Selectieleidraad Europese niet openbare aanbestedingsprocedure

SIEM, SOC, SOAR-dienstverlening

TenderNed kenmerk	: TN 600148
Zaaknummer	: 26-76552
Projectnummer	: P26-004
Uitgevoerd door	: Luc Peeters, Jan Grasdijk en Edwin Moraal
Versie	: Definitief
Datum	: 17 juli 2026

Inhoudsopgave

Begrippenlijst

Termen die in deze Selectieleidraad met een hoofdletter beginnen, hebben de hiernavolgende betekenis. Termen die niet in deze begrippenlijst zijn vermeld, maar wel zijn gedefinieerd in de Aanbestedingswet hebben de betekenis conform de Aanbestedingswet.

Aanbestedende dienst	Veiligheidsregio Noord- en Oost-Gelderland (VNOG)
Aanbestedingsdocumenten	Alle documenten die door VNOG in de aanbestedingsprocedure zijn gebracht, waaronder tevens de aankondiging van de Opdracht en de Nota's van Inlichtingen.
Aanbestedingswet 2012	Aanbestedingswet 2012, afgekort: Aw. De Aanbestedingswet kan worden geraadpleegd op wetten.overheid.nl.
BIO – Baseline Informatiebeveiliging Overheid	De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging binnen de Nederlandse overheid. De BIO bevat maatregelen en uitgangspunten voor het beheersen van informatiebeveiligingsrisico's en vormt een belangrijk referentiekader voor organisaties met een publieke of vitale taak.
CERT (Computer Emergency Response Team)	Een permanent inzetbaar Computer Emergency Response Team (CERT), waarbij gedurende vierentwintig (24) uur per dag, zeven (7) dagen per week en driehonderdvijfenzestig (365) dagen per jaar gekwalificeerde cybersecurityspecialisten beschikbaar zijn voor de analyse, beheersing en afhandeling van ernstige cybersecurityincidenten. De dienstverlening omvat ten minste technische incidentanalyse, digitale forensische onderzoeken, malware-analyse, containment-, eradication- en herstelwerkzaamheden, crisiscoördinatie, technisch incidentmanagement en advisering over mitigerende maatregelen. De dienstverlening is zodanig ingericht dat de continuïteit van de incidentrespons te allen tijde is gewaarborgd. Er is geen sprake van CERT-dienstverlening indien de ondersteuning uitsluitend bestaat uit telefonische bereikbaarheid, consignatie- of piketdiensten zonder de mogelijkheid tot directe operationele inzet.
Combinatie	Een samenwerkingsverband van twee of meer ondernemingen die gezamenlijk deelnemen aan de aanbestedingsprocedure en gezamenlijk verantwoordelijk zijn voor de uitvoering van de Opdracht.

Continuous Threat Exposure Management (CTEM),	Een risicogestuurde werkwijze waarbij continu digitale blootstellingen, kwetsbaarheden en aanvalspaden worden geïdentificeerd, geanalyseerd, geprioriteerd en opgevolgd, zodat cyberrisico's tijdig worden beperkt. De dienstverlening omvat ten minste exposure monitoring, het identificeren van kwetsbaarheden en het bieden van concreet handelingsperspectief ter verbetering van de digitale weerbaarheid.
Derde	Een natuurlijke persoon of rechtspersoon op wiens financiële en economische draagkracht of technische en beroepsbekwaamheid een Gegadigde of Inschrijver zich beroept om aan de gestelde Geschiktheidseisen te voldoen.
Economisch Meest Voordelige Inschrijver (EMVI)	Het gunningscriterium waarbij de Opdracht wordt gegund aan de Inschrijving met de beste prijs-kwaliteitverhouding.
Gegadigde	De marktpartij die participeert in fase 1 van deze aanbestedingsprocedure (en een verzoek tot deelname indient).
Geschiktheidseisen	Geschiktheidseisen zijn minimumeisen waaraan een Gegadigde dient te voldoen om voor deelname aan de Gunningsfase in aanmerking te komen. Indien niet aan een Geschiktheidseis wordt voldaan, wordt de Gegadigde uitgesloten van verdere deelname aan de aanbestedingsprocedure.
Geselecteerde Gegadigde	Het gunningscriterium waarbij de Opdracht wordt gegund aan de Inschrijving met de beste prijs-kwaliteitverhouding.
Gunningscriterium	Het criterium of de criteria op basis waarvan de Aanbestedende dienst bepaalt aan welke Inschrijver de Opdracht wordt gegund.
Gunningsfase	De tweede fase van een niet-openbare aanbesteding waarin Geselecteerde gegadigden een Inschrijving indienen en de Aanbestedende dienst, op basis van het gunningscriterium Economisch Meest Voordelige Inschrijving (EMVI), de Inschrijving met de beste prijs/kwaliteits-verhouding bepaald.
Gunningsleidraad	Het document behorende bij de Gunningsfase van een niet-openbare aanbesteding, waarin de eisen, Gunningscriteria en beoordelingsmethodiek voor het indienen van een Inschrijving zijn opgenomen.
Inschrijver	De geselecteerde Gegadigde voor fase 2 van deze aanbestedingsprocedure.

Inschrijving	De aanbieding die is ingediend door een Inschrijver in het kader van de onderhavige aanbestedingsprocedure.
Nota van Inlichtingen	Het document/de documenten met door potentiële Inschrijvers gestelde en door VNOG geanonimiseerde vragen over de aanbestedingsprocedure en de Aanbestedingsdocumenten, inclusief de antwoorden van VNOG op deze vragen.
Opdracht	De Opdracht die het voorwerp van deze aanbestedingsprocedure vormt en zoals die beschreven wordt in de Aanbestedingsdocumenten.
Opdrachtgever	De partij ten behoeve waarvan de Overeenkomst wordt gesloten.
Opdrachtnemer	De Inschrijver(s) aan wie de Opdracht gegund is (zijn) en met wie Opdrachtgever de Overeenkomst(en) heeft gesloten.
Onderaannemer	Een onderneming die door de Opdrachtnemer wordt ingezet voor de uitvoering van (een deel van) de Opdracht, zonder zelf contractpartij van de Opdrachtgever te zijn.
Ondernemer	Iedere natuurlijke persoon of rechtspersoon, dan wel een samenwerkingsverband daarvan, die goederen levert, diensten verricht of werken uitvoert.
Overeenkomst	De (raam)Overeenkomst, met inbegrip van eventuele bijlagen, die als resultaat van deze aanbestedingsprocedure met één Opdrachtnemer zal worden gesloten voor de Opdracht.
Programma van Eisen	Het document met daarin de eisen waaraan het uitgevraagde product, de uitgevraagde dienst en/of het uitgevraagde werk moet voldoen. Het betreffen zogenaamde uitvoeringsvoorwaarden, tenzij uitdrukkelijk anderszins weergegeven. Het Programma van Eisen is als bijlage toegevoegd.
Raamovereenkomst	Een overeenkomst tussen één of meer Opdrachtgevers en één of meer Opdrachtnemers met als doel gedurende een bepaalde periode de voorwaarden inzake te plaatsen opdrachten vast te leggen.
Selectiefase	De eerste fase van een niet-openbare aanbesteding waarin gegadigden een verzoek tot deelneming indienen en de Aanbestedende dienst, op basis van Uitsluitingsgronden, Geschiktheidseisen en selectiecriteria, bepaalt welke

	gegadigden worden uitgenodigd voor de Gunningsfase.
Selectieleidraad	Het document behorende bij de Selectiefase van een niet-openbare aanbesteding, waarin de procedure, voorwaarden, Uitsluitingsgronden, Geschiktheidseisen, selectiecriteria en overige informatie voor het indienen van een verzoek tot deelneming zijn opgenomen.
TenderNed	Het digitale online aanbestedingsplatform waarvan VNOG ten behoeve van deze aanbestedingsprocedure gebruik maakt en waarlangs deze hele aanbestedingsprocedure verloopt.
Uitsluitingsgronden	Omstandigheden die, indien Inschrijver daarin verkeert, kunnen leiden tot uitsluiting van verdere deelname aan deze aanbestedingsprocedure. Er wordt onderscheid gemaakt tussen facultatieve en verplichte Uitsluitingsgronden. De op de onderhavige aanbestedingsprocedure toepasselijke Uitsluitingsgronden vloeien voort uit het UEA.
Uniform Europees Aanbestedingsdocument (UEA)	Het UEA is de eigen verklaring van de Inschrijver zoals bedoeld in artikel 2.84 Aanbestedingswet 2012 over o.a. de Uitsluitingsgronden en de geschiktheidseisen.
Verificatiefase	De fase waarin VNOG bewijsstukken kan opvragen, controleren en verifiëren of de door een Gegadigde of Inschrijver verstrekte informatie juist is en of wordt voldaan aan de gestelde eisen en voorwaarden.
Verzoek tot Deelneming	De aanmelding die door een Gegadigde wordt ingediend in de Selectiefase van een niet-openbare aanbestedingsprocedure.
24/7 Eyes-on-Glass	Een permanent bemand Security Operations Center (SOC), waarbij gedurende vierentwintig (24) uur per dag, zeven (7) dagen per week en driehonderdvijfenzestig (365) dagen per jaar gekwalificeerde securityanalisten (minimaal L1 en L2 aanwezig) actief belast zijn met het realtime monitoren, analyseren, classificeren, verrijken, prioriteren en escaleren van security-events en beveiligingsincidenten. De dienstverlening is zodanig ingericht dat de continuïteit van de monitoring en opvolging te allen tijde is gewaarborgd, ook 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.

Inleiding

Voor u ligt de Selectieleidraad voor de Europese niet-openbare aanbesteding SIEM, SOC, SOAR-dienstverlening voor Veiligheidsregio Noord- en Oost-Gelderland (VNOG).

Doel van de aanbesteding
Het doel van deze aanbesteding is het sluiten van een overeenkomst met één opdrachtnemer voor de levering van SIEM-, SOC- en SOAR-dienstverlening voor een initiele periode van vier (4) jaar, met de optie voor VNOG om de overeenkomst tweemaal met twee (2) jaar te verlengen, derhalve een maximale looptijd van acht (8) jaar. De beoogde ingangsdatum van de overeenkomst is maandag 26 april 2027.

Deze Selectieleidraad heeft tot doel Gegadigden te selecteren die geschikt zijn om in de volgende fase een Inschrijving in te dienen. In hoofdstukken 3 en 4 is beschreven op welke wijze de selectie plaatsvindt, welke documenten moeten worden overgelegd en aan welke criteria moet worden voldaan om uitgenodigd te worden tot het indienen van een Inschrijving. Gegadigden worden uitgenodigd om op basis van de in deze Selectieleidraad opgenomen informatie een verzoek tot deelneming in te dienen, met inachtneming van de hierin gestelde eisen en voorwaarden.

Voor deze aanbestedingsprocedure wordt gebruikgemaakt van een elektronisch aanbestedingsplatform, namelijk TenderNed. Communicatie over inhoudelijke of procedurele aspecten dient uitsluitend elektronisch via TenderNed te geschieden. Voor instructies met betrekking tot het gebruik van TenderNed wordt verwezen naar www.tenderned.nl.

Aanbestedende dienst

1.1 Veiligheidsregio Noord- en Oost- Gelderland

De Aanbestedende dienst is VNOG. VNOG heeft één missie:

Samen werken aan veiligheid.

Onze belangrijkste doelen zijn het voorkomen, beperken en bestrijden van incidenten, rampen en crises, en herstel na een ontwrichte situatie. Dit doen wij samen met partners als politie, ambulancediensten, waterschappen en defensie.

Wij werken vanuit onze merken: VNOG, Brandweer en GHOR (geneeskundige hulpverlening in de regio).

VNOG is één van de 25 veiligheidsregio's in Nederland. In de regio werken 22 gemeenten samen, van Winterswijk tot Harderwijk. In de afdeling Risico- en crisisbeheersing komen de lijnen samen die VNOG met andere partners in de hulpverlening kent. Daarbij gaat het onder andere om Defensie, Rijkswaterstaat en waterschappen.

Een fijnmazig netwerk van 56 brandweerposten én betrokken (vrijwillige) medewerkers vormen de basis voor de uitruktaken van de brandweer in onze veiligheidsregio.

De GHOR geeft op basis van afspraken met ambulancediensten, zorginstellingen, zorgaanbieders en de GGD-invulling aan de geneeskundige hulpverlening bij rampen en ongevallen.

Voor meer informatie over VNOG wordt verwezen naar de website www.vnog.nl.

2 Algemene informatie en omschrijving van de opdracht

2.1 Omschrijving van de opdracht

Het doel van deze opdracht is het contracteren van één opdrachtnemer die VNOG ondersteunt bij het monitoren, detecteren, analyseren en opvolgen van cybersecuritydreigingen en beveiligingsincidenten door middel van geïntegreerde SIEM-, SOC- en SOAR-dienstverlening. VNOG beoogt hiermee de digitale weerbaarheid van de organisatie te versterken, de informatiebeveiliging verder te professionaliseren en tijdig te kunnen reageren op beveiligingsincidenten en dreigingen.

De scope van de opdracht omvat in ieder geval de levering, implementatie, inrichting, beheer en doorontwikkeling van SIEM-, SOC- en SOAR-dienstverlening, waaronder mede begrepen:

- Het verzamelen, correleren en analyseren van log- en securitydata;
- Security Monitoring en detectie van afwijkingen en dreigingen;
- Security Incident Response en opvolging van beveiligingsincidenten;
- Het beschikbaar stellen van een Security Operations Center (SOC);
- Use case management en optimalisatie van detectieregels;
- Rapportages en advisering over beveiligingsincidenten, dreigingen en trends;
- Ondersteuning bij compliance- en auditvraagstukken;
- Automatisering en orkestratie van securityprocessen middels SOAR-functionaliteiten;
- Onboarding van databronnen en koppelingen met relevante systemen van VNOG.

De volgende opties maken onderdeel uit van de opdracht:

- Wijziging van het aantal aangesloten databronnen en systemen;
- Aanvullende consultancy- en adviesdiensten op het gebied van cybersecurity en informatiebeveiliging;
- Uitbreiding van SOC-dienstverlening naar aanvullende serviceniveaus;
- Aanvullende incident response ondersteuning;
- Ondersteuning bij audits, compliance- en rapportagevraagstukken;
- Aanvullende trainingen en awarenessactiviteiten voor medewerkers van VNOG.

Buiten de scope van deze opdracht vallen in ieder geval:

- De levering en vervanging van generieke kantoorautomatiseringsmiddelen;

- Volledig beheer van de IT-infrastructuur van VNOG;
- Het uitvoeren van penetration tests en red teaming, tenzij expliciet als optie of aanvullende dienstverlening overeengekomen;
- De levering van niet aan de SIEM-, SOC- en SOAR-dienstverlening gerelateerde cybersecuritydiensten;
- Werkzaamheden die behoren tot reguliere functionele of technische beheeractiviteiten van applicatiesystemen van VNOG.

De overeenkomst
VNOG wenst met één Inschrijver die de economisch meest voordelige Inschrijving heeft gedaan een Overeenkomst te sluiten voor de levering van SIEM-, SOC- en SOAR-dienstverlening.

De uitvoering van de Overeenkomst vangt aan op 26 april 2027 en loopt tot en met 25 april 2031, met de optie voor VNOG om de Raamovereenkomst tweemaal eenzijdig te verlengen met een periode van twee (2) jaar, derhalve uiterlijk tot en met 25 april 2035.

De toekomstige Opdrachtnemer, en ook de door de Opdrachtnemer te leveren dienstverlening, dienen te voldoen aan de voorwaarden en eisen zoals opgenomen in de aanbestedingsdocumenten.

Budget
VNOG hanteert een plafondbedrag van Euro 1.400.000,- excl. BTW en excl. additionele dienstverlening (conform 2.1.3) voor deze dienst voor de volledige periode van 8 jaar (4 +2 +2). Een inschrijving boven dit plafondbedrag zal tot uitsluiting leiden.

2.1.1 Beveiligingsomgeving VNOG

VNOG beschikt over een complexe hybride IT- en OT-omgeving die de digitale ondersteuning vormt van haar primaire processen op het gebied van brandweerzorg, crisisbeheersing en rampenbestrijding. De dienstverlening die onderdeel uitmaakt van deze aanbesteding heeft betrekking op de beveiliging van onder meer endpoints, identiteiten, cloudomgevingen, netwerkcomponenten, OT-componenten en overige bedrijfskritische systemen.

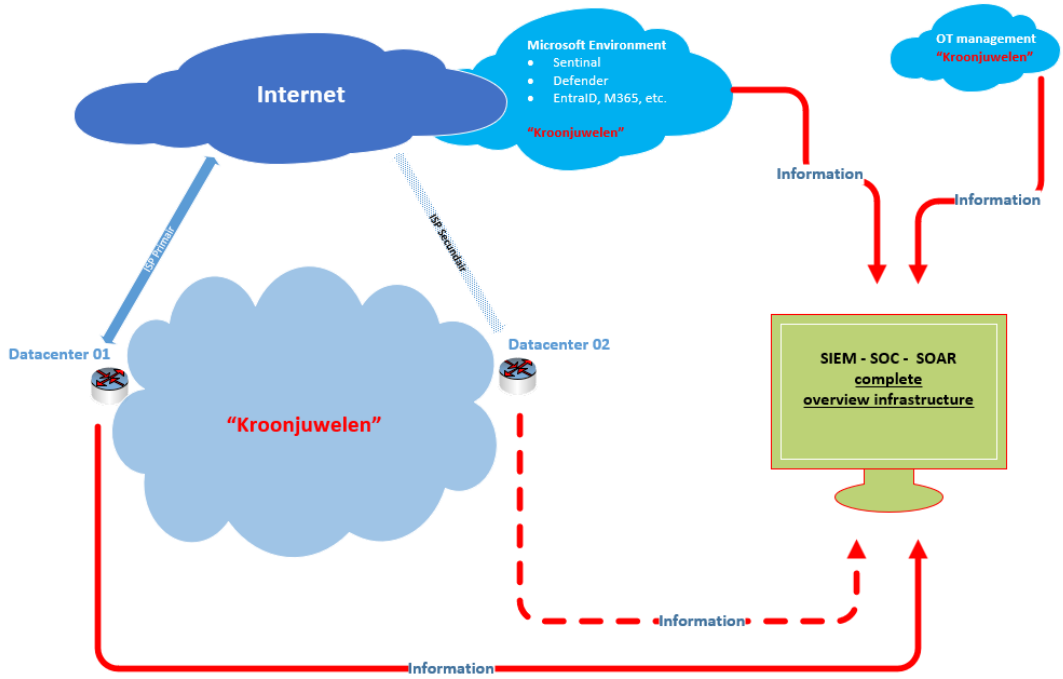
Figuur 1 geeft op hoofdlijnen een schematische weergave van de beveiligingsomgeving van VNOG en de belangrijkste beveiligingsdomeinen waarop de gevraagde dienstverlening betrekking heeft.

De weergegeven omgeving is bewust vereenvoudigd weergegeven. VNOG acht het vanuit beveiligingsoogpunt niet wenselijk om (in de selectiefase) gedetailleerde informatie te verstrekken over onder meer de netwerkarchitectuur, beveiligingsmaatregelen, detectiearchitectuur, logbronnen, use cases, playbooks, koppelingen, OT-componenten, bedrijfskritische systemen en overige bedrijfsgevoelige informatie.

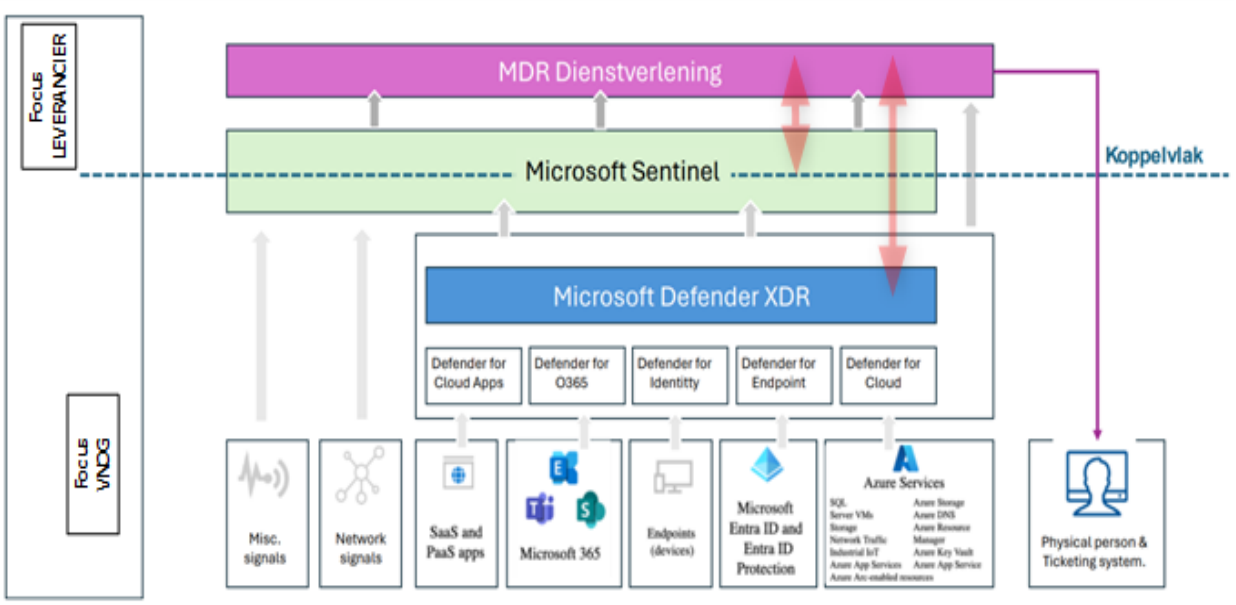
Openbaarmaking van dergelijke informatie kan inzicht geven in de wijze waarop VNOG haar digitale weerbaarheid heeft ingericht en daarmee het aanvalsoppervlak vergroten. Om die reden wordt deze informatie uitsluitend verstrekt voor zover dit noodzakelijk is

en uitsluitend en in beperkte mate aan de geselecteerde Gegadigden gedurende de gunningsfase. Ook met NDA's resteert verspreidings- en hergebruikrisico, zeker bij subcontractors of ketenpartijen. Gefaseerde en beperkte informatieverstrekking draagt bij aan de bescherming van de beveiligingsarchitectuur en vitale processen van VNOG en beschermt haar veiligheidsbelangen.

Informatieverstrekking kan een reëel veiligheidsrisico opleveren, waarbij openbaarmaking ernstig en onomkeerbaar is, die niet onder toepassing van de Aanbestedingswet kan worden beschermd. Daarmee betreft dit een opdracht waarbij informatieverstrekking en de openbaarmaking strijdig is met een essentieel veiligheidsbelang, waardoor de Aanbestedingswet niet van toepassing is (artikel 2.23 lid 1 sub e Aw). Opdrachtgever maakt hierdoor gebruik van de Aanbestedingswet Defensie- en Veiligheidsgebied (ADV).



Figuur 1 – Beveiligingsomgeving VNOG



Figuur 2 – Beveiligingsomgeving VNOG

2.1.2 24/7 Eyes-on-Glass

Tijdens de marktconsultatie is gebleken dat marktpartijen verschillende invullingen geven aan het begrip 24/7 monitoring. Aanbestedende dienst acht het daarom wenselijk dit begrip vooraf te verduidelijken. De definitie die Aanbestedende dienst voor deze aanbesteding hanteert voor 24/7 Eyes-on-glass is opgenomen als definitie.

Hiermee geeft Aanbestedende dienst het basisniveau voor deze voor haar essentiële dienstverlening aan.

2.1.3 Additionele dienstverlening

Aanbestedende dienst kan momenteel voor het direct reageren op, beheersen van en herstellen van acute veiligheidsincidenten gebruik maken van een landelijk gecontracteerde CERT-retainer. Deze overeenkomst zal in 2027 aflopen.

Aanbestedende dienst acht het vanuit het oogpunt van continuïteit, samenhang en effectieve incidentafhandeling wenselijk dat deze dienstverlening gedurende de looptijd van de Overeenkomst bij dezelfde Opdrachtnemer kan worden ondergebracht als de SIEM-, SOC- en SOAR-dienstverlening. Om die reden wenst Aanbestedende dienst de mogelijkheid te hebben deze dienstverlening als additionele dienstverlening af te nemen, indien de huidige overeenkomst afloopt of wordt beëindigd.

Om deze reden dient Gegadigde reeds in de selectiefase aan te tonen dat hij beschikt over de benodigde organisatorische inrichting, expertise en capaciteit om specialistische incidentrespons te kunnen leveren.

2.2 Opdeling in percelen

VNOG heeft ervoor gekozen de opdracht voor de SIEM-, SOC- en SOAR-dienstverlening niet op te delen in percelen.

VNOG acht het van belang dat detectie, monitoring, analyse, incidentopvolging en eventuele geautomatiseerde respons binnen één samenhangende dienstverlening worden uitgevoerd, met één centrale contractuele en operationele verantwoordelijkheid. Daarnaast draagt een integrale opdracht bij aan de continuïteit, snelheid van incidentafhandeling, eenduidige governance en beperking van afstemmings- en integratierisico's binnen de dienstverlening.

De gevraagde dienstverlening vormt één samenhangend geheel. De verschillende onderdelen zijn sterk met elkaar verbonden en kunnen niet goed los van elkaar worden uitgevoerd zonder afbreuk te doen aan de kwaliteit en effectiviteit van de dienstverlening. Daarnaast draagt één perceel bij aan een betere beheersbaarheid van de uitvoering. Het werken met één opdrachtnemer verkleint de risico's in de samenwerking, afstemming en verantwoordelijkheid.

Er zijn voldoende partijen die de gevraagde dienstverlening integraal kunnen aanbieden. Het opdelen in percelen is daarom niet noodzakelijk.

3 Informatie over de aanbesteding

3.1 Fasen

De aanbesteding wordt uitgevoerd volgens de niet-openbare procedure als bedoeld in de Aanbestedingswet op defensie- en veiligheidsgebied (ADV) en kent twee fasen:

- De Selectiefase en
- De Gunningsfase.

Fase 1: Selectiefase
In deze fase worden de aanmeldingen van gegadigden beoordeeld op grond van de gestelde aanmeldingsvoorwaarden, uitsluitingsgronden, geschiktheidseisen en, indien van toepassing, selectiecriteria.

Doel van deze fase is het selecteren van maximaal vijf (5) gegadigden, mits er voldoende geschikte gegadigden beschikbaar zijn.

Alle documenten die nodig zijn voor deze fase – waaronder deze Selectieleidraad en de bijlagen – zijn beschikbaar via het aanbestedingsplatform TenderNed. Gegadigden dienen op basis van deze documenten hun verzoek tot deelneming op te stellen en digitaal via TenderNed in te dienen.

Als de aanmelding wordt ingediend door een samenwerkingsverband, moeten de gevraagde gegevens en documenten worden verstrekt voor ieder afzonderlijk lid van het samenwerkingsverband.

Na sluiting van de aanmeldingsperiode worden de verzoeken tot deelneming als volgt beoordeeld:

- Toetsing aan de aanmeldingsvoorwaarden;
- Toetsing aan de uitsluitingsgronden en geschiktheidseisen;
- Toepassing van de selectiecriteria (als meer dan vijf gegadigden voldoen aan de minimumeisen).

De vijf hoogst gerangschikte gegadigden worden geselecteerd voor deelname aan de gunningsfase.

De Aanbestedende dienst behoudt zich het recht voor om bewijsstukken met betrekking tot de uitsluitingsgronden en geschiktheidseisen op te vragen bij de geselecteerde gegadigden. Deze bewijsstukken dienen binnen zeven (7) kalenderdagen na het verzoek te worden overgelegd. Als uit deze bewijsstukken blijkt dat de gegadigde niet voldoet aan de eisen, of zich bevindt in een uitsluitingsgrond, wordt de aanmelding alsnog terzijde gelegd.

Na afronding van de beoordeling ontvangen alle gegadigden bericht of zij al dan niet geselecteerd zijn voor de volgende fase van de aanbesteding.

Fase 2: Gunningsfase
De geselecteerde Gegadigden (in fase 2 genaamd Inschrijvers) worden uitgenodigd tot deelname aan de gunningsfase. Zij ontvangen hiertoe de Gunningsleidraad met daarin de eisen, gunningscriteria en beoordelingsmethodiek.

In de gunningsfase dienen de Inschrijvers een complete Inschrijving in, waaronder een prijsaanbieding. Deze Inschrijving wordt beoordeeld op basis van het gunningscriterium Economisch Meest Voordelige Inschrijving (EMVI), waarbij de beste prijs-kwaliteitsverhouding leidend is.

De Inschrijvers dienen een reële en marktconforme aanbieding te doen. Als de Aanbestedende dienst besluit tot gunning over te gaan, wordt de overeenkomst gegund aan de Inschrijver die voldoet aan de gestelde eisen en de economisch meest voordelige Inschrijving heeft ingediend.

De overige Inschrijvers ontvangen schriftelijk bericht van afwijzing.

3.2 Aanbestedingsplatform

De aanbestedingsprocedure verloopt via TenderNed. Communicatie over inhoudelijke aspecten en aspecten rond de aanbestedingsprocedure dienen te allen tijde elektronisch te geschieden via de vraag en antwoordmodule van TenderNed.

Het is niet toegestaan om tijdens deze aanbestedingsprocedure direct of indirect de (medewerkers van de) Aanbestedende dienst te benaderen over deze Aanbesteding zonder expliciete toestemming van Aanbestedend dienst. Dit op straffe van uitsluiting.

Voor vragen die alleen gaan over de werking of techniek van TenderNed, kunt u contact opnemen met de servicedesk van TenderNed. VNOG zal deze vragen en antwoorden niet opnemen en beantwoorden in de Nota van Inlichtingen.

3.3 Globale planning

De onderstaande tabel bevat de beoogde planning van de aanbestedingsprocedure. De Aanbestedende dienst behoudt zich het recht voor deze planning aan te passen. Aan deze planning kunnen geen rechten worden ontleend.

Eventuele wijzigingen worden via het aanbestedingsplatform TenderNed gecommuniceerd. De planning opgenomen in TenderNed is vanaf publicatie leidend.

Activiteiten	Datum
Selectiefase	
Publicatie Selectieleidraad via TenderNed	Vrijdag 17 juli 2026
Sluitingsdatum voor het indienen van vragen over de Selectieleidraad	**Vrijdag 28 augustus 2026, 12:00 uur**
Publicatie Nota van Inlichtingen	Vrijdag 11 september 2026
Sluitingsdatum voor het indienen van Verzoek tot Deelneming	**Vrijdag 25 september 2026, 12:00 uur**
Kennisgeving voorgenomen selectiebeslissing	Vrijdag 9 oktober 2026
Standstill periode	Zaterdag 10 oktober t/m donderdag 29 oktober 2026
Definitieve selectiebeslissing	Vrijdag 30 oktober 2026
Gunningsfase (indicatief)	
Versturen Gunningsleidraad aan geselecteerden	Maandag 2 november 2026
Sluitingsdatum voor het indienen van vragen over de Gunningsleidraad	**Vrijdag 20 november 2026, 12:00 uur**
Publicatie 1e Nota van Inlichtingen	Vrijdag 27 november 2026
Sluitingsdatum voor het indienen van vragen over de Gunningsleidraad	**Vrijdag 4 december 2026, 12:00 uur**
Publicatie 2e Nota van Inlichtingen	Vrijdag 11 december 2026
Sluitingsdatum voor het indienen van Inschrijvingen	**Vrijdag 8 januari 2027, 12:00 uur**
Mededeling voorlopige gunningsbeslissing	Vrijdag 5 februari 2027
Standstill periode	Zaterdag 6 februari t/m donderdag 25 februari 2027
Definitieve gunning	Vrijdag 26 februari 2027
Implementatieperiode	Vrijdag 26 februari t/m vrijdag 23 april 2027
Ingangsdatum overeenkomst	Maandag 26 april 2027

Gegadigden kunnen geen rechten ontlenen aan deze beoogde planning. De in dit (of het gewijzigde) tijdschema genoemde data over het indienen van vragen en het indienen van Inschrijvingen gelden als **fatale termijnen.**

3.4 Inschrijven in samenwerking met andere ondernemingen

Indien Gegadigde niet zelfstandig in de uitvoering van de Opdracht kan voorzien, is de mogelijkheid aanwezig om in te schrijven in samenwerking met andere ondernemingen. Inschrijven in samenwerking met andere ondernemingen kan op twee manieren:

- Ofwel als samenwerkingsverband ('combinatie') waarbij elke deelnemer aan het samenwerkingsverband ieder voor zich en gezamenlijk hoofdelijk aansprakelijk is voor de gestanddoening van de verplichtingen die voortvloeien uit de Inschrijving en ook de eventuele uitvoering van de Overeenkomst. In de bijlage 1 'Uniform Europees Aanbestedingsdocument' moet worden aangegeven wie de leiding (penvoerder) van het samenwerkingsverband heeft en als verantwoordelijk gemachtigde naar VNOG mag optreden;
- Ofwel als hoofdaannemer-onderaannemer constructie waarbij de hoofdaannemer optreedt als contractpartij en aansprakelijk is voor het nakomen van alle verplichtingen dus inclusief de verplichtingen die in onderaanneming worden gegeven.

Voor rechtspersonen die binnen dezelfde holding vallen geldt dat slechts één onderneming van de holding waartoe zij behoort zich kan aanmelden, tenzij de betreffende ondernemingen kunnen aantonen dat een eventuele offerte volgend op de aanmelding, volledig onafhankelijk van de andere Gegadigden (waaronder zij die deel uitmaken van de holding) wordt opgesteld, in vrije concurrentie tot stand komt, en er vertrouwelijkheid in acht wordt genomen. Indien dit niet kan worden aangetoond, leidt dit tot uitsluiting van verdere deelname voor alle Gegadigden uit die holding.

3.4.1 Aanmelden als samenwerkingsverband (combinatie)

Als een Inschrijving wordt ingezonden door een samenwerkingsverband moet:

- Iedere deelnemer van het samenwerkingsverband dient bijlage 1 'Uniform Europees Aanbestedingsdocument' rechtsgeldig te ondertekenen, alsmede Bijlage 4 'Verklaring Samenwerkingsverband' volledig ingevuld en rechtsgeldig ondertekend bij de aanmelding te voegen.
  Waarmee alle tot dat samenwerkingsverband behorende ondernemingen ieder voor zich en gezamenlijk hoofdelijke aansprakelijkheid aanvaarden voor de gestanddoening van de verplichtingen voortvloeiend uit de Inschrijving, en ook voor de eventuele uitvoering van de Overeenkomst.
- In het 'Uniform Europees Aanbestedingsdocument' (Deel II C) te worden aangegeven wie de overige deelnemer(s) in het samenwerkingsverband is/zijn, welke onderneming namens het samenwerkingsverband penvoerder is en als verantwoordelijk gemachtigde naar VNOG mag optreden en voor welke Geschiktheidseisen een beroep op de onderneming van de ondergetekende wordt gedaan.
- De combinatie dient gezamenlijk aan de geschiktheid eisen te voldoen.

3.4.2 Aanmelden als hoofdaannemer met onderaannemer(s)

In deze constructie is de hoofdaannemer Gegadigde. Indien wordt aangemeld als hoofdaannemer moet:

- in de bijlage 1 'Uniform Europees Aanbestedingsdocument' (Deel II D) te worden aangegeven voor welke Geschiktheidseisen Gegadigde een beroep doet op een onderaannemer (derde) en wie de onderaannemers (derden) zijn. Zowel de hoofdaannemer als de onderaannemer(s) op wie een beroep wordt gedaan, dienen het 'Uniform Europees Aanbestedingsdocument' in te vullen en rechtsgeldig te ondertekenen. Indien Gegadigde voor het voldoen aan één of meer Geschiktheidseisen een beroep doet op een derde, dient tevens Bijlage 5 'Verklaring Middelen Derden' volledig ingevuld en rechtsgeldig ondertekend bij de aanmelding te worden gevoegd.

De hoofdaannemer is bij deze constructie volledig aansprakelijk voor de gestanddoening van de verplichtingen voortvloeiend uit de Inschrijving en ook de eventuele uitvoering van de Overeenkomst. De hoofdaannemer is ook aansprakelijk voor de nakoming van de verplichtingen van de door hem ingeschakelde onderaannemer(s).

Indien Gegadigde een beroep doet op de financiële en economische draagkracht van een andere natuurlijke persoon of rechtspersoon (onderaannemer), is zowel de hoofdaannemer als de onderaannemers(s) op wie een beroep wordt gedaan hoofdelijk aansprakelijk voor de uitvoering van de opdracht.

VNOG kan van de winnende Gegadigde verlangen dat zij, als zij gebruik maakt van een of meer onderaannemers om zich te kwalificeren voor de Overeenkomst, de bewijsstukken overlegt waaruit blijkt dat zij bij de uitvoering van de Opdracht ook werkelijk gebruik kan maken van de betreffende onderaannemer(s) en welk gedeelte van deze Opdracht zij (eventueel) in onderaanneming wil geven. Ook kan VNOG verlangen dat de winnende Gegadigde, per onderaannemer, een verklaring van de betreffende onderaannemer overlegt waarin deze aangeeft bereid te zijn de genoemde werkzaamheden uit te voeren.

3.5 Nota van inlichtingen

VNOG heeft tijdens de Selectiefase twee vragenrondes voorzien. Alle tijdig en op de juiste wijze ingediende verzoeken tot nadere informatie (via de vraag & antwoordmodule van TenderNed) zullen door VNOG geanonimiseerd worden beantwoord en uiterlijk op genoemde data aan alle Gegadigden beschikbaar worden gesteld door publicatie van een Nota van Inlichtingen via TenderNed. Na 11 september 2026 heeft Gegadigde zijn recht ten aanzien van het inwinnen van informatie of het doen van voorstellen verwerkt.

Een Gegadigde kan VNOG verzoeken om bepaalde informatie niet in de Nota van Inlichtingen op te nemen, indien openbaarmaking van deze informatieschade zou toebrengen aan de gerechtvaardigde economische belangen van Gegadigde. Gegadigde kan voornoemde vragen uiterlijk stellen tot en met de in de planning genoemde data voor de vragenrondes aanleveren en moet ook motiveren waarom deze vragen

commercieel vertrouwelijk zijn. In het geval dat VNOG oordeelt dat de vragen commercieel vertrouwelijk zijn, zal zij aan Gegadigde individuele inlichtingen verstrekken. VNOG zal in de Nota van Inlichtingen vermelden dat er individuele inlichtingen zijn verstrekt.

Vragen die na de uiterste gelegenheid tot het indien van vragen door Gegadigde worden gesteld, worden niet door VNOG in behandeling genomen. Zij behoudt zichzelf echter het recht voor om vragen die na de uiterste gelegenheid tot het indienen van vragen, indien proportioneel en zulks ter beoordeling VNOG, alsnog te beantwoorden. De te laat gestelde vragen en mogelijk daarop gegeven antwoorden hebben geen opschortende werking voor de aanbestedingsprocedure.

Informatie die op een later moment verstrekt wordt prevaleert over wat daarvoor verstrekt is, tenzij expliciet anders aangegeven. Gegadigde kan geen rechten ontlenen aan mondeling gedane uitspraken van VNOG.

Als enig door VNOG verstrekte documenten volgens Gegadigde tegenstrijdigheden, onjuistheden of onduidelijkheden bevat, dient hij dit bij de vragenronde(n) kenbaar te maken. Als Gegadigde dit nalaat, heeft dat de consequentie dat hij, voor zo ver dit niet in strijd is met het proportionaliteitsbeginsel, zijn rechten ter zake de tegenstrijdigheid, onjuistheid of onduidelijkheid heeft verwerkt.

3.6 Klachten

Iedere Gegadigde heeft de gelegenheid om vragen te stellen over deze aanbestedingsprocedure. VNOG zal deze vragen op basis van haar ervaring en deskundigheid beantwoorden. Als de vragensteller het niet eens is met het antwoord en dit kenbaar wil maken in de vorm van een klacht of indien een belanghebbende anderszins een klacht heeft over de aanbestedingsprocedure, dient de Gegadigde onderstaande stappen te doorlopen:

Klachten dienen bij voorkeur te worden ingediend met gebruikmaking van ‘Bijlage 6 - Klachtenprocedure VNOG Inclusief Klachtenformulier’.

1. Klager kan zijn klacht kenbaar maken bij de klachtencommissie van de VNOG via;
   klachtenmeldpunt.aanbestedingen@nipv.nl
2. VNOG neemt de klacht in behandeling en stelt de klager per omgaande in kennis van de behandelaar en de verwachte afhandeltermijn;
3. VNOG handelt de klacht af en koppelt dit terug aan de Gegadigde en neemt, afhankelijk van het al dan niet gegrond verklaren van de klacht, passende maatregelen ten aanzien van de opvolging van de klacht of vervolgt de aanbestedingsprocedure ongewijzigd.

Indien klager het niet eens is met de uitspraak van de klachtencommissie van VNOG kan deze zich wenden tot de Commissie van Aanbestedingsexperts. Als bij deze Commissie van Aanbestedingsexperts een klacht m.b.t. deze aanbestedingsprocedure wordt ingediend, wordt klager verzocht hiervan een afschrift te zenden aan de onder paragraaf 2.3 genoemde contactpersoon van VNOG.

Een middels bovenstaande procedure(s) ingediende klacht heeft geen opschortende werking voor deze aanbestedingsprocedure. Een uitspraak van de Commissie van Aanbestedingsexperts is niet bindend voor VNOG. Alleen een rechterlijke uitspraak is bindend voor VNOG.

3.7 Indienen Verzoek tot deelneming

De sluitingsdatum voor het indienen van het Verzoek tot deelneming is in voorgaande planning opgenomen (zie Selectiefase). Indien de sluitingsdatum wijzigt, gebeurt dit enkel in TenderNed. Na de sluitingstermijn is het technisch gezien niet meer mogelijk om een Verzoek tot deelneming in te dienen. Er wordt dringend geadviseerd om niet tot het laatste moment te wachten met het indienen van een Verzoek tot deelneming.

Alleen een digitaal Verzoek tot deelneming die voor of op de uiterste sluitingsdatum is ingediend in TenderNed, wordt door VNOG in behandeling genomen, onder voorbehoud van de situatie als omschreven in artikel 2.109a Aw. Wanneer een Gegadigde zijn Verzoek tot deelneming niet tijdig kan indienen door storing van het elektronisch systeem waarmee het Verzoek tot deelneming moet worden ingediend, wordt een Verzoek tot deelneming aangemerkt als tijdig ingediend, als zich de situatie voordoet als omschreven in artikel 2.109a Aw.

Het risico van te late indiening van uw Verzoek tot deelneming en/of indiening van een onvolledig Verzoek tot deelneming ligt bij Gegadigde. De sluitingstijd voor indienen van Verzoeken tot deelneming zoals opgenomen in het aanbestedingsplatform is leidend en gaat boven alle andere tijdsaanduidingen.

De inhoud van het Verzoek tot deelneming wordt in het volgende hoofdstuk nader toegelicht.

4 Uitsluitingsgronden en Geschiktheidseisen

4.1 Inleiding

Om beoordeeld te worden volgens de gestelde Selectiecriteria (hoofdstuk 5) en om daarmee geselecteerd te worden moet de Gegadigde allereerst niet verkeren in de gestelde Uitsluitingsgronden én voldoen aan de gestelde Geschiktheidseisen. Het niet voldoen aan een of meerdere eisen betekent dat de betreffende Gegadigde niet in aanmerking komt voor selectie. Het verzoek tot deelneming zal dan terzijde worden gelegd en niet verder worden beoordeeld. Tenzij VNOG van opvatting is dat sprake is van een situatie als bedoeld in de artikelen 2.87a en 2.88 Aw.

In het kader van deze aanbesteding moet Gegadigde verschillende bewijsmiddelen aanleveren. Hier wordt onderscheid gemaakt tussen bewijsmiddelen die bij het verzoek tot deelneming ingediend dienen te worden en bewijsmiddelen die pas op verzoek ingediend dienen te worden. Dit is per eis nader uiteengezet.

Bewijsmiddelen die op verzoek van Aanbesteder overlegd dienen te worden moeten binnen 7 werkdagen na dit verzoek door Gegadigde worden overgelegd.

4.2 Uitsluitingsgronden

Op de Gegadigde zijn niet van toepassing de omstandigheden zoals verwoord in de verplichte en facultatieve uitsluitingsgronden. Door het invullen en uploaden van het Uniform Europees Aanbestedingsdocument (hierna: UEA) verklaart Gegadigde dat de in het UEA opgenomen uitsluitingsgronden niet op hem van toepassing zijn.

Daarnaast dient Gegadigde bij het Verzoek tot deelneming de rechtsgeldig ondertekende Bijlage 3 - Verklaring geen Russische betrokkenheid te overleggen.

Bewijsmiddel (op verzoek van Aanbestedende dienst):
De geselecteerde Gegadigde dient, binnen de door Aanbestedende dienst gestelde termijn, desgevraagd de volgende bewijsstukken te overleggen:

- een Gedragsverklaring Aanbesteden (GVA) afgegeven door het ministerie van Justitie en Veiligheid, die op het moment van indiening van de Inschrijving niet ouder is dan twee (2) jaar;
- een Verklaring betalingsgedrag nakoming fiscale verplichtingen afgegeven door de Belastingdienst, die op het moment van indiening van het Verzoek tot deelneming niet ouder is dan zes (6) maanden.

In geval van een samenwerkingsverband of hoofdaannemer/onderaannemer(s) dienen alle deelnemers te voldoen aan de uitsluitingsgronden en dit aan te tonen door middel van een afzonderlijk ingevuld UEA, overeenkomstig paragraaf 2.15.

Let op: het UEA vult op meerdere plaatsen automatisch de voor de Gegadigde positieve antwoorden in. Het blijft de verantwoordelijkheid van de Gegadigde om te controleren of deze antwoorden juist en volledig zijn.

4.3 Geschiktheidseisen

Via het stellen van Geschiktheidseisen moet blijken of de Gegadigde naar het oordeel van VNOG geschikt is. Door het beantwoorden van de vraag in Deel IV met "ja" en het ondertekenen van de bijlage 'Uniform Europees Aanbestedingsdocument' gaat Gegadigde akkoord met de Geschiktheidseisen beschreven in deze paragraaf.

4.3.1 Inschrijving handels en beroepsregister

Om de rechtsgeldigheid van de ondertekende verklaringen en bewijsmiddelen te kunnen vaststellen is het noodzakelijk dat Gegadigde een (kopie van) bewijs van inschrijving in het handels- en/of beroepenregister van de Kamer van Koophandel toevoegt aan het verzoek tot deelname van maximaal 6 maanden oud, te rekenen vanaf sluitingsdatum voor het indienen van het verzoek tot deelname.

Uit deze inschrijving in het handels- en/of beroepenregister moet de tekeningsbevoegdheid te blijken voor tenminste de Inschrijvingssom voor deze Opdracht van degene die het verzoek tot deelname heeft getekend. Mocht degene die het UEA en bewijsstukken heeft ondertekend, niet voorkomen op het uittreksel, dan moet uit een door de degene die wel op het uittreksel voorkomt bij wijze van volmacht opgestelde verklaring te blijken dat de ondertekenaar bevoegd is de Gegadigde rechtsgeldig te binden op het moment van ondertekening.

Ingeval in samenwerkingsverband (combinatie) wordt verzocht deel te nemen, moet iedere deelnemer aan het samenwerkingsverband afzonderlijk bovenstaande acties uitvoeren.
In het geval van een hoofdaannemer die een beroep doet op onderaannemer(s) dienen zowel de hoofdaannemer als de onderaannemer(s) het bovenstaande in te dienen.

Bewijsmiddel (Verzoek tot deelneming):
Gegadigde dient een 'bewijs van inschrijving in het handels- en/of beroepenregister van de Kamer van Koophandel' aan haar verzoek tot deelneming toevoegen.

4.3.2 Financiële en economische draagvlak, Beroeps en aansprakelijkheidsverzekering

Door het ondertekenen van het 'Uniform Europees Aanbestedingsdocument' verklaart Gegadigde:

- dat hij adequaat verzekerd is met een beroeps- en bedrijfsaansprakelijkheidsverzekering met een minimale dekking van € 1.250.000,- per aanspraak (eventueel gemaximeerd tot € 2.500.000,-) voor de uitvoering van de Opdracht. Indien de Overeenkomst met hem wordt gesloten, houdt Gegadigde deze verzekering gedurende de looptijd van de Overeenkomst in stand.

Bewijsmiddel (op verzoek):
Een kopie van een geldige polis of een verklaring van de verzekeraar waaruit blijkt dat Gegadigde beschikt over een beroeps- en bedrijfsaansprakelijkheidsverzekering.

4.3.3 Technische bekwaamheid - Kwaliteitsborging

Door het ondertekenen van het 'Uniform Europees Aanbestedingsdocument' verklaart Gegadigde:

- dat hij beschikt over een geldig **ISO 9001-certificaat** voor kwaliteitsmanagement, waarbij het certificaat is opgesteld door een certificatie-instelling, die erkend is binnen de (inter)nationale accreditatiestructuur.
  Of:
- dat hij een kwaliteitszorgsysteem heeft dat minimaal gelijkwaardig is aan **ISO 9001**. Onder gelijkwaardig wordt verstaan: het voldoen aan de volgende kenmerken:
  - kwaliteitszorg is organisatie breed verankerd (in beleid), geadopteerd door de verantwoordelijke directie en uitgedragen door deze directie (b.v. via kwaliteitshandboek). De directie draagt ook de verantwoordelijkheid voor correcte opzet, uitvoering en beheersing van het kwaliteitsbeleid;
  - aanwezigheid en organisatie brede uitvoering van relevante procedures over dienstverlening/eindproducten en beheer van middelen en documenten, waarbij continue verbetering een belangrijk aandachtspunt is;
  - aanwezigheid van de interne kwaliteitscyclus: meting, analyse en verbetering van kwaliteitsniveaus;
  - aanwezigheid van een periodieke onafhankelijke, deskundige audit op naleving van de kwaliteitsprocedures;
  - klant gerelateerde processen: er is een systeem om ervoor te zorgen dat (vanuit het perspectief van de klant) helder wordt gemaakt wat de behoefte van de klant is en dat deze behoefte verwerkt wordt in uw bedrijfsprocessen.

Bewijsmiddel (op verzoek):
Een kopie van een geldig ISO-certificaat of een beschrijving van een gelijkwaardig systeem.

Ingeval er in samenwerkingsverband (combinatie) wordt ingeschreven, moet iedere deelnemer aan dit samenwerkingsverband afzonderlijk aan de vereisten over de kwaliteitszorg te voldoen.

4.3.4 Technische bekwaamheid - Informatiebeveiliging

Door het ondertekenen van het 'Uniform Europees Aanbestedingsdocument' verklaart Gegadigde:

- dat hij beschikt over een geldig **ISO/IEC 27001-certificaat** voor informatiebeveiliging, waarbij het certificaat is opgesteld door een certificatie-instelling, die

erkend is binnen de (inter)nationale accreditatiestructuur, en waarvan de reikwijdte (scope) betrekking heeft op de aangeboden dienstverlening waarop deze aanbesteding ziet.
Of:

- dat hij een informatiebeveiligingsmanagementsysteem heeft dat minimaal gelijkwaardig is aan **ISO/IEC 27001**. Onder gelijkwaardig wordt verstaan: het voldoen aan de volgende kenmerken:
    - Informatiebeveiliging is organisatie breed verankerd in beleid, geadopteerd door de verantwoordelijke directie en uitgedragen door deze directie. De directie draagt ook de verantwoordelijkheid voor correcte opzet, uitvoering en beheersing van het informatiebeveiligingsbeleid;
    - aanwezigheid en organisatie brede uitvoering van relevante procedures voor het identificeren, beoordelen en beheersen van informatiebeveiligingsrisico's;
    - aanwezigheid van passende technische en organisatorische maatregelen voor de bescherming van vertrouwelijkheid, integriteit en beschikbaarheid van informatie;
    - aanwezigheid van procedures voor toegangsbeveiliging, logging, monitoring, incidentmanagement en wijzigingsbeheer;
    - aanwezigheid van een interne verbetercyclus gericht op meting, analyse, evaluatie en verbetering van het informatiebeveiligingsniveau;
    - aanwezigheid van een periodieke onafhankelijke, deskundige audit op naleving van de informatiebeveiligingsprocedures;
    - aanwezigheid van processen waarmee wordt geborgd dat informatiebeveiligingseisen van klanten worden vastgesteld, beoordeeld en verwerkt in de dienstverlening.
    - de reikwijdte van het informatiebeveiligingsmanagementsysteem heeft aantoonbaar betrekking op de dienstverlening waarop deze aanbesteding ziet.

Bewijsmiddel (op verzoek):
Een kopie van een geldig ISO-certificaat of een beschrijving van een gelijkwaardig systeem.

Ingeval er in samenwerkingsverband (combinatie) wordt ingeschreven, moet iedere deelnemer aan dit samenwerkingsverband afzonderlijk aan de vereisten over de informatiebeveiliging te voldoen.

4.3.5 Technische bekwaamheid – Beheersing van de dienstverlening

- Gegadigde beschikt over een geldig **SOC 2 Type II-rapport**, waaruit blijkt dat de beheersmaatregelen rondom de aangeboden dienstverlening gedurende de auditperiode aantoonbaar effectief hebben gefunctioneerd.
  Of:
- dat hij beschikt over een aantoonbaar gelijkwaardig assurance- of auditrapport. Onder gelijkwaardig wordt verstaan: het voldoen aan de volgende kenmerken:
    - periodieke onafhankelijke toetsing van de opzet, het bestaan en de werking van de beheersmaatregelen rondom de aangeboden dienstverlening;

- aantoonbare borging van de vertrouwelijkheid, integriteit en beschikbaarheid van de dienstverlening;
- aanwezigheid van passende beheersmaatregelen voor toegangsbeheer, logging, monitoring, wijzigingsbeheer en incidentmanagement;
- aantoonbare periodieke toetsing van de effectiviteit van de getroffen beheersmaatregelen;
- uitvoering van de audit door een onafhankelijke, deskundige auditor;
- verstrekking van een assurance- of auditrapport waaruit blijkt dat de beheersmaatregelen gedurende een representatieve auditperiode aantoonbaar effectief hebben gefunctioneerd.

Bewijsmiddel (op verzoek):
Een kopie van een geldig SOC 2 rapport of een beschrijving van een gelijkwaardig rapport.

Gegadigde moet aan haar verzoek tot deelneming toevoegen: een geldig SOC 2 Type II-rapport of een gelijkwaardig onafhankelijk assurance- of auditrapport (zoals het in bezit zijn van de combinatie van ISO 9001+27001+22301), inclusief de verklaring van de controlerend accountant of auditor.

Ingeval er in samenwerkingsverband (combinatie) wordt ingeschreven, moet iedere deelnemer aan dit samenwerkingsverband afzonderlijk aan de vereisten ten aanzien van de beheersing van de dienstverlening voldoen.

4.3.6 Applicatie integratie – Microsoft

Inschrijver beschikt over een aanzienlijk footprint voor Microsoft en maakt reeds gebruik van de beveiligingsproducten van Microsoft. De Inschrijver dient bij zijn Inschrijving te beschikken over het lidmaatschap van de Microsoft Intelligent Security Association (MISA).

Bewijsmiddel (op verzoek):
Gegadigde voegt een document toe waaruit blijkt dat hij lid is van de Microsoft Intelligent Security Association (MISA), bijvoorbeeld:

- een officiële bevestiging of verklaring van Microsoft;
- een vermelding in de officiële Microsoft MISA Partner Catalog; of
- een ander door Microsoft afgegeven of geverifieerd bewijsmiddel waaruit het MISA-lidmaatschap blijkt.

4.3.7 Technische bekwaamheid – Referentie

VNOG heeft de volgende kerncompetenties vastgesteld die overeenkomen met ervaring op essentiële punten van de Opdracht:

- Kerncompetentie 1: 24/7 SIEM, SOC, SOAR-dienstverlening voor een vitale of BIO-plichtige organisatie
- Kerncompetentie 2: Incidentrespons, handelingsperspectief en risicogestuurde opvolging van cyberincidenten
- Kerncompetentie 3: CERT-dienstverlening.

4.3.7.1 Kerncompetentie 1 – 24/7 SIEM-, SOC- en SOAR-dienstverlening voor een vitale of BIO-plichtige organisatie

Gegadigde heeft aantoonbare ervaring met het implementeren, inrichten, beheren en uitvoeren van geïntegreerde SIEM-, SOC- en SOAR-dienstverlening bij een organisatie van vitaal belang, een organisatie met een bedrijfskritische taak of een organisatie die zich conformeert aan de Baseline Informatiebeveiliging Overheid (BIO).

Uit de referentie blijkt ten minste dat Gegadigde verantwoordelijk is geweest voor:

- Het implementeren en/of operationeel maken van de SIEM-, SOC- en SOAR-dienstverlening;
- het leveren van een permanent bemande 24/7 Security Operations Center (SOC), gevestigd binnen de Europese Economische Ruimte (EER);
- het uitvoeren van 24/7 Eyes-on-Glass-monitoring, zoals gedefinieerd in de begrippenlijst;
- het borgen van de continuïteit van de dienstverlening, waaronder de beschikbaarheid van voldoende gekwalificeerde SOC-capaciteit, ook tijdens piekbelasting, uitval of verhoogde dreigingsniveaus;
- het verwerken, correleren en analyseren van relevante databronnen, waaronder endpoint-, netwerk-, cloud-, identity- en/of OT-bronnen, binnen de SIEM-omgeving van de opdrachtgever;
- het signaleren, analyseren en opvolgen van securitymeldingen en beveiligingsincidenten conform vooraf overeengekomen responstijden en escalatieprocedures;

4.3.7.2 Kerncompetentie 2 – Incidentrespons, handelingsperspectief en risicogestuurde opvolging van cyberincidenten

Gegadigde heeft aantoonbare ervaring met het reageren op, beperken van en ondersteunen bij het herstellen van ernstige cyberincidenten, bij een organisatie van vitaal belang, een organisatie met een bedrijfskritische taak of een organisatie die zich conformeert aan de Baseline Informatiebeveiliging Overheid (BIO).

Uit de referentie blijkt ten minste dat Gegadigde verantwoordelijk is geweest voor:

- het bieden van opvolging van ernstige cyberincidenten en/of securitymeldingen: het ondersteunen van de opdrachtgever tijdens de incidentrespons, crisiscoördinatie en besluitvorming;
- het uitvoeren van triage, analyse, classificatie, prioritering en escalatie van securitymeldingen en cyberincidenten;
- het adviseren over en ondersteunen bij containment-, mitigatie- en herstelmaatregelen, gericht op het beperken van de impact van het incident;
- het rapporteren over de aard, oorzaak, impact en afhandeling van het incident, inclusief aanbevelingen ter voorkoming van vergelijkbare incidenten;
- het ontwikkelen, tunen of verbeteren van detectieregels, use cases, playbooks en/of overige detectie- en responsmaatregelen naar aanleiding van het incident of actuele dreigingsinformatie.

4.3.7.3 Kerncompetentie 3 – CERT-dienstverlening

Gegadigde beschikt over en heeft aantoonbare ervaring met een gespecialiseerd Security Emergency Response Team (CERT of CSIRT), zoals gedefinieerd in de begrippenlijst, dat ten allen tijden beschikbaar is en kan ondersteunen bij ernstige cyberincidenten.

Uit de referentie blijkt ten minste dat Gegadigde verantwoordelijk is geweest voor:

- het beschikbaar stellen en operationeel inzetten van een CERT gedurende vierentwintig (24) uur per dag, zeven (7) dagen per week en driehonderdvijfenzestig (365) dagen per jaar: het beschikbaar hebben van gekwalificeerde cybersecurityspecialisten en daarmee ondersteunen van opdrachtgever voor de analyse, beheersing en afhandeling van ernstige cybersecurityincidenten;
- het uitvoeren van technische incidentanalyse en digitale forensische onderzoeken ter vaststelling van de aard, oorzaak en impact van cyberincidenten;
- het uitvoeren van containment-, eradication- en herstelwerkzaamheden, gericht op het beperken van de impact van het incident en het herstellen van de continuïteit van de dienstverlening;
- het analyseren van malware, Indicators of Compromise (IoC's) en overige technische indicatoren ter ondersteuning van de incidentafhandeling;
- het ondersteunen van de opdrachtgever bij technisch incidentmanagement, crisiscoördinatie en besluitvorming tijdens ernstige cyberincidenten;
- het leveren van ondersteuning op locatie, indien de aard of ernst van het incident daartoe aanleiding gaf;
- het opstellen van een incidentrapportage met bevindingen, root cause analyse en aanbevelingen ter voorkoming van vergelijkbare incidenten;
- het aantoonbaar samenwerken met de aangeboden SIEM-, SOC- en SOAR-dienstverlening, waarbij bevindingen uit incidenten zijn vertaald naar verbeterde detectieregels, use cases, playbooks en overige detectie- en responsmaatregelen.

Bewijsmiddel (Verzoek tot deelneming):
Ten einde aan te tonen te beschikken over de voornoemde kerncompetentie(s) levert Gegadigde per gevraagde kerncompetentie maximaal één referentie aan welke aan bovenvermelde eisen voldoet. Als in één referentie meerdere kerncompetenties tot uiting komen die voldoen aan de gestelde eisen, mag u voor die kerncompetenties dezelfde referentie gebruiken. Hiervoor gebruikt Gegadigde het Referentieformulier (Bijlage 2).

Gegadigde per hierboven vermelde kerncompetentie maximaal één referentie te hebben die voldoet aan de volgende eisen:

- de referentieopdracht moet in de drie (3) jaren voorafgaand aan de sluitingsdatum voor het verzoek tot deelname te zijn uitgevoerd of nog in uitvoering te zijn.

- Als de betreffende opdracht nog in uitvoering moet er tenminste één volledig jaar uitvoering gegeven zijn aan de Opdracht, gerekend vanaf het moment van aanvang van de werkzaamheden;
- de voor deze referentie uitgevoerde Opdracht valt onder de reikwijdte van de hierboven benoemde kerncompetenties; én
- de voor deze referentie uitgevoerde Opdracht is/wordt succesvol en naar tevredenheid van deze referent uitgevoerd;
- de opgegeven informatie is specifiek genoeg zodat uit de referentie eenduidig het volledige van de gevraagde kerncompetentie te herleiden moet zijn.
- Gegadigde toont de referentie aan door het volledig invullen en rechtsgeldig ondertekenen van Bijlage 2 – Referentieformulier

VNOG behoudt zich het recht voor zo nodig referenties op juistheid en volledigheid te controleren en zonder tussenkomst en/of toestemming van Gegadigde contact op te nemen met een of meer referenties.

5 Selectiecriteria

De verzoeken tot deelneming waarvoor geen uitsluitingsgronden van toepassing zijn en die voldoen aan de gestelde geschiktheidseisen, worden beoordeeld aan de hand van de selectiecriteria.

De behaalde scores op de selectiecriteria worden per gegadigde opgeteld. De totale score bepaalt de eindrangschikking. De vijf (5) hoogst scorende gegadigden worden geselecteerd voor deelname aan de Gunningsfase van deze aanbesteding.

Als minder dan vijf gegadigden voldoen aan de gestelde voorwaarden, worden slechts de gekwalificeerde gegadigden geselecteerd. Als bij de vaststelling van de rangorde meerdere gegadigden een gelijke score behalen waardoor het maximumaantal geselecteerden wordt overschreden, zal de Aanbestedende dienst tussen deze gegadigden **loten**.

5.1 Selectiecriteria en puntentoekenning

De onderstaande tabel toont de selectiecriteria en het maximaal te behalen puntenaantal per criterium.

Criterium	Maximaal te behalen punten
S1 Organisatorische opzet van uw SOC	60 punten
S2 Technische volwassenheid en Vendor expertise	40 punten
Totaal	**100**

5.2 Toelichting op de criteria

S1: Organisatorische opzet van uw SOC
Inschrijver beschrijft de organisatorische opzet van het aangeboden Security Operations Center (SOC) en toont aan op welke wijze de continuïteit, kwaliteit en volwassenheid van de dienstverlening zijn geborgd. De beschrijving dient aanvullend te zijn op de informatie die is verstrekt bij kerncompetentie 1.

De beschrijving dient minimaal de onderstaande onderwerpen te bevatten en omvat maximaal 5 pagina's A4 (een voorblad mag als extra A4-pagina worden toegevoegd), lettertype Aptos en lettergrootte 11. De gevraagde separate (ondersteunende)bijlagen/certificering wordt hierin niet inbegrepen. Het gebruiken van hyperlinks in de tekst is niet toegestaan.

Er kunnen voor dit criterium maximaal 60 punten worden behaald. De punten worden toegekend op onderstaande aspecten, waarbij er meer punten worden behaald naarmate er beter op gescoord wordt het aspect. De aspecten betreffen:

- Volwassenheid SOC-organisatie:

  - mate waarin 24/7 Eyes-on-Glass (conform de begrippenlijst) organisatorisch is ingericht, waarbij Inschrijver inzicht geeft in de personele inrichting van de 24/7-dienstverlening, waaronder ten minste de bezetting per dienst (L1/L2/L3), de fysieke aanwezigheid van securityanalisten gedurende de verschillende diensten, de wijze waarop continuïteit tijdens ploegwisselingen is geborgd, de inrichting van de overdracht tussen diensten (hand-over) en de beschikbaarheid van specialistische expertise buiten reguliere kantooruren.
  - een hogere score wordt bepaald door bijvoorbeeld CSA op L3 niveau, CompTIA Security+ (i.p.v. EC-Council), mate van CREST-accreditatie, de beschikbare operationele capaciteit, de mate waarin gedurende iedere dienst permanent gekwalificeerde securityanalisten fysiek aanwezig zijn, en/of een gestructureerde face-to-face hand-over tussen opvolgende diensten.
  - bewijslast: bijvoorbeeld een uittreksel van de actuele operationele procedures (SOP's), een geanonimiseerd organogram van de SOC-bezetting, een beschrijving van de personele bezetting per dienst (shiftmodel), inclusief de verdeling van L1-, L2- en L3-capaciteit gedurende een 24/7-cyclus, alsmede een overzicht van certificeringen.
- Case handling
  - mate waarin doorlooptijden, afhandeling door L1/L2/L3 en de afhandelingssnelheid wordt toegepast.
  - een hogere score wordt bepaald door bijvoorbeeld de mate waarin incidenten efficiënt worden afgehandeld door een duidelijk ingerichte L1-, L2- en L3-organisatie, met korte responstijden, duidelijke escalatieprocedures, eigenaarschap gedurende de volledige incidentafhandeling en aantoonbare sturing op KPI's en SLA's.
  - bewijslast: een beschrijving van het case handling-proces, inclusief de L1-, L2- en L3-inrichting, escalatiematrix, procesflow, KPI's/SLA's en eventueel voorbeeldrapportages over responstijden en afhandeling.
- Bedrijfscontinuïteit:
  - mate waarin de continuïteit van de dienstverlening is geborgd;
  - een hogere score wordt bepaald door bijvoorbeeld mate van continuïteit bij uitval van energie en/of netwerk, piekbelasting of verhoogde dreiging, de mate waarin de benodigde operationele capaciteit structureel binnen de eigen organisatie is geborgd (geen white label SOC = uitbesteding aan een partner), SOC gevestigd in de EER en mate van redundantie van personeel en SOC locatie (de mate waarin de dienstverlening onafhankelijk kan worden voortgezet bij uitval van een locatie of kritieke infrastructuur);
  - bewijslast: bijvoorbeeld architectuurdocument of Business Continuity Plan (BCP) waarin de redundante inrichting is beschreven, een beschrijving van de organisatorische continuïteitsmaatregelen of een verklaring waaruit blijkt dat het SOC binnen de EER is gevestigd.
- Certificeringen & Compliance:
  - uitvoering van de dienstverlening onder strikte compliance eisen aanvullend op de als geschiktheidseis gestelde SOC 2 Type II-verklaring (of gelijkwaardig);

- een hogere score wordt bepaald door bijvoorbeeld een beschrijving van een eigen additioneel bedrijfsproces.
- bewijslast: geschikte certificaten.

Bewijsmiddel (Verzoek tot deelneming):
Gegadigde dient een beschrijving aan haar verzoek tot deelneming toe te voegen. In de te overleggen bewijsmiddelen dienen de vermelde aspecten duidelijk herkenbaar te zijn.

Bovenstaande aspecten staan niet op volgorde van belangrijkheid en worden altijd in samenhang beoordeeld.

S2: Technisch volwassenheid en Vendor expertise
Gegadigde beschikt over aantoonbare technische volwassenheid en vendor expertise, additioneel aan kerncompetentie 2.

De beschrijving dient minimaal de onderstaande onderwerpen te bevatten en omvat maximaal 5 pagina's A4 (een voorblad mag als extra A4-pagina worden toegevoegd), lettertype Aptos en lettergrootte 11. De gevraagde separate (ondersteunende)bijlagen/certificering/partnerstatus wordt hierin niet inbegrepen. Het gebruiken van hyperlinks in de tekst is niet toegestaan.

Er kunnen voor dit criterium maximaal 40 punten worden behaald. De punten worden toegekend op onderstaande aspecten, waarbij er meer punten worden behaald naarmate er beter op gescoord wordt het aspect. De aspecten betreffen:

- Inzet van AI- en ML-modellen
  - mate waarin explainability, menselijke controle en bias-mitigatie geborgd zijn bij de inzet van AI- en ML-modellen binnen detectie, triage en responsprocessen.
  - een hogere score wordt bepaald door bijvoorbeeld de mate waarin AI- en ML-modellen aantoonbaar bijdragen aan de kwaliteit en snelheid van de detectie- en responsprocessen, waarbij de besluitvorming inzichtelijk, controleerbaar en herleidbaar is en menselijke validatie onderdeel uitmaakt van het proces
  - bewijslast: een beschrijving van de toegepaste AI- en ML-functionaliteiten, ondersteund met procesbeschrijvingen, architectuurdiagrammen, screenshots of andere documentatie waaruit de toepassing en borging blijkt.
- Threat hunting
  - mate waarin actieve threat hunting wordt toegepast;
  - een hogere score wordt bepaald door bijvoorbeeld een dedicated Threat Intelligence Team (naast de security-analisten die actief zijn met het monitoren, beoordelen, classificeren, verrijken en escaleren van security-events en incidenten) dat eigen use-cases ontwikkelt en onderhoudt.

  - bewijslast: een beschrijving van de inrichting van de threat hunting-capaciteit, de organisatie van het Threat Intelligence Team en voorbeelden van periodieke threat hunting-activiteiten, use-cases of rapportages.
- Partnerstatus
  - een aantoonbare hoge(re) status bij vendors zoals Microsoft (additioneel aan Partner status conform paragraaf 4.3.6) en relevante status bij andere A-merken;
  - een hogere score wordt bepaald door bijvoorbeeld het beschikken over meerdere geavanceerde partnerstatussen, specialisaties of fabrikantserkenningen bij de voor deze opdracht relevante technologieën, zoals Microsoft, Cisco, Dell, HPE-Aruba, Palo Alto Networks of vergelijkbare A-merken.
  - bewijslast: geldige partnercertificaten, fabrikantserkenningen, accreditaties of officiële verklaringen van de betreffende fabrikant waaruit de partnerstatus of specialisatie blijkt.
- Exposure monitoring
  - mate waarin Continuous Threat Exposure Management (CTEM) conform begrippenlijst wordt uitgevoerd;
  - een hogere score wordt bepaald door bijvoorbeeld de mate waarin continu extern aanvalsoppervlakbeheer (External Attack Surface Management), kwetsbaarheidsscans, monitoring van internet-exposed assets, domeinen, certificaten, cloudomgevingen en identiteiten structureel onderdeel uitmaken van de dienstverlening en proactief leiden tot handelingsperspectief voor de opdrachtgever. Daarbij wordt tevens beoordeeld in welke mate de Inschrijver een risicogestuurde CTEM-aanpak toepast, waarbij blootstellingen continu worden geïdentificeerd, geprioriteerd, gevalideerd en opgevolgd.
  - bewijslast: een beschrijving van de CTEM-/exposure monitoring-aanpak, ondersteund met voorbeeldrapportages, dashboards, screenshots of procesbeschrijvingen waaruit de werkwijze blijkt.

Bewijsmiddel (Verzoek tot deelneming):
Gegadigde dient een beschrijving aan haar verzoek tot deelneming toe te voegen. In de te overleggen bewijsmiddelen dienen de vermelde aspecten duidelijk herkenbaar te zijn.

Bovenstaande aspecten staan niet op volgorde van belangrijkheid en worden altijd in samenhang beoordeeld.

5.3 Beoordeling selectiecriteria

Ieder lid van de selectiecommissie voert eerst een individuele beoordeling uit. Per criterium wordt een waardering toegekend op een schaal van 1 tot 5. Vervolgens wordt in een consensusoverleg de beoordeling besproken en vastgesteld.
De individuele scores kunnen naar aanleiding van dit overleg worden aangepast. De definitieve score wordt vastgesteld op basis van consensus van de commissieleden.

Op grond van de eindscore worden de gegadigden gerangschikt. De vijf hoogst scorende gegadigden worden uitgenodigd voor de gunningsfase.

De selectiecommissie bestaat uit leden met de volgende functies:

- Chief Information Security Officer (CISO)
- Senior ICT Specialist & Security Officer (SO)
- 2 (Senior) ICT Specialisten

De commissie wordt voorgezeten door de inkoopadviseur die geen stemrecht heeft in de beoordeling.

5.3.1 Beoordelingskader

De onderstaande tabel geeft de beoordelingsschaal weer die wordt gehanteerd bij de waardering van de selectiecriteria.

Kwaliteit van de uitwerking	Score	Aantal punten %	Score S1 / S2
Uitmuntend; de Aanmelding is compleet en biedt veel toegevoegde waarde op de beoordelingscriteria.	*10*	*100%*	*S1 = 60 punten* *S2 = 40 punten*
Goed; de Aanmelding is compleet en biedt veel toegevoegde waarde op een of twee van de drie beoordelingscriteria en toegevoegde waarde op de andere beoordelingscriterium(s).	*7*	*70%*	*S1 = 42 punten* *S2 = 28 punten*
Voldoende; de Aanmelding is compleet en biedt toegevoegde waarde op de beoordelingscritertia.	*5*	*50%*	*S1 = 30 punten* *S2 = 20 punten*
Onvoldoende; de Aanmelding is niet compleet, voldoet niet aan de gestelde eisen of biedt onvoldoende aanknopingspunten voor beoordeling op de beoordelingscriteria.	*n.v.t*	*Geen* *(uitsluiting verdere deelname.)*	

Bij de beoordeling wordt tevens gelet op de volgende aspecten:

- Relevantie van de beantwoording ten opzichte van de gevraagde onderwerpen;
- Volledigheid van de beantwoording;
- Concretisering van de inhoud;
- Passendheid van de beantwoording bij de aard en omvang van de opdracht;
- Realistische en haalbare uitwerking.

Elke aanmelding wordt afzonderlijk beoordeeld op basis van haar eigen kenmerken. De selectiecommissie kan daarbij rekening houden met waarnemingen uit andere aanmeldingen, voor zover dit bijdraagt aan een evenwichtige en objectieve beoordeling.

6 Bijlagen

De volgende bijlagen maken integraal onderdeel uit van deze Selectieleidraad. Zij zijn separaat met de Selectieleidraad gepubliceerd.

BIJLAGE 1	Uniform Europees Aanbestedingsdocument
BIJLAGE 2	Referentieformulier
BIJLAGE 3	Verklaring Geen Russische Betrokkenheid
BIJLAGE 4	Verklaring Samenwerkingsverband
BIJLAGE 5	Verklaring Middelen Derden
BIJLAGE 6	Klachtenprocedure VNOG Inclusief Klachtenformulier
BIJLAGE 7	Marktconsultatieverslag SIEM, SOC, SOAR-dienstverlening

7 Checklist

In onderstaande tabel zijn alle documenten opgenomen, die door Inschrijver, op straffe van uitsluiting van de aanbestedingsprocedure, bij Inschrijving moeten worden ingediend:

Bij Verzoek tot Deelneming indienen:	
1	Uniform Europees Aanbestedingsdocument UEA (Bijlage 1)
2	Referentieformulier kerncompetenties (Bijlage 2)
3	Uitwerking Selectiecriterium S1
4	Uitwerking Selectiecriterium S2
5.	Verklaring Geen Russische Betrokkenheid (Bijlage 3)
6.	Uittreksel beroeps- of Handelsregister (KvK) (niet ouder dan 6 maanden)
7.	Verklaring Samenwerkingsverband (indien van toepassing, (Bijlage 4)
8.	Verklaring Middelen Derden (indien van toepassing) (Bijlage 5)
9.	Bewijsmiddel waaruit blijkt dat Gegadigde voldoet aan de eisen inzake Applicatie-integratie – Microsoft

In onderstaande tabel zijn de bewijsstukken opgenomen die door de Geselecteerde Gegadigden binnen zeven (7) kalenderdagen na een verzoek van VNOG moeten worden ingediend ten behoeve van de verificatie van de in het Uniform Europees Aanbeste-dingsdocument opgenomen verklaringen.

Na selectie en op verzoek indienen:	
1.	Gedragsverklaring Aanbesteden (GvA) (niet ouder dan 2 jaar) aan te vragen via; https://www.justis.nl/producten/gva/
2.	Verklaring Belastingdienst
3.	Bewijs van een beroeps- en bedrijfsaansprakelijkheidsverzekering
4.	Geldig ISO 9001-certificaat of gelijkwaardig bewijs
5.	Geldig ISO 27001-certificaat of gelijkwaardig bewijs
6.	Geldig SOC 2 Type II-rapport of een gelijkwaardig assurance- of auditrapport
7.	Goedkeurende accountantsverklaring of kopie van de samenstellingsverklaring

8.	Bewijs verzekering

Let op: Het aanvragen van een Gedragsverklaring Aanbesteden (GVA) kan twee (2) tot vier (4) weken duren. Aanbestedende dienst adviseert Gegadigde daarom de GVA tijdig aan te vragen. Indien de fysieke GVA ten tijde van de verificatie nog niet is ontvangen, volstaat gedurende de verificatietermijn de elektronische bevestiging van afgifte door Justis, mits hieruit de datum van afgifte blijkt. De fysieke GVA dient in dat geval onverwijld na ontvangst aan Aanbestedende dienst te worden verstrekt. Het niet tijdig overleggen van de gevraagde bewijsstukken kan leiden tot uitsluiting van de aanbestedingsprocedure.