



## SIEM/SOC Aanbesteding: Programma van Eisen

# Contents

|                                                      |    |
|------------------------------------------------------|----|
| SIEM/SOC Aanbesteding: Programma van Eisen .....     | 1  |
| Contents .....                                       | 2  |
| Inleiding.....                                       | 3  |
| 1 Algemene Eisen.....                                | 3  |
| 2 Oplossing.....                                     | 4  |
| 3 Implementatie.....                                 | 10 |
| 4 Documentatie, processen en communicatie .....      | 12 |
| 5 Prijsmodel .....                                   | 16 |
| 6 Privacy & Security .....                           | 17 |
| 7 Re-transitie en Exitplan .....                     | 20 |
| 8 SLA en dienstverlening .....                       | 21 |
| 9 Bijlages .....                                     | 24 |
| 9.1 Richtinggevende escalatiematrix bij eis 8.7..... | 24 |
| 9.2 Verantwoordelijkheden .....                      | 24 |

# Inleiding

In dit Programma van Eisen zijn de minimale eisen opgenomen waaraan de aangeboden SIEM-oplossing, gebaseerd op Microsoft Sentinel, en SOC-dienstverlening moeten voldoen. Deze eisen hebben betrekking op onder andere de technische oplossing, implementatie, dienstverlening, beveiliging, privacy, rapportage, continuïteit, exit voorzieningen en service levels. Inschrijvers dienen aan te tonen dat zij aan deze eisen voldoen en dat zij beschikken over de benodigde expertise, capaciteit en processen om de opdracht succesvol uit te voeren gedurende de gehele contractperiode.

## 1 Algemene Eisen

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1 | Opdrachtnemer verklaart akkoord te gaan met de GIBIT 2025 en de overige op de Overeenkomst van toepassing verklaarde voorwaarden. Algemene voorwaarden, branchevoorwaarden of andere voorwaarden van Opdrachtnemer worden uitdrukkelijk van de hand gewezen.                                                                                                                                                                                                                                                                                                                                                                   |
| 1.2 | Opdrachtnemer houdt alle technische, functionele en procesmatige documentatie gedurende de looptijd van de Overeenkomst actueel. Opdrachtgever heeft steeds toegang tot de meest recente versie. Gewijzigde documentatie wordt uiterlijk binnen tien werkdagen na de betreffende wijziging aan Opdrachtgever beschikbaar gesteld, tenzij de aard of urgentie van de wijziging eerdere oplevering vereist.                                                                                                                                                                                                                      |
| 1.3 | Medewerkers van Opdrachtnemer en door Opdrachtnemer ingeschakelde derden die toegang hebben tot gemeentelijke gegevens, systemen of de SIEM/SOC-omgeving zijn aantoonbaar op integriteit gescreend en gebonden aan geheimhouding. Voor deze medewerkers is vóór aanvang van de werkzaamheden een voor de functie passende en geldige Verklaring Omtrent het Gedrag beschikbaar. De Verklaring Omtrent het Gedrag is bij aanvang van de werkzaamheden niet ouder dan drie maanden. Opdrachtnemer verstrekt Opdrachtgever op verzoek bewijs dat aan deze eis wordt voldaan, met inachtneming van de toepasselijke privacyregels. |
| 1.4 | Opdrachtnemer beschikt over een geldig ISO 27001:2022-certificaat of gelijkwaardig certificaat waarvan de aangeboden dienstverlening onderdeel is van de scope.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## 2 Oplossing

| Nr.                                               | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 2.1                                               | <p>De SIEM/SOC oplossing ondersteunt initieel de volgende use-cases:</p> <table border="1"> <thead> <tr> <th data-bbox="323 387 719 427">Use-case</th><th data-bbox="719 387 1385 427">Doelstelling</th></tr> </thead> <tbody> <tr> <td data-bbox="323 427 719 546"><b>UC1 – Misbruik van identities</b></td><td data-bbox="719 427 1385 546">Detecteren van identiteitsmisbruik, accountovername, phishing-gerelateerde activiteiten en afwijkend authenticatiegedrag.</td></tr> <tr> <td data-bbox="323 546 719 665"><b>UC2 - Misbruik van privileged accounts</b></td><td data-bbox="719 546 1385 665">Detecteren van misbruik van beheerrechten, privilege-escalatie en verdachte beheeractiviteiten.</td></tr> <tr> <td data-bbox="323 665 719 784"><b>UC3 - Malware en ransomware</b></td><td data-bbox="719 665 1385 784">Detecteren van malware-infecties, ransomware-gerelateerde activiteiten, laterale beweging en sabotage van herstelvoorzieningen.</td></tr> <tr> <td data-bbox="323 784 719 943"><b>UC4 - Verdachte netwerk- en VPN-activiteit</b></td><td data-bbox="719 784 1385 943">Detecteren van misbruik van externe toegang, scanningactiviteiten, ongebruikelijke netwerkverbindingen en segmentoverschrijdende communicatie.</td></tr> <tr> <td data-bbox="323 943 719 1061"><b>UC5 - Uitval of manipulatie van logging</b></td><td data-bbox="719 943 1385 1061">Detecteren van uitval, verstoring of manipulatie van logging, monitoring en beveiligingsvoorzieningen.</td></tr> </tbody> </table> | Use-case | Doelstelling | <b>UC1 – Misbruik van identities</b> | Detecteren van identiteitsmisbruik, accountovername, phishing-gerelateerde activiteiten en afwijkend authenticatiegedrag. | <b>UC2 - Misbruik van privileged accounts</b> | Detecteren van misbruik van beheerrechten, privilege-escalatie en verdachte beheeractiviteiten. | <b>UC3 - Malware en ransomware</b> | Detecteren van malware-infecties, ransomware-gerelateerde activiteiten, laterale beweging en sabotage van herstelvoorzieningen. | <b>UC4 - Verdachte netwerk- en VPN-activiteit</b> | Detecteren van misbruik van externe toegang, scanningactiviteiten, ongebruikelijke netwerkverbindingen en segmentoverschrijdende communicatie. | <b>UC5 - Uitval of manipulatie van logging</b> | Detecteren van uitval, verstoring of manipulatie van logging, monitoring en beveiligingsvoorzieningen. |
| Use-case                                          | Doelstelling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| <b>UC1 – Misbruik van identities</b>              | Detecteren van identiteitsmisbruik, accountovername, phishing-gerelateerde activiteiten en afwijkend authenticatiegedrag.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| <b>UC2 - Misbruik van privileged accounts</b>     | Detecteren van misbruik van beheerrechten, privilege-escalatie en verdachte beheeractiviteiten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| <b>UC3 - Malware en ransomware</b>                | Detecteren van malware-infecties, ransomware-gerelateerde activiteiten, laterale beweging en sabotage van herstelvoorzieningen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| <b>UC4 - Verdachte netwerk- en VPN-activiteit</b> | Detecteren van misbruik van externe toegang, scanningactiviteiten, ongebruikelijke netwerkverbindingen en segmentoverschrijdende communicatie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| <b>UC5 - Uitval of manipulatie van logging</b>    | Detecteren van uitval, verstoring of manipulatie van logging, monitoring en beveiligingsvoorzieningen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| 2.2                                               | <p>De oplossing biedt ondersteuning en aanvullende use-case dekking voor de volgende logbronnen:</p> <ul style="list-style-type: none"> <li>• Microsoft Entra ID</li> <li>• Microsoft Active Directory</li> <li>• Cisco Duo</li> <li>• HelloID</li> <li>• Microsoft Defender for Endpoint</li> <li>• Microsoft Defender for Servers</li> <li>• Cisco Meraki</li> <li>• Barracuda</li> <li>• Microsoft 365 Audit Logs</li> <li>• Exchange Online Audit Logs</li> <li>• DNS</li> <li>• DHCP</li> <li>• SecureMe2 NIDS</li> <li>• Holm Security</li> </ul> <p>Van deze logbronnen wordt vereist dat de SIEM SOC oplossing passende aanvullende use-cases out of the box ondersteund.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |
| 2.3                                               | <p>De door Opdrachtnemer ingerichte SIEM/SOC-oplossing veroorzaakt geen onevenredige of merkbare verstoring van de prestaties of beschikbaarheid van het netwerk, de systemen, werkplekken en applicaties van Opdrachtgever.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |          |              |                                      |                                                                                                                           |                                               |                                                                                                 |                                    |                                                                                                                                 |                                                   |                                                                                                                                                |                                                |                                                                                                        |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | Opdrachtnemer bewaakt de belasting die wordt veroorzaakt door connectoren, agents, API-koppelingen, logtransport en gegevensverwerking en neemt zo nodig passende maatregelen.                                                                                                                                                                                                                                                                                                                                           |
| 2.4 | Opdrachtnemer past bij het ontwerp en de inrichting van de Oplossing gangbare architectuur- en beveiligingsprincipes toe. Koppelingen met interne systemen, externe systemen en netwerkcomponenten worden veilig, beheersbaar, controleerbaar en zo veel mogelijk op basis van gestandaardiseerde koppelingen uitgevoerd.                                                                                                                                                                                                |
| 2.5 | Opdrachtnemer legt in de technische documentatie vast welke netwerkprotocollen, API's, connectoren, agents, poorten, gegevensstromen en applicatiekoppelingen voor de Oplossing worden gebruikt. De gebruikte protocollen en koppelingen zijn actueel, worden versleuteld waar dit technisch mogelijk en passend is en bevatten geen protocollen of versies die algemeen als onveilig of verouderd worden aangemerkt.                                                                                                    |
| 2.6 | De voor de SIEM/SOC-dienstverlening verwerkte en opgeslagen gegevens van Opdrachtgever bevinden zich binnen de Europese Economische Ruimte, tenzij Opdrachtgever vooraf schriftelijk instemt met een afwijking. Deze eis geldt eveneens voor subverwerkers, supportlocaties en aanvullende systemen waarin log-, telemetrie-, incident- of supportgegevens van Opdrachtgever worden verwerkt. Afwijkingen worden vooraf inzichtelijk gemaakt en overeenkomstig de geldende privacy- en beveiligingsafspraken beoordeeld. |
| 2.7 | Door Opdrachtgever geautoriseerde medewerkers hebben rechtstreeks en tijdonafhankelijk toegang tot Microsoft Sentinel en tot de daarin beschikbare loggegevens, beveiligingsmeldingen, incidenten, onderzoeksgegevens, dashboards, rapportages, use-cases, detectieregels en configuraties. Deze toegang ondersteunt ten minste zelfstandig onderzoek, triage, verificatie, analyse en controle door Opdrachtgever.<br><br>Ook zijn de onderzoeken volledig download/exporteerbaar voor eigen opslag.                    |
| 2.8 | Autorisaties binnen de Oplossing zijn persoonsgebonden en worden ingericht volgens de beginselen van least privilege, need-to-know en functiescheiding. Rechten worden periodiek en ten minste jaarlijks beoordeeld. Rechten die niet langer noodzakelijk zijn, worden onverwijld ingetrokken.                                                                                                                                                                                                                           |
| 2.9 | Indien voor de uitvoering van de dienstverlening gebruik wordt gemaakt van een eigen identiteits- of gebruikersadministratie, ondersteunt deze provisioning, wijziging, blokkering en verwijdering van gebruikers via een gestandaardiseerde en beveiligde methode. De actuele status van identiteiten en autorisaties is opvraagbaar voor reconciliatie- en auditdoeleinden.                                                                                                                                            |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.10 | Alle relevante activiteiten van gebruikers, beheerders en serviceaccounts binnen de Oplossing worden vastgelegd in auditlogging. Dit omvat ten minste aanmeldingen, mislukte aanmeldpogingen, zoekopdrachten, exports, configuratiewijzigingen, autorisatiewijzigingen, wijzigingen aan detectieregels en playbooks en uitgevoerde responsacties. De auditlogging is voor geautoriseerde medewerkers van Opdrachtgever controleerbaar.                                                                                                                              |
| 2.11 | Accounts zijn individueel herleidbaar tot één natuurlijke persoon of aantoonbaar toegewezen technisch proces. Het gebruik van gedeelde persoonlijke beheeraccounts is niet toegestaan. Serviceaccounts worden uitsluitend gebruikt voor een vastgelegd technisch doel en worden passend beveiligd, beheerd en gemonitord.                                                                                                                                                                                                                                           |
| 2.12 | Opdrachtgever kan verlangen dat Opdrachtnemer technische informatie, configuratiegegevens, onderzoeksbevindingen en overige relevante gegevens over een beveiligingsincident deelt met Opdrachtgever of met een door Opdrachtgever aangewezen derde. Dit ontslaat Opdrachtnemer niet van de eigen analyse-, onderzoeks-, meldings- en adviesverplichtingen. Het delen vindt plaats via een passend beveiligd communicatiekanaal.                                                                                                                                    |
| 2.13 | Opdrachtnemer realiseert en onderhoudt de benodigde connectoren en koppelingen voor de overeengekomen logbronnen. Indien voor een relevante logbron geen standaardconnector beschikbaar is, adviseert Opdrachtnemer over een passende en beheerbare integratiemethode en implementeert Opdrachtnemer deze na instemming van Opdrachtgever. Klantspecifieke koppelingen worden gedocumenteerd, getest en overdraagbaar ingericht.                                                                                                                                    |
| 2.14 | Voor beveiligingsfuncties en gegevensuitwisseling wordt uitsluitend gebruikgemaakt van actuele, algemeen aanvaarde cryptografische protocollen en algoritmen. Verouderde of aantoonbaar kwetsbare protocollen, algoritmen en sleutelgroottes zijn niet toegestaan. Opdrachtnemer houdt rekening met actuele richtlijnen van bevoegde nationale en Europese autoriteiten en past de inrichting tijdig aan wanneer toegepaste cryptografie niet langer passend wordt geacht.                                                                                          |
| 2.15 | Opdrachtnemer stelt voor de Oplossing een High Level Design en, waar noodzakelijk voor implementatie en beheer, een Low Level Design op. De ontwerpen beschrijven ten minste de architectuur, componenten, gegevensstromen, koppelingen, beveiligingsmaatregelen, autorisaties, beheergrenzen, afhankelijkheden en verantwoordelijkheden. De ontwerpen worden afgestemd met Opdrachtgever, vóór implementatie ter goedkeuring voorgelegd en gedurende de looptijd actueel gehouden. Wijzigingen worden overeenkomstig het overeengekomen wijzigingsproces verwerkt. |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.16 | Microsoft Sentinel wordt ingericht binnen de bestaande Microsoft-tenant van Opdrachtgever. De Sentinel-omgeving, de gemeentelijke gegevens en de klantspecifieke configuraties blijven onder de technische en administratieve zeggenschap van Opdrachtgever.                                                                                                                                                                                                                                                                                                                  |
| 2.17 | De Oplossing ondersteunt correlatie van gebeurtenissen en beveiligingssignalen uit meerdere leveranciers, producten en gegevensbronnen. Correlatie moet ten minste mogelijk zijn tussen identiteits-, endpoint-, server-, netwerk-, e-mail-, cloud-, kwetsbaarheids- en incidentgegevens, voor zover de betreffende bronnen binnen de overeengekomen scope beschikbaar zijn.                                                                                                                                                                                                  |
| 2.18 | De Oplossing ondersteunt patroon-, gedrags- en risico gebaseerde detectie. Opdrachtnemer voert detectie uit op basis van actuele aanvalstechnieken zoals o.a. beschreven in het MITRE ATT&CK framework.                                                                                                                                                                                                                                                                                                                                                                       |
| 2.19 | Opdrachtnemer realiseert en onderhoudt een koppeling tussen Microsoft Sentinel en het SOC voor de registratie en actualisering van relevante beveiligingsincidenten. In de koppeling worden minimaal prioriteit, status, tijdlijn, betrokken identiteiten en assets, analyse, bewijslast en IOC's, impact, genomen acties, aanbevolen vervolgacties en het gevolgde escalatiepad verwerkt, voor zover deze gegevens beschikbaar en noodzakelijk zijn. De precieze gegevensuitwisseling en statussynchronisatie worden tijdens de implementatie met Opdrachtgever vastgesteld. |
| 2.20 | De Oplossing en de bijbehorende SOC-dienstverlening ondersteunen 24 uur per dag en 7 dagen per week de detectie, ontvangst en verwerking van beveiligingsmeldingen. Kritieke en hoge meldingen worden 24/7 overeenkomstig de overeengekomen termijnen getrieerd, geanalyseerd en zo nodig geëscaleerd. De toegepaste personele bezetting en eventuele hybride inzet van automatisering en menselijke analyse moeten aantoonbaar voldoen aan de eisen voor kwaliteit en reactietijd.                                                                                           |
| 2.21 | Opdrachtnemer levert een samenhangend technisch en functioneel ontwerp waarin wordt beschreven hoe Microsoft Sentinel, de SOC-dienstverlening, de aangesloten logbronnen, de gemeentelijke omgeving en eventuele aanvullende tooling gezamenlijk functioneren. Daarbij worden ook de beheergrenzen en verantwoordelijkheden van Opdrachtgever, Opdrachtnemer en betrokken derden inzichtelijk gemaakt.                                                                                                                                                                        |
| 2.22 | Opdrachtnemer adviseert Opdrachtgever bij het prioriteren en aansluiten van logbronnen en bij het definiëren, implementeren en doorontwikkelen van use-cases en detectieregels. Hierbij houdt Opdrachtnemer rekening met risico,                                                                                                                                                                                                                                                                                                                                              |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | detectiewaarde, beschikbare gegevens, privacy, gegevensvolume, kosten, beheerinspanning en behandelcapaciteit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 2.23 | Opdrachtgever blijft eigenaar van de gegevens, use-cases, klantspecifieke detectieregels, rapportagesjablonen, connectorconfiguraties, playbooks, workbooks, dashboards en overige klantspecifieke configuraties die binnen de omgeving van Opdrachtgever worden gerealiseerd. Opdrachtgever behoudt permanent rechtstreeks toegang tot deze onderdelen. Voor reeds bestaande generieke intellectuele eigendomsrechten van Opdrachtnemer wordt aan Opdrachtgever ten minste een toereikend gebruiksrecht verleend voor de uitvoering, continuïteit en overdracht van de dienstverlening. |
| 2.24 | De eisen aan monitoring, triage, incidentafhandeling, rapportage, beheer, continuïteit en ondersteuning zijn opgenomen in de daaropvolgende hoofdstukken van dit Programma van Eisen. Deze eisen maken onverkort deel uit van de aangeboden Oplossing en dienstverlening.                                                                                                                                                                                                                                                                                                                |
| 2.25 | De Oplossing is plaats- en tijdonafhankelijk toegankelijk voor daartoe geautoriseerde medewerkers van Opdrachtgever. Toegang vindt plaats via een beveiligde verbinding en is voorzien van multifactor-authenticatie.                                                                                                                                                                                                                                                                                                                                                                    |
| 2.26 | Gegevens van Opdrachtgever zijn technisch en logisch gescheiden van gegevens van andere klanten van Opdrachtnemer. Andere klanten, gebruikers of onbevoegde medewerkers kunnen geen toegang krijgen tot gegevens, zoekresultaten, incidentinformatie, configuraties of rapportages van Opdrachtgever.                                                                                                                                                                                                                                                                                    |
| 2.27 | Opdrachtnemer gebruikt gegevens van Opdrachtgever uitsluitend voor de uitvoering van de Overeenkomst. Gegevens worden niet verkocht, gedeeld of voor eigen commerciële doeleinden, profilering of training van AI-modellen gebruikt. Verstrekking aan derden vindt uitsluitend plaats wanneer dit vooraf is geaccordeerd door Opdrachtgever, noodzakelijk is voor de dienstverlening, contractueel is toegestaan en voldoet aan de overeengekomen privacy- en beveiligingsvoorwaarden.                                                                                                   |
| 2.28 | Gegevens die binnen de verantwoordelijkheid van Opdrachtnemer worden opgeslagen, worden versleuteld met actuele en algemeen aanvaarde cryptografische technieken. Sleutelbeheer wordt passend ingericht en toegang tot sleutels is beperkt tot daartoe bevoegde personen en processen.                                                                                                                                                                                                                                                                                                   |
| 2.29 | Gegevens die tussen Opdrachtgever, Opdrachtnemer, Microsoft Sentinel, logbronnen, supportvoorzieningen en overige gekoppelde systemen worden uitgewisseld, worden tijdens transport versleuteld met actuele en algemeen aanvaarde cryptografische technieken.                                                                                                                                                                                                                                                                                                                            |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.30 | Opdrachtnemer borgt de continuïteit van de door Opdrachtnemer geleverde onderdelen van de SIEM/SOC-dienstverlening. Opdrachtnemer stelt vóór ingebruikname een continuïteitsplan, een herstelplan en een exitplan beschikbaar. Deze plannen beschrijven ten minste uitvalscenario's, herstelprocedures, verantwoordelijkheden, communicatie, gegevensoverdracht, kennisoverdracht en ondersteuning bij een eventuele overgang naar Opdrachtgever of een opvolgende leverancier.                                                                                               |
| 2.31 | Opdrachtnemer zorgt ervoor dat medewerkers die voor de uitvoering van de Opdracht worden ingezet beschikken over aantoonbaar actuele kennis en, waar relevant, passende certificeringen voor de toegewezen werkzaamheden. Opdrachtnemer onderhoudt deze kennis gedurende de looptijd door middel van opleiding, training en periodieke bijscholing. Op verzoek verstrekt Opdrachtnemer een geactualiseerd overzicht van relevante rollen, deskundigheid en certificeringen, zonder onnodige persoonsgegevens te delen.                                                        |
| 2.32 | Opdrachtnemer implementeert, onderhoudt, test, documenteert en optimaliseert de voor Opdrachtgever ingerichte use-cases en detectieregels. Dit omvat ten minste het configureren van detecties, het integreren van benodigde gegevensbronnen, het valideren van detectieresultaten, het verminderen van false positives en het ontwikkelen, testen en onderhouden van bijbehorende playbooks. Klantspecifieke use-cases worden in samenwerking met het securityteam van Opdrachtgever opgesteld en uitsluitend na de overeengekomen test en autorisatie in productie genomen. |

### 3 Implementatie

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1 | Opdrachtnemer is eindverantwoordelijk voor de volledige en samenhangende implementatie van de aangeboden SIEM/SOC-dienstverlening en fungeert gedurende de implementatie als centraal aanspreekpunt voor Opdrachtgever. Opdrachtnemer stuurt de eigen medewerkers, onderaannemers en betrokken partners aan en coördineert de technische en organisatorische afstemming met de door Opdrachtgever aangewezen interne en externe partijen.                                                                                                                                                                                                                                                                                                                                                    |
| 3.2 | Opdrachtnemer verzorgt tijdens de implementatie passende opleiding, instructie en begeleiding voor de door Opdrachtgever aangewezen security-, beheer- en regiemedewerkers. De opleiding sluit aan op de feitelijke inrichting, rollen en bevoegdheden en behandelt ten minste het gebruik van Microsoft Sentinel, de beschikbare dashboards en rapportages, het raadplegen en onderzoeken van meldingen en incidenten, zoek- en exportmogelijkheden, escalatieprocedures, responsmandaten en kostenbewaking.                                                                                                                                                                                                                                                                                |
| 3.3 | Opdrachtnemer rondt de initiële implementatie af binnen de in het geaccepteerde implementatieplan vastgelegde termijn en zorgt ervoor dat de SIEM/SOC-dienstverlening uiterlijk op <b>1 maart 2027</b> operationeel in gebruik kan worden genomen. Bij de initiële oplevering zijn minimaal de overeengekomen essentiële logbronnen aangesloten en zijn de vijf initiële use-cases geïmplementeerd, getest, gedocumenteerd en door Opdrachtgever geaccepteerd. Deze verplichting geldt onder de voorwaarde dat Opdrachtgever en betrokken derden de vooraf overeengekomen informatie, toegangen, besluiten en medewerking tijdig beschikbaar stellen. Opdrachtnemer meldt iedere dreigende afwijking van de planning direct, inclusief oorzaak, gevolgen en voorgestelde beheersmaatregelen. |
| 3.4 | Opdrachtnemer verleent per contractjaar kosteloos medewerking aan maximaal twee reguliere audits die door of namens Opdrachtgever worden uitgevoerd. Dit laat wettelijke auditrechten en incidentele toetsingen naar aanleiding van calamiteiten, beveiligingsincidenten, substantiële wijzigingen of compliance verzoeken onverlet. Opdrachtnemer verstrekt binnen een redelijke termijn de benodigde informatie en medewerking, voor zover de audit betrekking heeft op de uitvoering van de Opdracht.                                                                                                                                                                                                                                                                                     |
| 3.5 | Opdrachtnemer beschrijft in het implementatieplan de activiteiten, benodigde capaciteit, verantwoordelijkheden en afhankelijkheden van Opdrachtnemer, Opdrachtgever en betrokken derden. De taakverdeling moet doelmatig en proportioneel zijn en aansluiten op de kennis, bevoegdheden en technische                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>mogelijkheden van de betrokken partijen. Opdrachtnemer blijft verantwoordelijk voor de regie op de implementatie en mag werkzaamheden niet zonder voorafgaande afstemming bij Opdrachtgever neerleggen.</p> <p>Configuratiewerkzaamheden aan gemeentelijke systemen worden uitgevoerd door Opdrachtgever of de betreffende IT-dienstverlener wanneer Opdrachtnemer daartoe geen toegang of bevoegdheid heeft. Opdrachtnemer verstrekt hiervoor tijdig volledige en uitvoerbare instructies en ondersteunt de betrokken partij bij de uitvoering en validatie.</p> |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 4 Documentatie, processen en communicatie

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.1 | Strategische, tactische en formele communicatie tussen Opdrachtnemer en Opdrachtgever vindt plaats in het Nederlands. Dit geldt tevens voor incidentmeldingen, adviezen, rapportages, verslagen en procedurele documentatie. Operationele communicatie mag, na instemming van Opdrachtgever, in het Engels plaatsvinden wanneer specialistische technische ondersteuning dit noodzakelijk maakt.                                                                                                                                                                                                                                                                                                                                                                                       |
| 4.2 | De aangeboden SIEM/SOC-dienstverlening ondersteunt 24 uur per dag en 7 dagen per week de detectie, ontvangst en verwerking van beveiligingsmeldingen. Kritieke en hoge meldingen worden 24/7 overeenkomstig de overeengekomen termijnen getrieerd, geanalyseerd en zo nodig geëscaleerd.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 4.3 | De eisen aan de bereikbaarheid, beschikbaarheid, triage, analyse, melding en escalatie van beveiligingsincidenten zijn opgenomen in hoofdstuk 8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 4.4 | De eisen aan de rapportages, overlegstructuren, evaluaties en managementinformatie zijn opgenomen in hoofdstuk 8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 4.5 | Opdrachtnemer verzorgt de schriftelijke verslaglegging van projectmatige, tactische en strategische overleggen en verstrekt het conceptverslag uiterlijk binnen vijf werkdagen na het overleg digitaal aan Opdrachtgever. Voor operationele overleggen kan worden volstaan met een actie- en besluitenlijst. Opdrachtgever kan binnen vijf werkdagen na ontvangst correcties of aanvullingen doorgeven. Na verwerking daarvan stelt Opdrachtnemer het verslag definitief vast.                                                                                                                                                                                                                                                                                                         |
| 4.6 | De eisen aan het beheer, de optimalisatie en de doorontwikkeling van use-cases, detectieregels en playbooks zijn opgenomen in hoofdstuk 8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 4.7 | Een door het SOC over te dragen beveiligingsincident wordt via email/telefonisch overgedragen en wordt in een door de gemeente toegankelijk portal geregistreerd. De registratie bevat, voor zover beschikbaar en relevant, minimaal: prioriteit en classificatie; datum en tijd van detectie, triage en escalatie; betrokken IP-adressen, identiteiten, accounts, assets, systemen en locaties; een tijdlijn; een beschrijving van de waarneming en uitgevoerde analyse; beschikbare bewijslast en Indicators of Compromise; de mogelijke en vastgestelde impact; reeds uitgevoerde acties; aanbevolen vervolgacties; het gevolgde escalatiepad; de risico's van voorgestelde mitigerende maatregelen; en het resterende risico. Persoonsgegevens en andere gevoelige gegevens worden |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | uitsluitend opgenomen voor zover dit noodzakelijk is voor de analyse en afhandeling van het incident.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 4.8  | Opdrachtnemer registreert, onderzoekt en reduceert false positives door middel van structurele tuning van detectieregels, use-cases, drempelwaarden en gegevensverrijking. De vermindering van false positives mag niet leiden tot een ongecontroleerde of onbedoelde afname van de overeengekomen detectiedekking. Wijzigingen worden getest, gedocumenteerd en overeenkomstig het afgesproken wijzigingsproces doorgevoerd.                                                                                                                                                              |
| 4.9  | Planbaar preventief onderhoud wordt vooraf afgestemd met Opdrachtgever en vindt plaats binnen een overeengekomen onderhoudsvenster. Opdrachtnemer kondigt planbaar onderhoud minimaal vier weken vooraf aan, tenzij een kortere termijn noodzakelijk is vanwege een urgent beveiligingsrisico of een wijziging van een onderliggende clouddienst. Onderhoud met mogelijke impact op kritieke onderdelen van de dienstverlening wordt zoveel mogelijk buiten de reguliere kantoortijden van Opdrachtgever uitgevoerd.                                                                       |
| 4.10 | Opdrachtgever mag, na voorafgaande afstemming over doel, scope, methode en tijdstip, kwetsbaarhedenanalyses en penetratietesten uitvoeren of laten uitvoeren op de onderdelen van de Oplossing waarvoor Opdrachtnemer verantwoordelijk is. De uitvoering mag de dienstverlening aan Opdrachtgever of andere klanten niet onevenredig verstoren. Opdrachtnemer verleent medewerking aan de uitvoering en opvolging van de bevindingen. Beperkingen die voortvloeien uit voorwaarden van Microsoft of andere betrokken platformleveranciers worden vooraf inzichtelijk gemaakt.              |
| 4.11 | Opdrachtnemer implementeert voor Opdrachtgever een actueel en overzichtelijk dashboard waarin de werking en resultaten van de SIEM/SOC-dienstverlening inzichtelijk zijn. Het dashboard toont ten minste aantallen en trends van beveiligingsmeldingen en incidenten, verdeling naar prioriteit en status, resultaten van use-cases, prestaties ten opzichte van de SLA, bron- en connectorgezondheid, false positives, detectiewijzigingen en relevante ontwikkelingen in het dreigingsbeeld. Geautoriseerde medewerkers van Opdrachtgever hebben rechtstreeks toegang tot het dashboard. |
| 4.12 | Opdrachtnemer beschikt over voldoende gekwalificeerde capaciteit om bij kritieke en hoge beveiligingsincidenten tijdig aanvullende analyse en ondersteuning te leveren. De beschikbaarheid, starttermijnen, reikwijdte en eventuele kosten van specialistische incidentresponse worden vastgelegd in de SLA en het Prijzenblad. Inzet op locatie vindt uitsluitend plaats wanneer dit afzonderlijk is overeengekomen of door Opdrachtgever als optionele dienstverlening wordt afgenomen.                                                                                                  |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.13 | Opdrachtnemer is verantwoordelijk voor lifecycle-, patch- en kwetsbaarheidsbeheer van alle componenten die door Opdrachtnemer worden geleverd of beheerd. Opdrachtnemer houdt deze componenten gedurende de looptijd ondersteund, actueel en veilig. Opdrachtnemer informeert Opdrachtgever tijdig over relevante updates, upgrades, kwetsbaarheden, end-of-life- of end-of-supportdata en wijzigingen met mogelijke gevolgen voor de beschikbaarheid, beveiliging, werking of kosten van de dienstverlening.                                         |
| 4.14 | Opdrachtnemer informeert Opdrachtgever onverwijld wanneer actuele dreigingsinformatie, early warnings of Indicators of Compromise wijzen op een concrete of aannemelijke dreiging voor Opdrachtgever, Nederlandse gemeenten, de gebruikte technologieën of de relevante leveranciersketen. Opdrachtnemer beoordeelt de mogelijke relevantie en impact en adviseert Opdrachtgever over passende detectie- en mitigerende maatregelen.                                                                                                                  |
| 4.15 | Opdrachtnemer borgt gedurende de looptijd de beschikbaarheid en overdracht aan opdrachtgever van relevante domeinspecifieke, technische, organisatorische en procesmatige kennis. Kennisdeling omvat ten minste actuele dreigingen, aanvalstechnieken, Microsoft Sentinel, detectie-engineering, incidentanalyse, rapportage, beheer en relevante ontwikkelingen in de dienstverlening. De wijze, frequentie en doelgroepen van de kennisoverdracht worden vastgelegd in het DAP.                                                                     |
| 4.16 | Opdrachtnemer levert uiterlijk vier weken na de start van de implementatie een eerste volledige versie van het Dossier Afspraken en Procedures. Het DAP moet vóór ingebruikname door beide partijen zijn vastgesteld. Dit geldt onder de voorwaarde dat Opdrachtgever de benodigde informatie en besluiten tijdig beschikbaar stelt. Opdrachtnemer is gedurende de looptijd penvoerder van het DAP en houdt het document actueel. Wijzigingen worden in overleg met Opdrachtgever vastgesteld.                                                        |
| 4.17 | Opdrachtnemer richt een aantoonbaar proces in voor tijdige triage, analyse, classificatie, melding en escalatie van beveiligingsincidenten. Waar beschikbare early warnings, threat intelligence of Indicators of Compromise daartoe aanleiding geven, handelt Opdrachtnemer proactief door relevante detecties te controleren of aan te passen en Opdrachtgever te adviseren over mitigerende maatregelen. Responsacties in de gemeentelijke omgeving worden uitsluitend uitgevoerd binnen vooraf schriftelijk vastgelegde bevoegdheden en mandaten. |
| 4.18 | Opdrachtnemer rapporteert op een duidelijke en voor de betreffende doelgroep begrijpelijke wijze. Operationele informatie wordt beschikbaar gesteld aan het security- en beheerteam via dashboards, incidentregistraties en operationele rapportages. Tactische en strategische rapportages bevatten passende duiding                                                                                                                                                                                                                                 |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | van trends, risico's, prestaties, kostenontwikkeling en verbetermogelijkheden en zijn bruikbaar voor management- en verantwoordingsdoeleinden.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 4.19 | Opdrachtnemer gebruikt Microsoft Sentinel binnen de Microsoft-tenant van Opdrachtgever als centraal platform voor beveiligingsmonitoring, correlatie, onderzoek en incidentregistratie. Aanvullende applicaties, rapportagevoorzieningen of BI-functionaliteiten mogen worden gebruikt wanneer deze aantoonbare meerwaarde bieden en geen afbreuk doen aan de toegang, zeggenschap, beveiliging, performance, overdraagbaarheid en gegevensbescherming van Opdrachtgever. Alle klantspecifieke configuraties en relevante gegevens blijven rechtstreeks toegankelijk voor Opdrachtgever. |

## 5 Prijsmodel

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.1 | Het ingevulde prijzenblad geeft een volledig overzicht van de totale kosten van de Inschrijving en maakt de totale kosten van de SIEM/SOC-dienstverlening over de initiële contractduur van vier jaar inzichtelijk. Alle eenmalige, periodieke en variabele kosten die noodzakelijk zijn voor het uitvoeren van de Opdracht worden in het Prijzenblad opgenomen. Dit omvat ten minste de kosten voor implementatie, inrichting, aansluiting van de initiële logbronnen, realisatie van de vijf initiële use-cases, SOC-dienstverlening, beheer, rapportage, ondersteuning, kennisoverdracht en de overige aangeboden prestaties. |
| 5.2 | Inschrijver vult het prijzenblad volledig en overeenkomstig de daarin opgenomen instructies in. Alle gevraagde prijscomponenten, eenheidsprijzen, hoeveelheden, toelichtingen en aannames worden ingevuld. Indien een onderdeel niet van toepassing is of zonder afzonderlijke kosten wordt aangeboden, vermeldt Inschrijver uitdrukkelijk 'niet van toepassing' respectievelijk € 0,00. Het niet volledig invullen of ongeoorloofd aanpassen van het Prijzenblad kan leiden tot ongeldigheid van de Inschrijving.                                                                                                               |
| 5.3 | De aangeboden prijzen en tarieven zijn vast tot het moment waarop indexering overeenkomstig de Overeenkomst is toegestaan. Indexering kan eenmaal per kalenderjaar plaatsvinden volgens de indexeringsbepaling en het objectieve prijsindexcijfer zoals opgenomen in de Overeenkomst. De eerste indexering mag plaatsvinden op <b>1 januari 2028</b> . Opdrachtnemer dient een voorgenomen indexering tijdig schriftelijk en met een controleerbare berekening aan Opdrachtgever voor te leggen. Indexering wordt uitsluitend toegepast na schriftelijke instemming van Opdrachtgever.                                           |
| 5.4 | Indien Opdrachtgever gebruik maakt van een verlengingsoptie, blijven de laatst geldende prijzen en tarieven van toepassing, met inachtneming van de toegestane jaarlijkse indexering. Opdrachtnemer mag vanwege het enkele feit dat de Overeenkomst wordt verlengd geen aanvullende toeslagen, implementatiekosten of andere prijsaanpassingen in rekening brengen.                                                                                                                                                                                                                                                              |
| 5.5 | Voor prijscomponenten die afhankelijk zijn van volumes of gebruik, vermeldt Inschrijver de gehanteerde eenheid, het bijbehorende tarief en alle aannames die aan het tarief ten grondslag liggen. Dit geldt onder meer voor logvolume, gegevensinname, retentie, aanvullende logbronnen, aanvullende use-cases, aanvullende ondersteuning en overige variabele dienstverlening. De relatie tussen de gehanteerde eenheid, de opgegeven kengetallen en het tarief moet duidelijk en controleerbaar zijn.                                                                                                                          |

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.6  | De implementatie wordt aangeboden tegen een vaste prijs. Deze vaste prijs omvat alle werkzaamheden die noodzakelijk zijn om de overeengekomen initiële implementatiescope volledig, werkend en geaccepteerd op te leveren. Daaronder vallen ten minste projectmanagement, ontwerp, inrichting, configuratie van Microsoft Sentinel, aansluiting van de overeengekomen initiële logbronnen, implementatie en acceptatie van de vijf initiële use-cases, inrichting van de SOC-dienstverlening, documentatie, opleiding, testen, herstel van bevindingen en ondersteuning tijdens de stabilisatieperiode. |
| 5.7  | De totale implementatiekosten bedragen maximaal €15.000 euro. Kosten die naar hun aard behoren tot de structurele dienstverlening mogen niet uitsluitend of onevenredig als implementatiekosten worden opgevoerd.                                                                                                                                                                                                                                                                                                                                                                                       |
| 5.8  | Opdrachtnemer verleent bij beëindiging van de Overeenkomst medewerking aan de overdracht en re-transitie overeenkomstig het Exitplan. Het opstellen, actueel houden en regulier uitvoeren van het Exitplan, waaronder documentatie, gegevensoverdracht en reguliere kennisoverdracht, is inbegrepen in de aangeboden prijzen. Alleen aantoonbare aanvullende werkzaamheden die buiten de overeengekomen exit verplichtingen vallen, kunnen na voorafgaande schriftelijke opdracht van Opdrachtgever als meerwerk in rekening worden gebracht tegen de overeengekomen tarieven.                          |
| 5.9  | Alle kosten die noodzakelijk zijn om aan de eisen van de aanbestedingsdocumenten en de door Inschrijver aangeboden prestaties te voldoen, worden geacht in de aangeboden prijzen te zijn inbegrepen, tenzij het Prijzenblad een onderdeel uitdrukkelijk als afzonderlijke of optionele prijscomponent aanwijst. Kosten die niet in het Prijzenblad zijn vermeld, kunnen niet aanvullend aan Opdrachtgever in rekening worden gebracht.                                                                                                                                                                  |
| 5.10 | Meerwerk wordt uitsluitend uitgevoerd en in rekening gebracht nadat Opdrachtgever hiervoor vooraf schriftelijk opdracht heeft verstrekt. Een voorstel voor meerwerk bevat ten minste een omschrijving van de werkzaamheden, de aanleiding, het beoogde resultaat, de benodigde inzet, de doorlooptijd, de gehanteerde tarieven en de totale verwachte kosten. Werkzaamheden die nodig zijn om een fout, tekortkoming of onvolledigheid van Opdrachtnemer te herstellen, gelden niet als meerwerk.                                                                                                       |

## 6 Privacy & Security

| Nr. | Omschrijving |
|-----|--------------|
|-----|--------------|

|     |                                                                                                                                                                                                                                                                                                                                                                                    |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.1 | Persoonsgegevens en overige gemeentelijke gegevens blijven onder de zeggenschap van Opdrachtgever. Opdrachtnemer verwerkt deze uitsluitend voor de uitvoering van de Overeenkomst, conform de instructies van Opdrachtgever en de Verwerkersovereenkomst.                                                                                                                          |
| 6.2 | Opdrachtnemer gebruikt gemeentelijke gegevens, waaronder loggegevens, telemetrie, incidentinformatie en false positives, niet voor commerciële doeleinden, profilering of training van AI-modellen. Gebruik van volledig geanonimiseerde informatie voor verbetering van de dienstverlening is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever. |
| 6.3 | Opdrachtgever blijft eigenaar van alle klantspecifieke instellingen, configuraties, use-cases, detectieregels, queries, playbooks, dashboards, rapportages en documentatie. Voor generieke componenten van Opdrachtnemer ontvangt Opdrachtgever een toereikend gebruiksrecht voor continuïteit en overdracht van de dienstverlening.                                               |
| 6.4 | Opdrachtnemer houdt wijzigingen en versies van klantspecifieke detectieregels, queries, drempelwaarden, use-cases, playbooks en overige automatiseringslogica aantoonbaar bij. De versiehistorie vermeldt minimaal de wijziging, datum, aanleiding, uitgevoerde test en autorisatie. Opdrachtgever heeft toegang tot deze versiehistorie.                                          |
| 6.5 | Opdrachtnemer past aantoonbaar Security by Design, Privacy by Design en Privacy by Default toe. Wijzigingen met gevolgen voor gegevensverwerking, autorisaties, beveiliging, datastromen of retentie worden vooraf afgestemd met de door Opdrachtgever aangewezen security-, privacy- en architectuurfunctionarissen.                                                              |
| 6.6 | Opdrachtnemer beperkt de verwerking van persoonsgegevens en gevoelige gegevens tot wat noodzakelijk is voor de dienstverlening. Waar mogelijk worden filtering, masking, pseudonimisering of uitsluiting van niet-noodzakelijke gegevens toegepast, zonder de overeengekomen detectiedekking te beperken.                                                                          |
| 6.7 | Incidentinformatie, loggegevens, bewijslast, IoC's en persoonsgegevens worden uitsluitend gedeeld via door Opdrachtgever goedgekeurde systemen en beveiligde communicatiekanalen.                                                                                                                                                                                                  |
| 6.8 | Voorafgaand aan de inzet van AI-functionaliteit informeert Opdrachtnemer Opdrachtgever over het doel, het gebruikte model, de verwerkte gegevens, gegevenslocaties, betrokken subverwerkers, risico's en menselijke controle. Al waarbij gemeentelijke gegevens worden verwerkt, wordt uitsluitend ingezet na voorafgaande schriftelijke toestemming van Opdrachtgever.            |

|      |                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.9  | Uitkomsten van AI, machine learning of andere geautomatiseerde analyses worden vóór escalatie of uitvoering van een responsactie beoordeeld door een gekwalificeerde medewerker, tenzij voor de betreffende actie vooraf schriftelijk mandaat is verleend.                                                      |
| 6.10 | Opdrachtnemer meldt een vastgestelde of vermoedelijke ongeoorloofde verwerking, toegang, verstrekking, wijziging, vernietiging of verlies van gemeentelijke gegevens onverwijld aan Opdrachtgever. De melding bevat de beschikbare informatie over aard, omvang, impact en genomen of voorgestelde maatregelen. |

## 7 Re-transitie en Exitplan

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                               |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.1 | Gedurende de re-transitie zet Opdrachtnemer de dienstverlening voort tegen de geldende voorwaarden, tarieven en serviceniveaus.                                                                                                                                                                                                            |
| 7.2 | Opdrachtnemer levert uiterlijk zes maanden voor het einde van de Overeenkomst een actueel overzicht van alle voor overdracht relevante gegevens, configuraties, koppelingen, use-cases, detectieregels, playbooks, documentatie, incidenten en afhankelijkheden. Bij eerdere beëindiging wordt dit overzicht zo spoedig mogelijk geleverd. |
| 7.3 | Opdrachtnemer verleent volledige medewerking aan overdracht van de dienstverlening aan Opdrachtgever of een opvolgende leverancier. Gemeentelijke gegevens, configuraties en documentatie worden volledig en in een gangbaar, bruikbaar formaat overgedragen.                                                                              |
| 7.4 | Na schriftelijke acceptatie van de overdracht trekt Opdrachtnemer alle niet langer noodzakelijke toegangen en koppelingen in en verwijdert Opdrachtnemer alle gemeentelijke gegevens buiten de door Opdrachtgever beheerde omgevingen. Opdrachtnemer verstrekt hiervan een vernietigingsverklaring.                                        |
| 7.5 | Opdrachtnemer levert vóór ingebruikname een Exitplan en houdt dit gedurende de Overeenkomst actueel. Het Exitplan beschrijft minimaal de planning, verantwoordelijkheden, gegevens- en kennisoverdracht, overdracht van openstaande incidenten, intrekking van toegangen en verwijdering van gegevens.                                     |
| 7.6 | Opdrachtnemer richt de dienstverlening overdraagbaar in en voorkomt onnodige leveranciersafhankelijkheid.                                                                                                                                                                                                                                  |
| 7.7 | Reguliere exit werkzaamheden zijn inbegrepen in de aangeboden prijzen. Aanvullende werkzaamheden worden alleen na voorafgaande schriftelijke opdracht als meerwerk uitgevoerd.                                                                                                                                                             |

## 8 SLA en dienstverlening

| Nr. | Omschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.1 | Opdrachtnemer stelt na gunning samen met Opdrachtgever de SLA op, binnen de kaders van het Programma van Eisen, de Inschrijving en de Overeenkomst. De SLA wordt vóór ingebruikname vastgesteld en bevat ten minste de servicevensters, prioriteiten, meetpunten, triage-, meld- en escalatietermijnen, beschikbaarheid, rapportages, onderhoud, overlegstructuren en escalatieprocedures. Opdrachtnemer is penvoerder van de SLA en houdt deze gedurende de looptijd actueel.<br>Een concept SLA dient te worden bijgevoegd bij de inschrijving.                                                                                                                                                                                                                |
| 8.2 | Opdrachtnemer ondersteunt de overeengekomen dienstverlening gedurende de volledige looptijd van de Overeenkomst, inclusief de verlengingsopties. Opdrachtnemer informeert Opdrachtgever minimaal twee maanden vooraf over wijzigingen of het vervallen van functionaliteit, tenzij een kortere termijn wordt veroorzaakt door Microsoft, een beveiligingsrisico of een andere niet door Opdrachtnemer beïnvloedbare omstandigheid. Opdrachtnemer beschrijft de gevolgen en adviseert over passende alternatieven of mitigerende maatregelen.                                                                                                                                                                                                                     |
| 8.3 | Updates en wijzigingen mogen niet leiden tot een ongecontroleerde vermindering van de overeengekomen functionaliteit, detectiedekking, beveiliging of dienstverlening. Opdrachtnemer test relevante wijzigingen vooraf waar dit technisch mogelijk is en legt de resultaten, risico's en herstelmaatregelen vast. Indien voortzetting van een eerdere versie technisch niet mogelijk is, stelt Opdrachtnemer samen met Opdrachtgever passende vervangende maatregelen vast.                                                                                                                                                                                                                                                                                      |
| 8.4 | Opdrachtnemer levert maandelijks een operationele rapportage en per kwartaal een tactische rapportage. De rapportages bevatten ten minste informatie over incidenten, prioriteiten, triage- en meldtijden, SLA-prestaties, use-cases, detectiewijzigingen, false positives, bron- en connectorgezondheid, uitgevoerde wijzigingen, trends, relevante dreigingen, gegevensverbruik, kostenontwikkeling en verbeteradviezen.                                                                                                                                                                                                                                                                                                                                       |
| 8.5 | De servicedesk van Opdrachtnemer is op werkdagen minimaal van 08.00 tot 18.00 uur telefonisch en digitaal bereikbaar. Voor kritieke en hoge beveiligingsincidenten is 24/7 ondersteuning beschikbaar overeenkomstig de termijnen uit dit hoofdstuk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 8.6 | Opdrachtnemer garandeert een beschikbaarheid van minimaal 99,9% per kalendermaand voor de door Opdrachtnemer beheerde onderdelen van de SIEM/SOC-dienstverlening. Hieronder vallen minimaal de operationele monitoring, incidentverwerking, escalatie en bereikbaarheid van het SOC. 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.<br>Opdrachtnemer monitort actief de beschikbaarheid, volledigheid en actualiteit van aangesloten logbronnen. Uitval van kritieke logstromen/logbronnen wordt binnen één uur gedetecteerd, geregistreerd en gemeld aan Opdrachtgever. |

|      |                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.7  | Opdrachtnemer werkt mee aan het opstellen en onderhouden van een escalatiematrix. Deze bevat minimaal vier escalatieniveaus, de bijbehorende contactpersonen en vervangers, bereikbaarheid, verantwoordelijkheden, communicatiemiddelen en criteria voor opschaling. De escalatiematrix wordt opgenomen in de SLA en het DAP.                                                                                 |
| 8.8  | Indien in een kalendermaand een overeengekomen servicenorm niet wordt behaald, initieert Opdrachtnemer een overleg op escalatieniveau 2. Opdrachtnemer licht de oorzaak toe en legt de afgesproken acties en besluiten schriftelijk vast.                                                                                                                                                                     |
| 8.9  | Indien dezelfde of een vergelijkbare servicenorm gedurende twee achtereenvolgende kalendermaanden niet wordt behaald, initieert Opdrachtnemer een overleg op escalatieniveau 3. Opdrachtnemer levert daarbij een verbeterplan met oorzaakanalyse, maatregelen, verantwoordelijken en termijnen. Het overleg en het verbeterplan vinden uiterlijk binnen één kalendermaand na de tweede overschrijding plaats. |
| 8.10 | Opdrachtnemer initieert een overleg op escalatieniveau 4 indien overeengekomen verbetermaatregelen niet tijdig worden uitgevoerd, een verbeterplan onvoldoende resultaat oplevert of sprake is van een ernstige of structurele tekortkoming.                                                                                                                                                                  |
| 8.11 | Opdrachtnemer voert minimaal 95% van de vooraf overeengekomen en door Opdrachtgever geautoriseerde wijzigingen en updates in één keer correct uit. Herstelwerkzaamheden als gevolg van een fout van Opdrachtnemer worden niet als afzonderlijke succesvolle wijziging aangemerkt en niet als meerwerk in rekening gebracht.                                                                                   |
| 8.12 | Opdrachtgever mag een beveiligingsmelding of incident gemotiveerd laten herclassificeren naar een hogere prioriteit. Bij een aantoonbaar kritieke dreiging mag Opdrachtgever een onmiddellijke hogere prioriteit verlangen. Opdrachtnemer past vanaf het moment van herclassificatie de bijbehorende termijnen en escalatieprocedure toe.                                                                     |
| 8.13 | Opdrachtnemer meldt minimaal 95% van de door Opdrachtnemer als beveiligingsincident geclassificeerde meldingen binnen de voor de betreffende prioriteit geldende meldtijd aan Opdrachtgever.                                                                                                                                                                                                                  |
| 8.14 | Opdrachtnemer levert voor minimaal 95% van de beveiligingsincidenten 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.                                                    |
| 8.15 | Opdrachtnemer verstrekt uiterlijk 1 november van ieder kalenderjaar een releasekalender voor het daaropvolgende jaar met de op dat moment bekende geplande releases en wijzigingen die invloed kunnen hebben op de dienstverlening.                                                                                                                                                                           |
| 8.16 | Opdrachtnemer verstrekt uiterlijk 1 november van ieder kalenderjaar een onderhoudskalender voor het daaropvolgende jaar. Aanvullend planbaar preventief onderhoud wordt minimaal vier weken vooraf aangekondigd. Urgent beveiligingsonderhoud wordt zo spoedig mogelijk met Opdrachtgever afgestemd.                                                                                                          |

|      |                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.17 | Opdrachtnemer levert bijgewerkte technische, functionele en procesdocumentatie uiterlijk binnen vijf werkdagen na implementatie van een relevante wijziging op.                                                                                                                                                                 |
| 8.18 | Eenmaal per kwartaal vindt een operationeel overleg plaats tussen Opdrachtgever en Opdrachtnemer. Hierin worden minimaal incidenten, SLA-prestaties, brongezondheid, false positives, wijzigingen, openstaande acties en de dagelijkse samenwerking besproken.                                                                  |
| 8.19 | Tweemaal per jaar vindt een tactisch overleg plaats. Hierin worden minimaal de geleverde prestaties, trends, risico's, kostenontwikkeling, verbeterplannen, capaciteit, use-caseontwikkeling en noodzakelijke wijzigingen in de SLA of het DAP besproken.                                                                       |
| 8.20 | Eenmaal per jaar vindt een strategisch overleg plaats. Dit overleg richt zich op de langetermijnontwikkeling van de dienstverlening, relevante dreigingen, innovatie, contractuele samenwerking, roadmap, budget en digitale weerbaarheid van Opdrachtgever.                                                                    |
| 8.21 | Op verzoek van Opdrachtgever verzorgt Opdrachtnemer maximaal tweemaal per jaar kosteloos een technische, innovatie-, informatie- of adviessessie. Deze sessies zijn gericht op relevante marktontwikkelingen, nieuwe dreigingen, aanvullende use-cases, technologie, kostenoptimalisatie of verbetering van de dienstverlening. |
| 8.22 | Opdrachtnemer werkt na gunning mee aan het opstellen van een RACI-matrix voor de uitvoering en het beheer van de SIEM/SOC-dienstverlening. De matrix wordt vóór ingebruikname vastgesteld, opgenomen in het DAP en gedurende de looptijd actueel gehouden.                                                                      |

## 9 Bijlages

### 9.1 Richtinggevende escalatiematrix bij eis 8.7

| Escalatieniveau | Aanleiding                                       | Vertegenwoordiging<br>Opdrachtgever               | Vertegenwoordiging<br>Opdrachtnemer          |
|-----------------|--------------------------------------------------|---------------------------------------------------|----------------------------------------------|
| <b>1</b>        | Reguliere operationele afstemming                | Operationeel verantwoordelijke                    | Operationeel verantwoordelijke               |
| <b>2</b>        | Eenmalige SLA-afwijking of operationeel knelpunt | Operationeel verantwoordelijke en contractmanager | Operationeel verantwoordelijke               |
| <b>3</b>        | Herhaalde afwijking of onvoldoende verbetering   | Contractmanager en contracteigenaar               | Operationeel verantwoordelijke en teamleider |
| <b>4</b>        | Ernstige of structurele tekortkoming             | Contracteigenaar en verantwoordelijk management   | Verantwoordelijk management                  |

De namen, vervangers, telefoonnummers, e-mailadressen en bereikbaarheidsafspraken worden vastgelegd in de definitieve escalatiematrix.

### 9.2 Verantwoordelijkheden

| Activiteit                                    | Gemeente<br>Vijfheerenlanden | Opdrachtnemer | Gezamenlijk |
|-----------------------------------------------|------------------------------|---------------|-------------|
| Contract- en leveranciersmanagement           | X                            |               |             |
| Operationele uitvoering SOC-dienstverlening   |                              | X             |             |
| 24/7 monitoring, triage en analyse            |                              | X             |             |
| Beheer Microsoft Sentinel-configuratie        |                              | X             |             |
| Beheer gemeentelijke bron- en doelsystemen    | X                            |               |             |
| Aansluiten en testen van logbronnen           |                              |               | X           |
| Ontwikkelen en onderhouden standaarddetecties |                              | X             |             |
| Prioriteren van klantspecifieke use-cases     |                              |               | X           |
| Testen en documenteren van detectieregels     |                              | X             |             |

|                                                        |   |   |   |
|--------------------------------------------------------|---|---|---|
| Autoriseren van klantspecifieke detecties              | X |   |   |
| Tuning en reduceren van false positives                |   |   | X |
| Classificeren en melden van incidenten                 |   | X |   |
| Besluitvorming over bedrijfsimpact en risicoacceptatie | X |   |   |
| Uitvoeren van vooraf gemandateerde responsacties       |   | X |   |
| Uitvoeren van niet-gemandateerde wijzigingen           | X |   |   |
| Rapportages en managementinformatie                    |   | X |   |
| Opstellen en onderhouden SLA, DAP en RACI              |   |   | X |
| Continuïteitsplan SOC-dienstverlening                  |   | X |   |
| Gemeentelijk incidentresponsplan                       | X |   |   |
| Exit en overdracht                                     |   |   | X |