Vraagnummer	Vraag	Antwoord
1	Is er een reden dat VNOG besloten heeft om niet aan de centrale uitvraag van het NIPV mee te doen? Zoja, welke?	VNOG heeft besloten niet deel te nemen aan de gezamenlijke aanbesteding vanuit het NIPV omdat het Programma van Eisen nog niet volledig was uitgewerkt en tevens niet aansloot bij ons verwachtingspatroon.
2	Kunt u aangeven welk belang VNOG hecht aan digitale onafhankelijkheid en datasoevereiniteit, en hoe dit zich vertaalt naar de beoogde dienstverlening en leverancierskeuze?	Voor de VNOG is digitale onafhankelijkheid en soevereiniteit essentieel om de betrouwbaarheid van onze publieke dienstverlening te waarborgen. Wij hechten er grote waarde aan dat onze data binnen de Europese rechtsorde wordt verwerkt en beheerd. Wij zoeken een partner die onafhankelijk is van grootmachten buiten de EU en die transparantie biedt over de gebruikte technologieketen.
3	Kunt u verduidelijken in welke OT-systemen onderdeel zijn van de beoogde scope, en welke specifieke eisen of beperkingen hierbij gelden (netwerk of ook op scada/plc-niveau?	De scope omvat de OT-systemen die direct invloed hebben op onze operationele slagkracht, zoals de aansturing van kazerne-faciliteiten, alarmeringssystemen en kritieke gebouwbeheersystemen. Het is cruciaal dat de security-oplossing niet alleen IT begrijpt, maar ook de specifieke protocollen en gedragingen van deze OT-omgevingen herkent.
4	Kunt u toelichten welke concrete knelpunten of verbeterpunten VNOG heeft ervaren in de huidige SOC-dienstverlening, met name op het gebied van incidentopvolging en samenwerking?	Laten we voorop stellen dat de bestaande SOC diensverlening goed is mbt tot snelheid en kwaliteit van triage en escalatie evenals de de beschikbaarheid van specialistische ondersteuning tijdens (grootschalige) incidenten. Een belangrijk verbeterpunt binnen een nieuwe samenwerking betreft het vergroten van de proactiviteit in detectie, dreigingsduiding en incidentopvolging. Op basis van eerdere ervaringen is gebleken dat puur technische monitoring (alleen alerts sturen) onvoldoende is. Een belangrijk verbeterpunt is de vertaalslag van technische dreigingen naar operationele risico's en het ontbreken van proactieve ondersteuning bij peace time value. Wij zoeken een partner die deze kloof overbrugt door middel van een resultaatgerichte aanpak. Gezien de diversiteit in specialistische kennis binnen onze organisatie en de beperkte beschikbaarheid hiervan buiten kantoortijden of tijdens afwezigheid van interne specialisten, bestaat behoefte aan een dienstverlening die sterker ondersteunt op continue monitoring, contextuele analyse en geautomatiseerde/gedelegeerde/gemandateerde opvolging

5	In de aanbestedingsdocumentatie wordt gevraagd om 24/7 SOC/SIEM-dienstverlening en monitoring. Kunt u bevestigen of hiermee expliciet wordt bedoeld dat er 24 uur per dag, 7 dagen per week sprake moet zijn van continu menselijk toezicht door SOC-medewerkers, ook wel “eyes on glass”, en of dit als knock-outcriterium geldt? Onze dienstverlening voorziet in 24/7 monitoring, waarbij detectie, correlatie, triage en eerste opvolgacties automatisch worden uitgevoerd via vooraf ingerichte flows en playbooks. Wanneer menselijke beoordeling of interventie nodig is, worden SOC-medewerkers automatisch en direct ingeschakeld. Hierdoor vindt de eerste respons zonder vertraging plaats en worden noodzakelijke vervolgstappen direct opgepakt. Kunt u bevestigen dat een dergelijke 24/7 monitoring- en responsinrichting, waarbij automatisering de initiële detectie en opvolging verzorgt en SOC-medewerkers direct worden ingeschakeld waar nodig, voldoet aan de gestelde eis? Of is permanente fysieke/menselijke bezetting achter een scherm gedurende 24/7 vereist?	Ja. Met de gevraagde 24/7 SOC/SIEM-dienstverlening wordt expliciet bedoeld dat sprake moet zijn van continue fysieke/menselijke bezetting door SOC-medewerkers (“eyes on glass/eyes on screen”), gedurende 24 uur per dag en 7 dagen per week. De betreffende dienstdoende engineer dient afdoende kennis te hebben om zo snel mogelijk een zelfstandigee triage uit te voeren. VNOG acht dit noodzakelijk gezien het gewenste niveau van operationele volwassenheid, de aard van de dienstverlening en de vereiste snelheid van detectie, dreigingsduiding en incidentopvolging. Het toepassen van automatisering, SOAR-functionaliteit, playbooks en geautomatiseerde triage wordt daarbij gezien als ondersteunend aan de dienstverlening, maar niet als vervanging van continue menselijke monitoring en directe menselijke beschikbaarheid. Een dienstverlening waarbij uitsluitend geautomatiseerde monitoring plaatsvindt en SOC-medewerkers uitsluitend reactief of on-demand worden ingeschakeld, voldoet daarom niet aan de gestelde eis.. Dit is een knock out criteria.
6	Kan de aanbestedende dienst aangeven wat de planning is voor de vervolgfase, de aanbesteding?	Na de verdiepende gesprekken die zullen plaatsvinden naar aanleiding van de marktconsultatie zal de aanbesteding worden voorbereid. We verwachten rond medio augustus/september te publiceren.
7	Hoe vertaalt VNOG de kwalificatie als “vitale aanbieder” binnen de NIS2 concreet naar eisen aan SOC/SIEM/SOAR (zoals beschikbaarheid, RTO/RPO, escalatietijden, redundantie etc.)?	Juridisch vallen veiligheidsregio's niet onder NIS2, Wel is er een sterke bestuurlijke en maatschappelijke verwachting om vergelijkbare (of zelfs betere) maatregelen en governance toe te passen. Het ontslaat het ons er dus niet van om als vitale aanbieder hoge eisen aan te stellen onze zorgplicht. Dit betekent dat wij niet kunnen volstaan met standaardoplossingen; wij vereisen een partner die aantoonbaar voldoet aan strenge normen (zoals ISO 27001/ 22301) en die ons helpt om aantoonbaar 'in control' te zijn door middel van continue monitoring, snelle responstijden en uitgebreide rapportage over onze weerbaarheid.
8	De VNOG ziet SOAR-functionaliteit als optionele component. Waarom wordt er juist niet ingezet op SOAR, mede vanwege toenemende dreiging van (door AI versnelde) aanvallen?	VNOG ziet SOAR als een krachtig middel om de snelheid van respons te verhogen, maar we willen voorkomen dat automatisering een doel op zich wordt. Het moet een logische aanvulling zijn op de expertise van de analisten in het SOC. Een partij die SOAR effectief kan inzetten om menselijke expertise te versterken, heeft echter een streepje voor.

9	De VNOG heeft het over doorontwikkeling van use cases. Worden deze use cases ter overname aangeboden (met andere woorden, zijn deze in eigendom van VNOG) of moet de bibliotheek met use cases opnieuw worden opgebouwd?	Wij verwachten een hybride model. De leverancier dient een robuuste set aan standaard use cases mee te leveren gebaseerd op actuele dreigingsinformatie. Tegelijkertijd willen we samen met de partner specifieke use cases ontwikkelen die aansluiten op de unieke processen van de veiligheidsregio.
10	In hoeverre overweegt VNOG vooraf mandaat te verlenen voor (semi) geautomatiseerde mitigerende acties, en voor welke typen assets of scenario's?	Dit is bespreekbaar onder strikte voorwaarden. Wij zoeken een partner die we zodanig vertrouwen dat zij, binnen vooraf afgestemde kaders (playbooks), direct actie kunnen ondernemen (zoals het isoleren van een besmet systeem) om verdere schade te voorkomen, met name buiten kantoortijden.
11	Maakt VNOG onderscheid tussen reguliere security-incidenten en crisissituaties (zoals GRIP), en wordt van de SOC verwacht hierin te kunnen opschalen qua werkwijze?	Ja. Voor reguliere incidenten verwachten we een efficiënte afhandeling via de MDR-dienst. In het geval van een grootschalige crisissituatie verwachten we echter dat de partner direct mee kan opschalen en onderdeel wordt van ons crisisteam, waarbij strategisch advies en hands-on incident response hand in hand gaan.
12	Worden eisen verwacht t.a.v. overdraagbaarheid van use-cases, playbooks, documentatie en data bij contractbeëindiging?	Ja, wij willen vendor lock-in voorkomen. Alle ontwikkelde logica, playbooks en documentatie moeten eigendom blijven van de VNOG of op een zodanige manier gedeeld worden dat een eventuele overdracht in de toekomst transparant en zonder verlies van kennis kan plaatsvinden. We zoeken een partner die werkt volgens 'open' standaarden.
13	VNOG vraagt aantoonbaarheid van controls, maar het is niet duidelijk voor wie. Welke type rapportages worden er in het contract verwacht? Voor welke doelgroep(en)?	Er wordt nergens gevraagd over aantoonbaarheid van controls, wellicht dat deze vraag niet goed geformuleerd is en derhalve niet beantwoord kan worden.
14	Wij adviseren VNOG om de uiteindelijke uitvraag in de aanbesteding zo te formuleren dat 'appels met appels' vergeleken kunnen worden. Dat betekent dat we adviseren om vooraf na te denken over het SOC/SIEM-model, aantal assets, prijsmodel, en Total Cost of Ownership (TCO), inclusief kosten voor logopslag- en retentie. Dit is relevant voor de verschillende log-, asset- en incidentmodellen die SOC/SIEM-partijen leveren.	Bedankt voor de opmerking. Wij zullen jullie opmerking in overweging nemen tijdens de voorbereiding van de aanbesteding.