Bijlage 1 – Programma van Eisen

'SIEM, SOC, SOAR-dienstverlening'

Dit Programma van Eisen (PvE) bevat de gestelde eisen voor de SIEM-, SOC- en SOAR-dienstverlening en geldt gedurende de volledige looptijd van de overeenkomst. Nadere werkafspraken worden vastgelegd in het Dossier Afspraken en Procedures (DAP)

1. Algemene eisen	
1.1	VNOG gebruikt Microsoft Sentinel als Security Information and Event Management (SIEM)-oplossing en Microsoft Defender XDR voor proactieve bescherming en response. Inschrijver dient deze te integreren in de uitgevraagde dienstverlening.
1.2	VNOG maakt gebruik van netwerkcomponenten (routers/firewalls in de datacenters) met de mogelijkheid om bekende en onbekende bedreigingen en afwijkend gedrag te detecteren en hierop te alarmeren. Inschrijver dient deze (desgewenst via de SIEM-oplossing van VNOG) te integreren in de uitgevraagde dienstverlening.
1.3	Eventuele voor de dienstverlening benodigde specifieke hardware- en softwarecomponenten worden in abonnementsvorm geleverd. Eventuele logforwarders worden door VNOG geleverd.
1.4	Alle informatie die betrekking heeft op beveiligingsincidenten, waaronder meldingen, onderzoeksgegevens, log- en eventdata, verrijkte gegevens en vastgelegde opvolgingsacties, mag niet verloren gaan. Opdrachtnemer treft aantoonbaar passende technische en organisatorische maatregelen om verlies, beschadiging of ongeautoriseerde wijziging van deze informatie te voorkomen.
1.5	Inschrijver levert de aangeboden SOC-dienst met toepassing of configuratie van een uitgebreide bibliotheek met detectiemogelijkheden om bekende afwijkingen te detecteren die kunnen leiden tot een security-incident.
1.6	Deze uitgebreide bibliotheek met detectiemogelijkheden wordt door Inschrijver continu actueel gehouden volgens de dan toepasselijke stand der techniek, kennis, kunde en dreigingsbeeld. Het moet mogelijk zijn om snel detectie (o.a. op basis van Threat Intelligence) van nieuwe dreigingen toe te voegen, zowel door de opdrachtnemer als opdrachtgever, waarbij de opdrachtnemer beheerder van en verantwoordelijk voor de inhoud en actualiteit van deze bibliotheek is.

1.7	De Opdrachtnemer accepteert Bijlage 5 - ARBIT 2022 onverkort en zonder voorbehoud.
1.8	De Opdrachtnemer voldoet aan de Algemene Verordening Gegevensbescherming (AVG) en is bereid een verwerkersovereenkomst conform (Bijlage 6) te sluiten alvorens persoonsgegevens worden verwerkt.
1.9	De volledige implementatie is uiterlijk afgerond aan het einde van de implementatieperiode zoals opgenomen in de Gunningsleidraad (beoogd 23 april 2027), tenzij schriftelijk anders met VNOG overeengekomen.
1.10	De implementatie en onboarding van de SIEM-, SOC- en SOAR-dienstverlening vindt plaats zonder verlies van monitoring-, detectie- en responscapaciteit. Bestaande beveiligingsfunctionaliteiten blijven operationeel totdat de nieuwe dienstverlening aantoonbaar functioneert en door VNOG is geaccepteerd.
1.11	De Opdrachtnemer meldt ieder vermoedelijk of vastgesteld informatiebeveiligingsincident dat de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens, systemen of dienstverlening van VNOG kan aantasten, onverwijld na ontdekking bij VNOG. Kritieke incidenten worden direct telefonisch gemeld. Een eerste schriftelijke melding volgt zo spoedig mogelijk en uiterlijk binnen 24 uur na ontdekking." "De eerste melding bevat, voor zover op dat moment bekend: • de aard, ernst, omvang en vermoedelijke oorzaak van het incident; • het moment van ontdekking en de vermoedelijke aanvang; • de getroffen gegevens, systemen, accounts en dienstverlening; • de mogelijke gevolgen voor VNOG en betrokkenen; • de reeds getroffen beheers- en herstelmaatregelen; • de nog te nemen maatregelen en het verwachte vervolg; • de contactgegevens van de verantwoordelijke incidentcoördinator. De Opdrachtnemer houdt VNOG actief op de hoogte totdat het incident volledig is afgehandeld, stelt relevante loggegevens en onderzoeksinformatie beschikbaar, bewaart mogelijk bewijsmateriaal en verleent alle redelijkerwijs noodzakelijke medewerking aan onderzoek, containment, herstel, evaluatie en eventuele wettelijke meldingen. Externe communicatie of melding aan derden vindt uitsluitend plaats na afstemming met VNOG, tenzij een wettelijke verplichting zich daartegen verzet.
1.12	De Opdrachtnemer levert een online serviceportaal waarin VNOG de status van meldingen, incidenten, changes, KPI's, rapportages en relevante managementinformatie real-time kan raadplegen.

1.13	De Opdrachtnemer beschikt gedurende de volledige looptijd over aantoonbare kennis en expertise van de door VNOG afgenomen Microsoft Security-omgeving, waaronder Microsoft Sentinel en Microsoft Defender XDR, alsmede van overige oplossingen die Opdrachtnemer voor de dienstverlening inzet**.** Op verzoek van VNOG toont Opdrachtnemer dit aan met relevante en actuele certificeringen van medewerkers, leverancierspartnerstatussen, referentieopdrachten of gelijkwaardige bewijsstukken. Tevens toont Opdrachtnemer aan dat hij rechtstreeks of via een geautoriseerde samenwerkingspartner toegang heeft tot productondersteuning, beveiligings- en productupdates en technische escalatiemogelijkheden bij de betreffende leveranciers.
1.14	Medewerkers van Opdrachtnemer die werkzaamheden uitvoeren op locatie van VNOG beschikken over een geldige Verklaring Omtrent het Gedrag (VOG), niet ouder dan twee (2) jaar, welke op verzoek van VNOG kan worden overgelegd.
1.15	Alle communicatie met VNOG vindt in beginsel in de Nederlandse taal plaats. Dit geldt in ieder geval voor reguliere klantgesprekken, evaluaties, governanceoverleggen, service reviews, operationele overleggen en communicatie tijdens beveiligingsincidenten. Indien voor de behandeling van een beveiligingsincident specialistische expertise nodig is, mag de communicatie met en door deze specialisten in het Engels (Cambridge Engels of vergelijkbaar niveau) plaatsvinden. Ook het gebruik van gangbare Engelstalige cybersecurity- en productterminologie is toegestaan wanneer dit de technische communicatie en eenduidigheid ten goede komt.

1.16	VNOG blijft eigenaar en contracthouder van de Microsoft Sentinel- en Microsoft Defender XDR-omgeving en draagt de kosten van de bestaande Microsoft-licenties, tenzij in de overeenkomst uitdrukkelijk anders is bepaald. VNOG en Opdrachtnemer zijn gezamenlijk betrokken bij de inrichting, configuratie en het beheer van Microsoft Sentinel en Microsoft Defender XDR. De taken, verantwoordelijkheden, bevoegdheden en verantwoordingslijnen worden vóór aanvang van de dienstverlening vastgelegd in een door beide partijen goedgekeurde RACI-matrix in het Dossier Afspraken en Procedures (DAP). De RACI-matrix bevat ten minste afspraken over: • het toekennen, wijzigen, periodiek beoordelen en intrekken van toegangsrechten; • het aansluiten, configureren, bewaken en beëindigen van log- en gegevensbronnen; • het ontwikkelen, testen, goedkeuren, implementeren en beheren van detectieregels en usecases; • het ontwikkelen, testen en uitvoeren van SOAR-playbooks en de daarbij geldende mandaten; • configuratie-, wijzigings- en versiebeheer; • de monitoring van beschikbaarheid, correcte werking en volledigheid van datastromen; • de opslaglocatie, retentie en verwijdering van log- en eventdata; • het beheer van ingestie, datavolumes en opslagcapaciteit; • de verantwoordelijkheid voor licentie-, ingestie-, opslag-, retentie- en overige gebruikskosten; • de escalatie- en besluitvormingsprocedure bij afwijkingen, risico's en kostenoverschrijdingen. VNOG behoudt de uiteindelijke beslissingsbevoegdheid over materiële wijzigingen in haar Microsoft-omgeving. Opdrachtnemer voert geen wijziging uit die gevolgen kan hebben voor functionaliteit, beveiliging, logvolume, retentie, licenties of kosten zonder voorafgaande schriftelijke goedkeuring van VNOG. Opdrachtnemer brengt VNOG vooraf schriftelijk op de hoogte van de verwachte technische, operationele en financiële gevolgen van een voorgestelde wijziging. Daarbij verstrekt Opdrachtnemer ten minste een onderbouwde raming van de gevolgen voor het logvolume en de licentie-, ingestie-, opslag- en retentiekosten. Na uitvoering bewaakt Opdrachtnemer de werkelijke gevolgen en meldt hij materiële afwijkingen onverwijld aan VNOG.

1.17	Usecases, detectieregels, SOAR-playbooks, koppelingen, scripts en configuraties die Opdrachtnemer specifiek voor VNOG ontwikkelt of inricht (maatwerk), worden gedocumenteerd en, voor zover technisch passend, binnen de Microsoft Sentinel-omgeving van VNOG vastgelegd. VNOG kan dit maatwerk gedurende en na afloop van de overeenkomst zonder aanvullende kosten gebruiken en laten gebruiken door een door VNOG aangewezen opvolgende leverancier. Voor zover in het maatwerk reeds bestaande, generieke content van Opdrachtnemer is verwerkt die noodzakelijk is voor het gebruik daarvan, verleent Opdrachtnemer VNOG hierop een niet-exclusief, eeuwigdurend en kosteloos gebruiksrecht, dat VNOG ook door een opvolgende leverancier mag laten uitoefenen. De bepalingen over intellectuele eigendom in de ARBIT 2022 blijven onverminderd van toepassing voor zover deze VNOG verdergaande rechten verlenen.

1.18	De tussen VNOG en Opdrachtnemer overeengekomen processen, procedures, taken, verantwoordelijkheden en werkafspraken worden vastgelegd in een Dossier Afspraken en Procedures (DAP). Opdrachtnemer stelt het DAP op en levert een concept aan gelijktijdig met het implementatie- en migratieplan (eis 8.3, uiterlijk 12 maart 2027). VNOG stelt het DAP uiterlijk vóór de formele acceptatie vast (eis 8.6, uiterlijk 23 april 2027). Het DAP bevat ten minste: • de verantwoordelijkheidsverdeling (RACI) (eis 1.16); • de contact-, notificatie- en escalatiematrix (eis 2.8 en SLA-05); • de werkwijze voor registratie, prioritering, afhandeling en voortgangscommunicatie van meldingen en incidenten (SLA-01 t/m SLA-07); • de samenwerking en escalatie tijdens GRIP-opschaling (SLA-02); • de aangesloten log- en gegevensbronnen en de retentietermijnen (eisen 3.2 en 8.8); • het beheer van usecases, detectieregels en playbooks, inclusief de mandaten voor geautomatiseerde maatregelen (eisen 6.1 t/m 6.3); • de procedure voor wijzigingen in de omgeving van VNOG (eis 8.7); • de rapportage- en overlegstructuur (eis 5.4 en SLA-03); • de activeringsprocedure voor CERT-inzet en afgeroepen opties (eisen 9.1 t/m 9.9); • de procedure, planning en verantwoordelijkheden voor het opstellen en vaststellen van het exitplan. Het exitplan wordt na vaststelling (overeenkomstig eis 7.1) als integraal onderdeel aan het DAP toegevoegd. De latere toevoeging van het exitplan staat niet in de weg aan de vaststelling en acceptatie van de eerste versie van het DAP. Opdrachtnemer houdt het DAP actueel en past dit in overleg met VNOG aan bij iedere relevante wijziging in de dienstverlening, organisatie of technische inrichting. Wijzigingen worden van kracht na schriftelijke vaststelling door VNOG. Het DAP werkt de overeenkomst, dit Programma van Eisen en de SLA uit en kan daarvan niet afwijken; bij strijdigheid gaan deze documenten voor.
1.19	Opdrachtnemer wijst gedurende de gehele looptijd een vaste Nederlandstalige accountmanager aan als primair aanspreekpunt.

2. Eisen aan triage, onderzoek, classificatie en reactie	
2.1	Inschrijver heeft een eigen SOC-team, gevestigd binnen de Europese Economische Ruimte (EER).

2.2	Van Inschrijver wordt verwacht dat het eigen SOC-team het 24/7 Eyes-on-Glass-principe hanteert, conform de definitie in de Gunningsleidraad (§2.1.2 en begrippenlijst): een permanent bemand SOC waarbij gedurende 24 uur per dag, 7 dagen per week, 365 dagen per jaar gekwalificeerde securityanalisten (minimaal L1 en L2) actief belast zijn met het realtime monitoren, analyseren, classificeren, verrijken, prioriteren en escaleren van security-events en beveiligingsincidenten, met geborgde continuïteit tijdens ploegwisselingen, pauzes, ziekte, verlof of andere vormen van uitval. Er is geen sprake van 24/7 Eyes-on-Glass indien de monitoring uitsluitend plaatsvindt door middel van geautomatiseerde detectie, AI-functionaliteit, consignatie- of piketdiensten.
2.3	Inschrijver biedt een 24/7 telefonisch bereikbare servicedesk met rechtstreeks contact met, dan wel directe doorgeleiding naar, ter zake kundig personeel voor vragen over meldingen en/of opvolgingsadviezen. De voertaal is bij voorkeur Engels (Cambridge Engels of vergelijkbaar niveau), maar Nederlands is ook toegestaan.
2.4	De voertaal van het serviceportaal van Opdrachtnemer is Engels. Dit geldt voor de gebruikersinterface, meldingen, tickets, technische omschrijvingen, statusinformatie, opvolgingsadviezen en de in het serviceportaal beschikbare technische documentatie. Hieronder vallen in ieder geval technische incidentrapportages, forensische onderzoeksrapporten, malwareanalyses, Indicators of Compromise (IoC's), technische tijdlijnen en aanvalsanalyses. Documentatie die is bestemd voor besluitvorming binnen VNOG wordt in het Nederlands aangeleverd. Hieronder vallen in ieder geval managementsamenvattingen, situatiebeelden, impactanalyses en adviezen aan de crisisorganisatie van VNOG. Bij ieder technisch incidentrapport voegt Opdrachtnemer een Nederlandstalige managementsamenvatting toe. De overige communicatie met VNOG, waaronder accountmanagement, service reviews en governanceoverleggen, vindt plaats in het Nederlands, overeenkomstig paragraaf eis 1.15
2.5	Inschrijver is in staat de analyse van security-events binnen een realistische tijd uit te voeren (triage binnen enkele minuten na detectie; reactie en oplossing conform de reactie- en oplostijden in Bijlage 4 – Service Level Agreement (SLA)) en het aantal false positives tot een minimum te beperken. Inschrijver biedt de mogelijkheid om, op aangeven van VNOG, specifieke false-positive-meldingen voor een bepaalde periode op "mute" te zetten / te "white-listen" Opdrachtnemer rapporteert periodiek over het aantal en het aandeel foutpositieve meldingen en de genomen verbetermaatregelen (zie eis 5.4).
2.6	VNOG kan verplicht zijn incidenten te delen met een sectorale of landelijke CERT. Inschrijver faciliteert dat incidenten met een specifieke prioriteit, na goedkeuring van VNOG, met de betreffende CERT worden gedeeld.

2.7	Alle meldingen, ongeacht classificatie of prioriteit, worden direct en volledig vastgelegd en beschikbaar gesteld in het serviceportaal van Opdrachtnemer. VNOG ontvangt van iedere melding tevens een notificatie per e-mail. Meldingen met prioriteit 1 of prioriteit 2 worden daarnaast telefonisch aan de door VNOG aangewezen contactpersonen gemeld. VNOG kan desgewenst per prioriteit, meldingstype en contactpersoon aanvullende sms-notificaties (en/of andere ondersteunde opties) laten instellen.
2.8	Bij aanvang van de dienstverlening stellen VNOG en Opdrachtnemer gezamenlijk een contact-, notificatie- en escalatiematrix vast. Hierin worden per prioriteit minimaal de contactpersonen, rollen, communicatiekanalen, bereikbaarheid, volgorde van benadering, escalatieniveaus en termijnen voor ontvangstbevestiging vastgelegd. De matrix wordt periodiek en na iedere relevante organisatorische wijziging gecontroleerd en op verzoek van VNOG aangepast. Opdrachtnemer bewaakt bij meldingen met prioriteit 1 en prioriteit 2 actief de ontvangstbevestiging door VNOG. Blijft deze binnen de in de matrix vastgelegde termijn uit, dan benadert Opdrachtnemer onverwijld de eerstvolgende contactpersoon volgens de matrix, totdat de ontvangst is bevestigd.
2.9	Waar technisch mogelijk worden meldingen automatisch aangemaakt in het ticketsysteem van VNOG door een koppeling op het ITSM van VNOG.
2.10	Opdrachtnemer neemt bij ieder incidentticket, naast de technische details, een duidelijke omschrijving op van de (vermoedelijke) oorzaak, impact en mogelijke gevolgen van het incident. Deze toelichting wordt opgesteld in begrijpelijke-technische taal, zodat zij ook bruikbaar is voor de professionalisering van de IT Specialisten van VNOG. Wanneer de definitieve oorzaak bij registratie nog niet bekend is, vermeldt Opdrachtnemer dit expliciet en neemt hij een voorlopige duiding op. Het ticket wordt gedurende het onderzoek actueel gehouden en na afronding aangevuld met de vastgestelde oorzaak, getroffen maatregelen, eventuele restrisico's en het geadviseerde vervolg.

3. Eisen aan de log- en eventdata	
3.1	De aangeboden dienstverlening is voldoende robuust om het benodigde volume aan logdata en events te kunnen verwerken en in de daarvoor overeengekomen omgeving (zie eis 1.18) bij Inschrijver op te slaan voor de overeengekomen retentietijd.

3.2	Voor de aangeleverde log- en eventdata vanuit de SIEM-/SOC-oplossing **gelden ten minste de volgende retentietermijnen:** • log- en eventdata die noodzakelijk zijn voor monitoring, detectie, incidentonderzoek en threat hunting blijven gedurende **minimaal zes (6) maanden (180 dagen)** direct en zonder voorafgaande herstelactie doorzoekbaar in het SIEM (hot/searchable); • alle log- en eventdata worden gedurende **minimaal twaalf (12) maanden** bewaard en blijven beschikbaar voor incidentonderzoek, forensisch onderzoek, rapportage en auditdoeleinden;; • relevante security-, identiteits-, beheer- en auditlogs worden gedurende minimaal **vierentwintig (24) maanden** bewaard. Gegevens ouder dan zes (6) maanden (180) dagen mogen daarbij in een langetermijn- of archieflaag worden opgeslagen; • gearchiveerde gegevens worden op verzoek van VNOG uiterlijk binnen **twee (2) werkdagen** opnieuw volledig doorzoekbaar en exporteerbaar gemaakt in een gangbaar, gedocumenteerd en bruikbaar formaat; • de integriteit, authenticiteit, volledigheid, tijdsynchronisatie en herleidbaarheid van de bewaarde gegevens blijven gedurende de volledige bewaartermijn gewaarborgd. De definitieve bewaartermijnen worden per gegevenscategorie, binnen de toepasselijke wettelijke kaders en met inachtneming van de hiervoor genoemde minimumtermijnen, vastgelegd in het Dossier Afspraken en Procedures (DAP) en, voor zover persoonsgegevens worden verwerkt, in de Verwerkersovereenkomst. Afwijking naar een kortere bewaartermijn is uitsluitend toegestaan indien een wettelijke verplichting dit vereist of VNOG hiermee vooraf schriftelijk instemt. Opdrachtnemer maakt vooraf inzichtelijk welke gevolgen de gekozen retentietermijnen hebben voor opslag, beschikbaarheid, prestaties en kosten. De procedure, prioritering en maximale termijn voor het beschikbaar stellen van gearchiveerde gegevens die noodzakelijk zijn voor de afhandeling van een incident met prioriteit 1 of 2, worden vastgelegd in het Dossier Afspraken en Procedures (DAP). Hierbij geldt dat deze gegevens met voorrang beschikbaar worden gesteld binnen de in Bijlage A (door opdrachtnemer op te leveren document) vastgelegde termijn.
3.3	Voor de aangeleverde log- en eventdata geldt dat deze bij Inschrijver zodanig moet worden opgeslagen dat de beschikbaarheid, integriteit en vertrouwelijkheid gegarandeerd zijn, en dat deze beschikbaar is voor analyse van historische data (forensisch en post-mortem) en als bewijsmateriaal gebruikt kan worden in eventuele strafzaken.

3.4	De aangeboden SIEM-, SOC-, SOAR- en XDR-dienstverlening ondersteunt de geautomatiseerde uitwisseling van cyberdreigingsinformatie conform **STIX 2.1 en TAXII 2.1**. Opdrachtnemer realiseert, configureert en beheert de benodigde koppeling(en) met de door VNOG aangewezen dreigingsinformatiebronnen, waaronder waar van toepassing het NCSC. De koppeling ondersteunt ten minste het geautomatiseerd en beveiligd ontvangen, verwerken en actualiseren van dreigingsinformatie en Indicators of Compromise. Ook ondersteunt de koppeling, na voorafgaande toestemming van VNOG, het terugleveren van relevante dreigingsinformatie en sightings. Opdrachtnemer zorgt ervoor dat ontvangen dreigingsinformatie bruikbaar wordt gemaakt voor detectieregels, usecases, verrijking van meldingen en SOAR-playbooks. De werking van de koppeling wordt bewaakt, getest en aantoonbaar vastgelegd. Uitwisseling van VNOG-specifieke informatie vindt uitsluitend plaats binnen het door VNOG verleende mandaat. Deze eis sluit aan op de opname van STIX/TAXII 2.1 op de 'pas toe of leg uit'-lijst sinds 1 juli 2026. Wissel effectiever dreigingsinformatie uit met STIX/TAXI 2.1 | NCSC en Versie 2.1 van STIX en TAXII per 1 juli 2026 verplicht voor de overheid | NCSC
3.5	Delen van de aangeleverde log- en eventdata kunnen door VNOG worden geëxporteerd en gearchiveerd buiten de systemen van Inschrijver.
3.6	Bij exporteren en archivering van log- en eventdata wordt de bijbehorende metadata meegeleverd.
3.7	De export van log- en eventdata vindt plaats in een gedocumenteerd, gangbaar en door VNOG bruikbaar formaat, zonder verlies van tijdstempels, brongegevens, classificaties en overige relevante metadata.

4. Eisen aan de beveiliging	
4.1	Alle data wordt opgeslagen en verwerkt binnen de Europese Economische Ruimte (EER).
4.2	Alle data wordt versleuteld opgeslagen (minimaal AES-256) en versleuteld verstuurd, conform de meest recente ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.
4.3	Inschrijver past het principe van "least privilege" en "need to know" toe en beperkt zo de toegang tot het noodzakelijke. Dit geldt ook voor service-, machine- en functionele accounts.

4.4	Inzage van logdata is alleen mogelijk voor VNOG en bevoegde medewerkers van Opdrachtnemer, tenzij vooraf uitdrukkelijk en schriftelijk toestemming is gegeven door VNOG of de rechter daartoe opdracht geeft. Toegang wordt verleend op basis van rol en noodzaak, is toetsbaar en wordt ingetrokken zodra de noodzaak vervalt.
4.5	Inschrijver gebruikt multifactor-authenticatie voor toegang tot alle rapportages/portalen, voor zowel beheerders als gebruikers.
4.6	Toegang tot log- en eventdata wordt rolgebaseerd, doelgebonden en toetsbaar ingericht. Opdrachtnemer registreert toekenning, wijziging, gebruik en intrekking van deze toegangsrechten.
4.7	De aangeboden oplossing en dienstverlening voldoen gedurende de looptijd van de overeenkomst aan de voor de opdracht relevante open standaarden die zijn opgenomen op de 'Pas toe of leg uit'-lijst en de "Aanbevolen standaarden" van het Forum Standaardisatie. De Opdrachtnemer past daarnaast, voor zover passend binnen de scope en technische inrichting van de dienstverlening, de door het Forum Standaardisatie aanbevolen standaarden toe (Lijst open standaarden | Forum Standaardisatie).
4.8	Opdrachtnemer verstrekt gegevens uitsluitend aan derden na voorafgaande schriftelijke toestemming van VNOG of wanneer een daartoe bevoegde instantie dit op een geldige wettelijke grondslag vordert.

5. Eisen aan de rapportage	
5.1	Rapportages vanuit de geleverde dienst worden via een serviceportaal, dan wel op een laagdrempelige passende wijze, aan VNOG beschikbaar gesteld. Via dit portaal ontvangt VNOG ook relevante dreigingsinformatie (threat intelligence).
5.2	De rapportages zijn opgesteld in de Nederlandse taal, waarbij het gebruik van Engelse termen inclusief gegenereerde alerts in het Engels (korte berichten met dreigings- en technische informatie) is toegestaan. Voor technische documentatie en incidentrapportages geldt eis 2.4.
5.3	De voorziening voor rapportages maakt het voor VNOG mogelijk om rapportages op te stellen op meerdere managementniveaus, alsmede trendrapportages.
5.4	Opdrachtnemer rapporteert overeenkomstig SLA-03 (maandelijkse operationele rapportage en driemaandelijkse trend- en servicerapportage) en organiseert minimaal eenmaal per kwartaal een serviceoverleg (de kwartaalreview uit SLA-03), waarin in ieder geval incidenten, dreigingen, trends, prestaties, verbetermaatregelen en ontwikkelingen binnen de dienstverlening worden besproken.

5.5	De oplossing dient (near) real-time monitoring en dashboards (idealiter in een “single pane of glass”) beschikbaar te stellen.

6. Use case management, detectie en SOAR-automatisering	
6.1	Inschrijver levert structureel usecasemanagement en ondersteunt VNOG bij het identificeren, prioriteren, ontwikkelen, testen en periodiek evalueren van usecases en detectieregels. Deze worden risicogestuurd afgestemd op het actuele dreigingsbeeld, de bedrijfsprocessen en de IT/OT-omgeving van VNOG en gekoppeld aan MITRE ATT&CK, de Lockheed Martin Cyber Kill Chain of een aantoonbaar gelijkwaardig raamwerk. Inschrijver verwerkt relevante wijzigingen in dreigingen en risico’s tijdig in de usecases en detectieregels.
6.2	Inschrijver biedt SOAR-functionaliteit waarmee securityprocessen, waaronder triage, verrijking, escalatie en responsmaatregelen, geautomatiseerd en tussen verschillende beveiligingsoplossingen georkestreerd kunnen worden. De uitvoering vindt plaats op basis van met VNOG afgestemde playbooks en mandaten. Voor kritieke of potentieel verstorende maatregelen is voorafgaande menselijke beoordeling en goedkeuring vereist, tenzij VNOG hiervoor uitdrukkelijk mandaat aan Opdrachtnemer heeft verleend. Alle geautomatiseerde en handmatige handelingen zijn herleidbaar en worden controleerbaar vastgelegd.
6.3	Opdrachtnemer evalueert en actualiseert de detectieregels en playbooks periodiek en bij relevante wijzigingen in het dreigingsbeeld, de risico’s of de IT/OT-omgeving van VNOG. Bevindingen en geleerde lessen uit incidenten, onderzoeken en oefeningen worden aantoonbaar en binnen een met VNOG overeengekomen termijn vertaald naar verbeterde detectieregels, usecases en playbooks. Wijzigingen worden getest, gedocumenteerd en na afstemming met VNOG gecontroleerd in gebruik genomen.
6.4	Opdrachtnemer ondersteunt VNOG bij compliance-, verantwoordings- en auditvraagstukken die betrekking hebben op de geleverde SIEM-, SOC- en SOAR-dienstverlening. Deze ondersteuning omvat ten minste het tijdig beschikbaar stellen van relevante documentatie, rapportages, loggegevens en overige auditbewijzen, evenals het geven van toelichting aan VNOG en door VNOG aangewezen auditors of toezichthouders. Eventuele bevindingen worden gezamenlijk beoordeeld en vertaald naar aantoonbare verbetermaatregelen.

7. Eisen aan de re-transitie	
7.1	Opdrachtnemer stelt bij aanvang van de dienstverlening, doch uiterlijk binnen vier (4) maanden na de ingangsdatum van de overeenkomst, in overleg met VNOG een gedetailleerd exitplan op. Het exitplan wordt vastgelegd in het Dossier Afspraken en Procedures (DAP) en bevat ten minste: • de planning, activiteiten, verantwoordelijkheden en contactpersonen van VNOG en Opdrachtnemer; • de maatregelen voor het waarborgen van de continuïteit en beveiliging tijdens de transitie; • de overdracht van de dienstverlening, kennis, documentatie en configuraties; • de overdracht van usecases, detectieregels, playbooks, koppelingen en maatwerk; • de overdracht of export van log-, incident- en rapportagegegevens in een gangbaar, open en bruikbaar formaat; • de ondersteuning van VNOG en een eventuele opvolgende leverancier; • de intrekking van toegangsrechten en beëindiging van koppelingen; • de teruggave en aantoonbare verwijdering van gegevens, na goedkeuring door VNOG; • de voor de verschillende exitactiviteiten geldende doorlooptijden. Opdrachtnemer evalueert en actualiseert het exitplan periodiek, op verzoek van VNOG en bij materiële wijzigingen in de dienstverlening. De uitvoering van het exitplan mag niet leiden tot een verminderde beschikbaarheid, beveiliging of kwaliteit van de dienstverlening.
7.2	Opdrachtnemer verwerkt iedere overeengekomen wijziging in het exitplan uiterlijk binnen tien (10) werkdagen na vaststelling daarvan in het Dossier Afspraken en Procedures (DAP). De gewijzigde versie wordt ter beoordeling en goedkeuring aan VNOG voorgelegd en voorzien van versienummer, wijzigingsdatum en een overzicht van de aangebrachte wijzigingen.

7.3	Opdrachtnemer is in staat het vastgestelde exitplan op eerste schriftelijk verzoek van VNOG in werking te stellen en de daarin opgenomen exitactiviteiten binnen twintig (20) werkdagen volledig uit te voeren. Binnen deze termijn draagt Opdrachtnemer de dienstverlening, gegevens, documentatie, configuraties, usecases, detectieregels, playbooks, koppelingen en overige overeengekomen onderdelen gecontroleerd over aan VNOG of een door VNOG aangewezen opvolgende leverancier. Afwijking van deze termijn is uitsluitend toegestaan na voorafgaande schriftelijke instemming van VNOG. De uitvoering van het exitplan mag niet leiden tot een onaanvaardbare vermindering van de continuïteit, beschikbaarheid of beveiliging van de dienstverlening. Opdrachtnemer verleent volledige medewerking aan de opvolgende leverancier, waaronder een partij met wie VNOG een wachtkamerovereenkomst heeft gesloten (Bijlage 7), en stemt de overdracht af op het transitieplan van die leverancier.
7.4	Gedurende de periode van retransitie continueert Inschrijver alle dienstverlening tegen de overeengekomen voorwaarden, totdat de opvolgende leverancier de dienstverlening aantoonbaar operationeel heeft overgenomen, met een maximum van drie (3) maanden na inwerkingstelling van het exitplan, of zoveel langer als VNOG en Opdrachtnemer schriftelijk overeenkomen.
7.5	Bij retransitie van de dienstverlening stelt Opdrachtnemer alle bij hem of zijn onderaannemers opgeslagen VNOG-gerelateerde log-, event-, incident- en rapportagegegevens, inclusief de bijbehorende metadata, tijdstempels en relevante context, volledig aan VNOG beschikbaar. De gegevens worden geleverd in een gangbaar, open, gedocumenteerd en voor VNOG of een opvolgende leverancier bruikbaar formaat. Het intellectuele eigendom van Opdrachtnemer hoeft niet te worden overgedragen, voor zover het uitsluiten daarvan de volledigheid, leesbaarheid, interpreteerbaarheid, bruikbaarheid of overdraagbaarheid van de VNOG-gegevens niet beperkt. Opdrachtnemer verstrekt de documentatie die noodzakelijk is om de overgedragen gegevens correct te kunnen verwerken en interpreteren. Voor maatwerk geldt eis 1.18.

7.6	Opdrachtnemer draagt uiterlijk bij afronding van de retransitie alle vertrouwelijke informatie en gegevens van VNOG over aan VNOG of een door VNOG aangewezen partij. Nadat VNOG de volledige en bruikbare overdracht heeft bevestigd, verwijdert Opdrachtnemer deze informatie uit zijn systemen, omgevingen en back-ups en ziet hij erop toe dat zijn onderaannemers hetzelfde doen. Opdrachtnemer behoudt geen kopieën, tenzij een wettelijke verplichting of een voorafgaande schriftelijke afspraak met VNOG dit vereist. In dat geval: • informeert Opdrachtnemer VNOG over de grondslag, gegevenscategorieën en bewaartermijn; • blijft de informatie passend beveiligd en uitsluitend toegankelijk voor het doel waarvoor bewaring noodzakelijk is; • wordt de informatie niet voor andere doeleinden verwerkt; • vernietigt Opdrachtnemer de informatie aantoonbaar zodra de bewaartermijn is verstreken of de grondslag voor bewaring vervalt. Op verzoek van VNOG verstrekt Opdrachtnemer een schriftelijke verklaring waaruit blijkt dat de gegevens volledig en overeenkomstig deze eis zijn verwijderd.

8. Onboarding	
8.1	De onboardingdiensten worden geleverd door vakbekwaam personeel dat voldoet aan de eisen die gelden in de branchestandaard.
8.2	Opdrachtnemer start op **vrijdag 26 februari 2027** met de implementatie. Uiterlijk binnen eenentwintig (21) kalenderdagen na de definitieve gunning, derhalve uiterlijk op **vrijdag 19 maart 2027**, monitort Opdrachtnemer de bestaande XDR- en SIEM-omgeving van VNOG, detecteert en beoordeelt hij relevante dreigingen en kan hij VNOG hierover informeren en alarmeren. De periode van **vrijdag 19 maart 2027 tot en met vrijdag 23 april 2027** wordt gebruikt om, in overleg met VNOG, een baseline voor de detectieregels vast te stellen. Opdrachtnemer analyseert gedurende deze periode het normale gedrag en de reguliere activiteiten binnen de omgeving van VNOG en gebruikt de verkregen inzichten om detectieregels, drempelwaarden en prioriteiten af te stemmen en ongewenste foutpositieve meldingen te beperken. Kritieke meldingen en vermoedelijke beveiligingsincidenten worden gedurende deze periode onverminderd opgevolgd en aan VNOG gemeld. De volledige dienstverlening, inclusief de overeengekomen en vastgelegde baseline, is uiterlijk op, **vrijdag 23 april 2027**, operationeel, inclusief formele acceptatie. Voor het moment waarop de vergoeding verschuldigd is, geldt eis 11.5.

8.3	Opdrachtnemer levert uiterlijk binnen tien (10) werkdagen na de definitieve gunning, derhalve uiterlijk op **vrijdag 12 maart 2027**, een gedetailleerd implementatie- en migratieplan ter beoordeling en goedkeuring aan VNOG op. Het plan bevat ten minste: • de planning, fasering en mijlpalen; • de taken, verantwoordelijkheden en benodigde inzet van beide partijen; • de afhankelijkheden en benodigde toegang tot systemen en gegevensbronnen; • een risicoanalyse met bijbehorende beheersmaatregelen; • test-, terugval- en herstelscenario's; • de acceptatiecriteria en acceptatieprocedure; • de inrichting van de monitoring en alarmering; • de aanpak voor het vaststellen en optimaliseren van de baseline en detectieregels; • de wijze waarop de continuïteit en beveiliging tijdens de implementatie worden gewaarborgd. • de afstemming met en overdracht vanuit de huidige dienstverlener van VNOG (zie eis 8.8). Opdrachtnemer verwerkt opmerkingen van VNOG zodanig dat het definitieve plan uiterlijk vóór aanvang van de monitoring en baselineperiode op **vrijdag 19 maart 2027** door VNOG kan worden vastgesteld.

8.4	Opdrachtnemer verzorgt tijdens de implementatieperiode minimaal twee (2) fysieke workshops van elk minimaal twee (2) uur op een door VNOG aangewezen locatie. De workshops zijn gericht op de kennismaking van de betrokken geledingen binnen VNOG met de werking; • mogelijkheden en reikwijdte van de **SIEM-, SOC- en SOAR-dienstverlening**; • de organisatorische impact van de dienstverlening op de bestaande processen, werkwijzen, taken, verantwoordelijkheden, bevoegdheden en benodigde beschikbaarheid van VNOG; • de operationele rol- en verantwoordelijkheidsverdeling tussen VNOG en Opdrachtnemer bij detectie, triage, analyse, escalatie, containment, incidentrespons en herstel; • de afspraken over classificatie, prioritering, alarmering, escalatie, communicatie en samenwerking tijdens beveiligingsincidenten; • het gebruik van het serviceportaal, waaronder het raadplegen en opvolgen van meldingen en incidenten, rapportages, dashboards en relevante koppelingen met de systemen van VNOG; • de toepassing van geautomatiseerde playbooks en de verdeling van mandaten, inclusief de maatregelen waarvoor voorafgaande toestemming van VNOG vereist is. Aansluitend verzorgt Opdrachtnemer gedurende de looptijd van de overeenkomst mimaal twee (2) keer per contractjaar een fysieke actualisatie- of verdiepingsworkshop. Hierbij wordt specifiek ingegaan op ontwikkelingen en wijzigingen binnen de SIEM-, SOC- en SOAR-dienstverlening en de daaruit voortvloeiende organisatorische impact voor VNOG. De inhoud wordt afgestemd op het actuele dreigingsbeeld, ervaringen uit incidenten, wijzigingen in de dienstverlening en de behoeften van de betrokken geledingen binnen VNOG. Opdrachtnemer stemt de inhoud, doelgroep en planning vooraf af met VNOG en stelt het gebruikte materiaal digitaal beschikbaar. De kosten van voorbereiding, uitvoering, reis en materiaal zijn inbegrepen in de aangeboden dienstverlening.
8.5	Inschrijver verzorgt training en kennisoverdracht aan de systeem- en netwerkbeheerders van VNOG (maximaal 6 personen) op het gebied van bediening, beheer, monitoring en opvolging van de SIEM-, SOC- en SOAR-oplossing.

8.6	Opdrachtnemer voert uiterlijk binnen drie (3) maanden na de definitieve gunning, in samenwerking met VNOG, een integrale beoordeling uit van de inrichting en configuratie van de Microsoft Defender XDR-suite en de daarop aangesloten log- en gegevensbronnen. De beoordeling omvat ten minste: • de configuratie en onderlinge samenhang van de gebruikte Microsoft Defender-componenten; • de dekking en kwaliteit van detecties, policies, sensoren en bestaande log- en gegevensbronnen; • de aansluiting op Microsoft Sentinel, SOAR-processen en overige relevante beveiligingsoplossingen; • de afstemming op het actuele dreigingsbeeld, de risico's en de IT/OT-omgeving van VNOG; • mogelijkheden voor verbetering van detectie, triage, automatisering en respons; • eventuele configuratierisico's, blinde vlekken en foutpositieve meldingen; • de noodzaak en toegevoegde waarde van aanvullende log- en gegevensbronnen. Opdrachtnemer adviseert VNOG schriftelijk en risicogestuurd over eventueel benodigde aanvullende log- en gegevensbronnen. Het advies bevat ten minste de verwachte verbetering van de detectiedekking, prioriteit, technische vereisten, afhankelijkheden en de gevolgen voor implementatie, beheer, licenties, opslag, dataverkeer en overige kosten. Opdrachtnemer legt de bevindingen, risico's en geprioriteerde verbetervoorstellen schriftelijk vast en bespreekt deze met VNOG. Wijzigingen en de aansluiting van aanvullende logbronnen worden uitsluitend na voorafgaande goedkeuring van VNOG doorgevoerd. De overeengekomen verbeteringen, configuratieafspraken en logbronnen worden vastgelegd in het Dossier Afspraken en Procedures (DAP).
8.7	Opdrachtnemer sluit tijdens de implementatieperiode, in samenwerking met VNOG, de bij aanvang overeengekomen log- en gegevensbronnen (basisscope zoals beschreven in de Gunningsleidraad) aan op de dienstverlening, waaronder de netwerkcomponenten uit eis 1.2, en configureert de koppeling tussen Microsoft Sentinel en Microsoft Defender XDR, zodat de detectiemogelijkheden van deze bronnen volledig worden benut. De aangesloten bronnen worden vastgelegd in het DAP.
8.8	De huidige SOC-/MDR-dienstverlening van VNOG eindigt op 30 april 2027. Opdrachtnemer richt de implementatie zodanig in dat de dienstverlening vóór die datum volledig operationeel en geaccepteerd is (eis 8.3) en stemt de overgang, voor zover nodig via VNOG, af met de huidige dienstverlener, zodat geen onderbreking van monitoring, detectie en respons ontstaat (eis 1.10).

9. Additionele diensten	
9.1	VNOG kan gedurende de looptijd van de overeenkomst de monitoringdekking van de SIEM-, SOC-, SOAR- en MDR-dienstverlening laten wijzigen of uitbreiden (het aansluiten van nieuwe **kroonjuwelen**, OT-omgevingen, datacenters en Microsoft-diensten (figuur 1 uit de Gunningsleidraad)). Dit kan betrekking hebben op het aansluiten, aanpassen of beëindigen van databronnen, systemen, omgevingen en koppelingen, waaronder: • Microsoft Sentinel, Defender XDR, Microsoft 365, Entra ID en Azure; • firewall-, netwerk-, endpoint-, identity-, cloud-, SaaS- en PaaS-bronnen; • systemen en infrastructuur binnen de datacenters van VNOG; • OT-systemen en OT-beheeromgevingen; • door VNOG als kroonjuweel of bedrijfskritisch aangemerkte systemen; • serviceportalen, ticketsystemen en overige relevante technische koppelingen. Opdrachtnemer brengt voorafgaand aan een wijziging ten minste de technische en organisatorische impact, implementatiewerkzaamheden, doorlooptijd en gevolgen voor usecases, detectieregels, playbooks, logvolume, retentie, licenties en kosten in kaart. Wijzigingen worden uitsluitend uitgevoerd na schriftelijke opdracht van VNOG. VNOG heeft geen verplichting tot afname van deze optie of tot afname van een minimumaantal aanvullende bronnen, systemen of koppelingen. Het niet afnemen van deze optie heeft geen gevolgen voor de overeengekomen basisdienstverlening, monitoringdekking en prijs.

9.2	VNOG kan gedurende de looptijd van de overeenkomst aanvullende consultancy- en adviesdiensten op het gebied van cybersecurity en informatiebeveiliging als optie afroepen. Deze diensten kunnen onder meer betrekking hebben op: • strategisch en tactisch securityadvies; • risico-, dreigings- en impactanalyses; • architectuur- en configuratieadvies; • ondersteuning bij cyberweerbaarheid en bedrijfscontinuïteit; • advies over BIO, NIS2 en overige relevante wet- en regelgeving; • ondersteuning bij audits, assessments en verbeterprogramma's; • advies naar aanleiding van incidenten, oefeningen of wijzigingen in het dreigingsbeeld. • ondersteuning bij het inrichten van de randvoorwaarden voor SOC-dienstverlening, in lijn met de SOC Readiness QuickScan van het Ministerie van Justitie en Veiligheid (VSSR) of een gelijkwaardig kader. Voorafgaand aan iedere opdracht verstrekt Opdrachtnemer een voorstel met ten minste de scope, aanpak, planning, inzet, beoogde resultaten en kosten. Uitvoering vindt uitsluitend plaats na schriftelijke opdracht van VNOG. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen van aanvullende consultancy- en adviesdiensten heeft geen gevolgen voor de inhoud, kwaliteit of prijs van de overeengekomen basisdienstverlening.

9.3	VNOG kan gedurende de looptijd van de overeenkomst de SOC-dienstverlening als optie laten uitbreiden met aanvullende of verhoogde serviceniveaus. Deze uitbreiding kan onder meer betrekking hebben op: • kortere triage-, reactie-, escalatie- of hersteltijden; • aanvullende monitoring-, analyse- en threat-huntingactiviteiten; • uitgebreidere incidentopvolging, containment en herstelondersteuning; • verhoogde beschikbaarheid of inzet van gespecialiseerde securityanalisten; • aanvullende rapportages, dashboards en overlegmomenten; • aanvullende monitoring van specifieke systemen, omgevingen of dreigingen; • uitgebreidere ondersteuning tijdens ernstige beveiligingsincidenten of cybercrises. Voorafgaand aan iedere uitbreiding verstrekt Opdrachtnemer een voorstel waarin ten minste de scope, het serviceniveau, de bijbehorende prestatie-indicatoren, de implementatietermijn en de kosten zijn opgenomen. De uitbreiding wordt uitsluitend uitgevoerd na schriftelijke opdracht van VNOG en vastgelegd in het Dossier Afspraken en Procedures (DAP) en, indien van toepassing, de SLA. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen van aanvullende serviceniveaus heeft geen gevolgen voor de inhoud, kwaliteit, continuïteit of prijs van de overeengekomen basisdienstverlening.

9.4	VNOG kan gedurende de looptijd van de overeenkomst aanvullende specialistische ondersteuning bij audits, compliance- en rapportagevraagstukken als optie afroepen. Deze ondersteuning betreft werkzaamheden die aantoonbaar buiten de reguliere verantwoordings-, informatie- en medewerkingsverplichtingen van de basisdienstverlening vallen en kan onder meer bestaan uit: • inhoudelijke begeleiding bij interne en externe audits of assessments; • aanvullende bewijsverzameling en dossieropbouw; • uitvoering van gap- en impactanalyses; • advisering over BIO, NIS2 en overige relevante wet- en regelgeving; • ondersteuning bij het opstellen van verbeterplannen en verantwoordingsrapportages; • maatwerkrapportages en aanvullende analyses; • deelname van specialisten aan auditgesprekken met auditors of toezichthouders. Voorafgaand aan iedere opdracht verstrekt Opdrachtnemer een voorstel met de scope, aanpak, planning, beoogde resultaten, benodigde inzet en kosten. Uitvoering vindt uitsluitend plaats na schriftelijke opdracht van VNOG. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen daarvan doet geen afbreuk aan de reguliere verplichting van Opdrachtnemer om relevante documentatie, rapportages, loggegevens, auditbewijzen en toelichtingen binnen de basisdienstverlening beschikbaar te stellen.

9.5	VNOG kan gedurende de looptijd van de overeenkomst aanvullende trainingen en awarenessactiviteiten op het gebied van cybersecurity en informatiebeveiliging als optie afroepen. Deze activiteiten zijn aanvullend op de workshops en kennisoverdracht die onderdeel zijn van de basisdienstverlening en kunnen onder meer bestaan uit: • doelgroepgerichte trainingen voor ICT-, security-, management- en crisisfunctionarissen; • table-topoefeningen en simulaties van cyberincidenten; • trainingen over SIEM-, SOC- en SOAR-processen, incidentrespons en crisiscoördinatie; • kennissessies over actuele dreigingen, aanvalstechnieken en geleerde lessen uit incidenten; • beperkte awarenessactiviteiten voor specifieke doelgroepen of thema's. Deze optie omvat geen organisatiebreed of doorlopend securityawarenessprogramma, tenzij VNOG hiervoor afzonderlijk schriftelijk opdracht verleent. Voorafgaand aan iedere activiteit verstrekt Opdrachtnemer een voorstel met de doelgroep, leerdoelen, inhoud, vorm, duur, planning en kosten. Uitvoering vindt uitsluitend plaats na schriftelijke opdracht van VNOG. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen daarvan heeft geen gevolgen voor de workshops, instructies en kennisoverdracht die binnen de overeengekomen basisdienstverlening moeten worden geleverd.

9.6	VNOG kan gedurende de looptijd van de overeenkomst aanvullende CERT-/CSIRT- en incidentresponsdiensten als optie afroepen in de vorm van een losse opdracht. **Het betreft incidentele inzet op verzoek van VNOG, zonder vooraf gereserveerde beschikbaarheid of gegarandeerde responstijd. Voor vooraf gegarandeerde beschikbaarheid en responscapaciteit geldt de CERT-retainer uit eis 9.7.** Deze diensten worden ingezet naast de reguliere detectie, triage, escalatie en incidentopvolging die onderdeel zijn van de basisdienstverlening en kunnen onder meer bestaan uit: • on-site en remote ondersteuning bij ernstige beveiligingsincidenten of cybercrises; • digitaal forensisch onderzoek; • malwareanalyse en analyse van Indicators of Compromise; • ondersteuning bij containment, eradication en herstel; • veiligstelling, verzameling en analyse van digitaal bewijsmateriaal; • reconstructie van aanvalspaden en technische tijdlijnen; • ondersteuning bij crisiscoördinatie en technische afstemming met onder meer het NCSC, ketenpartners en andere betrokken partijen; • technische incidentrapportages, evaluaties en verbetervoorstellen. Voorafgaand aan de inzet, of bij spoedeisende incidenten zo spoedig mogelijk daarna, verstrekt Opdrachtnemer inzicht in de aard, omvang, beschikbaarheid, responstijd, inzetvoorwaarden en kosten. De wijze van activering, contactpersonen, bevoegdheden, responstijden en tarieven worden vooraf vastgelegd in het Dossier Afspraken en Procedures (DAP). VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen van deze aanvullende diensten beperkt niet de incidentdetectie, triage, escalatie en reguliere respons die onderdeel zijn van de basisdienstverlening.

9.7	VNOG kan gedurende de looptijd van de overeenkomst een CERT-retainer, conform de definitie in de Gunningsleidraad, als aanvullende dienstverlening afroepen. Anders dan bij de losse opdracht uit eis 9.6 gaat het hierbij om vooraf gecontracteerde beschikbaarheid en gegarandeerde responscapaciteit. Deze optie kan worden geactiveerd indien de huidige landelijk gecontracteerde CERT-retainer van VNOG afloopt, wordt beëindigd of niet langer passend beschikbaar is. Het einde van de huidige retainer is voorzien in 2027. Inschrijver toont bij inschrijving aan te beschikken over de organisatorische inrichting, gekwalificeerde expertise en voldoende capaciteit om specialistische incidentrespons te kunnen leveren. Dit omvat ten minste: • permanente bereikbaarheid en een vastgelegde activeringsprocedure; • specialistische remote en on-site incidentrespons; • digitaal forensisch onderzoek en malwareanalyse; • veiligstelling en analyse van digitaal bewijsmateriaal; • ondersteuning bij containment, eradication en herstel; • technische rapportage en ondersteuning bij evaluatie en nazorg; • vooraf vastgelegde beschikbaarheids-, opkomst- en responstijden. Indien Inschrijver voor deze dienstverlening gebruikmaakt van een onderaannemer, blijft Inschrijver integraal verantwoordelijk voor de beschikbaarheid, kwaliteit, beveiliging en naleving van de overeengekomen eisen. De inhoud, capaciteit, responstijden, activeringsprocedure, tarieven en overige voorwaarden van de CERT-retainer worden vóór activering in overleg met VNOG vastgelegd in het Dossier Afspraken en Procedures (DAP) en, indien van toepassing, de SLA. VNOG heeft geen verplichting deze optie af te nemen.

9.8	VNOG kan gedurende de looptijd van de overeenkomst **Vulnerability Management as a Service** als additionele dienst afroepen. VNOG heeft geen afname- of omzetverplichting. Deze optie maakt geen onderdeel uit van de kwalitatieve beoordeling of de gunningscriteria. Inschrijver neemt hiervoor wel de gevraagde afzonderlijke tarieven op in het prijzenblad. De dienstverlening omvat het periodiek identificeren, analyseren, risicogestuurd prioriteren, rapporteren en opnieuw controleren van technische kwetsbaarheden binnen de door VNOG aangewezen interne IT-omgeving. Onder *as-a-service* wordt verstaan dat Opdrachtnemer de voor de uitvoering benodigde hardware, software, scanvoorzieningen en licenties levert en verantwoordelijk is voor de installatie, configuratie, beveiliging, actualisatie, beschikbaarheid en het technisch beheer daarvan. Na afroep van de optie voert Opdrachtnemer ten minste de volgende werkzaamheden uit: • minimaal eenmaal per vier (4) weken een kwetsbaarheidsscan van de overeengekomen scope; • aanvullende scans op verzoek van VNOG, bijvoorbeeld bij een ernstige actuele kwetsbaarheid of een materiële wijziging in de omgeving; • validatie en analyse van de scanresultaten, waaronder het zoveel mogelijk beperken van foutpositieve bevindingen; • risicogestuurde prioritering op basis van ten minste technische ernst, actuele misbruikbaarheid, beschikbare dreigingsinformatie, blootstelling en het belang van het getroffen systeem voor VNOG; • rapportage van de bevindingen, risico's en concrete hersteladviezen; • onverwijlde melding van kritieke kwetsbaarheden conform de overeengekomen contact- en escalatiematrix; • uitvoering van een herscan nadat VNOG een kwetsbaarheid heeft verholpen, om de effectiviteit van de maatregel vast te stellen; • periodieke rapportage over openstaande kwetsbaarheden, doorlooptijden, trends en restrisico's. De scanfrequentie, scope, uitzonderingen, scanvensters, authenticatiemethode, rapportage, escalatieafspraken, verwerking van gegevens en verantwoordelijkheidsverdeling worden vóór ingebruikname vastgelegd in het Dossier Afspraken en Procedures (DAP). De dienstverlening wordt uitgevoerd overeenkomstig de actuele stand van de techniek en, voor zover toepasselijk, in lijn met de beste praktijken uit de **Handreiking kwetsbaarhedenscans Rijksoverheid (CIO Rijk, 2021)** of een aantoonbaar gelijkwaardig en actueler kader.

	De uitvoering van scans mag niet leiden tot een onaanvaardbare verstoring van de systemen of bedrijfsvoering van VNOG. Actieve exploitatie van aangetroffen kwetsbaarheden vindt uitsluitend plaats na voorafgaande schriftelijke toestemming van VNOG. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen van aanvullende consultancy- en adviesdiensten heeft geen gevolgen voor de inhoud, kwaliteit of prijs van de overeengekomen basisdienstverlening.

9.9	VNOG kan gedurende de looptijd van de overeenkomst **Continuous Threat Exposure Management as a Service** als addaitionele dienst afroepen. VNOG heeft geen afname- of omzetverplichting. Deze optie maakt geen onderdeel uit van de kwalitatieve beoordeling of de gunningscriteria. Inschrijver neemt de gevraagde tarieven afzonderlijk op in het prijzenblad. De CTEM-dienst ondersteunt VNOG bij het continu identificeren, analyseren, prioriteren, valideren en reduceren van relevante cyberexposure binnen de overeengekomen IT-, cloud-, identity-, netwerk- en, indien van toepassing, OT-omgeving. Onder *as-a-service* wordt verstaan dat Opdrachtnemer de benodigde expertise, processen, hardware, software, platformvoorzieningen en licenties levert en verantwoordelijk is voor de installatie, configuratie, beveiliging, actualisatie, beschikbaarheid en het technisch beheer daarvan. Na afroep omvat de dienstverlening ten minste: • het gezamenlijk vaststellen en periodiek actualiseren van de scope, kroonjuwelen en kritieke bedrijfsprocessen; • het verzamelen en correleren van gegevens over kwetsbaarheden, configuratiefouten, identities, toegangsrechten, externe blootstelling, aanvalspaden en relevante dreigingsinformatie; • het risicogestuurd prioriteren van exposures op basis van technische ernst, actuele misbruikbaarheid, bereikbaarheid, dreigingsinformatie, aanvalspaden en de bedrijfswaarde van het getroffen systeem; • het identificeren van mogelijke aanvalsroutes naar de kroonjuwelen en kritieke processen van VNOG; • het valideren of geprioriteerde exposures daadwerkelijk misbruikbaar zijn, zonder verstoring van de dienstverlening en uitsluitend binnen het door VNOG verleende mandaat; • het adviseren over passende beheers- en herstelmaatregelen; • het bewaken van de opvolging en het controleren van de effectiviteit van uitgevoerde maatregelen; • het periodiek rapporteren over trends, restrisico's, aanvalspaden, voortgang en aantoonbare risicoreductie; • het vertalen van relevante bevindingen naar verbeteringen in usecases, detectieregels en SOAR-playbooks. De scope, analysemethoden, validatieactiviteiten, rapportagecyclus, mandaten, escalatieafspraken en verantwoordelijkheidsverdeling worden vóór ingebruikname vastgelegd in het Dossier Afspraken en Procedures (DAP).

	Actieve validatie, aanvalssimulatie of exploitatie vindt uitsluitend plaats na voorafgaande schriftelijke toestemming van VNOG en mag niet leiden tot een onaanvaardbare verstoring van de systemen of bedrijfsvoering. VNOG heeft geen afname- of omzetverplichting voor deze optie. Het niet afnemen van aanvullende consultancy- en adviesdiensten heeft geen gevolgen voor de inhoud, kwaliteit of prijs van de overeengekomen basisdienstverlening.
9.10	Indien VNOG zowel Vulnerability Management as a Service (9.8) als CTEM (9.9) afneemt, geldt dat: • de vulnerabilitymanagementdienst de technische scan-, analyse-, herstel- en herscanfunctie levert; • de CTEM-dienst deze resultaten combineert met aanvullende exposure- en dreigingsinformatie en vertaalt naar aanvalspaden en risicogestuurde prioriteiten; • gegevens, tooling en resultaten zoveel mogelijk worden hergebruikt; • overlappende werkzaamheden niet dubbel in rekening worden gebracht; Opdrachtnemer vooraf inzichtelijk maakt welke activiteiten en kosten onder iedere dienst vallen.
9.11	Opdrachtnemer laat de additionele diensten uitvoeren door aantoonbaar vakbekwaam personeel dat beschikt over actuele, voor de betreffende werkzaamheden relevante kennis, opleiding en ervaring. De ingezette medewerkers werken overeenkomstig algemeen aanvaarde beroeps- en kwaliteitsnormen en de actuele stand van de techniek. Op verzoek van VNOG toont Opdrachtnemer dit aan met relevante certificeringen of cv's.

10. Compliance en regelgeving	
10.1	De aangeboden oplossing en dienstverlening voldoen gedurende de volledige looptijd van de overeenkomst aan de toepasselijke Europese en Nederlandse wet- en regelgeving op het gebied van informatiebeveiliging, cybersecurity, privacy en gegevensbescherming, waaronder in ieder geval de AVG en de daarop gebaseerde Nederlandse uitvoeringswetgeving. Opdrachtnemer volgt relevante wijzigingen in wet- en regelgeving actief en voert tijdig de noodzakelijke aanpassingen door. Opdrachtnemer informeert VNOG onverwijld over wijzigingen of omstandigheden die gevolgen kunnen hebben voor de naleving, beveiliging, gegevensverwerking of dienstverlening en verstrekt op verzoek aantoonbare documentatie over de getroffen maatregelen. Deze verplichtingen gelden eveneens voor door Opdrachtnemer ingeschakelde onderaannemers en subverwerkers.

10.2	De oplossing en dienstverlening ondersteunen VNOG aantoonbaar bij het voldoen aan en verantwoorden over de voor VNOG relevante eisen uit: • de Algemene verordening gegevensbescherming (AVG); • de Baseline Informatiebeveiliging Overheid (BIO); • de NIS2-richtlijn en de daarop gebaseerde Nederlandse wet- en regelgeving; • ISO/IEC 27001; • SOC 2 of een aantoonbaar gelijkwaardig assurancekader. Opdrachtnemer stelt hiervoor passende beveiligingsmaatregelen, rapportages, loggegevens, auditinformatie en overige bewijsstukken beschikbaar. Op verzoek licht Opdrachtnemer toe hoe de geleverde dienstverlening aansluit op de genoemde kaders en werkt hij mee aan relevante audits en assessments. De ondersteuning door Opdrachtnemer laat de eigen verantwoordelijkheid van VNOG voor naleving van de toepasselijke wet- en regelgeving en normenkaders onverlet.
10.3	Alle VNOG-gerelateerde gegevens worden binnen de Europese Economische Ruimte (EER) opgeslagen en verwerkt, overeenkomstig eis 4.1. Dit geldt tevens voor log- en eventdata, incidentgegevens, metadata, back-ups, rapportages en gegevens die voor beheer- en ondersteuningsdoeleinden worden verwerkt. Opslag, verwerking of toegang van buiten de EER is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van VNOG en met inachtneming van de toepasselijke privacywetgeving en contractuele afspraken. Opdrachtnemer verstrekt op verzoek inzicht in de gebruikte verwerkingslocaties en de betrokken onderaannemers en subverwerkers.
10.4	Opdrachtnemer biedt transparantie over: • subverwerkers; • datalocaties • supportlocaties.

10.5	Voor zover van toepassing op de scope van de opdracht ondersteunt en gebruikt de aangeboden oplossing de open standaarden die zijn opgenomen op de actuele **'pas toe of leg uit'-lijst** en de **lijst met aanbevolen standaarden** van het Forum Standaardisatie, overeenkomstig eis 4.7. Indien Opdrachtnemer een toepasselijke standaard niet kan of zal toepassen, motiveert hij dit vooraf schriftelijk en beschrijft hij: • waarom toepassing niet mogelijk of doelmatig is; • welke gelijkwaardige standaard of oplossing wordt toegepast; • wat de gevolgen zijn voor interoperabiliteit, beveiliging, gegevensuitwisseling, beheer en leveranciersafhankelijkheid; • op welke wijze toekomstige ondersteuning of migratie wordt gewaarborgd. De toepassing van standaarden dient gedurende de looptijd aan te sluiten op de dan actuele lijsten van het Lijst open standaarden | Forum Standaardisatie. Wijzigingen die gevolgen hebben voor de dienstverlening worden vooraf met VNOG afgestemd.

11. Facturatie en betaling	
11.1	Facturen worden elektronisch aangeleverd, bij voorkeur via Peppol. Indien Opdrachtnemer de factuur niet via Peppol kan aanleveren, dienen de facturen in PDF per mail te worden verstuurd naar financiën@vnog.nl .
11.2	Facturen voldoen aan de wettelijke factuurvereisten en bevatten een verplichtingennummer/routenummer, dat na gunning kenbaar wordt gemaakt.
11.3	VNOG hanteert een betalingstermijn van 30 dagen na ontvangst van de factuur.
11.4	Indien facturen niet voldoen aan eis 11.1 en 11.2, is VNOG bevoegd de betalingsverplichting op te schorten totdat de ontbrekende gegevens zijn aangeleverd. VNOG stelt Opdrachtnemer hiervan op de hoogte.
11.5	De vergoeding voor monitoring en detectie is verschuldigd naar rato vanaf het moment dat de monitoring van de bestaande XDR- en SIEM-omgeving aantoonbaar operationeel is (eis 8.2, uiterlijk 19 maart 2027). De vergoeding voor de volledige dienstverlening is verschuldigd vanaf de formele acceptatie door VNOG. Eenmalige kosten voor implementatie en onboarding worden uitsluitend in rekening gebracht voor zover deze in het Prijzenblad zijn opgenomen.