

Vragen t.b.v. marktconsultatie

Datum: 18-3-2024

Versie: 0.1



Centraal Orgaan opvang asielzoekers

Vraagnr.	Onderwerp	Document	Paragraaf, Artikelnaam of figuur/tabel	Vraag	Antwoord
1	Encryptie			Moet alleen zichtbaar gemaakt worden of een encryptie is gebruikt of moet data ook decrypted worden voor inspectie?	Zichtbaar maken is een must. Als de tool kan ontsleutelen is dit prima, maar niet noodzakelijk.
2	Kenmerken van endpoints?			Hoeveel detail wil je van de endpoint hebben	Minimaal Hostnaam, IP-adres, OS, platform (cloud,/on-prem)
3	Beleidsregels			Welke beleidsregels wil je valideren en bekijken. Netwerk en applicatieregels, authenticatie?	Compliancyregels vanuit diverse bronnen (NORA, IB, privacy)
4	PEP functies			Wat wordt er bedoeld? Wordt met PEP, Policy Enforcement Point bedoeld?	Policy Enforcement Point inderdaad.
5	Integraties van Systemen			Integratie in welke systemen worden er bedoeld?	Integratie met monitoringtools, IAM en SIEM
6	Segmenteren/Microsegmenteren			Segmentatie kan zichtbaar worden gemaakt, moet de oplossing ook impact van segmentatie doortesten?	Ja, we zien het als pluspunt als de impact van een door te voeren change (segmentatie) inzichtelijk is. Inzicht is Must have, impactbepaling is Should have.
7	Vendor agnostisch ?			Het COA geeft aan dat de "tool" vendor agnostisch dient te zijn, kan men delen waarom dit zo belangrijk is voor het COA	Om een vendor lockin te voorkomen. M.n. omdat we bij een toekomstige licecycle vervanging niet weten welke leverancier/merk geplaatst zal worden.
8	CRM			Welke CRM systeem wordt er gebruikt?	Onduidelijk waarom dit in deze context relevant is. Graag toelichting.
9	Segmentatie en policy enforcement			Kunt u hier verder uitleg bij geven wat hiermee word bedoeld?	Dit staat uitgelegd in de marktconsultatie.
10	Policy enforcement			Welke policies worden hier bedoeld?	Dit staat uitgelegd in de marktconsultatie.
11	Marktconsultatie			Wie zijn er vanuit COA betrokken bij de marktconsultatie?	Het projectteam
12	Compliance			Moet de oplossing ook compliant zijn aan de NIS2 regulerings normen?	COA conformeert zich aan de NIS2 richtlijnen.
13		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 1.4	Normaalgesproken wordt installatie van de oplossing uitgevoerd door Professional Services Engineers vanuit ons als fabrikant. Dit wordt zo uitgevoerd om een vlotte en succesvolle installatie en configuratie volgens best practises te garanderen. Installatie verloopt altijd in samenwerking en in overeenstemming met u als klant. Vervolgens wordt de oplossing opgeleverd aan de ICT beheerorganisatie. Is deze werkwijze akkoord voor COA?	Ja, zolang installatie onder supervisie van COA gebeurt en documentatie moet een herinstallatie van het systeem kunnen ondersteunen.
14		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 2.20 & 2.35	Lijken hetzelfde te zijn. Is dit een Must have of Should have?	Volledig inzicht in verkeersstromen is een musthave. De voorbeelden zijn voorbeelden. Welk inzicht kunnen jullie geven? Wat is jullie toegevoegde waarde in het creeren van het inzicht dat COA nodig heeft?
15		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 2.20, 2.36 & 2.37	Lijken gericht te zijn op het verkrijgen van EDR/NDR functionaliteit. Deze kunnen inderdaad een behoorlijke performance impact met zich meebrengen. Is dit project gericht op het verkrijgen van (micro) segmentatie functionaliteit of ook op het verkrijgen/vervangen van EDR functionaliteit?	Scope is inzicht creeren en doorvoeren van (micro) segmentatie. EDR functionaliteit is niet onderdeel van dit project.
16		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 2.44 & 2.45	Lijken hetzelfde te zijn. Is dit een Must have of Should have?	Verschil zit hem in het woord Leader en Challenger.
17		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 4.1	Deze cel is blanco, is hiervoor additionele informatie beschikbaar?	Cel is blanco omdat er op dit moment geen eisen zijn op het gebied van recordmanagement.
18		COA_Verkeersstroomtooling requirements_v0.2	Requirement: 11.1	Hier wordt verwezen naar SLAs in punten 10 en 11. De overige cellen mbt SLA zijn blanco. Is hiervoor additionele informatie beschikbaar?	Er lopen nog interne discussies over de invulling hiervan. Wat zou jullie aanbeveling zijn op dit gebied?
19				Is het COA geïnteresseerd om geavanceerde aanvallen te detecteren die niet worden gedetecteerd door klassieke tools die op basis van signatures werken.	Als dit kan binnen de enkele tool/applicatie waar COA naar op zoek is en het voldoet aan de overige gestelde requirements dan is COA hier zeker in geïnteresseerd.
20				Is het COA geïnteresseerd in het gebruik van ML/AI detecties op het gebied van netwerk/server/appliacatie performance data, om sneller afwijkingen in het normale gedrag te herkennen? Het doel is om sneller issues in te detecteren en daarna eenvoudiger met de inzichten vanuit de analyse het issue op te lossen.	Als dit kan binnen de enkele tool/applicatie waar COA naar op zoek is en het voldoet aan de overige gestelde requirements dan is COA hier zeker in geïnteresseerd.
21				Beschikt COA op dit moment over licenties voor tools die inzicht en informatie verschaffen over verkeersstromen en segmentatie? Zo ja, welke van deze tools worden er op dit moment door COA (of door een externe beheerpartij) daadwerkelijk gebruikt?	Panorama (firewall management), Cisco ACI, SolarWinds, Wireshark .
22				Wil het COA naast het kunnen herkennen of data encrypted of niet encrypted is, de mogelijkheid hebben om te kunnen decrypten? Hackers verstoppen zich vaak in het encrypted verkeer van hun slachtoffers om onopgemerkt te blijven. Door data te decrypten, zoals TLS maar ook Microsoft protocols, kunnen hackers in een vroegtijdig stadium ontdekt worden. Daarnaast kan dit inzichten geven in problemen met applicaties die anders lastig te troubleshooten zijn.	Dit is niet noodzakelijk.
23				Wil het COA dat de oplossing één geconsolideerd dashboard heeft waar de gehele multi/hybrid cloud attack surface zichtbaar is in één oogopslag?	COA wil één tool voor het inzichtelijk maken van verkeersstromen voor zowel end-points, het on-prem DC en de cloud.
24				Is het de bedoeling dat onafhankelijk van de functionaliteiten die gebruikt worden er geen performance degradatie ontstaat in het product?	Geen merkbare performance degradatie voor de COA eind-gebruikers.
25				Is het de bedoeling dat de oplossing een zo breed mogelijke protocol ondersteuning heeft, waaronder DB, Kerberos LDAP, MS-RPC, NFS, CIFS, SMTP, SNMP, Syslog, VOIP, RADIUS, DNS, HTTP, ICMP etc.	Wat verstaan jullie onder ondersteuning? Het is minimaal de bedoeling dat de applicatie/poort wordt herkent en en wordt gemapt op het protocol om de betreffende verkeersstroom kenbaar te maken en op in te grijpen.
26				Is het de bedoeling dat asset discovery automatisch door het product uitgevoerd moet worden	Dit moet een continue proces zijn, zodra er nieuwe end-points zijn binnen het netwerk moeten deze worden

Vragen t.b.v. marktconsultatie

Datum: 18-3-2024

Versie: 0.1



COACentraal Orgaan opvang asielzoekers

Vraagnr.	Onderwerp	Document	Paragraaf, Artikelnaam of figuur/tabel	Vraag	Antwoord
27				Hoeveel maanden geschiedenis verwacht COA in het product voor forensische analyse als het gaat om metadata en transactie data?	Dit hangt samen met het risicoprofiel van een eventueel incident. Richtlijnen van bewaartermijnen. Laag 6 maanden Midden 1 jaar Hoog 1.5 jaar Informatiebeveiliging incident** 3 jaar
28				Is het de bedoeling dat COA de tooling zelf gaat gebruiken met eigen mensen en middelen of de tooling als managed dienst gaat afnemen bij de leverancier?	De COA beheerders zullen zelf beheer uitvoeren op de applicatie. Waar nodig met ondersteuning van de leverancier.
29				Er zijn meerdere tools met verschillende functionaliteiten en prijsmodellen beschikbaar die COA helpen bij het realiseren van haar doelstellingen voor meer inzicht in verkeersstromen en het toepassen van segmentatie. Heeft COA een (indicatie) van het budget dat beschikbaar wordt gesteld voor het verwerven van de tooling cq. dienst?	Nee
30				In verband met de voorbereiding op het gesprek en de demo verzoeken wij COA om inschrijvers tijdig uit te nodigen voor marktverkenning.	