GEMEENTE Lansingerland

Marktconsultatie

“SOC met SIEM”

Naam aanbesteding: SOC met SIEM
Corsanummer: Z-22-000229
Datum: 21-4-2022

Inhoud

1. Inleiding

De gemeente Lansingerland nodigt geïnteresseerde partijen graag uit voor haar marktconsultatie omtrent het inzetten van een Security Operation Centre (SOC) en het inrichten van een Security Information & Event Management (SIEM) .

1.1 Algemeen

De gemeente Lansingerland oriënteert zich op de het inrichten en inzetten van een SOC en een daarvoor benodigd SIEM. Als onderdeel van deze oriëntatie organiseert de gemeente een schriftelijke marktconsultatie. In dit protocol schetsen wij de wijze hoe wij deze marktconsultatie vormgeven.

Deze marktconsultatie wordt geïnitieerd vanuit het team Informatievoorziening & Automatisering binnen het domein Bedrijfsvoering. Het cluster Inkoop ondersteunt bij de marktconsultatie.

Wij verzoeken u vriendelijk om u te verdiepen in dit protocol indien u geïnteresseerd bent in of deelneemt aan de marktconsultatie.

Gemeente Lansingerland heeft dit protocol met grote zorg samengesteld. Mocht u vragen hebben, verwacht de gemeente dat u deze stelt.

1.2 Doel marktconsultatie

Om de gelijkheid en transparantie te waarborgen hanteert de gemeente een openbare marktconsultatie. Dit is één van de instrumenten die een rol spelen bij de verdere besluitvorming omtrent aanbestedingsprocedure(s). Met deze marktconsultatie vragen wij feedback/input op onze vragen.

2. De Opdracht

2.1 Opdrachtgever

Gemeente Lansingerland
Lansingerland is een dynamische gemeente in het hart van de Metropoolregio Rotterdam Den Haag en bestaat uit de kernen Berkel en Rodenrijs, Bergschenhoek en Bleiswijk. De gemeente kenmerkt zich door mooie woonwijken en goede voorzieningen zoals winkels, scholen, sportaccommodaties, recreatiemogelijkheden en een rijk verenigingsleven. In Lansingerland wonen meer dan 60.000 mensen; de gemeente groeit in een passend tempo naar een omvang van 75.000 inwoners.

2.2 Opdracht

Aanleiding
Gezien de toenemende complexiteit van dreigingen en aanvallen zijn preventieve beveiligingsmaatregelen steeds vaker niet meer toereikend. Om geavanceerde dreigingen, zowel vanuit binnen als buiten de organisatie, te kunnen adresseren is het essentieel om over de juiste hulpmiddelen en processen te beschikken, waarmee (mogelijke) dreigingen en aanvallen in een zeer vroeg stadium gedetecteerd kunnen worden. Op basis van deze vroegtijdige detectie kan er actie ondernomen worden om de aanval zo snel mogelijk te stoppen of in een aantal gevallen zelfs te voorkomen. Het implementeren en in gebruik nemen van en SOC dat werkt op basis van een SIEM is een vereiste vanuit de BIO.

Doelstelling
Systematisch in de gaten houden wat er gebeurt binnen de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren en hiermee de vervolgschade beperken.

Inhoud opdracht
Het inzetten van Security Operation Centre (SOC) met het inrichten van een Security Information & Event Management (SIEM) om ervoor te zorgen dat aanvallen in een zo vroeg mogelijk stadium worden gedetecteerd, zodat aanvallen kunnen worden gedwarsboomd en de gevolgen van aanvallen worden verminderd of in sommige gevallen worden voorkomen. Daarnaast leeft de behoefte om retrospectief terug te kunnen kijken naar eerdere gebeurtenissen om hiervan te leren, om op basis daarvan beheersmaatregelen aan te scherpen of uit te breiden.

Met SOC krijgen het SOC en de gemeente real-time inzicht in de activiteiten die plaatsvinden binnen de ICT-infrastructuur en zal het SOC afwijkingen rapporteren aan de gemeente. Dit stelt de gemeente in staat om direct en adequaat te reageren op verdachte activiteiten in het netwerk. Een SOC richt zich op het monitoren van dreigingen en de kwalificatie van afwijkende gebeurtenissen. Ervaring vanuit de IBD leert dat het uitbesteden van deze monitoring wenselijk is, omdat het veel tijd en capaciteit van de interne organisatie vergt.

3. Marktconsultatie voor aanbieders

3.1 Aankondiging marktconsultatie

De aankondiging van deze marktconsultatie wordt digitaal uitgevoerd. De aankondiging is gepubliceerd via het online aanbestedingsplatform TenderNed.
Na deze aankondiging verloopt ook de verdere communicatie omtrent de marktconsultatie via TenderNed.

3.2 Planning van de marktconsultatie

Hieronder staat de planning van de marktconsultatie. **Let op: de planning in dit document is leidend en niet de planning in TenderNed.**

Stap	Planning
Publicatie op TenderNed van de schriftelijke vragen van de gemeente	21 april 2022
Uiterlijke ontvangst van vragen	28 april 2022 vóór 10.00 uur
Publicatie nota van Inlichtingen	10 mei 2022
Uiterlijke ontvangst van antwoorden op de schriftelijke vragen van geïnteresseerde partijen.	18 mei 2022, 12.00 uur
Toelichtende gesprekken	30 en 31 mei 2022

De gemeente kan de planning wijzigen.

3.3 Vragen

U kunt vragen stellen over deze marktconsultatie tot de datum zoals vermeld in paragraaf 3.2. Uw vragen kunt u stellen via de vraag & antwoord module van Tenderned.

De geanonimiseerde vragen en antwoorden worden op de in de planning opgenomen datum gepubliceerd op Tenderned in de vorm van een nota van inlichtingen.

3.4 Indienen beantwoording

Deelnemers dienen uiterlijk op de in de planning aangegeven datum en tijdstip de antwoorden op de vragen in het marktconsultatiedocument in de vorm van een Word of PDF document in te dienen via Tenderned.

3.5 Toelichtende gesprekken

Een selectie van de marktpartijen die tijdig gereageerd hebben kan vervolgens in de gelegenheid worden gesteld de ingediende antwoorden mondeling toe te lichten, waarbij de gemeente de mogelijkheid heeft nadere vragen te stellen over de gegeven antwoorden. Deze gesprekken worden één op één gevoerd met de marktpartijen en duren maximaal 50 minuten.

Tijdens deze toelichting wordt tevens de mogelijkheid geboden een presentatie (kort en bondig, maximaal 20 minuten) te geven ter ondersteuning van de ingediende antwoorden. Het geven van een bedrijfspresentatie is uitdrukkelijk niet toegestaan.

3.6 Verslag

De bevindingen van de marktconsultatie worden naar inzicht van de gemeente Lansingerland gebruikt ten behoeve van het opstellen van de aanbestedingsstrategie en de aanbestedingstukken. Vanuit het oogpunt van transparantie worden de algehele bevindingen van de marktconsultatie daarnaast ook vastgelegd in een geabstraheerd en geanonimiseerd marktconsultatieverslag dat te zijner tijd deel uit zal maken van de aanbestedingstukken.

4. Voorwaarden aan de marktconsultatie

4.1 Verslaglegging

De informatie die de gemeente ontvangt gebruiken wij om verder vorm te geven aan de aanbestedingsprocedure. De informatie die wij ontvangen die als (commercieel) vertrouwelijk ten opzichte van concurrentie kan worden aangemerkt zullen wij in geen enkel geval openbaar maken e/o delen met derden.

4.2 Verkenning als voorbereiding op de aanbestedingsprocedure

Deze verkenning is geen uitnodiging tot een inschrijving, maar een consultatieronde. Het is enkel een onderzoek ter voorbereiding op de voorbereiding van de aanbesteding. U bent vrij om de vragen te beantwoorden. U kunt echter geen enkel recht ontlenen aan deze consultatie, waaronder bijvoorbeeld het recht op verkrijging van inzage in (concept)aanbestedingsstukken, informatie, of een eventuele opdracht. Deelname geschiedt op basis van volledige vrijblijvendheid en voor eigen rekening en risico van de deelnemers.

4.3 Auteursrecht

De gemeente Lansingerland heeft het auteursrecht op dit document. Geïnteresseerde mag uitsluitend voor eigen gebruik ten behoeve van deelname aan de marktconsultatie een beperkt aantal kopieën maken. Onder eigen gebruik wordt in dit kader ook gebruik door eventuele onderaannemers verstaan

4.4 Communicatie

Het is geïnteresseerden binnen het kader van deze marktconsultatie niet toegestaan om op andere wijze contact op te nemen met gemeente Lansingerland over deze marktconsultatie dan zoals in dit protocol is omschreven.

4.5 Geen tegemoetkoming kosten deelname marktconsultatie

De gemeente keert geen tegemoetkoming in kosten voor deelname aan deze marktconsultatie uit.

5. Marktconsultatievragen

In onderstaande paragrafen zijn de marktconsultatievragen per onderwerp beschreven. Deelnemer wordt verzocht deze vragen schriftelijk te beantwoorden en uiterlijk op de in de planning aangegeven datum en tijdstip in te dienen.

5.1 Algemeen

Vraag 1
Hoe denkt u dat wij de opdracht zo aantrekkelijk mogelijk in de markt kunnen zetten? Wat kunnen we meenemen in de eisen en wensen en wat zijn absolute go/no go zaken? Dit om onze aanbestedingsstukken zo goed mogelijk af te stemmen met de wensen en mogelijkheden binnen de markt.

Vraag 2
Zijn er zaken die u kwijt wilt met betrekking tot deze aanbesteding die wij mee kunnen nemen?
De SOC dienstverlening is de kern van de uitvraag, waarbij SIEM ondersteunend is aan deze dienstverlening. Hoe zien jullie deze aanpak?

Vraag 3
Indien een toelichtend gesprek gewenst is, wat zijn de contactgegevens van de persoon binnen uw organisatie die we hiervoor kunnen benaderen?

5.2 Use cases

Vraag 4
Op basis waarvan heeft u een dekkende set van use cases?

a) Hoeveel zijn dat er?
b) zijn er beperkingen tav onderliggende technologie (niet beschikbaar voor bepaalde OS, softwareleverancier, cloud service provider, etc.)?
c) In hoeverre dekken jullie frameworks zoals MagMa en/of Mitre Att&ck af?

Vraag 5
Hoe (snel) zorgen jullie op eigen initiatief voor additionele use cases obv nieuwe IOC/nieuwe kwetsbaarheden/malware/…? Bijvoorbeeld: Log4J, Spring4Sh, printnightmare maar ook kleinere issues
Hoe (snel) hebben jullie dat bij Log4J en bij printnightmare gedaan?

Vraag 6
Hoe gaan jullie om met door de klant gedefinieerde use cases? En welke inspanningen vergt het opnemen van een door de klant gedefinieerde nieuwe use case aan jullie kant?

5.3 SIEM

Vraag 7
Hoe verzamelt u loginformatie (agents, standaard interfaces)

a) Voor: windows clients, smartphones, netwerkinfra, servers op Linux (CentOS,Debian,Red Hat,Suse), Windows 2012 – 2019, Oracle Solaris?
b) Welke standard interfaces worden ondersteund voor het aanleveren van loginformatie?
c) Zijn er beperkingen tav onderliggende technologie (niet beschikbaar voor bepaalde OS, softwareleverancier, cloud service provider, etc.
d) Advies/ervaringen tav verzamelen met/zonder agents

Vraag 8
Hoe gaat u om met/ wat zijn uw ervaringen met input uit Vulnerability scanners, zoals Nessus?

Vraag 9
Hoe koppelen jullie met service management tooling van de gemeente (inschieten van incidenten/meldingen), zoals Topdesk?

a) Met welke SM-tooling hebben jullie API's?

Vraag 10
Welke producten gebruikt u, zijn dit mainstream producten en/of zelfbouw?

Vraag 11
Levert u extra sensoren en/of honeypots?

Vraag 12
Welke feedback/reactie verwachten jullie na een melding van de klant?

Vraag 13
Ondersteunt u: dedicated SIEM on-premise (onder beheer van SOC), remote SIEM op SOC-locatie of SIEM in de cloud?

a) Wat zien jullie als voordelen/nadelen
b) welke opties biedt u aan?
c) Zijn licenties en hardware voor het SIEM van de SOC leverancier of van de klant?
d) svp een overzichtstekening van de infrastructuur/architectuur zoals u die voorstaan aanlevert.

Vraag 14
Welke SIEM producten worden ondersteund door het SOC?

Vraag 15
Hoe werkt de onboarding van klanten die van een andere leverancier overstapt naar u?

Vraag 16
Bent u bereid het door u in het kader van de opdracht ingerichte SIEM over te dragen aan een andere SOC-leverancier in het kader van een exit-strategie?

Vraag 17
Op welke wijze kunnen klanten toegang (leesrechten) krijgen op Siem/SOC dienst?

a) Welke toegang is er, bijv. dashboards?
b) Hoe is authenticatie geregeld, denk hierbij aan SAML / AAD integratie, etc.

Vraag 18
Is er een dashboard beschikbaar dat toegankelijk is voor de klant?
Welke informatie is er op het dashboard beschikbaar?

5.4 Migratie en randvoorwaarden

Vraag 19
Kunt u een kostenindicatie geven o.b.v. scope (in aantal assets, niet in logvolume)

a) De totale kosten, inclusief onderhoud van de aangesloten assets (18 hosts, 40 linux vm's, 120 Windows server VM's, ca 500 windows clients, SaaS: office365, AzureAD)
b) Wat zijn de kosten voor extra aan te sluiten assets
c) Pricingmodel fixed price/maand of per melding)?
d) Welke inspanningen (kwantitatief) zijn naar uw ervaring nodig aan de zijde van de klant bij de inrichting van de SOC/het SIEM.

Vraag 20
Wat is de benodigde bandbreedte o.b.v. de scope?