



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Verslag Marktconsultatie SIEM/SOC diensten

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage F2 Behorend bij

Europese aanbesteding Uitbesteden Infrastructuurdiensten en SIEM/SOC diensten

ten behoeve van het

**ministerie van Binnenlandse Zaken en
Koninkrijksrelaties**

Datum	08 juli 2019
Kenmerk	201850054.011.018

Inleiding

Graag willen we de deelnemende marktpartijen nogmaals danken voor de gegeven input op onze vragen in deze marktconsultatie. Wij gebruik de input om de aanbesteding nader vorm te geven.

Hieronder leest u per vraag een beknopte weergave de gegeven antwoorden. Neem gerust contact met ons op wanneer u vragen heeft over dit eindverslag van de marktconsultatie. U kunt de betrokken inkoopadviseur bereiken via Tendered of via steven.roos@rijksoverheid.nl

Verslag per vraag

Algemeen

Vraag 1	Wat zijn uw ervaringen met de demarcatie van SOC-dienstverlening en de samenwerking met securitypersoneel van uw klant? Wat is uw advies voor Logius voor deze scheiding van verantwoordelijkheden?
Antwoord	De markt kent gemixte ervaringen met deze demarcatie. Stap 1 is een assessment of de organisatie wel klaar is voor deze dienstverlening. Stap 2 is checkvragen of er zaken adequaat zijn ingeregeld. Verantwoordelijkheid in de dienstverlening is altijd een onderwerp van discussie, van signaleren tot opvolging. Er moeten heldere afspraken gemaakt worden over wat Logius doet en wat de leverancier doet. Advies: vooraf escalatie paden helder maken en hierover afspraken maken. De markt kan niet per definitie adviseren dat Logius minder op de regie moet zitten en meer moet uitbesteden. Dit is afhankelijk van de mogelijkheden van Logius omtrent dit onderwerp. Er kan/gaat veel tijd zitten in regievoeren en er moet vertrouwen zijn in de leverancier als er meer wordt uitbesteed. Het bewaken van SLA's is een continue uitdaging, waarvoor Logius wel volwassen genoeg moet zijn.

Vraag 2	Wat zijn uw ervaringen met de contractvorm waarbinnen ruimte bestaat om n.a.v. voortschrijdende inzichten en marktontwikkelingen de SOC-dienstverlening in samenwerking/partnership met Logius adequaat en optimaal te houden? Wat is uw advies voor Logius daarin?
Antwoord	Om de start, groei en schaalbaarheid van een oplossing te waarborgen, is het van belang dat de partijen op continue basis met elkaar in gesprek zijn over de business, risico's met als uitkomst het Risk Based Scoping proces. Door deze methodiek zal bijvoorbeeld een matrix die Logius in deze heeft opgesteld vanzelf aansluiten op de processen van de dienstverlener. Een praktijkvoorbeeld is waarbij de klant een deel van het werk zelf doet (applicatie use case bijvoorbeeld) en de leverancier de standaard use cases blijft monitoren. Advies: Waar de specifieke kennis binnen Logius aanwezig is, doe het dan vooral zelf. Denk aan 1^e, 2^e en 3^e lijnsdiensten. Leverancier doet monitoring en de 1^e en 2^e lijn, en dan is Logius de 3^e lijn SOC.

Vraag 3	Wat is volgens u de toekomst van IT-tooling voor SOC? Wat is uw visie op de veranderingen in tooling mogelijkheden en SOC werkwijzen binnen een contractperiode? Hoe zou u die veranderingen als SOC dienstverlener willen vormgeven?
Antwoord	SIEM gaat van rule based naar pattern based (machine learning in Splunk), SOC is de trend een shift richting opensource en security orchistratie.

	Er is een duidelijke verandering gaande op de wijze waarop de tooling routine werkzaamheden van SOC-analisten kan overnemen en in verregaande mate kan automatiseren. Artificial intelligence en user behaviour analyse-technieken worden in de toonaangevende producten steeds verder doorgevoerd.
Vraag 4	Wat zijn volgens u de aandachtspunten t.a.v. integratie met monitoring, logging, security sensing e.d. zoals ingericht door derde partijen binnen de Logius-omgeving?
Antwoord	Dit is sterk afhankelijk van welke vorm van regievoering Logius op zich wil nemen. Ticketing systeem/model is een onderwerp dat goed moet worden belegd. Schrijf voor welke ticketing systeem leidend wordt. De ervaring leert dat er vaak gebruik gemaakt kan worden van een basisset van use cases die rule based zijn. Deze basisset wordt aangevuld met risk based use cases. Advies: Zorg voor fasering van de migratie en doe niet teveel tegelijk. Sluit risico-gebaseerd aan en verlies hierbij de cyber killchain niet uit het oog. De meest risicovolle bedrijfsapplicaties zijn niet altijd één op één de eerste componenten die je zou moeten willen bewaken. Vaak is het bewaken van algemenere aanvalsvectoren zoals het email systeem (denk aan phishing en besmette bijlages) en web-proxies (besmette advertenties, besmette downloads en/of images) een veel effectievere eerste stap om te nemen. Sluit risico gebaseerd component na component aan en neem de tijd om de beveiligingsinformatie en het normale gedrag van deze logbronnen goed te leren kennen en de hiervoor relevante use cases en bijbehorende afhandelingsprocedures voor meldingen goed in te regelen. Het volwassen maken van het SOC duurt in de regel daarom ook enkele jaren voordat deze haar maximale effectiviteit bereikt en is daarnaast nooit af.

Vervolgstappen

Logius is momenteel doende met het vaststellen van de meest passende aanbestedingsstrategie. De door u gegeven input draagt daaraan bij. De publicatie van de aanbesteding zal eveneens via TenderNed geschieden en wij streven ernaar deze zo spoedig mogelijk te kunnen publiceren.