



Verslag Marktconsultatie

In de periode van 24 maart t/m 27 maart heeft Aanbestedende Dienst (in het vervolg: AD) met 6 marktpartijen (in het vervolg: Partijen) gesproken. Dit document en zijn bijlagen geven op anonieme wijze een verslag van de besproken aspecten en ingediende antwoorden op de vragen.

De vragen 2 t/m 9 uit de schriftelijke consultatie zijn samengevat in de bijlage '20250523 Antwoorden marktconsultatie'

Opbrengst gesprekken en de schriftelijke marktconsultatie t.a.v. eisen en opdracht

Procedure: Partij geeft aan dat een niet-openbare aanbesteding met onder andere een dialoogronde, als kwalitatief beter wordt ervaren.

Procedure: Partij geeft aan een aanbesteding te adviseren met een selectiefase en een gunningsfase, met een dialoogronde in de gunningsfase.

Opdracht: Dreigingsanalyse wordt nu uitgevraagd, maar dat is feitelijk meer dan Threat Intelligence. Het advies van Partij is om Threat Intelligence als vast onderdeel van de opdracht uit te vragen en dreigingsanalyse eventueel optioneel te maken.

Opdracht: Partij adviseert om bij de kostenoptimalisatie goed te kijken naar de data ingestie, en goed te filteren bij de bron.

Opdracht: Partij adviseert om duidelijk aan te geven wat de verwachtingen zijn bij incident respons.

Opdracht: Partij geeft aan dat Honeypots niet gebruikelijk zijn in gemeentelijke infrastructuur.

Opdracht: Partij geeft aan dat Threat Intelligence en Threat Hunting zou passen als vast onderdeel van de aanbesteding, dus niet optioneel.

Opdracht: Partij geeft aan dat Threat Intelligence in haar ogen een eis zou moeten zijn. Dit betreft het inwinnen van informatie over bedreigingen. Dat kan door middel van feeds, maar er zijn nog diverse andere mogelijkheden.

Opdracht: Partij is benieuw hoe AD tegen de kostenoptimalisatie aan kijkt. AD geeft aan hierin zoekende te zijn en zich ook via vraag 3 uit de marktconsultatie graag laat adviseren hoe dit kan worden uitgevraagd.

Opdracht: Partij koppelt terug dat in de situatie van AD het niet heel zinvol is om Honeypots af te nemen. Deze worden vooral gebruikt om kennis te ontwikkelen over hoe aanvallers acteren, deze informatie kan weer worden gebruikt in threat intelligence. Partij adviseert dan ook om geen Honeypots uit te vragen.

Opdracht: Partij vraagt zich af waarom AD een NDR zou willen, aangezien dit prijzig is en gezien de (cloud only) situatie van AD niet nodig lijkt.

Opdracht: Threat hunting wordt wel eens verward met indicator sweeping. De termen moeten worden onderzocht en goed worden toegelicht wat de AD precies wil.

Eis 1.1: Partij adviseert om niet de aansluiting met IBD-CERT te eisen, maar een samenwerking met IBD-CERT, met concrete en actuele voorbeelden daarvan.

Eis 1.1: Partij informeert of er een vergelijkbaar alternatief mogelijk is voor de verbondenheid aan de IBD-CERT. AD geeft aan dat dit IBD-CERT dient te zijn en dit geldt als een knock-out criterium. Het staat alle partijen vrij om zich als leverancier hier bij aan te sluiten.

Eis 1.1: Partij vraagt waarom de verbondenheid met IBD-CERT wordt geëist, en niet met NCSC. Katwijk geeft aan dat de gemeente zich bij de IBD dient te registreren, het IBD-CERT is een sectorale CERT voor het NCSC.

Eis 1.2: Partij adviseert om niet de status van Microsoft Security Partner te eisen, maar concrete en actuele voorbeelden van de samenwerking als Microsoft Security Partner.

Eis 1.2: Partij vraagt of de status van Microsoft Security Partner een harde eis is, of dat het opleidingsniveau van de individuele medewerkers wellicht leidend zou moeten zijn.

Eis 1.3: Partij adviseert één gemeentelijke referent te vragen en één referent die gebaseerd is op Microsoft Sentinel.

Eis 1.3: Partij vraagt of referenties anders dan Nederlandse gemeente zijn toegestaan. AD geeft aan dit in ogenschouw te nemen, maar ten minste een Nederlandse lokale overheid 2x als referentie te willen zien.

Eis 1.4: Partij geeft aan dat het derde punt onduidelijk is, wie moet daar aan voldoen. De formulering veroorzaakt verwarring. AD geeft aan deze formulering nader te beschouwen.

Eis 1.4: Partij is van mening dat de eis om op verzoek een SOC type 2 rapport op te stellen, te zwaar is. AD neemt dit in overweging.

Eis 2.1: Partij vraagt of het hebben van een standby volstaat in plaats van 'eyes on the screen'. AD geeft aan dat dit niet volstaat.

Eis 2.2: Partij geeft aan dat er een combinatie wordt gehanteerd en vanuit dat opzicht de eis anders geformuleerd kan worden. AD geeft aan dit nader te onderzoeken.

Eis 2.2: Partij wijst op de (geo-) politieke verschuivingen en wijst daarbij op de eis om Sentinel als MDR oplossing te gebruiken. Partij ziet deze eis als beperkend, zowel voor de AD als voor de markt. AD geeft aan dat de gekozen oplossing past binnen de visie van AD en qua integratie past bij de overige producten die worden afgenomen vanuit de Microsoft 365 E5 licentie.

Eis 2.3 werd door een Partij ter discussie gesteld, dit werkt beperkend in de markt. Partij heeft klanten uiteindelijk zien terugschalen naar de eis om alleen Nederlands te communiceren binnen kantooruren.

Eis 2.4 en 9.1: Partij is benieuwd hoe deze eisen t.a.v. andere landen in de EER gelden, en welke screening er dan nodig is. AD geeft aan zich hierop te gaan beraden.

Eis 2.5: Partij vraagt hoe AD aankijkt tegen SOAR, het automatisch handelen n.a.v. events. AD heeft hierin zeker interesse, op basis van goede afspraken.

Eis 2.7: Partij adviseert de eis te formuleren op het gewenste resultaat en niet op de techniek.

Eis 2.7: Partij geeft aan dat Copilot for security nog niet op kan boksen tegen menselijke intelligentie, en bovendien een aanzienlijke kostenpost is. AD geeft aan dit na de vragenronde al te hebben afgezwakt tot een wens.

Eis 4.1: Partij adviseert op te passen met eisen rondom MITRE ATT&CK, 100% dekking is niet mogelijk.

Eis 5.11: Partij is gewoon deze afspraken in een DAP op te nemen. AD geeft aan dat het gaat om vastlegging van de afspraken.

Eis 5.18: Partij wijst erop dat de AD goed moet beseffen wat deze eis inhoudt.

Eis 5.2: Partij doet een suggestie voor marktconforme oplostijden.

Eis 5.20: Partij geeft aan hier mogelijk een extra server voor nodig te hebben, voor wie zijn dan de kosten en het beheer. AD geeft aan dat kosten en beheer in dat geval voor AD zijn.

Eis 5.4: Partij adviseert op te passen met de term 'direct beschikbaar' om geen claim van exclusiviteit te pretenderen.

Eis 5.4: Partij vraagt of AD hier meer neigt naar invulling door een Service Delivery Manager danwel een Security analist. AD geeft aan gevoelsmatig meer naar een SDM te neigen, maar overweegt dit en beraadt zich op de formulering

Eis 5.6: Partij adviseert deze eis als partnership te formuleren.

Eis 5.7: Partij adviseert goed naar deze formulering te kijken.

Eis 7.2: Partij geeft aan dat de verbondenheid aan de grote USA bedrijven groot is, en het gebruik van producten van bedrijven uit de USA derhalve niet te vermijden is. Deze bedrijven hebben wel datacenters in Europa.