



Marktraadpleging SIEM/SOC oplossing ACM

1 Naam van de behoeftesteller

Autoriteit Consument & Markt (ACM), onderdeel van het ministerie van Economische Zaken en Klimaat.

De Autoriteit Consument en Markt maakt zich als toezichthouder sterk om markten beter te laten werken, voor mensen en bedrijven. Nu en in de toekomst. Met dat doel houdt de ACM toezicht op de mededinging, een aantal specifieke sectoren en het consumentenrecht.

2 Achtergrond

Door de positie van de ACM in de samenleving is zij een interessant target voor cybercrime en spionage. De ACM wil data voldoende beschermen tegen verschillende dreigingen. Dreigingen, die met het werken met meer data ook steeds complexer worden.

Continue monitoring van applicaties en netwerken zorgt voor structurele bewaking van kritische beheerprocessen en data. Om de digitale weerbaarheid van de organisatie te versterken, wenst de ACM een nieuw Security Information & Event Management (SIEM) en Security Operations Center (SOC) oplossing te realiseren om detectie van digitale bedreigingen en afwijkend gedrag en response toekomstbestendig te moderniseren.

Moderne SIEM-oplossing

Snelle detectie van dreigingen en afwijkend gedrag en response is noodzakelijk om de effectieve duur van cyberdreigingen bij de ACM te voorkomen of beperken. Daarmee is SIEM een belangrijke maatregel ten behoeve van het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid. De ACM is over de huidige SIEM-oplossing onvoldoende tevreden wat betreft het gebruik van specifieke use cases en is tevens benieuwd welke nieuwe technologieën (zoals SOAR) de markt ontwikkeld heeft.

Hoogover zijn de wensen van de ACM aan de nieuw te realiseren SIEM-oplossing hieronder te vinden. De te verwerven SIEM-oplossing:

- biedt mogelijkheden voor eigen analysewerkzaamheden;
- biedt mogelijkheid om specifieke use-cases te ontwikkelen;
- maakt gebruik van threat intelligence feeds;
- kan geautomatiseerd ingrijpen;
- is aan te sluiten op zowel on-premise infrastructuur sources als cloud infrastructuur, zodat de oplossing werkt binnen een hybride infrastructuur;
- is makkelijk schaalbaar en kan goed meebewegen in de ACM transitie richting de cloud;
- heeft een intuïtieve interface met gebruiksvriendelijke statistieken voor rapportage, audit en verder onderzoek.

SOC-dienstverlening uitbesteden

De ACM overweegt om de SOC diensten te beleggen bij een externe partij, omdat de ACM specialistische kennis uit de markt goed wil benutten. Te denken valt aan:

- Security monitoring op de baseline en aanvullende specifieke use cases middels de SIEM-oplossing.
- Eerste een tweedelijns afhandeling van security incidenten en beoordeling van alerts (8 uur x 5 dagen per week).
- Doorontwikkeling van use cases en overige SOC-technieken/aspecten op eigen initiatief en in opdracht van en in samenwerking met ACM.
- Threat intelligence van externe bronnen monitoren.

3 Doel marktraadpleging

De ACM wil een beeld vormen over de verschillende SIEM-oplossingen die in de markt verkrijgbaar zijn. Daarnaast wil de ACM SOC-diensten mogelijk beleggen bij een externe partij en is zij daarom benieuwd welke partijen dat kunnen uitvoeren, welke rol zij zouden kunnen hebben bij de nieuwe SIEM-oplossing en wat er komt kijken bij het uitbesteden van een SOC.

4 Vraagstelling

De ACM oriënteert zich dus op de aanschaf van een nieuwe SIEM-oplossing en mogelijk over het uitbesteden van SOC-diensten. U wordt uitgenodigd om de onderstaande vragen zo volledig mogelijk te beantwoorden. Het is uiteraard ook mogelijk dat u geïnteresseerd bent in één van deze twee onderdelen (de SIEM-oplossing óf de SOC-diensten). Dan nodigen wij u uit de vragen of delen van de vragen op dat onderdeel te beantwoorden.

1. Wat zijn volgens u de kaders en principes die de ACM moet opnemen in de aanbestedingsdocumenten ten behoeve van uw informatievoorziening om een goede inschrijving te kunnen indienen?
2. Welke techniek (zoals bijvoorbeeld rule-based, machine learning, AI, SOAR) past uw SIEM-oplossing toe bij het detecteren van en reageren op cyberdreigingen?
3. Welke functionaliteiten heeft uw SIEM-oplossing?
 - Waaronder (maar niet limitatief):
 - Netwerkforensische mogelijkheden
 - Functionaliteiten voor gegevensonderzoek en – analyse
 - Geautomatiseerde responsemogelijkheden en diens kwaliteit
 - Native ondersteuning voor logboekbronnen
4. Hoe implementeert u de SIEM-oplossing en/of de SOC dienstverlening en wat is de bijbehorende doorlooptijd hiervan?
5. Wat zijn de tijdsduur en kosten van implementatie en de licentiemodellen/kosten (in de vorm van bijvoorbeeld een staffel) behorende bij uw SIEM-oplossing en uw SOC-dienstverlening?
6. Hoe flexibel is uw oplossing qua geleverde functie als op- en afschaling, waaronder de mogelijke transitie van on-premise naar de cloud?
7. Op welke manier integreert de SOC dienstverlener de nieuwe ACM SIEM-oplossing? Hoe gaat het in zijn werk wanneer de ACM besluit om de hele SIEM/SOC functie aan u uit te besteden?

8. Welke Service Level Agreement (SLA)-opties zijn volgens u mogelijk om overeen te komen in een toekomstige overeenkomst voor uw SIEM-oplossing en SOC-dienstverlening, en tegen welke kosten?
9. Wat zijn volgens u de kritische succesfactoren voor het outsourcen van een SOC?
10. Heeft u nog overige aanbevelingen die in uw antwoorden niet zijn genoemd?

5 Procedure

Geïnteresseerden kunnen zich tot uiterlijk **14 maart 2023** per e-mail aanmelden via iuc.accountacm@rvo.nl t.a.v. J. de Kleer. Eventuele vragen en opmerkingen over deze marktraadpleging kunnen ook via dit mailadres gesteld worden.

Voeg bij uw antwoord per e-mail graag uw bedrijfsgegevens en de antwoorden op de gestelde vragen toe.

De ACM is geïnteresseerd in uw antwoorden. Heeft u daarnaast nog andere nuttige opmerkingen die de ACM kan gebruiken in de eventuele opdracht, dan ziet de ACM deze graag tegemoet.

6 Resultaten van de marktraadpleging

Als resultaat van de marktraadpleging kan de ACM besluiten om een vervolgtraject te starten. De ACM kan de informatie die verzameld is naar aanleiding van deze marktraadpleging gebruiken bij het formuleren van een aanbesteding. Gegadigden dienen er rekening mee te houden dat informatie die zij in het kader van deze marktraadpleging verstrekken, openbaar (zij het in geanonimiseerde vorm) kan worden gemaakt. Er zal na afloop van deze marktraadpleging dan ook een samenvattend verslag worden gedeeld waarin de resultaten (met uitzondering van concurrentiegevoelige informatie) worden uiteengezet.

De ACM wil de door geïnteresseerden verstrekte informatie zonder voorbehouden kunnen gebruiken. Om deze reden zal de ACM eventuele claims/voorbehouden van geïnteresseerden over het gebruik van informatie of vertrouwelijkheid, niet honoreren. Door het deelnemen aan deze marktraadpleging stemt u hiermee in.

De marktraadpleging is voor alle partijen (de ACM en de geïnteresseerden) vrijblijvend en houdt op geen enkele wijze een verplichting in om met deelnemers in een bepaalde rechtsverhouding te treden. Er kunnen geen rechten worden ontleend aan deelname aan de marktraadpleging of tijdens de marktraadpleging verstrekte informatie.

7 Toelichtingsgesprek/presentatie

De ACM zou naar aanleiding van deze marktraadpleging, indien nodig, graag maximaal vijf geïnteresseerde partijen, op niet-willekeurige wijze, uitnodigen voor een toelichtingsgesprek en/of presentatie. Mocht de ACM dit nodig achten en u daarvoor willen uitnodigen, dan ontvangt u daarover zo spoedig mogelijk (na 14 maart 2023) een uitnodiging van.

Ik zie graag uw reactie uiterlijk **14 maart 2023** tegemoet.

Met vriendelijke groet,

Jordy de Kleer
Inkoper IUC EZK