# Marktconsultatiedocument
# SIEM, SOC, SOAR-dienstverlening

Ten behoeve van Veiligheidsregio Noord- en Oost-Gelderland

| | |
|---|---|
| Datum | 24-04-2026 |
| Status | Definitief |
| Versie | 1.0 |

| | |
|---|---|
| Projectnummer/kenmerk | P26-004 |
| TenderNed referentie | TN 586756 |

| | |
|---|---|
| Auteur | Edwin Moraal (CISO – ICT Adviseur) |
| Organisatieonderdeel | Bedrijfsvoering (Informatie) |

## 1.1 Beschrijving organisatie

Veiligheidsregio Noord- en Oost-Gelderland (hierna: VNOG) heeft één duidelijke missie: *samen werken aan veiligheid*. Vanuit deze missie richt de organisatie zich op het voorkomen, beperken en bestrijden van incidenten, rampen en crises, evenals op het herstel na ontwrichtende situaties. Dit gebeurt in nauwe samenwerking met partners zoals de politie, ambulancediensten, waterschappen en Defensie.

VNOG is één van de 25 veiligheidsregio's in Nederland en omvat een samenwerkingsverband van 22 gemeenten, van Winterswijk tot Harderwijk. Binnen de afdeling Risico- en Crisisbeheersing komen de samenwerkingen met diverse hulpverleningspartners samen, waaronder Defensie, Rijkswaterstaat en waterschappen.

De organisatie werkt vanuit drie belangrijke onderdelen: VNOG, Brandweer en GHOR (Geneeskundige Hulpverleningsorganisatie in de Regio). De brandweerzorg wordt ondersteund door een fijnmazig netwerk van 56 brandweerposten en betrokken, veelal vrijwillige medewerkers die de basis vormen voor de uitruktaken binnen de regio.

De GHOR is verantwoordelijk voor de coördinatie van de geneeskundige hulpverlening bij rampen en ongevallen. Dit gebeurt op basis van afspraken met onder andere ambulancediensten, zorginstellingen, zorgaanbieders en de GGD.

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

## 1.2 Achtergrond en aanleiding

VNOG is verantwoordelijk voor crisisbeheersing, brandweerzorg, risicobeheersing en bevolkingszorg binnen een omvangrijk en divers werkgebied. De digitale weerbaarheid van VNOG is direct verbonden aan de continuïteit van hulpverlening en crisiscoördinatie. Verstoringen in IT- en OT-systemen kunnen daarbij directe impact hebben op de publieke veiligheid. VNOG is aangemerkt als vitale aanbieder, hetgeen leidt tot verhoogde eisen op het gebied van digitale weerbaarheid, informatiebeveiliging en continuïteit.

De dreiging voor publieke organisaties ontwikkelt zich snel en kenmerkt zich door toenemende professionalisering, schaalvergroting en een groeiende geopolitieke component. In deze context maakt VNOG momenteel gebruik van SOC-dienstverlening. Aangezien de huidige contractperiode afloopt, is VNOG bezig met de voorbereiding van een aanbestedingsprocedure. De beoogde dienstverlening betreft SOC-dienstverlening, inclusief de inzet van SIEM, en waar relevant SOAR-functionaliteit.

In de afgelopen contractperiode heeft VNOG ervaring opgedaan met incidentafhandeling in crisissituaties, de samenwerking tussen leverancier en interne organisatie en de vertaling van dreigingsinformatie naar concreet risicobeheer. Uit een uitgevoerde veiligheids- en proportionaliteitsanalyse blijkt dat de inzet van deze dienstverlening noodzakelijk, proportioneel

en gerechtvaardigd is, mede gezien de hoge classificatie van beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

Tegelijkertijd constateert VNOG dat verdere doorontwikkeling van de huidige dienstverlening noodzakelijk is. In de huidige situatie ligt de nadruk sterk op detectie en signalering, terwijl behoefte bestaat aan meer concreet handelingsperspectief en ondersteuning bij de opvolging van incidenten, zodat sneller en effectiever kan worden gehandeld bij (dreigende) verstoringen. Daarnaast wenst VNOG verder ontzorgd te worden door een partner die aantoonbaar ervaring heeft met vitale organisaties en crisisomgevingen, en die in staat is om dienstverlening te leveren die aansluit bij het mission critical karakter van de organisatie.

Met deze aanbestedingsprocedure beoogt VNOG de dienstverlening verder te professionaliseren. VNOG zoekt daarbij een partner die:

- Aantoonbaar beschikt over 24/7 operationele volwassenheid, passend bij een vitale organisatie, inclusief “eyes on glass”-monitoring door gekwalificeerde analisten;
- Duurzame continuïteit en leveringszekerheid kan garanderen binnen Europese juridische, soevereiniteits- en privacykaders (o.a. BIO, AVG en NIS2);
- Transparantie en aantoonbaarheid biedt in detectiedekking, use-case volwassenheid en de kwaliteit, snelheid en effectiviteit van de respons;
- Aantoonbaar aansluit op (dreigings)informatie-uitwisseling en samenwerking met nationale gremia, zoals het NCSC, en relevante sectorale samenwerkingsverbanden;
- Proactieve ondersteuning bij (dreigende en gemelde) incidenten integraal onderdeel maakt van de dienstverlening, inclusief threat hunting, use-case tuning en continue verbetering;
- Innovatie en doorontwikkeling structureel verankert in de dienstverlening, gericht op het verhogen van detectiecapaciteit, automatisering (SOAR) en reductie van responstijden;
- In staat is om aantoonbaar te rapporteren op effectiviteit, risico-reductie en compliance, passend bij bestuurlijke verantwoording.

De uitvraag wordt ingericht op basis van een risico gestuurde benadering, waarbij aantoonbare reductie van exploiteerbare risico’s centraal staat.

De inzichten uit deze marktconsultatie worden gebruikt om de scope van de opdracht, de uitvraag en de aanbestedingsstrategie verder te concretiseren.

## 1.3 DOELSTELLINGEN VAN DE MARKTCONSULTATIE

VNOG bevindt zich in een oriënterende fase ten aanzien van een voorgenomen aanbesteding voor SIEM,SOC,SOAR-dienstverlening. De exacte scope en inhoud van de opdracht zijn op dit moment nog niet volledig uitgewerkt. Met deze marktconsultatie beoogt VNOG inzicht te verkrijgen in de mogelijkheden binnen de markt en input op te halen voor de verdere uitwerking van de opdracht, de eisen en de aanbestedingsstrategie.

VNOG wil met deze aanbesteding een beter beeld krijgen van het actuele marktaanbod, de beschikbare oplossingen en de mogelijkheden en beperkingen zoals die door marktpartijen worden gezien. De ontvangen reacties worden gebruikt als input voor het verder vormgeven van zowel de opdracht als de aanbestedingsstrategie.

De marktconsultatie wordt schriftelijk uitgevoerd. Deelname is vrijwillig en brengt voor marktpartijen geen verplichtingen met zich mee. VNOG is niet verplicht om de opgehaalde informatie geheel of gedeeltelijk te verwerken in een eventuele vervolgstap of aanbesteding.

Deelname aan deze marktconsultatie heeft geen invloed op een eventuele deelname aan een toekomstige aanbestedingsprocedure. Aan deze marktconsultatie kunnen door marktpartijen geen rechten worden ontleend.

VNOG wil de beoogde scope, eisen en de contractuele randvoorwaarden toetsen, valideren en waar nodig aanscherpen, mede aan de hand van de in de markt beschikbare oplossingen die kunnen bijdragen aan de verdere professionalisering van de dienstverlening op het gebied van detectie, respons en geautomatiseerde opvolging van cyberdreigingen en –incidenten.

De doelstellingen van deze marktconsultatie zijn:

- Inzicht verkrijgen in de mate van belangstelling van marktpartijen voor de beoogde opdracht;
- Verkennen in hoeverre de opdracht het best functioneel dan wel technisch kan worden gespecificeerd, en welke normen, standaarden en best practices daarbij passend zijn;
- Inzicht verkrijgen in de wijze waarop marktpartijen invulling geven aan detectie, respons, threat hunting, use-caseontwikkeling, automatisering en proactieve dienstverlening;
- Ophalen van informatie over relevante marktontwikkelingen, innovatieve oplossingsrichtingen en beschikbare diensten die bijdragen aan de verdere professionalisering van de dienstverlening van VNOG;
- Komen tot een realistische, proportionele en toekomstbestendige opdrachtomschrijving.

## 1.4 PROCEDURE VAN DE MARKTCONSULTATIE

De marktconsultatie verloopt als volgt:

- De marktconsultatie start met publicatie van dit document op TenderNed.
- Geïnteresseerde marktpartijen kunnen deelnemen door de vragen te beantwoorden en deze **uiterlijk op 12 mei 2026 via TenderNed** in te dienen.
- Vragen over deze marktconsultatie kunnen via TenderNed worden gesteld. Alle communicatie verloopt uitsluitend via TenderNed.
- Na sluiting van de schriftelijke ronde beoordeelt VNOG de ontvangen reacties.
- VNOG kan op basis van de ontvangen reacties een selectie maken van marktpartijen die worden uitgenodigd voor een nadere toelichting in een individueel gesprek. Deze gesprekken zijn bedoeld om de beantwoording van de vragen te verdiepen en vinden plaats in de periode van **8-12 juni 2026 of 22-26 juni 2026** en duren maximaal 2 uur per partij.
- De conceptversie van het marktconsultatieverslag wordt voorafgaand aan publicatie gedeeld met de betreffende marktpartijen voor verificatie op feitelijke onjuistheden en herleidbaarheid. Als binnen twee (2) weken geen reactie wordt ontvangen, gaat VNOG ervan uit dat geen bezwaar bestaat tegen publicatie.
- Indien VNOG besluit een aanbesteding te starten, wordt het marktconsultatieverslag gepubliceerd als onderdeel van de aanbestedingsstukken.
- Alle ontvangen informatie wordt vertrouwelijk behandeld.
- Eventuele kosten die marktpartijen maken voor deelname aan deze marktconsultatie worden niet door VNOG vergoed.
- VNOG behoudt zich het recht voor om de marktconsultatie tijdelijk op te schorten of volledig te stoppen.

## 1.5 PLANNING

Hieronder is de planning van de marktconsultatie weergegeven.

| **Actie** | **Datum** |
|---|---|
| Publicatie marktconsultatie | Vrijdag 24 april 2026 |
| Deadline stellen van vragen over marktconsultatiedocument | Dinsdag 12 mei 2026 |
| Publicatie Nota van Inlichtingen | Vrijdag 22 mei 2026 |
| Uiterste datum indienen reacties op gestelde vragen | Woensdag 27 mei 2026, 12:00 uur |
| Selectie en uitnodiging gesprekken | Vrijdag 29 mei 2026 |
| Gesprekken | Maandag 8 t/m vrijdag 12 juni en/of maandag 22 juni t/m vrijdag 26 juni |

*VNOG bepaalt, afhankelijk van het aantal reacties, welke week wordt benut voor de gesprekken en informeert alle marktpartijen zo spoedig mogelijk na beoordeling van de reacties over het vervolg.*

## BIJLAGE 1. VRAGENLIJST MARKTCONSULTATIE

**Organisatie en ervaring**

1. Heeft u ervaring met de gevraagde dienstverlening bij organisaties in de vitale sector? Zo ja, kunt u dit kort toelichten?
2. Werkt u samen met externe partijen (bijv. voor threat intelligence of incident response)? Zo ja, hoe is deze samenwerking ingericht? En welke onderdelen van de dienstverlening voert u zelf uit en welke via partners?

**Dienstverlening en oplossingsrichting**

3. Wat is de gemiddelde implementatietermijn om de SIEM, SOC-SOAR dienstverlening operationeel te krijgen?
4. Welke aanvullende of optionele diensten kunt u aanbieden bovenop de gevraagde dienstverlening, en in welke situaties acht u deze relevant?
5. Hoe borgt u de continuïteit van uw 24/7 SOC-dienstverlening (bijvoorbeeld bij uitval of piekbelasting)?
6. Hoe geeft u invulling aan detectie, respons en proactieve dienstverlening (zoals threat hunting)?
7. Hoe zorgt u dat uw dienstverlening aansluit op een risicogestuurde aanpak? Maakt u daarbij gebruik van bepaalde frameworks, methodieken of standaarden? Zo ja, licht dit toe.
8. In hoeverre bent u in staat om hybride omgevingen (on-premise IT, cloud en eventueel OT) integraal te monitoren, en welke beperkingen of aandachtspunten ziet u hierbij?
9. Welke KPI's en prestatie-indicatoren worden volgens u gebruikt om de kwaliteit van SOC-dienstverlening te meten, en welke acht u passend voor VNOG?

**Techniek en architectuur (verkennend)**

10. Welke architectuur- of oplossingsrichtingen ziet u als passend voor SIEM, SOC, SOAR-dienstverlening bij organisaties zoals VNOG?
11. Welke vormen van netwerkdetectie acht u passend, en wat zijn daarbij de belangrijkste afwegingen?
12. Hoe zorgt u dat detectie meegroeit met nieuwe en onbekende dreigingen (bijv. zonder afhankelijk te zijn van alleen signatures)?
13. Welke vormen van geautomatiseerde respons zijn volgens u gebruikelijk en wenselijk binnen SOC-dienstverlening?
14. Hoe voorkomt u afhankelijkheid van specifieke leveranciers (vendor lock-in) en hoe blijft de oplossing toekomstbestendig?
15. Hoe maakt u inzichtelijk welke dreigingen en aanvalstechnieken (bijv. op basis van MITRE ATT&CK) worden gedetecteerd en waar eventuele blinde vlekken in de detectie aanwezig zijn?

**Werking van de SOC-dienstverlening**

16. Levert u een 24/7 "eyes-on-screen" SOC-dienst? Kunt u kort toelichten hoe deze is ingericht?
17. Hoe worden incidenten en meldingen gecommuniceerd richting de klant?
18. Welke rol verwacht u van de klant (VNOG) bij incidentafhandeling en samenwerking?
19. Hoe borgt u de continuïteit van de dienstverlening bij verstoringen (bijv. uitval van een SOC-locatie)?

20. In hoeverre acht u het wenselijk dat een SOC zelfstandig mitigerende maatregelen neemt (bijv. isoleren van systemen), en welke randvoorwaarden en verantwoordelijkheden zijn hierbij van belang?
21. Hoe organiseert u de samenwerking met bestaande IT- en OT-leveranciers Opdrachtgever, met name bij incidenten, escalaties en wijzigingen?

**Specificatie, innovatie en marktontwikkelingen**

22. Wat is volgens u de beste manier om deze dienstverlening uit te vragen: functioneel of technisch? Licht uw antwoord toe.
23. Welke normen en standaarden acht u relevant voor deze dienstverlening?
24. Welke innovaties of ontwikkelingen in SIEM, SOC, SOAR-dienstverlening zijn volgens u relevant voor VNOG?
25. Hoe borgt u dat uw dienstverlening zich continu doorontwikkelt op basis van nieuwe dreigingen, technologieën (waaronder AI en automatisering) en wet- en regelgeving (bijv. NIS2), en hoe vertaalt u dit naar concrete verbeteringen voor de klant?

**Kosten en contract**

26. Hoe adviseert u om de prijsstelling voor SIEM, SOC, SOAR-dienstverlening zodanig in te richten dat inschrijvingen onderling goed vergelijkbaar zijn (bijv. onderscheid tussen implementatie, vaste kosten en variabele kosten)? Ga daarbij in op relevante prijscomponenten en mogelijke eenheden (bijv. per asset, bandbreedte, logvolume, use case of omgeving).

**Overig**

27. Zijn er aandachtspunten, risico's of alternatieve oplossingsrichtingen die VNOG volgens u moet meenemen in de verdere uitwerking van de aanbesteding?

**Als u geïnteresseerd bent in deelname aan deze marktconsultatie, verzoeken wij u uw antwoorden in te dienen middels het Antwoordenformulier Marktconsultatie SIEM, SOC, SOAR-dienstverlening (bijlage 1), uiterlijk op woensdag 27 mei 2026, 12:00 uur via TenderNed. Het antwoordenformulier wordt door VNOG in Word-formaat beschikbaar gesteld.**