Nota van Inlichtingen
Marktconsultatie SOC met SIEM

Gemeente Lansingerland
Corsanummer Z-22-000229
10-5-2022

Nr.	Onderwerp	Vraag	Antwoord
1	Vraag 19	De aan te bieden dienstverlening is gelicenseerd op de totale som van het aantal assets in uw omgeving (workstations, desktop, laptops & servers zowel virtuele als fysieke systemen). Kunt u graag aangeven of de 678 assets die u bij vraag 19 vermeld het juiste aantal vertegenwoordigd of wat is anders de hoeveeelheid assets in de totale omgeving?	De infrastructuur van de gemeente Lansingerland omvat ongeveer: 160 Servers, 30 switches, 60 WiFi Access Points, 2 WiFi Controllers en 2 Firewalls. Dit is het aantal voor de marktconsultatie. Mogelijk aan te passen bij de uiteindelijke aanbesteding.
2		U vraagt expliciet om een advies en de invulling door een derde partij, betekent dit ook dat in de beantwoording en voorstel aanvullende diensten die een aantoonbare bijdrage leveren aan de doelen opgenomen mogen worden of dient inschrijver zich te houden aan de kaders van SOC SIEM?	Indien u er aanvullende diensten zijn die een aantoonbaarbare bijdrage leveren aan oize doelen dan mag u dit in uw antwoord uitwerken. Wij zullen bij het formuleren van de aanbestedingsstukken u suggesties indien wenselijk meenemen. U dient expliciet aan te geven als dit vertrouwelijk informatie betreft en wij dit niet mogen delen in het marktconsultatieverslag.
3		Is uw organisatie bereidt om een meerjarige (licentie en diensten)overeenkomst aan te gaan met de SOC Leverancier?	ja
4		Wat zijn de door u gewenste facturatietermijnen van de SOC SIEM oplossing en de bijbehorende dienstverlening?	We gaan er vanuit dat de Algemene Inkoopvoorwaarden IT gemeente Lansingerland 2019 (zie website) van toepassing zijn op de overeenkomst. In artikel 9. Betaling, facturatie en vergoeding zijn de hieraan verbonden voorwaarden terug te vinden.
5		Wat is de rolverdeling van het Team Informatievoorziening & Automatisering en uit hoeveel medewerkers bestaat het team?	De afdeling I&A heeft ca. 40 medewerkers (incl. Post/Archief, IT-beheer en Informatiebeheer, service desk en applicatiebeheer.)
6		Welk Team binnen uw organisatie gaat verantwoordelijk zijn voor de opvolging van acties na.v. notificaties en alerts (remediation) aangegeven vanuit de SOC Leverancier?	het team IT-Beheer, ondersteunt door andere teams, zoals applicatiebeheer
7		Van welk perceel van de GGI-veilig aanbesteding (1, 2 en/of 3) maakt uw organisatie gebruik?	geen
8		Gebruikt uw organisatie momenteel een Vulnerability Management en/of SIEM oplossing en zo ja, welke?	Nessus voor vulnerability mgt., geen SIEM oplossing, wel FortiAnalyzer voor de Fortinet Firewalls/IDS en overige Fortinet producten.
9		Staat uw organisatie er voor open om bij een succesvolle implementatie en uitvoering van de SOC dienstverlening als (publieke) referentie(case) op te treden van Leverancier?	In principe staan we daar voor open. Dit antwoord dient op geen enkele wijze te worden geinterpreteerd als toezegging.
10	Vraag 12	Wat bedoelt u met "melding van de klant" bij vraag 12? Bedoelt u wellicht een melding vanuit het SOC aan de klantorganisatie?	De vraag is als volgt bedoeld: welke reactie verwacht het SOC (van jullie) van de gemeente (de klant) nadat het SOC een melding heeft gedaan bij de gemeente (de klant)
11		Welke endpoint beveiliging software wordt er momenteel gebruikt?	De gemeente Lansingerland gebruikt momenteel FortiClient als endpoint protection oplossing binnen de infrastructuur en Windows Defender op laptops.
12		Hoe is jullie kijk op geautomatiseerde respons mogelijkheden?	Graag jullie visie daarop in het kader van de marktconsultatie
13		Is support/aanwezigheid in Nederland van toegevoegde waarde voor jullie?	ja, dit zien we vooralsnog als een must (Nederlandstalig)
14		Is het van belang welke locatie de data verwerkt wordt? Zoja, waar ligt de voorkeur?	Ja, in de Europese Economische Ruimte is een must
15		Hoe groot is jullie IT team? Hoeveel FTE houdt zich gericht met IT security bezig?	De afdeling I&A heeft ca. 40 medewerkers. Bij ca. 6 FTE is security een van de onderdelen van de dagelijkse werkzaamheden
16		Is extra dienstverlening in de vorm van incident respons een toevoeging?	Graag jullie visie daarop in het kader van de marktconsultatie
17		Is een koppeling met Azure AD van toegevoegde waarde?	Wij zien een koppeling met Azure AD noodzakelijk voor authenticatie op het portaal van de oplossing. Tevens zien wij een (API) koppeling voor het loggen van events binnen Azure AD. Richting de toekomst verwachten wij meer Azure / Office365 diensten in te zetten waar door een koppeling met deze omgeving zeer belangrijk is.
18		Hoeveel waarde hechten jullie aan referenties van andere gemeentes?	Daar hechten we aan. We gaan ook graag met hen in gesprek.

19		In het document TN358533 - SF01 Vooraankondiging 20220421140600.pdf zijn veel velden ingevuld, maar niet alle. Hierdoor is het niet helder welke paragrafen al correct zijn ingevuld en welke niet. Bijvoorbeeld de paragraaf Gunningscriteria geeft de suggestie dat de aanbiedingen alleen op prijs beoordeeld zullen worden. Kunt u a.u.b. in dit document aangeven welke paragrafen nog definitief gevuld moeten worden?	Deze vooraankondiging betreft een marktconsultatie. Verdere info wordt bij de publicatie van de aanbesteding meegegeven.
20		Wij kunnen ons namelijk niet voorstellen dat dit het enige gunningscriterium zal zijn. Welke andere criteria worden gehanteerd?	We gaan er voorlopig van uit dat het gunningscriteria beste prijs kwaliteitsverhouding zou zijn.
21		Wat voor soort aanbesteding volgt na de marktconsultatie? Wordt dat een openbare, een niet-openbare of een onderhandse aanbesteding?	Dit wordt waarschijnlijk een openbare Europese aanbesteding.
22		Paragraaf 5.1 vraag 1: kunt u verder verduidelijken wat met “zo aantrekkelijk mogelijk” wordt bedoeld?	Voor de markt passend en zo laagdrempelig mogelijk waarin ruimte voor onderscheidend vermogen is.
23		Paragraaf 5.2 vraag 4: Bij SOC/SIEM opdrachten hanteert aanbieder de aanpak dat eerst de basis goed wordt ingericht en dat daarna wordt uitgebreid. Ook bij use cases wordt in eerste instantie ingezet op een basisset en uitgebreid naar een geavanceerde set. Doorlooptijd van implementatie hiervan heeft vaak te maken met capaciteit, volwassenheidsniveau en ambitie van de opdrachtgever. In hoeverre moet rekening worden gehouden met groei in aantal logbronnen (assets) en aantal en complexiteit van use cases?	1) Wij gaan er van uit dat een groot aantal use cases met bekende Indicators of Compromise snel kan worden geimplementeerd. 2) Het aantal logbronnen zal niet spectaculair stijgen, maar wel conform de groei van de IT omgeving, waaronder verschuiving van on-premise naar cloud. 3) We gaan uit van de standaardset van use cases van de leverancier. Mogelijk wordt dit op termijn geleidelijk uitgebreid met organisatiespecifieke use cases.
24		Paragraaf 5.3 vraag 9: de SIEM oplossing van aanbieder kan met heel veel verschillende SM-tooling koppelen. Kunt u specifieker aangeven met welke SM-tooling u graag zou willen koppelen?	Op dit moment wordt Topdesk gebruikt, maar de toekomstige SM-tooling wordt onderzocht. Daarom graag aangeven waar jullie (goed) mee kunnen koppelen
25		Paragraaf 5.3 vraag 12: kunt u deze vraag verduidelijken?	De vraag is als volgt bedoeld: welke reactie verwacht het SOC (van jullie) van de gemeente (de klant) nadat het SOC een melding heeft gedaan bij de gemeente (de klant)
26		Paragraaf 5.3 vraag 15: Wordt hier onboarding van de SOC-dienst bedoeld of de technische onboarding van het SIEM?	Beide
27		Paragraaf 5.4 vraag 19: u vraagt de aanbieders om de kosten per asset te berekenen. Sommige assets (bijvoorbeeld firewalls) produceren significant meer logging dan andere assets. Licenties van SIEM oplossingen zijn op basis van de hoeveelheid logging die voor klanten wordt verwerkt. Waarop baseert u de wens om de kosten per asset uit te vragen?	Gevraagd wordt om de totale kosten voor de hele IT omgeving en de kosten voor extra assets. Wanneer het nodig is om de kosten voor extra assets de differentieren naar type asset, staat het u vrij dat te doen. De behoefte aan de kosten voor extra assets wordt gevraagd met het oog op mogelijke geleidelijke uitbreiding van de infrastructuur.
28		Aanbieders zullen in dat geval per type asset aannames moeten maken over de hoeveelheid logging, die de assets gaan genereren. Gemeente Lansingerland zal hiervoor veel meer informatie moeten aanleveren, zoals het exacte type asset en een schatting van de hoeveelheid logging dat deze asset zal genereren. Omdat het lastig is om dit soort informatie accuraat aan te leveren is de kans heel groot dat dit in de praktijk niet correct is. Om deze reden hebben alle SIEM aanbieders hun licentiemodel gebaseerd op logging-volume in plaats van het aantal assets. Vallen firewalls ook binnen de genoemde assets?	1) Wij gaan er van uit dat u beter in staat bent de hoeveelheid logging voor verschillende assets in te schatten dan wij. Wij verwachten dat u uw inschatting per type asset in de beantwoording van deze marktconsultatie opneemt en welke aannames u daarbij doet. U geeft aan dat meer informatie over de exacte assets nodig is. U kunt aangeven welke informatie dat precies is. Dan kunnen we dat meenemen in de uiteindelijke aanbesteding. 2) Firewalls vallen ook binnen de genoemde assets.
29		Kunt u een inschatting geven van de hoeveelheid logging, die door de genoemde assets (zoals serversystemen en SaaS oplossingen) per dag wordt gegenereerd?	Neen. Wij gaan er van uit dat u beter in staat bent de hoeveelheid logging voor verschillende assets in te schatten dan wij.
30		Vaak is het bij clientsystemen verstandiger om alleen logging van de endpointmanagementsystemen (die bijvoorbeeld clientmeldingen van onderschepte malware ontvangen) te gebruiken. Wat is de reden dat u 500 windows clients op het SIEM platform wenst aan te sluiten?	In het kader van de marktconsultatie horen wij graag de voor- en nadelen die u ziet voor beide mogelijkheden.
31		Paragraaf 5.4 vraag 20: om deze vraag te kunnen beantwoorden is een aantal gegevens nodig. Allereerst de hoeveelheid logging die per dag wordt verwerkt. En ten tweede waar de logging wordt verwerkt en opgeslagen; op een centrale of op meerdere decentrale locaties. Kunt u van de genoemde assets aangeven hoe deze verdeeld zijn over verschillende locaties?	1) Wij gaan er van uit dat u beter in staat bent de hoeveelheid logging voor verschillende assets in te schatten dan wij. 2) Waar de logging wordt verwerkt en opgeslagen hangt af van de door u voorgestelde oplossing/architectuur. De Assets staan in twee gespiegelde rekencentra, plus mobiele assets, zoals laptops, plus SaaS applicaties
32		Heeft Gemeente Lansingerland een eigen ICT afdeling, of is dit uitbesteed aan een externe IT partij?	De gemeente heeft een eigen ICT afdeling.
33		Indien de IT is uitbesteed, hoe ziet deze samenwerking eruit, welke afspraken zijn er gemaakt over het verwerken van meldingen, is er een SLA beschikbaar?	n.v.t.
34		Is er een Incident Response Plan beschikbaar?	Er wordt gewerkt aan een incidentprocedure.
35		Is er binnen Gemeente Lansingerland een 24/7 piketdienst beschikbaar?	ja
36		Welke security processen en oplossingen (security tooling) zijn er op dit moment ingeregeld?	Als oplossing zijn firewalls, vulnerability scanning en end point protection geimplementeerd. Kunt u aangeven aan welke processen/oplossingen u nog meer denkt?

37		Is er een servicedesk beschikbaar?	ja
38		Als een IT incident zich voordoet, hoe gaat de gemeente daarmee om buiten kantoortijden?	Wij verwachten van het SOC dat zij in bepaalde acute gevallen zelf ingrijpt, in andere gevallen de piketdienst telefonisch informeert en in gevallen, die kunnen wachten tot de volgende werkdag per e-mail en/of een ticket in de SM-tooling informeert. In het kader van de implementatie wordt e.e.a. nader afgestemd.
39		Is er een strategisch beleidskader mbt informatie veiligheid?	Binnen de organisatie bestaat een strategisch informatiebeveiligingsbeleid.
40		Werken jullie samen met andere gemeentes met uitzondering van de aansluitende gemeentes Berkel en Rodenrijs, Bergschenhoek en Bleiswijk?	Lansingerland is één gemeente, waarvan de voormalige gemeenten Berkel en Rodenrijs, Bergschenhoek en Bleiswijk deel uit maken. Op ICT gebied wordt niet operationeel samengewerkt met andere gemeenten.
41		Welke belangrijke applicaties zijn essentieel voor de gemeente?	De gemeente Lansingerland heeft een applicatielandschap dat niet veel afwijkt van andere gemeenten. In de basis gebruikt de gemeente Lansingerland een kantoorautomatisering omgeving zoals die aanwezig is bij veel organisaties. We verwachten van u adequate kennis van de gemeentelijke informatieverwerking. We verwachten niet dat de keuze voor een SOC/SIEM partij af hangt van de leverancierskeuze voor specifieke applicaties.
42		Is er een overzicht beschikbaar van het IT landschap van Gemeente Lansingerland? Met o.a. de volgende onderdelen; Wij adviseren dit overzicht mee te nemen in de komende uitvraag. • Onpremise en/of Cloud? • Welke Firewalls? • Hoeveel werkplekken zijn er binnen Gemeente Lansingerland? • Maken jullie gebruik van thuiswerkplekken? • Welke EDR/IDS/Vulnerability oplossingen/scanning zijn er nu al aanwezig? • Van hoeveel data centers maken jullie gebruik? • Hoeveel kantoren en werkplekken zijn er aanwezig? • Aantal internet break-outs? • Maakt de gemeente gebruik van Bring Your Own Device (BYOD)?	- voornamelijk on-premise, aangevuld met SaaS applicaties - Fortinet Firewalls - ca. 500 werkplekken/laptops - Er wordt gebruik gemaakt van thuiswerkplekken op zakelijke apparatuur (laptops) - EDR: Forticlient, IDS: Fortinet firewalle, Vulnerability scanning: Nessus - twee locaties in eigen beheer - twee kantoorlocaties: gemeentehuis en gemeentewerf met 350 kantoorwerkplekken/docking stations/bureau's - Er is één generieke internetaansluiting en één KPN-Gemnet/Diginetwerkaansluiting. - De gemeente maakt geen gebruik van BYOD (ook niet voor smartphones). Medewerkers kunnen wel op eigen device werken (binnen Citrix omgeving).
43		Op welke manier wil de gemeente de rapportages aangeleverd krijgen?	Voor specifieke meldingen, zie punt 38, voor periodieke overzichten: in een dashboard en per email.
44		Is er binnen de gemeente een SIEM aanwezig	neen. Daarom is een SIEM onderdeel van deze marktconsultatie. Er wordt wel gebruik gemaakt van Fortianalyser m.b.t. de firewalls.
45		Wat wordt er bij vraag 15 bedoelt met ‘klanten’ gaat dit om de Gemeente Lansingerland?	ja
46		Graag ontvangen wij extra toelichting over vraag 20.	De gemeente beoogd in te schatten of de huidige bandbreedte adequaat is, waarbij deze af zal hangen van de door u voorgestelde oplossing/architectuur.
47		Is de aanname juist dat Gemeente Lansingerland niet heeft meegedaan met de aanbesteding GGI-Veilig van VNG voor het perceel SIEM/SOC?	ja
48		Is het de wens van Gemeente Lansingerland om 24x7 SOC dienstverlening af te nemen of alleen tijdens kantoortijden.	24x7