Gemeente Gouda

Bijlage A1 Programma van Eisen

Inschrijver wordt verzocht deze Bijlage volledig in te vullen en als Bijlage bij te voegen.

Inschrijver wordt verzocht van alle in de Bijlage genoemde Eisen te verklaren of Inschrijver deze voorschriften accepteert en conform de procedure handelt / heeft gehandeld. Inschrijver dient, indien Inschrijver de Eisen accepteert, in de tabellen in de daarvoor bestemde kolom een ***'ja'*** te plaatsen, een ***'nee'*** leidt tot uitsluiting.

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	Ja/Nee
E1	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 deze diensten. 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 gecompromiteerde (hier voor een test aangewezen) assets is aangetoond voor de verschillende asset-typen - Het interface met Topdesk is gerealiseerd en functioneel - Threat intelligence is geïmplementeerd en passend ingericht en eerste meldingen zijn gedaan - Threat hunting is geïmplementeerd en heeft eerste resultaten opgeleverd - Werkafspraken tussen SOC en de aanbestedende dienst zijn gemaakt, onder andere over: escalatieladder en bevoegdheden tav initiele 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	
E2	Vanaf de start van de implementatie dient de dienstverlening binnen 3 maanden operationeel te zijn, inclusief acceptatie.	
E3	De inschrijver rapporteert tijdens de implementatie wekelijks over de voortang van de implementatie in relatie tot de planning (conform Plan van Aanpak)	
E4	De inschrijving is in de Nederlandse taal opgesteld.	
E5	Contractering en communicatie geschieden in de Nederlandse taal. Urgente technische-operationele communicatie mag 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)	
E6	Door inschrijving verklaart Inschrijver onvoorwaardelijk akkoord te gaan met alle eisen en voorwaarden beschreven in deze Aanbestedingsleidraad, de bijbehorende bijlagen en overige aanbestedingsstukken.	

E7	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. Opdrachtgever 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.	
E8	Deze eis is vervallen.	
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.	

1.2. Commerciële eisen aan de opdracht

Nr.	Omschrijving	Ja/Nee
E10	Alle aangeboden prijzen, tarieven en kosten zijn vermeld in euro's, zoveel mogelijk gespecificeerd, exclusief Nederlands geldende BTW-tarieven.	
E11	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 aanbestedende dienst. Hetgeen door inschrijver wordt uitgewerkt in het kwalitatief gunningscriterium is in de opgegeven prijs van inschrijver inbegrepen.	
E12	Inschrijver sluit daar waar uitgevraagd of op verzoek een onderhoudsovereenkomst af 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.	
E13	Binnen de onderhoudsovereenkomst vallen ook de updates van software, besturingssystemen en eventuele firmware, ongeacht de versie(s) en (nieuwe/extra) functionaliteiten.	
E14	Garantie en support voor eventueel benodigde hard- en software dienen voor de gehele contractperiode te zijn afgekocht bij de fabrikant.	
E15	Opdrachtgever 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.	
E16	Bij opdrachtverlening zal, indien van toepassing, de eventuele verrekening plaats vinden op basis van de werkelijk gerealiseerde aantallen.	

1.3. Facturatie eisen aan de opdracht

Nr.	Omschrijving	Ja/Nee
E17	U dient een aparte factuur te sturen voor eenmalige kosten en een aparte factuur voor maandelijks terugkerende kosten.	
E18	De facturatie vind maandelijks achteraf plaats op basis van een vaste dag van de maand aangesloten assets. De inschrijver staat het vrij om de prijzen per assettype te differentiëren.	
E19	Facturering van leveringen en diensten dienen na ontvangst van levering of uitvoering van dienstverlening plaats te vinden. Inschrijver factureert maandelijks **uitsluitend** digitaal door facturen in PDF-formaat te mailen aan: facturen@gouda.nl. t.a.v. onder vermelding van de volgende kenmerken: - projectnummer - verplichtingennummer - de datum van geleverde dienstverlening - het btw-bedrag - btw-nummer van Opdrachtnemer - KvK-nummer van Opdrachtnemer - Bankrekeningnummer van Opdrachtnemer Indien deze kenmerken ontbreken vindt geen betaling plaats en zal de factuur worden geretourneerd.	
E20	Aanbestedende dienst stelt het volgende facturatieschema en betalingscondities voor: • Incidentele kosten worden na acceptatie van de aanbestedende dienst gefactureerd. • De maandelijkse kosten worden gefactureerd vanaf acceptatie door de aanbestedende dienst. Voor acceptatiecriteria zie algemene eisen	

1.4. Eisen aangaande Ondersteuning

Nr.	Omschrijving	Ja/Nee
E21	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.	
E22	Opdrachtnemer evalueert in het eerste jaar per ***kwartaal*** met de aanbestedende dienst de gang van zaken met betrekking tot de Overeenkomst. Daarna vindt ***halfjaarlijks*** een evaluatie plaats dan wel vaker als Opdrachtgever hier om verzoekt. De onderwerpen worden in overleg tussen de Gemeente en Opdrachtnemer nader bepaald.	
E23	Inschrijver levert op verzoek van en in overleg met de gemeente 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	
E24	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 de aanbestedende dienst op regelmatige basis de voortgang van openstaande issues/verbeterpunten. De gemeente stelt ook een vast contactpersoon (en vervanger) aan.	

E25	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.	
E26	De mate en vorm van communicatie wordt vastgelegd in een OLA of SLA. Deze dient vanuit inschrijver opgeleverd te worden.	
E27	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 opdrachtgever)	

1.5. Eisen aan de SOC dienstverlening

Nr.	Omschrijving	Ja/Nee
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. Na gunning wordt afgestemd:* - *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	De inschrijver voorziet de aanbestedende dienst van advies over communicatie- en handelingsplannen bij inbreuken.	
E36	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	
E37	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.	
E38	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	

E39	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.	
E40	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)	
E41	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: CISO en/of hoofd ICT)	

1.6. Eisen aan de SIEM-oplossing/-dienstverlening

Nr.	Omschrijving	Ja/Nee
E42	De inschrijver biedt het SIEM als dienst aan, inclusief levering van software, inrichting en beheer. Voor lokale log-collectie mag gebruik gemaakt worden van (kale) virtuele machine(s) die door de aanbestedende dienst ter beschikking word(en) gesteld. Dat kan ook met behulp van de aanlevering van een VM-image aan de aanbestedende dienst.	
E43	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.	
E44	De beschikbaarheid van het SIEM is 99,9% 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).	
E45	De inschrijver maakt minimaal 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.	
E46	De inschrijver neemt door de aanbestedende dienst gespecificeerde Use Cases op in het SIEM en de documentatie is voor de aanbestedende dienst beschikbaar.	
E47	De loginformatie wordt 12 maanden bewaard. Daarna worden de log-gegevens (semi-) automatisch verwijderd. Van deze periode is ten minste de afgelopen 30 dagen hot storage.	
E48	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.	
E49	Op aanvraag en 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.	
E50	De dienst voorziet in een online dashboard en inzage in de alerts voor de aanbestedende dienst.	
E51	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)	
E52	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	
E53	Het SIEM/SOC voorziet in een koppeling met Topdesk, zodat alerts geautomatiseerd kunnen worden doorgegeven.	
E54	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	