



Resultaat Marktraadpleging SIEM/SOC oplossing ACM

Op 13 februari 2023 is de markt uitgenodigd om informatie en inzichten aan te leveren aangaande een SIEM/SOC oplossing voor de Autoriteit Consument en Markt (ACM). 28 partijen hebben deelgenomen aan de marktconsultatie met als resultaat onderstaand (gecomprimeerde) beeld.

1 Kaders en principes

Mensen, processen en technologie zijn drie hoofdcomponenten die moeten samenwerken om een succesvol cyber dreigingen te detecteren, hierop te reageren en de ACM veilig te houden. Daarbinnen is een SIEM-oplossing als bouwsteen een krachtige tool, maar meerdere partijen geven aan dat dit op zichzelf geen brede security dekking biedt en de nodige complexiteit met zich meebrengt. Een MDR-oplossing waarbinnen SIEM, EDR en NDR zijn samengevoegd volgens de *SOC Visibility Triad visie van Gartner* en het *Mitre&Att&ck Framework* worden vaak benoemd.

Daarnaast dient de ACM de volgende kaders en principes te stellen voor een eventuele aanbesteding:

1. **Scope en doelstellingen:** Geef een duidelijke beschrijving van de scope (24x7) en de doelstellingen. Dit omvat de functies en kenmerken die een monitoringoplossing moet hebben en de diensten die door het SOC moeten worden geleverd, maar bovenal ook een duidelijk beleidskader van de ACM met een visie en daarbij behorende strategie. Focus op de 'waarom-vraag' en laat de invulling voor het 'hoe' aan de markt over.
2. **Inzicht en overzicht:** om een aanbieding te kunnen doen, is behoefte aan de volgende informatie:
 - a. Een gedetailleerd overzicht van de (netwerk)beveiligingsinfrastructuur;
 - b. Aantal assets en overige componenten die gemonitord dienen te worden;
 - c. Een overzicht van de bestaande beveiligingscomponenten en security tooling;
 - d. Indicaties van Events Per Second (EPS) of Gigabytes/dag die in de huidige omgeving gemonitord worden;
 - e. Inzicht in huidige use cases en tevens welke type van belang zijn voor de ACM;
3. **Andere relevante diensten:** Overweeg andere relevante diensten als Threat Hunting, Incident Response en Vulnerability Management;
4. **Dialoog:** Zorg voor een aanbesteding met voldoende ruimte voor dialoog en meerdere rondes Nota van Inlichtingen.

2 Techniek

Deelnemers dragen verschillende SIEM-oplossingen aan, waaronder:
Rapid7, Elastic, Splunk, Microsoft Sentinel, Logpoint, OpenTEXT/ArcSight, TrendMicro, Cyrebro, Darktrace.

Alle oplossingen zijn flexibel op- en af te schalen.

3 Implementatie

Voor implementatie van monitoringoplossingen zijn meerdere scenario's mogelijk:

1. Consultancy voor de implementatie van een SIEM-oplossing door leverancier. SIEM/SOC in eigen beheer.
2. Consultancy voor de implementatie van een SIEM-oplossing en het beheer van het SIEM door leverancier. SOC in eigen beheer.
3. Zowel de implementatie van de SIEM-oplossing als het beheer van het SIEM en de SOC-dienst door de leverancier.

Voor elk scenario geldt een ander implementatieplan en met bijbehorende kosten. Gemiddeld genomen duurt de implementatie 12 weken. Kosten zijn te verdelen in: implementatiekosten en vaste maandelijkse kosten (data ingest, aantal endpoints), gewenste service levels.

4 Kritische succesfactoren

Belangrijkste succesfactor voor het outsourcen van een SOC is de onderlinge samenwerking. Communicatie, verantwoordelijkheden vastleggen en elkaar leren kennen. Ook is het belangrijk om elkaar als partners te zien en de SOC-dienstverlener de ruimte geven om invloed uit te oefenen op welke use-cases worden overgenomen en welke niet.

5 Verdiepende gesprekken

Naar aanleiding van de reacties op de marktconsultatie heeft de ACM vier partijen uitgenodigd om vervolgvragen te stellen over de specifieke deelname of over het algemene beeld dat de ACM had verkegen. Doel van de gesprekken was specifieke onderdelen uit de reacties te verhelderen, zodat de ACM bij de aanbesteding de juiste terminologie hanteert en beter kan specificeren wat haar behoeften zijn.

In deze verdiepende gesprekken is ingegaan op de volgende onderwerpen:

- Visie op Managed Detection & Response en SIEM
- Bouwblokken voor detectie en response: EDR, vulnerability management, incident response
- Aanbesteding: als tooling veelal hetzelfde kan, wat zijn de onderscheidende kwaliteiten die de markt typeren?

Hier is samengevat het volgende uitgekomen:

SIEM-implementaties zijn complex en veelal kostbaar, omdat de prijs vaak wordt berekend op basis van data-ingest. Een oplossing berekent de prijs op aantal endpoints. Daarnaast bieden NDR en EDR het voordeel dat deze makkelijk te implementeren zijn en een groot deel van het aanvalsoppervlak dekken. Marktpartijen maken daarnaast keuzes voor de te gebruiken detectie-oplossingen binnen hun eigen stack op basis van de kwaliteit van de producten en tevens de kennisopbouw van de SOC-analisten. Dat maakt dat marktpartijen niet zomaar vendor agnostisch zijn, waar de ACM rekening mee dient te houden bij haar uitvraag. Incident response en vulnerability management zijn aparte bouwblokken die de ACM apart moet beschrijven in haar aanbesteding mocht een toekomstige leverancier ook deze dienstverlening dient te leveren. Tot slot werden samenwerking en partnerschap besproken als onderscheidende kwaliteit binnen een aanbesteding.

Op basis van deze informatie en het algemene beeld uit de marktraadpleging, zal de ACM nu een Europese aanbesteding voorbereiden. Verwachting is dat deze in juni 2023 wordt gepubliceerd.