Nr.	Paragraaf	Vraag	Beantwoording
1	2.1 Omschrijving van de Opdracht	Er wordt specifiek gevraagd om de inzet van honeypots als onderdeel van de SOC-SIEM dienstverlening. Wij hebben hierover enkele vragen ter verduidelijking, omdat in de huidige security-markt ook andere (soms effectievere en beter schaalbare) methoden voor vroegtijdige detectie van intrusies worden toegepast, zoals moderne deception platforms of deceptors. Deze oplossingen bouwen verder op het basisconcept van een traditionele honeypot, maar zijn doorgaans breder inzetbaar, bieden een grotere dekking (zoals identity lures, endpoint- en cloud deception, AD objects, etc.) en zijn vaak efficiënter in beheer vanwege automatische orchestration en integratie met SIEM/SOAR. Daarom willen wij graag de volgende vragen stellen ter verduidelijking van uw keuze: 1.Kunt u toelichten waarom specifiek is gekozen voor honeypots als verplicht onderdeel van de dienstverlening? Zijn er specifieke detectiedoelen of dreigingsscenario's waarin volgens u uitsluitend een traditionele honeypot effectief kan zijn, en niet een (breder) deception platform of vergelijkbare alternatieven? 2.Staat u open voor alternatieve invullingen van deze eis, bijvoorbeeld met moderne deception-oplossingen die dezelfde (of mogelijk betere) dekking, effectiviteit en lagere operationele belasting bieden? Indien nee, kunt u aangeven waarom dergelijke alternatieven voor BUCH niet volstaan? 3.Indien honeypots in uw visie onmisbaar zijn, kunt u onderbouwen waarom deze keuze de voorkeur verdient boven andere vormen van deception? Met deze vragen beogen wij te begrijpen of de verplichte inzet van honeypots voortkomt uit specifieke vereisten binnen uw threat landscape, of dat functionele equivalenten (zoals distributed deception tokens, endpoint/identity telemetry of netwerk-based analytics) ook tot de gewenste doelen kunnen leiden.	1. Er is gekozen voor honeypots omdat die een extra mogelijkheid bieden aanvallen in een vrij vroeg stadium van de kill-chain te detecteren, namelijk in de fase van internal discovery/lateral movement. Er zijn geen specifieke dreigingsscenario's waarin per definitie alleen een traditionele honeypot effectief kan zijn. Of een breder deception platform of andere alternatieven functioneel voldoen kunnen we niet beoordelen op basis van de informatie uit de vraagstelling. 2. De aanbestedende dienst staat open voor alternatieve invullingen, wanneer de gevraagde functionaliteit wordt geboden en wordt voldaan aan het Programma van Eisen (waarbij mogelijk een alternatieve invulling van E55 mogelijk is). U dient dit in uw beschrijving van de oplossing aan te tonen. Kortom: u kunt voor "honeypots" ook een andere oplossing met dezelfde functionaliteit lezen. 3. n.v.t. gezien het antwoord op onderdeel 2 van uw vraag.
2	2.1 Omschrijving van de Opdracht	U omschrijft ook wat de opdracht niet omvat. Heeft het uw voorkeur dat uw SOC leverancier toch ook de expertise kan bieden op andere cybersecurity diensten, zoals Penetratietesten, Continue Security Testing, Applicatiebeveiliging, Security Awareness Training, Red Teaming, Purple Teaming, Threat Modelling etc.?	De aanbestedende dienst zal expertise en dienstverlening op andere gebieden niet betrekken in de beoordeling van uw inschrijving.
3	4.6 Inschrijven als Combinatie of met gebruikmaking van een Derde	In deze paragraaf refereert u aan het inschrijven als combinatie of gebruikmaking van een Derde. Heeft het uw voorkeur dat uw SOC leverancier haar diensten niet uitbesteed aan derde partijen, maar dit zelf doet?	Er is geen voorkeur.
4	Bijlage H – E9	U eist dat alle verwerking van persoonsgegevens plaatsvindt binnen de Europese Economische Ruimte (EER). Inschrijver werkt met een hybride SOC vanuit Nederland en een zogeheten derde land buiten de EER. Is het acceptabel voor de opdrachtgever om akkoord te gaan met verwerking buiten de EER mits de door de Autoriteit Persoonsgegevens (AP) opgestelde richtlijnen voor verwerking buiten de EER op basis van een door de EC vastgesteld modelcontract gevolgd worden? (Zie art.46 van de AVG)	Neen
5	Bijlage H – E32	U eist dat tijdens openingstijden triage/analyse van hoge/kritieke alerts binnen 5 minuten plaatsvinden. Inschrijver hanteert hiervoor 30 min maar verzorgd in samenspraak met opdrachtgever op basis van het Dossier Afspraken en Procedures voor vooraf gedefinieerde scenario's (automatische) mitigerende acties. Is het acceptabel voor de opdrachtgever dat de inschrijver alternatieve triage tijden hanteert?	Neen, echter mogelijk is er een misverstand: E32 gaat over de start van de triage van hoge/kritieke alerts, niet zoals u in uw vraag lijkt te veronderstellen over de afronding daarvan. Daarnaast moet worden voldaan aan eis E33. Bij het starten van de triage pas na/binnen 30 minuten lijkt dat niet haalbaar.
6	Subgunningscriterium kwaliteit 2: Beschrijving van de oplossing	"Gezien het aantal onderwerpen dat inschrijvers moeten meenemen in de beantwoording voor het beschrijven van de oplossing is op basis van onze ervaring 7 x A4 te weinig voor een volledige beschrijving. Bent u bereid om dit aan te passen naar maximaal 10 x A4?"	Ja
7	Subgunningscriterium kwaliteit 3: Dekking van Use cases	Gezien onze ervaring bij het beschrijven van de dekking is de huidige limiet weinig voor een volledige beschrijving. Bent u bereid de paginalimiet voor dekking use cases verhogen naar 4 x A4?	Ja
8	Beschrijvend document SOC SIEM, Paragraaf 7.1	Het Plan van Aanpak mag maximaal 6 pagina's exclusief afbeeldingen zijn. Inschrijver heeft de voorkeur afbeeldingen en de tekst bij elkaar te zodat ze elkaar versterken Hiermee wordt echter het maximum aantal pagina's overschreden. Inschrijver verzoekt om een maximum aantal pagina's inclusief afbeeldingen op 9 te stellen. Kunt u hiermee instemmen?	Ja

Vraag over nummer 2 van NVI, onderdeel E33	Wij hanteren voor een Prio H-melding de volgende definitie: Prio H Incident – Er is geen directe incident response nodig, maar er is wel onmiddellijk actie vereist om escalatie te voorkomen. Zonder tijdige opvolging kan de situatie binnen korte tijd leiden tot een daadwerkelijk incident. Ondernomen actie bij Prio H-meldingen: Interne opvolging via ticketsysteem. Directe communicatie met relevante specialisten voor triage. Indien zich aanvullende incidenten voordoen, wordt geëscaleerd naar de hoogste prioriteit. De opdrachtnemer heeft hierin een actieve rol in detectie, opvolging en afhandeling. Concreet betekent dit: Actie: per e-mail. Doel: binnen 24 uur contact leggen, informeren en melding afhandelen. Vraag: Kunt u aangeven of u zich kunt vinden in deze definitie van een Prio H-melding en ermee akkoord bent dat deze meldingen binnen 24 uur opgepakt en afgehandeld moeten worden?	Neen, uw werkwijze borgt ons inziens onvoldoende dat een Prio H tijdig wordt opgevolgd, terwijl u aangeeft dat er onmiddelijk acite vereist is om escalatie te voorkomen. Uw aanpak "directe communicatie met relevante specialisten" lijkt in lijn met eis E33.