Bijlage H ‘Programma van eisen’

Met het doen van een inschrijving gaat inschrijver onvoorwaardelijk akkoord met alle eisen uit het Programma van Eisen.

Inschrijver dient zich aan onderstaande voorschriften te houden. Afwijkingen van hetgeen is voorgeschreven worden niet geaccepteerd en leiden tot ongeldigheid en/of het niet (verder) in behandeling nemen van de Inschrijving.

De eisen in het Programma van Eisen heeft een knock-out karakter: het niet voldoen aan één of meerdere van deze eisen leidt automatisch tot uitsluiting.

1.1 Algemene eisen aan de opdracht

Nr.	Omschrijving
E1	Uw inschrijving (offerte) is ten minste geldig voor een periode van 90 dagen, te rekenen vanaf datum indienen Inschrijving. Tijdens deze periode heeft de Inschrijving het karakter van een onherroepelijk aanbod. Op verzoek van de aanbestedende dienst dient de inschrijver deze termijn te verlengen met 90 dagen. De inschrijving heeft een gestanddoeningstermijn van 90 kalenderdagen. Indien tegen de gunningsbeslissing een kort geding aanhangig wordt gemaakt, wordt de gestanddoeningstermijn - indien nodig - automatisch verlengd met een termijn van 45 dagen na de dag van de uitspraak van de rechter.
E2	Vanaf start van de overeenkomst dient zo spoedig als mogelijk overgegaan te worden tot implementatie, echter uiterlijk binnen 3 weken. De kosten van de dienstverlening worden in rekening gebracht vanaf oplevering en acceptatie van de dienstverlening. Acceptatie vindt plaats op basis van de volgende criteria: - SIEM is geïmplementeerd voor de aanbestedende dienst en ingericht voor en afgestemd op de omgeving van de aanbestedende dienst, waarbij kinderziektes, false-positives etc. zijn herkend en opgelost. - Alle log-bronnen in scope zijn aangesloten op het SIEM - De opslag van verzamelde (log-)informatie is ingericht, incl. eventuele overdracht van hot- naar cold-storage - De werking van de initiële response door isolatie van gecompromitteerde (hier voor een test aangewezen) assets is aangetoond voor de verschillende asset-typen - Het interface met Topdesk is gerealiseerd en functioneel - NDR is geïmplementeerd, passend ingericht en aangesloten op het SIEM - Honeypots zijn geïmplementeerd, passend ingericht en aangesloten op het SIEM - Alle overige log-bronnen in scope zijn aangesloten op het SIEM - Threat intelligence is geïmplementeerd en passend ingericht en eerste meldingen zijn gedaan - Threat hunting is geïmplementeerd en heeft eerste resultaten opgeleverd - Melding en triage van kwetsbaarheden - Werkafspraken tussen SOC en de aanbestedende dienst zijn gemaakt, onder andere over: escalatieladder en bevoegdheden tav initiële respons. - Het SOC is ingericht en operationeel voor de aanbestedende dienst en eerste meldingen zijn gedaan - Er is voldaan aan de overige eisen uit het beschrijvend document en het pakket van eisen
E3	Vanaf de start van de implementatie dient de dienstverlening binnen 3 maanden operationeel te zijn, inclusief acceptatie. Uitzondering daarop is de logging door bedrijfsapplicaties, die niet voorzien in een standaard interface voor logging. Deze worden in een tweede fase ge-onboard, die gepland zal worden op basis van een nadere inventarisatie. NB wel in scope is de logging van toegang via AzureAD tot deze bedrijfsapplicaties, zoals geslaagde en niet-geslaagde inlogpogingen.
E4	De inschrijver rapporteert tijdens de implementatie wekelijks over de voortang van de implementatie in relatie tot de planning (conform Plan van Aanpak)
E5	De inschrijving is in de Nederlandse taal opgesteld.
E6	Contractering en communicatie geschieden in de Nederlandse taal. Urgente technische-operationele communicatie mag buiten kantoortijden schriftelijk en mondeling in het Engels plaats vinden, mits op taalniveau B2 of hoger van het CEFR (zie https://www.coe.int/en/web/common-

	european-framework-reference-languages/level-descriptions, maar mondeling/telefonisch contact binnen kantoortijden dient in het Nederlands te geschieden.
E7	Door inschrijving verklaart Inschrijver onvoorwaardelijk akkoord te gaan met alle eisen en voorwaarden beschreven in deze Aanbestedingsleidraad, de bijbehorende bijlagen en overige aanbestedingsstukken.
E8	Alle door Inschrijver in het kader van deze aanbesteding overgelegde gegevens en gedane verklaringen zijn door Inschrijver naar waarheid ingevuld en kunnen te allen tijde gestand worden gedaan. Aanbestedende dienst behoudt zich het recht op schadevergoeding voor, in het geval van onjuiste en/of onvolledige informatie en/of het niet kunnen nakomen van wat door Inschrijver is aangeboden.
E9	Alle verwerking van persoonsgegevens vind plaats binnen de Europese Economische Ruimte (EER). Dat wil onder andere zeggen dat alle personeel, apparatuur, gegevensopslag en netwerkverbindingen die voor de aanbestedende diensten worden gebruikt, zich binnen de EER bevinden.
E10	De informatie, met betrekking tot de het Beschrijvend document en de uitgebrachte Inschrijving, wordt vertrouwelijk behandeld en uitsluitend gebruikt voor de aanbestedingsprocedure. Inschrijvers mogen de gegevens uit de Aanbestedingsdocumenten alleen gebruiken voor het doel waarvoor ze zijn verstrekt, namelijk het uitbrengen van de Inschrijving. Een Inschrijver zal deze verplichting eveneens opleggen aan de door hem in te schakelen Derden, bijvoorbeeld een adviesbureau dat Inschrijver begeleidt bij het doen van de Inschrijving of een Derde waar mogelijk een beroep op wordt gedaan. Deze geheimhouding blijft ook na afloop van de aanbestedingsprocedure van kracht. De Inschrijvers waarborgen dat gegevens, die door de Aanbestedende dienst ter beschikking zijn gesteld, na gebruik worden vernietigd.

1.2 Commerciële eisen aan de opdracht

Nr.	Omschrijving
E11	Alle aangeboden prijzen, tarieven en kosten zijn vermeld in euro's, zoveel mogelijk gespecificeerd, exclusief Nederlands geldende BTW-tarieven.
E12	Inschrijver is bij haar inschrijving uitgegaan van geldende prijzen voor de dienstverlening en/of levering. Niet genoemde kosten kunnen onder geen geval alsnog in rekening worden gebracht bij de Werkorganisatie BUCH. Hetgeen door inschrijver wordt uitgewerkt in het kwalitatief gunningscriterium is in de opgegeven prijs van inschrijver inbegrepen.
E13	Inschrijver verklaart dat hij ermee akkoord gaat dat prijswijzigingen niet eerder van kracht zijn dan na schriftelijke goedkeuring door Aanbestedende dienst.
E14	Inschrijver sluit een onderhoudsovereenkomst af voor de onderdelen van de oplossing met een looptijd gelijk aan de contractduur, welke direct bij de producent is ondergebracht. Na deze periode dient u de supportperiode te kunnen verlengen gelijk aan de contractperiode, incl. verleningen.
E15	Binnen de onderhoudsovereenkomst vallen ook de updates van software, besturingssystemen en eventuele firmware, ongeacht de versie(s) en (nieuwe/extra) functionaliteiten.
E16	Garantie en support voor eventueel benodigde hard- en software dienen voor de gehele contractperiode te zijn afgekocht bij de fabrikant.
E17	Aanbestedende dienst zal geen prijsonderhandelingen voeren. De prijs wordt derhalve volledig bepaald door het uitbrengen van de offerte. De aanbieder krijgt aan de hand van deze offerteaanvraag slechts één gelegenheid om een aanbieding uit te brengen.

1.3 Facturatie eisen aan de opdracht

Nr.	Omschrijving
E18	Inschrijver mag zich niet beroepen op een lead kwalificatie/korting of andere vorm van korting bij de vendor(en), waarbij mogelijk andere inschrijvende partijen een achterstand hebben in prijsverhoudingen. Wanneer korting door lead verkregen wordt, moet dit bij de Werkorganisatie BUCH kenbaar gemaakt te worden. De verkregen korting moet dan in het prijzenblad kenbaar gemaakt worden.

1.4 Eisen aangaande Ondersteuning

Nr.	Omschrijving
E19	Inschrijver levert, implementeert en richt afgestemd op de aanbestedende dienst in alle producten, diensten en functionaliteiten zoals beschreven in dit document conform dit Plan van Eisen. Ook wanneer technische componenten benodigd voor gespecificeerde dienstverlening niet expliciet genoemd wordt.
E20	Opdrachtnemer evalueert per ***kwartaal*** met de aanbestedende dienst de gang van zaken met betrekking tot de Overeenkomst. De onderwerpen worden in overleg tussen de Gemeente en Opdrachtnemer nader bepaald.
E21	Inschrijver levert op verzoek van en in overleg met de aanbestedende dienst eens per maand de volgende service level rapportages te overhandigen: • Verrichtte requests/aanvragen van de aanbestedende dienst en status • Aantallen events/alerts, meldingen aan de gemeente en incidenten naar classificatie, zoals informational, low, medium, high, critical • Beschikbaarheid van diensten SOC en SIEM over de rapportageperiode • Evaluatie en aanbevelingen • Klachten en klachtafhandeling
E22	Inschrijver stelt een vast contactpersoon (en vervanger) aan voor alle communicatie tussen de gemeente en Inschrijver gedurende de implementatie en uiteindelijke acceptatie. Het contactpersoon rapporteert tevens aan Werkorganisatie BUCH op regelmatige basis de voortgang van openstaande issues/verbeterpunten. De gemeente stelt ook een vast contactpersoon (en vervanger) aan.
E23	Inschrijver stelt zich als tactisch en strategische partner voor de gemeente op. Dit houdt in dat zij proactief acteert op wijzigingen/verbeteringen of andere zaken welke betrekking hebben op de aangeboden oplossing. De frequentie van dergelijk overleg en deze activiteiten moet minimaal 1 maal per jaar zijn, in het eerste contractjaar minimaal 1 maal per kwartaal.
E24	De mate en vorm van communicatie wordt vastgelegd in een OLA of SLA. Deze dient vanuit inschrijver opgeleverd te worden.
E25	Inschrijver dient bij gunning, als aanvulling op de geëiste OLA / SLA, gezamenlijk een DAP overeen te komen waarin minimaal de navolgende onderwerpen belegd zijn: • Strategische en tactisch advies • Melding van en advies over door het SOC vastgestelde beveiligingsissues • Een klachtenprocedure • Problem support (actief en reactief) • Escalatiemodel (opdrachtnemer en Aanbestedende dienst)

1.5 Duurzaamheid en kwaliteit

Nr.	Omschrijving
E26	De organisatie van de inschrijver moet een duurzaamheidsbeleid voeren (Maatschappelijk Verantwoord Ondernemen - MVO), waarin de sociale, milieu en economische aspecten geïntegreerd zijn.

1.6 Eisen aan de leverancier en de toeleveringsketen

Nr.	Omschrijving
E27	Op basis van de Verordening (EU) nr. 833/2014 van de Raad van 31 juli 2014 mag er geen sprake zijn van enige Russische betrokkenheid bij uitvoering van de Opdracht. Met ondertekening van de. Inschrijving verklaart Inschrijver dat er geen sprake is van Russische betrokkenheid bij de uitvoering van deze Overeenkomst die de drempels van artikel 5 duodecies van EU Verordening (EU) 833/2014 van 31 juli 2014 (betreffende de betreffende beperkende maatregelen naar aanleiding van de acties van Rusland die de situatie in Oekraïne destabiliseren, zoals gewijzigd bij Verordening2022/578 van 8 april 2022) overschrijdt. Zo nodig kan Aanbestedende dienst bij de onderneming aanvullende bewijzen opvragen hoe de eigendomsstructuur dan wel controle is geregeld.

1.7 Eisen aan de SOC dienstverlening

Nr.	Omschrijving

E28	Het SOC voert een triage en analyse uit op alerts vanuit het SIEM, zodat de aanbestedende dienst alleen meldingen ontvangt, waarbij acties nodig zijn, bijvoorbeeld door systeem- en/of netwerkbeheerders.
E29	Het SOC isoleert assets/plaatst deze in quarantaine om een aanval of inbreuk te dwarsbomen en/of in te dammen via isolatie van assets met behulp van EDR en/of de blokkering van gebruikers in AAD/IntraID of AD. Na gunning worden nadere afspraken gemaakt over : - de situaties waarin deze bevoegdheden moeten/mogen worden gebruikte - communicatie en beslisprotocol met bevoegdheden van de inschrijver - werkwijze per assettype afhankelijk van de functionaliteit van EDR en de toewijzing van bevoegdheden aan de inschrijver. Het gaat daarbij om containment, zodra een inbreuk is geconstateerd.
E30	Het SOC adviseert in het incident response proces in afstemming met management en/of beheerders van de aanbestedende dienst die door het SOC geconsulteerd zullen worden en die acties uitvoeren waartoe zij wel en het SOC niet geautoriseerd is.
E31	Openingstijden van het SOC zijn werkdagen van 8.00-18.00 Buiten dit tijdsvenster is er een SOC-analist stand-by om in het geval van een vermoedde inbreuk een triage/analyse uit te voeren en waar nodig in te grijpen en melding te doen bij de gemeente.
E32	Tijdens openingstijden, start de triage/analyse van hoge/kritieke alerts binnen 5 minuten.
E33	Tijdens openingstijden, wordt de aanbestedende dienst binnen 30 minuten gecontacteerd over hoge/kritieke alerts incl. status
E34	Buiten openingstijden, wordt de aanbestedende dienst binnen 1 uur gecontacteerd over vermoedde inbreuken
E35	Hoge en kritieke alerts worden meteen geautomatiseerd gemeld via het ticketing systeem van de aanbestedende dienst.
E36	De inschrijver voorziet de aanbestedende dienst van advies over communicatie- en handelingsplannen bij inbreuken.
E37	De aanbestedende dienst heef contact met een vaste SOC analist, die de organisatie en ICT infrastructuur van de aanbestedende dienst goed kent. Er is een competente vervanger voor deze SOC-analist bij afwezigheid.
E38	Het SOC levert ten minste maandelijks een operationele rapportages over de bevindingen met adviezen voor verbetering, dat wordt besproken met de in de vorige eis genoemde SOC-analist (van de zijde van de aanbestedende dienst: TISO)
E39	Het SOC levert ten minste eens per kwartaal een rapportage over de dienstverlening die wordt besproken op tactisch niveau.(van de zijde van de aanbestedende dienst: Leveranciersmanager, CISO en/of hoofd ICT)

1.8 Eisen aan de SIEM-oplossing/-dienstverlening

Nr.	Omschrijving
E40	De inschrijver biedt het SIEM als dienst aan, inclusief levering van software, inrichting en beheer. Voor lokale log-collectie en honeypots mag gebruik gemaakt worden van (kale) virtuele machine(s) die door de aanbestedende dienst ter beschikking word(en) gesteld.
E41	Voor het SIEM worden toekomstbestendige producten uit de markt ingezet. Producten waarvan de leverancier end-of-life heeft aangekondigd of een productstrategie waarin SIEM niet meer centraal staat, voldoen niet aan deze eis.
E42	De beschikbaarheid van het SIEM is 99,8% per maand excl. beschikbaarheid van een eventueel gebruikte (kale) VM die door de aanbestedende dienst ter beschikking wordt gesteld en excl. Met de aanbestedende dienst afgestemde onderhoudsvensters (max 1 uur/maand).
E43	De inschrijver maakt ten minste gebruik van een set van Use Cases die door de leverancier van het gebruikte SIEM-product wordt geleverd, onderhouden en worden aangevuld op basis van nieuwe kwetsbaarheden, bedreigingen en Indicators of Compromise.
E44	De inschrijver neemt door de aanbestedende dienst gespecificeerde Use Cases op in het SIEM en de documentatie is voor de aanbestedende dienst beschikbaar.
E45	De loginformatie wordt 13 maanden bewaard. Daarna worden de log-gegevens (semi-)automatisch verwijderd. Van deze periode is ten minste de afgelopen 30 dagen hot storage.
E46	Deze bewaartermijn is op wens van de aanbestedende dienst aan te passen. Toelichting: De gemeente wil de flexibiliteit hebben de bewaartermijn aan te passen, wanneer daar gedurende de contractperiode

	aanleiding toe is, bijvoorbeeld bij voortschrijdend inzicht. In dat geval zou de bewaartermijn bijvoorbeeld uitgebreid kunnen worden naar 18 of 24 maanden.
E47	Aan het einde van het contract worden de loggegevens in het SIEM in een gestandaardiseerd formaat, zoals bijvoorbeeld JSON of XML, overgedragen aan de aanbestedende dienst.
E48	De dienst voorziet in een online dashboard en inzage in de alerts voor de aanbestedende dienst.
E49	Toegang tot dashboard via het internet is versleuteld met protocollen volgens het Forum Standaardisatie https://www.forumstandaardisatie.nl/open-standaarden en de toegang beveiligd met Meer-Factor-Authenticatie (MFA)
E50	De verbinding tussen het netwerk van de aanbestedende dienst en het SIEM is versleuteld met protocollen volgens het Forum Standaardisatie https://www.forumstandaardisatie.nl/open-standaarden
E51	Het SIEM/SOC voorziet in een koppeling met Topdesk, zodat alerts geautomatiseerd kunnen worden doorgegeven in twee richtingen.
E52	De inschrijver voorziet de aanbestedende dienst aanwijzingen voor de aansluiting en configuratie van log-bronnen, zodat de voor detectie van de door u onder het kwalitatieve criterium Use Cases ook daadwerkelijk kunnen worden gedetecteerd op de logbron. Het gaat daarbij bijvoorbeeld om het instellen van audit policies in Windows en vergelijkbare instellingen op andere operating systems

1.9 Eisen aan de NDR dienstverlening

Nr.	Omschrijving
E53	NDR voorziet het SIEM van loginformatie over alle netwerkactiviteiten door informatie van SPAN ports van netwerkcomponenten te verwerken.
E54	NDR bewaakt zowel het externe verkeer als het interne verkeer.

1.10 Eisen aan de Honeypots

Nr.	Omschrijving
E55	De honeypots worden geïnstalleerd op een virtual machine, die door de aanbestedende dienst ter beschikking worden gesteld. (net als de productieservers)
E56	De honeypots zijn voor een indringer niet te onderscheiden van productiesystemen
E57	De honeypots dekken een brede functionaliteit af, in ieder geval webserver, databaseserver, storage en rdp.
E58	De honeypots melden alle activiteiten aan het SIEM
E59	De honeypots emuleren functionaliteit, zonder de geëmuleerde software te gebruiken.
E60	De inschrijver adviseert over de effectieve inzet van honeypots

1.11 Eisen aan de Threat Intelligence dienstverlening

Nr.	Omschrijving
E61	Het SOC voert Threat Intelligence uit: het inwinnen en analyseren van informatie over ontwikkelingen van dreigingen en aanvallen en het vertalen daarvan naar aanvullende maatregelen, ter ondersteuning van de overige dienstverlening van het SOC
E62	De inschrijver maakt gebruik van erkende threat intelligence feeds en eigen analyses. NB Het gaat om generieke threat intelligence, niet specifiek op de aanbestedende dienst gerichte bedreigingen.
E63	Voor Threat Intelligence worden toekomstbestendige mainstream feeds/diensten uit de markt ingezet met minimaal maatwerk.

1.12 Eisen aan de Threat Hunting dienstverlening

Nr.	Omschrijving
E64	Het SOC voert Threat hunting uit: Een pro-actieve aanpak om nog niet bekende beveiligingsissues binnen het netwerk en de systemen van de aanbestedende dienst op te sporen