

Aanbestedingsdocument

Europese aanbesteding, openbare procedure

Dienstverlening SIEM-SOC voor Veiligheidsregio Haaglanden



Versie : Definitief
Datum : 29 juli 2026

Inhoudsopgave

HOOFDSTUK 1	DEZE AANBESTEDING	3
1.1	Inleiding	3
1.2	Veiligheidsregio Haaglanden	3
1.3	Afdeling ICT-beheer van de VRH	4
1.4	Huidige situatie ICT- en security-omgeving van de VRH	5
1.5	Doelstelling en uitgangspunten van de opdracht	8
1.6	In scope	10
1.7	Niet in scope	10
1.8	Optioneel	10
1.9	Omvang van de opdracht	10
1.10	Aard van de opdracht	11
1.11	Overeenkomst	11
HOOFDSTUK 2	PROCEDURE	12
2.1	Keuze aanbestedingsprocedure	12
2.2	Digitaal aanbesteden via TenderNed	12
2.3	Contact tijdens de aanbestedingsprocedure	12
2.4	Wijze van inschrijving	12
2.5	Planning	12
2.6	Nota van inlichtingen	13
2.7	Verificatiebezoek	13
2.8	Bezwaar maken	13
HOOFDSTUK 3	UITSLUITINGSGRONDEN EN GESCHIKTHEIDSEISEN	14
3.1	Uniform Europees Aanbestedingsdocument (UEA)	14
3.2	Uitsluitingsgronden	14
3.3	Economische en financiële draagkracht	15
3.4	Technische en beroepsbekwaamheid	15
3.5	Samenvattend	17
HOOFDSTUK 4	BEOORDELING VAN DE INSCHRIJVINGEN	18
4.1	Gunningscriteria	18
4.2	Beoordelingsprocedure Kwaliteit	18
4.3	Beoordelingsmethodiek Kwaliteit	18
HOOFDSTUK 5	VRAAGSTELLING EN GUNNINGSCRITEIA	20
5.1	Kwaliteitscriterium 1: SIEM	20
5.2	Kwaliteitscriterium 2: SOC	22
5.3	Kwaliteitscriterium 3: Advisering	24
5.4	Kwaliteitscriterium 4: Implementatieplan	25
5.5	Prijs implementatie en maandelijks dienstverlening SIEM-SOC	26
	Bijlage 1 – Uniform Europees Aanbestedingsformulier	27
	Bijlage 2 - Concept overeenkomst dienstverlening SIEM-SOC	27
	Bijlage 3 - Concept verwerkersovereenkomst	27
	Bijlage 4 - Inkoopvoorwaarden VNG GIBIT 2025	27
	Bijlage 5 – Verklaring akkoord vaste prijzen dienstverlening SIEM-SOC	27

Hoofdstuk 1 Deze aanbesteding

1.1 Inleiding

Voor u ligt het aanbestedingsdocument van de Europese openbare aanbesteding voor het sluiten van een overeenkomst met één leverancier voor het leveren van dienstverlening SIEM-SOC voor Veiligheidsregio Haaglanden (afgekort VRH).

Deze aanbesteding richt zich op professionele marktpartijen met aantoonbare expertise in SIEM-SOC-dienstverlening en de toepassing daarvan binnen organisaties met bedrijfskritische processen. Van inschrijvers wordt verwacht dat zij ervaring hebben met het inrichten en uitvoeren van security monitoring en incidentrespons in lijn met de Baseline Informatiebeveiliging Overheid (afgekort BIO2), de ISO 27001/2 en de NIS2-richtlijn, waaronder risico gebaseerde beveiliging, continue monitoring, detectie en opvolging van beveiligingsincidenten.

Hoewel de markt voor dienstverlening SIEM-SOC- in algemene zin breed en ontwikkeld is, geldt dat voor de specifieke combinatie van gevraagde technologie, integratie met de Microsoft security stack en de relevante compliance-eisen (BIO2, ISO 27001/2 en NIS2) sprake is van een selecte groep geschikte aanbieders. Mede hierom worden zaken als geldende wet- en regelgeving, normering en toepassing/gebruik algemeen bekend verwacht. De VRH acht de markt desondanks voldoende concurrerend om op transparante en objectieve wijze tot gunning over te gaan.

De aankondiging van deze opdracht is gepubliceerd op www.TenderNed.nl.

In dit aanbestedingsdocument en bijbehorende bijlagen worden de opdracht, de aanbestedingsprocedure, de eisen aan inschrijvers en hun inschrijvingen en de wijze waarop de inschrijvingen worden beoordeeld toegelicht.

1.2 Veiligheidsregio Haaglanden

Veiligheidsregio Haaglanden is een dynamische organisatie met betekenisvol werk. Alles wat we doen richt zich op het vergroten van de veiligheid van de bevolking en bezoekers van de regio Haaglanden. Wij hebben daarmee één doel: een (brand)veilige regio Haaglanden. Met onze medewerkers regelen wij de dagelijkse brandweezorg, geneeskundige hulpverlening en organiseren wij de 112-meldkamer van de brandweer in de regio Haaglanden. In Nederland zijn er 25 veiligheidsregio's.

De regio Haaglanden bestaat uit negen gemeenten: Den Haag, Delft, Leidschendam-Voorburg, Midden-Delfland, Pijnacker-Nootdorp, Rijswijk, Wassenaar, Westland en Zoetermeer.

Het is een gevarieerde omgeving met stadskernen, grote woongebieden, natuurgebieden (bijvoorbeeld het strand en de duinen), intensief verkeer en openbaar vervoer, hoogbouw, kassengebied, landelijk gebied, kantoren, winkelgebieden, industrie en speciale gebruikers als universiteiten, het Binnenhof, Koninklijk huis, ministeries enzovoort.

De VRH heeft 1 meldkamer, 20 kazernes en 3 kazernes met kantoor.

Bij de VRH hebben bijna 1.500 personen een dienstverband, waarvan ruim 330 als vrijwilliger.

De VRH bestaat uit drie directies:

- brandweezorg;

- geneeskundige zorg;
- bedrijfsvoering.

CIO-Bureau

Vanuit de directie Bedrijfsvoering wordt de organisatie VRH op verschillende gebieden ondersteunt. In nauwe samenwerking met ICT Beheer (zie paragraaf 1.3 Afdeling ICT-beheer van de VRH) zorgt het CIO-Bureau voor de continuïteit, kwaliteit en ontwikkeling van de informatievoorziening. Daarbij staat het ondersteunen van de primaire processen van de VRH centraal. Het CIO-Bureau vervult hiermee een belangrijke regie-, advies- en controlefunctie binnen de organisatie. Vanuit deze rol ontwikkelt en bewaakt het CIO-Bureau beleid, kaders en richtlijnen die bijdragen aan een betrouwbare, veilige en toekomstbestendige informatievoorziening. De afdeling adviseert management en directie bij strategische en tactische vraagstukken op het gebied van digitalisering en informatiebeheer. Daarnaast ziet het CIO-Bureau toe op de naleving van vastgestelde kaders, wet- en regelgeving en interne afspraken.

Meer informatie over de organisatie kunt u vinden op onze website www.vrh.nl.

1.3 Afdeling ICT-beheer van de VRH

Binnen de directie Bedrijfsvoering is de afdeling ICT Beheer verantwoordelijk voor de kantoorautomatisering van de VRH. Op dit moment bestaat Team ICT Beheer uit 11 personen, met de volgende functies: teamleider, 2 Servicedesk medewerkers, 5 functioneel beheerders, ICT-adviseur, security beheerder en projectleider ICT. Team ICT Beheer is verantwoordelijk voor:

Regie Kantoorautomatisering/werkplek beheer

Aansturen van commerciële dienstverleners in multivendor constructie. Deze constructie is vanaf 1 januari 2026 operationeel en bevat de volgende onderdelen:

Beheer Cloud security center

Uitvoering door leverancier KPN, overeenkomst loopt tot 01-01-2027.

Op hoofdlijn zijn taken:

- security monitoring;
- 24/7 opvolging van mogelijke security incidenten vanuit het Cloud Security Center die gedetecteerd worden door de Microsoft E5 security tools.

Technisch ICT-beheer

Uitvoering door leverancier Proact, overeenkomst is gestart per 01-07-2026.

Op hoofdlijn zijn taken:

- technisch beheer Azure tenant en Microsoft 365 omgeving;
- technisch beheer werkplekken medewerkers VRH;
- security-beheer werkplekken;
- eindgebruikersdiensten;
- beheer Microsoft 365.

Connectiviteitsdiensten

Uitvoering door leverancier Proxsys, overeenkomst is gestart per 01-01-2026.

Op hoofdlijn zijn taken:

- leveren van verbindingen voor ontsluiting van de verschillende locaties voor toegang tot Azure;
- network as a Service voor zowel LAN als WLAN.

Servicedesk

Verzorgen van in-house servicedesk, maandag tot en met vrijdag van 8.00 tot 16.30 uur. Het on-site supportteam bestaat uit 2 servicedesk medewerkers en 1 functioneel beheerder met de rol van incident/probleem coördinator. Waarvan een medewerker de rol van incident/problem-coördinator heeft.

Hardware

Ondersteunen van gebruikers in ICT-behoefte, vervangen en vernieuwen van ICT-middelen. Voor aanschaf van hardware maakt de VRH gebruik van dienstverlening via een hardwarebroker.

Software

Beheren van overeenkomsten voor de levering van de softwarelicenties, onder andere Microsoft 365 F3, F5 en E5 licenties. Voor aanschaf van Microsoft-licenties maakt de VRH gebruik van dienstverlening via een softwarebroker.

1.4 Huidige situatie ICT- en security-omgeving van de VRH

Algemeen beeld security en monitoring

De VRH heeft haar informatiebeveiliging ingericht conform de Baseline Informatiebeveiliging Overheid (BIO) en bereidt zich voor op de implementatie van de BIO2-richtlijnen. Daarbij wordt gewerkt volgens een risico gebaseerde benadering waarbij maatregelen worden vastgesteld op basis van beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van informatie voor de VRH. De VRH heeft zich gecommitteerd aan volwassenheidsniveau 3 van de BIO2 norm per 2027 en niveau 4 in 2029.

De ingezette Microsoft-securitydiensten ondersteunen de invulling van diverse BIO- en BIO2-maatregelen op het gebied van:

- identiteits- en toegangsbeheer;
- logging en monitoring;
- detectie van beveiligingsincidenten;
- kwetsbaarhedenbeheer;
- bescherming van eindgebruikersapparatuur;
- bescherming van data en informatieobjecten;
- continuïteits- en herstelmaatregelen.

Security monitoring, incidentdetectie en opvolging dragen bij aan het aantoonbaar beheersen van cyberrisico's en ondersteunen de VRH bij het voldoen aan de eisen vanuit BIO2, ISO 27001/2, AVG en (toekomstige) NIS2-verplichtingen.

De VRH beschikt over een grotendeels Microsoft-georiënteerde ICT-omgeving. Security monitoring 24/7, dreigingsdetectie en incidentmanagement zijn centraal ingericht binnen het Cloud Security Center voor Microsoft Cloud door de huidige leverancier (zie paragraaf 1.3 Afdeling ICT-beheer van de VRH, Regie Kantoorautomatisering/werkplek beheer) op basis van de beschikbare Microsoft E5 Security-functionaliteiten van de VRH.

Het signaleren en escaleren van security-incidenten, het analyseren van kwetsbaarheden en dreigingen en het classificeren van incidenten worden uitgevoerd door de huidige leverancier met behulp van verschillende Microsoft security stacks en E5 licenties. Opvolging wordt uitgevoerd of door de huidige leverancier of de VRH.

Enkele kenmerken van de huidige ICT- en securityomgeving van de VRH:

Microsoft Security E5-licenties en gekoppelde beveiligingsworkloads binnen het Cloud Security Center

- circa 1.300 gebruikers maken gebruik van de Microsoft Security E5-functionaliteiten waaronder Identity Protection, Endpoint Protection en Data & Apps Protection;
- circa 27 workloads binnen Platform Protection.

Inzet van Microsoft-securitydiensten

De VRH maakt intensief gebruik van de Microsoft Defender- en Purview-suite en breidt deze omgeving naar behoefte verder uit. De volgende componenten zijn (deels) operationeel:

- Microsoft Defender for Cloud Apps;
- Microsoft Defender for Endpoint;
- Microsoft Defender for Identity;
- Microsoft Defender for Servers;
- Microsoft Defender for Office 365;
- de verschillende Defender-componenten worden centraal gecorreleerd binnen Microsoft Defender XDR;
- Microsoft Purview (compliance, data governance);
- Microsoft Sentinel.

Microsoft Sentinel fungeert als centrale SIEM-oplossing en is volledig geïntegreerd met de Microsoft-tenant van de VRH. Microsoft Sentinel wordt verrijkt met dreigingsinformatie en detectieregels die periodiek worden geoptimaliseerd op basis van dreigingsontwikkelingen. Binnen Sentinel worden loggegevens verzameld en gecorreleerd afkomstig van onder andere:

- Microsoft 365;
- Microsoft Entra ID en Entra ID Protection;
- Microsoft Defender for Cloud Apps;
- Microsoft Defender for Endpoint;
- Microsoft Defender for Identity;
- Microsoft Defender for Office 365;
- Microsoft Defender XDR;
- Microsoft Purview (incl. Insider Risk Management).

De verzamelde logging wordt gebruikt voor het detecteren van dreigingen, afwijkingen en mogelijke security-incidenten. Analyse en opvolging worden uitgevoerd door de betreffende leverancier in multi-vendorconstructie.

Azure-omgeving en beheerstructuur

De Azure-omgeving vormt de primaire Cloud infrastructuur van VRH en is ingericht volgens gangbare best practices. Kenmerken van de inrichting:

- structurering op basis van resource groups;
- toepassing van RBAC (role-based access control);
- inzet van Privileged Identity Management (PIM);
- gebruik van tagging en beleidsregels (policy enforcement);
- volledige inrichting conform change management.

Actieve Azure-diensten omvatten onder meer:

- Azure Virtual Desktop;
- VPN Gateway;
- Azure Key Vault;
- Log Analytics Workspace;
- Microsoft Sentinel;
- Microsoft Defender for Cloud;
- Azure Storage Accounts;

- Azure Automation (runbooks en procesautomatisering).
- Daarnaast is Microsoft Entra Domain Services ingericht.

Devicebeheer en Zero Trust

De VRH hanteert een Zero Trust-beveiligingsmodel als uitgangspunt. Devicebeheer wordt uitgevoerd met Microsoft Intune:

- werkplekken (laptops en desktops) worden centraal beheerd;
- mobiele apparaten worden via Intune geconfigureerd en beheerd;
- distributie van applicaties en configuraties verloopt geautomatiseerd.

Toegepaste beveiligingsmaatregelen omvatten:

- Multi-Factor Authentication (MFA);
- Conditional Access policies;
- Compliant device checks;
- beperking van lokale administratorrechten.

Identiteitenbeheer en IAM

Voor identity- en accessmanagement maakt VRH gebruik van Microsoft Entra ID. Visma Youforce is het bronsysteem voor personeels- en contractgegevens. HelloID is operationeel ingericht als centrale provisioning- en service-automationlaag tussen Youforce, Entra ID en gekoppelde doelapplicaties. Via HelloID worden processen voor instroom, doorstroom en uitstroom geautomatiseerd. Dit omvat het aanmaken, wijzigen, blokkeren en beëindigen van accounts en het automatisch toekennen en intrekken van groepen, autorisaties, licenties en overige producten. Tijdelijke of aanvullende aanvragen en beheerhandelingen verlopen via gecontroleerde workflows met autorisatie, logging en, waar van toepassing, een einddatum.

Externe partijen maken gebruik van B2B-accounts. Verhoogde toegang tot kritische resources wordt volgens het least-privilegeprincipe toegekend via PIM en goedkeuringsprocessen.

Monitoring, logging en alerting

Monitoring en logging binnen de VRH wordt uitgevoerd via:

- Microsoft Sentinel;
- Azure Log Analytics;
- Azure Monitor;

Deze tooling wordt ingezet voor:

- security monitoring;
- infrastructuurmonitoring;
- Cloud resource monitoring;
- Netwerk- en werkplekmonitoring.

Daarnaast wordt gebruik gemaakt van:

- Threat intelligence voor het verrijken van detecties;
- Threat hunting voor het proactief identificeren van dreigingen;
- use case tuning voor het optimaliseren van detectieregels en het beperken van false positives.

Alerting wordt deels geautomatiseerd afgehandeld via de Microsoft tooling en deels door menselijke opvolging.

Back-up en herstel

De VRH hanteert een hybride back-upstrategie:

- VEEAM voor back-up van Microsoft 365 (Exchange, OneDrive, SharePoint, Teams);
- Azure-native back-updiensten voor Azure workloads (VMs, files).

Retentiebeleid en configuratie zijn afgestemd op wettelijke verplichtingen en compliance-eisen.

Compliance en gegevensbeheer (Purview)

Microsoft Purview wordt ingezet als centrale oplossing voor:

- compliancebeheer;
- archivering;
- data governance.

Onder andere de volgende onderdelen zijn (deels) ingericht:

- retention policies;
- data labeling;
- eDiscovery.

Deze inrichting wordt verder uitgebreid in lijn met wet- en regelgeving (onder andere archiefwetgeving).

Update-, lifecycle- en applicatiebeheer Updatebeleid

- Windows- en security-updates worden uitgerold via Intune;
- third-party updates worden centraal beheerd;
- Azure Automation (runbooks en procesautomatisering).

Lifecyclebeheer

De VRH hanteert beleid voor lifecyclemanagement van hardware, software en diensten.

Applicatiebeheer:

- werkplekapplicaties worden uitgerold via Intune;
- serverapplicaties worden beheerd via Azure Automation;
- applicaties worden centraal aangeboden via gecontroleerde kanalen (Company Portal/ MyApps);

Alleen gevalideerde versies worden beschikbaar gesteld.

1.5 Doelstelling en uitgangspunten van de opdracht

De VRH zoekt een leverancier voor de uitvoering van dienstverlening SIEM- en SOC, bestaande uit twee cruciale componenten van een effectieve cyberbeveiligings-strategie waarbij samenwerking met de VRH cruciaal is:

Security Information and Event Management (SIEM)

Door de combinatie van een professioneel ingericht Security Operations Center (SOC) en een moderne SIEM-oplossing wil de VRH haar digitale weerbaarheid structureel versterken en voorbereid zijn op toenemende cyberdreigingen, BIO2 en toekomstige wet- en regelgeving.

De aangeboden dienstverlening SIEM- en SOC dient de VRH te ondersteunen bij het versterken van haar digitale weerbaarheid en het voldoen aan relevante wet- en regelgeving, normenkaders en beveiligingsrichtlijnen. De VRH verwacht daarbij dat de hiervoor benodigde reguliere functionaliteiten, rapportages, advisering en ondersteuning integraal onderdeel uitmaken van de aangeboden dienstverlening. De VRH heeft Microsoft Sentinel aangewezen als strategische SIEM-oplossing. De opdrachtnemer sluit met zijn dienstverlening aan op de bestaande Microsoft-securityarchitectuur van de VRH en benut daarbij de aanwezige Microsoft Security E5-functionaliteiten.

Belangrijke uitgangspunten hierbij zijn:

- maximale benutting van de bestaande Microsoft-investeringen;
- native integratie met Microsoft Defender-, Microsoft Entra- en Microsoft Purview-componenten;
- centrale verzameling, correlatie en analyse van security-events;
- ondersteuning van SIEM- en SOAR-functionaliteiten;

- ondersteuning van threat intelligence, threat hunting en use case management;
- schaalbaarheid voor toekomstige uitbreiding van logbronnen en securitydiensten.

De opdrachtnemer levert zijn dienstverlening op basis van Microsoft Sentinel. De inzet van een alternatieve SIEM-oplossing acht de VRH niet doelmatig, vanwege de impact op integratie, beheer, licenties en bestaande investeringen. Een alternatieve SIEM-oplossing zou kunnen leiden tot:

- dubbele licentiekosten;
- extra integratie-inspanningen;
- verhoogde beheercomplexiteit;
- verminderde benutting van reeds gedane investeringen.

De opdrachtnemer levert de operationele SIEM- en SOC-dienstverlening en voert minimaal de volgende werkzaamheden uit:

- 24/7 monitoring van security-events en beveiligingsmeldingen;
- analyse, triage en classificatie van security-events, dreigingen en incidenten;
- correlatie en verrijking van security-data binnen Microsoft Sentinel;
- uitvoering van threat intelligence-activiteiten ter verrijking van detecties;
- uitvoering van proactieve threat hunting-activiteiten;
- beheer, optimalisatie en doorontwikkeling van detectieregels, analytics rules, use cases en automatiseringen;
- escalatie van incidenten conform overeengekomen procedures en serviceniveaus;
- rapportage over incidenten, dreigingen, trends, kwetsbaarheden en dienstverlening;
- ondersteuning bij incidentrespons binnen de overeengekomen scope;
- advisering over verbetermaatregelen ten aanzien van informatiebeveiliging, monitoring en detectie.

1.5.2 Security Operations Center (SOC)

Het SOC vormt de operationele uitvoeringsorganisatie voor monitoring, detectie, analyse van beveiligingsincidenten en first response (bijvoorbeeld isolatie van device en/of account). De opdrachtnemer draagt zorg voor het tijdig identificeren, analyseren, classificeren en escaleren van beveiligingsdreigingen, met als doel het beperken van risico's en het ondersteunen van de continuïteit van de dienstverlening van de VRH.

1.5.3 Samenwerking en doelstellingen van de overeenkomst

Momenteel neemt de VRH de dienstverlening SIEM- en SOC af van een externe dienstverlener. Deze overeenkomst eindigt op 31 december 2026. Met deze aanbesteding beoogt de VRH een overeenkomst aan te gaan met één opdrachtnemer voor de levering, continuering en verdere ontwikkeling van de dienstverlening SIEM- en SOC vanaf 1 januari 2027.

De overeenkomst is gericht op een duurzame samenwerking waarbij de opdrachtnemer niet uitsluitend een uitvoerende rol vervult, maar tevens optreedt als kennispartner en adviseur op het gebied van securitymonitoring, dreigingsdetectie en security operations.

Met het afsluiten van de overeenkomst wenst de VRH de volgende doelstellingen te realiseren:

- het structureel versterken van de digitale weerbaarheid en veerkracht van de VRH;
- het realiseren van een hoogwaardige en toekomstbestendige dienstverlening SIEM- en SOC;
- het verkrijgen van continu inzicht in de beveiligingsstatus van de ICT-omgeving en het tijdig signaleren van risico's, kwetsbaarheden en dreigingen;
- het realiseren van een samenhangende aanpak voor monitoring, detectie, analyse, incidentrespons en beveiligingsondersteuning;

- het optimaal benutten van de bestaande Microsoft-securityarchitectuur en beschikbare Microsoft Security E5-functionaliteiten;
- het ondersteunen van de VRH bij het voldoen aan de BIO2, ISO 27001/2, AVG, NIS2 en overige relevante wet- en regelgeving;
- het waarborgen van continuïteit, overdraagbaarheid en beheersbaarheid van de ingerichte dienstverlening.

Van de opdrachtnemer wordt verwacht dat deze actief bijdraagt aan de doorontwikkeling van de dienstverlening door middel van advies, rapportages, verbetervoorstellen en kennisdeling. Daarbij houdt de opdrachtnemer rekening met ontwikkelingen op het gebied van technologie, cyberdreigingen, wet- en regelgeving en relevante best practices.

De dienstverlening dient zodanig te worden ingericht en gedocumenteerd dat deze gedurende de looptijd van de overeenkomst beheersbaar blijft en bij afloop van de overeenkomst overdraagbaar is aan de VRH of een opvolgende leverancier. De VRH wenst niet in een situatie van vendor lock-in te geraken.

De contacten tussen opdrachtnemer en de VRH verlopen in beginsel via Team ICT Beheer van de VRH. De VRH blijft verantwoordelijk voor de regie, beleidsvorming, risicobeheersing en besluitvorming met betrekking tot de ICT- en informatiebeveiligingsomgeving. De opdrachtnemer vervult hierin een uitvoerende, signalerende en adviserende rol.

1.6 In scope

De volgende werkzaamheden vallen binnen de scope van onderhavige opdracht:

Dienstverlening SIEM-SOC

Aard van de diensten:

1. Continu monitoren, detecteren en analyseren van beveiligingsincidenten (SIEM);
2. Operationele uitvoering van Security Operations Center (SOC)-processen;
3. Advisering.

1.7 Niet in scope

Alle niet genoemde dienstverlening valt niet onder deze overeenkomst.

1.8 Optioneel

Als het voor het functioneren van de VRH ICT-dienstverlening nodig is om (tijdelijk) taken toe te voegen aan de opdracht voor dienstverlening SIEM-SOC, ziet de VRH deze als optioneel. Daarmee kunnen deze, in overleg en met afstemming met opdrachtnemer, worden toegevoegd als onderdeel van deze aanbesteding en de daaruit volgende overeenkomst. Eventuele (tijdelijke)aanvullingen, die tijdens de looptijd worden ingezet, worden als onderdeel van deze aanbesteding en de daaruit volgende overeenkomst gezien.

1.9 Omvang van de opdracht

De huidige dienstverlening Cloud security center eindigt rechtswege per 31 december 2026. De opdracht bestaat uit leveren van dienstverlening SIEM-SOC per 1 januari 2027, inclusief ondersteuning en optioneel toe te voegen functionaliteiten. De opdrachtwaarde volgt uit de aanbesteding. Gezien de hoogte van het ramingsbedrag is hiervoor een Europese aanbesteding nodig.

Samenvoegen van opdrachten en verdeling in percelen

Naar het oordeel van de VRH is bij deze opdracht geen sprake van het onnodig samenvoegen van opdrachten. De gevraagde dienstverlening is beschikbaar in de markt. Voor de VRH is een totaaloplossing op de gevraagde dienstverlening wenselijk en noodzakelijk in verband met het aflopen van de huidige overeenkomst.

1.10 Aard van de opdracht

De CPV-code die van toepassing is op deze opdracht:

72000000-5 – IT-diensten: advies, softwareontwikkeling, internet en ondersteuning

1.11 Overeenkomst

Voor deze opdracht wordt gebruik gemaakt van één overeenkomst, gebaseerd op de VNG standaard, te starten in 2026 voor de implementatie en met ingebruikname dienstverlening SIEM-SOC vanaf 1 januari 2027. De overeenkomst wordt aangegaan voor 4 jaar met vervolgens verlengingsopties van telkens 1 jaar. Hiermee is de overeenkomst voor onbepaalde tijd.

Met deze looptijd verwacht de VRH doelmatig gebruik te kunnen maken van de samenwerking en de functionaliteit zolang deze voldoen. Als de samenwerking of het systeem niet meer voldoet of als interne of externe ontwikkelingen dit nodig maken, zal dat het moment zijn dat de VRH de overeenkomst beëindigt. Ook voor de leverancier geeft dit de kans op een passend rendement en de prikkel het systeem te blijven ontwikkelen om blijvend aan de vraag te voldoen.

In Bijlage 2 is de (concept) overeenkomst Dienstverlening SIEM-SOC opgenomen die voor deze opdracht gebruikt zal worden, in combinatie met Inkoopvoorwaarden VNG GIBIT 2025 (Bijlage 4) en de verwerkersovereenkomst (Bijlage 3). Deze documenten zijn gebaseerd op de VNG-standaarden welke paritair tot stand zijn gekomen in overleg tussen de VNG, gemeenten en het bedrijfsleven. Mede hierom is er geen intentie om hier aanpassingen op te maken.

Voorstellen voor aangepaste teksten, minder relevante artikelen buiten werking verklaren en verschuiven van verantwoording of aansprakelijkheid zullen door de VRH niet gehonoreerd worden en bij voorkeur dient u deze niet in. Met uw inschrijving gaat u akkoord met deze overeenkomsten en voorwaarden.

Hoofdstuk 2 Procedure

2.1 Keuze aanbestedingsprocedure

Op deze aanbesteding is de Aanbestedingswet 2012 van toepassing. Deze Europese aanbesteding betreft een openbare procedure. Er is gekozen voor een openbare procedure vanwege de samenstelling van de markt en het niet beperkte aantal aanbieders in dit marktsegment. Gezien de professionele markt wordt algemene kennis van aanbestedingsprocedures verondersteld aanwezig te zijn. Door het indienen van een inschrijving stemt de inschrijver in met de voorwaarden van deze aanbesteding en de voorwaarden voor de dienstverlening die daaruit volgen.

De opdracht zal gegund worden op basis van de beste prijs-kwaliteitverhouding. De VRH behoudt zich het recht voor deze procedure aan te passen en eventueel niet of aangepast tot gunning en opdrachtverstrekking over te gaan. Op deze aanbestedingsprocedure is Nederlands recht van toepassing. Een eventueel geschil wordt beslecht door de bevoegde rechter in Den Haag.

Na de aanbesteding volgt het proces van opdrachtverstrekking, afstemming, inrichting, implementatie en ingebruikname.

2.2 Digitaal aanbesteden via TenderNed

De gehele aanbesteding verloopt digitaal via TenderNed. Dit betekent onder meer dat:

- a) Alle aanbestedingsstukken kosteloos en digitaal ter beschikking worden gesteld via TenderNed.
- b) Het stellen van vragen plaatsvindt via de berichtenfunctie van TenderNed (er wordt geen gebruik gemaakt van de vraag en antwoordfunctie) in overeenstemming met de in dit aanbestedingsdocument opgenomen planning en voorschriften.
- c) Inschrijvingen digitaal dienen te worden ingediend volgens de in dit aanbestedingsdocument opgenomen planning en voorschriften.
- d) Ook alle verdere correspondentie vindt plaats via de berichtenmodule van TenderNed.

2.3 Contact tijdens de aanbestedingsprocedure

Alle correspondentie vindt in beginsel dus plaats via TenderNed. Mocht dit om technische redenen niet mogelijk of contact anderszins daadwerkelijk noodzakelijk zijn, dan kunt u per mail contact opnemen via inkoop@vrh.nl. Het opnemen van contact met betrekking tot deze aanbesteding via andere wegen of met andere medewerkers van de VRH of dienstverleners aan de VRH is niet gewenst en kan leiden tot uitsluiting.

2.4 Wijze van inschrijving

Een natuurlijk persoon, rechtspersoon en/of vennootschap mag slechts eenmaal (hetzij individueel of hetzij in combinatie of als onderaannemer) aanbieden. Inschrijvingen worden bij zo veel mogelijk als PDF ingediend, bij voorkeur als één document. Alleen ingediende documenten worden beoordeeld, links of verwijzingen worden niet beoordeeld.

Zowel tijdens deze aanbestedingsprocedure als de dienstverlening erna, verwacht de VRH te kunnen communiceren in het Nederlands.

2.5 Planning

Binnen een aanbestedingsprocedure dienen geïnteresseerden op verschillende momenten tijdig acties te nemen. In de planning zijn deze vetgedrukt. De VRH streeft ernaar de hiernavolgende planning te realiseren. Zonder expliciet tegenbericht, in de vorm van een nota van inlichtingen, dienen geïnteresseerden hiervan uit te gaan.

Activiteit	Datum & Tijd
Publiceren aankondiging op TenderNed	29 juli 2026
Uiterste datum voor het stellen van vragen, 1 ^e ronde	Maandag 17 augustus 2026 voor 10:00 uur
Publicatie nota van inlichtingen, 1 ^e ronde	Uiterlijk 28 augustus 2026
Uiterste datum voor het stellen van vragen, 2 ^e ronde	Vrijdag 4 september 2026 voor 10:00 uur
Publicatie nota van inlichtingen, 2 ^e ronde	Uiterlijk 15 september 2026
Sluiting termijn voor het indienen van een aanbidding	Maandag 28 september 2026 12:00 uur
Versturen mededeling gunningsbeslissing en start opschortende termijn/ bezwaartermijn	Begin oktober 2026
Verificatiebezoek leverancier	Oktober 2026
Einde opschortende termijn/ bezwaartermijn	20 dagen na bericht
Opdrachtverstrekking/ ondertekening	Oktober 2026
Afstemming, inrichting en implementatie	Vanaf ondertekening
Ingebruikname	1 januari 2027

2.6 Nota van inlichtingen

Over deze uitnodiging tot inschrijving kunt u vragen stellen. Dit doet u online via TenderNed. U kunt dit doen tot de in paragraaf 2.5 Planning vermelde datum. De taal voor het stellen van de vragen is Nederlands.

2.7 Verificatiebezoek

Tijdens periode voorlopige gunning brengt de VRH, leden van team ICT Beheer, bezoek aan leverancier op de locatie waar de dienstverlening ingevuld moet worden. Dit bezoek is ter verificatie van de gegeven antwoorden met de situatie ter plaatse. Bij negatieve verificatie kan de VRH het gunningsbesluit herzien.

2.8 Bezwaar maken

Na voorlopige gunning start de reguliere opschortende termijn/ bezwaartermijn van 20 kalenderdagen. Mocht een leverancier tijdens het aanbestedingstraject een reden voor bezwaar hebben tegen het proces of gemaakte keuzes dan dient deze leverancier dit bezwaar direct kenbaar te maken per mail op inkoop@vrh.nl. De VRH zal per mail zo snel mogelijk reactie geven op het bezwaar. In principe loopt het traject door. Als een leverancier, na beantwoording, van mening is dat zijn bezwaar een reden is waarom de procedure geen voortgang kan hebben, dan dient deze leverancier dit bezwaar via een kort geding voor te leggen voor toetsing bij de kantonrechter. Zonder kort geding blijft de procedure doorlopen. Een bezwaar in de opschortende termijn/ bezwaartermijn kan daarmee alleen betrekking hebben op de inhoudelijke beoordeling, niet op het aanbestedingsproces of daarin gemaakte keuzes.

Hoofdstuk 3 Uitsluitingsgronden en geschiktheidseisen

In dit hoofdstuk worden de eisen aan de inschrijvers omschreven. De criteria vallen uiteen in uitsluitingscriteria en minimumeisen. De uitsluitingscriteria en geschiktheidseisen zijn als onderdeel van het Uniform Europees Aanbestedingsdocument (UEA) opgenomen. Bij de eisen staat telkens aangegeven welke bewijsvoering aangeleverd moet worden en wanneer.

Deze fase heeft bij deze aanbesteding tot doel de inschrijver te controleren op uitsluitingsgronden (bijv.: faillissement, valse verklaringen, afdracht sociale lasten en belastingen) en de geschiktheid van de inschrijver vast te stellen voor de uitvoering van de opdracht. Om de geschiktheid te kunnen bepalen is een aantal criteria vastgesteld die bestaan uit eisen aan de beroepsbekwaamheid (bijv.: inschrijving handelsregister) en eisen op het terrein van financiële draagkracht.

Een inschrijving waarop een Uitsluitingsgrond van toepassing is wordt terzijde gelegd en komt niet in aanmerking voor selectie.

Alle Geschiktheidseisen betreffen minimumeisen. Dit betekent dat voor iedere eis afzonderlijk een op onderhavige opdracht afgestemd minimum is vastgesteld waaraan de inschrijver moet voldoen. Een inschrijving die niet voldoet aan deze eisen wordt terzijde gelegd en komt niet in aanmerking voor selectie.

Wij wijzen er met nadruk op dat de VRH zich het recht voorbehoudt onvolledige inschrijvingen en inschrijvingen waarin niet alle vragen zijn beantwoord, niet verder in behandeling te nemen.

3.1 Uniform Europees Aanbestedingsdocument (UEA)

Minimumeis

Een volledig rechtsgeldig ingevulde UEA welke is opgenomen als separaat pdf-formulier als onderdeel van Bijlage 1 Uniform Europees Aanbestedingsdocument.

Als een rechtsgeldig ondertekende UEA in de inschrijving ontbreekt, wordt de inschrijver uitgesloten van deelname.

Inschrijven als samenwerkingsverband

Alle leden van het samenwerkingsverband moeten de UEA overleggen.

N.B. Het gaat hier om een samenwerkingsverband en niet om de situatie waarin een beroep wordt gedaan op een derde als onderaannemer. Derden waarop door de onderneming een beroep wordt gedaan, hoeven de UEA niet in te vullen.

3.2 Uitsluitingsgronden

Alle verplichte en facultatieve wettelijke uitsluitingsgronden voor aanbestedingen boven de Europese drempels zijn op deze aanbesteding van toepassing. De VRH kiest hiervoor omdat zij geen zaken wil doen met een ondernemer op wie één van deze omstandigheden van toepassing is. De van toepassing zijnde uitsluitingsgronden zijn aangevinkt onder deel III van het **Uniform Europees Aanbestedingsdocument**.

Voor wat betreft de bewijsvoering is het uitgangspunt dat inschrijvers bij hun inschrijving kunnen volstaan met het bijvoegen van het **Uniform Europees Aanbestedingsdocument** en dat de VRH na de selectie de bewijsstukken kan opvragen bij de geselecteerde inschrijvers. Dit neemt niet weg dat de VRH hier op elk moment eerder in de procedure aan inschrijvers om kan verzoeken om vast te stellen of inschrijvers niet moeten worden uitgesloten, als dit naar het oordeel van de VRH noodzakelijk is voor het verloop van de procedure.

Een inschrijver dient op eerste verzoek van de VRH binnen vijf werkdagen nadere bewijsstukken te kunnen overleggen om het verklaarde voor wat betreft de uitsluitingsgronden te staven. Als blijkt dat

inschrijver niet voldoet of de benodigde bewijsstukken niet tijdig kan overleggen, kan hij alsnog worden uitgesloten. Als dit na de selectie plaatsvindt, kan de selectie ongedaan gemaakt worden voor deze leverancier. Als inschrijver op de hoogte is van feiten en/of omstandigheden die zich hebben voorgedaan in de periode nadat het stuk is afgegeven die eventueel tot het toepassen van de uitsluitingsgrond zouden kunnen leiden, dient hij dit aan de VRH te melden.

3.3 Economische en financiële draagkracht

Door het aanvinken van 'Ja' in onderdeel α in Deel IV van het UEA ("Algemene aanwijzing voor alle selectiecriteria") verklaart de inschrijver dat zijn onderneming voldoet aan alle hiernavolgende geschiktheidseisen:

- Inschrijver dient voldoende economische en financiële draagkracht te hebben om de continuïteit van zijn dienstverlening te waarborgen.
- Inschrijvers die niet aan alle gestelde eisen voldoen, worden uitgesloten van verdere deelname aan deze aanbesteding.
- Inschrijver dient, op verzoek van de VRH binnen 5 werkdagen de hieronder gevraagde gegevens aan te leveren zodat zijn economische en financiële draagkracht kan worden beoordeeld.

Minimumeis

A) Als geschiktheidseis geldt dat inschrijver voldoende financiële en economische draagkracht moet hebben om continuïteit gedurende de contractperiode, inclusief eventuele verlengingen, te waarborgen. Ook verklaart de Inschrijver dat zijn onderneming voldoet aan de gestelde eisen met betrekking tot financiële- en economische draagkracht dat:

Inschrijver beschikt over een beroeps-en bedrijfsaansprakelijkheidsverzekering met een minimale dekking tot 1 miljoen euro per gebeurtenis per jaar.

Op verzoek verstrekt de inschrijver als bewijsplicht aan de VRH een duplicaat verzekeringscertificaat of een verklaring van de verzekeraar dat aan de door de VRH gestelde eis wordt voldaan.

B)

Controleverklaring met goedkeurende strekking zonder continuïteitsparagraaf

Inschrijver dient financieel en economisch draagkrachtig te zijn om de opdracht met goed resultaat te kunnen uitvoeren. Inschrijver dient zijn financiële- en economische draagkracht aan te tonen door middel van een controleverklaring met goedkeurende strekking betreffende de jaarrekening over de twee meest recent afgesloten boekjaren. De controleverklaring met goedkeurende strekking over de jaarrekening mag – met betrekking tot het meest recent afgesloten boekjaar - ook géén zogenaamde continuïteitsparagraaf (d.w.z. een verplichte toelichtende paragraaf in de jaarrekening wegens ernstige onzekerheid over de continuïteit) bevatten. Het is verder niet nodig om jaarrekeningen, jaarverslagen etc. als bewijsstukken toe te voegen.

Op verzoek verstrekt de voorlopig hoogst scorende inschrijver als bewijsplicht aan de VRH gerichte informatie als een accountantsverklaring.

Inschrijven als samenwerkingsverband

Indien sprake is van een samenwerkingsverband, dan dient slechts één deelnemer in zijn geheel te voldoen aan de eisen t.a.v. financieel economische draagkracht. In Deel II onderdeel C van het UEA dient aangegeven te worden welke deelnemer van het samenwerkingsverband invulling geeft aan het criterium financieel economische draagkracht.

3.4 Technische en beroepsbekwaamheid

Minimumeis inschrijving in het nationale beroeps-/handelsregister

De inschrijver (alle leden van het samenwerkingsverband) dient een recente verklaring (niet ouder dan zes maanden gerekend vanaf de uiterste datum voor het indienen van inschrijvingen) aan te kunnen

leveren waaruit blijkt dat de inschrijver volgens de eisen die gelden in het land waarin de inschrijver is gevestigd, is ingeschreven in het nationale beroeps- of handelsregister. Binnen Nederland vervult een uittreksel van inschrijving in het handelsregister van de Kamer van Koophandel deze functie. Indiening van een kopie van deze inschrijving volstaat.

Uit de verklaring dient onder meer te blijken dat degene die de inschrijving heeft ondertekend, een rechtsgeldig bevoegd vertegenwoordiger van de inschrijver is.

Deze verklaring dient na een verzoek binnen 5 werkdagen door inschrijver aangeleverd te worden.

Minimumeis: Gecertificeerd ISO 27001

De inschrijver dient een geldig certificaat aan te kunnen leveren waaruit blijkt dat de inschrijver op de sluitingsdatum van deze aanbesteding gecertificeerd is volgens ISO 27001.

Deze verklaring dient na een verzoek van de VRH binnen 5 werkdagen door inschrijver aangeleverd te worden.

Minimumeis Kerncompetenties

De VRH heeft drie kerncompetenties geïdentificeerd waarover de inschrijver naar haar oordeel moet beschikken om de opdracht succesvol uit te kunnen voeren.

Kerncompetentie 1: ervaring met het leveren van dienstverlening SIEM om een Microsoft Cloud omgeving maximaal te beschermen

Inschrijver, als leverancier, heeft aantoonbare ervaring met het verzorgen van dienstverlening SIEM aan organisaties met minimaal 500 medewerkers. In de 36 maanden voor de sluitingsdatum heeft de inschrijver minimaal 5 klanten met een dergelijke omvang voorzien van een dienstverlening SIEM.

Kerncompetentie 2: ervaring met het leveren van dienstverlening SOC om een Microsoft Cloud omgeving maximaal te beschermen

Inschrijver, als leverancier, heeft aantoonbare ervaring met het verzorgen van dienstverlening SOC aan organisaties met minimaal 500 medewerkers. In de 36 maanden voor de sluitingsdatum heeft de inschrijver minimaal 5 klanten met een dergelijke omvang voorzien van een dienstverlening SOC.

Kerncompetentie 3: ervaring met BIO/BIO2 en overheidsorganisaties

Inschrijver heeft aantoonbare ervaring met het leveren van SIEM- en SOC-dienstverlening aan organisaties waarop de Baseline Informatiebeveiliging Overheid (BIO/BIO2) van toepassing is. De inschrijver heeft aantoonbare kennis van en ervaring met de eisen die voortvloeien uit de BIO/BIO2 en relevante wet- en regelgeving op het gebied van informatiebeveiliging. In de 36 maanden voorafgaand aan de sluitingsdatum heeft de inschrijver minimaal 3 overheidsorganisaties of andere vergelijkbare gereguleerde organisaties voorzien van SIEM- en/of SOC-dienstverlening. De inschrijver dient aantoonbaar ervaring te hebben met:

- monitoring, detectie, analyse en afhandeling van beveiligingsincidenten;
- logging en audit-trails ten behoeve van compliance en verantwoording;
- advisering over informatiebeveiligingsmaatregelen;
- ondersteuning van BIO/BIO2-compliance;
- rapportages ten behoeve van audits, ENSIA, interne controles of vergelijkbare verantwoordingsprocessen.

De inschrijver verklaart door inschrijving aan deze minimumeisen te voldoen. Als de inschrijver aan alle eisen voldoet, volstaat voor de inschrijving het invullen van het **Uniform Europees Aanbestedingsformulier** (Deel IV).

Op verzoek verstrekt de inschrijver aan de VRH een overzicht van referentiegegevens die door de VRH kunnen worden gecontroleerd. Referenties worden uitsluitend als geldig beschouwd indien de betreffende opdracht door de inschrijver is uitgevoerd.

Als niet aan de bovengenoemde vereisten is voldaan, kan de inschrijving worden uitgesloten.

3.5 Samenvattend

Als u, als inschrijver, voldoet aan de gestelde eisen, vult u het Uniform Europees Aanbestedingsdocument in en zorgt u voor rechtsgeldige ondertekening.

De VRH kan bewijslast opvragen, welke dan binnen vijf werkdagen moet worden aangeleverd.

Hoofdstuk 4 Beoordeling van de inschrijvingen

Als een inschrijving niet op eerdere gronden is uitgesloten en de aanbieding tijdig is ingediend, wordt overgegaan tot de inhoudelijke beoordeling van het aanbod van inschrijver. De aanbieding met de hoogste score (beste prijs-kwaliteitsverhouding) is de aanbieding waaraan gegund wordt. Na de aanbesteding volgt het proces van opdrachtverstrekking, afstemming en overname dienstverlening.

4.1 Gunningscriteria

Er wordt gegund op basis van **beste prijs-kwaliteitverhouding**, waarbij de inschrijving op kwaliteit beoordeeld wordt. Prijzen vormen geen onderscheidend onderdeel van de gunningsbeoordeling, de VRH heeft in paragraaf 5.5 Prijs implementatie en maandelijks dienstverlening SIEM-SOC vaste tarieven geformuleerd.

Voor de gunningscriteria worden beoordelingscijfers toegekend op een schaal van 0 tot en met 10, welke wordt gewogen met hieronder genoemde wegingsfactor. De inschrijving met het hoogste behaalde puntentotaal wordt aangemerkt als de winnende inschrijving.

Gunningscriteria	Subcriterium	Wegingsfactor
Kwaliteit 1.000 punten	K1 - SIEM	35
	K2 - SOC	35
	K3 - Advisering	20
	K4 - Implementatie	10
Maximaal te behalen punten: 1.000		

4.2 Beoordelingsprocedure Kwaliteit

Voor de beoordeling van de kwalitatieve gunningscriteria (K1 t/m K4) wordt een beoordelingscommissie samengesteld. Dit beoordelingsteam bestaat uit diverse materiedeskundigen vanuit de VRH, met aansturing vanuit projectmanagement en inkoop.

Leden van de beoordelingscommissie beoordelen de inschrijving op de gunningscriteria onafhankelijk van elkaar en op basis van eigen deskundigheid, waarna binnen de beoordelingscommissie de scores en motivaties in consensus tot één eindscore wordt vastgesteld. Er wordt dus geen gemiddelde score berekend.

Als meerdere inschrijvingen eindigen met een gelijke score op de winnende positie, geeft de beoordeling op het gunningscriterium Kwaliteit (totaal van de vragen 5.1 tot en met 5.4) de doorslag. In het onwaarschijnlijke geval dat ook dit geen uitsluitsel geeft, wordt er geloot tussen de gelijk scorende leveranciers.

4.3 Beoordelingsmethodiek Kwaliteit

Voor elk subcriterium zijn er vragen, waarvan de beantwoording door de VRH beoordeeld zal worden. De beoordeling wordt gemaakt op basis van de verstrekte antwoorden op de gestelde vragen. Uiteraard worden alle vragen beoordeeld vanuit het belang van de VRH en de aansluiting op het vraagstuk.

In consensus zal door de beoordelingscommissie een rapportcijfer (0 t/m 10) worden toegekend volgens onderstaande tabel:

Cijfer	Omschrijving
10	Uitstekend
9	Zeer goed
8	Goed
7	Ruim voldoende
6	Voldoende
5	Matig
4	Onvoldoende
3	Ruim onvoldoende
2	Slecht
1	Zeer slecht
0	Geen antwoord

De open vraagstelling geeft inschrijvers de gelegenheid zich inhoudelijk te onderscheiden en daarmee de VRH de kans op het beste beschikbare aanbod, en dit te kunnen beoordelen op aansluiting op de vraag en de organisatie VRH. Enige subjectiviteit in de beoordeling is hierbij nodig. Als waarborg voor voldoende objectiviteit is het beoordelingsproces ingericht met het oordeel in consensus door een commissie met een brede expertise en een beoordelingsproces onder toezicht van de afdeling inkoop.

Een onvoldoende score op een vraag (cijfer 4 of lager) kan leiden tot een afwijzing (knock-out).

Hoofdstuk 5 Vraagstelling en gunningscriteria

In paragraaf 1.5 Doelstelling en uitgangspunten van de opdracht is de cloudsecurityomgeving van de VRH op hoofdlijnen beschreven en is een overzicht gegeven van de gevraagde dienstverlening. In dit hoofdstuk 5 Vraagstelling en gunningscriteria beschrijft de VRH de kwaliteitsaspecten die van belang zijn voor de uitvoering van de opdracht en waarop de inschrijvingen worden beoordeeld.

Per kwaliteitscriterium formuleert de VRH haar doelstelling, de bijbehorende beoordelingsaspecten. Inschrijvers dienen hun aanbieding hierop te baseren.

Voor alle vragen geldt dat de inschrijver:

- relevante algemene en specifieke ontwikkelingen beschrijft;
- gemaakte keuzes motiveert;
- aangeeft welke kwaliteits- en continuïteitswaarborgen worden geboden;
- geen verwijzingen opneemt naar externe websites of internet.

Om een efficiënte en objectieve beoordeling mogelijk te maken mag de totale beantwoording van de kwaliteitscriteria maximaal 50 A4-pagina's omvatten. Hierbij gelden de in dit hoofdstuk opgenomen maxima per kwaliteitscriterium.

De VRH beoordeelt de beantwoording integraal en in onderlinge samenhang. Daarbij wordt onder andere gekeken naar:

- aansluiting op de doelstellingen van de VRH;
- kwaliteit en haalbaarheid van de voorgestelde aanpak;
- mate van borging van continuïteit en kennis;
- concrete invulling van processen en dienstverlening;
- overdraagbaarheid;
- leesbaarheid en structuur.

De beantwoording dient begrijpelijk te zijn voor zowel ICT-specialisten als niet-technische gebruikers.

5.1 Kwaliteitscriterium 1: SIEM

De VRH wenst een hoogwaardige, toekomstbestendige SIEM- en SOC-dienstverlening die aansluit op de bestaande Microsoft-securityarchitectuur zoals beschreven in paragraaf 1.4 Huidige situatie ICT- en security-omgeving van de VRH.

Voor het verlenen van dienstverlening SIEM is het belangrijk dat de leverancier zowel bestaande en toekomstige technologieën actief beheert. Dit omvat het:

- het borgen van kwaliteit, continuïteit, schaalbaarheid, overdraagbaarheid en toekomstbestendigheid van de security monitoring- en analyseomgeving;
- de dienstverlening dient bij te dragen aan het vergroten van de digitale weerbaarheid van de VRH en het ondersteunen van de organisatie bij het voldoen aan BIO, BIO2, AVG en NIS2;
- inrichten en doorontwikkelen van monitoring-, detectie- en rapportagefunctionaliteiten;
- integreren en beheren van nieuwe (Microsoft) technologieën en databronnen binnen de dienstverlening;
- beheren, onderhouden en optimaliseren van het bestaande SIEM-platform;
- de opdrachtnemer dient zorg te dragen voor effectieve monitoring, detectie, analyse, classificatie, escalatie en rapportage van beveiligingsincidenten binnen de Microsoft Sentinel-omgeving van de VRH.

Vraag 1: Beschrijf op welke wijze u de SIEM-dienstverlening voor de VRH uitvoert binnen de bestaande Microsoft Sentinel-omgeving. Uw beschrijving bevat maximaal 15 pagina's (formaat A4, enkelzijdig, inclusief bijlagen, verwijzingen, voorbeelden enzovoort, exclusief rapportages, voorbladen, inhoudsopgave en ondertekenveld). Ga hierbij ten minste in op de volgende onderwerpen:

Dienstverleningsmodel

- Beschrijf uw SIEM-dienstverlening inclusief de aangeboden functionaliteiten, verantwoordelijkheden, processen en dienstverleningstijden, de afbakening van verantwoordelijkheden tussen opdrachtnemer en VRH en de wijze waarop wordt aangesloten op de bestaande Microsoft-securityarchitectuur.

Logmanagement en dataverwerking

- Beschrijf hoe loggegevens worden verzameld, verwerkt, gecorreleerd en beveiligd binnen Microsoft Sentinel. Ga hierbij in op:
 - onboarding van nieuwe en bestaande databronnen;
 - datakwaliteit;
 - correlatie van gebeurtenissen;
 - bewaartermijnen;
 - performance en schaalbaarheid.

Samenwerking met ketenpartners en beheerders

- Beschrijf hoe u samenwerkt met de leverancier(s) verantwoordelijk voor technisch beheer van de werkplekomgeving, Microsoft 365-omgeving en overige ICT-dienstverlening. Ga daarbij in op:
 - verantwoordelijkheidsverdeling;
 - operationele afstemming;
 - incidentafhandeling;
 - wijzigingsbeheer;
 - escalatieprocedures;
 - gezamenlijke verbetering van de securitymonitoring.

Detectie- en use-casebeheer

- Beschrijf hoe detectieregels, use cases, analytics rules en automatiseringen worden ingericht, beheerd en doorontwikkeld gedurende de looptijd van de overeenkomst.
- Beschrijf tevens:
 - prioritering van verbeteringen;
 - beheer van false positives;
 - kwaliteitsborging van detecties.

Wet- en regelgeving

- Beschrijf hoe uw dienstverlening bijdraagt aan naleving van:
 - ISO 27001/2
 - BIO2;
 - AVG;
 - NIS2;
- Geef daarbij aan hoe u wijzigingen in wet- en regelgeving vertaalt naar concrete verbetermaatregelen binnen de dienstverlening.

Beschikbaarheid en continuïteit

- Beschrijf op welke wijze u de continuïteit van de dienstverlening, de beschikbaarheid van monitoring en de kwaliteit van de dienstverlening borgt gedurende de gehele contractperiode. Voeg een voorbeeld van Service Level Agreement (afgekort SLA) bij. Beschrijf:
 - beschikbaarheid;
 - responstijden;
 - oplostijden;
 - escalatieniveaus;

- rapportageverplichtingen;
- prestatie-indicatoren.

Rapportages

- Voeg een voorbeeld toe van:
 - maandrapportage;
 - kwartaalrapportage;
 - managementrapportage.
- Beschrijf tevens welke KPI's, trends, risico's, dreigingen en verbeterpunten hierin worden opgenomen.

Exitstrategie

- Beschrijf uw exitstrategie en de wijze waarop u overdraagbaarheid van kennis, documentatie, configuraties, detectieregels, use cases en procedures naar de VRH of een opvolgende leverancier waarborgt.

Let op dat de uitwerking van het bovenstaande niet vrijblijvend is, maar in uitvoering moet worden gebracht tijdens de uitvoering van aangevraagde opdracht(en).

De inschrijver mag aanvullende onderwerpen opnemen indien deze aantoonbaar bijdragen aan de doelstellingen van de VRH. Dit houdt in dat de voornoemde onderwerpen nadrukkelijk geen afzonderlijke gunningscriteria zijn. De VRH is bevoegd de uitwerking van Kwaliteitscriterium 1 door inschrijver te laten verduidelijken in de verificatiefase en de initiële score na verduidelijking bij te stellen.

De door inschrijver aangeleverde beantwoording van dit onderdeel wordt in zijn totaliteit beoordeeld. Belangrijke aandachtspunten in de beoordeling zijn de mate waarop de SIEM-dienstverlening aansluit op de VRH-organisatie, relevantie, kwaliteit, borging, uitvoerbaarheid en continuïteit.

De beschrijving wordt mede beoordeeld op leesbaarheid, volledigheid, overtuiging en concreetheid van het aanbod voor de totale contractduur.

5.2 Kwaliteitscriterium 2: SOC

De VRH wenst een Security Operations Center dat 24x7 ondersteuning biedt bij monitoring, detectie, analyse en opvolging van beveiligingsincidenten.

Vraag 2: Beschrijf op welke wijze u de SOC-dienstverlening voor de VRH uitvoert. Uw beschrijving bevat maximaal 15 pagina's (formaat A4, enkelzijdig, inclusief bijlagen, verwijzingen, voorbeelden enzovoort, exclusief voorbladen, inhoudsopgave en ondertekenveld). Ga hierbij ten minste in op de volgende onderwerpen:

Security monitoring

- Beschrijf:
 - de inrichting van uw SOC;
 - de beschikbare bezetting;
 - de wijze waarop 24x7 monitoring plaatsvindt;
 - de werkwijze voor triage en classificatie van incidenten.

IAM

- Beschrijf voor IAM-gebeurtenissen:
 - de wijze voor monitoring;
 - de wijze voor, detectie;

- de wijze voor onderzoek.

Threat Intelligence

- Beschrijf op welke wijze threat intelligence wordt toegepast binnen de dienstverlening. Ga hierbij in op:
 - gebruikte informatiebronnen;
 - verrijking van detecties;
 - vertaling naar nieuwe use cases;
 - periodieke actualisatie.

Darkweb-monitoring

- Beschrijf op welke wijze actieve Darkweb-scans worden uitgevoerd om mogelijke gelekte data, accounts, credentials en andere aan de VRH gerelateerde informatie te identificeren. Ga hierbij in op:
 - welke bronnen worden geraadpleegd;
 - hoe worden bevindingen gevalideerd en gecorreleerd met bestaande detecties binnen Microsoft Sentinel;
 - beschrijven van de wijze van rapportage, escalatie en opvolging van geconstateerde blootstellingen.

Threat Hunting

- Beschrijf uw aanpak voor threat hunting. Ga hierbij in op:
 - frequentie;
 - methodiek;
 - gebruikte expertise;
 - rapportage van bevindingen;
 - opvolging van geconstateerde risico's.

Incidentrespons

- Beschrijf uw werkwijze voor:
 - classificatie van incidenten;
 - escalatie, waaronder de gehanteerde escalatieniveaus, de escalatiecriteria, de wijze van communicatie en afstemming met de VRH en – indien van toepassing – andere betrokken leveranciers;
 - communicatie richting VRH;
 - ondersteuning tijdens incidentrespons.
- Beschrijf welke inzet en beschikbaarheid van Team ICT Beheer gedurende de dienstverlening door u wordt verwacht.

Let op dat de uitwerking van het bovenstaande niet vrijblijvend is, maar in uitvoering moet worden gebracht tijdens de uitvoering van aangevraagde opdracht(en).

De inschrijver mag aanvullende onderwerpen opnemen indien deze aantoonbaar bijdragen aan de doelstellingen van de VRH. Dit houdt in dat de voornoemde onderwerpen nadrukkelijk geen afzonderlijke gunningscriteria zijn. De VRH is bevoegd de uitwerking van Kwaliteitscriterium 2 door inschrijver te laten verduidelijken in de verificatiefase en de initiële score na verduidelijking bij te stellen.

De door inschrijver aangeleverde beantwoording van dit onderdeel wordt in zijn totaliteit beoordeeld. Belangrijke aandachtspunten in de beoordeling zijn de mate waarop de SOC-dienstverlening aansluit op de VRH-organisatie, relevantie, kwaliteit, borging, uitvoerbaarheid en continuïteit.

De beschrijving wordt mede beoordeeld op leesbaarheid, volledigheid, overtuiging en concreetheid van het aanbod voor de totale contractduur.

5.3 Kwaliteitscriterium 3: Advisering

Dit kwaliteitscriterium heeft betrekking op het identificeren van kansen en risico's door de inschrijver. Het streven van de VRH is zo snel mogelijk risico's te mitigeren (minimaliseren).

Vraag 3: Geef een beschrijving van maximaal 10 pagina's A4 (enkelzijdig, inclusief bijlagen, verwijzingen, voorbeelden enzovoort) met hierin ten minste de volgende onderwerpen:

Strategische advisering

- Beschrijf op welke wijze u de VRH proactief adviseert over:
 - cyberdreigingen;
 - doorontwikkeling van de SIEM- en SOC-dienstverlening;
 - nieuwe Microsoft-functionaliteiten;
 - optimalisatie van detectie- en responsprocessen;
 - verbetering van de beveiligingspositie;
 - het verstrekken van ISAE-verklaringen type 1 en 2.
- Beschrijf op welke wijze u de VRH gedurende de looptijd van de overeenkomst proactief adviseert over relevante ontwikkelingen op het gebied van cyberdreigingen, wet- en regelgeving, normenkaders, beveiligingsrichtlijnen en technische ontwikkelingen. Geef daarbij aan hoe u deze ontwikkelingen vertaalt naar concrete adviezen, verbetervoorstellen en benodigde aanpassingen binnen de SIEM- en SOC-dienstverlening.

Beschrijf tevens in hoeverre de voor deze ontwikkelingen benodigde reguliere functionaliteiten, rapportages, advisering en ondersteuning onderdeel uitmaken van de aangeboden dienstverlening en geef expliciet aan welke onderdelen daar eventueel buiten vallen.

Kansen- en risicodossier

- Beschrijf de belangrijkste kansen en risico's ten aanzien van de dienstverlening SIEM-SOC (die binnen en buiten de invloedssfeer van de inschrijver vallen) en wat voor gevolg(en) de kans of het risico kan hebben.

Prioriteren

- Beschrijf op welke wijze u de geïdentificeerde kansen en risico's prioriteert. Beschrijf de door u gehanteerde mitigerende beheersmaatregelen.

Let op dat de uitwerking van het bovenstaande niet vrijblijvend is, maar in uitvoering moet worden gebracht tijdens de uitvoering van aangevraagde opdracht(en).

De inschrijver mag aanvullende onderwerpen opnemen indien deze aantoonbaar bijdragen aan de doelstellingen van de VRH. Dit houdt in dat de voornoemde onderwerpen nadrukkelijk geen afzonderlijke gunningscriteria zijn. De VRH is bevoegd de uitwerking van Kwaliteitscriterium 3 door inschrijver te laten verduidelijken in de verificatiefase en de initiële score na verduidelijking bij te stellen.

De door inschrijver aangeleverde beantwoording van dit onderdeel wordt in zijn totaliteit beoordeeld. Belangrijke aandachtspunten in de beoordeling zijn de mate waarop de advisering aansluit op de VRH-organisatie, relevantie, kwaliteit, borging, uitvoerbaarheid en continuïteit.

De beschrijving wordt mede beoordeeld op leesbaarheid, volledigheid, overtuiging en concreetheit van het aanbod voor het totale kansen- en risicodossier.

5.4 Kwaliteitscriterium 4: Implementatieplan

Dit kwaliteitscriterium heeft betrekking op de implementatie en overname van de huidige cloudsecuritydienstverlening van de VRH naar de door de inschrijver aangeboden SIEM- en SOC-dienstverlening.

Na gunning wordt de implementatieplanning in overleg met de VRH vastgesteld. De einddatum van de huidige overeenkomst en de continuïteit van de dienstverlening zijn daarbij randvoorwaardelijk. Gezien het belang van de dienstverlening, de impact op de organisatie en de beschikbare capaciteit binnen de VRH, wordt een zorgvuldige en beheersbare overgang verwacht.

De VRH verwacht van de inschrijver een helder, realistisch en uitvoerbaar implementatieplan waarin inzichtelijk wordt gemaakt hoe de overname van de dienstverlening wordt voorbereid, uitgevoerd en geborgd. Daarbij wordt verwacht dat de inschrijver een actieve, faciliterende en ondersteunende rol vervult en aantoonbare toegevoegde waarde levert gedurende het gehele implementatietraject.

Vraag 4: Beschrijf op welke wijze u de implementatie en overname van de dienstverlening voor de VRH uitvoert. Uw beschrijving bevat maximaal 10 pagina's (formaat A4, enkelzijdig, inclusief bijlagen, verwijzingen, voorbeelden enzovoort, exclusief voorbladen, inhoudsopgave en ondertekenveld). Ga hierbij ten minste in op de volgende onderwerpen:

Projectaanpak

- Beschrijf uw projectaanpak en de wijze waarop u de implementatie bij de VRH vormgeeft. Ga hierbij in op:
 - de fasering van het implementatietraject;
 - randvoorwaarden en afhankelijkheden;
 - risico's en beheersmaatregelen;
 - de verwachte bijdrage van de VRH;
 - de overdracht van het implementatieteam naar de beheer- en uitvoeringsorganisatie;
 - de migratie, overname en borging van actuele en historische gegevens uit de huidige cloudsecurityomgeving;
 - de motivering van gemaakte keuzes.

Rollen en verantwoordelijkheden

- Beschrijf de rollen, verantwoordelijkheden en benodigde inzet van de bij de implementatie betrokken partijen. Ga daarbij in
 - de samenstelling van het implementatieteam;
 - de rollen, verantwoordelijkheden en expertise van de betrokken medewerkers;
 - de rol van Team ICT Beheer van de VRH gedurende de implementatie;
 - de verwachte inzet vanuit de VRH, uitgesplitst naar functies, expertisegebieden en benodigde uren. Licht toe waarom de voorgestelde bezetting passend is voor een succesvolle uitvoering van de implementatie.

Planning en beheersing

- Beschrijf hoe u een tijdige en beheerste implementatie waarborgt. Ga hierbij in op:
 - de projectplanning;
 - de relatie met de beëindiging van de huidige dienstverlening;
 - mijlpalen en besluitmomenten;
 - doorlooptijden;
 - benodigde inzet van medewerkers;
 - kritieke afhankelijkheden;
 - de momenten waarop inzet van de VRH noodzakelijk is.

Let op dat de uitwerking van het bovenstaande niet vrijblijvend is, maar gedurende de uitvoering van de overeenkomst daadwerkelijk moet worden gerealiseerd.

De inschrijver mag aanvullende onderwerpen opnemen indien deze aantoonbaar bijdragen aan de doelstellingen van de VRH. De voornoemde onderwerpen vormen nadrukkelijk geen afzonderlijke gunningscriteria. De VRH is bevoegd de uitwerking van Kwaliteitscriterium 4 in de verificatiefase te laten verduidelijken en de initiële score naar aanleiding daarvan bij te stellen.

De door de inschrijver aangeleverde beantwoording van dit onderdeel wordt integraal beoordeeld. Belangrijke aandachtspunten daarbij zijn de mate waarin de implementatie aansluit op de situatie en doelstellingen van de VRH, de kwaliteit en haalbaarheid van de aanpak, de beheersing van risico's en afhankelijkheden, de borging van kennis en continuïteit, en de uitvoerbaarheid van de planning.

De beschrijving wordt mede beoordeeld op leesbaarheid, volledigheid, overtuigingskracht en concreetheid van het aanbod voor de totale implementatieduur.

5.5 Prijs implementatie en maandelijkse dienstverlening SIEM-SOC

De VRH streeft naar een juist kostenniveau van de dienstverlening SIEM-SOC. Bieden van transparantie, eerlijke tarieven en voorspelbaarheid door de inschrijver zijn daarbij noodzakelijk voor de VRH. Voor de VRH dienen er geen verborgen kosten te zijn.

De VRH heeft een vaste prijs voor de implementatie en vaste prijs voor maandelijks dienstverlening SIEM-SOC vastgesteld. Deze tarieven maken geen onderdeel uit van de gunningsbeoordeling. De opdracht wordt gegund op basis van de beste kwaliteitsverhouding, waarbij kwaliteit voor 100% bepalend is.

Inschrijvers dienen deze tarieven te accepteren. Andere dan de hier onder genoemde tarieven mogen niet in rekening worden gebracht:

Prijs implementatie:

Voor de eenmalige implementatie van de SIEM-SOC dienst betaalt de VRH een vooraf bepaalde vaste "all-in" tarief van € 30.000 exclusief BTW. All-in betreft alle kosten van benodigde implementatiewerkzaamheden, zoals projectmanagement en onboarding, koppeling van logbronnen, configuratie van SIEM-platform, use cases, detectieregels, rapportages, acceptatie- en testfase etc.

Van deze vergoeding mag 50% bij aanvang van de implementatie in rekening worden gebracht en 50% na succesvolle afronding van de implementatie.

Prijs dienstverlening SIEM-SOC per maand:

Voor de aangeboden dienstverlening SIEM-SOC inclusief advisering betaalt de VRH een vooraf bepaald vaste "all-in" maandtarief van € 15.000 exclusief btw. All-in betreft alle kosten voor onder andere 24/7 SOC-dienstverlening, monitoring, detectie, incidentanalyse, rapportages, advisering, alle benodigde software en systemen, scans, opslagcapaciteit, dataverbruik, beheer en onderhoud. Alle kosten die noodzakelijk zijn voor de uitvoering van de SIEM-SOC dienstverlening zijn inbegrepen in het maandtarief.

Dit maandtarief mag maandelijks vooraf in rekening worden gebracht bij VRH. De VRH betaalt correcte facturen met een betaaltermijn 30 dagen.

Vraag 5: Vul uw gegevens in op het blad **Verklaring akkoord vaste prijzen dienstverlening SIEM-SOC** (Bijlage 5) en onderteken voor akkoord. De verklaring wordt uitsluitend beoordeeld op volledigheid en akkoordverklaring van de inschrijver.

Bijlage 1 – Uniform Europees Aanbestedingsformulier

Deze is als separaat document te downloaden via www.tenderned.nl

Bijlage 2 - Concept overeenkomst dienstverlening SIEM-SOC

Deze is als separaat document te downloaden via www.tenderned.nl

Bijlage 3 - Concept verwerkersovereenkomst

Deze is als separaat document te downloaden via www.tenderned.nl

Bijlage 4 - Inkoopvoorwaarden VNG GIBIT 2025

Deze is als separaat document te downloaden via www.tenderned.nl

Bijlage 5 – Verklaring akkoord vaste prijzen dienstverlening SIEM-SOC

Deze is als separaat document te downloaden via www.tenderned.nl