	Programma van Eisen - Aanbesteding SIEM-SOC
	Toelichting eisen: In kolom B staan de eisen geformuleerd ten aanzien van de Oplossing waarmee inschrijver de Opdracht invult. Het niet kunnen voldoen aan (een van) deze eisen is een knock-out criterium.
1.	**Auditing**
1.1	Alle inzage- en beheeracties in de aangeboden oplossing worden automatisch vastgelegd in een auditlog. Deze log is continu en in real-time beschikbaar voor aangewezen medewerkers. In de auditlog worden in ieder geval met een timestamp de mutaties in autorisaties, gevoelige data en configuratie-instellingen opgenomen.
1.2	De auditlog moet zodanig worden ingericht dat gebruikers van het systeem deze niet kunnen wijzigen.
2.	**Bronaansluitingen**
2.1	De SIEM oplossing ondersteunt minimaal de volgende typen logbronnen of aansluitingen zoals aangegeven in bijlage 12 - ~~huidige situatie~~ Detailinformatie.
2.2	Het toevoegen, verwijderen en wijzigen van databronnen dient in overleg met de opdrachtgever te gebeuren. Indien nodig wordt dit projectmatig uitgevoerd, waarbij de opdrachtnemer de documentatie en architectuurplaat bijwerkt.
2.3	Vanaf de start van de implementatie moet de dienstverlening binnen 3 maanden operationeel zijn, inclusief de inrichting van het SIEM, de onboarding van assets/logbronnen en de SOC-dienst.
3.	**Detectie**
3.1	Compliancy- en securitypakketten (zoals baselines, use cases en threat intelligence) voor het SIEM dienen standaard meegeleverd en door de opdrachtnemer onderhouden te worden, zonder extra kosten voor het gebruik van de betreffende use cases of correlatieregels. Daarnaast wordt van de opdrachtnemer verwacht dat hij zelf de actualiteit in de gaten houdt en de use cases aanvult bij opkomende bedreigingen om de effectiviteit en actualiteit te waarborgen.
3.2	De set van Use Cases moet een breed scala van relevante en detecteerbare aanvalstechnieken uit het MITRE ATT&CK-framework (https://attack.mitre.org) dekken, met prioriteit voor technieken die aansluiten bij specifieke dreigingen en risico's binnen de infrastructuur van opdrachtgever.

3.3	De ruleset voor netwerkdetectie moet actueel zijn en minimaal in staat zijn om dagelijks de relevante updates te krijgen. De ruleset moet geavanceerde detectie van bestaande en opkomende bedreigingen in het netwerkverkeer mogelijk maken. Daarnaast wordt van de opdrachtnemer verwacht dat hij zelf de actualiteit in de gaten houdt en de ruleset aanvult bij opkomende bedreigingen.
3.4	Alleen aangewezen medewerkers van de opdrachtgever kunnen na instemming van opdrachtnemer wijzigingen doorvoeren die betrekking hebben op het detectiebeleid en de respons, zoals het aanpassen van afspraken over wanneer contact wordt opgenomen bij bepaalde typen alerts of het whitelisten van specifiek verkeer.
3.5	De correlatieregels op basis van use-cases en policies moeten toepasbaar zijn op zowel real-time als historische data en events.
3.6	De aangeboden oplossing moet in staat zijn om ongewenste software en websites te detecteren die een bedreiging kunnen vormen, zoals remote control applicaties, phishing- en malwaresites, en sites met hacktools.
3.7	De oplossing moet events van verschillende bronnen en apparaten kunnen correleren, zodat misbruik nauwkeuriger gedetecteerd kan worden.
3.8	De verwerking van de loginformatie gebeurt vrijwel realtime, met een maximale vertraging van 10 minuten. Wanneer een clouddienst de data echter later aanlevert, kan deze uiteraard niet realtime worden verwerkt.
3.9	De opdrachtnemer gebruikt geen componenten in de SIEM oplossing die een afhankelijkheid creëren met de opdrachtnemer tenzij op verzoek van de opdrachtgever. Bij het in gebruik nemen van componenten die een afhankelijkheid creëren moet er een exit strategie uitgewerkt zijn.
3.10	AI-tools en hun leveranciers dienen te voldoen aan de Europese AI act. Opdrachtnemer is verplicht de conformiteit van alle ingezette AI-tools hierop te toetsen en afwijkingen hierop aan de opdrachtnemer ter besluitvorming voor te leggen.

3.11	Indien leverancier gebruik maakt van AI tooling (generatief of analytisch) in de dienstverlening, moet dit vooraf expliciet worden gemeld inclusief datalocatie, subverwerkerslijst, trainingsmodel, gebruik en impact op persoonsgegevens. AI tooling mag geen data gebruiken voor modeltraining tenzij opdrachtgever expliciet en schriftelijk toestemming verleent (art. 13, 14 en 16 van de GIBIT).
3.12	Er worden geen hardwarecomponenten geïnstalleerd op de infrastructuur van de opdrachtgever.
3.13	In het prijsinvulformulier moeten prijzen per logbron worden aangegeven in drie categorieën, namelijk: A, B en C. De prijzen zijn indicatief.
4.	**Dienstverlening**
4.1	Opdrachtnemer is verantwoordelijk en draagt zorg voor het leveren, inrichten, en actueel houden van de SIEM oplossing en de meegeleverde SOC dienstverlening. Dit betreft de volledige dienstverlening en infrastructuur van de geleverde ict-prestatie.
4.2	Opdrachtnemer draagt er zorg voor dat de SIEM/SOC-dienstverlening meegroeit met ontwikkelingen op het gebied van wet- en regelgeving, nieuwe dreigingen en nieuwe inzichten en best practices op het gebied van informatiebeveiliging.
4.3	De contactpersonen en de uitvoerende medewerkers van de Opdrachtnemer beheersen de Nederlandse taal op niveau B1, zowel mondeling als schriftelijk.
4.4	De SOC-dienstverlening moet 24/7 actief zijn.
4.5	Het SOC moet de events bekijken en incidenten prioriteren. Bij een incident moet er een handelingsperspectief zijn dat beschrijft hoe en met welke prioriteit het incident opgevolgd moet worden.
4.6	Bij de hoogste classificatie (prio 1) geldt een mandaat actie dat binnen 30 minuten na bekendheid van het incident moeten worden uitgevoerd. Dit zal ook direct vermeld moeten worden aan de opdrachtgever. Overige prio's worden in overleg met elkaar afgestemd.

4.7	Het moet eenvoudig zijn om de dienst op of af te schalen bij een verandering in het aantal logbronnen die worden verwerkt. Dit betekent dat, afhankelijk van de behoefte, de dienst maandelijks of vaker kan worden aangepast om meer of minder logbronnen op te nemen, zonder dat dit ten koste gaat van de flexibiliteit of de continuïteit van de dienst.
4.8	De opdrachtnemer stelt een vaste contactpersoon (en vervanger) aan voor alle communicatie tussen de opdrachtgever en de opdrachtnemer gedurende de gehele periode van de implementatie en de operationele fase van de dienstverlening. Deze contactpersoon is verantwoordelijk voor de communicatie en afhandeling van alle meldingen en vragen met betrekking tot de SIEM SOC-dienstverlening en fungeert als primair aanspreekpunt voor de opdrachtgever. De contactpersoon moet: - Beschikbaar zijn voor het bespreken en afhandelen van gemelde problemen, incidenten en vragen in relatie tot de SIEM SOC-dienstverlening. - Proactief opvolging geven aan lopende problemen en incidenten. - Direct bereikbaar zijn via Microsoft Teams, telefoon of e-mail voor ad-hoc vragen en urgente situaties. - Regelmatig rapporteren aan de opdrachtgever over de voortgang van openstaande issues en verbeterpunten, in relatie tot de planning. - Advies bieden zonder extra kosten wanneer de opdrachtgever vragen heeft over de SIEM SOC-dienstverlening. - Optreden als sparringpartner bij het bespreken van nieuwe technologieën en ontwikkelingen in het vakgebied. Het hebben van een vast aanspreekpunt bevordert de efficiëntie en transparantie in het afhandelingsproces, zorgt voor een nauwe samenwerking tussen opdrachtgever en opdrachtnemer, en ondersteunt de opdrachtgever bij strategische en operationele vragen. De opdrachtgever stelt eveneens een vast contactpersoon (en vervanger) aan. De vaste contactpersoon (en vervanger) is verantwoordelijk voor de tactische en procesmatige regie op de dienstverlening (zoals de genoemde Service Delivery Manager). Deze persoon is het vaste aanspreekpunt tijdens kantoortijden. Voor de operationele 24/7-afhandeling van individuele meldingen en incidenten accepteert de opdrachtgever dat dit wordt uitgevoerd door het roulerende team van het SOC (1e, 2e en 3e lijn). De opdrachtnemer dient er echter voor zorg te dragen dat elke dienstdoende analist toegang heeft tot de klantspecifieke informatie van de opdrachtgever, zodat de continuïteit en kwaliteit van de afhandeling geborgd zijn.
4.9	Voor de opdrachtgever is inzichtelijk welke bronnen zijn aangesloten op het SIEM, welke use-cases worden gebruikt, op welke Indicator of Compromise (IoC's) wordt gecontroleerd en wat de specifieke instellingen zijn (bijvoorbeeld welke drempelwaarden zijn ingesteld).

4.10	Om de uitvoering van de opdracht door de opdrachtnemer continu te verbeteren, evalueert de opdrachtgever de dienstverlening periodiek, maar minimaal ~~één keer per maand~~ vier (4) keer per jaar. Deze evaluaties worden gezamenlijk uitgevoerd, zodat beide partijen de gelegenheid hebben om bevindingen en inzichten te delen. Op basis van deze evaluatie kunnen schriftelijke afspraken worden gemaakt over geconstateerde tekortkomingen, aandachtspunten en verbeteringen/maatregelen, zoals het verminderen van false positives. Deze afspraken zijn bindend, tenzij ze in strijd zijn met de overeenkomst of tenzij anders overeengekomen.
4.11	De opdrachtnemer biedt het SIEM als dienst aan, inclusief inrichting, monitoring en beheer.
4.12	De opdrachtnemer gebruikt voor de inrichting van de SIEM oplossing de bestaande Microsoft Sentinel omgeving in de bestaande Microsoft Azure tenant van de opdrachtgever.
4.13	Opdrachtnemer levert een gedetailleerd post-incident rapport en adviseert verbeteringen in de door opdrachtnemer beheerde ict-omgeving en -processen om toekomstige incidenten te voorkomen. Daarnaast worden er aanbevelingen richting opdrachtgever gedaan over het oplossen van organisatiekwetsbaarheden die buiten de invloedsfeer van de opdrachtnemer vallen.
4.14	Bij foutmeldingen, zoals het niet meer ontvangen van loginformatie, neemt de opdrachtnemer binnen 1 uur contact op met de opdrachtgever.
4.15	Het SOC is gevestigd binnen de Europese Economische Ruimte (EER).
4.16	De SIEM oplossing blijft ten alle tijde toegankelijk voor geauthoriseerde medewerkers van de opdrachtgever.

4.17	~~De opdrachtnemer levert een Incident Response (IR) retainer waarmee de opdrachtgever 24/7 directe toegang heeft tot een team van cyberbeveiligingsexperts, met vooraf vastgestelde reactietijden en tarieven, teneinde schade te beperken en herstel te versnellen. De retainer biedt gegarandeerde beschikbaarheid bij incidenten, inclusief directe telefonische ondersteuning en een overeengekomen starttijd voor het onderzoek. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor onder meer digitaal forensisch onderzoek, juridische ondersteuning en begeleiding bij communicatie met toezichthouders en verzekeraars. Daarnaast omvat de retainer proactieve voorbereidende diensten, zoals het opstellen van een Incident Response-plan en het verzorgen van trainingen, met als doel het beperken van financiële, reputatie- en juridische schade.~~ De opdrachtnemer levert een Incident Response (IR) retainer waarmee de opdrachtgever 24/7 directe toegang heeft (via een dedicated noodnummer, telefonisch) tot een team van cyberbeveiligingsexperts, met vooraf vastgestelde reactietijden en tarieven, teneinde schade te beperken en herstel te versnellen. De retainer biedt gegarandeerde beschikbaarheid bij incidenten, inclusief directe telefonische ondersteuning en een overeengekomen starttijd voor het onderzoek. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor onder meer digitaal forensisch onderzoek, juridische ondersteuning en begeleiding bij communicatie met toezichthouders en verzekeraars. Daarnaast omvat de retainer proactieve voorbereidende diensten, zoals het helpen van de opdrachtnemer bij het opstellen of actualiseren van een Incident Response-plan, afgestemd op de organisatie van de opdrachtgever, en het verzorgen van trainingen (minimaal één IR-oefening of training per jaar voor relevante medewerkers), met als doel het beperken van financiële, reputatie- en juridische schade. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor: 1) digitaal forensisch onderzoek (inclusief loganalyse, malware-onderzoek en vaststelling van de oorzaak en impact); 2) mitigatie- en herstelmaatregelen; 3) rapportage: de opdrachtgever ontvangt na afronding van een incident een schriftelijk incidentrapport, inclusief tijdlijn, bevindingen, genomen maatregelen en aanbevelingen.
5.	**Gegevensbeveiliging**

5.1	Alle gegevens moeten beveiligd worden opgeslagen, zowel tijdens transport als wanneer ze zijn opgeslagen. Dat houdt in dat de gegevens encrypted worden opgeslagen of getransporteerd, en niet leesbaar / manipuleerbaar voor anderen zijn. Met de term 'beveiligd worden' bedoelen wij dat de gegevens tijdens zowel opslag als transport op een manier worden beschermd die waarborgt dat deze: **1. Geëncrypt worden opgeslagen en getransporteerd:** -Gegevens dienen minimaal versleuteld te worden met een actuele en algemeen geaccepteerde encryptiestandaard (bijvoorbeeld AES-256 voor opslag en TLS 1.2 of hoger voor transport). -Dit zorgt ervoor dat de gegevens niet toegankelijk of leesbaar zijn voor onbevoegden. **2. Niet leesbaar zijn voor onbevoegden:** **-**Alleen geautoriseerde gebruikers en systemen mogen toegang hebben tot de gegevens, waarbij encryptiesleutels veilig worden beheerd. **3. Niet manipuleerbaar zijn tijdens transport of opslag:** -Maatregelen zoals integriteitscontroles (bijvoorbeeld hashing) moeten worden toegepast om te voorkomen dat gegevens ongeautoriseerd worden gewijzigd of gemanipuleerd. **4. Bescherming tegen ongeautoriseerde toegang:** -Toegang tot gegevens moet worden geregeld via sterke authenticatie en toegangscontrole (bijvoorbeeld multi-factor authenticatie en rolgebaseerde toegangsrechten). **5. Naleving van relevante wet- en regelgeving:** **-**De beveiliging moet voldoen aan geldende wettelijke eisen en richtlijnen, zoals de AVG/GDPR, BIO2, NIS2 en eventueel andere relevante normen zoals ISO 27001.
5.2	De opslag van de applicatie, gegevens en overige onderdelen van de SIEM-oplossing moet fysiek plaatsvinden binnen de Europese Economische Ruimte en bij een hostingpartij/datacenter zonder vestiging in de Verenigde Staten, vanwege de USA Freedom Act. Als alternatief kan de opdrachtnemer garanderen dat de data niet opgevraagd kan worden onder de USA Freedom Act.
5.3	Alle gegevensverwerking vindt plaats binnen de EU/EER; opslag buiten de EU is niet toegestaan.

5.4	Er zijn maatregelen genomen om verlies van incidenten te voorkomen, zelfs bij connectiviteitsproblemen, hacks en denial of service-aanvallen. Logevents mogen tijdens verstoringen niet verloren gaan en moeten worden gebufferd zodat ze later nog zichtbaar zijn.
6.	**Kwaliteitswaarborging**
6.1	Medewerkers van de opdrachtnemer die toegang hebben tot de verzamelde gegevens, zijn gescreend op integriteit. De minimale eis is dat zij bij indiensttreding een voor de functie geldende Verklaring omtrent Gedrag (VOG) hebben overlegd die niet ouder is dan drie maanden.
6.2	De opdrachtnemer moet de privacy en bescherming van de verzamelde gegevens waarborgen in overeenstemming met relevante wet- en regelgeving, zoals de AVG.
6.3	De deelnemer stelt jaarlijks een verklaring van een onafhankelijke nationale of Europese IT-auditor (zoals NOREA, ISACA of vergelijkbaar) beschikbaar waaruit blijkt dat aan de eisen voor informatieveiligheid wordt voldaan. De dienstverlening valt binnen de scope van het managementsysteem voor informatiebeveiliging (ISO 27001 en eventuele vergelijkbare kwaliteitssystemen voor informatiebeveiliging) waarover de opdrachtnemer beschikt. Op verzoek stelt de opdrachtnemer een verklaring van een onafhankelijke derde beschikbaar waaruit blijkt dat de informatieveiligheid van de ICT-oplossing in lijn is met de eisen van de opdrachtgever en dat de maatregelen gedurende het gehele jaar goed hebben gefunctioneerd. Dit kan door middel van verklaringen zoals een SOC 2-rapport, een ISAE 3000-verklaring of een vergelijkbaar document.
6.4	De opdrachtnemer moet een geldig kwaliteitscertificaat kunnen overleggen dat gebaseerd is op de ISO 27001-standaard voor kwaliteitsmanagement.
6.5	De opdrachtnemer moet een geldig kwaliteitscertificaat kunnen overleggen dat gebaseerd is op de ISO 9001-standaard voor kwaliteitsmanagement.

6.6	De opdrachtnemer garandeert dat hij en eventuele door hem ingeschakelde derden voldoen en blijven voldoen aan alle wettelijke bepalingen en voorschriften, en dat zij beschikken en blijven beschikken over alle vereiste vergunningen, beschikkingen en verklaringen voor de dienstverlening en het ondernemerschap.
6.7	Opdrachtnemer dient voor het rechtmatig uitvoeren van forensisch onderzoek naar persoonsgegevens te beschikken over een geldige POB-vergunning op grond van de Wpbr.
7.	**Notificatie**
7.1	De dienst moet notificaties voor meldingen via telefoon en e-mail kunnen leveren.
7.2	Opdrachtgever en opdrachtnemer moeten specifieke afspraken kunnen maken over de situaties waarin notificaties volgen en hoe deze worden verzonden.
7.3	Bij een telefonische notificatie moeten meerdere personen gebeld kunnen worden via een bel-lijst.
7.4	Bij een incident moet de dienst automatisch een melding kunnen maken in het incidentmanagementsysteem (Topdesk) van de opdrachtgever.
8.	**Rapportage**
8.1	De opdrachtnemer biedt rapportagefunctionaliteit of richt dit in binnen de Microsoft Sentinel installatie van de opdrachtgever.
8.2	Opdrachtnemer is bereid en in staat om eens per kwartaal, 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

8.3	Rapportages bieden ondersteuning bij het afleggen van verantwoording over de van toepassing zijnde normenkaders BIO2 en NIS2 en relevante opvolgers.
9.1	**Retentie**
9.1	De oplossing biedt de mogelijkheid om delen van de log- en eventdata te bevriezen, zodat deze data bewaard blijft totdat de bevriezing wordt opgeheven. Deze data moet bewaard kunnen worden zo lang als noodzakelijk is voor de afhandeling van een incident en ook voor de afhandeling van eventuele claims in vervolg op het incident.
9.2	De opdrachtgever moet zelf, binnen de wettelijke mogelijkheden, de retentietijden van opgeslagen data kunnen bepalen en naar eigen keuze kunnen verlengen of verkorten.
9.3	De minimale bewaartermijn van log- en eventdata die gerelateerd is aan een alert is drie jaar, tenzij de wetgeving een langere bewaartermijn vereist.
9.4	De minimale bewaartermijn voor log- en eventdata die niet hebben geleid tot een alert is zes maanden.
9.5	De minimale bewaartermijn van auditlogdata is drie jaar, tenzij de wetgeving een langere bewaartermijn vereist.
10.	**Retransitie en beëindiging**
10.1	Bij het eerste verzoek stelt de opdrachtnemer binnen 10 werkdagen een gedetailleerd exitplan op, conform de GIBIT artikel 5.3.
10.2	De opdrachtnemer ondersteunt kosteloos de eventuele migratie naar een nieuwe dienstverlener met een exitplan. Daarbij committeert de opdrachtnemer zich aan exit-neutraliteit: geen lock-in, geen commerciële drempels en volledige overdraagbaarheid van data, configuraties en use-cases. Dit is inclusief volledige overdraagbaarheid van data, configuraties, documentatie en kennisoverdracht om continuïteit bij opvolging te waarborgen.

10.3	Er wordt een exit-plan opgesteld en afgestemd binnen 3 maanden na de afronding van de implementatie van de SIEM/SOC dienstverlening. Bij beëindiging van de overeenkomst draagt de opdrachtnemer alle relevante data, configuraties en documentatie over aan de opdrachtgever. De opdrachtnemer garandeert volledige verwijdering van data van de opdrachtgever uit zijn systemen na overdracht.
10.4	Tijdens de periode van retransitie moet de opdrachtnemer alle dienstverlening voortzetten volgens de overeengekomen voorwaarden.
10.5	De opdrachtnemer zal aan het einde van de overeenkomst of de retransitie alle vertrouwelijke informatie retourneren zonder een kopie te behouden, tenzij anders overeengekomen op basis van een (wettelijke) eis of verplichting, of aanvullende afspraken. Als het langer bewaren van een kopie van vertrouwelijke informatie verplicht is, zal deze informatie worden vernietigd zodra de bewaartermijn is verstreken.
11.	**Contract en SLA**
11.1	De opdrachtnemer bespreekt de beheeractiviteiten periodiek (4 x per jaar) met de opdrachtgever en draagt verbetervoorstellen voor.
11.2	Indien de opdrachtnemer werkt met onderaannemers, is hij verantwoordelijk voor het naleven van de contract- en SLA-afspraken door deze onderaannemers, zoals opgesteld tussen de opdrachtgever en opdrachtnemer.
11.3	Om de afgesproken kwaliteit te waarborgen, de dienstenniveaus te realiseren en verbeteringen door te voeren, is regelmatig overleg op verschillende organisatieniveaus noodzakelijk. De periodieke rapportages, zoals vermeld in ~~eis 9.3~~ eis 8.2 in deze bijlage, maken hier deel van uit. De opdrachtnemer moet uitleggen hoe de communicatie met de opdrachtgever wordt georganiseerd, inclusief frequentie, onderwerpen en betrokken niveaus. Daarnaast vindt er jaarlijks een evaluatie plaats, die zowel de communicatie als de naleving van de SLA betreft.

11.4	Patchmanagement wordt procesmatig en procedureel uitgevoerd, ondersteund door richtlijnen, zodat de laatste (beveiligings)patches tijdig in de oplossing worden geïnstalleerd. Deze eis heeft uitsluitend betrekking op de systemen, tooling en infrastructuur die de opdrachtnemer inzet of beschikbaar stelt voor het leveren van de dienstverlening.
11.5	De opdrachtnemer biedt een deskundige Nederlandstalige helpdesk aan voor zowel technische als functionele ondersteuning. Deze helpdesk is bereikbaar via telefoon, e-mail en/of een webportaal. De helpdesk fungeert als centraal punt voor het melden van incidenten, het stellen van vragen, en het indienen van wijzigingsvoorstellen. Tevens verstrekt de helpdesk informatie en inzicht in de voortgang en afhandeling van deze meldingen.
11.6	Het SOC is 24/7 bemand. Er is minimaal één SOC-analist stand-by om in het geval van een vermoedde inbreuk een triage/analyse uit te voeren en waar nodig een melding te doen bij de opdrachtgever.
11.7	De Service Level Agreement (SLA) vormt de basis voor deze samenwerking. De SLA omvat duidelijke afspraken, prestatie-indicatoren en kwaliteitseisen met betrekking tot de oplossing en de bijbehorende dienstverlening. ~~De definitieve SLA wordt vastgesteld bij gunning en overeengekomen tussen de opdrachtnemer en de opdrachtgever. Een concept/voorbeeld aanleveren als bijlage aan uw inschrijving is een vereiste~~. De definitieve SLA wordt, in samenspraak, na definitieve gunning vastgesteld. Bij voorlopige gunning wordt, door de voorlopig gegunde partij een concept/voorbeeld SLA aangeleverd.
11.8	De opdrachtnemer kwalificeert als verwerker voor deze opdracht. Als onderdeel van de overeenkomst zullen opdrachtgever en opdrachtnemer een verwerkersovereenkomst sluiten, conform de bijlage 9 bij de leidraad.
11.9	Minimale beschikbaarheid van de SIEM/SOC-dienst is 99,9% gemeten over 1 maand (+/- 44 minuten) voor alle onderdelen, exclusief de Microsoft Sentinel infrastructuur en de infrastructuur van de opdrachtgever.
11.10	Incidenten worden binnen vooraf vastgestelde tijd afgehandeld afhankelijk van ernstniveau (P1, P2, P3) zoals beschreven in de SLA
12.	**Architectuur en documentatie**

12.1	Na definitieve gunning en vóór de start van het implementatietraject levert de opdrachtnemer een informatiearchitectuur en technisch ontwerp aan. Dit ontwerp, gepresenteerd in ArchiMate of Microsoft Visio, brengt de nieuwe situatie in kaart en beschrijft de voorzieningen, koppelingen en afhankelijkheden met andere informatievoorzieningen.
12.2	~~Bij inschrijving~~ Bij voorlopige gunning geeft de ~~opdrachtnemer~~ voorlopig gegunde partij aan welke minimale vereisten de opdrachtgever moet voldoen om de SIEM oplossing te realiseren. Dit omvat vereisten zoals bandbreedte van de internetsnelheid, benodigde poorten, firewallinstellingen, systeemeisen voor servers en cliëntsystemen, enzovoort.
13.	**Financieel**
13.1	Facturen dienen bij voorkeur als e-factuur (overeenkomstig de eisen voor facturatie zoals opgenomen in de gemeentelijke ICT-kwaliteitsnormen) ingediend te worden Peppol-netwerk (OIN 00000001809249066000). Als opdrachtnemer niet in staat is om e-facturen)op de voorgeschreven wijze) te versturen, mogen facturen als Pdf-bestand per email verzonden worden naar: crediteurenadministratie@steenwijkerland.nl.
13.2	Betaling van de implementatiekosten vindt plaats op factuur binnen 30 dagen na ontvangst van de factuur, na ontvangst en volledige goedkeuring van de overeengekomen zaken door de opdrachtnemer.
13.3	Betaling van de exploitatiekosten vindt plaats per maand achteraf binnen 30 dagen na ontvangst van de factuur op verzamelnota voorzien van een specificatie.
13.4	Het is opdrachtnemer toegestaan geoffreerde prijzen zoals ingediend bij inschrijving en vastgelegd in het prijzenblad te indexeringen conform artikel 3.2. van de concept overeenkomst (Bijlage 6).