Marktconsultatie MDR - maart/april 2025

Nr.	Vraag	Partij 1	Partij 2
1	1. In bijlage treft u de belangrijkste concept eisen aan voor de Europese Aanbesteding. Zijn deze naar uw inzicht proportioneel? Welke eisen ontbreken hier	zie separaat document	zie separaat document
2	2. Hoe zien gegadigden het proces na de triage, wat zijn de vervolgstappen in het proces indien er een urgente bedreiging is vastgesteld? Ziet u een rol voor de opdrachtnemer in dit Incident Respons Proces (o.a. bij het forensisch onderzoek en	IR diensten zouden moeten worden aangeboden, belangrijk zijn goede afspraken over het mandaat.	Partij beschrijft haar handboek waarin procedures beschreven zijn voor verschillende typen en impact van
3	3. Aanbestedende dienst wil (zoals in de concept eisen benoemd), m.b.v. Microsoft Sentinel in haar eigen tenant werken als MDR oplossing. Dit betekent dat het verzamelen van teveel logdata zal leiden tot hoge Microsoft licentie kosten. Welke mogelijkheden zien gegadigden om in het belang van Opdrachtgever te doen aan kostenoptimalisatie v.w.b. de Microsoft Sentinel gerelateerde kosten? Welke eisen / wensen kan Opdrachtgever formulieren om aan marktpartijen te vragen om	AD kan ON vragen om te helpen bij het opzetten en uitvoeren van een opslagbeleid.	Partij omschrijft aan de hand van een voorbeeld uit een andere aanbesteding hoe AD de wens tot kostenbeheersing goed zou kunnen formuleren, en wat hierbij de overwegingen zijn.
4	4. Hoe kunnen inschrijvers onderscheidend zijn t.a.v. het configureren van detectieregels? Welke eisen of wensen kan Aanbestedende Dienst formuleren om naast het minimaal vereiste (i.h.k.v. wet- en regelgeving zoals BIO en NIS2) ook flexibel gebruik te maken van nieuwe ontwikkelingen en inzichten vanuit de Opdrachtnemer?	Het onderscheid zit in de kwaliteit van de detectieregels, niet in de kwantiteit. Partij benadrukt het automatiseren van het proces van leveren van detectieregels, alsmede het	Partij beschrijft het proces van detection engineering als een onderscheidend vermogen, en het doen van eigen onderzoek.
5	5. Welke gunningscriteria m.b.t. kwaliteit adviseert u ons te gebruiken?	Detectie, SLA, expertise en rapportage.	Partij beschrijft klanttevredenheid en verwijst naar een andere Europese aanbesteding voor de
6	6. Wat voor mogelijkheden zien gegadigden om autonoom te opereren (d.w.z. zelfstandig schade beperkende acties uitvoeren zonder tussenkomst van Opdrachtgever). Deze acties worden uiteraard gecombineerd met communicatie richting gemeente.	Partij benoemt het belang van autonoom handelen en benadrukt duidelijke afspraken over mandaat en communicatie.	Partij beschrijft de business impact, context en details als belangrijke factoren om een ingreep te doen, en maakt hierbij onderscheid in de

Marktconsultatie MDR - maart/april 2025

Nr.	Vraag	Partij 1	Partij 2
7	7. Welke dienstverlening kan de markt bieden in geval van cyberincidenten (zoals ransomware, dataexfiltratie en malware infectie)?	IR diensten	Partij beschrijft de mogelijkheden van haar CERT team.
8	8. Hoe adviseert u Aanbestedende Dienst om haar prijzenformulier vorm te geven teneinde een goede vergelijking te kunnen maken en een representatieve prijs voor de dienstverlening uit te vragen? M.a.w. welke informatie heeft u nodig en welke flexibiliteit heeft u nodig om in het document de juiste kostendrijvers en aantallen te kunnen opsommen om te komen tot een totaalprijs voor de dienstverlening.	Partij benoemt diverse kosten soorten voor eenmalige, terugkerende en incidentele kosten.	Partij adviseert om te denken in eenheidsprijzen en om voor de kostendrijvers te werken met inschattingen als er geen cijfers bekend zijn. Aandacht voor groei wordt
9	9. Wat zijn nieuwe ontwikkelingen en hoe kunnen wij dit in de aanbesteding meenemen?	nvt	Partij ziet OT-security als een ontwikkeling maar adviseert dit onderwerp niet op te nemen als

Nr.	Partij 3	Partij 4	Partij 5	Partij 6
1	zie separaat document	zie separaat document	zie separaat document	zie separaat document
2	Partij benoemt triage, isolatie en advisering.	Partij beschrijft de mogelijkheden bij een incident en de stappen bij een urgente bedreiging.	Partij benoemt het belang van een gestructureerd stappenplan en beschijft dat.	Partij omschrijft het mandaat voor impact-beperkende acties. Verder worden IR en forensische diensten
3	Partij benoemt mogelijkheden om de data ingestie te beperken.	Partij benoemt afstemming tijdens de onboarding fase om een optimale configuratie van de omgeving te realiseren en beschrijft hoe zij voor AD de consumptie beheersbaar kan houden.	Partij benoemt enkele belangrijke strategieën en overwegingen om de dataverzameling en de kosten te optimaliseren.	Partij adviseert om NDR buiten scope te laten en om andere logbronnen zoveel mogelijk buiten het MS-ecosysteem te houden. Hiermee blijven kosten beheersbaar.
4	Partij benoemt het meedenken over het inrichten van regels op basis van usecases.	Partij beschrijft het gebruik van geavanceerde technologieën, contextuele detectie en automatisering en orkestratie.	Partij benoemt enkele manieren om geavanceerde technieken toe te passen bij het configureren van detectieregels.	Partij beschrijft detection engineering, het omzetten van nieuwe kwetsbaarheden in passende regels. Threat hunting en Threat Intelligence advissert partij als vast onderdeel van
5	Partij benoemt het partnerschap met een contactpersoon, en het bieden van meer dan standaard regels.	Partij beschrijft enkele geadviseerde gunningscriteria met betrekking tot kwaliteit.	Partij benoemt enkele aanbevolen gunningscriteria ter overweging.	Partij heeft deze vraag, gezien het antwoord, niet correct geïnterpreteerd.
6	Partij benoemt first response, het blokkeren van hosts of gebruikers zonder tussenkomst van AD, dit uiteraard op basis van duidelijke	Partij beschrijft de mogelijkheden tot autonoom handelen, met aandacht voor mandaat, afspraken en communicatie.	Partij benoemt enkele situaties waarin zij autonoom handelen zou willen toepassen.	Partij verwijst naar het antwoord op vraag 2, waar haar diensten zijn beschreven.

Nr.	Partij 3	Partij 4	Partij 5	Partij 6
7	Partij benoemt forensische ondersteuning.	Partij beschrijft haar diensten in geval van cyberdreigingen en incidenten.	Partij beschrijft haar dienstverlening bij cybersecurity incidenten.	Partij verwijst naar het antwoord op vraag 2, waar haar diensten zijn beschreven, en geeft enkele
8	Partij benoemt dat moet kunnen worden gecalculeerd met aantallen endpoints, GB ingestie, log sources, meta data.	Partij adviseert een flexibel PxQ model te hanteren, en geeft hiervan een beschrijving. De kostendrijvers voor de dienstverlening worden benoemd, waarvan de aantallen bekend moeten	Partij benoemt diverse aspecten om rekening mee te houden teneinde een prijzenformulier te construeren dat leidt tot een representatieve prijs voor de dienstverlening op basis waarvan	Partij ziet graag onderscheid tussen prijs voor onboarding en dienstverlening. Partij spreekt ook de behoefte uit om de prijzen te mogen indexeren.
9	Partij benoemt SOAR, obv machine learning en AI, maar benoemt ook de waarde van menselijk denken.	Partij beschrijft AI en ML, en beschrijft hoe zij dit toepast in haar dienstverlening.	Partij benoemt enkele recente trends en beschijft hoe deze kunnen worden geïntegreerd in het	Partij benoemt continuous vulnerability management, purple teaming en incident response