GGD Zaanstreek-Waterland

Nota van inlichtingen

Betreft:	Marktconsultatie Detect & Respons
Datum:	27-6-2023

Nota van inlichtingen

Deze nota van Inlichtingen maakt integraal onderdeel uit van de aanbestedingsstukken. De vragen van een voorgaande nota van inlichtingen worden steeds herhaald. Nieuwe vragen en antwoorden worden onder aan de lijst toegevoegd. Daar waar de antwoorden strijdig zouden zijn, geldt voor dat deel het antwoord met het hoogste nummer.

1. Mededeling(en) aanbestedende dienst

1.1 Inhoudelijke mededeling

De GGD is enthousiast over de vragen die tot nu toe gesteld zijn. De GGD wil benadrukken dat de organisatie niet bekend is met de gevraagde dienstverlening en daarom ten volste geadviseerd wil worden in de geboden oplossing. Dit betekent dat wij open staan voor verschillende implementatievormen om de benodigde detectie en response te realiseren.

De GGD wenst dat de leverancier op basis van informatie die tot op heden verstrekt is, hierin meedenkt en passende dienstverlening of varianten in dienstverlening met voors en tegens adviseert.

1.2 Wijziging planning marktconsultatiegesprekken

In afwijking van wat in paragraaf 2.4.2. van het marktconsultatiedocument wordt vermeldt, zullen in plaats van 5 gesprekken maximaal 4 gesprekken worden gevoerd. Het tijdschema ziet er na deze wijziging als volgt uit:

Datum	Tijdvak
12 juli 2023	8.30 uur tot 10.00 uur
12 juli 2023	10.30 uur tot 12.00 uur
12 juli 2023	13.00 uur tot 14.30 uur
12 juli 2023	15.00 uur tot 16.30 uur

U wordt bij uw aanmelding voor een gesprek verzocht een voorkeur voor een tijdstip én een alternatief op te geven. We wijzen er nogmaals op dat een verzoek voor een gesprek geen garantie biedt dat u daadwerkelijk wordt uitgenodigd.

2. Vragen en antwoorden

Nr.	Label	Onderwerp
1.		Huidige situatie
Vraag	Kunt u meer inzicht geven in de huidige tooling en security-omgeving? Wij zijn met name geïnteresseerd in Firewall, Endpoint, huidige tooling en de Microsoft-omgeving. Dit geeft ons als leverancier een kader om relevant te zijn in onze beantwoording van uw marktconsultatie.	
Antwoord	De GGD heeft Sophos central Intercept X advanced endpoint & Server & Firewall XG wordt later XGS (x-stream protection, webserver protection en E-mail protection als technische beveiligingsmaatregelen.	

Nr.	Label	Onderwerp
2.		Huidige situatie
Vraag	Kunt u de aantallen en soorten gebruikers aangeven? Dit is relevant om te voldoen aan de door u gevraagde prijsindicatie.	
Antwoord	De GGD heeft naar schatting 550 medewerkers. Het is onduidelijk wat de leverancier bedoelt met soorten gebruikers.	

Nr.	Label	Onderwerp
3.		Huidige situatie
Vraag	Hoe heeft u momenteel de endpoints en servers beschermd.	
Antwoord	De GGD heeft Sophos central Intercept X advanced endpoint & Server & Firewall XG wordt later XGS (x-stream protection, webserver protection en E-mail protection als technische beveiligingsmaatregelen.	

Nr.	Label	Onderwerp
4.		Huidige situatie
Vraag	Betreft de omgeving een on-premise, hybride en/of cloud?	
Antwoord	Onze Infrastructuur is voornamelijk on-premise en de meeste applicaties worden extern gehost (SaaS). De externe SaaS applicaties vallen buiten scope van deze uitvraag.	

Nr.	Label	Onderwerp
5.		Huidige situatie
Vraag	Wordt er gebruik gemaakt van Microsoft Azure/ O365 en hoe is de bescherming daarop geregeld?	
Antwoord	GGD maakt gebruikt van office 2019, de wens is om uiteindelijk te migreren naar O365. De leverancier dient hiermee rekening te houden in de beantwoording en de prijsopgave.	

Nr.	Label	Onderwerp
6.		Gewenste situatie
Vraag	Is het de bedoeling dat op heel het infrastructuur Detection & response geregeld wordt en dient de firewall geïntegreerd te worden? Kunt u ook aantallen geven?	
Antwoord	GGD wenst in zo vroeg mogelijk stadium van de kill-chain aanvallen te kunnen detecteren. Blinde vlekken kunnen resulteren in een tragere identificatie en response. Afhankelijk van de prijsontwikkeling is het wenselijk om de gehele infrastructuur met uitzondering van de externe Saas Applicaties en mobiele te laten monitoren. GGD-ZW wenst dat de leverancier meedenkt in het komen tot een passende dekking in relatie tot detectie. GGD ziet graag in de beantwoording dit terug.	

Nr.	Label	Onderwerp
7.		Gewenste situatie
Vraag	Detetion & Response kan ingeregeld worden dat dit als een dienst afgenomen wordt. Wat wil GGD Zaanstreek hier zelf in betekenen. Zijn er activiteiten die GGD zelf wil doen of wordt alles uitbesteedt?	
Antwoord	Voor een algemeen antwoord verwijst de GGD naar paragraaf 2.2 van de marktconsultatie documentatie. De GGD wil idealiter zelf in control zijn over de response activiteiten (isoleren end-points etc) maar wordt graag bijgestaan door de leverancier met advies in relatie tot de nemen stappen. Ingeval van grootschalige calamiteiten zoals Ransomware is het wenselijk dat de ondersteuning wordt uitgebreid met bijvoorbeeld crisisondersteuning en forensisch onderzoek. Daarnaast heeft de GGD contacten met Z-CERT en GGD-GHOR voor ondersteuning met betrekking tot incident-response.	

	De GGD staat open voor meerdere implementatiemogelijkheden en wenst dat de leverancier hier inzicht in geeft en zijn visie op deelt met bijbehorende prijsopbouw, zodat de GGD een gerichtere aanvraag in de markt kan uitzetten.

Nr.	**Label**	**Onderwerp**
8.		Gewenste situatie
Vraag	Wat zijn uw verwachtingen met betrekking tot de detectie van beveiligingsincidenten? Wilt u proactief worden geïnformeerd over mogelijke dreigingen of pas wanneer er daadwerkelijke incidenten plaatsvinden?	
Antwoord	De GGD wil ook geïnformeerd worden over risico's en gebeurtenissen die uit de monitoring geïdentificeerd worden. Reguliere risico's worden graag behandeld in vorm van rapportage en hoge risico's dienen acuut gemeld te worden.	

Nr.	**Label**	**Onderwerp**
9.		Huidige situatie
Vraag	Welke maatregelen hebt u genomen om uw netwerk- en systeembeveiliging te verbeteren zelf zonder een formele detection- en response oplossing?	
Antwoord	Met betrekking tot de veiligheid wordt niet in volledig detail hierover uitgeweid. Zie voor de technische beveiligingsmaatregelen de beantwoording bij vraag 1 en daarnaast wordt o.a. netwerksegmentatie toegepast.	

Nr.	**Label**	**Onderwerp**
10.		Gewenste situatie
Vraag	Zijn er regelgeving of compliance vereisten waaraan uw organisatie moet voldoen met betrekking tot beveiligingsincidenten en bescherming van gegevens?	
Antwoord	NEN7510 en mogelijk BIO in de toekomst.	

Nr.	**Label**	**Onderwerp**
11.		Gewenste situatie
Vraag	Welke verwachtingen heeft uw organisatie met betrekking tot de implementatie tijd van de oplossing. Dient het voor een bepaalde datum gerealiseerd te worden?	
Antwoord	Dit is afhankelijk van de complexiteit en benodigde inspanning van de implementatie. Wij bepalen graag samen met de leverancier de benodigde planning.	

Nr.	**Label**	**Onderwerp**
12.		Huidige situatie
Vraag	Wat is de omvang van uw organisatie; - Medewerkers - Endpoint - Servers - E.d.	
Antwoord	Medewerkers naar inschatting 550 Switches 32 Windows 10 devices 500 Fysieke servers 6 VM's 40 Thin Clients 150 — Worden op termijn vervangen door laptops Overige netwerk devices 25 — Firewall/router/Access points Printers 32	

Nr.	Label	Onderwerp
13.		Algemeen
Vraag	Hoe wordt op dit moment de verzameling van Threat Intelligence gedaan? Welke platformen en bronnen worden er gebruikt?	
Antwoord	De GGD heeft nog geen capability ingericht rondom Threat Intelligence, maar ontvangt reguliere dreigingsinformatie vanuit Z-CERT. Het is wenselijk dat de leverancier kan aansluiten op het Zorg Detectie Netwerk van Z-CERT om Threat Intelligence informatie te ontvangen en hierop te acteren.	

Nr.	Label	Onderwerp
14.		Vragenlijst, vraag 10
Vraag	Welke grote cyberrisico's ziet de GGD? Kunt u een top 5 aangeven?	
Antwoord	In onze huidige strategie is voornamelijk de focus gelegd op het voorkomen, detecteren, reageren en herstellen op Ransomware. Daarnaast is een GGD-breed risico de kans op datalekken.	

Nr.	Label	Onderwerp
15.		Huidige situatie
Vraag	Hoe wordt op dit moment de security volwassenheid gemeten? Welk framework wordt er gebruikt? Bijvoorbeeld NIST CSF, CIS, BIO, NEN7510 etcetera.	
Antwoord	NEN7510 en CIS en mogelijk in de toekomst de BIO.	

Nr.	Label	Onderwerp
16.		Vragenlijst, vraag 8
Vraag	Om een indicatie te geven van de kosten hebben wij meer informatie nodig over de scope zoals: aantal geregistreerde users in AD/AAD, endpoints (werkplekken en servers) applicaties, SIEM (bijv Sentinel) etc. Kunt u ons meer informatie geven om een indicatie te geven van de onboarding en terugkerende kosten?	
Antwoord	Medewerkers naar inschatting 550	
	Switches 32	
	Windows 10 devices 500	
	Fysieke servers 6	
	VM's 40	
	Thin Clients 150	Worden op termijn vervangen door laptops
	Overige netwerk devices 25	Firewall/router/Access points
	Printers 32	

Nr.	Label	Onderwerp
17.		Vragenlijst, vraag 1
Vraag	Er wordt in vraag 1 gevraagd om twee concrete voorbeelden van ervaring in de zorg. Wij kunnen in een marktconsultatie geen referenties geven zonder een NDA en/of toestemming van de klant. Kunnen wij de trajecten beschrijven zonder te verwijzen naar specifieke zorg organisaties?	
Antwoord	De GGD heeft begrip voor de situatie dat toestemming nodig is voor de klant. De GGD heeft voorkeur voor een zo gedetailleerd mogelijk omschrijving van de referentie(s). Indien dit niet mogelijk is om de klantnaam te noemen, dan volstaat een algemene toelichting (omvang, branche, digitale omgeving).	

Nr.	Label	Onderwerp
18.		Vragenlijst, vraag 8

Vraag	Is er al een voorkeur van security technology stack? Welke vendor/oplossingen gebruikt GGD momenteel voor de infrastructuur zoals opgegeven in het document?
Antwoord	De GGD heeft Sophos central Intercept X advanced endpoint & Server & Firewall XG wordt later XGS (x-stream protection, webserver protection en E-mail protection als technische beveiligingsmaatregelen.

Nr.	**Label**	**Onderwerp**
19.		Algemeen
Vraag	Hoe wordt momenteel de monitoring op de Firewall en Endpoint detectie gedaan?	
Antwoord	De GGD heeft Sophos central Intercept X advanced endpoint & Server & Firewall XG wordt later XGS (x-stream protection, webserver protection en E-mail protection als technische beveiligingsmaatregelen en meldingen worden handmatig opgevolgd.	

Nr.	**Label**	**Onderwerp**
20.		Algemeen
Vraag	Welke oplossingen worden er gebruikt voor het verzamelen, opslaan en correleren van loggegevens?	
Antwoord	Geen	

Nr.	**Label**	**Onderwerp**
21.		Algemeen
Vraag	Hoe ziet het huidige applicatielandschap van de GGD er uit?	
Antwoord	Zorg applicaties worden extern gehost bij meerdere leveranciers. De Corona applicaties worden gemonitord door GGD-GHOR. Naar verwachting is het mogelijk dat deze monitoring gaat uitbreiden naar alle extern gehoste applicaties bij GGD-GHOR. Voor deze reden valt monitoring van de externe SaaS Applicaties buiten scope van deze uitvraag.	

Nr.	**Label**	**Onderwerp**
22.		Algemeen
Vraag	Zijn er globale netwerkdesign of Azure landingzone tekeningen die de GGD zou kunnen delen?	
Antwoord	Voor veiligheidsredenen worden deze niet gedeeld tijdens de marktconsultatie fase.	

Nr.	**Label**	**Onderwerp**
23.		Vragenlijst
Vraag	Om de vraag "Met welke eenmalige en structurele kosten dient de GGD rekening te houden met betrekking tot de dienstverlening? Kunt u een indicatie geven van deze kosten?" te kunnen beantwoorden, kan ik aangeven dat dit bepaald wordt door de prijs per gebruiker voor de endpointprotectie en protected throughput voor de netwerkprotectie. Kunt u aangeven welk endpointprotectie product er gebruikt wordt en hoeveel licenties hiervan aanwezig zijn, en welke firewalls (merk en type) de GGD heeft?	
Antwoord	De GGD heeft Sophos central Intercept X advanced endpoint & Server & Firewall XG wordt later XGS (x-stream protection, webserver protection en E-mail protection als technische beveiligingsmaatregelen.	

Nr.	**Label**	**Onderwerp**
24.		Vraag 8

Vraag	Opdrachtgever maakt gebruik van de Microsoft Sentinel oplossing om de MDR dienstverlening op te leveren. De kosten voor de Managed dienst zijn afhankelijk van de gekozen modules, welke van de drie modules en opties heeft klant behoefte aan: • Cloud monitoring (on-premises, AWS, Azure) • Werkplek monitoring (users & apps) • Werkplek & Endpoint monitoring (users, apps & devices) Opties: • Forensic research • ITSM integratie
Antwoord	Op basis van deze vraag is het nog niet duidelijk wat de geboden dienstverlening inhoud en kan de GGD hier geen antwoord op geven. De GGD wenst dat de leverancier op basis van informatie die tot op heden verstrekt is, hierin meedenkt en passende dienstverlening of varianten in dienstverlening met voors en tegens adviseert.

Nr.	**Label**	**Onderwerp**
25.		Algemeen
Vraag	Daarnaast hebben wij de volgende gegevens nodig ten behoeve van het afgeven van een kosten indicatie • Gewenste retentie van data • De Events per Second van de devices welke in scope zijn, of het aantal Gigabytes per Day getal wat aan log bestanden wordt gegenereerd. • Verder het aantal en soort devices welke log bestanden gaan genereren richting Sentinel, bijvoorbeeld 1 x FortiAnalyzer, 2x CISCO ASA switch, 20 x Windows 2016 Servers etc.	
Antwoord	Afhankelijk van de kosten wil de GGD een data retentie van minstens een half jaar tot een jaar. De GGD wenst hierin een advies te ontvangen van de leverancier. Het aantal Events per Second is niet inzichtelijk. Hieronder een overzicht van de bedrijfsmiddelen, dit betreffen Windows 2019 servers, VMware/VSphere/Sophos/CISCO & Dell switches. Medewerkers naar inschatting 550 Switches 32 Windows 10 devices 500 Fysieke servers 6 VM's 40 Thin Clients 150 Worden op termijn vervangen door laptops Overige netwerk devices 25 Firewall/router/Access points Printers 32	

Nr.	Label	Onderwerp
26.		Vragenlijst
Vraag	U geeft aan: "Heeft uw organisatie ervaring met het leveren van de uitgevraagde diensten inclusief volledige implementatie ervan binnen de zorg? Zo ja, welke ervaring (graag twee concrete voorbeelden aanleveren)?". Het gebruik van Detect & Response is nog vrij nieuw binnen de zorg sector en niet elke organisatie die daarvan gebruik maakt wil dit aan de buitenwereld laten weten. Mogen wij ook voorbeelden noemen van aan de zorg gerelateerde organisaties die medische gegevens verwerken?	
Antwoord	De GGD heeft voorkeur voor een zo gedetailleerd mogelijk omschrijving van de referentie(s). Indien dit niet mogelijk is om de klantnaam te noemen, dan volstaat een algemene toelichting (omvang, branche, digitale omgeving).	