Nota van Inlichtingen 4: 'SIEM SOC'
Referentie: IBMN-2026-VIJ-CM-001
Gemeente Vijfheerenlanden
Datum: donderdag 19 november 2026

Mededelingen aanbestedende dienst:

1) In verband met enkele wijzigingen (o.a. kerncompetentie(s) en implementatiebudget) wijzigt de planning voor deze aanbesteding en is een extra Nota van Inlichtingen toegevoegd. De nieuwe planning is als volgt:

Vrijgave (huidige) Nota van Inlichtingen: Donderdag 19 november 2026
Stellen vragen extra inlichtingenronde: **Maandag 7 december 2026 uiterlijk 11:00 uur**
Vrijgave extra Nota van Inlichtingen: Donderdag 17 december 2026
Datum en tijd ontvangst inschrijvingen: **Dinsdag 5 januari 2027 uiterlijk 11:00 uur**
Beoordeling: Aansluitend
Demonstraties: **Maandag 18 januari 2027 en/of dinsdag 19 januari 2027 tussen 10:00 en 16:00 uur.**
Voornemen tot gunning: Verwacht week 5 / 6 – 2027
Contractafstemming en ondertekening: Verwacht week 8 / 9 – 2027
Implementatieperiode: Start zo snel mogelijk aansluitend
Ingangsdatum Overeenkomst / systeem operationeel: Donderdag 1 april 2027

2) De kerncompetenties worden als volgt aangepast:

Om in aanmerking te (kunnen) komen voor gunning van de Opdracht, dient een Inschrijver te beschikken over aantoonbare ervaring met de uitvoering én oplevering (Kerncompetenties 1 en 2) van tenminste één (1) 'opdracht' (per kerncompetentie) in de afgelopen drie (3) jaar (voorafgaande aan datum inschrijving) die betrekking heeft (had) op:

Kerncompetentie 1

het opzetten en het beheren van een SIEM-oplossing, op basis van Microsoft Sentinel, voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers.

Kerncompetentie 2

het leveren van SOC-diensten voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers.

Concreet: 24x7 uur reageren op alarmen uit een SIEM door event classificatie, triage en analyse en (mogelijk geautomatiseerd) actie te ondernemen ten behoeve van isolatie en eerste herstel. SOC-werkzaamheden vinden primair plaats in een eigen SOC van opdrachtnemer (niet via een derde partij). Indien werkzaamheden buiten de primaire SOC-locatie worden uitgevoerd, bijvoorbeeld in het kader van consignatie-, bereikbaarheids- of piketdiensten, dient de inschrijver aan te tonen welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen.

De inschrijver dient aantoonbaar ervaring te hebben met:
- Monitoring, detectie, analyse en afhandeling van beveiligingsincidenten;
- Logging en audit-trails ten behoeve van compliance en verantwoording;
- Uitvoeren van root-cause analyses met betrekking tot de gemelde incidenten;
- Advisering over informatiebeveiligingsmaatregelen;

3) SentinelOne vervangt Microsoft Defender for Servers, is de verplichte initiële serverlogbron en telt mee in de beoordelingsprijs. Microsoft Defender for Servers is uitsluitend een optie zonder afnameverplichting en telt niet mee in de beoordelingsprijs.

4) Het implementatiebudget wordt verhoogd naar max. € 30.000,- (excl BTW) (was € 15.000,- excl BTW)

Vraag	Verwijzing	Vraag	Antwoord
1	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 20, 21 en 24 t/m 27; Nvl 2 antw. 121 en 204	Eenheid 'per Gb' – periode en meetmethode. In het gewijzigde Prijzenblad hebben Cisco Meraki (200), Barracuda (100), DNS (1000), DHCP (50), SecureMe2 NIDS (10) en Holm Security (10) de eenheid 'per Gb'. De kolom F heet 'Kosten / jaar'. In antwoord 121 geeft de aanbestedende dienst aan dat er geen gegevens zijn over logvolumes. Vraag: Gaat het bij de genoemde aantallen om het totale ingestvolume in Gb per jaar, of om Gb per dag of per maand? Op welke wijze en met welke bron wordt het werkelijke volume tijdens de looptijd gemeten (bijvoorbeeld de Usage-tabel in Microsoft Sentinel)?	De aantallen bij de eenheid 'per Gb' betreffen het volume in gigabyte (GB) per contractjaar per logbron. Deze aantallen zijn indicatief en worden uitsluitend gebruikt voor de beoordeling en vergelijkbaarheid van de inschrijvingen; er kunnen geen rechten aan worden ontleend. De prijs per GB betreft uitsluitend de vergoeding die Opdrachtnemer zelf rekent voor zijn eigen dienstverlening op de data van de betreffende logbron, zoals verwerking, analyse, correlatie en monitoring door het SOC. De prijs per GB betreft uitdrukkelijk níet de kosten voor opslag, ingestie of retentie in Microsoft Sentinel/Log Analytics; die kosten worden rechtstreeks door Opdrachtgever aan Microsoft betaald en worden niet in het Prijzenblad opgenomen (zie ook de antwoorden 13, 30 en 42 in Nota van Inlichtingen 2). Voor GB is gekozen omdat dit voor deze logbronnen de enige bruikbare meeteenheid is. Tijdens de looptijd wordt het werkelijke volume per logbron vastgesteld aan de hand van het in Microsoft Sentinel geregistreerde ingestvolume (de Usage-tabel van de Log Analytics-workspace). Verrekening vindt plaats tegen de aangeboden, bindende prijs per GB. In het gewijzigde Prijzenblad (bijlage 1) bij deze Nota van Inlichtingen is de eenheid verduidelijkt tot 'per GB' en in kolom D prijs per eenheid per jaar (dienstverlening Opdrachtnemer, excl. Microsoft-kosten)'.
2	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 20–27; Nvl 2 antw. 47 en 204	Gb-regels en beoordelingsprijs. In antwoord 204 staat: 'Uitsluitend componenten die op deze eenheden (gebruikers, endpoints en servers) zijn gebaseerd, tellen mee in de beoordelingsprijs. Hanteert Inschrijver een andere eenheid, dan wordt die component niet beoordeeld.' De Gb-regels 20, 21 en 24 t/m 27 worden in de formule van F37/F40 echter wel opgeteld. Vraag: Kan de aanbestedende dienst bevestigen dat de door de aanbestedende dienst zelf voorgeschreven Gb-regels volledig meetellen in de beoordelingsprijs? Kan zij ook bevestigen dat de prijs per Gb uitsluitend de SOC-dienstverlening van Opdrachtnemer betreft, en niet de ingest- en retentiekosten van Microsoft Sentinel, die volgens antwoord 47 rechtstreeks door de gemeente worden gedragen?	Ja. Alle prijsregels van de initiële scope in het Prijzenblad (regels 14 tot en met 30), inclusief de door Aanbestedende Dienst voorgeschreven regels met de eenheid 'per Gb', tellen volledig mee in de beoordelingsprijs (F37 en F40). Het antwoord op vraag 204 in Nota van Inlichtingen 2 wordt hierbij gecorrigeerd: de zinnen 'Uitsluitend componenten die op deze eenheden zijn gebaseerd, tellen mee in de beoordelingsprijs. Hanteert Inschrijver een andere eenheid, dan wordt die component niet beoordeeld.' vervallen. Aanbestedende Dienst bevestigt tevens dat de prijs per GB uitsluitend de eigen dienstverlening van Opdrachtnemer betreft en niet de ingest- en retentiekosten van Microsoft Sentinel, die rechtstreeks door Opdrachtgever worden gedragen (zie het antwoord op vraag 1).
3	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 14 t/m 17, 22 en 23	Aantallen gebruikers versus accounts. Voor Entra ID, Cisco Duo, HelloID, M365 Audit Logs en Exchange Online Audit Logs wordt gerekend met 680 gebruikers. Voor Microsoft Active Directory wordt gerekend met 799 accounts. Vraag: Welke accounts zijn in de 799 AD-accounts begrepen (bijvoorbeeld service-, beheer-, functionele, gedeelde of uitgeschakelde accounts)? Welke definitie van 'gebruiker' respectievelijk 'account' geldt bij wijziging van aantallen tijdens de looptijd? Mag een inschrijver een 'account' anders beprijzen dan een 'gebruiker', terwijl het in veel gevallen om dezelfde identiteit gaat?	De 799 accounts in Microsoft Active Directory betreffen alle actieve (ingeschakelde) accounts, dus naast de accounts van medewerkers ook service-, beheer-, functionele en gedeelde accounts. Uitgeschakelde accounts zijn niet meegeteld. De 680 gebruikers betreffen de actieve medewerkers (natuurlijke personen) die gebruikmaken van de Microsoft-omgeving. Tijdens de looptijd gelden dezelfde definities: 'gebruiker' is een actieve medewerker (natuurlijk persoon); 'account' is een actief, ingeschakeld account in Active Directory. Uitgeschakelde accounts tellen niet mee. Bij wijziging van aantallen gelden de aangeboden, bindende prijzen per eenheid (zie het antwoord op vraag 193 in Nota van Inlichtingen 2). Inschrijver is vrij om per prijsregel een eigen tarief te hanteren; een 'account' mag dus anders worden beprijsd dan een 'gebruiker'. Aanbestedende Dienst geeft Inschrijver wel in overweging om te voorkomen dat voor dezelfde identiteit binnen het Microsoft-ecosysteem meerdere keren wordt gerekend. Indien de dienstverlening voor een identiteit al in een andere prijsregel is verdisconteerd, mag Inschrijver in de betreffende regel € 0,00 invullen en dit toelichten in de kostentoelichting (zie het antwoord op vraag 206 in Nota van Inlichtingen 2).

4	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 18, 19 en 49	Endpoints, servers en Defender for Servers. MDE wordt geprijsd per endpoint (658) en SentinelOne per server/vm (106). Daarnaast is 'Microsoft Defender for Servers' opgenomen als dienst zonder afnameverplichting (regel 49). Vraag: Kan de aanbestedende dienst bevestigen dat de 658 endpoints uitsluitend werkplekken/clients betreffen en geen servers bevatten, zodat er geen overlap is met de 106 servers/vm's? Wat is bij regel 49 de bedoelde eenheid en het aantal (per server, gelijk aan de 106 servers)?	Ja. De 658 endpoints (regel 18, Microsoft Defender for Endpoint) betreffen uitsluitend werkplekken (laptops en desktops). Hierin zijn geen servers en geen mobiele devices opgenomen. Er is dus geen overlap met de 100 servers/vm's in regel 19. Voor de duidelijkheid: in het oude prijzenblad stond 106, maar dit is aangepast naar het correcte aantal van 100 servers/vm's. De servers van Opdrachtgever worden op dit moment beveiligd met SentinelOne. SentinelOne voor Servers (regel 19) is daarom de verplichte serverlogbron binnen de initiële scope en vervangt Microsoft Defender for Servers als logbron in eis 2.2 (zie het antwoord op vraag 11). Regel 49 'Microsoft Defender for Servers' onder 'Scope zonder afnameverplichting' betreft een mogelijke toekomstige overstap van SentinelOne naar Microsoft Defender for Servers. In het gewijzigde Prijzenblad bij deze Nota van Inlichtingen is voor regel 49 de eenheid 'per server/vm' met een aantal van 1 opgenomen. Deze regel telt niet mee in de beoordelingsprijs.
5	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 28, 29, 31 t/m 36; NvI 2 antw. 204	Lege regels en 'overig, namelijk'. De regels 28, 29 en 31 t/m 35 hebben geen omschrijving, eenheid of aantal. Regel 36 'overig, namelijk' heeft de eenheid 'per jaar/eenheid', maar geen aantal. In antwoord 204 wordt verwezen naar de regels 'per jaar/asset' en 'overig, namelijk' voor variabele kosten van maximaal drie eenheden. Vraag: Mag de inschrijver in deze regels zelf een omschrijving, eenheid én aantal invullen? Tellen deze regels mee in de beoordelingsprijs (de formule in F37 telt ze op), of worden ze volgens antwoord 204 buiten beoordeling gelaten wanneer een andere eenheid dan gebruikers, endpoints of servers wordt gehanteerd? Indien ze niet meetellen: hoe wordt dit technisch in het Prijzenblad verwerkt?	Nee. De regels 28, 29 en 31 tot en met 35 zijn uitsluitend witregels die de logbronnen (regels 14 tot en met 27) visueel scheiden van de vaste kosten (regel 30). Zij zijn niet bedoeld om in te vullen. Regel 36 'overig, namelijk' vervalt. In het gewijzigde Prijzenblad bij deze Nota van Inlichtingen zijn de witregels vergrendeld en is regel 36 verwijderd. Inschrijver neemt alle kosten van de initiële scope op in de prijsregels per logbron (regels 14 tot en met 27) of in regel 30 'Vaste kosten SOC Basisdienstverlening'. Al deze regels tellen volledig mee in de beoordelingsprijs (zie het antwoord op vraag 2). De antwoorden op de vragen 82 en 204 in Nota van Inlichtingen 2 worden hierbij gecorrigeerd voor zover daarin wordt verwezen naar de regels 'per jaar/asset' en 'overig, namelijk'. Kosten mogen niet dubbel worden opgenomen: kosten die in regel 30 zijn verwerkt, worden niet ook per logbron in rekening gebracht, en omgekeerd.
6	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regel 57; NvI 2 antw. 192 en 196	Uurtarief additionele dienstverlening. Volgens antwoord 192 telt het uurtarief niet mee in de beoordelingsprijs. Volgens antwoord 196 wordt het aansluiten van aanvullende logbronnen gedurende de looptijd als meerwerk uitgevoerd op basis van dit uurtarief. Het uurtarief is daarmee relevant voor de totale kosten, maar niet onderscheidend in de beoordeling. Vraag: Hanteert de aanbestedende dienst een maximum uurtarief, of een toets op abnormaal hoge tarieven? Gelden de 40 uur in kolom D uitsluitend als fictief aantal zonder afnameverplichting? Geldt het uurtarief voor alle profielen (analist, engineer, consultant) of mag per profiel een tarief worden opgegeven?	Aanbestedende Dienst hanteert geen maximum uurtarief. Wel geldt §1.20 van het Aanbestedingsdocument: Aanbestedende Dienst behoudt zich het recht voor kennelijk onredelijke, irreële of ongeloofwaardige (eenheids)prijzen, dan wel de betreffende inschrijving, terzijde te leggen. De 40 uur in regel 57 zijn fictief en indicatief. Er is geen afnameverplichting en er kunnen geen rechten aan worden ontleend. Het uurtarief telt niet mee in de beoordelingsprijs (zie het antwoord op vraag 192 in Nota van Inlichtingen 2). Inschrijver geeft één uurtarief op dat geldt voor alle profielen (onder meer analist, engineer en consultant). Dit tarief is bindend en geldt voor meerwerk gedurende de looptijd, waaronder het aansluiten van aanvullende logbronnen (zie het antwoord op vraag 196 in Nota van Inlichtingen 2).
7	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 43–51; NvI 2 antw. 46 en 66	Prijsregel extra use-case. In het antwoord op vraag 66 (en antwoord 46) wordt verwezen naar een prijscomponent in Bijlage F1 voor het 'Opnemen extra use case op wens van de klant'. Deze regel komt in het gewijzigde Prijzenblad niet (meer) voor. Regel 47 betreft nu 'Low interaction Honeypots'. Vraag: Wordt deze prijsregel alsnog toegevoegd aan het Prijzenblad onder 'Scope zonder afnameverplichting'? Of moeten aanvullende use-cases worden geprijsd via het uurtarief in regel 57? Zo ja, kan de aanbestedende dienst dit bevestigen?	Nee, de prijsregel 'Opnemen extra use case op wens van de klant' wordt niet opnieuw aan het Prijzenblad toegevoegd. Aanvullende use-cases verschillen sterk in aard en omvang en laten zich daardoor niet in één vaste prijs vangen. Aanbestedende Dienst bevestigt dat aanvullende use-cases, die buiten de vijf initiële use-cases (eis 2.1) en de passende aanvullende use-cases voor de logbronnen uit eis 2.2 vallen, gedurende de looptijd als meerwerk worden uitgevoerd conform eis 5.10. Opdrachtnemer doet hiervoor vooraf een voorstel op basis van het uurtarief in regel 57 van het Prijzenblad (zie ook het antwoord op vraag 6). De verwijzingen naar deze prijsregel in de antwoorden op de vragen 46 en 66 in Nota van Inlichtingen 2 worden hierbij in die zin gecorrigeerd.
8	Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regel 51; PvE eis 2.20; NvI 2 antw. 81 en 197	Servicevenster en piketdienst versus 'eyes on screen'. Uit de antwoorden 81 en 197 volgt dat 24/7 detectie, triage, analyse en escalatie onderdeel zijn van de basisdienstverlening. 'Eyes on screen' (regel 51) is een optionele meerprijs ten opzichte van een piketdienst. Vraag: Kan de aanbestedende dienst bevestigen dat de basisdienstverlening buiten kantoortijden mag worden ingevuld met geautomatiseerde monitoring en een piketdienst, mits de normen voor P1 en P2 worden gehaald? Welk servicevenster (dagen en tijden) hanteert de aanbestedende dienst voor P3- en P4-meldingen?	Ja. Aanbestedende Dienst bevestigt dat de basisdienstverlening buiten kantoortijden mag worden ingevuld met geautomatiseerde monitoring in combinatie met een 24/7 bereikbare piketdienst, mits aantoonbaar aan de kwaliteitseisen en de termijnen voor P1- en P2-meldingen wordt voldaan (zie de antwoorden op de vragen 20, 81 en 140 in Nota van Inlichtingen 2). 'Eyes on screen' (regel 51) blijft een optionele meerprijs zonder afnameverplichting. Voor P3- en P4-meldingen gelden de reactie- en escalatietermijnen uit SLA8, binnen het servicevenster op werkdagen van 08:00 tot 18:00 uur. Buiten dit venster lopen deze termijnen niet door; zij worden voortgezet bij aanvang van het eerstvolgende servicevenster. Voor P1- en P2-meldingen gelden de termijnen onverkort 24/7.

9	NvI 2 antw. 28; GIBIT 2025 art. 11.8; Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regel 40	Indexering. In de Nota van Inlichtingen is aangegeven dat indexering vanaf 1 januari 2028 mogelijk is. De beoordelingsprijs gaat uit van negen maal de (ongeïndexeerde) jaarlijkse kosten. Vraag: Welk indexcijfer wordt gehanteerd (bijvoorbeeld de CBS-index cao-lonen of de DPI) en met welke peilmaand? Is de indexering ook van toepassing op de bindende prijzen per eenheid, het uurtarief en de prijzen van de diensten zonder afnameverplichting?	Aanbestedende dienst bevestigt dat voor indexering artikel 11.8 GIBIT 2025 van toepassing is. Dit betekent dat indexering voor het eerst per 1 januari 2028 kan plaatsvinden. De indexering is gemaximeerd overeenkomstig het op het moment van aankondiging laatst door het CBS gepubliceerde definitieve prijsindexcijfer dienstenprijzen commerciële dienstverlening en transport (index 2021=100), groep J6202, over het gehele jaar in vergelijking met het prijsindexcijfer van het jaar daarvoor van diezelfde index. Er wordt derhalve geen afzonderlijke peilmaand gehanteerd. De indexeringsregeling is van toepassing op de overeengekomen (jaar)tarieven en doorlopende vergoedingen als bedoeld in artikel 11.8 GIBIT 2025, waaronder de bindende eenheidsprijzen en uurtarieven, voor zover deze gedurende de looptijd worden toegepast. Dit geldt eveneens voor de prijzen van diensten zonder afnameverplichting, voor zover deze diensten gedurende de looptijd worden afgenomen. Voor de beoordeling van de inschrijvingen wordt geen rekening gehouden met toekomstige indexering. De beoordelingsprijs wordt berekend op basis van de in Bijlage F1 opgenomen ongeïndexeerde prijzen en de in het aanbestedingsdocument opgenomen berekeningswijze.
10	Aanbestedingsdocument §6.6; Bijlage J Uitvoeringsprotocol Social Return; NvI 2 antwoord op onze vraag 5	Social return – invulling buiten de AV-regio (vervolgvraag). In de Nota van Inlichtingen is bevestigd dat de grondslag de totale opdrachtwaarde over 9 jaar is en dat de invulling na gunning met het Adviespunt Social Return wordt afgestemd. Het tweede deel van onze vraag is echter niet beantwoord. Vraag: Accepteert de aanbestedende dienst dat Opdrachtnemer, die buiten de AV-regio is gevestigd, de social return-verplichting (geheel of gedeeltelijk) invult in de eigen regio, mits dit binnen de kaders van het Uitvoeringsprotocol Social Return gebeurt? Zo nee, welk deel moet minimaal binnen de AV-regio worden gerealiseerd?	De Aanbestedende dienst verduidelijkt het antwoord op vraag 5 van Nota van Inlichtingen 2 als volgt. Invulling van de Social Return-verplichting buiten de AV-regio is niet op voorhand uitgesloten. De concrete invulling van de Social Return-verplichting wordt na gunning door Opdrachtnemer afgestemd met het Adviespunt Social Return en dient te passen binnen de kaders van het Uitvoeringsprotocol Social Return. De Aanbestedende dienst schrijft geen afzonderlijk minimumpercentage voor dat binnen de AV-regio moet worden gerealiseerd. Een eventuele invulling geheel of gedeeltelijk buiten de AV-regio is echter niet automatisch toegestaan, maar dient vooraf te worden afgestemd en akkoord bevonden in het kader van de uitvoering van de Social Return-verplichting.
11	Bijlage A – Programma van Eisen, eis 2.2; Gewijzigde Bijlage F1 – Prijzenblad dd 30-10-2026, regels 19 en 49; NvI 2 antw. 30, 44 en 142	SentinelOne versus Microsoft Defender for Servers. In PvE eis 2.2 en NvI 2 antwoord 44 is Microsoft Defender for Servers een verplichte logbron binnen de initiële scope. In het gewijzigde Prijzenblad is in regel 19 echter 'SentinelOne voor Servers' (106 servers/vm) opgenomen en is Defender for Servers verplaatst naar 'Scope zonder afnameverplichting' (regel 49). Vraag: Kan de aanbestedende dienst bevestigen dat de servers op dit moment met SentinelOne worden beveiligd en dat SentinelOne in de initiële scope Defender for Servers als logbron vervangt? Wordt eis 2.2 hierop aangepast? Welk SentinelOne-product en welke licentie (bijv. Singularity Complete/Control) wordt gebruikt, en is de benodigde API-toegang voor koppeling met Microsoft Sentinel aanwezig? Is de inzet van Defender for Servers (regel 49) bedoeld als toekomstige vervanging van SentinelOne?	Ja. De servers van Opdrachtgever worden op dit moment beveiligd met SentinelOne. SentinelOne voor Servers (regel 19, 100 servers/vm's) vervangt Microsoft Defender for Servers als verplichte logbron in de initiële scope. Eis 2.2 wordt hierbij gewijzigd: in de opsomming van logbronnen wordt 'Microsoft Defender for Servers' vervangen door 'SentinelOne (servers)'. Het antwoord op vraag 44 in Nota van Inlichtingen 2 (alle veertien logbronnen behoren tot de initiële scope) geldt onverkort, met SentinelOne in plaats van Defender for Servers. SentinelOne wordt door Opdrachtgever zelf beheerd. Het gebruikte SentinelOne-product is SentinelOne Singularity Control Cloud Workload. Opdrachtgever verleent de voor de koppeling benodigde medewerking en toegang, overeenkomstig eis 3.5. Regel 49 'Microsoft Defender for Servers' is opgenomen als mogelijke toekomstige vervanging van SentinelOne. Een dergelijke overstap is binnen de eerstkomende twaalf maanden niet voorzien. Afname gebeurt uitsluitend na afzonderlijke opdracht van Opdrachtgever (zie ook het antwoord op vraag 4).
12	PvE 5.1; AD § 1.1.3, § 5.1.2; Prijzenblad F1 r.40	PvE 5.1 spreekt van een ‘initiële contractduur van vier jaar’, terwijl het Aanbestedingsdocument een vaste looptijd van drie jaar na implementatie noemt en het Prijzenblad rekent met implementatiekosten + 9 × jaarlijkse kosten. Kunt u bevestigen dat de vaste looptijd drie jaar bedraagt en dat de beoordeelde totaalprijs uitgaat van negen jaar?	Ja. Aanbestedende dienst verwijst naar de beantwoording van vragen 27, 39, 40 en 159 van Nota van Inlichtingen 2 d.d. 30 oktober 2026. Zoals daarin reeds is verduidelijkt, betreft de vermelding van een initiële contractduur van vier jaar in PvE 5.1 een verschrijving. De overeenkomst kent, na de implementatieperiode, een vaste looptijd van drie (3) jaar, met vervolgens drie (3) optionele verlengingen van telkens twee (2) jaar. De maximale looptijd bedraagt daarmee negen (9) jaar. Voor de berekening van de beoordelingsprijs verwijst Aanbestedende dienst tevens naar vraag 192 van voornoemde Nota van Inlichtingen. De beoordelingsprijs bestaat uit de eenmalige kosten voor ontwerp en implementatie plus negen (9) maal de jaarlijkse kosten, overeenkomstig het gewijzigde Prijzenblad F1 dat als bijlage 1 bij deze Nota van Inlichtingen is toegevoegd.
13	AD § 1.16; PvE 3.3	Tussen de verwachte contractondertekening (week 4/5 – 2027) en de ingangsdatum 1 maart 2027 liggen circa vier tot vijf weken. Staat de gemeente toe dat de intake en voorbereidende werkzaamheden direct na het definitief worden van de gunning starten, en kan de gemeente bevestigen welke logbronnen zij als ‘essentieel’ beschouwt voor oplevering op 1 maart 2027?	Direct na het voornemen tot gunnen is er een periode van "standstill" van toepassing waarin geen werkzaamheden mogen worden verricht. De dag na het einde van de standstill termijn kan de overeenkomst getekend worden, waarmee de gunning definitief is en direct met het werk gestart kan worden. Ten aanzien van de essentiële logbronnen: alle veertien in eis 2.2 genoemde logbronnen (met SentinelOne in plaats van Microsoft Defender for Servers, zie het antwoord op vraag 11) zijn onderdeel van de initiële scope en moeten bij de initiële oplevering zijn aangesloten, getest, operationeel en geaccepteerd. Gefaseerde aansluiting ná ingebruikname voldoet niet (zie het antwoord op vraag 44 in Nota van Inlichtingen 2). De beoogde opleveringsdatum is uitgesteld naar 1 April 2027.

14	A1 SLA26 (Boeteclausule)	Kunt u verduidelijken waarop ‘twee of meer per maand’ betrekking heeft (aantal overschrijdingen van de servicenorm per prioriteit, of aantal incidenten van die prioriteit)? Hoe verhoudt de boete zich tot de normpercentages van 95% in PvE 8.13 en 8.14, is er een maximum per maand bij samenloop van categorieën, en betreft ‘maandelijkse kosten’ de maandelijkse vergoeding exclusief Azure-verbruik?	De eisen 8.13 en 8.14 uit het PvE worden als volgt aangepast: 8.13 - Opdrachtnemer meldt als beveiligingsincident geclassificeerde meldingen binnen de voor de betreffende prioriteit geldende meldtijd aan Opdrachtgever. 8.14 - Opdrachtnemer levert binnen de overeengekomen termijn een eerste bruikbare analyse en advies over de noodzakelijke vervolg- of mitigerende maatregelen. Definitieve oplossing van het incident kan afhankelijk zijn van Opdrachtgever of betrokken derden en valt daarom niet zonder meer onder deze norm. ‘Maandelijkse kosten’ is de maandelijkse vergoeding die Opdrachtnemer voor de SOC-dienstverlening in rekening brengt, exclusief Azure-verbruik en Microsoft-licenties (die Opdrachtgever rechtstreeks aan Microsoft betaalt) en exclusief de eenmalige implementatievergoeding.
15	A1 DIV31; A1 SLA 1.2 (Archiefwet)	A1 DIV31 vereist dat logdata in de SIEM en rapportagedata in de SOC-omgeving na maximaal één jaar worden vernietigd. Geldt dit ook voor incidentdossiers en auditlogging die nodig zijn voor forensisch onderzoek, verantwoording of archiefwettelijke verplichtingen, en wie besluit over langere bewaring bij een lopend onderzoek?	DIV31 (vernietiging uiterlijk één jaar na vastlegging) geldt voor logdata in de SIEM-oplossing en rapportagedata in de SOC-omgeving. Voor incidentdossiers en auditlogging is ditzelfde termijn bedoeld, met inachtneming van wettelijke bewaarplichten, waaronder de Archiefwet. Bij een lopend onderzoek of een wettelijke bewaarplicht besluit Opdrachtgever schriftelijk over langere bewaring, met vermelding van de reden en de uiterste bewaardatum.
16	A1 TECH25	A1 TECH25 vraagt een app voor Android, iPhone of iPad. Volstaat toegang via een responsive webportaal en de Microsoft-apps (bijv. Microsoft Defender/Azure-app) met MFA, of verwacht de gemeente een specifieke native app van de opdrachtnemer?	Eis TECH25 is vervallen (zie het antwoord op vraag 37 in Nota van Inlichtingen 2). Een specifieke native app wordt niet verlangd. De toegangseisen uit de eisen 2.7 en 2.25 van het Programma van Eisen blijven onverkort van toepassing: tijd- en plaatsonafhankelijke toegang via een beveiligde verbinding met multifactorauthenticatie.
17	PvE 1.4; A1 TECH13	Welke certificaten of verklaringen accepteert de gemeente als ‘gelijkwaardig’ aan ISO 27001:2022 (PvE 1.4) respectievelijk ‘vergelijkbaar’ aan ISO 20000 (A1 TECH13)? Mag de inschrijver zich hiervoor beroepen op de certificering van een groepsmaatschappij of onderaannemer waarvan de aangeboden dienstverlening onderdeel is van de scope?	Voor zover de vraag betrekking heeft op TECH13 en ISO 20000 verwijst de Aanbestedende dienst naar de eerdere beantwoording, waaronder vraag 3, vraag 37 en vraag 190 van Nota van Inlichtingen 2. TECH13 is vervallen. Een ISO 20000-certificaat of vergelijkbaar wordt derhalve niet verlangd. Voor PvE 1.4 blijft de eis inzake ISO 27001:2022 of gelijkwaardig onverkort van toepassing, zoals reeds bevestigd in het antwoord op vraag 37. Onder gelijkwaardig verstaat de Aanbestedende dienst een aantoonbare borging van informatiebeveiliging die naar aard, reikwijdte en waarborgen ten minste een gelijkwaardig niveau biedt als ISO/IEC 27001:2022. Het is aan de inschrijver om de gelijkwaardigheid met passende bewijsstukken aan te tonen. Voor zover een inschrijver zich hiervoor beroept op een groepsmaatschappij of onderaannemer, dient de betreffende certificering of gelijkwaardige borging daadwerkelijk betrekking te hebben op de organisatie en dienstverlening die voor de uitvoering van deze opdracht worden ingezet en moet de relevante dienstverlening binnen de scope daarvan vallen. Een certificering van een groepsmaatschappij of onderaannemer kan dus niet zonder meer worden beschouwd als certificering van de inschrijver zelf.
18	Prijzenblad F1 r.14–27, kolom ‘Aantal’	Kan de gemeente per logbron de te hanteren eenheid en het aantal opgeven (bijv. aantal gebruikers, endpoints, servers, netwerkapparaten, gemiddeld dagelijks logvolume in GB), zodat alle inschrijvers op dezelfde aantallen inschrijven? Zijn Azure-verbruikskosten (Sentinel/Log Analytics-ingest en retentie) en Microsoft-licenties voor rekening van de gemeente en buiten de inschrijfprijs?	De te hanteren eenheden en aantallen per logbron zijn opgenomen in het Prijzenblad (gebruikers, accounts, endpoints, servers/vm's en GB per jaar); zie het gewijzigde Prijzenblad bij deze Nota van Inlichtingen en de antwoorden op de vragen 1 tot en met 5. Alle inschrijvers rekenen met deze aantallen. Ja. Azure-verbruikskosten (waaronder Microsoft Sentinel/Log Analytics-ingest en -retentie) en Microsoft-licenties zijn voor rekening van Opdrachtgever en vallen buiten de inschrijfprijs (zie de antwoorden op de vragen 13, 30 en 42 in Nota van Inlichtingen 2).
19	Prijzenblad F1 r.28–34	Rijen 28 t/m 34 hebben de eenheid ‘per jaar/asset’ maar geen omschrijving. Mogen inschrijvers hier zelf assetcategorieën invullen (bijv. endpoints, servers), en tellen deze mee in de beoordeelde totaalprijs?	Nee. De regels 28 tot en met 34 (behalve regel 30) zijn witregels en niet bedoeld om in te vullen. Zie het antwoord op vraag 5.
20	PvE 5.6, 5.7; Prijzenblad F1 r.9	Valt de stabilisatieperiode na livegang (PvE 5.6) onder de vaste implementatieprijs van maximaal € 15.000, of mag deze onder de structurele dienstverlening vallen? Is het maximum van € 15.000 exclusief btw?	De stabilisatieperiode na livegang valt onder de vaste implementatieprijs; eis 5.6 noemt 'ondersteuning tijdens de stabilisatieperiode' uitdrukkelijk als onderdeel daarvan. Het maximum voor de implementatievergoeding is verhoogd naar € 30.000 exclusief btw. Reguliere SOC-dienstverlening die vanaf de ingebruikname wordt geleverd, valt onder de periodieke kosten.

21	AD § 4.2 d; PvE 8.1; A1 SLA 1.1	Mag de concept-SLA bestaan uit de standaard SLA van de inschrijver met een klantspecifiek addendum (A1 SLA 1.1), en wordt de concept-SLA beoordeeld of uitsluitend op aanwezigheid gecontroleerd?	Ja. Op grond van eis SLA 1.1 (Bijlage A1) mag de concept-SLA bestaan uit de standaard SLA van Inschrijver, aangevuld met een klantspecifiek addendum, mits het geheel volledig voldoet aan de GIBIT 2025 en de eisen uit de aanbestedingsstukken. Bij tegenstrijdigheid prevaleert het addendum. De concept-SLA wordt niet afzonderlijk beoordeeld of gescoord; zij is een verplicht in te dienen document en wordt op aanwezigheid gecontroleerd (zie het antwoord op vraag 24 in Nota van Inlichtingen 2). De concept-SLA mag geen voorbehouden of afwijkingen van de eisen bevatten.
22	PvE 1.2 en 8.17	PvE 1.2 noemt tien werkdagen en PvE 8.17 vijf werkdagen voor het leveren van bijgewerkte documentatie na een wijziging. Kunt u bevestigen dat de termijn van vijf werkdagen leidend is?	Nee. De termijn van tien werkdagen uit eis 1.2 is leidend. Eis 8.17 wordt hierbij gewijzigd: 'vijf werkdagen' wordt vervangen door 'tien werkdagen'. Deze termijn geldt voor alle technische, functionele en procesmatige documentatie na de implementatie van een relevante wijziging, tenzij de aard of urgentie van de wijziging eerdere oplevering vereist (eis 1.2).
23	PvE 8.18; DAP-praktijk	PvE 8.18 noemt een operationeel overleg per kwartaal. Staat de gemeente open voor een aanvullende maandelijkse service review, of heeft een kwartaalfrequentie de voorkeur?	Het operationeel overleg per kwartaal uit eis 8.18 is een minimum. Aanbestedende Dienst staat open voor een aanvullende maandelijkse service review. Inschrijver mag deze aanbieden; de kosten daarvan zijn inbegrepen in de aangeboden prijzen. De definitieve overlegfrequentie wordt na gunning vastgelegd in het DAP.
24	AD § 1.3, § 4.2	De bijlagen B (UEA), D, F (Inschrijvingsbiljet), G–J (Overeenkomst, GIBIT 2025, Verwerkersovereenkomst, Uitvoeringsprotocol Social Return) zijn niet in alle downloads aanwezig. Kunt u bevestigen dat deze via TenderNed beschikbaar zijn, of deze alsnog publiceren?	Ja. Alle in de aanbestedingsstukken genoemde bijlagen, zijn via TenderNed beschikbaar gesteld en kunnen daar worden gedownload. Waarbij wel wordt opgemerkt dat een bijlage D en G niet apart downloadbaar zijn, maar ter info zijn opgenomen in het aanbestedingsdocument. Aanbestedende dienst ziet daarom geen aanleiding deze documenten opnieuw te publiceren. Indien een inschrijver problemen ondervindt bij het downloaden of raadplegen van de documenten via TenderNed, kan hiervoor contact worden opgenomen met de helpdesk van TenderNed.
25	AD § 5.1.1 D (Demonstratie)	Kunt u de casus of minimale scenario's voor de demonstratie op 7/8 december 2026 vooraf delen, en mag de demonstratie plaatsvinden in een representatieve demo-omgeving van de inschrijver (geen gemeentelijke data)?	Nee. Aanbestedende Dienst deelt vooraf geen casus of minimale scenario's. Conform §5.1.1 van het Aanbestedingsdocument werkt Inschrijver minimaal één use case naar eigen keuze uit; tijdens de demonstratie kan de beoordelingscommissie vragen stellen en aanvullende scenario's voorleggen die aansluiten bij de beoordelingsaspecten van gunningscriterium D (zie de antwoorden op de vragen 77 en 164 in Nota van Inlichtingen 2). Ja, de demonstratie mag plaatsvinden in een representatieve demo-omgeving van Inschrijver met gesimuleerde of geanonimiseerde gegevens, zonder gemeentelijke data (zie het antwoord op vraag 77 in Nota van Inlichtingen 2). Overigens de in de vraag genoemde demonstratiedata zijn inmiddels gewijzigd; zie de planning onder Mededelingen Aanbestedende Dienst.
26	AD § 5.1.1 (paginalimiet)	Tellen voorblad, inhoudsopgave en kop-/voetteksten mee in de maximaal acht A4 voor de gunningscriteria A, B en C, en is het toegestaan tabellen en figuren met een kleinere tekengrootte dan 10 punt op te nemen?	Aanbestedende dienst verwijst naar de beantwoording van vragen 9, 38 en 76 van Nota van Inlichtingen 2. Zoals daar reeds is aangegeven, geldt voor de uitwerking van de gunningscriteria A, B en C gezamenlijk een maximum van acht inhoudelijke A4-pagina's. Voorblad/omslag en inhoudsopgave tellen niet mee. Buiten deze acht A4 mogen uitsluitend de planning en het RACI-model als bijlage worden toegevoegd. Afbeeldingen en figuren die onderdeel vormen van de inhoudelijke uitwerking vallen binnen het maximum van acht A4. Kop- en voetteksten tellen niet afzonderlijk mee voor de paginalimiet. Voor de inhoudelijke uitwerking geldt de voorgeschreven minimale tekengrootte van 10 punt. Het verkleinen van tekst in tabellen of figuren om meer inhoud binnen de maximale paginalimiet te kunnen opnemen, is dus niet toegestaan.
27	PvE 2.6	Geldt de EER-eis van PvE 2.6 ook voor incidentmeldingen per sms/telefonie en voor Microsoft-diensten waarvoor Microsoft zelf de verwerkingslocatie bepaalt (bijv. Microsoft threat intelligence)?	Eis 2.6 ziet op gegevens van Opdrachtgever: log-, telemetrie-, incident- en supportgegevens van Opdrachtgever mogen niet buiten de Europese Economische Ruimte worden verwerkt of opgeslagen, tenzij Opdrachtgever daar vooraf schriftelijk mee instemt. Het ophalen van gegevens uit bronnen buiten de EER naar de omgeving van Opdrachtgever, zoals externe threat-intelligencefeeds, is wel toegestaan. Voor de gemeente is het momenteel niet duidelijk wat de impact is van de genoemde gevraagde afwijkingen.
28	Technisch – PvE 2.2, 2.13 (HelloID, SecureMe2 NIDS, Holm Security)	Welke exportmogelijkheden bieden de huidige omgevingen van HelloID, SecureMe2 NIDS en Holm Security (syslog/CEF, REST-API, webhook, versie en licentievorm), zijn deze cloud- of on-premises afgenomen, en staat de licentie/leverancier API-toegang voor logexport toe? Wie is per product het technisch aanspreekpunt (gemeente of leverancier)?	Holm Security en SecureMe2 NIDS en HelloID bieden een API voor logexport; voor het gebruik daarvan zijn geen aanvullende licenties nodig (zie de antwoorden op de vragen 32 en 143 in Nota van Inlichtingen 2). Opdrachtgever is voor alle genoemde producten het technisch aanspreekpunt en coördineert waar nodig de contacten met de betreffende leveranciers.
29	Technisch – PvE 2.2 (Cisco Duo, Cisco Meraki, Barracuda)	Welke Barracuda-producten zijn in gebruik (bijv. CloudGen Firewall, Email Protection, WAF), en welke Cisco Meraki-componenten (MX, MS, MR) en Cisco Duo-edities? Verloopt externe toegang (VPN) via Meraki, Barracuda of een andere oplossing?	De Barracuda-omgeving betreft twee firewalls; de Cisco Meraki-omgeving bestaat uit dertien appliances (zie het Prijzenblad). Externe toegang (VPN) verloopt via Microsoft RRAS. Specifieke componenten worden pas gedeeld na gunning.

30	Technisch – PvE 2.2 (DNS, DHCP)	Op welk platform draaien DNS en DHCP (bijv. Windows Server, Meraki, Infoblox of anders), on-premises of in Azure, en is DNS-query-logging technisch beschikbaar en toegestaan?	DNS en DHCP draaien op de Active Directory-domeincontrollers van Opdrachtgever (zie het antwoord op vraag 32 in Nota van Inlichtingen 2). DNS-query-logging is technisch beschikbaar en mag worden ingeschakeld. Opdrachtnemer adviseert daarbij over een passende balans tussen detectiewaarde en datavolume (eis 2.22).
31	Technisch – Gunningscriterium B (mobiele endpoints, AD, Entra ID, servers)	Welke infrastructuuraantallen kan de gemeente delen: aantal gebruikers, Windows-werkplekken, mobiele devices, servers (on-premises en Azure), domeincontrollers, AD-forests/domeinen en netwerkcomponenten? Welk platform wordt gebruikt voor beheer van mobiele devices (bijv. Microsoft Intune), en is Defender for Endpoint op mobiele devices uitgerold?	De aantallen gebruikers (680), AD-accounts (799), werkplekken (658) en servers/vm's (100) zijn opgenomen in het Prijzenblad (zie ook de antwoorden op de vragen 3 en 4). Er is sprake van één Active Directory-domein. 3 Domaincontrollers. Mobiele devices worden beheerd met Microsoft Intune; Microsoft Defender for Endpoint is niet uitgerold op mobiele devices.
32	Technisch – PvE 2.16, 2.20; randvoorwaarden Microsoft-licenties	Welke Microsoft-licenties zijn aanwezig (bijv. Microsoft 365 E3/E5, Defender for Endpoint P1/P2, Defender for Servers Plan 1/2, Defender for Identity, Entra ID P1/P2) en zijn Defender for Endpoint/Servers al op alle endpoints en servers onboarded?	M365 E5 licenties 700 stuks, Defender for Endpoint P2 inbegrepen in M365 E5 licenties, Defender for Identity is inbegrepen in de M365 E5 licenties, Defender for Servers geen licenties, Entra ID P2 14 licenties, Defender for Endpoints is onboarded op alle endpoints.
33	Technisch – PvE 2.16, 4.19 (Azure-omgeving)	Beschikt de gemeente al over een Azure-subscription en/of Log Analytics workspace voor Sentinel, in welke Azure-regio, en wordt Azure Arc gebruikt voor on-premises servers? Mag de opdrachtnemer de workspace en Azure-resources inrichten via geautomatiseerde (infrastructure-as-code) uitrol?	Er is op dit moment geen Microsoft Sentinel-omgeving en geen Log Analytics-workspace (zie de antwoorden op de vragen 125 en 141 in Nota van Inlichtingen 2); de inrichting daarvan is onderdeel van de opdracht. Ja, Opdrachtnemer mag de workspace en Azure-resources inrichten via geautomatiseerde uitrol (infrastructure-as-code), mits dit aansluit op de omgeving van Opdrachtgever en de gebruikte code en configuratie worden gedocumenteerd en overdraagbaar zijn (eisen 2.13, 2.23 en 7.6).
34	Technisch – PvE 5.5; Prijzenblad F1 r.14–27 (logvolume)	Is het gemiddelde dagelijkse logvolume (GB/dag) per logbron bekend of kan de gemeente een meting faciliteren? Zo niet, mogen inschrijvers rekenen met eigen kengetallen, mits als aanname in het Prijzenblad vermeld?	Nee, het werkelijke logvolume per logbron is niet bekend en een meting kan vooraf niet worden gefaciliteerd (zie de antwoorden op de vragen 121 en 162 in Nota van Inlichtingen 2). De GB-aantallen in het Prijzenblad zijn schattingen die uitsluitend dienen voor de vergelijkbaarheid van de inschrijvingen; Aanbestedende Dienst vraagt de prijs per GB. Inschrijvers rekenen in het Prijzenblad met de daarin opgenomen aantallen. Eventuele eigen kengetallen en aannames kan Inschrijver toelichten in de kostentoelichting (zie het antwoord op vraag 206 in Nota van Inlichtingen 2), zonder dat deze de aantallen in het Prijzenblad vervangen. Zie ook het antwoord op vraag 1.
35	Technisch – PvE 2.3, 2.5, 3.5 (logcollector)	Kan de gemeente voor bronnen zonder native connector een (Linux-)server of VM beschikbaar stellen als logcollector (on-premises of in Azure), en wie beheert deze: de gemeente, haar IT-dienstverlener of de opdrachtnemer? Welke netwerksegmentatie en firewallprocedures gelden voor het openen van poorten?	Ja. Opdrachtgever stelt waar nodig een virtuele machine beschikbaar als logcollector (zie het antwoord op vraag 32 in Nota van Inlichtingen 2). Uitgangspunt is dat Opdrachtgever het beheer verzorgt tot en met de hypervisor, en dat Opdrachtnemer het beheer verzorgt vanaf de VM, inclusief de installatie en het beheer van het besturingssysteem en de collectorsoftware. De precieze afspraken en beheergrenzen worden tijdens de implementatie vastgesteld en vastgelegd in het DAP en de RACI-matrix. Wijzigingen aan netwerksegmentatie en firewalls (zoals het openen van poorten) worden door Opdrachtgever uitgevoerd op basis van tijdige en volledige instructies van Opdrachtnemer (eis 3.5).
36	Technisch – PvE 2.19, 4.7 (ITSM-koppeling)	Gebruikt de gemeente een eigen ITSM- of meldingensysteem (bijv. TOPdesk) waarmee incidentregistratie gekoppeld moet worden, of volstaat registratie in het portaal van de opdrachtnemer met directe toegang voor de gemeente?	Opdrachtgever gebruikt TOPdesk. Een koppeling tussen de SIEM/SOC-oplossing en TOPdesk is niet vereist. Incidentregistratie in Microsoft Sentinel en/of het portaal van Opdrachtnemer, met directe toegang voor Opdrachtgever, volstaat (eisen 2.19, 4.7 en 4.19; zie de antwoorden op de vragen 147 en 148 in Nota van Inlichtingen 2). E-mail en telefoon zijn de primaire kanalen voor melding en escalatie aan Opdrachtgever (eis 4.7); voor P1- en P2-incidenten vindt escalatie telefonisch plaats (zie het antwoord op vraag 80 in Nota van Inlichtingen 2).
37	Technisch – PvE 3.5, 4.17 (derden en responsacties)	Welke derden beheren de bron- en doelsystemen (werkplek, servers, netwerk, beveiligingscomponenten) en kunnen zij configuratiewijzigingen binnen de implementatieperiode (februari 2027) uitvoeren? Welke geautomatiseerde responsacties (bijv. account blokkeren, sessies intrekken, isoleren van endpoints of servers) acht de gemeente op voorhand mandateerbaar?	Het beheer van de bron- en doelsystemen (werkplekken, servers, netwerk en beveiligingscomponenten) wordt door Opdrachtgever zelf uitgevoerd, waar nodig ondersteund door externe consultants. Opdrachtgever heeft in de implementatieperiode (maart 2027) capaciteit beschikbaar om de benodigde configuratiewijzigingen uit te voeren, op basis van tijdige en volledige instructies van Opdrachtnemer (eis 3.5). Opdrachtgever wijst op voorhand geen specifieke responsacties aan; de mandaten worden tijdens de implementatie per use-case of responsactie schriftelijk vastgelegd in het DAP en de playbooks (zie de antwoorden op de vragen 21 en 149 in Nota van Inlichtingen 2). Geautomatiseerde responsacties via API op netwerkapparatuur, zoals het blokkeren van IP-adressen of URL's, zijn daarbij toegestaan, binnen de vast te leggen mandaten.

38	Aanbestedingsdocument:	Is het voor de gemeente een vereiste dat de SOC medewerkers fysiek in Nederland gevestigd zijn?	Nee, Aanbestedende Dienst stelt geen eis aan de fysieke vestigingsplaats van SOC-medewerkers in Nederland. Wel gelden onverkort: eis 2.6 (verwerking van en toegang tot gegevens van Opdrachtgever uitsluitend binnen de EER, zie ook het antwoord op vraag 60 in Nota van Inlichtingen 2), eis 1.3 (screening en een geldige Verklaring Omtrent het Gedrag vóór aanvang van de werkzaamheden) en §2.2.1 van het Aanbestedingsdocument (Nederlandse taal in de contacten met Opdrachtgever). Voor werk buiten de primaire SOC-locatie geldt daarnaast hetgeen bij Kerncompetentie 2 is bepaald over beveiligingsmaatregelen.
39	NvI 2 vraag 35, 100, 101, 180	Het is leverancier echter niet toegestaan aansprakelijkheid voor indirecte schade en/of gevolgschade te aanvaarden. Bent u bereid om aansprakelijkheid voor indirecte schade en/of gevolgschade uit te sluiten indien er sprake is van een limitatieve opsomming bestaande uit uitsluitend de volgende schadesoorten: gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, reputatieschade en schade door bedrijfsstagnatie?	Nee. Aanbestedende dienst verwijst naar de beantwoording van vragen 35, 100 en 101 van Nota van Inlichtingen 2. Daarin is reeds aangegeven dat Aanbestedende dienst niet instemt met het uitsluiten van indirecte schade en/of gevolgschade en dat artikel 17 GIBIT 2025 ongewijzigd van toepassing blijft. Ook de nu voorgestelde limitatieve opsomming van gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, reputatieschade en schade door bedrijfsstagnatie geeft Aanbestedende dienst geen aanleiding hiervan af te wijken. Artikel 17 GIBIT 2025 bevat reeds een regeling waarbij de aansprakelijkheid voor overige schade is begrensd. De voorgestelde aanvullende uitsluiting wordt daarom niet overgenomen.
40	Paragraaf 3.2.1 Kerncompetentie 1	In de eerste NvI heeft de aanbestedende dienst aangegeven niet positief te kunnen reageren op onderstaande vraag met betrekking tot de referentie-eis. Wij verzoeken de aanbestedende dienst deze vraag nogmaals in overweging te nemen. Een heroverweging zou de mogelijkheid tot deelname voor meer marktpartijen kunnen verruimen en daarmee de keuze uit inschrijvingen voor de gemeente vergroten. Aanbestedende dienst verlangt ervaring met het opzetten en beheren van een Microsoft Sentinel SIEM-oplossing voor een gemeentelijke organisatie van minimaal 420 gebruikers. Gezien de aard van de gevraagde dienstverlening zijn vergelijkbare eisen en complexiteit ook aanwezig bij andere overheidsorganisaties, zoals provincies, veiligheidsregio's, omgevingsdiensten, waterschappen en uitvoeringsorganisaties. Deze organisaties werken eveneens binnen de kaders van BIO, hybride ICT-infrastructuren en Microsoft-omgevingen. Kan de aanbestedende dienst bevestigen dat referenties van dergelijke overheidsorganisaties eveneens als passend bewijs voor Kerncompetentie 1 worden geaccepteerd, mits wordt voldaan aan de overige eisen ten aanzien van omvang, complexiteit en scope?	De kerncompetenties worden als volgt aangepast: Om in aanmerking te (kunnen) komen voor gunning van de Opdracht, dient een Inschrijver te beschikken over aantoonbare ervaring met de uitvoering én oplevering (Kerncompetenties 1 en 2) van tenminste één (1) 'opdracht' (per kerncompetentie) in de afgelopen drie (3) jaar (voorafgaande aan datum inschrijving) die betrekking heeft (had) op: Kerncompetentie 1 het opzetten en het beheren van een SIEM-oplossing, op basis van Microsoft Sentinel, voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Kerncompetentie 2 het leveren van SOC-diensten voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Concreet: 24x7 uur reageren op alarmen uit een SIEM door event classificatie, triage en analyse en (mogelijk geautomatiseerd) actie te ondernemen ten behoeve van isolatie en eerste herstel. SOC-werkzaamheden vinden primair plaats in een eigen SOC van opdrachtnemer (niet via een derde partij). Indien werkzaamheden buiten de primaire SOC-locatie worden uitgevoerd, bijvoorbeeld in het kader van consignatie-, bereikbaarheids- of piketdiensten, dient de inschrijver aan te tonen welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen. De inschrijver dient aantoonbaar ervaring te hebben met: - Monitoring, detectie, analyse en afhandeling van beveiligingsincidenten; - Logging en audit-trails ten behoeve van compliance en verantwoording; - Uitvoeren van root-cause analyses met betrekking tot de gemelde incidenten; - Advisering over informatiebeveiligingsmaatregelen; Bij inschrijving dient u de aangepaste Bijlage E - Document Bewijsstuk referentie dd 19-11-2026 te gebruiken en in te dienen welke als Bijlage 2 bij deze NvI 4 is toegevoegd.

41	Paragraaf 3.2.1 Kerncompetentie 1 en Kerncompetentie 2	In de 1e NvI heeft de aanbestedende dienst aangegeven niet positief te kunnen reageren op de hierna gestelde vraag m.b.t. de referentie. Wij stellen de vraag nog een keer in de hoop dat de reactie heroverwogen wordt; Kan de aanbestedende dienst bevestigen dat overal waar in de kerncompetenties de term gemeentelijke organisatie wordt gebruikt, gelezen mag worden overheidsorganisatie binnen de Nederlandse publieke sector, waaronder gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen en gemeenschappelijke regelingen? Hierdoor blijft de gevraagde ervaring inhoudelijk gelijkwaardig terwijl de mededinging wordt vergroot.	De kerncompetenties worden als volgt aangepast: Om in aanmerking te (kunnen) komen voor gunning van de Opdracht, dient een Inschrijver te beschikken over aantoonbare ervaring met de uitvoering én oplevering (Kerncompetenties 1 en 2) van tenminste één (1) 'opdracht' (per kerncompetentie) in de afgelopen drie (3) jaar (voorafgaande aan datum inschrijving) die betrekking heeft (had) op: Kerncompetentie 1 het opzetten en het beheren van een SIEM-oplossing, op basis van Microsoft Sentinel, voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Kerncompetentie 2 het leveren van SOC-diensten voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio's, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Concreet: 24x7 uur reageren op alarmen uit een SIEM door event classificatie, triage en analyse en (mogelijk geautomatiseerd) actie te ondernemen ten behoeve van isolatie en eerste herstel. SOC-werkzaamheden vinden primair plaats in een eigen SOC van opdrachtnemer (niet via een derde partij). Indien werkzaamheden buiten de primaire SOC-locatie worden uitgevoerd, bijvoorbeeld in het kader van consignatie-, bereikbaarheids- of piketdiensten, dient de inschrijver aan te tonen welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen. De inschrijver dient aantoonbaar ervaring te hebben met: - Monitoring, detectie, analyse en afhandeling van beveiligingsincidenten; - Logging en audit-trails ten behoeve van compliance en verantwoording; - Uitvoeren van root-cause analyses met betrekking tot de gemelde incidenten; - Advisering over informatiebeveiligingsmaatregelen; Bij inschrijving dient u de aangepaste Bijlage E - Document Bewijsstuk referentie dd 19-11-2026 te gebruiken en in te dienen welke als Bijlage 2 bij deze NvI 4 is toegevoegd.
42	PVE 2.2	Eis 2.2 noemt Microsoft Defender for Servers als logbron. In de gewijzigde Bijlage F1 van 30-10-2026 staat in rij 19 SentinelOne voor Servers, en Defender for Servers in rij 49 onder 'Scope zonder afnameverplichting'. Kunt u aangeven of eis 2.2 of Bijlage F1 leidend is? Staat de gemeente open voor het gebruik van Microsoft Defender for Servers in plaats van SentinelOne, zodat servers, endpoints en identiteiten in één Defender XDR-omgeving samenkomen? Kan de inschrijver dit in zijn inschrijving als advies opnemen, zonder dat dit wordt aangemerkt als variant of voorbehoud?	Het gewijzigde Prijzenblad is leidend: SentinelOne is de verplichte serverlogbron en eis 2.2 wordt daarop aangepast (zie het antwoord op vraag 11). Een overstap naar Microsoft Defender for Servers is binnen de eerstkomende twaalf maanden niet voorzien; daarom is Defender for Servers als optie zonder afnameverplichting opgenomen (regel 49). Inschrijver mag in de uitwerking van gunningscriterium B (advies voor het aansluiten van bronnen) een advies opnemen over een toekomstige overstap naar Microsoft Defender for Servers. Dit wordt niet als variant of voorbehoud aangemerkt, mits de inschrijving en het Prijzenblad volledig zijn gebaseerd op SentinelOne als verplichte serverlogbron en het advies geen voorwaarde aan de inschrijving verbindt.
43	Aanbestedingsdocument SIEM SOC §5.1.1 (p. 24)	Kunt u aangeven of de inschrijver in de uitwerking van criteria A, B en C URL's mag opnemen naar voorbeelden, bijvoorbeeld op GitHub of eigen blogs?	Nee. De uitwerking van de gunningscriteria A, B en C wordt uitsluitend beoordeeld op de inhoud van de ingediende documenten, binnen de maximale omvang van acht A4 (§5.1.1 van het Aanbestedingsdocument). Inhoud waarnaar via een URL wordt verwezen, zoals voorbeelden op GitHub of blogs, wordt niet bij de beoordeling betrokken.
44	NvI 2 vraag 35, 100, 101, 180	Het is leverancier echter niet toegestaan aansprakelijkheid voor indirecte schade en/of gevolgschade te aanvaarden. Bent u bereid om aansprakelijkheid voor indirecte schade en/of gevolgschade uit te sluiten indien er sprake is van een limitatieve opsomming bestaande uit uitsluitend de volgende schadesoorten: gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, reputatieschade en schade door bedrijfsstagnatie?	Nee. Aanbestedende dienst verwijst naar de beantwoording van vragen 35, 100 en 101 van Nota van Inlichtingen 2. Daarin is reeds aangegeven dat Aanbestedende dienst niet instemt met het uitsluiten van indirecte schade en/of gevolgschade en dat artikel 17 GIBIT 2025 ongewijzigd van toepassing blijft. Ook de nu voorgestelde limitatieve opsomming van gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, reputatieschade en schade door bedrijfsstagnatie geeft Aanbestedende dienst geen aanleiding hiervan af te wijken. Artikel 17 GIBIT 2025 bevat reeds een regeling waarbij de aansprakelijkheid voor overige schade is begrensd. De voorgestelde aanvullende uitsluiting wordt daarom niet overgenomen.

45	Nvl 2 vraag 53	In antwoord op vraag 53 geeft u aan dat de aanbestedingsstukken geen gezamenlijk maandmaximum voor boetes vastleggen en dat de definitieve SLA de eventuele samenloop nader moet uitwerken. Deze financiële voorwaarden zijn van belang voor onze risico-inschatting en prijsstelling vóór inschrijving. Bent u bereid vast te leggen dat de gezamenlijke SLA-boetes en servicecredits per kalendermaand maximaal 100% bedragen van de maandelijkse vergoeding voor de betreffende dienstverlening? Indien u dit voorstel niet overneemt, wilt u dan vóór de inschrijfdatum aangeven welke cumulatieregels en welk gezamenlijk maximum gelden?	Nee. De Aanbestedende Dienst neemt het voorgestelde gezamenlijke maandplafond van 100% van de maandelijkse vergoeding niet over. Wel is verduidelijkt dat SLA26 alleen ziet op minimaal twee aantoonbare, aan Opdrachtnemer toerekenbare overschrijdingen van de toepasselijke servicenorm per prioriteit in een kalendermaand. Dit betekent dus een maximale boete van 200% van de maandvergoeding.
46	Nvl 2 vraag 52 en 53	Eén gebeurtenis kan leiden tot overschrijding van meerdere SLA-normen, bijvoorbeeld voor beschikbaarheid, detectie, reactie en escalatie. Uit de antwoorden op vragen 52 en 53 blijkt nog niet hoe deze samenloop meetelt voor de boetegrondslag. Bent u bereid vast te leggen dat bij één gebeurtenis met meerdere rechtstreeks samenhangende SLA-overschrijdingen: maximaal één overschrijding meetelt voor de drempel 'twee of meer per kalendermaand' uit SLA26; en voor die gebeurtenis geen afzonderlijke boetes per overschreden SLA-norm cumuleren, maar uitsluitend de hoogste toepasselijke boete geldt? Indien u dit niet bevestigt, wilt u dan de telwijze en boeteberekening voor deze situatie vóór de inschrijfdatum vastleggen?	Nee. De Aanbestedende Dienst bevestigt niet dat bij één gebeurtenis met meerdere rechtstreeks samenhangende SLA-overschrijdingen maximaal één overschrijding meetelt of dat uitsluitend de hoogste toepasselijke boete geldt. Als de totale afhandelingstijd (detectie+reactie+escalatietijd) echter binnen het voor de betreffende prioriteit geldende tijdvenster blijft, wordt dit als één overschrijding beschouwd.
47	Nvl 2 vragen 162, 193 en194	De antwoorden op vragen 193 en 194 schrijven de beoordelingsaantallen voor en bepalen dat de aangeboden eenheidsprijzen bij aantalswijzigingen bindend blijven. Voor de prijsregels met de eenheid 'Gb' vragen wij om verduidelijking van de bijbehorende reken- en meetgrondslag. Wilt u per betreffende prijsregel aangeven: - of 'Gb' staat voor gigabyte (GB) of gigabit (Gb); - of het opgegeven aantal een volume per dag, maand of contractjaar betreft, dan wel een andere grondslag; - hoe en met welke frequentie toe- en afnames doorwerken in de vergoeding? Wilt u deze uitgangspunten eenduidig opnemen in het prijzenblad of de invulinstructie, zodat alle inschrijvers dezelfde beoordelings- en verrekenbasis hanteren?	Gb' staat voor gigabyte (GB). Het opgegeven aantal betreft het volume per contractjaar per logbron. De prijs per GB betreft uitsluitend de eigen dienstverlening van Opdrachtnemer en niet de Microsoft-kosten. Het werkelijke volume wordt vastgesteld aan de hand van het ingestvolume in Microsoft Sentinel en wordt eens per kwartaal opnieuw beoordeeld; verrekening vindt plaats tegen de bindende prijs per GB. Zie het antwoord op vraag 1 en het gewijzigde Prijzenblad bij deze Nota van Inlichtingen, waarin de eenheid is verduidelijkt tot 'per GB per jaar'.
48	PvE 2.2 en 2.13; gewijzigd Bijlage F1, rijen 14-27	Kunt u per initiële logbron de leidende leverancier, product/variant, editie of licentie, deploymentvorm, aantal tenants/instanties, connector/API en technische aansluitgereedheid verstrekken? Wilt u tevens per prijsregel de teldefinitie, peildatum en behandeling van test-, uitgeschakelde en dubbel getelde objecten bevestigen?	Zie voor de beschikbare informatie per logbron de antwoorden op de vragen 3, 4, 11 en 28 tot en met 33. Een volledige inventaris met productversies, edities en connectorgereedheid per logbron is niet beschikbaar (zie de antwoorden op de vragen 120 en 123 in Nota van Inlichtingen 2). Teldefinities: zie het antwoord op vraag 3 ('gebruiker' = actieve medewerker; 'account' = actief, ingeschakeld AD-account) en vraag 4 ('endpoint' = werkplek; servers/vm's afzonderlijk in regel 19). Uitgeschakelde accounts worden niet meegeteld; dubbeltelling van servers en werkplekken is uitgesloten. De aantallen in het Prijzenblad zijn indicatief en gelden voor de beoordeling; bij wijzigingen tijdens de looptijd gelden de bindende prijzen per eenheid (zie het antwoord op vraag 193 in Nota van Inlichtingen 2).
49	PvE 2.2; gewijzigd Bijlage F1, rijen 19 en 49	Kunt u bevestigen dat SentinelOne voor Servers voor 106 servers/VM's de verplichte initiële serverbron en beoordelingsregel is, en dat Microsoft Defender for Servers uitsluitend een optie zonder afnameverplichting betreft?	Ja, dat bevestigt Aanbestedende Dienst. SentinelOne voor Servers (regel 19, 100 servers/vm's) is de verplichte initiële serverlogbron en telt mee in de beoordelingsprijs. Microsoft Defender for Servers (regel 49) is uitsluitend een optie zonder afnameverplichting en telt niet mee in de beoordelingsprijs. Zie het antwoord op vraag 11.
50	Gewijzigd Bijlage F1, rijen 28-36; Nvl 2 vraag 204	Nvl 2 staat variabele periodieke kosten en vermelding van de gehanteerde eenheid toe. In het beschermde prijzenblad zijn de omschrijving, eenheid en aantallen van rijen 28-35 echter niet invulbaar en staat in rij 36 de eenheid vast. Waar moeten deze componenten en concrete eenheden worden ingevuld? Wilt u een gecorrigeerd invulbaar prijzenblad publiceren?	De regels 28, 29 en 31 tot en met 35 zijn witregels en niet bedoeld om in te vullen; regel 36 'overig, namelijk' vervalt. Alle kosten worden opgenomen in de prijsregels per logbron of in regel 30 'Vaste kosten SOC Basisdienstverlening'. In het gewijzigde Prijzenblad (bijlage 1) bij deze Nota van Inlichtingen is dit verwerkt. Zie het antwoord op vraag 5.
51	PvE 8.13 en 8.14 / SLA26 / Nvl 2 vraag 55	In antwoord op vraag 55 onderscheidt u de SLA-termijnen per incident van de prestatienormen van minimaal 95% over de rapportageperiode. Telt iedere aantoonbare, aan Opdrachtnemer toerekenbare overschrijding van een individuele SLA-termijn mee voor de boetedrempel 'twee of meer per kalendermaand' uit SLA26, ook wanneer Opdrachtnemer over de toepasselijke meetperiode aan de betreffende 95%-prestatienorm voldoet? Wilt u expliciet bevestigen of in die situatie een boete op grond van SLA26 van toepassing is?	De eisen 8.13 en 8.14 uit het PvE worden als volgt aangepast: 8.13 - Opdrachtnemer meldt als beveiligingsincident geclassificeerde meldingen binnen de voor de betreffende prioriteit geldende meldtijd aan Opdrachtgever. 8.14 - Opdrachtnemer levert binnen de overeengekomen termijn een eerste bruikbare analyse en advies over de noodzakelijke vervolg- of mitigerende maatregelen. Definitieve oplossing van het incident kan afhankelijk zijn van Opdrachtgever of betrokken derden en valt daarom niet zonder meer onder deze norm.

52	PvE 8.13 en 8.14 / Nvl 2 vraag 55	In antwoord op vraag 55 verwijst u voor de meetperiode en berekeningswijze van de 95%-prestatienormen naar de SLA. Wilt u voor beide prestatienormen vóór inschrijving aangeven: - welke meetperiode geldt? - of de berekening afzonderlijk per prioriteitscategorie of over alle betreffende meldingen respectievelijk incidenten plaatsvind? - hoe de berekening plaatsvindt bij weinig of geen meldingen of incidenten, inclusief eventuele afrondingsregels of minimumaantallen? Deze uitgangspunten zijn nodig om de prestaties en gevolgen van een individuele termijnoverschrijding eenduidig vast te stellen.	De eisen 8.13 en 8.14 uit het PvE worden als volgt aangepast: 8.13 - Opdrachtnemer meldt als beveiligingsincident geclassificeerde meldingen binnen de voor de betreffende prioriteit geldende meldtijd aan Opdrachtgever. 8.14 - Opdrachtnemer levert binnen de overeengekomen termijn een eerste bruikbare analyse en advies over de noodzakelijke vervolg- of mitigerende maatregelen. Definitieve oplossing van het incident kan afhankelijk zijn van Opdrachtgever of betrokken derden en valt daarom niet zonder meer onder deze norm.
53	Nvl 2 vraag 25 en 68	Volgens antwoord 25 eindigt de detectietijd zodra de alert in het SIEM beschikbaar is voor het SOC. SLA8 omschrijft de reactietijd als de tijd tussen detectie/classificatie en het starten van onderzoek of containmentmaatregelen. Wilt u vóór inschrijving per prioriteit de objectief geregistreerde start- en eindmomenten van zowel de reactie- als de escalatietermijn vastleggen? Wilt u daarbij expliciet aangeven of de termijnen beginnen bij beschikbaarheid van de alert voor het SOC, bij classificatie door het SOC of op een ander moment, en welke registratie voor de meting leidend is?	Ja. Aanbestedende Dienst legt de start- en eindmomenten per termijn als volgt vast; deze gelden voor alle prioriteiten. Detectietijd: vanaf het genereren van het event in het bronsysteem tot het moment waarop de alert of het incident in Microsoft Sentinel is aangemaakt en voor het SOC beschikbaar is (zie het antwoord op vraag 25 in Nota van Inlichtingen 2). Reactietijd: vanaf het moment waarop de alert of het incident in Microsoft Sentinel is aangemaakt tot de eerste aantoonbare actie van het SOC, zoals het toewijzen van het incident, het op actief zetten ervan of het starten van onderzoek of containmentmaatregelen. De classificatie door het SOC valt binnen de reactietijd. Escalatietijd: vanaf hetzelfde moment tot het melden van het incident aan Opdrachtgever, telefonisch voor P1 en P2 en per e-mail voor P3 en P4 (SLA8). Leidend voor de meting zijn de tijdstempels in Microsoft Sentinel in de tenant van Opdrachtgever. Het tijdstip van de melding wordt in het incident vastgelegd. Bij herclassificatie naar een hogere prioriteit (eis 8.12) gelden de termijnen van de nieuwe prioriteit vanaf het moment van herclassificatie. Voor P3 en P4 lopen de reactie- en escalatietermijn binnen het servicevenster (zie het antwoord op vraag 8).
54	vragen 58 en 80.	Antwoord 80 schrijft telefonische escalatie van P1- en P2-incidenten voor. Antwoord 58 bepaalt dat Opdrachtnemer bij onbereikbaarheid van Opdrachtgever de contactpogingen registreert en het afgesproken escalatiepad blijft volgen. Bevestigt u dat voor het behalen van de escalatietermijn het aantoonbaar geregistreerde tijdstip van de eerste telefonische escalatiepoging volgens de overeengekomen procedure geldt, mits Opdrachtnemer ook de voorgeschreven vervolgacties, aanvullende notificaties en escalatie naar vervangers uitvoert? Bevestigt u dat het vervolgens uitblijven van bereikbaarheid of ontvangstbevestiging door Opdrachtgever op zichzelf geen aan Opdrachtnemer toerekenbare termijnoverschrijding oplevert? Indien u dit niet bevestigt, welk objectief geregistreerd moment geldt dan als eindmoment van de escalatietermijn?	Ja. Voor het behalen van de escalatietermijn geldt het aantoonbaar geregistreerde tijdstip waarop Opdrachtnemer de eerste telefonische escalatiepoging uitvoert volgens de overeengekomen procedure. Dit geldt mits Opdrachtnemer de voorgeschreven vervolgacties, aanvullende notificaties en escalatie naar vervangers tijdig en aantoonbaar uitvoert. Het uitblijven van bereikbaarheid of een ontvangstbevestiging door Opdrachtgever levert op zichzelf geen aan Opdrachtnemer toerekenbare termijnoverschrijding op. Opdrachtnemer registreert de contactpogingen, tijdstippen, gebruikte kanalen en gevolgde escalatiestappen.
55	PvE 8.6 / SLA15	Eis 8.6 en antwoord 57 bepalen dat de beschikbaarheidsnorm van minimaal 99,9% per kalendermaand geldt voor de door Opdrachtnemer beheerde onderdelen van de SIEM/SOC-dienstverlening. Bevestigt u dat de berekening voor deze onderdelen uitgaat van 24 uur per dag en zeven dagen per week? Indien voor bepaalde onderdelen een ander servicevenster geldt, wilt u dit per onderdeel specificeren? Valt vooraf met Opdrachtgever overeengekomen gepland onderhoud buiten de beschikbaarheidsberekening? Zo ja, onder welke voorwaarden en hoe verwerkt u de onderhoudsduur in de totale meettijd en de geregistreerde uitvaltijd?	Ja. Voor de beschikbaarheidsnorm van minimaal 99,9% per kalendermaand geldt een meetvenster van 24 uur per dag en zeven dagen per week voor de door Opdrachtnemer beheerde onderdelen van de SIEM/SOC-dienstverlening. Dit betreft in ieder geval de operationele monitoring, incidentverwerking, escalatie en bereikbaarheid van het SOC. Voor deze onderdelen geldt geen afwijkend servicevenster. Dit sluit aan bij de eisen dat beveiligingsmeldingen 24/7 worden gedetecteerd, ontvangen en verwerkt en dat kritieke en hoge meldingen 24/7 worden opgevolgd (eisen 2.20, 4.2 en 8.6). Vooraf met Opdrachtgever afgestemd en overeengekomen gepland onderhoud valt buiten de beschikbaarheidsberekening, mits het binnen het overeengekomen onderhoudsvenster wordt uitgevoerd en tijdig is aangekondigd. De onderhoudsduur wordt dan niet opgenomen in de totale meettijd en niet geregistreerd als uitvaltijd voor de berekening van de beschikbaarheid. Het onderhoud en de afgesproken duur worden wel afzonderlijk geregistreerd en gerapporteerd. Een onvoorziene verlenging van het onderhoud of uitval buiten het overeengekomen onderhoudsvenster telt wel mee als uitvaltijd. De afspraken over onderhoudsvensters, meetmethode en rapportage worden vastgelegd in de SLA, overeenkomstig eis 8.1; planbaar onderhoud wordt vooraf afgestemd en vindt plaats binnen een overeengekomen onderhoudsvenster, conform eis 4.9.
56	PvE 1.2 en 8.17, Nvl 2 vraag 57	Eis 1.2 schrijft voor dat gewijzigde documentatie uiterlijk binnen tien werkdagen beschikbaar wordt gesteld, terwijl eis 8.17 voor bijgewerkte technische, functionele en procesdocumentatie een termijn van vijf werkdagen na implementatie van een relevante wijziging noemt. Kan Aanbestedende Dienst bevestigen welke termijn prevaleert en op welke typen documentatiewijzigingen beide termijnen van toepassing zijn?	De termijn van tien werkdagen uit eis 1.2 is leidend. Eis 8.17 wordt hierbij gewijzigd: 'vijf werkdagen' wordt vervangen door 'tien werkdagen'. Deze termijn geldt voor alle technische, functionele en procesmatige documentatie na de implementatie van een relevante wijziging, tenzij de aard of urgentie van de wijziging eerdere oplevering vereist (eis 1.2).
57	Gewijzigde Bijlage F1 dd 30-10-2026	Bij Cisco Meraki, Barracuda, DNS, DHCP, SecureMe2 NIDS en Holm Security is de eenheid “per Gb” opgenomen, met aantallen van 10 tot 1.000. Kunt u aangeven op welke periode deze aantallen betrekking hebben (per dag, per maand of per jaar)? Moet de prijs per eenheid gelden voor het verwerkte logvolume in Microsoft Sentinel, of voor het volume dat het bronsysteem aanlevert?	Het aantal betreft GB per contractjaar. De prijs per GB geldt voor het volume dat in Microsoft Sentinel wordt ingelezen (ingestvolume), en betreft uitsluitend de eigen dienstverlening van Opdrachtnemer, niet de Microsoft-kosten. Zie het antwoord op vraag 1.

58	Gewijzigde Bijlage F1 dd 30-10-2026	In de gewijzigde Bijlage F1 is in rij 19 “SentinelOne voor Servers” opgenomen. “Microsoft Defender for Servers” staat nu in rij 49 onder “Scope zonder afnameverplichting”. Eis 2.2 noemt Microsoft Defender for Servers als logbron, en volgens vraag 44 zijn alle veertien logbronnen uit eis 2.2 onderdeel van de initiële scope. Kunt u bevestigen dat SentinelOne (voor 106 servers/VM’s) Microsoft Defender for Servers vervangt als logbron in eis 2.2? Wilt u daarbij aangeven welk SentinelOne-product en welke licentie wordt gebruikt, en of Defender for Servers nog binnen de initiële scope valt?	Ja. SentinelOne (100 servers/vm's) vervangt Microsoft Defender for Servers als logbron in eis 2.2; Defender for Servers valt niet binnen de initiële scope maar is een optie zonder afnameverplichting (regel 49). Voor product, licentie en API-toegang: Zie het antwoord op vraag 11.
59	Nvl 2, vragen 32, 48 en 167 en PvE eisen 4.17 en 2.2	Subgunningscriterium B vraagt een beschrijving van geautomatiseerde respons via SOAR. Voor responsacties op netwerkniveau (zoals het blokkeren van een IP-adres of URL) is API-toegang tot de Barracuda-firewalls en Cisco Meraki-componenten nodig. Kunt u aangeven of het beheer van deze apparatuur bij de gemeente zelf of bij een externe ICT-dienstverlener ligt? Kunt u daarnaast bevestigen dat Opdrachtnemer, binnen de vooraf vastgelegde mandaten, API-toegang tot deze apparatuur kan krijgen voor geautomatiseerde responsacties?	Het beheer van de Barracuda-firewalls en de Cisco Meraki-componenten ligt bij Opdrachtgever zelf (zie ook het antwoord op vraag 37). Ja, Opdrachtnemer kan API-toegang tot deze apparatuur krijgen voor geautomatiseerde responsacties, zoals het blokkeren van een IP-adres of URL, uitsluitend binnen de vooraf schriftelijk vastgelegde bevoegdheden en mandaten (eis 4.17).
60	Nvl 2, vragen 21, 25 en 55	In Nvl 2 (vraag 25) is bepaald dat de detectietijd loopt van het genereren van het event in het bronsysteem tot het moment waarop de alert in de SIEM beschikbaar is. Vanaf dat moment lopen de reactie- en escalatietijden uit SLA8. Om deze termijnen eenduidig in de concept-SLA vast te leggen, vragen wij: a) Telt een geautomatiseerde melding aan Opdrachtgever met een eerste classificatie als tijdige reactie in de zin van SLA8, of verwacht u een melding na menselijke beoordeling? b) Telt een geautomatiseerde responsactie waarvoor vooraf schriftelijk mandaat is verleend (vraag 21) als tijdige reactie of eerste mitigerende stap voor de termijnen van SLA8? c) Kunt u bevestigen dat de detectietijd stopt op het moment dat de alert in Microsoft Sentinel beschikbaar is, en dat de classificatie door het SOC daarna onder de reactietijd valt?	a) Nee. De reactietijd uit SLA8 is de tijd die het SOC nodig heeft om een alert in behandeling te nemen. Die tijd begint zodra de alert in Microsoft Sentinel beschikbaar is en eindigt wanneer een SOC-analist de alert aantoonbaar in behandeling neemt. Voor het halen van de reactietijd is nog geen melding aan Opdrachtgever nodig. Een geautomatiseerde melding met een eerste classificatie geldt daarom niet als tijdige reactie in de zin van SLA8. De escalatie aan Opdrachtgever volgt daarna, binnen de escalatietermijn voor de betreffende prioriteit. Aanbestedende Dienst verwacht dat deze escalatie plaatsvindt na menselijke beoordeling door het SOC. b) Nee. Een geautomatiseerde responsactie waarvoor vooraf schriftelijk mandaat is verleend (zie het antwoord op vraag 21 in Nota van Inlichtingen 2), kan een incident indammen of afwenden. Zo’n actie vervangt echter niet de beoordeling van het incident door een analist, bijvoorbeeld om de aard en omvang van een aanval of de handelwijze van een gemotiveerde actor vast te stellen. Een geautomatiseerde responsactie telt daarom niet als tijdige reactie voor de termijnen van SLA8. Uitvoering van zo’n actie binnen het verleende mandaat blijft uiteraard toegestaan en gewenst (eis 4.17). c) Ja. De detectietijd eindigt op het moment dat de alert in Microsoft Sentinel beschikbaar is voor het SOC (zie het antwoord op vraag 25 in Nota van Inlichtingen 2). De reactietijd is de maximale tijd tussen dat moment en het eerste aantoonbare moment waarop het SOC de alert in behandeling neemt. De classificatie door het SOC valt daarmee onder de reactietijd.
61	Nvl 2, vragen 50 en 136 en Aanbestedingsdocument §3.2.1	In Nvl 2 handhaaft u de eis dat de referenties zijn uitgevoerd bij een gemeentelijke organisatie. U motiveert dit met de noodzaak om ervaring aan te tonen binnen de gemeentelijke ICT-context, waaronder informatiebeveiliging en de voor gemeenten relevante wettelijke en beleidsmatige kaders (vr. 50 en 136). Op grond van art. 1.10 en art. 2.90 lid 2 Aw 2012 en voorschrift 3.5 F van de Gids Proportionaliteit moet een geschiktheidseis zien op de kerncompetenties van de opdracht, niet op het soort opdrachtgever. De gevraagde kerncompetenties zijn het inrichten en beheren van Microsoft Sentinel in een hybride omgeving en 24/7 SOC-dienstverlening. Die zijn technisch en organisatorisch gelijk bij andere Nederlandse overheidsorganisaties die onder de BIO2 vallen. Bovendien toetst u de door u genoemde gemeentelijke kaders al apart in Bijlage E (Kerncompetentie 2): de inschrijver moet aantonen dat zijn SOC-processen, detectieregels, rapportages en incidentafhandeling aansluiten op de BIO2 en de relevante wet- en regelgeving voor gemeenten. a) Welke concrete, voor deze opdracht essentiële competentie toetst u met de eis “gemeentelijke organisatie” die niet al wordt geborgd door de genoemde BIO2-eis in Kerncompetentie 2? b) Bent u bereid de eis te formuleren als: “een Nederlandse overheidsorganisatie die valt onder de BIO2, met een vergelijkbare complexiteit en hybride ICT-infrastructuur van tenminste 420 gebruikers”? De door u beoogde borging blijft dan volledig behouden, terwijl geschikte inschrijvers niet onnodig worden uitgesloten. c) Zo nee, kunt u gemotiveerd toelichten waarom de eis volgens u niet in strijd is met art. 1.10 en art. 2.90 lid 2 Aw 2012 en voorschrift 3.5 F van de Gids Proportionaliteit, en waarom de bestaande BIO2-eis daarvoor onvoldoende is?	De kerncompetenties worden als volgt aangepast: Om in aanmerking te (kunnen) komen voor gunning van de Opdracht, dient een Inschrijver te beschikken over aantoonbare ervaring met de uitvoering én oplevering (Kerncompetenties 1 en 2) van tenminste één (1) ‘opdracht’ (per kerncompetentie) in de afgelopen drie (3) jaar (voorafgaande aan datum inschrijving) die betrekking heeft (had) op: Kerncompetentie 1 het opzetten en het beheren van een SIEM-oplossing, op basis van Microsoft Sentinel, voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio’s, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Kerncompetentie 2 het leveren van SOC-diensten voor een Nederlandse overheidsorganisatie in de publieke sector waaronder overheidsorganisaties zoals bijvoorbeeld: Gemeenten, provincies, veiligheidsregio’s, omgevingsdiensten, waterschappen, gemeenschappelijke regelingen en uitvoeringsorganisaties met een vergelijkbare complexiteit en hybride ICT-infrastructuur (zowel on-premises als Cloud), van tenminste 420 gebruikers. Concreet: 24x7 uur reageren op alarmen uit een SIEM door event classificatie, triage en analyse en (mogelijk geautomatiseerd) actie te ondernemen ten behoeve van isolatie en eerste herstel. SOC-werkzaamheden vinden primair plaats in een eigen SOC van opdrachtnemer (niet via een derde partij). Indien werkzaamheden buiten de primaire SOC-locatie worden uitgevoerd, bijvoorbeeld in het kader van consignatie-, bereikbaarheids- of piketdiensten, dient de inschrijver aan te tonen welke technische en organisatorische beveiligingsmaatregelen zijn getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen.

			De inschrijver dient aantoonbaar ervaring te hebben met: - Monitoring, detectie, analyse en afhandeling van beveiligingsincidenten; - Logging en audit-trails ten behoeve van compliance en verantwoording; - Uitvoeren van root-cause analyses met betrekking tot de gemelde incidenten; - Advisering over informatiebeveiligingsmaatregelen; Bij inschrijving dient u de aangepaste Bijlage E - Document Bewijsstuk referentie dd 19-11-2026 te gebruiken en in te dienen welke als Bijlage 2 bij deze NvI 4 is toegevoegd.
62	PVE TECH25	Aanbestedende Dienst vraagt om aan App. Kan Aanbestedende Dienst bevestigen dat een via SmartPhone bereikbare en bruikbare webapplicatie voldoende om deze eis in te vullen?	Eis TECH25 is vervallen; een specifieke app wordt niet verlangd. Zie het antwoord op vraag 16 en het antwoord op vraag 37 in Nota van Inlichtingen 2.
63	PVE eis 4.19	Inschrijver ondersteunt de gevraagde SIEM-dienstverlening met Microsoft Sentinel conform de uitgangspunten van de aanbesteding. Voor automatisering, orkestratie, verrijking, responsacties en incidentafhandeling kan gebruik worden gemaakt van een geïntegreerd SOAR-platform dat informatie uitwisselt met Microsoft Sentinel en andere relevante securitybronnen. Kan Opdrachtgever bevestigen dat een dergelijke architectuur is toegestaan, mits Microsoft Sentinel het centrale SIEM-platform binnen de omgeving van Opdrachtgever blijft	Ja. Zie het antwoord op vraag 203 in Nota van Inlichtingen 2: een geïntegreerd SOAR-platform is toegestaan, mits Microsoft Sentinel binnen de tenant van Opdrachtgever het centrale platform blijft (eis 4.19) en de toegang, zeggenschap, beveiliging, overdraagbaarheid en gegevensbescherming van Opdrachtgever niet worden beperkt.
64	PVE eis 4.19	Inschrijver maakt voor de uitvoering van SIEM/SOC-dienstverlening gebruik van een eigen Microsoft Sentinel-omgeving, waarin detectieregels, use-cases, analytics rules en automatiseringen centraal worden beheerd voor meerdere klanten. Via Microsoft Lighthouse wordt de klantspecifieke Sentinel -instance binnen deze omgeving gekoppeld aan de Microsoft Sentinel-omgeving van Opdrachtgever voor monitoring en beheer. Bij deze werkwijze blijft alle log- en detectiedata eigendom van en opgeslagen binnen de tenant van Opdrachtgever, terwijl Inschrijver de dienstverlening centraal kan beheren en doorontwikkelen. Dit draagt tevens bij aan veiligheid, overdraagbaarheid en voorkomt afhankelijkheid van één leverancier. Kan Opdrachtgever bevestigen dat deze wijze van dienstverlening binnen de uitgangspunten van de aanbesteding is toegestaan? Indien dit niet het geval is, verzoeken wij u toe te lichten waarom dit niet mogelijk is.	Ja. Zie het antwoord op vraag 202 in Nota van Inlichtingen 2: deze werkwijze is toegestaan, mits Microsoft Sentinel in de tenant van Opdrachtgever de primaire Sentinel-omgeving blijft en Opdrachtgever daarover de technische en administratieve zeggenschap behoudt (eis 2.16).
65	PVE eis 2.2	Inschrijver is van mening dat niet alle genoemde logbronnen relevant zijn voor de uitgevraagde security monitoring. Gaat opdrachtgever ermee akkoord dat Inschrijver logbronnen risico-gebaseerd aansluit waaronder in elk geval die logbronnen die input leveren voor de in eis 2.1 genoemde use-cases? Zo voorkomen we dat niet-relevante logbronnen worden aangesloten wat onnodig hoge kosten voor gemeente Vijfheerenlanden met zich mee brengt, en handelen we in lijn met PvE-eis 2.22.	Nee. Zie het antwoord op vraag 201 in Nota van Inlichtingen 2. Alle veertien logbronnen uit eis 2.2 (met SentinelOne in plaats van Microsoft Defender for Servers, zie het antwoord op vraag 11) behoren tot de initiële scope (zie het antwoord op vraag 44 in Nota van Inlichtingen 2).
66	NvI, aangepaste Prijzenblad	In het prijzenblad wordt SentinelOne voor Servers beschreven. Heeft Aanbestedende dienst op dit moment haar serverpark uitgerust met SentinelOne software?	Ja, het serverpark van Opdrachtgever is op dit moment uitgerust met SentinelOne. Zie het antwoord op vraag 11.
67	NvI 201 antwoord	Inschrijver denkt altijd met de klant mee en stelt haar configuratie samen op basis van de business case waarbij Security Monitoring relevantie versus kosten worden afgewogen. In dat kader en op basis van ruime ervaring binnen de lokale overheid, is inschrijver voornemens alleen die logbronnen op te nemen die vanuit security monitoring oogpunt relevant zijn. Toelichting hierover wordt verstrekt in de kostenspecificatie die wordt meegestuurd. Is dat akkoord?	Gedeeltelijk. De veertien logbronnen uit eis 2.2 (met SentinelOne in plaats van Microsoft Defender for Servers, zie het antwoord op vraag 11) blijven vereist. Inschrijver kan in zijn inschrijving voorstellen een of meer logbronnen uit te sluiten, met een goede motivering (bijvoorbeeld geen of onvoldoende detectiewaarde, of aansluiting technisch niet redelijk mogelijk). Dit voorstel neemt Inschrijver op in het Implementatieplan, gunningscriterium A, onderdeel 3; de kwaliteit van de motivering weegt mee in de beoordeling van dat criterium. Inschrijver prijst wel alle veertien logbronnen in het Prijzenblad, zodat de beoordelingsprijzen vergelijkbaar blijven. Vóór de gunning beslist Aanbestedende Dienst of zij met de voorgestelde uitsluiting instemt. Bij instemming wordt de logbron niet aangesloten en niet in rekening gebracht; zonder instemming sluit Opdrachtnemer de logbron aan tegen de aangeboden prijs. Een voorstel tot uitsluiting geldt niet als voorbehoud of variant. Naast de vijf initiële use-cases (eis 2.1) verwacht Aanbestedende Dienst dat Opdrachtnemer de detectie per logbron aanvult met passende use-cases op basis van de beschikbare informatie (eis 2.2). Ook een logbron met beperkte detectiewaarde kan zinvol zijn om aan te sluiten, al is het maar om de logs veilig te stellen, bijvoorbeeld voor onderzoek achteraf. Aanbestedende Dienst weegt dit mee bij de beoordeling van een voorstel tot uitsluiting. Inschrijver kan in zijn kostentoelichting en in zijn advies voor het aansluiten van bronnen (gunningscriterium B) aangeven hoe hij per logbron een passende balans bereikt tussen detectiewaarde, datavolume en kosten.

68	Nvl 1, vragen 62 en 89; Bijlage A1, A28-A32; GIBIT 2025, art. 4.3, 10.14 en 11.3	Hoewel de prijsplicht uit A30 is vervallen en artikel 11.3 GIBIT van toepassing blijft, blijven A29 en A32 onmiddellijke respectievelijk voorafgaande aanpassing aan nieuwe wetgeving verlangen. Kan Aanbestedende Dienst bevestigen dat bij nieuwe of gewijzigde wet- en regelgeving eerst gezamenlijk de impact, noodzakelijke wijziging, planning en vergoeding worden vastgesteld, dat Opdrachtnemer een redelijke implementatietermijn krijgt vanaf het moment waarop de verplichting voldoende concreet en uitvoerbaar is, en dat een termijn niet fataal is voor zover tijdige aanpassing redelijkerwijs onmogelijk is door ontbrekende guidance, afhankelijkheid van derden of disproportionele technische impact?	Gedeeltelijk. Aanbestedende Dienst laat de termijn van drie maanden vóór inwerkingtreding uit eis A32 vervallen. Eis A32 wordt hierbij gewijzigd: de zinsnede '(uiterlijk 3 maanden van tevoren)' vervalt. De ICT-Prestatie moet uiterlijk op de datum van inwerkingtreding van de nieuwe of gewijzigde wet- en regelgeving volledig zijn aangepast, getest en door Opdrachtgever geaccepteerd (eis A29). Bij nieuwe of gewijzigde wet- en regelgeving doet Opdrachtnemer tijdig een voorstel voor de implementatie, waarna deze in afstemming met Opdrachtgever wordt ingepland (eis A28). Een vergoeding is uitsluitend aan de orde onder de voorwaarden van artikel 11.3 GIBIT 2025: de werkzaamheden waren redelijkerwijs niet te voorzien of zijn disproportioneel in omvang, en Opdrachtgever heeft vooraf toestemming gegeven. De zinsnede in eis A32 'Deze wijzigingen worden beschouwd als onderhoud en leiden niet tot separate vergoedingen' geldt met inachtneming van artikel 11.3 GIBIT 2025. Voor het fatale karakter van de termijn gelden de artikelen 4.3 en 10.14 GIBIT 2025 onverkort: de termijn is niet fataal voor zover Opdrachtnemer aantoont dat de wijziging niet voorzienbaar was, of dat de inwerkingtredingstermijn gelet op de aard en omvang van de aanpassingen redelijkerwijs te kort was. Een ruimere uitzondering, zoals bij ontbrekende guidance of afhankelijkheid van derden, wordt niet aanvaard (zie de antwoorden op de vragen 89 en 187 in Nota van Inlichtingen 2).
69	Nvl 1, vragen 58 en 80; PvE 4.17 en 8.7; Bijlage A1, SLA8	De gemeente garandeert niet afzonderlijk dat 24/7 bevoegde contactpersonen beschikbaar zijn. Kan Aanbestedende Dienst bevestigen dat tijd na aantoonbare tijdige escalatie waarin geen bevoegde gemeentelijke contactpersoon of vervanger bereikbaar is, niet meetelt voor reactie-, escalatie- of hersteltijden van Opdrachtnemer en niet tot een SLA-overschrijding of boete kan leiden? Kan zij tevens bevestigen dat Opdrachtnemer zonder voorafgaand schriftelijk mandaat niet aansprakelijk is voor schade die voortvloeit uit het niet of later uitvoeren van een responsactie waarvoor besluitvorming van Opdrachtgever nodig is?	Ja, wij bevestigen dat tijd waarin na een aantoonbaar tijdige escalatie volgens de overeengekomen procedure geen bevoegde contactpersoon van Opdrachtgever of aangewezen vervanger bereikbaar is, niet meetelt voor reactie-, escalatie- of hersteltijden die afhankelijk zijn van besluitvorming of medewerking van Opdrachtgever. Deze periode leidt daarom op zichzelf niet tot een aan Opdrachtnemer toerekenbare SLA-overschrijding of boete, mits Opdrachtnemer de afgesproken contactpogingen, aanvullende notificaties en escalatie naar vervangers uitvoert en registreert. De contactpersonen, vervangers, bereikbaarheid en escalatiestappen worden vastgelegd in de escalatiematrix en de SLA (PvE 8.7). Wij bevestigen tevens dat Opdrachtnemer zonder vooraf schriftelijk vastgelegd mandaat geen responsactie uitvoert waarvoor besluitvorming van Opdrachtgever vereist is. Opdrachtnemer is niet aansprakelijk voor schade die voortvloeit uit het niet of later uitvoeren van zo'n responsactie doordat de vereiste besluitvorming of toestemming van Opdrachtgever uitblijft. Deze bevestiging laat de verplichting van Opdrachtnemer onverlet om het incident tijdig te melden en te escaleren, de ondernomen contactpogingen vast te leggen en binnen het verleende mandaat passende acties uit te voeren (PvE 4.17).
70	Nvl 1, vragen 49, 155 en 156; PvE 4.12, 5.9 en 8.14; Bijlage F1 CERT/IR	De beantwoording rekent naast triage, analyse en advies ook ondersteuning van de door de gemeente ingeschakelde IR-partij, aanvullende zoekopdrachten en monitoring op hernieuwde activiteit tot de reguliere dienstverlening, zonder maximale duur of inzet te noemen. Kan Aanbestedende Dienst deze reguliere ondersteuning begrenzen tot de eerste analyse en een redelijke maar in tijd beperkte inzet, waarna aanvullende specialistische inzet uitsluitend onder de optionele CERT/IR-post of na meerwerkopdracht plaatsvindt? Zo nee, welke maximale inzet moet iedere inschrijver uniform in de vaste vergoeding calculeren?	Aanbestedende Dienst stelt geen maximum in uren of duur vast, maar bakent de reguliere ondersteuning naar haar aard af. Binnen de vaste vergoeding valt de ondersteuning die Opdrachtnemer op afstand levert vanuit zijn eigen informatiepositie en met de telemetrie die beschikbaar is in Microsoft Sentinel, de Microsoft Defender-producten en de overige aangesloten logbronnen, zolang het incident loopt. Dit omvat: de eerste analyse en het advies (eis 8.14), het delen van analyses, tijdlijnen, bewijslast en IOC's met de door Opdrachtgever ingeschakelde IR-partij, het uitvoeren van aanvullende zoekopdrachten en het monitoren op hernieuwde activiteit (zie de antwoorden op de vragen 155 en 156 in Nota van Inlichtingen 2). Niet binnen de vaste vergoeding vallen: digitaal forensisch onderzoek op endpoints, servers, identiteitssystemen en netwerkcomponenten, inzet op locatie, en hands-on containment- of herstelwerkzaamheden buiten de vooraf vastgelegde mandaten. Deze worden uitgevoerd door de IR-partij van Opdrachtgever, of door Opdrachtnemer uitsluitend na afzonderlijke opdracht onder de optionele post 'CERT Dienstverlening en IR Retainers' (regel 50) of als meerwerk conform eis 5.10.

71	NvI 1, vragen 35, 100, 101 en 128; GIBIT 2025, art. 17.3 en 17.4	Aanbestedende Dienst handhaaft artikel 17 GIBIT 2025 en sluit indirecte schade en gevolgschade niet uit. Gelet op de beperkte contractwaarde, de verzekerbaarheid en paragraaf 3.9 van de Gids Proportionaliteit verzoekt Inschrijver opnieuw om indirecte schade, gevolgschade, gederfde winst, omzetverlies, gemiste besparingen en vertragingsschade uit te sluiten, behoudens opzet of bewuste roekeloosheid van de bedrijfsleiding van Opdrachtnemer. Is Aanbestedende Dienst bereid artikel 17 dienovereenkomstig aan te passen? Zo nee, kan zij concreet motiveren waarom deze risicoverdeling voor deze opdracht proportioneel en marktconform is? Inschrijver constateert dat Aanbestedende Dienst de aansprakelijkheidslimieten uit artikel 17.3 en 17.4 GIBIT 2025 ongewijzigd handhaaft. Gelet op de aard en omvang van deze opdracht, de beperkte jaarlijkse contractwaarde en de verzekerbaarheid van de betreffende risico's acht Inschrijver deze limieten nog steeds disproportioneel. Mede gelet op paragraaf 3.9 van de Gids Proportionaliteit verzoekt Inschrijver Aanbestedende Dienst daarom de totale aansprakelijkheid van Opdrachtnemer, behoudens de gebruikelijke uitzonderingen voor onder meer opzet en bewuste roekeloosheid, te beperken tot éénmaal de jaarlijkse contractwaarde per contractjaar. Is Aanbestedende Dienst bereid artikel 17 dienovereenkomstig aan te passen? Zo nee, kan zij concreet motiveren waarom de huidige aansprakelijkheidslimieten, afgezet tegen de contractwaarde, het daadwerkelijke risicoprofiel van deze opdracht, de verzekerbaarheid en de in de IT-/cybersecuritymarkt gebruikelijke risicoverdeling, proportioneel zijn?	Nee. De Aanbestedende dienst neemt de voorgestelde wijzigingen niet over. Voor de beantwoording wordt tevens verwezen naar de beantwoording van vragen 35, 100, 101 en 128 uit de eerdere Nota van Inlichtingen. De Aanbestedende dienst heeft de aansprakelijkheidsregeling opnieuw beoordeeld, mede in het licht van paragraaf 3.9 van de Gids Proportionaliteit, en ziet geen aanleiding haar eerdere standpunt te wijzigen. Artikel 17 GIBIT 2025 bevat reeds een gedifferentieerde en begrensde aansprakelijkheidsregeling. Voor persoons\- en zaakschade geldt een afzonderlijk maximum en voor overige schade is de aansprakelijkheid gekoppeld aan de Jaarvergoeding en zowel per gebeurtenis als per jaar gemaximeerd. Bij de beoordeling is niet uitsluitend de financiële omvang van de opdracht betrokken, maar ook de aard en het daadwerkelijke risicoprofiel van de dienstverlening. De onderhavige SIEM SOC-dienstverlening betreft een bedrijfskritische informatiebeveiligingsdienstverlening. Een toerekenbare tekortkoming kan, ook wanneer de jaarlijkse contractwaarde relatief beperkt is, gevolgen hebben voor onder meer informatiebeveiliging, beschikbaarheid en continuïteit van gemeentelijke dienstverlening, incidentdetectie en incidentafhandeling. De potentiële schade hoeft daarom niet evenredig te zijn aan de jaarlijkse contractwaarde. De Aanbestedende dienst volgt evenmin het voorstel om indirecte schade, gevolgschade, gederfde winst, omzetverlies, gemiste besparingen en vertragingsschade als categorieën op voorhand volledig uit te sluiten. De GIBIT 2025 kiest bewust niet voor een onderscheid tussen directe en indirecte schade, maar voor een begrenzing naar aard en omvang van de schade. Daarbij gelden tevens de wettelijke vereisten voor aansprakelijkheid en schadevergoeding, waaronder toerekenbaarheid en causaal verband. De door Inschrijver voorgestelde beperking tot eenmaal de jaarlijkse contractwaarde per contractjaar acht de Aanbestedende dienst, gelet op het hiervoor beschreven risicoprofiel, onvoldoende. De bestaande regeling biedt Opdrachtnemer reeds vooraf bepaalbare aansprakelijkheidsmaxima en sluit aan bij de systematiek van de GIBIT 2025, waarbij de aansprakelijkheid voor overige schade is gekoppeld aan de Jaarvergoeding. De GIBIT 2025 houdt daarbij tevens rekening met de verzekerbaarheid van de aansprakelijkheidsrisico's. De Aanbestedende dienst acht de bestaande verdeling van risico's, gelet op de aard, omvang en mogelijke gevolgen van tekortkomingen binnen deze specifieke opdracht, proportioneel. Dat een individuele Inschrijver een verdergaande beperking of andere risicoverdeling gebruikelijk of wenselijk acht, geeft de Aanbestedende dienst geen aanleiding om voor deze opdracht van de GIBIT 2025 af te wijken. Artikel 17 GIBIT 2025 blijft derhalve ongewijzigd van toepassing.
72	NvI 1, vragen 33, 48, 157 en 167; PvE 3.3 en 3.5; GIBIT 2025, art. 4.2	Aanbestedende Dienst handhaaft 1 maart 2027 als beoogde livegang, garandeert niet dat alle documentatie volledig en actueel beschikbaar is en verstrekt geen uitputtend overzicht van betrokken leveranciers. Kan zij bevestigen dat de fatale implementatietermijn van rechtswege wordt verlengd met iedere aantoonbare vertraging in deze afhankelijkheden die niet aan Opdrachtnemer is toe te rekenen?	Nee, dat bevestigt Aanbestedende Dienst niet in deze vorm. Allereerst is de beoogde livegang gewijzigd van 1 maart 2027 naar 1 april 2027 (zie de rectificatie bij deze Nota van Inlichtingen). De implementatietermijn wordt niet automatisch verlengd bij vertraging. Bij een aantoonbare vertraging die niet aan Opdrachtnemer is toe te rekenen en die het gevolg is van een afhankelijkheid van Opdrachtgever of van door Opdrachtgever ingeschakelde derden, geldt het volgende: Opdrachtnemer meldt de (dreigende) vertraging direct en schriftelijk aan Opdrachtgever. Hij geeft daarbij de oorzaak, de verwachte gevolgen voor de planning en de voorgestelde maatregelen aan. Opdrachtnemer neemt redelijke maatregelen om de gevolgen van de vertraging te beperken, bijvoorbeeld door andere werkzaamheden naar voren te halen. Opdrachtgever en Opdrachtnemer stellen in overleg een aangepaste planning vast. Een eventuele verlenging is niet langer dan de vertraging die daadwerkelijk door de betreffende afhankelijkheid is ontstaan. Vertraging die niet tijdig en gemotiveerd is gemeld, geeft geen recht op aanpassing van de planning. Artikel 4.2 GIBIT 2025 blijft onverkort van toepassing. Aanbestedende Dienst merkt daarnaast op dat de Nota's van Inlichtingen openbaar zijn. Gedetailleerde informatie over de ICT-omgeving, de betrokken leveranciers en de documentatie wordt daarom in deze fase bewust beperkt gedeeld, in het belang van de informatieveiligheid van Opdrachtgever. Deze informatie wordt na gunning, bij aanvang van de implementatie, aan Opdrachtnemer verstrekt (zie ook het antwoord op vraag 79).

73	NvI 1, vragen 31, 32, 44, 45, 47, 118 en 158; PvE 2.2, 2.13, 3.3, 5.6 en 5.7	Uit de beantwoording volgt dat Aanbestedende Dienst verlangt dat alle veertien genoemde logbronnen worden aangesloten, ongeacht de concrete detectiewaarde en de daarmee gemoeide implementatie-inspanning en kosten. Voor verschillende niet-standaardlogbronnen kan aansluiting aanzienlijke aanvullende ontwikkel- en implementatiewerkzaamheden vergen, terwijl voor de implementatie een maximaal budget van € 15.000 geldt en de implementatietermijn uiterst beperkt is. Inschrijver is van mening dat een deskundige SOC/MDR-dienstverlener de ruimte dient te krijgen om zelf binnen de kaders functioneel en risicogebaseerd te bepalen welke logbronnen noodzakelijk en doelmatig zijn om het door Aanbestedende Dienst verlangde beveiligings- en beschermingsniveau te realiseren. Het verplicht aansluiten van een logbron die geen of slechts beperkte aanvullende detectiewaarde biedt, leidt immers tot extra kosten en implementatie-inspanning zonder dat daar noodzakelijkerwijs een wezenlijke verbetering van de beveiliging tegenover staat. Is Aanbestedende Dienst daarom bereid de eis zodanig aan te passen dat Opdrachtnemer als deskundig leverancier zelf, op basis van een gemotiveerde risico- en detectiewaardeanalyse, mag bepalen welke van de genoemde logbronnen worden aangesloten, mits Opdrachtnemer kan aantonen dat daarmee een passend en ten minste gelijkwaardig beveiligings- en beschermingsniveau wordt gerealiseerd? Hiermee kan binnen de door Aanbestedende Dienst gehanteerde kostenraming kostenefficiënt worden gehandeld, zonder wezenlijke verslechtering van het beveiligingsniveau. Zo nee, kan Aanbestedende Dienst gemotiveerd toelichten waarom aansluiting van ieder van de veertien logbronnen noodzakelijk is, ongeacht de door de deskundige leverancier vastgestelde detectiewaarde, kosten en implementatie-inspanning?	Nee. Aanbestedende Dienst handhaaft dat alle veertien logbronnen uit eis 2.2 (met SentinelOne in plaats van Microsoft Defender for Servers, zie het antwoord op vraag 11) worden aangesloten. Motivering: de veertien logbronnen zijn door Aanbestedende Dienst geselecteerd als noodzakelijk voor een volledige dekking van de vijf initiële use-cases uit eis 2.1 (zie het antwoord op vraag 32 in Nota van Inlichtingen 2). Zij dekken samen de domeinen identiteit, endpoint, server, netwerk/externe toegang, e-mail/cloud en kwetsbaarheden, waartussen eis 2.17 correlatie verlangt. Het weglaten van een bron vermindert die correlatiemogelijkheden en daarmee de detectiedekking. Bovendien maakt een vaste set logbronnen de inschrijvingen onderling vergelijkbaar. Kostenefficiëntie wordt bereikt binnen de logbron, niet door logbronnen weg te laten: Opdrachtnemer adviseert per logbron welke gegevens worden ingelezen en past, na goedkeuring van Opdrachtgever, filtering en transformatie toe (eis 2.22; zie de antwoorden op de vragen 153 en 162 in Nota van Inlichtingen 2). Wel is met deze NVI bepaald dat het maximale implemenatiebudget naar €30.000,- (excl BTW) is verhoogd.
74	NvI 1, vragen 26, 52 en 53; GIBIT 2025, art. 10.12, 10.13 en 17	Kan Aanbestedende Dienst bevestigen dat voor één en dezelfde tekortkoming geen cumulatie plaatsvindt van SLA26, een servicecredit, tijdelijke malus, prijsvermindering en volledige schadevergoeding, en dat ieder betaald boete- of servicecreditbedrag volledig in mindering komt op iedere schadevergoeding wegens dezelfde tekortkoming?	Nee. De Aanbestedende Dienst bevestigt niet dat voor één en dezelfde tekortkoming geen cumulatie kan plaatsvinden van SLA26. (NVI1: 100, 101, 180.) Aritkel 17 van GIBIT blijft ongewijzigd.
75	NvI 1, vragen 26, 52 en 53; Bijlage A1, SLA26	In NvI 1 heeft Aanbestedende Dienst verduidelijkt dat de boeteregeling eerst wordt toegepast bij twee of meer aantoonbare en aan Opdrachtnemer toerekenbare overschrijdingen van de betreffende servicenorm. De financiële consequenties blijven naar het oordeel van Inschrijver echter disproportioneel in verhouding tot de aard, omvang en contractwaarde van de opdracht en het daadwerkelijke risico dat Aanbestedende Dienst bij een overschrijding loopt. Dit geldt in het bijzonder voor P3- en P4-incidenten. Overschrijding van de daarvoor geldende KPI's leidt in de regel niet tot een materiële verhoging van het beveiligingsrisico die toepassing van een boete van 25% van de maandelijkse vergoeding rechtvaardigt. Voor P1- en P2-incidenten acht Inschrijver een beperkte boeteregeling wel verdedigbaar, mits deze wordt gekoppeld aan de mate waarin de KPI over de betreffende meetperiode daadwerkelijk wordt overschreden en de financiële consequentie proportioneel wordt gemaximeerd. Daarbij is tevens relevant dat bij daadwerkelijk geleden schade de contractuele aansprakelijkheidsregeling onverkort van toepassing blijft. Mede gelet op paragraaf 3.9 van de Gids Proportionaliteit verzoekt Inschrijver Aanbestedende Dienst daarom de regeling te heroverwegen. Is Aanbestedende Dienst bereid SLA26 zodanig aan te passen dat (i) de boeteregeling uitsluitend van toepassing is op P1- en P2-incidenten, (ii) uitsluitend een overschrijding van de betreffende KPI met meer dan 5% over een kalendermaand tot een boete kan leiden, en (iii) de boete wordt gemaximeerd op 25% van de maandelijkse opdrachtsom voor P1 respectievelijk 15% voor P2, een en ander nader vast te leggen in de definitieve SLA? Zo nee, kan Aanbestedende Dienst gemotiveerd toelichten waarom de bestaande regeling, mede in verhouding tot het daadwerkelijke beveiligingsrisico en de overige contractuele remedies, proportioneel wordt geacht?	Nee. Aanbestedende Dienst handhaaft de boeteregeling uit SLA26; zie het antwoord op vraag 45. De boeteregeling geldt ook voor P3- en P4-meldingen. De termijnen voor deze prioriteiten (een reactietijd van vier respectievelijk acht uur, binnen het servicevenster) bieden Opdrachtnemer ruim voldoende tijd. Aanbestedende Dienst acht het daarom zeer onwaarschijnlijk dat deze termijnen bij een deugdelijke uitvoering van de dienstverlening worden overschreden, en ziet geen aanleiding de regeling voor deze prioriteiten te beperken.
76	NvI 1, vragen 25, 54 en 69; Bijlage A1, SLA8; PvE 8.6, 8.13 en 8.14	De detectietijd vangt volgens de beantwoording aan bij het genereren van het relevante event in het bronsysteem en eindigt wanneer de alert in het SIEM voor het SOC beschikbaar komt. Deze periode omvat verwerking en transport binnen gemeentelijke systemen, connectoren en Microsoft-diensten waarop Opdrachtnemer niet steeds invloed heeft. Kan Aanbestedende Dienst bevestigen dat alleen vertraging die aantoonbaar binnen de invloedssfeer van Opdrachtnemer ligt als SLA-overschrijding wordt aangemerkt en meetelt voor de 95%-normen en SLA26, en dat bron-, netwerk-, connector- en Microsoftvertraging buiten die invloedssfeer wordt uitgesloten?	Gedeeltelijk. De oplossing, inclusief het transport van logdata van het bronsysteem naar Microsoft Sentinel, moet zo zijn ingericht dat de detectietijden uit SLA8 worden gehaald. Vertraging in die transportlaag komt daarom in beginsel voor rekening van Opdrachtnemer. Niet als overschrijding gelden: - vertraging door overmacht, zoals uitval of verstoring van Microsoft-clouddiensten (zie ook eis 8.6); - vertraging die aantoonbaar door Opdrachtgever wordt veroorzaakt. Het is aan Opdrachtnemer om aan te tonen dat een van deze uitzonderingen van toepassing is. Daarbij geldt dat Opdrachtnemer de gezondheid van de logging bewaakt: use-case UC5 (eis 2.1) vraagt het detecteren van uitval, verstoring of manipulatie van logging, en eis 8.6 vraagt dat uitval van kritieke logstromen binnen één uur wordt gedetecteerd en gemeld. Vertraging in een logstroom die Opdrachtnemer niet tijdig signaleert, komt voor zijn rekening. De 95%-normen in de eisen 8.13 en 8.14 zijn vervallen; zie het antwoord op vraag 14.

77	Nvl 1, vragen 22 en 149; PvE 6.8 en 6.9	Aanbestedende Dienst heeft bevestigd dat AI-functionaliteit na bespreking eenmalig in het DAP kan worden goedgekeurd. Kan zij bevestigen dat dit ook geldt voor de door Inschrijver standaard gebruikte AI-agent en AI/ML-functionaliteit binnen de centrale SOAR-/SOC-tooling, mits doel, model, gegevenscategorieën, locaties, subverwerkers, risico's en menselijke controle vooraf transparant zijn beschreven, en dat binnen de aldus goedgekeurde scope geen afzonderlijke toestemming per incident of verwerking nodig is?	Ja. De werkwijze uit het antwoord op vraag 22 in Nota van Inlichtingen 2 geldt ook voor de standaard door Inschrijver gebruikte AI-agent en AI/ML-functionaliteit in de centrale SOAR-/SOC-tooling. Opdrachtnemer legt deze functionaliteit vooraf ter bespreking voor met de informatie die eis 6.8 voorschrijft. Na goedkeuring door Opdrachtgever wordt de toegestane functionaliteit vastgelegd in het DAP; binnen die goedgekeurde scope is geen afzonderlijke toestemming per incident of verwerking nodig. Nieuwe of gewijzigde AI-functionaliteit wordt opnieuw ter goedkeuring voorgelegd. De eisen 2.6, 2.27, 6.2 en 6.9 blijven onverkort van toepassing; gemeentelijke gegevens worden niet gebruikt voor training van AI-modellen.
78	Nvl 1, vragen 166-168; PvE 2.2, 2.13 en 5.10	Het antwoord op vraag 166 stelt dat de veertien bronnen niet zonder meer een uitputtende afbakening vormen, terwijl alle noodzakelijke kosten volgens eis 5.9 in de prijs moeten zijn inbegrepen. Kan Aanbestedende Dienst bevestigen dat de vaste initiële en periodieke prijs uitsluitend betrekking heeft op de veertien uitdrukkelijk genoemde logbronnen en de overeengekomen functionaliteit, en dat iedere later toegevoegde logbron, systeem of beveiligingsoplossing uitsluitend na afzonderlijke schriftelijke opdracht en prijsafspraak wordt aangesloten en beheerd?	Ja. De vaste initiële en periodieke prijzen hebben betrekking op de veertien logbronnen uit eis 2.2 (met SentinelOne in plaats van Microsoft Defender for Servers, zie het antwoord op vraag 11), de vijf initiële use-cases en de overige in de aanbestedingsstukken beschreven dienstverlening, tegen de in het Prijzenblad opgenomen eenheden. Iedere later toe te voegen logbron, systeem of beveiligingsoplossing wordt uitsluitend aangesloten en beheerd na afzonderlijke voorafgaande schriftelijke opdracht van Opdrachtgever, als meerwerk conform eis 5.10 en op basis van het uurtarief in het Prijzenblad (zie het antwoord op vraag 196 in Nota van Inlichtingen 2). Het antwoord op vraag 166 in Nota van Inlichtingen 2 wordt in die zin verduidelijkt: de opdracht sluit het later aansluiten van andere bronnen niet uit, maar dat valt niet onder de vaste prijzen. Wijzigingen in aantallen binnen de bestaande logbronnen (zoals meer gebruikers, endpoints, servers of GB) zijn geen meerwerk; daarvoor gelden de bindende prijzen per eenheid.
79	Nvl 1, vragen 120, 121, 123, 143 en 144; PvE 2.2, 2.13 en 5.5	Voor verschillende logbronnen ontbreken nog productversies, edities, deploymentvormen, interfaces, concrete aantallen en gemeten logvolumes, terwijl alle veertien bronnen verplicht binnen de initiële scope vallen. Kan Aanbestedende Dienst uiterlijk vóór de inschrijfdatum per logbron een actuele technische inventaris verstrekken, inclusief product/versie, deploymentvorm, beschikbare connector of API, benodigde rechten en licenties, aantallen assets en betrokken beheerder/leverancier? Kan zij bevestigen dat verschillen tussen deze inventaris en de feitelijke situatie na gunning die aantoonbaar extra werkzaamheden veroorzaken als scopewijziging of meerwerk worden behandeld?	Zie voor de beschikbare technische informatie de antwoorden op de vragen 3, 4, 11 en 28 tot en met 37. Een volledige technische inventaris per logbron (versies, edities, rechten) kan vóór de inschrijfdatum niet worden verstrekt (zie de antwoorden op de vragen 120, 123 en 157 in Nota van Inlichtingen 2); Opdrachtgever stelt de beschikbare informatie bij aanvang van de implementatie ter beschikking. Aanbestedende Dienst bevestigt niet dat ieder verschil tussen de verstrekte informatie en de feitelijke situatie als meerwerk wordt behandeld. Het aansluiten van de veertien logbronnen uit eis 2.2, inclusief eventueel benodigde alternatieve integratiemethoden (eis 2.13), valt binnen de aangeboden prijzen (zie de antwoorden op de vragen 31 en 45 in Nota van Inlichtingen 2). Meerwerk is uitsluitend aan de orde bij aantoonbare uitbreidingen buiten de overeengekomen scope, conform eis 5.10.
80	Nvl 1, vragen 102, 104 en 108; GIBIT 2025, art. 17.5, 18 en 21.7	Kan Aanbestedende Dienst bevestigen dat toezichthoudersboetes en aanspraken van derden uitsluitend voor rekening van Opdrachtnemer komen voor zover zij rechtstreeks en aantoonbaar zijn veroorzaakt door een toerekenbare tekortkoming van Opdrachtnemer, met toepassing van causaliteit en eigen schuld van Opdrachtgever? Kan zij tevens bevestigen dat voor Derdenprogrammatuur geen verdergaande IE-vrijwaring wordt verlangd dan Opdrachtnemer redelijkerwijs van de betreffende rechthebbende verkrijgt, tenzij de inbreuk door Opdrachtnemer zelf is veroorzaakt of had moeten worden onderkend?	Nee. De Aanbestedende dienst neemt de voorgestelde aanvullingen en beperkingen niet over en verwijst tevens naar de antwoorden op vragen 102, 104 en 108 uit de eerdere Nota van Inlichtingen. Voor aansprakelijkheid, waaronder aansprakelijkheid in verband met toezichthoudersboetes en aanspraken van derden, gelden de voorwaarden, beperkingen en uitzonderingen van artikel 17 GIBIT 2025 en het toepasselijke recht. De beoordeling van aansprakelijkheid en de omvang daarvan vindt plaats aan de hand van deze bepalingen en de omstandigheden van het concrete geval. De Aanbestedende dienst ziet geen aanleiding deze regeling nader aan te vullen of te beperken. Ten aanzien van intellectuele-eigendomsrechten en Derdenprogrammatuur blijven eveneens de betreffende bepalingen van de GIBIT 2025 ongewijzigd van toepassing. De Aanbestedende dienst stemt niet in met een beperking van de verplichtingen van Opdrachtnemer tot hetgeen deze zelf van een derde of rechthebbende heeft bedongen of kan verkrijgen. De artikelen 17, 18, 21 en 23 GIBIT 2025 blijven ongewijzigd van toepassing.
81	Nvl 1, vraag 57; PvE 8.6; Bijlage A1, SLA15	Aanbestedende Dienst handhaaft een beschikbaarheid van 99,9% per kalendermaand voor de door Opdrachtnemer beheerde onderdelen. Kan zij bevestigen dat deze beschikbaarheid per afzonderlijk overeengekomen en objectief meetbaar dienstonderdeel wordt berekend, met uitsluiting van gepland onderhoud, overmacht, noodonderhoud, fouten of handelingen van Opdrachtgever en derden, uitval van gemeentelijke systemen en Microsoft-diensten, en perioden waarin de dienst wel beschikbaar is maar een niet-kritieke functionaliteit is verminderd?	Ja, met de volgende verduidelijking. De beschikbaarheidsnorm van minimaal 99,9% per kalendermaand geldt voor de door Opdrachtnemer beheerde onderdelen van de SIEM/SOC-dienstverlening. De beschikbaarheid wordt gemeten voor de overeengekomen, door Opdrachtnemer beheerde onderdelen; de meetmethode en rapportage worden in de SLA vastgelegd. Uitval van gemeentelijke systemen, logbronnen of onderliggende Microsoft-clouddiensten wordt niet aan Opdrachtnemer toegerekend, tenzij Opdrachtnemer de uitval heeft veroorzaakt of onvoldoende passende maatregelen heeft getroffen.
82	Nvl 1, vraag 55; Bijlage A1, SLA8; PvE 8.8-8.14	Aanbestedende Dienst heeft geantwoord dat de termijnen uit SLA8 voor iedere melding gelden, terwijl de 95%-norm bepaalt of de afzonderlijke prestatienorm over de rapportageperiode is behaald. Kan zij bevestigen dat een incidentele overschrijding binnen de resterende 5% wel wordt gerapporteerd, maar niet zonder meer geldt als het niet behalen van de betreffende servicenorm of als een afzonderlijke overschrijding voor SLA26, zolang de 95%-prestatienorm over de overeengekomen meetperiode wordt gehaald? Zo nee, hoe verhouden de 95%-norm en de voor iedere melding geldende norm zich dan tot elkaar zonder de 95%-tolerantie feitelijk betekenisloos te maken?	De vraag naar de resterende 5% is niet meer van toepassing. De prestatienormen van 95% uit de eisen 8.13 en 8.14 vervallen volgens de meest recente wijzigingen in deze Nota van Inlichtingen 4.

BIJLAGEN:

1) Bijlage 1 bij Nvl 4 - Gewijzigde Bijlage F1 - Prijzenblad SIEM SOC dd 19-11-2026.xlsx
2) Bijlage 2 bij Nvl 4 - Aangepaste Bijlage E - Document Bewijsstuk referentie dd 19-11-2026.docx