Algemene informatie

Aanbesteding:	Managed SIEM / SOC
Aanbestedende Dienst:	Veiligheidsregio Twente
Referentie:	Z2500XX/MASM

Toelichting:
Hierbij de 2e en laatste NVI;
AD gaat er vanuit dat Gegadigden hiermee over voldoende informatie beschikken om een Inschrijving te kunnen doen.
Inschrijvingen dienen uiterlijk op maandag 27 oktober 2025 vóór 12:00 uur te zijn ingediend.

AD wenst u succes bij het opstellen en indienen van uw Inschrijving.

Namens Veiligheidsregio Twente,

Maarten Smelt
Strategisch Inkoper

Vraag en antwoord

Ref.nr.	**Onderwerp:**
104	Algemeen

Vraag:
Gekwalificeerde digitale handtekeningen, bijvoorbeeld met DocuSign, ValidSign, of Adobe Sign voldoen aan de Europese eIDAS-verordening (electronic IDentification, Authentication and trust Services) die in 2016 is ingevoerd. Deze verordening zorgt ervoor dat gekwalificeerde digitale handtekeningen veilig en in de hele EU rechtsgeldig zijn. Strikt genomen heeft een gekwalificeerde digitale handtekening op een digitaal document (PDF) zelfs meer juridische bewijskracht dan enkel een digitale kopie (scan) van een met een natte handtekening getekend papieren document. Ook leveren alle aanbieders dan een bijdrage om papier te besparen.
Kunt u bevestigen dat u wat betreft rechtsgeldige ondertekening, waar dat wordt gevraagd, akkoord gaat met een gekwalificeerde digitale handtekening? Indien u dit niet accepteert, kunt u uw beslissing dan toelichten?

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
105

Onderwerp:
NVI3

Vraag:
u geeft aan dat het huidige budget is gebaseerd op de huidige kosten voor de SIEM/SOC dienstverlening. Kunt u formeel bevestigen dat een NIS2 compliant invulling van 24/7 eyes on screen (dus ingevuld via een SOC binnen de EU of EER) daar nu ook onderdeel van uitmaakt?

Antwoord:
Ja.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
106

Onderwerp:
NVI3

Vraag:
Kunt u uw definitie van 'eyes on screen' formuleren om misverstanden uit te sluiten voor wat betreft de door u verwachte dienstverlening? De gangbare invulling van deze 'eyes on screen' is via een op basis van ploegendienst ingericht SOC waarbij er 24 uur per dag mensen actief zijn. Dit komt neer op een teamgrootte van minimaal 12 personen waarbij er overuren, weekenddiensten en feestdagenvergoedingen worden betaald. Dit zijn hoogopgeleide specialisten en om deze dienst te leveren vanuit Nederland

voor het budget dat u voor ogen hebt, is moeilijk te rijmen met gangbare salarissen. Een piketdienst waarbij mensen wakker worden gebeld in geval van een P1 of P2 lijkt de enige reële manier om binnen budget een 24x7 dienst te leveren, dus het is voor ons belangrijk om exact te begrijpen wat u voor ogen hebt wanneer u 'eyes on screen' als eis stelt.

Antwoord:
De definitie die u schetst van ‘eyes on screen’ – een 24/7 bemand SOC met continue monitoring – is correct, met de toevoeging dat deze invulling niet exclusief voor onze organisatie hoeft te zijn. Het is dus toegestaan dat deze dienst wordt geleverd vanuit een gedeelde SOC-omgeving, zolang 24/7 actieve monitoring en directe opvolging van incidenten gewaarborgd zijn. Hiermee sluiten we uit dat een piketdienst of reactieve aanpak voldoet aan deze eis.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
107

Onderwerp:
NVI38

Vraag:
Het is ons niet duidelijk hoe om te gaan met de eis dat 'alle benodigde licenties en opslagcapaciteit' onderdeel dienen te zijn van de dienst. Verwacht u bijvoorbeeld dat gegadigde de Microsoft licenties voor endpoints levert, en levert u zelf de Sentinel opslag van 1TB zoals uw antwoord op NVI38 suggereert, of moet Gegadigde deze in de dienst meecalculeren? Graag ontvangen wij een overzicht van de licenties /abonnementen die u op dit moment reeds in bezit hebt en die door gegadigde niet hoeven te worden aangeboden.

Antwoord:
De eis dat ‘alle benodigde licenties en opslagcapaciteit’ onderdeel van de dienst moeten zijn, heeft geen betrekking op Microsoft-licenties in het algemeen, aangezien de opdrachtgever reeds over deze licenties beschikt.

Kosten voor Microsoft Sentinel vallen wél binnen de scope van deze aanbesteding. Niet alle logbronnen komen momenteel in Microsoft Sentinel terecht; de huidige opslaginstelling in Sentinel is 30 dagen.

De genoemde 1TB betreft de hoeveelheid data die wij momenteel richting het SOC sturen; dit omvat niet alleen Sentinel-data, maar ook firewall-logs, etc. Wij verwachten dat inschrijvers deze uitgangspunten respecteren en Sentinel-kosten meecalculeren, inclusief voldoende capaciteit en integratie om logdata te verwerken binnen de MDR-dienst.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
108

Onderwerp:
Huidige leverancier

Vraag:
Kunt u aangeven wat de belangrijkste redenen zijn dat u overweegt te wisselen van huidige partner? Zijn er specifieke pijnpunten bij de huidige partij?

Antwoord:
Vanuit wet- en regelgeving (Aanbestedingswet 2012) zijn we verplicht deze dienst aan te besteden.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 109

Onderwerp:
Voordeel andere VR's

Vraag:
Hecht de opdrachtgever waarde aan het feit dat een leverancier ook 24/7 monitoring uitvoert voor andere veiligheidsregio’s, gezien de mogelijke meerwaarde voor threat hunting en het tijdig signaleren van vergelijkbare dreigingen binnen vergelijkbare organisaties?

Antwoord:
Geen invloed op de beoordeling.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 110

Onderwerp:
SOAR-functionaliteit buiten scope

Vraag:
Waarom is automatische response (SOAR-functionaliteit) expliciet buiten scope geplaatst? Wat als de endpoint agent dit kan?

Antwoord:
Automatische response (SOAR-functionaliteit) is expliciet buiten scope geplaatst om de focus te houden op monitoring en detectie binnen de MDR-dienst. Indien een endpoint agent over automatische response beschikt, heeft dit geen invloed op de beoordeling van de inschrijving. Het gebruik van SOAR-functionaliteit mag dus worden toegepast, maar levert geen extra punten of voordeel op binnen deze aanbesteding.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
111

Onderwerp:
BD 7,4

Vraag:
4e alinea: AD stelt dat ‘alleen referentieopdrachten in aanmerking worden genomen die Inschrijver zelf heeft uitgevoerd (dus zonder tussenkomst van een onderaannemer)’. Vervolgens stelt AD in de 5e alinea: ‘Ervaring van een onderaannemer wordt door de VRT uitsluitend in aanmerking genomen indien bij Inschrijving wordt vermeld dat een beroep wordt gedaan op de ervaring van deze derde en wordt voldaan aan de overige voorwaarden van paragraaf 5.3.’

Inschrijver concludeert uit de combinatie en volgtijdelijkheid van bovenstaande citaten dat referentieopdrachten uitgevoerd door een onderaannemer door AD wel in aanmerking worden genomen, mits de inschrijver een beroep doet op de technische bekwaamheid van deze onderaannemer als derde. Kunt u dit bevestigen? Indien u dit niet kunt bevestigen kunt dan toelichten waarom u deze situatie niet accepteert?

Verder wordt in het tweede citaat nog verwezen naar voorwaarden in paragraaf 5.3. Deze paragraaf heeft echter alleen betrekking op inschrijven als Samenwerkingsverband. Kunt u aangeven welke overige voorwaarden hier worden bedoeld, betrekking hebben op de situatie dat inschrijver voor het voldoen aan de ervaringseis een beroep doet op een derde?

Antwoord:
E.e.a. is inderdaad onduidelijk geformuleerd;

Er kan wel degelijk gebruik worden gemaakt van de ervaring van een 'onderaannemer', deze 'onderaannemer' met specifieke ervaring zoals gevraagd in de geschiktheidseisen ('Eisen betreffende de Inschrijver') zal dan zelf ook 'Inschrijver' moeten zijn.

Indien gebruik wordt gemaakt van 'een derde' (mogelijke een 'onderaannemer') voor het aantonen dat voldaan wordt aan de

'geschiktheidseisen', middels referenties van die 'derde', dan dient te worden ingeschreven als een Samenwerkingsverband (Bijlage X invullen en ondertekenen). Deze derde dient dan ook een eigen UEA in te vullen, te ondertekenen en in te dienen; Inschrijver beschikt immers zelf niet over de gevraagde ervaring, maar het 'samenwerkingsverband' beschikt wel over de nodige ervaring.

Referentieopdrachten van een 'onderaannemer' mogen worden ingediend, enkel als deze 'onderaannemer' dan participeert in het Samenwerkingsverband en dus de verklaring Samenwerkingsverband (bijlage X) wordt ingevuld en door die derde een eigen UEA wordt ingediend.

De verwarring die mogelijk ontstaat: een 'onderaannemer' is geen 'derde', een 'derde' kan wel 'onderaannemer' zijn. Een 'onderaannemer' kan een deel van de opdracht gaan uitvoeren, een 'derde' participeert in de Inschrijving als Samenwerkingsverband.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
112

Onderwerp:
Logging volume

Vraag:
De kosten voor uitgaande dataopslag van 1TB zijn aanzienlijk. Is de opdrachtgever bereid om deze data – met een minimale retentieperiode – via een koppeling beschikbaar te stellen aan het SIEM van opdrachtnemer, waarbij de verdere retentie plaatsvindt binnen de eigen infrastructuur van de opdrachtgever?

Antwoord:
Nee.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
113

Onderwerp:
24/7 eyes on screen

Vraag:
De opdrachtgever heeft aangegeven behoefte te hebben aan 24/7 eyes on screen, ook wanneer dit afwijkt van gangbare adviezen. Is het toegestaan om deze continue monitoring in te richten met gespreide teams, waarbij het dagdeel wordt ingevuld door een Nederlands SOC en de avond- en nachturen door een ander, internationaal opererend team? Een voorbeeld van een dergelijke aanpak is het ‘follow-the-sun’-model.

Antwoord:
Ja dat mag. Zie ook antwoord op vraag 106.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
114

Onderwerp:
Bijlage 7A Al19

Vraag:
Inschrijver heeft de vraag gesteld (ref nr. 91 NVI 1): Kunt u aangeven hoeveel van elke alert momenteel (gemiddeld per maand) gemeld worden? Hierop is geantwoord dat deze informatie naar mening van Opdrachtgever

niet relevant is voor de aanbesteding.
Inschrijver verzoekt Opdrachtgever om deze vraag toch te beantwoorden omdat het antwoord wezenlijk inzage geeft in de te verwachten werkdruk en daarmee kosten. Dit is naar mening van Inschrijver van wezenlijk belang voor het bepalen van de pricing en dus relevant voor de aanbesteding.

Antwoord:
Het aantal alerts per maand varieert afhankelijk van de actuele dreigingssituatie en de ingestelde detectieregels.
De opdrachtgever acht het niet relevant om binnen deze aanbesteding exacte aantallen te delen, aangezien de dienst zodanig ingericht moet zijn dat zowel piek- als reguliere volumes adequaat verwerkt kunnen worden.

Daarbij geldt dat opdrachtgever en opdrachtnemer gezamenlijk moeten streven naar het minimaliseren van het aantal alerts, bijvoorbeeld door optimalisatie van detectieregels, het instellen van baselines en het reduceren van false positives.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
115

Onderwerp:
Beschrijvend document - Bijlage 7A Programma van Eisen / TE 9 / Pagina 49

Vraag:
In relatie tot TE 9: hoeveel ICT-medewerkers dienen toegang te krijgen tot het ticketsysteem?

Antwoord:
Ongeveer 10 personen.

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
116

Onderwerp:
NVI vraag 25, pagina 16

Vraag:
In de eerste NVI gaf de opdrachtgever aan dat Defender for Cloud en alle Defender XDR-modules inclusief EDR reeds zijn geïmplementeerd. Tevens werd in antwoord op vraag 25 aangegeven dat ook SentinelOne wordt gebruikt. Kunt u toelichten waarvoor SentinelOne momenteel wordt ingezet?

Antwoord:
Wordt gebruikt door de huidige dienstverlener.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
117

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Worden er op dit moment dreigingen in de OT/IoT-omgeving gedetecteerd? Zo ja, welke oplossing wordt hiervoor gebruikt? Indien dit niet het geval is, is de opdrachtgever voornemens om een beveiligingsoplossing voor OT/IoT aan te schaffen?

Antwoord:

Dreigingen in de OT/IoT-omgeving worden momenteel niet actief met een aparte oplossing gemonitord, maar wel passief gedetecteerd via Microsoft Defender, en de opdrachtgever is niet voornemens op korte termijn een specifieke OT/IoT-beveiligingsoplossing aan te schaffen, al wordt toekomstige uitbreiding niet uitgesloten.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
118

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Hoeveel van de in bijlage 7B beschreven use-cases zijn momenteel geïmplementeerd?

Antwoord:
Op dit moment zijn circa 10 van de in bijlage 7B beschreven use-cases operationeel geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
119

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Zijn er bestaande use-cases die overgenomen dienen te worden in de nieuwe situatie? Zo ja, hoeveel betreft dit er?

Antwoord:
Ja, er dienen bestaande use-cases te worden overgenomen. Het betreft ongeveer 10 kernscenario's, gericht op detectie van kritieke incidenten, loganalyse en responsacties.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
120

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Welk SIEM-systeem wordt momenteel door de opdrachtgever gebruikt?

Antwoord:
Dit is geen relevante informatie om een goede Inschrijving te kunnen doen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
121

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Worden deze firewalls gebruikt voor centrale internettoegang voor zowel LAN (IT) als IoT-netwerken? Zo niet, hoe wordt het internetverkeer vanuit LAN- en IoT-segmenten op de verschillende locaties gerouteerd?

Antwoord:
Ja.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
122

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Wordt het verkeer tussen systemen in LAN- en IoT-omgevingen altijd via deze firewalls gerouteerd?

Antwoord:
Ja.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 123

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Zijn de firewalls ingericht als centraal netwerkknooppunt, met zichtbaarheid over alle verkeersstromen binnen zowel IT- als IoT/OT-netwerken?

Antwoord:
Ja.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 124

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
De opdrachtgever gaf aan twee Palo Alto firewalls te gebruiken. Kunt u toelichten waar deze firewalls zijn geplaatst en of ze als stand-alone of in een cluster zijn geïmplementeerd?

Antwoord:
Zijn als Active-Passive Cluster, ieder één van datacenterlocaties

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:

Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 125

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Welk type VPN-netwerk wordt door de opdrachtgever gebruikt (bijvoorbeeld MPLS, IPsec-VPN)?

Antwoord:
IPsec-VPN

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 126

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Hoeveel netwerksegmenten (zowel LAN als IoT/OT) zijn er per locatie aanwezig?

Antwoord:
10, zie ook vraag 117

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
127

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Op hoeveel locaties zijn IoT-apparaten geïmplementeerd?

Antwoord:
32, zie ook vraag 117

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
128

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Hoeveel on-premises datacenters zijn er operationeel binnen de organisatie van de opdrachtgever?

Antwoord:
2

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
129

Onderwerp:
Beschrijvend document - 3.4 Voorwerp van de Opdracht (scope)

Vraag:
Kunt u aangeven hoeveel fysieke locaties de opdrachtgever momenteel in gebruik heeft?

Antwoord:
32

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
130

Onderwerp:
Overeenkomst Artikel 18

Vraag:
18.4 - De inhoud van de onder de Inkoopvoorwaarden gesloten Overeenkomst(en) als zodanig mag/mogen met andere gemeenten, aan gemeenten gelieerde rechtspersonen en gemeentelijke samenwerkingsverbanden worden gedeeld.

Inschrijver acht het in verband met de inschrijving c.q. overeenkomst opgenomen vertrouwelijke informatie ongewenst dat deze door de AD met de in dit artikel genoemde partijen kan worden geeld zonder dat hiervoor vooraf toestemming door de leverancier is gegeven. Is AD bereid dit aan te

passen?

Antwoord:
Niet Akkoord; AD is immers een gemeenschappelijke regeling van 14 Gemeenten.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
131

Onderwerp:
Overeenkomst Artiel 16

Vraag:
Inschrijver heeft kennisgenomen van de in de NVI I gegeven antwoorden van AD op de met betrekking tot dit artikel gestelde vragen/gedane voorstellen. Niettemin verzoekt Inschrijver AD dringend haar antwoord te heroverwegen en de aansprakelijkheid clausule aan te passen tot een meer marktconforme. Inschrijver stelt voor:
- De aansprakelijkheid voor direct schade per gebeurtenis te beperken tot maximaal de door AD aan leverancier betaalde bedragen in de periode van 12 maanden voorafgaande aan de schade toebrengende gebeurtenis;
- De totale aansprakelijkheid van leverancier voor directe schade onder de overeenkomst te maximeren tot tweemaal de opdrachtwaarde;
- De beperking van aansprakelijkheid geldt ook voor eventuele door leverancier onder de overeenkomst gegeven garanties en/of vrijwaringen
- De aansprakelijkheid van leverancier voor indirecte of gevolgschade uit te sluiten.
Is AD hiertoe bereid?

Antwoord:
AD blijft bij haar oorspronkelijke antwoord op vraag 83; de kern uit dit antwoord is en blijft: Er is wel degelijk sprake van limitering van de hoogte van aansprakelijkheid; Naast de limitering van de hoogte van de aansprakelijkheid in artikel 16.3 en 16.4 (GIBIT), sluit AD aan bij het systeem van het BW.

Anders dan dus wellicht zou worden gesteld is van een onbeperkte, ongelimiteerde, of niet-proportionele aansprakelijkheid geen sprake. Vandaar dat geleund wordt op het hiervoor al beschreven wettelijke stelsel bij de bepaling van de schadeomvang. In de aansprakelijkheidsclausule wordt onderscheid gemaakt tussen enerzijds persoons- en zaakschade en anderzijds overige schade. Het onderscheid tussen deze twee schadesoorten sluit aan bij verzekeringen die in de markt worden aangeboden.

Er wordt zodoende uitdrukkelijk ook geen onderscheid gemaakt tussen directe en indirecte schade. Dit onderscheid komt in de Nederlandse wet niet voor en het is (daarmee) vaak onduidelijk wat er precies met het onderscheid wordt bedoeld.

Bij onduidelijkheid is geen van de partijen gebaat.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
132

Onderwerp:
Overeenkomst Artikel 11

Vraag:
11.2 - De facturering van de vergoedingen vindt, tenzij anders overeengekomen, als volgt plaats. Van eenmalige vergoedingen is 30% eerst opeisbaar na integrale Acceptatie. Periodieke vergoedingen zijn bij vooruitbetaling verschuldigd, doch 30% van de vergoedingen is eerst opeisbaar na integrale Acceptatie. Voor Derdenprogrammatuur is 100% verschuldigd bij levering. Het bepaalde omtrent uitgestelde opeisbaarheid is niet van toepassing indien voor de ICT Prestatie geen Acceptatieprocedure wordt uitgevoerd. Voor de resterende 70% van de eenmalige en periodieke vergoedingen worden in de Overeenkomst afspraken gemaakt.

De vergoeding en de wijze van facturatie zijn opgenomen in de Inschrijving van Leverancier. Een en ander overeenkomstig het bepaalde in artikel 10 van de concept overeenkomst. Kan AD bevestigen dat dit correct is en het bepaalde in dit artikel, mede gelet op de bepaling in geval tegenstijdigheden

niet van toepassing is?

Antwoord:
De vergoeding is inderdaad opgenomen in de Inschrijving (Prijzenblad) van Leverancier.
De wijze van facturatie is opgenomen in art. 11 GIBIT-2023 en art. 10 van de Concept-Overeenkomst.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
133

Onderwerp:
Overeenkomst Arikel 4.2

Vraag:
4.2 - De volgende termijnen zijn – in afwijking van het vorige lid – in alle gevallen fataal:
i. een in de Overeenkomst of het Implementatieplan opgenomen specifieke einddatum voor de Implementatie (waarbij daarmee verband houdende tussentijdse opleverdata niet fataal zijn);
ii. indien het Overeengekomen gebruik omvat dat de Implementatie of de levering van Updates en/of Upgrades tijdig voor de inwerkingtreding van (een wijziging in) Wet- en regelgeving is afgerond: de ingangsdatum van die (gewijzigde) Wet- en regelgeving.

Inschrijver gaat er vanuit dat het antwoord dat AD heeft gegeven ten aanzien van artikel 4.1 ook geldt voor de in dit artikel opgenomen termijnen. Correct?

Antwoord:
Uiteraard; zie ook vraag en antwoord 90 (NVI-1).

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
134

Onderwerp:
7.3 - In navolging van artikel 35 GIBIT 2023 is de TPM-verklaring bijgesloten in de bijlage bij de Overeenkomst "Bijlage TPM verklaring bij Overeenkomst".

Vraag:
Bedoelt AD dat de TPM verklaring onderdeel is van de overeenkomst? Betekent dit dat het in artikel 35 GIBIT bepaalde met dit artikel wordt ‘overruled’ en niet meer van toepassing is? Graag vernemen wij van AD of het voorgaande juist is en zo niet hoe dit artikel moet worden geïnterpreteerd.

Antwoord:
De TPM verklaring is geen onderdeel van de Overeenkomst en Art. 35 GIBIT wordt niet overruled: er mag bij verificatie een TPM-verklaring of een Certificering worden aangereikt.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
135

Onderwerp:
5.2 - De Acceptatieprocedure verloopt conform het in nader overleg vast te stellen testprotocol.

Vraag:
Inschrijver gaat ervan uit dat het in dit artikel genoemde acceptatie-protocol na ondertekening van de overeenkomst tussen partijen gezamenlijk wordt

overeengekomen. Is dit een juiste aanname?

Antwoord:
Dat is juist.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
136

Onderwerp:
4.2 - De Implementatie dient uiterlijk op 30-01-2026 te zijn voltooid.

Vraag:
Inschrijver gaat ervan uit dat het in NVI I door de AD ten aanzien van artikel 4.1 van de GIBIT gegeven antwoord ook voor dit artikel van toepassing is. Is dit een juiste aanname?

Antwoord:
Zie vraag en antwoord 133.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
137

Onderwerp:
3.1 - De Overeenkomst treedt in werking op 3 november 2025.

Vraag:
In het beschrijvend document is opgenomen dat de overeenkomst als ingangsdatum 1 december 2025 heeft. Kan de AD aangeven hoe dit artikel moet worden gelezen in relatie tot het beschrijvend document?

Antwoord:
AD heeft in de huidige planning het voornemen om definitief te gunnen eind november 2025; de Overeenkomst kan dan in gaan op 1 december 2025; mits er geen obstakels in het gunningsproces ontstaan. Vanaf 'definitieve gunning' kunnen Opdrachtgever en Opdrachtnemer in goed overleg concreet starten met de uitvoer van de Opdracht.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
138

Onderwerp:
Algemeen

Vraag:
In de algemene praktijk blijkt vaak dat de beantwoording van vragen niet de complete duidelijkheid verschaft die door de vragensteller werd beoogd. Het is gebruikelijk dat in dergelijke gevallen verduidelijkingsvragen gesteld kunnen worden ook al voorziet de planning niet meer in een formele (verduidelijkings)vragenronde. Kunt u bevestigen dat u inschrijvers na publicatie van NvI 2 nog ruimte biedt tot het stellen van verduidelijkingsvragen? Indien dit niet het geval is, kunt u dit dan beargumenteren.

Antwoord:
NVI-2 is inderdaad bedoeld als verduidelijkingvragen-ronde n.a.v. de in NVI-1 gestelde vragen en antwoorden; AD is van mening dat na het beantwoorden van de vragen middels deze NVI-2 er voldoende mogelijkheid is geweest voor verduidelijking van de uitvraag en dat de Gegadigden over voldoende informatie beschikken om een kwalitatief goede Inschrijving te kunnen doen. Uiteraard zal na het 'voornemen tot gunning' tussen

Opdrachtgever en beoogd Opdrachtnemer een 'Verificatie' en (mogelijk na 'gunning') nog een 'finetuning' plaatsvinden op mogelijk dan nog aanwezige marginale onduidelijkheden.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
139

Onderwerp:
Prijzenblad

Vraag:
Rapportages zijn volgens onze aanpak inbegrepen in de maandelijkse MDR-dienstverlening en worden niet afzonderlijk geprijsd. In het prijzenblad wordt echter een aparte regel opgenomen voor “rapportages en compliance-ondersteuning”. Kunt u bevestigen dat inschrijvers in het prijzenblad een bedrag van €0 mogen opnemen voor deze post, indien rapportages en compliance-ondersteuning al zijn inbegrepen in de vaste maandelijkse dienstkosten?

Antwoord:
Ja, inschrijvers mogen in het prijzenblad een bedrag van €0 opnemen voor de post “rapportages en compliance-ondersteuning”, indien deze rapportages en compliance-ondersteuning al zijn inbegrepen in de vaste maandelijkse dienstkosten van de MDR-dienstverlening.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 140

Onderwerp:
Prijzenblad

Vraag:
Kunt u verduidelijken wat wordt bedoeld met het begrip “compliance-ondersteuning” zoals gebruikt het prijzenblad: Betreft dit ondersteuning bij normenkaders zoals BIO, NEN 7510 of ISO 27001 of gaat het om ondersteuning bij audits, logging-inzage of documentatie voor verantwoordingsdoeleinden?

Graag een toelichting zodat inschrijvers deze post correct kunnen interpreteren en uniform kunnen verwerken in hun inschrijving.

Antwoord:
Compliance-ondersteuning betreft zowel ondersteuning bij normenkaders (zoals BIO, NEN 7510, ISO 27001) als bij audits, logging-inzage en documentatie voor verantwoordingsdoeleinden.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. 141

Onderwerp:
NvI 1 beantwoording vraag 94

Vraag:
In vraag 94 bevestigt VRT dat IoT/OT binnen scope valt van de opdracht. Microsoft Defender for Endpoint (in combinatie met XDR) is in staat is om IoT/OT-apparaten via passieve netwerkmonitoring in ‘discovery only mode’ te detecteren. Dit vereist geen aanvullende licentie, maar voor aanvullende functionaliteit zoals:
- risicobeoordeling,
- gedragsanalyse,

- OT-protocol-inspectie,
- of actieve threat detection,
is Microsoft Defender for IoT licentiëring nodig. Deze wordt doorgaans gelicenseerd per locatie of per OT-sensor, en is dus afhankelijk van de aard en omvang van de OT-omgeving.

Wij stellen voor om deze aanvullende licentiebehoefte – indien van toepassing – na gunning gezamenlijk met VRT te beoordelen, zodat de omvang, inrichting en kosten in overleg kunnen worden vastgesteld. Kunt u hiermee akkoord gaan?
Als u hier niet mee akkoord kunt gaan dan ontvangen wij graag de volgende informatie ten behoeve van een correcte inschatting in deze fase:
- het aantal locaties waar OT-/IoT-apparatuur zich bevindt;
- en per locatie een indicatie van het aantal te monitoren apparaten of netwerksegmenten.

Antwoord:
Zie antwoord op vraag 117.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
142

Onderwerp:
NvI 1 beantwoording vraag 38

Vraag:
In de beantwoording van vraag 38 geeft VRT aan dat Microsoft Sentinel niet binnen de TCO valt. Tegelijkertijd is Sentinel door opdrachtnemer vereist als SIEM-oplossing, waarbij ingestuurde logbronnen automatisch Azure-opslagkosten genereren.
In vraag 5 wordt verwezen naar een uitgangspunt van 1 TB logging per maand ten behoeve van " licentiekosten". Kunt u bevestigen dat inschrijvers dit volume als bindend uitgangspunt mogen hanteren in hun prijsvoorstel, zodat er sprake is van een gelijk speelveld voor alle aanbieders die Microsoft Sentinel inzetten?

Daarnaast verzoeken wij om duidelijkheid over de volgende situatie:
Indien het logvolume in de praktijk hoger blijkt te zijn dan het genoemde uitgangspunt (bijvoorbeeld door groei in logbronnen of verkeerd ingeschatte omvang), mag de opdrachtnemer de meerkosten voor logopslag dan doorbelasten aan VRT?

Antwoord:
Ja, Indien het daadwerkelijke logvolume in de praktijk hoger blijkt te zijn dan dit uitgangspunt, mogen de meerkosten voor extra logopslag in overleg worden doorbelast aan VRT. Zie ook vraag 107.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
143

Onderwerp:
BD 9.1.2

Vraag:
In het beschrijvend document wordt bij de planning gevraagd om het opnemen van een datum voor het "uitvoeren en accepteren van data migratie". Aangezien er volgens onze informatie geen migratie plaatsvindt vanuit een bestaand SIEM/SOC-systeem, verzoeken wij om verduidelijking: Kunt u hiervoor aangeven of er sprake is van een daadwerkelijke datamigratie, en zo ja, welke data of componenten de VRT verwacht te migreren naar het nieuwe MDR-platform? Indien dit niet van toepassing is, stellen wij voor om deze eis te laten vervallen of te herformuleren in het kader van technische afstemming of acceptatie van initiële logconnecties.

Antwoord:
Er is geen sprake van een daadwerkelijke datamigratie vanuit een bestaand SIEM/SOC-systeem.

De vermelding in de planning is bedoeld om het moment van technische afstemming en acceptatie van initiële logconnecties vast te leggen.
Wel willen we voorkomen dat er gedurende de implementatie dubbele tooling of agents gelijktijdig op endpoints actief zijn, zodat performance en

stabiliteit gewaarborgd blijven.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
144

Onderwerp:
BD 9.1.1

Vraag:
In het kader van gunningscriterium K1 wordt een grote hoeveelheid inhoudelijke informatie gevraagd, waaronder een uitgebreide beschrijving van de dienst, implementatieaanpak, monitoring, rapportage, communicatie, kwaliteitsborging, risicobeheersing en testplan.
Bent u bereid het maximaal toegestane aantal pagina's voor K1 te verruimen van 8 naar 10 A4-pagina's (exclusief bijlagen), zodat inschrijvers deze onderdelen zorgvuldig en volledig kunnen uitwerken binnen de gevraagde structuur en begrijpelijkheid?

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.

Onderwerp:

145 BD 3.4.5

Vraag:
Kunt u aangeven welke Microsoft-licenties van toepassing zijn op de 557 Entra ID Guest Users die in paragraaf 3.4.5 worden genoemd en of deze gastgebruikers beschikken over beveiligingsfunctionaliteit (zoals Defender P1/P2 of Azure AD Premium)? Dienen inschrijvers deze accounts wel of niet mee te nemen in de dekking van de MDR-dienst?

Antwoord:
De 557 Entra ID Guest Users vallen onder onze Microsoft Entra ID P2-licentie en hebben daarmee toegang tot P2-functionaliteiten.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr. **Onderwerp:**
146 NvI 1 beantwoording vragen 20, 49-53 en 67

Vraag:
In het antwoord op vraag 67 bevestigt VRT dat de vijf genoemde logbronnen in scope zijn voor de opdracht. Aangezien deze scope direct van invloed is op de prijsstelling van de inschrijving, vragen wij het volgende ter verduidelijking:

- In de beantwoording van de vragen 49 t/m 53 worden meerdere Azure-resources benoemd. Kunt u bevestigen dat deze Azure-resources volledig binnen scope vallen van de opdracht, en dat elke inschrijver deze dient mee te nemen in de aangeboden functionaliteit en prijs?

- In paragraaf 3.4.4 van het beschrijvend document worden onder andere de Palo Alto firewalls en Aruba ClearPass genoemd als logbronnen die onder de scope vallen. In de beantwoording van vraag 20 wordt het uitlezen van deze netwerkcomponenten echter als optioneel bestempeld. Kunt u verduidelijkken of deze netwerkcomponenten (Palo Alto en ClearPass) wél of niet verplicht onderdeel uitmaken van de logscope en dat een inschrijver

dit in de prijs dient op te nemen?

Ter bevordering van een gelijke en transparante beoordeling stellen wij voor dat de volledige scope zoals beschreven in paragraaf 3.4.4 (functioneel) én paragraaf 3.4.5 (aantallen), aangevuld met de Azure-resources zoals benoemd in de beantwoording van vragen 49 t/m 53, geldt als bindende scope waarvoor een prijs opgenomen dient te worden. Kunt u dit bevestigen?

Antwoord:
De volgende logbronnen vallen expliciet binnen de scope van de initiële SIEM-implementatie en dienen derhalve onderdeel te zijn van de Inschrijving qua functionaliteit en prijs:

Microsoft Azure / Microsoft 365: Exchange Online, SharePoint, Teams, EntraID – inclusief gebruikersactiviteiten, authenticaties, configuratiewijzigingen en beleidsgebeurtenissen.

Microsoft Defender: Endpointbeveiligingsdata zoals malwaredetecties, verdachte processen en gedragsanalyses.

Palo Alto Firewalls: Netwerkverkeer, toegangsverzoeken, threat logs en configuratiewijzigingen.

Microsoft (Event)logs: Authenticatiepogingen, systeemgebeurtenissen, foutmeldingen en applicatiegedrag.

Aruba ClearPass: Authenticatie- en toegangslogs, RADIUS-verzoeken, policy-evaluaties en device profiling.

Deze bronnen zijn actief en beschikbaar binnen VRT en vormen het uitgangspunt voor de SIEM-dienstverlening.

Uitbreiding van deze logbronnen is mogelijk na gunning, maar AWS is niet aanwezig en valt dus buiten scope.

Zowel de Palo Alto firewalls als Aruba ClearPass zijn verplicht onderdeel van de logscope.

In paragraaf 3.4.4 van het beschrijvend document worden deze componenten expliciet genoemd als logbronnen die binnen scope vallen voor de initiële implementatie van de SIEM-oplossing.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
147

Onderwerp:
NVI vraag 3

Vraag:
Inschrijver stelt dat het budget niet toereikend is voor de gevraagde dienstverlening: SOC SIEM op IT, OT en IoT componenten inclusief NDR. Kunt u toelichten welke oplossing er op dit moment gebruikt wordt, zodat Inschrijver weet waarmee Aanbestedende Dienst de oplossing vergelijkt? Dit zorgt er tevens voor dat Inschrijver een oplossing biedt die hetzelde dan wel meer biedt dat de huidige situatie.

Antwoord:
Op dit moment is er geen specifieke NDR-oplossing geïmplementeerd binnen Veiligheidsregio Twente. Detectie en monitoring vinden plaats via een combinatie van SIEM/SOC-dienstverlening, waarbij logdata uit firewalls, endpoints en cloudplatforms (zoals Microsoft 365 en Defender for Endpoint) centraal worden verzameld en geanalyseerd.

Voor OT/IoT-componenten wordt passieve detectie toegepast via Microsoft Defender, maar er is geen actieve OT/IoT-beveiligingsoplossing operationeel.
De huidige inrichting is gebaseerd op het defense-in-depth-principe, waarbij technologie en mensen samenwerken om verdachte activiteiten te detecteren en erop te reageren.

Inschrijvers worden uitgenodigd om een voorstel te doen dat minimaal gelijkwaardig is aan deze situatie en waar mogelijk aanvullende functionaliteit biedt.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025

Ref.nr.
148

Onderwerp:
Beschrijvend document - Bijlage 7A TE13

Vraag:
Er wordt gevraagd om detectie van afwijkend netwerkverkeer. Dit komt eigenlijk neer op een verplichte NDR-component. Kunt u aangeven of deze aanname juist is? Zo ja, kunt u aangeven welke oplossing er op dit moment voor NDR (netwerk detectie en response) gebruikt wordt? Deze informatie is nodig om tot een goed vergelijkbaar voorstel te komen, zodat Veiligheidsregio Twente het best passende voorstel ontvangt.

Antwoord:
De aanname dat detectie van afwijkend netwerkverkeer automatisch een verplichte NDR-component impliceert, is onjuist. Firewall-logs en endpointgedrag leveren eveneens waardevolle input voor deze detectie en worden momenteel actief ingezet binnen Veiligheidsregio Twente. Er is geen specifieke NDR-oplossing geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 2

Percelen: P1 SIEM/SOC

Beantwoord op: 8 okt 2025