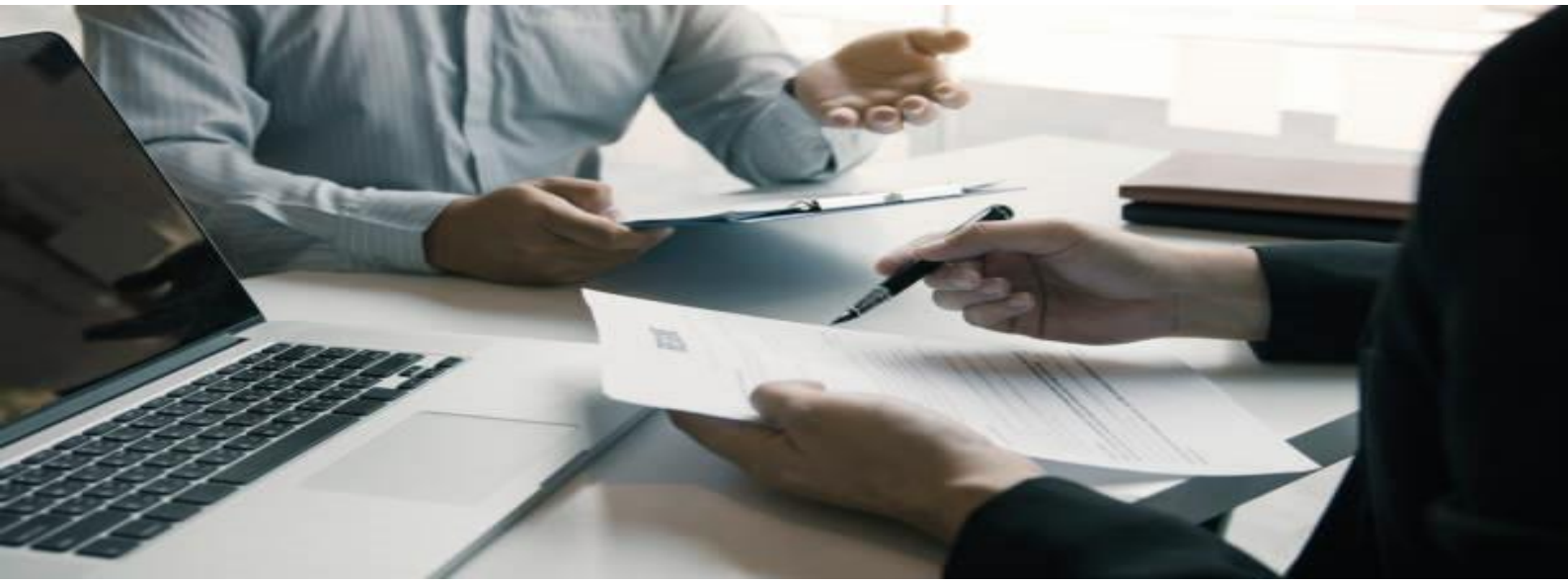
COA Centraal Orgaan opvang asielzoekers

Geanonimiseerd marktconsultatieverslag

“Tooling verkeerstromen en segmentatie”



Datum: 06-05-2024

1. Inleiding

In dit hoofdstuk wordt een toelichting gegeven over de marktconsultatie en waarom deze heeft plaats gevonden. Ook wordt de gevolgde procedure beschreven die is afgelegd voor het uitvoeren van de marktconsultatie. De opdrachtgever van de marktconsultatie is het Centraal Orgaan opvang Asielzoekers (hierna COA).

1.1 Aanleiding

Het COA ziet de marktconsultatie als een belangrijk middel om te bepalen hoe zij de offerteaanvraag idealiter kan inrichten. De uitkomsten op de vragen van de marktconsultatie worden waar relevant en waar mogelijk gebruikt als input voor de definitieve aanbestedingsdocumenten. Het doel van het COA is om met behulp van de marktconsultatie de aanbestedingsstukken zo goed mogelijk te laten aansluiten bij het beschikbare aanbod in de markt.

1.2 Gevolgde procedure

Het COA heeft een marktconsultatiedocument opgesteld dat is geüpload in de TenderNed omgeving. In dat marktconsultatiedocument is het volgende beschreven:

- Inleiding;
- Aanleiding functionele aanvraag;
- Doel en uitgangspunten;
- Use-cases;
- Planning.

Na het vaststellen van het marktconsultatiedocument zijn de volgende stappen doorlopen:
1. Publicatie van de marktconsultatie op Tenderned
De marktconsultatie is op 7 maart 2024 gepubliceerd op www.tenderned.nl onder het Tenderned-kenmerk: TN 455867.

2. Indienen schriftelijk beantwoording door marktpartijen
Marktpartijen zijn verzocht uiterlijk op donderdag 14 maart 2024, 17.00 uur hun vragen te stellen over de requirements.

3. Toelichtende gesprekken met de marktpartijen
Na beantwoording van de vragen door het COA zijn enkele marktpartijen uitgenodigd voor een gesprek. De gesprekken hebben op 27 maart, 28 maart, en 22 april plaatsgevonden.

4. Marktconsultatieverslag
In de week van 29 april 2024 is het marktconsultatieverslag opgesteld en vastgelegd door het aanbestedingsteam van het COA. In het marktconsultatieverslag is zowel de schriftelijke als de mondelinge beantwoording opgenomen. In hoofdstuk 2 van dit document is het geanonimiseerd marktconsultatieverslag uitgewerkt.

2. Resultaten

In dit hoofdstuk worden de gestelde vragen beantwoord door het COA.
De gestelde vragen vanuit de markt en de antwoorden vanuit het COA worden gedeeld met als doel, alle geïnteresseerde marktpartijen te voorzien van de informatie die het COA ontvangen heeft en derhalve een gelijk speelveld te creëren zonder afbreuk te doen aan de commercieel vertrouwelijke aard van de informatie. Om deze reden is het marktconsultatieverslag dan ook geanonimiseerd.

2.1 Gestelde vragen en antwoorden

Vraagnr.	Vraag	Antwoord
1	Moet alleen zichtbaar gemaakt worden of een encryptie is gebruikt of moet data ook decrypted	Zichtbaar maken is een must. Als de tool kan ontsleutelen is dit prima, maar niet noodzakelijk.
2	Hoeveel detail wil je van de endpoint hebben	Minimaal Hostnaam, IP-adres, OS, platform (cloud,/on-prem)
3	Welke beleidsregels wil je valideren en bekijken. Netwerk en applicatieregels, authenticatie?	Compliancyregels vanuit diverse bronnen (NORA, IB, privacy)
4	Wat wordt er bedoeld? Wordt met PEP, Policy Enforcement Point bedoeld?	Policy Enforcement Point inderdaad.
5	Integratie in welke systemen worden er bedoeld?	Integratie met monitoringtools, IAM en SIEM
6	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	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	Welke CRM systeem wordt er gebruikt?	Onduidelijk waarom dit in deze context relevant is. Graag toelichting.
9	Kunt u hier verder uitleg bij geven wat hiermee word bedoeld?	Dit staat uitgelegd in de marktconsultatie.
10	Welke policies worden hier bedoeld?	Dit staat uitgelegd in de marktconsultatie.
11	Wie zijn er vanuit COA betrokken bij de marktconsultatie?	Het projectteam
12	Moet de oplossing ook compliant zijn aan de NIS2 regulerings normen?	COA conformeert zich aan de NIS2 richtlijnen.
13	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	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 creeeren van het inzicht dat COA nodig heeft?

15	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 creeeren en doorvoeren van (micro) segmentatie. EDR functionaliteit is niet onderdeel van dit project.
16	Lijken hetzelfde te zijn. Is dit een Must have of Should have?	Verschil zit hem in het woord Leader en Challenger.
17	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	Hier wordt verwezen naar SLAs in punten 10 en 11. De overige cellen m.b.t. 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/applicatie 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 bedoelding dat onafhankelijk van de functionaliteiten die gebruikt worden er geen performance degradatie ontstaat in het product?	Geen merkbare performance degradatie voor de COA eindgebruikers.
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 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 zonder enige handmatige aanpassingen van de eindgebruiker?	Dit moet een continue proces zijn, zodra er nieuwe end-points zijn binnen het netwerk moeten deze worden herkend.

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 c.q. dienst?	Nee

2.2. Inzichten n.a.v. mondelinge gesprekken met marktpartijen

Naar aanleiding van de gesprekken is gebleken dat de ‘must have’ gestelde requirements niet met behulp van 1 specifieke tool gefaciliteerd kunnen worden. Hiervoor is in bijna alle gevallen aanvullende tooling nodig om de ‘must haves’ volledig af te kunnen dekken. Bijna alle gepresenteerde tools geven inzicht in verkeersstromen, end-points, risico’s en kwetsbaarheden. Sommige tools zijn netwerk centrisch gericht en sommigen agent-based. De netwerk centrische tools halen data binnen door sensoren in het netwerk/locaties te plaatsen, wat een complexere implementatie met zich meebrengt dan de tooling met een agent-based oplossing. Daarnaast bieden een aantal tools een NPR en NDR functionaliteit, wat veel informatie geeft aangaande security monitoring. Het aanbrengen van segmentatie is een belangrijke requirement en zal bepalend zijn bij het uitvragen van een geschikte tool.