerde dreiging beoordeelt en vervolgens handmatig maatregelen neemt om de impact te beperken of een incident te stoppen. Daarbij kun je denken aan handelingen zoals: • het isoleren van een systeem, • het blokkeren van een verdachte gebruiker of verbinding, • het stoppen van een schadelijk proces, • of het adviseren over vervolgstappen wanneer directe actie in de omgeving niet mogelijk is. Alle acties gebeuren dus bewust en gecontroleerd, na menselijke beoordeling, en nooit volledig automatisch.
25	**Alerts**	Vallen alerts vanuit Microsoft 365/Entra ID binnen de scope van de monitoring, of richt u zich primair op infrastructuurcomponenten?	Ja, alerts vanuit Microsoft 365/Entra ID vallen binnen scope.
26	**Scope**	U geeft aan dat werkplekken op dit moment buiten scope vallen van deze opdracht. Betekent dit dat endpoint detection & response (EDR) voor de 840 werkplekken (VDI en laptops) volledig buiten de MSSP-dienstverlening blijft, of verwacht u wel monitoring van beveiligingssignalen die via Microsoft Defender for Endpoint of vergelijkbare tooling vanaf deze endpoints worden gegenereerd binnen uw Microsoft 365 omgeving?	In een later stadium zullen wij voornemens zijn inderdaad de EDR/XDR oplossing die we gebruiken te koppelen aan Elastic ELK, waardoor deze informatie beschikbaar komt. Dit wordt nader in de aanbestedingsdocumentatie gespecificeerd.