



Nota van Inlichtingen 'Marktraadpleging SIEM/SOC oplossing ACM'

Datum: 2 maart 2023

In deze nota van inlichtingen geeft opdrachtgever antwoord op de in het kader van de hierboven marktraadpleging gestelde vragen en geplaatste opmerkingen. Deze nota van inlichtingen maakt onderdeel uit van de marktraadpleging 'SIEM/SOC oplossing ACM'.

Vraag	Vraag	Antwoord
1.	Jullie vermelden dat jullie momenteel al gebruik maken van een SIEM oplossing, kunnen jullie ook meedelen welke SIEM dit vandaag is en waarom deze niet voldoet aan de verwachting?	Deze informatie wordt op een later moment in de aanbestedingsprocedure gedeeld. In algemene zin geldt dat de bekende beperkingen van het werken met sec correlatieregels maken dat de ACM de markt wil verkennen richting nieuwe en andere technologieën, zoals SOAR.
2.	ACM heeft een bestaande SIEM-oplossing waarover zij niet tevreden is. Welke zaken zou zij vooral verbeterd willen zien?	Zie antwoord op vraag 1.
3.	Waarom richt ACM zich alleen op SIEM en niet zoals door Gartner geadviseerd in haar SOC Visibility Triad op SIEM/UEBA, Network Detection en End-point detectie?	Qua tooling richt de aanbesteding zich op SIEM. Qua SOC-dienstverlening verwacht de ACM dat een marktpartij bij de beantwoording van de vragen haar SOC-dienstverlening presenteert. Daarin staat de keuze vrij om dat in lijn met het concept van de Gartner SOC Visibility Triad te doen.
4.	Jullie vermeldde in de marktraadpleging de wens om "geautomatiseerd in te grijpen" P1 – Moderne SIEM Oplossing. Bedoelen jullie dat deze functionaliteit per definitie aanwezig moet zijn in de SIEM, of mag dit als oplossing voorgesteld worden in combinatie met een SOAR? Beiden zijn aparte technologieën die los van elkaar bestaan. Er bestaan echter ook SIEM technologieën zoals bijvoorbeeld Microsoft Sentinel waar een beperkte SOAR-functionaliteit is ingebouwd. Graag verduidelijking over de verwachting of wens hieromtrent.	De ACM is geïnteresseerd in informatie over beide opties (aparte technologie en geavanceerde SIEM).
5.	Gezien onze core-business (SOC en CSIRT-services), wordt er vanuit de SOC en CSIRT standaard in het Engels gecommuniceerd met onze klanten. Is dit acceptabel voor de aanbesteder of verwachten jullie een	De voorkeur is om communicatie met de ACM in het Nederlands te laten plaatsvinden. Daarbij is het in ieder

Vraag	Vraag	Antwoord
	dienstverlening volledig en uitsluitend in het Nederlands.	geval van belang om ten minste een Nederlands aanspreekpunt bij Opdrachtnemer te hebben.
6.	Staat de aanbesteder open voor een SIEM en SOAR as-a-service of wensen jullie beide technologieën volledig aan te kopen en in eigen beheer te nemen? Een SOAR kan als een service afgenomen bijvoorbeeld, en de SIEM in eigen beheer, of beiden as-a-service. Een eigen SOAR zal veel duurder uitkomen voor de aanbesteder dan bijvoorbeeld as-a-service. Hetzelfde geldt (ook, maar niet altijd) voor SIEM. Graag verduidelijking hieromtrent.	De ACM wil een beeld vormen over de verschillende SIEM-oplossingen die in de markt verkrijgbaar zijn. De ACM is geïnteresseerd in informatie over beide opties (as-a-service of eigen beheer), zodat zij naast het formuleren van technische requirements ook keuzes kan maken over sourcing.
7.	Er staat bij de Outsourcing van SOC Services ACM voor First-Line & Second-Line dat de verwachting enkel 8x5 is, maar een SOC (voor ons alvast) is enkel en alleen een 24/7 contract, aangezien de alerts 24/7 zullen binnen komen, en deze bijgevolg ook standaard onmiddellijk worden opgenomen door onze SOC wanneer deze binnenkomen.	Duidelijk.
8.	Wat verstaat ACM onder de termen kaders en principes die zij in vraag 1 hanteert?	Hier doelt de ACM op de minimale en/of maximale eisen die de ACM volgens u kan/moet opnemen in de toekomstige aanbestedingsdocumenten.
9.	In vraag 5 vraagt ACM naar kosten van implementatie en benodigde licenties. Waarom wil ACM dat in deze fase al weten? Het is namelijk erg lastig een indicatie te geven zonder een beeld te hebben bijvoorbeeld infrastructuur, hoeveelheid LOGs, end-points., etc.	De vraag naar inzicht in de kosten heeft te maken met een meerjarenraming voor informatiebeveiliging. Een indicatie die gebaseerd is op een schatting met kosten voor een gemiddelde klant, qua omvang bij voorkeur 600-800 medewerkers, en omschrijving waaruit de kosten bestaan, is in deze fase voor de ACM voldoende.
10.	In de beschrijving wordt aangegeven dat geïnteresseerden zich tot uiterlijk 14 maart 2023 per e-mail kunnen aanmelden. Bedoelt u hiermee dat tot die datum de ACM inschrijvingen op de marktraadpleging kunnen worden ingediend?	14 maart 2023 is de uiterlijke datum waarop partijen (geïnteresseerden) zich kunnen aanmelden én antwoord kunnen geven op de gestelde vragen. Uw reactie kunt u aan ons toesturen via iuc.accountacm@rvo.nl t.a.v. J. de Kleer.