Opdrachtbeschrijving

De gemeente Katwijk voert deze Europese Aanbesteding uit om een overeenkomst af te sluiten met een Opdrachtnemer die een Managed Detectie en Response (MDR) dienst levert. Wij verwachten van deze dienstverlening:

- Continue monitoring en detectie – 24/7 bewaking van endpoints, identiteiten, accounts en cloudomgeving om bedreigingen in realtime te identificeren.
- Geavanceerde dreigingsanalyse – Gebruik van machine learning en dreigingsinformatie (Threat Intelligence) om verdachte activiteiten te herkennen, eventueel gebruik makend van AI.
- Incidentrespons en mitigatie – Actieve ondersteuning bij het indammen en neutraliseren van cyberaanvallen om schade te minimaliseren.
- Forensisch onderzoek en rapportage – Analyse van beveiligingsincidenten om de oorzaak te achterhalen en toekomstige aanvallen te voorkomen.
- Expertbeheer en ondersteuning – Het uit handen nemen van dreigingsdetectie en -respons.

Hierbij zijn een aantal randvoorwaarden, namelijk dat :

- Wij de MDR oplossing met behulp van Microsoft Sentinel in onze eigen Microsoft Katwijk tenant vorm willen geven.
- Wij optimaal gebruik willen maken van de mogelijkheden van onze Microsoft 365 E5 licenties en verder willen bouwen op de huidige inrichting o.a. Intune, Defender for Cloud en Conditional Access policies.
- Wij ambiëren om mitigatie van beveiligingsincidenten binnen afgesproken kaders zoveel mogelijk zonder tussenkomst van de gemeente te laten uitvoeren.
- Aan alle eisen zoals in het Programma van eisen uiteengezet, wordt voldaan.

Scope / Omgeving gemeente Katwijk

Katwijk heeft een moderne IT-omgeving waarvan de belangrijkste kenmerken zijn:

- De omgeving is Microsoft-based, we maken zoveel mogelijk gebruik van Microsoft producten.
- We beschikken over een Microsoft 365 E5 licentie en de daarbij behorende producten zijn grotendeels ingezet.
- SAAS tenzij, wij nemen onze applicaties waar mogelijk als SAAS dienst af.
- In onze Azure Cloud draaien ongeveer 30 servers, er draaien geen servers meer on-premise.
- Moderne werkplek, eigen medewerkers werken op laptops die via VPN met onze Azure Cloud zijn verbonden. Externe medewerkers werken op een Windows 365 virtuele desktop.
- De client omgeving bestaat uit ruim 900 Windows clients, 650 Android clients en 30 iOS/iPadOS clients (totaal ongeveer 1600 endpoints).
- De Gemeente Katwijk is in bezit van 950 Microsoft 365 E5 licenties.

- Beheer van de omgeving geschiedt door eigen medewerkers, waar nodig met ondersteuning van partners.

Gewenst eindresultaat

De opdrachtnemer dient de bestaande Sentinel inrichting te gaan beheren en hiervan de SOC-dienstverlening te leveren. Het acteren op basis van events van potentiële dreigingen en risico's wordt bij de implementatie ingeregeld en afspraken hierover worden vastgelegd in een SLA.

Diverse logbronnen zijn aangesloten op Sentinel, zoals Microsoft Azure, Microsoft EntraID, Microsoft Active Directory, Microsoft Defender for Endpoint, Defender for Identity, Conditional Access, Microsoft 365 en Azure Firewall.

De Gemeente Katwijk wil na het sluiten van de overeenkomst via een scan of via workshops (de mogelijke uitbreiding van) de scope van de Usecases gezamenlijk bepalen.

Bij de inrichting zal de Opdrachtnemer ons ontzorgen door middel van projectbegeleiding en het in samenspraak definiëren en uitwerken van praktische Usecases. Afspraken over o.a. rapportages en processen dienen te worden gemaakt in documenten zoals een DAP en/of een SLA.

Verder dient de Opdrachtnemer een (API-) koppeling naar de Topdesk omgeving te realiseren, zodat beveiligingsincidenten worden geregistreerd en kunnen worden opgepakt vanuit Topdesk. Over de te verrichten handelingen bij diverse categorieën security incidenten worden ook afspraken gemaakt.

Opdrachtnemer adviseert de Gemeente Katwijk gevraagd en ongevraagd over nieuwe ontwikkelingen in de markt en over nieuwe producten.

Bij het aansluiten van eventuele toekomstige logbronnen zal samen met de Gemeente Katwijk een (mini-)project worden opgestart.