Algemene informatie

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

Toelichting:
Hierbij de 1ste Nota van Inlichtingen (NVI-1);
Aanbestedende dienst (AD) vertrouwt erop dat gegadigden hiermee over voldoende en duidelijke info beschikken om een goede Inschrijving te kunnen doen.
Mochten er naar aanleiding van de hierbij gegeven antwoorden toch nog vragen of onduidelijkheden zijn, dan kunnen deze vragen worden gesteld voor NVI-2. Desbetreffende vragen dienen uiterlijk 1 oktober a.s. vóór 8:30 uur te worden ingediend via de 'vraag-en-antwoord-module' van TenderNed; vragen op een andere wijze ingediend worden niet in behandeling genomen. AD doet hierbij het dringende verzoek om in deze module slecht 1 vraag per keer te stellen en om duidelijk aan te geven op welke 'vraag/antwoord' uit NVI-1 de nadere vraag voor NVI-2 betrekking heeft.
AD wenst u succes met het opstellen van uw Inschrijving.
Inschrijvingen dienen uiterlijk 27 oktober a.s. vóór 12:00 uur te worden ingediend via TenderNed.

Namens VRTwente,
Alfons Oosthof en Maarten Smelt

Vraag en antwoord

Ref.nr.	**Onderwerp:**
1	Aanbestedingsleidraad: OT

Vraag:
Wij maken uit uw aanvraag op dat zowel IT als OT binnen scope is. Kunt u duiden wat voor OT de VR in huis heeft?

Antwoord:
Zie vragen en antwoorden 94 en 98.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
2

Onderwerp:
Eyes on Screen

Vraag:
Gegadigde vraagt uw akkoord voor het invullen van de SOC dienstverlening buiten kantooruren door een consignatiedienst die automatisch wordt gealarmeerd en waarbij een gekwalificeerde medewerker binnen 15 minuten operationeel is om een relevante melding op te pakken.

Antwoord:
Niet akkoord. Als vitale organisatie eisen wij 24/7 actieve beschikbaarheid van SOC-dienstverlening. Een consignatie- of piketregeling buiten kantoortijden voldoet niet aan onze continuïteitseisen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
3

Onderwerp:
Budget

Vraag:
Gegadigde vraagt u het maximale jaarbudget te verhogen van € 75.000,- naar € 90.000,- per jaar, gaat u akkoord?

Antwoord:
Het gestelde maximale jaarbudget is op dit moment voor dergelijke diensten gebudgetteerd binnen de Aanbestedende dienst; dit is zo gesteld, mede op basis van de huidige kosten voor deze dienstverlening. Het staat Inschrijvers uiteraard vrij om in te schrijven boven het gestelde budgetplafond. Beschrijvend document par. 9.3.2. geeft dan ook aan dat Inschrijvingen met een hoger bedrag terzijde kunnen worden gelegd; M.a.w. Inschrijvingen met

een hoger bedrag zullen niet terzijde worden gelegd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
4

Onderwerp:
leidraad 9.3.2 budget

Vraag:
u geeft aan dat het jaarbudget voor de complete dienst beperkt is tot 75.000 eur, oftewel 6250eur per maand. kijkend naar de scope van de opdracht, de daarvoor benodigde licenties, de salariscomponent die gemoeid gaat met 24x7 eyes on screen en de verwachting rond rapportages en responstijden is dit niet toereikend om een kwalitatief hoogwaardige dienst aan te bieden. Kunt u uitleggen waarom u voor dit budgetplafond kiest en op grond waarvan u meent dat dit voldoende is voor een hoogwaardige SIEM/SOC dienst?

Antwoord:
Zie vraag en antwoord 3.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.

Onderwerp:

5 leidraad 9.3.2 budget

Vraag:
de licentiekosten zijn afhankelijk van de hoeveelheid log data die moet worden opgeslagen. Kunt u inzicht geven in de hoeveelheid data (in GB's) die momenteel worden gegenereerd en opgeslagen?

Antwoord:
Om een eerlijk vergelijk te kunnen maken tussen de verschillende aanbieders, dienen inschrijvers uit te gaan 1TB aan logging per maand.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. **Onderwerp:**
6 bijlage 7a - AL 13

Vraag:
kunt u bevestigen dat de audit uitsluitend betrekking heeft op het SOC van de gegadigde?

Antwoord:
Ja dat is juist.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
7

Onderwerp:
bijlage 7a - TE 07

Vraag:
kunt u een overzicht geven van de beschikbare netwerkcapaciteit op de LAN en WAN componenten van uw omgeving?

Antwoord:
Na opdracht wordt alle noodzakelijke informatie gedeeld. Er is voldoende capaciteit aanwezig.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
8

Onderwerp:
bijlage 7a - TE 10

Vraag:
is er reeds een bestaande escalatiematrix of is het ontwerpen en uitwerken van het proces onderdeel van de opdracht?

Antwoord:
Er is een bestaande escalatiematrix beschikbaar. Tijdens kantoortijden is de servicedesk bereikbaar en voor urgente meldingen is er een 24x7 een ICT medewerker beschikbaar (piket).

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
9

Onderwerp:
bijlage 7a - TE 17

Vraag:
kunt u toelichten hoe u dit in de praktijk ziet?

Antwoord:
In de praktijk zorgt de opdrachtnemer ervoor dat alle relevante log data, die door producten en diensten bij de opdrachtgever worden gegenereerd, worden opgenomen in de SOC-dienstverlening. Dit betreft niet alleen de reeds bekende en bestaande logresources die bij de opdrachtgever in gebruik zijn, maar ook eventuele extra logresources die tijdens de contractperiode beschikbaar komen of ontdekt worden.
Dit betekent: Inzicht en integratie van bestaande logresources: De opdrachtnemer maakt gebruik van de reeds beschikbare logbronnen en integreert deze in het monitoring- en detectieproces.Aanvullende logresources: Naast de generieke en bekende logdata zal de opdrachtnemer ook zoeken naar en waar mogelijk integreren van aanvullende logresources die op dit moment mogelijk nog niet zichtbaar zijn, maar die wel beschikbaar kunnen zijn binnen de infrastructuur van de opdrachtgever. Dit kan bijvoorbeeld het ontsluiten van log data zijn van toegangssystemen, OT-apparatuur, of andere gespecialiseerde systemen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
10

Onderwerp:
bijlage 7a - TE 23

Vraag:
beschikt u over een up to date CMDB die hiervoor kan worden gebruikt en verleent u toegang tot de user directory gegevens??

Antwoord:
Ja, er is een up-to-date CMDB. Zie ook vraag 101

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
11

Onderwerp:
Gunningscriterium K1

Vraag:
Vanaf bullet “Beschrijving van de voorgestelde projectorganisatie…” en daarna geeft u punten aan die naar onze mening thuishoren onder 9.1.2. Gunningscriterium K2. Ziet u dit ook? Zo niet, kunt u dan een toelichting geven in wat u in de beantwoording van deze punten wilt terugzien ten opzichte van het implementatieplan?

Antwoord:
AD accepteert een overlap / herhaling van elementen binnen de gunningscriteria K1 en K2. Beide gunningscriteria worden integraal beoordeeld door dezelfde beoordelaars. Zoals ook aangegeven bij beide gunningscriteria: ""Dit gunningscriterium is een functioneel gunningscriterium. Ter beoordeling van de wijze waarop de Inschrijver een SIEM-SOC dienst concreet gaat realiseren / implementeren wil de VRT daarom in ieder geval de bovengenoemde onderwerpen terugzien in Plan van aanpak / Beschrijving aangeboden dienst / Implementatieplan / Planning. De overige onderwerpen die de Inschrijver van belang acht om de VRT te laten zien waarop de Inschrijver een SIEM-SOC dienst concreet wenst te gaan realiseren / implementeren, laat de VRT over aan de eigen invulling en creativiteit van de Inschrijver. Dit houdt in dat deze onderwerpen nadrukkelijk geen afzonderlijke gunningscriteria zijn. De VRT beoordeelt Plan van aanpak / Beschrijving aangeboden dienst / Implementatieplan /

Planning integraal en beoordeelt
aldus integraal de mate waarin de Inschrijver een SIEM-SOC dienst concreet wenst te gaan realiseren / implementeren in de specifieke
situatie bij Opdrachtgever.
Uw Inschrijving op K1 en K2 wordt integraal beoordeeld; m.a.w. als er elementen dubbel worden beantwoord, wordt dit uiteraard niet dubbel beoordeeld.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
12

Onderwerp:
Betreft 9.1.1 Gunningscriterium K1

Vraag:
U vraagt inzage in de CV’s van in te zetten projectleider en inhoudsdeskundige. Dit is geen gangbare vraag in dit soort aanbestedingen en past ook niet in het door u gevraagde maximum aantal pagina’s. Wij werken met projectteams van senior, ervaren en gecertificeerde medewerkers, maar wij hebben geen CV’s die wij direct delen met onze klanten. Kunt u akkoord gaan om dit punt te schrappen?

Antwoord:
Akkoord; CV's en persoonlijke gegevens hoeven niet te worden aangeleverd en zullen niet inhoudelijk worden beoordeeld. AD vormt zich echter graag wel een beeld van de ervaring / kwalificaties van de diverse bij de opdracht betrokken functionarissen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 13

Onderwerp:
Bijlage 7A, AL7

Vraag:
Wij hebben een beschrijving hiervoor maar deze is alleen voor intern gebruik en kunnen wij niet delen met derden. Kunt u akkoord gaan met alleen het aantonen van de certificeringen ISO27001 en ISAE3402, waaruit blijkt dat wij dit uiteraard wel op orde hebben?

Antwoord:
De vraagstelling is onduidelijk in relatie tot Bijlage 7A, AL7; We gaan ervan uit dat u Bijlage 7A, AL1 bedoeld? ISO27001 certificering of gelijkwaardig wordt door Inschrijver verklaard door invullen en ondertekenen UEA; na voornemen tot gunning dient de bewijslast (certificaat) door de beoogd Opdrachtnemer te worden aangeleverd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. 14

Onderwerp:
Bijlage 7A, DI 1. en DI 4

Vraag:
Onze oplossing biedt u een 24/7 security monitoring inclusief detectie en response. Het SOC is tijdens kantooruren volledig bemenst. Buiten kantooruren werken we met een piketdienst welke direct acteert bij meldingen van het type high/critical. Wij hebben meerdere klanten in de kritieke infrastructuur die deze werkwijze zeer acceptabel vinden en waarbij hun digitale veiligheid op hoog niveau geborgd blijft, waarbij wij dit

tegelijkertijd tegen acceptabele kosten kunnen aanbieden. Kunt u zich vinden in onze werkwijze en de eis aanpassen?

Antwoord:
Zie vraag 2.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
15

Onderwerp:
Bijlage 7A, TE 8

Vraag:
Voor al onze klanten werken wij met een mailkoppeling. Kunt u zich erin vinden dat de basis functies gerealiseerd worden door middel van een mailkoppeling in plaats van via de API?

Antwoord:
Akkoord; Wij kunnen ons erin vinden dat de basisfunctionaliteiten worden gerealiseerd via een mailkoppeling in plaats van een directe API-integratie, mits dit op een gestructureerde en betrouwbare manier gebeurt. Een belangrijk aspect hierbij is dat het ticketnummer altijd in het onderwerpveld van de e-mail wordt opgenomen. Dit maakt het mogelijk om berichten automatisch te koppelen aan het juiste incident in ons systeem.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 16

Onderwerp:
Bijlage 7A, TE 10

Vraag:
Vraag 6: Bijlage 7A, TE 10:
Wij hanteren standaard voor al onze klanten, waarvan een aantal in de kritieke infrastructuur vallen, de volgende responsetijden bij een Critical Impact Melding:
Binnen kantoortijden: tijd tussen identificatie van een incident en telefonische melding aan de klant: > 15 min
Binnen kantoortijden: tijd tussen identificatie van een incident en initieel mitigatieadvies aan de klant (per mail of telefonisch): > 30 min
Buiten kantoortijden: tijd tussen identificatie van een incident en telefonische melding aan de klant: > 30 min
Buiten kantoortijden: tijd tussen identificatie van een incident en initieel mitigatieadvies aan de klant (per mail of telefonisch): > 60 min

Standaard hanteren wij de volgende responsetijd voor overige incidenten:
Binnen kantoortijden: tijd tussen identificatie van een incident en melding bij klant (per mail): > 1 uur
Binnen kantoortijden: tijd tussen identificatie van een incident en initieel mitigatieadvies aan de klant (per mail): > 2 uur

Op basis van onze ervaring is dit ruim voldoende om snel te reageren op incidenten, gedegen advies te geven en op tijd mitigerende maatregelen te kunnen nemen.
Kunt u akkoord gaan met deze responsetijden?

Antwoord:
Zie vraag en antwoord 74.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
17

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
TE25 Wat dient er op de X te staan? En betreft het hier usecases of dectectieregels?

Antwoord:
Zie vraag 73: "Usecases"

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
18

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
TE24/26 Dienen de kosten voor het ontwikkelen van organisatiespecifieke usecases als extra kosten in rekening worden gebracht of dient dit inclusief te zijn?

Antwoord:
Extra kosten.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
19

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
TE14 Worden hier de layers van het Purdue-model of het OSI-model bedoeld?

Antwoord:
OSI-Model

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
20

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
TE13/14/15 Naar mening van opdrachtnemer zijn deze use cases alleen goed te detecteren met netwerksensor functionaliteit. Dient deze technologie onderdeel te zijn van het voorstel? En is opdrachtgever zich bewust van de budgetaire consequenties hiervan?

Antwoord:
Opdrachtnemer mag deze optioneel aanbieden, maar wordt niet meegenomen in de beoordeling.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
21

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
TE1/2 Welke EDR tool wordt er op de servers (zowel Linux als Microsoft) gebruikt?

Antwoord:
Microsoft Defender (Linux, iOS en Windows)

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
22

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
DI 4 Waar kunnen we dit integraal ontwerp (en dus deze definities) vinden?

Antwoord:
Er is geen separaat document "integraal ontwerp" opgenomen in de

aanbestedingsstukken waarin de definities van SOC-niveaus 1, 2 en 3 zijn vastgelegd. In deze aanbesteding laten wij de nadere invulling en interpretatie van deze niveaus over aan de inschrijver, binnen algemeen geaccepteerde marktstandaarden. U wordt gevraagd deze definities en de wijze waarop u invulling geeft aan de personele bezetting te beschrijven in het plan van aanpak.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
23

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
AL17 Dit is niet zozeer de classificatie van de melding, maar meer de afmeldinformatie (eerder weet je immers niet of dit wordt gevolgd). Is het opdrachtnemer toegestaan de eigen classificatie te gebruiken?

Antwoord:
Akkoord, mits afgestemd met opdrachtgever.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
24

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
AL16 Is het niet logisch dat tijdens de transitieperiode gedurende enige tijd de dubbele monitoringssoftware wel aanwezig is? Anders zal baselining van de nieuwe situatie niet mogelijk zijn of worden opdrachtnemer gedwongen met dezelfde tooling te werken als de oude leverancier.

Antwoord:
Eis blijft staan, het onboarden van de systemen zal de oude client worden verwijdert en de nieuwe client, mits van toepassing worden geïnstalleerd. Ter aanvulling: deployment van software verloopt via MS Intune.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
25

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
AL16 Welke monitorings software wordt er door de huidige leverancier gebruikt?

Antwoord:
SentinelOne

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
26

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
AL13 Zou opdrachtgever er in willen toestemmen dat dit geen directe concurrent van opdrachtnemer betreft?

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
27

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
9.1 We zien 40 punten voor kwaliteit en 60 punten voor prijs. Doorgaans worden er meer punten voor kwaliteit gegeven dan voor prijs. Zou u willen toelichten waarom voor deze verhouding is gekozen?

Antwoord:
Voor deze Aanbesteding is gekozen voor een verhouding waarbij prijs zwaarder weegt dan kwaliteit; Aanbestedende dienst staat het vrij om de verhouding in te vullen zoals ze dit nuttig acht. De belangrijkste kwaliteitsaspecten zijn als minimumeisen reeds opgenomen in de

aanbestedingsdocumenten. Hierdoor is het onderscheidend vermogen op kwaliteit beperkt. Gezien het beschikbare budget en het feit dat wij als aanbestedende dienst verantwoordelijk omgaan met publieke middelen, vinden wij het belangrijk om prijs zwaarder te laten meewegen in de beoordeling. Daarnaast is het zo, dat de beoordeling van het onderdeel Prijs als relatieve beoordeling zal plaatsvinden en afhankelijk van de markt / Inschrijvers het ondenkbaar is dat een Inschrijver op dit onderdeel geen punten zal scoren.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
28

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
3.4.5 Wat is de geschatte logingest uit deze logbronnen?

Antwoord:
Zie vraag 5.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 29

Onderwerp:
Beschrijvend Document Publicatie EU Managed SIEM_SOC 2025 VRTwente

Vraag:
3.4.2 Is het mogelijk om gebruik te maken van de Sentinel omgeving in de Microsoft tenant van opdrachtgever om de SIEM functionaliteit in te vullen?

Antwoord:
Zie vraag 38.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 30

Onderwerp:
Programma van Eisen

Vraag:
AL 14. Opdrachtnemer gebruikt voor alarm escalaties (onversleutelde) e-mail. Kan opdrachtgever hiermee akkoord gaan?
AL 17. Opdrachtnemer gebruikt de volgende alarm classificaties:
- Actual threat
- False positive
- False negative
- Maintenance/changes
- Misconfiguration
- Allowlisted
- Red team/security-/pentest
- Correct trigger

Zijn dit acceptabele classificaties voor Opdrachtgever?
AL 19. Opdrachtnemer gebruikt de volgende prioritering van incidenten:
Hoog
• Urgentie: Onmiddellijke actie vereist.
• Beschrijving: Er is mogelijk kwaadaardig gedrag waargenomen of er is inbreuk gepleegd op een account of host.
Medium

• Urgentie: Snelle actie vereist.
• Beschrijving: Mogelijk kwaadaardig gedrag of indicatoren van kwaadaardig gedrag in het verleden dat niet direct aandacht vereist.
Laag
• Urgentie: Moet worden onderzocht, geen urgentie.
• Beschrijving: Er is verdacht gedrag gedetecteerd dat kan duiden op kwaadaardige activiteiten, maar het kan ook een verkeerde configuratie of goedaardige activiteit zijn.
Is dit een acceptabele prioritering voor opdrachtgever?
DI1. De monitoringoplossing van opdrachtnemer is actief 24 uur per dag, 7 dagen per week, 365 dagen per jaar. Tijdens reguliere kantoortijden worden alle typen beveiligingsincidenten geanalyseerd door ons Security Operations Center (SOC). Buiten kantoortijden worden high risk incidenten opgevolgd via een piketdienst van het SOC. We kunnen in overleg met de klant bepaalde alerts gedurende kantooruren een lagere kwalificatie laten genereren dan buiten kantooruren zodat alerts die binnen kantooruren bijvoorbeeld een "low" of "medium" classificatie zouden krijgen, buiten kantooruren een "high" alert geven. Gaat opdrachtgever akkoord met deze voorgestelde invulling van de monitoringdienst?
DI4. Opdrachtnemer werkt met een piketdienst waarbij analisten buiten kantoortijden zelfstandig incidenten onderzoeken. Al onze analisten worden opgeleid om ten alle tijden een volledige analyse te kunnen doen. Hierbij kunnen we echter niet garanderen dat er altijd minimaal 40% tier 2 analisten beschikbaar zijn. Gaat opdrachtgever akkoord met deze invulling?
TE9 & T12. Opdrachtnemer werkt met ServiceNow als ticketing systeem, waarbij de toegang is geregeld met een wachtwoord en MFA. SSO is hierbij geen mogelijkheid voor externen (zoals onze klanten). Gaat opdrachtgever akkoord met deze werkwijze?
TE10. Opdrachtnemer werkt met de volgende respons tijden voor escalaties:
- Hoge prioriteit: escalatie binnen 1 uur per email, binnen 15 minuten na escalatie telefonisch contact.
- Medium prioriteit: email escalatie binnen 4 uur.
- Lage prioriteit: email escalatie binnen 8 uur.
Zijn bovenstaande response tijden acceptabel voor Opdrachtgever?
TE 14. Opdrachtnemer biedt geen monitoring op traffic flooding/DOS aanvallen vanwege de beperkte mitigatiemogelijkheden. Is dot voor Opdrachtgever akkoord?
T21. Opdrachtnemer heeft geen specifieke alerting op onjuiste tijdsaanduidingen. Er zijn wel alarmen als er enige tijd geen logging binnen is in gekomen (per logbron) en als er vertragingen zitten in de keten (problemen bij Microsoft). Daarnaast houden we rekening met wat vertraging in onze use cases, doordat servers de data niet direct naar Sentinel doorsturen. In hoeverre is dit acceptabel voor Opdrachtgever?
TE 23. Opdrachtnemer geeft verbanden tussen security meldingen tekstueel weer. Wat verwacht opdrachtgever van een visuele weergave?
T28. Dreigingslandschappen zijn continu in beweging, Opdrachtnemer houdt zich dagelijks hiermee bezig en ontwikkelt waar nodig nieuwe use cases om hierop in te spelen. Opdrachtgever wordt van deze ontwikkelingen op de

hoogte gehouden o.a. middels de maandelijkse rapportage en eerder als dit relevant is, maar er worden geen maandelijkse voorstelmomenten gedaan. In de afgelopen 6 maanden zijn er 20 nieuwe use cases aan de baseline toegevoegd. Is deze werkwijze voor Opdrachtgever acceptabel?

Antwoord:
Allereerst wenst AD op te merken dat het stellen van meerdere vragen in één vraag inefficiënt en onduidelijk is. Verzoek is dan ook om in geval van NVI-2 slechts 1 vraag per keer te stellen in de 'vraag-antwoord-module' van TenderNed;

AL14 Akkoord,
AL 17 Akkoord, mits vooraf overleg zodat deze wel aan ge-eiste responsetijden voldoen
AL 19 Niet akkoord, opdrachtgever is van mening dat de genoemde urgentie goed is beschreven
DI. 1 Niet akkoord
DI4 Niet akkoord
TE9 & T12 Niet akkoord
TE10. Zie vraag 74
AL 14. Niet akkoord
TE21. Zie vraag 72
TE23: Relatie tussen incidenten/detectie dien eenvoudig zichtbaar te zijn.
TE. 28 Opdrachtnemer wil graag wel maandelijks overleg.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. **Onderwerp:**
31 9.3.2 Maximaal beschikbaar jaarbudget

Vraag:
In het geval dat het fictieve aantal van 100 uren meerwerk voor extra consultancy tijdens de overeenkomst wordt overschreden, kan het zijn dat het jaarbudget boven het maximum van € 75.000,-- uitkomt. Mag Inschrijver ervan uitgaan dat meerwerk dat boven de 100 uren uitkomt in rekening mag

wordt gebracht?

Antwoord:
De 100 uren extra consultancy uren meerwerk (P2) zijn als aantal fictief. Deze maken slechts deel uit van van de berekening om te komen tot de totaalprijs / jaarprijs over de jaren 2 t/m 4 en optiejaren 5 en 6 (Blauwe cel op Prijzenblad). Nogmaals: deze 100 uur zijn een fictieve inschatting om een objectief vergelijk te kunnen maken tussen Inschrijvers op het Uurtarief voor Consultancy bij meerwerk. Meerwerk mag in het algemeen (dus ook ook onder de fictief gestelde 100 uur) uiteraard na Opdracht vanuit Opdrachtgever, in rekening worden gebracht. Aanbestedende dienst wenst hiermee enkel een inzicht te krijgen in het uurtarief voor meerwerk. De fictieve 100 uur is dus geen integraal onderdeel van de uiteindelijke Opdracht.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
32

Onderwerp:
9.3.2 Maximaal beschikbaar jaarbudget - plafondbedrag

Vraag:
Inschrijver kan het maximaal beschikbaar jaarbudget van € 75.000,-- niet over de volle looptijd van 6 jaar verantwoorden. Kunt u het plafondbedrag derhalve verhogen naar € 90.000,--?

Antwoord:
Zie vraag en antwoord 3.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
33

Onderwerp:
Gunningscriterium K1 en K2

Vraag:
In Gunningscriterium K1 vraagt u in de laatste bullit en sub bullits (voorgestelde projectorganisatie) naar elementen die normaliter onderdeel zijn van het implementatieplan en beter passen bij K2 Implementatie. Omdat K1 en K2 een andere weging hebben is nu onduidelijk wat waar beschreven dient te worden. Bent u bereid dit aan te passen zodat het onderwerp projectorganisatie (laatste bullit) bij K2 beschreven moet worden?

Antwoord:
Zie vraag en antwoord 11.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
34

Onderwerp:
7.4 Referenties

Vraag:
Mag Inschrijver ook referenties aanleveren met vergelijkbare service en dienstverlening als onderhavige opdracht, maar buiten de (semi) overheid sector? Indien u niet akkoord gaat, graag uw motivatie.

Antwoord:
Referentie-eis wordt bijgesteld: zowel Publieke- als Private sector is akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
35

Onderwerp:
Prijzenblad

Vraag:
Opdrachtgever stelt een maximumbedrag van €75.000 per jaar beschikbaar. Hoe gaat Opdrachtgever om met een groei van te beschermen assets als gevolg van de groei van de organisatie, in relatie tot het gestelde maximumbedrag?

Antwoord:
In geval van aanzienlijke uitbreiding van de organisatie zal het beschikbare budget meegroeien.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
36

Onderwerp:
BD 3.1

Vraag:
Opdrachtgever spreekt over een landelijk SOC. Doelt Opdrachtgever hier op

een SOC gebaseerd in Nederland met Nederlandse voertaal?

Antwoord:
Nee, hiermee wordt het NIPV (=koepelorganisatie Veiligheidsregio's) - SOC bedoeld.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
37

Onderwerp:
BD 7a, AL 7

Vraag:
Kunt u bevestigen dat, op basis van de gestelde locatie-eis, het níet is toegestaan dat logdata, verwerking van gegevens, monitoring en response-activiteiten vanuit de EER worden doorgestuurd naar, of worden uitgevoerd vanuit, een SOC buiten de EER — ook niet indien er sprake is van een formele SOC-vertegenwoordiging binnen de EER?

Antwoord:
Zie vraag 93.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
38

Onderwerp:
BD 9.1.5

Vraag:
In paragraaf 9.1.5 wordt vermeld dat de aangeboden prijzen all-in zijn, inclusief benodigde licenties, opslagcapaciteit en dataverbruik. Kunt u expliciet bevestigen of de volgende kosten wél of géén onderdeel vormen van de TCO zoals opgenomen in het prijzenblad: Microsoft gebruikskosten van Microsoft Sentinel, waaronder opslag, data-ingestie en retentie.

Antwoord:
Sentinel is geen onderdeel van de TCO. Indien er bepaalde zaken binnen Sentinel aangezet moeten worden waarvoor opdrachtgever kosten zou moeten maken dient dit in uw Inschrijving duidelijk te worden en dient dit in overleg met Opdrachtgever te gaan. Opdrachtgever is voornemens geen uitbreiding op Sentinel te doen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
39

Onderwerp:
Bijlage 7a, TE9

Vraag:
Bij deze eis wordt gesteld dat alle ICT-medewerkers van de opdrachtgever toegang dienen te krijgen tot het ticketsysteem van de opdrachtnemer. Is het koppelen van de dienst aan het ticketsyeem van de opdrachtnemer een geaccepteerd alternatief? Dit is voor ons gebruikelijk. Kunt u bevestigen dat een dergelijke koppeling als gelijkwaardige invulling van de eis wordt geaccepteerd?

Antwoord:
Akkoord.

Fase:

Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
40

Onderwerp:
BD 3.4.5

Vraag:
Wij vernemen graag of Veiligheidsregio Twente voornemens is om de huidige F3-gebruikers op termijn (en zo ja welke termijn) te voorzien van een F5 en/of F5 Security Add-on

Antwoord:
Neen, vooralsnog is dit niet aan de orde.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
41

Onderwerp:
Algemeen

Vraag:
Kan veiligheidsregio Twente aangeven welke strategische IT- en security-roadmap relevant is voor de organisatie gedurende de contract periode.

Antwoord:

VRT heeft security hoog in het vaandel. Word niet in NVI behandeld en wordt na gunning kenbaar gemaakt.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
42

Onderwerp:
Algemeen

Vraag:
Kan Veiligheidsregio Twente specificeren welke rollen en functies vertegenwoordigd zijn in het beoordelingsteam?

Antwoord:
Informatiemanager, Specialist Informatiemanagement, en IT-Inkoper /Medewerker Informatievoorziening; onafhankelijk voorzitter: Strategisch Inkoper.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
43

Onderwerp:
Bijlage 7a, D17

Vraag:
Hier wordt gesteld dat de opdrachtgever proactief analyseert op afwijkingen in gedrag op zowel IT- als OT-componenten. Wij constateren echter dat niet wordt gespecificeerd welke OT-componenten hieronder worden verstaan. Kunt u aangeven op welke typen OT-omgevingen en -componenten dit concreet betrekking heeft en welke in scope zijn?

Antwoord:
Zie vragen en antwoorden 20, 94 en 98

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
44

Onderwerp:
BD 9.1.3

Vraag:
Voor Gunningscriterium K3: Service Level Agreement (SLA) wordt in de aanbestedingsstukken aangegeven dat de beantwoording maximaal 6 A4 mag beslaan. In de nadere tekst onder dit criterium wordt echter een maximum van 5 A4 genoemd. Kunt u bevestigen van welke omvang (5 of 6 A4) wij bij de beantwoording dienen uit te gaan?

Antwoord:
Hiervoor is voor Inschrijvers 6A4 beschikbaar.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. 45

Onderwerp:
BD 9.1.1 en 9.1.2

Vraag:
Wij constateren dat in de aanbestedingsstukken wordt verwezen naar “opleidingen” voor medewerkers en functioneel beheerders. In de context van een managed SIEM/SOC-dienstverlening is voor ons niet duidelijk welke verwachtingen hieraan verbonden zijn. Kunt u nader toelichten:
- Voor welke doelgroepen deze opleidingen bedoeld zijn;
- Welke kennis- en vaardigheidsniveaus beoogd worden;
- Hoe vaak en in welke vorm u deze opleidingen wenst (bijvoorbeeld klassikaal, e-learning, of awareness-campagnes);
- En of er specifieke certificeringen of toetsingsmomenten worden verwacht?

Antwoord:
De opleidingen zijn bedoeld voor medewerkers van de servicedesk en beheerders. Het betreft trainingen in het gebruik van de tooling die door de opdrachtnemer wordt geleverd en gebruikt voor monitoring en dienstverlening. De trainingen dienen aan te sluiten op de afgenomen diensten en tooling, met focus op praktisch gebruik; dit mag in de vorm van klassikale sessies, e-learning of workshops. Er worden geen formele certificeringen vereist, maar de opdrachtgever verwacht aantoonbare kennisoverdracht en gebruiksklaar opleiden van betrokken medewerkers.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. 46

Onderwerp:
BD 9.1.1

Vraag:

Voor Gunningscriterium K1: Plan van aanpak / beschrijving aangeboden dienst geldt als voorwaarde dat de beantwoording maximaal 5 A4 mag beslaan. Gezien de omvang en detailrijkheid van de gevraagde onderwerpen achten wij dit ambitieus. Om de beantwoording zo volledig en transparant mogelijk te houden, stellen wij voor om de gevraagde cv's van de medewerkers binnen de projectorganisatie, het testplan, voorbeeld rapportages en het communicatieplan als afzonderlijke bijlagen op te nemen. Gaat Veiligheidsregio Twente akkoord met dit voorstel?

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
47

Onderwerp:
BD 3.4.4

Vraag:
Hoe beheert veiligheidsregio Twente op dit moment haar gebruikersidentiteiten (bijvoorbeeld volledig in Entra ID, in combinatie met on-premises AD), en over hoeveel identiteiten gaat het in totaal?

Antwoord:
Beheer gaat middels IAM software, die heeft een koppeling met HR systeem. On-premises AD in combinatie met EntraID. Zie 3.4.5 Beschrijvend Document.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
48

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal Kubernetes-clusters binnen uw Azure/AWS-omgeving

Antwoord:
Geen Kubernets clusters aanwezig.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
49

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal databases binnen uw Azure/AWS-omgeving

Antwoord:
40

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
50

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal app services binnen uw Azure/AWS-omgeving

Antwoord:
20

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
51

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal opslagaccounts binnen uw Azure/AWS-landingszone?

Antwoord:
15

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
52

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal keyvaults binnen uw Azure/AWS-landingszone?

Antwoord:
2

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
53

Onderwerp:
BD 3.4.4

Vraag:
Indien van toepassing, kunt u ons inzicht geven in het aantal abonnementen binnen uw Azure/AWS-landingszone?

Antwoord:
1 subscription; Wel 2 Tenants

Fase:

Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
54

Onderwerp:
BD 3.4.4

Vraag:
Op welke landingszone worden de core business applicaties van uw organisatie ingezet? Is dit Azure, AWS, On-Prem?

Antwoord:
Combinatie Azure en on-prem. AD maakt geen gebruik van AWS.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
55

Onderwerp:
BD 3.4.4

Vraag:
Met betrekking tot de Aruba- en Palo Alto-infrastructuurcomponenten: kunt u aangeven hoeveel managementconsoles momenteel actief worden gebruikt voor het beheer, en om welke specifieke oplossingen het daarbij gaat?

Antwoord:

Aruba central; voor beheer Aruba Infra. 2 x Palo Alto Firewall.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
56

Onderwerp:
BD 3.4.4

Vraag:
Wil uw organisatie gebruik maken van onze expertise om de verschillende Defender producten te implementeren?
(Indien nog niet geïmplementeerd natuurlijk)

Antwoord:
Nee, Defender is reeds geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
57

Onderwerp:
BD 3.4.4

Vraag:
Is Microsoft Defender for Cloud Apps (MDCA) geïmplementeerd? Zo niet,

staat dit op de agenda/roadmap?

Antwoord:
Ja, is reeds geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
58

Onderwerp:
BD 3.4.4

Vraag:
Is Microsoft Defender for Cloud (MDC) geïmplementeerd? Zo niet, staat dit op de agenda/roadmap?

Antwoord:
Ja, is reeds geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
59

Onderwerp:
BD 3.4.4

Vraag:
Is Microsoft Defender voor Office 365 (MDO) geïmplementeerd? Zo niet, staat dit op de agenda/roadmap?

Antwoord:
Ja, is reeds geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 60

Onderwerp:
BD 3.4.4

Vraag:
Is Microsoft Defender for Identity (MDI) geïmplementeerd? Zo niet, staat dit op een agenda/roadmap?

Antwoord:
Ja, is reeds geïmplementeerd.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.

Onderwerp:

61 BD 3.4.4

Vraag:
Wij constateren dat in deze paragraaf verschillende Microsoft-technologieën worden genoemd. Om ons voorstel zo goed mogelijk te laten aansluiten bij de strategische uitgangspunten van Veiligheidsregio Twente, vernemen wij graag in welke mate er sprake is van een Microsoft-first strategie en hoe dit van invloed is op de selectie van oplossingen en leveranciers.

Antwoord:
AD is gestandaardiseerd op Microsoft, maar heeft geen Microsoft-first strategie.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. **Onderwerp:**
62 Beschrijvend document (BD) 2.4

Vraag:
De opdrachtgever geeft aan dat er reeds een SIEM/SOC-dienstverlening actief is. In Gunningscriterium K2: Implementatieplan / planning wordt uitsluitend gevraagd om een implementatieplan. Een eventuele migratie van bestaande tooling en data wordt in dit criterium niet benoemd. Is een migratie van bestaande tooling en data zoals usecases, playbooks ook onderdeel hiervan?

Antwoord:
Nee, dit is geen onderdeel.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
63

Onderwerp:
Beschrijvend Document, Aanleiding, beschrijving huidige situatie (par 3.1 p. 7)

Vraag:
Er wordt aangegeven dat het NIPV werkt aan een gezamenlijke SOC-oplossing die pas medio 2026 aanbesteed wordt. Verwacht de VRT dat de hier te gunnen oplossing tijdelijk wordt ingezet tot het landelijke SOC beschikbaar is, of gaat VRT uit van volledige benutting van de contractlooptijd (4+2 jaar)?

Antwoord:
Zie Bijlage 2A Concept-Overeenkomst: Art. 3 Overeenkomst wordt gesloten voor de periode van 4 jaar en kent 2 x de optie om met 1 jaar te verlengen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
64

Onderwerp:
Beschrijvend Document, Gewenste situatie (par 3.3 p.7)

Vraag:
In paragraaf 3.3 wordt een maximaal jaarbudget van €75.000 excl. BTW genoemd. Kan VRT aangeven of dit budget geldt voor de som van de opgegeven eenmalige en maandelijkse kosten, of alleen voor de structurele (maandelijkse) kosten?

Antwoord:
Zie de blauwe cellen op het Prijzenblad en zie ook vraag en antwoord 3 en 31.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 65

Onderwerp:
Beschrijvend Document, Bijlage 10 Prijzenblad SIEM_SOC

Vraag:
Na bestudering van de kostencomponenten in Bijlage 10 (Prijzeninvulblad) komt Inschrijver tot de conclusie dat het genoemde jaarbudget van € 75.000, -- (excl. btw) mogelijk niet toereikend is om de gevraagde dienstverlening volledig te dekken, zeker indien zowel de eenmalige als de maandelijks terugkerende kosten hieronder moeten vallen. Is de Aanbestedende Dienst bereid het jaarbudget te verhogen naar € 100.000, -- (excl. btw)?

Antwoord:
Zie vraag en antwoord 3.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.

Onderwerp:

66 Beschrijvend Document, Bijlage 10-Prijzenblad SIEM_SOC

Vraag:
Het prijzenblad vermeldt geen indexatieclausule. Wordt prijsindexatie gedurende de looptijd (4+2 jaar) toegestaan, en zo ja, volgens welke index (bijvoorbeeld CBS Dienstprijzenindex (DPI)?

Antwoord:
Zie Bijlage 2 A, Concept- Overeenkomst: artikel 10.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. **Onderwerp:**
67 Beschrijvend Document, Scope logbronnen (par. 3.4.4, p. 9)

Vraag:
Kan Inschrijver er vanuit gaan dat de genoemde logbronnen (Azure/M365, Defender, Palo Alto firewalls, Windows Eventlogs, Aruba ClearPass) volledig zijn voor de initiële implementatie? Of wordt van de opdrachtnemer verwacht om ook aanvullende logbronnen te identificeren en te integreren? Is er een lokale log-structuur beschikbaar waar alle logging centraal binnenkomt?

Antwoord:
De inschrijver kan er van uitgaan dat de genoemde logsources in basis voldoende zijn om de initiële implementatie te kunnen uitvoeren. Opdrachtgever verwacht wel van inschrijver om actief mee te denken over aanvullende logbronnen die mogelijk van belang kunnen zijn. Er is geen lokale log-structuur beschikbaar.

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
68

Onderwerp:
Beschrijvend Document, Uitgangssituatie licenties, werkplekken, servers en gebruikers (par. 3.4.5 p. 9-10)

Vraag:
In paragraaf 3.4.5 (p. 9-10) wordt vermeld dat de VRT beschikt over 645 M365 F3-licenties. Kan VRT bevestigen of deze gebruikers ook beschikken over een Microsoft F5 security add-on (zoals Defender for Identity, Defender for Endpoint P2, Cloud App Security), of dat dit niet het geval is?

Antwoord:
Dit is niet het geval.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
69

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eis AL 22)

Vraag:
De eis AL 19 beschrijft de gevraagde responsetijden op incidenten. De eis TE 10 beschrijft de communicatievorm waarover incidenten gemeld dienen te worden (telefonisch or per e-mail). Eis TE 10 noemt echter ook responsetijden, maar deze wijken af van de tijden onder AL 19. Kunnen wij AL 19 opvatten als geldende eis voor responsetijden en TE 10 als geldende eis voor communicatiemedia, en daarmee de responsetijden uit TE 10

loslaten?

Antwoord:
Zie vraag en antwoord 74.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
70

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eisen DI 7, TE 14 t/m 16)

Vraag:
In de eisen DI 7 en TE 14 t/m 16 wordt gesproken over de OT-infrastructuur en het OT-landschap van opdrachtgever. Valt het monitoren van OT binnen scope, en moeten wij dit zien als uitbreiding van de scope beschreven in paragraaf 3.4.4 (Huidige logbronnen)? Kunt u de OT-infrastructuur nader beschrijven, zodat wij de aangeboden oplossing daarop kunnen toesnijden?

Antwoord:
Zie vraag en antwoord 98.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 71

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eis TE 17)

Vraag:
Kunt u bevestigen dat paragraaf 3.4.4 (Huidige logbronnen) alle producten en diensten beschrijft waarvan in eis TE 17 wordt gevraagd aan te geven in hoeverre deze in de SOC/SIEM dienstverlening zijn op te nemen?

Antwoord:
Dat is juist; hierbij de bevestiging.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. 72

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eis TE 21)

Vraag:
De eis stelt: “Log- en eventdata met een onjuiste tijdsaanduiding moet worden gesignaleerd als incident.” Kunt u beschrijven welke vormen van onjuistheid u verwacht in tijdsaanduidingen en welk doel het signaleren daarvan als incident dient, zodat wij beter in staat zijn te beschrijven hoe onze oplossing aan uw behoeften voldoet?

Antwoord:
Onjuistheden in tijdsaanduidingen betreffen bijvoorbeeld afwijkingen van de systeemklok, ontbrekende tijdstempels of een onlogische volgorde in logs. Er moet een logische tijdsvolgorde zijn; afwijkingen kunnen duiden op logmanipulatie of synchronisatieproblemen. Daarom moet dit als incident worden gesignaleerd.

Fase:
Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
73

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eis TE 25)

Vraag:
De eis stelt: “De SOC-dienst moet aantoonbaar in staat zijn om ten minste X vooraf opgestelde use cases te implementeren en onderhouden.” Kunt u een indicatie geven van de waarde van “X”?

Antwoord:
Zie bijlage 7B. Correctie van de eis: De SOC-dienst moet aantoonbaar in staat zijn om ten minste 17 vooraf opgestelde use cases te implementeren en onderhouden.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
74

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eisen AL 19)

Vraag:
In de eis ‘AL 19’ stelt u de volgende richtlijn voor de Time to Respond:
• Critical (P1): 20 minuten
• High (P2): 1 uur
• Medium (P3): 4 uur
• Low (P4): 16 uur

Deze normering is aanzienlijk strenger dan de richtlijnen die gelden bij andere veiligheidsregio's waar Inschrijver actief is. Daar wordt het volgende gehanteerd:
• Critical (P1): 30 minuten binnen kantoortijd en 1 uur buiten kantoortijd
• High (P2): 2 uur
• Medium (P3): 8 uur
• Low (P4): 24 uur

Is de Aanbestedende Dienst bereid deze richtlijn te hanteren voor de Time to Respond? Onder Time to Respond wordt hier verstaan: de tijd tussen het starten van het actieve onderzoek naar het incident en het nemen van de eerste risicobeperkende maatregelen.

Antwoord:
Opdrachtgever herformuleert de volgende eisen Al. 19 en TE. 10.
TE.10
De opdrachtnemer dient een alarmeringsmechanisme te implementeren dat meldingen afhandelt op basis van hun impactniveau. Het mechanisme moet voldoen aan de volgende specifieke en meetbare eisen:
1. Critical Impact Meldingen:
Telefonisch contact: De opdrachtnemer dient binnen 30 minuten na detectie van een critical impact melding telefonisch contact op te nemen met de aangewezen contactpersonen volgens de escalatiematrix.
E-mail: Daarnaast dient er binnen 30 minuten een e-mail te worden verzonden naar de relevante contactpersonen.
2. High Impact Meldingen:
Telefonisch contact: Bij meldingen met een high impactniveau dient de opdrachtnemer binnen 60 minuten na detectie telefonisch contact op te nemen met de aangewezen contactpersonen volgens de escalatiematrix.
E-mail: Daarnaast dient er binnen 60 minuten een e-mail te worden verzonden naar de relevante contactpersonen.
3. Medium Impact Meldingen:
E-mail: Bij meldingen met een medium impactniveau dient de opdrachtnemer binnen 4 uur na detectie een e-mail te verzenden naar de relevante contactpersonen.
4. Low Impact Meldingen:
E-mail: Bij meldingen met een low impactniveau dient de opdrachtnemer binnen 16 uur na detectie een e-mail te verzenden naar de relevante contactpersonen.

AL. 19
Opdrachtnemer draagt zorg voor een tijdige prioritering van- en respons op-security incidenten door melding aan de Opdrachtgever. Hierbij voldoet Opdrachtnemer aan de volgende richtlijn: Time to respond:
• Critical (P1). - 30 min
• High (P2) – 60 minuten
• Medium (P3) – 4 uur
• Low (P4). – 16 uur

Onder time to respond wordt hier verstaan: de maximale tijd tussen het (automatisch) genereren van een alarm, en het melden van een (mogelijk) incident bij de Opdrachtgever.
Opdrachtgever staat open om de tijden samen met opdrachtnemer voor de medium en low meldingen nog te kunnen wijzigen indien noodzakelijk.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
75

Onderwerp:
Beschrijvend Document

Vraag:
In punt 4.15 wordt aangegeven dat alle corresspondentie en in te dienen stukken in de Nederlandse taal dienen te worden opgesteld. In Bijlage 7 punt AL2 staat dat alle documentatie en correspondentie tijden de uitvoering van het contract zowel in de Nederlandse als de Engelse taal dient plaats te vinden.

Voor deze uitvraag werken wij nauw samen met een gespecialiseerde vendor van MDR software. Al hun bedrijfscommunicatie alsmede hun SOC is volledig Engelstalig in uitvoering. Dat betekent dat specifieke documenten zoals een Service Agreement, DAP of implementatieplan in het Engels wordt opgesteld. Kan het VRT aangeven of dat acceptabel is. Zonee, kan het VRT onderbouwen waarom specifieke documenten in de Nederlandse taal opgesteld dienen te zijn?

Antwoord:
Technische documentatie mag in de Engelse taal worden aangeleverd. SLA, DAP en het implementatieplan dienen echter in het Nederlands te worden opgesteld, omdat deze documenten richtinggevend zijn voor de uitvoering van het contract, toezicht en verantwoording, en voor alle betrokkenen – inclusief niet-technische stakeholders – begrijpelijk en juridisch eenduidig moeten zijn.

Fase:

Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
76

Onderwerp:
Bijlage 2A - Art. 12 – Data

Vraag:
Dit artikel stelt als voorwaarde dat alle data kosteloos beschikbaar moet zijn, inclusief documentatie en IE-rechten bij Opdrachtgever. Opdrachtgever is eigenaar data en Leverancier behoudt rechten op methodieken/tools. Leverancier acht het redelijk om voor het verstrekken van data een redelijke vergoeding aan Leverancier te mogen vragen op basis van vooraf overeengekomen tarieven. Kan Opdrachtgever hiermee instemmen? Zo nee, waarom niet?

Antwoord:
Akkoord; Als Inschrijver hiervoor kosten rekent, dienen deze eventuele kosten integraal te worden verwerkt in zijn Inschrijving en in de TCO.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
77

Onderwerp:
Bijlage 2A - Art. 11 – Contactpersonen

Vraag:

Contactpersonen mogen niet per se bindende afspraken maken; dit geeft het risico op onbedoelde verplichtingen. Beperken bevoegdheid contactpersonen tot operationele afspraken, geen contractwijzigingen acht Leverancier redelijk. Kunt u akkoord gaan met aanpassing van het artikel alszodanig? Zo nee, waarom niet?

Antwoord:
Niet akkoord; binnen AD hebben contracteigenaar / contractbeheerder in de rol van contactpersoon de bevoegdheid om in afstemming met Opdrachtnemer bindende afspraken te maken; dit zijn inderdaad wederzijdse verplichtingen. Contactpersoon Opdrachtnemer kan uiteraard dergelijke afspraken eerst intern bij Opdrachtnemer voorleggen, alvorens afspraak bindend wordt. Er kan nimmer sprake zijn van afspraken die mogelijk leiden tot een 'wezenlijke wijziging'.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
78

Onderwerp:
Bijlage 2A - Art. 10.3 – Vergoedingen Exit-plan

Vraag:
Ten tijde van het aangaan van de Overeenkomst is niet vast te stellen wat de situatie is bij einde Overeenkomst. Deze situatie - bij einde Overeenkomst - dient leidend te zijn voor het uiteindelijk op te stellen Exitplan. Daarbij dienen partijen tevens de omvang van de verschuldigde exitvergoeding overeen te komen. Deze is ten tijde van het aangaan van de Overeenkomst niet bekend. Leverancier stelt voor het artikel alszodanig aan te passen. Kunt u daarmee akkoord gaan? Zo nee, waarom niet?

Antwoord:
AD is van mening dat Opdrachtnemer als ervaren en gespecialiseerd dienstverlener goed zou moeten kunnen calculeren wat eventuele kosten voor een voorgestelde Exit strategie (Gunningscriterium K4) / Exit plan zullen zijn; deze kosten zijn vervolgens goed te verdisconteren in de

Inschrijving.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
79

Onderwerp:
Bijlage 2a - Art. 8 – Exit-plan

Vraag:
Levernacier hanteert voor haar klanten een Exitstrategie. Deze is leidend voor het uiteindelijk op te stellen Exitplan. Reden hiervoor is gelegen in het feit dat ten tijde van het aangaan van de Overeenkomst niet vast te stellen is wat de situatie is bij einde Overeenkomst. Deze situatie - bij einde Overeenkomst - dient leidend te zijn voor het uiteindelijk op te stellen Exitplan. De uitgangspunten voor het op te stellen Exitplan worden beschreven in de Exitstrategie. Kan Opdrachtgever hiermee akkoord gaan? Zo nee, waarom niet?

Antwoord:
Zie vraag en antwoord 78.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.

Onderwerp:

80 Bijlage 2a - Art. 1 – Voorwerp van de Overeenkomst

Vraag:
Alle aanbestedingsdocumenten maken integraal deel uit en hiërarchie legt Inschrijving Leverancier laag in derangorde. Dit vergroot de kans op tegenstrijdige verplichtingen.Voorstel: hiërarchie aanpassen zodat Inschrijving gelijkwaardig of hoger is dan GIBIT. Kunt u daarmee akkoord gaan?

Antwoord:
Niet akkoord; als de rangorde wordt gewijzigd, is er even zo goed een risico op 'tegenstrijdige verplichtingen'; deze worden juist geëlimineerd door voor het aangaan van de overeenkomst een rangorde te bepalen.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. **Onderwerp:**
81 Inkoopvoorwaarden GIBIT 17.2

Vraag:
Ten behoeve van de uitoefening van zijn bedrijf heeft leverancier verzekeringen uitgenomen op condities die voor zijn bedrijf te doen gebruikelijk zijn. Leverancier zal deze verzekeringen ten behoeve van deze overeenkomst in stand houden. De dekking van de verzekeringen is echter gebaseerd op de bedragen zoals geformuleerd bij de vragen/tekstvoorstellen bij artikel 5 1
13.2 t/m 13.5. Wij gaan ervan uit dat wij hiermee kunnen volstaan. Klopt deze aanname?

Antwoord:
AD begrijpt de strekking van deze vraag niet; er is immers binnen de GIBIT geen artikel 5 1; art. 13.2 t/m 13.5 heeft betrekking op Algoritmische toepassingen. Graag uw vraag specifieker formuleren t.b.v. NVI-2.

Fase:

Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
82

Onderwerp:
Inkoopvoorwaarden GIBIT 17.1

Vraag:
Ten behoeve van de uitoefening van zijn bedrijf heeft leverancier verzekeringen uitgenomen op condities die voor zijn bedrijf te doen gebruikelijk zijn. Leverancier zal deze verzekeringen ten behoeve van deze overeenkomst in stand houden. De dekking van deze verzekeringen is echter gebaseerd op de bedragen zoals geformuleerd bij de vragen/tekstvoorstellen bij artikel 13.2 t/m 13.5. Bent u bereid hiermee in te stemmen?

Antwoord:
Zie vraag en antwoord 81.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
83

Onderwerp:
Inkoopvoorwaarden GIBIT 16.6

Vraag:
Het is leverancier niet toegestaan onbeperkte aansprakelijkheid voor schade

te aanvaarden. Leverancier ziet graag dat de bepalingen onder i), iii) en iv) ook onder de aansprakelijkheidsbeperking van artikel 13.3 en 13.4 vallen. Bent u hiertoe bereid? Tekstvoorstel: De in dit artikel bedoelde beperking van aansprakelijkheid komt te vervallen indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel.

Antwoord:
Niet akkoord: Dit is zeker geen beroep op onbeperkte aansprakelijkheid; Gebreken in Prestaties kunnen tot grote, vaak moeilijk op voorhand te overziene consequenties in de vorm van (gevolg)schades leiden. Teneinde de daaruit voor de markt voortvloeiende risico's beheersbaar en daarmee verzekerbaar te houden, is afgezien van toepassing van het in beginsel onbeperkte wettelijke aansprakelijkheidsregime. In plaats daarvan is gekozen voor een regeling waarbij onderscheid wordt gemaakt tussen persoons- en zaakschade alsmede daaruit voortvloeiende schade (de zogenoemde indirecte of gevolgschade) en overige schade. Voor persoons- en zaakschade en daaruit voortvloeiende schade, welke schades doorgaans vallen onder de dekking van een aansprakelijkheidsverzekering bedrijven (AVB), is aansluiting gezocht bij het daarvoor gebruikelijk in de IT-markt verzekerde bedragen.
De opgenomen uitzondering met betrekking op schade als gevolg van het schenden van wet- en regelgeving op het terrein van het beschermen van persoonsgegevens; Het beschermen van natuurlijke personen bij het verwerken van persoonsgegevens is een grondrecht. Schending van dit grondrecht kan leiden tot ernstige schade bij natuurlijke personen.
Door snelle technologische ontwikkelingen en globalisering zijn de afgelopen periode nieuwe uitdagingen voor het beschermen van persoonsgegevens ontstaan. Met de Europese AVG is in 2018 een krachtiger beschermingsregime geïntroduceerd.
De bescherming van persoonsgegevens heeft geleid tot een substantiële toename van de financiële risico's van het verwerken van persoonsgegevens. Voor het verdelen van aansprakelijkheid voor privacy schendingen is in de GIBIT aansluiting gezocht bij de aansprakelijkheidsverdeling in de AVG. Maximeren van aansprakelijkheid zou afbreuk doen aan het met de AVG beoogde doeltreffende, evenredige en afschrikkende sanctioneren van onrechtmatige verwerking van persoonsgegevens. Mede daarom is in art. 16.5 (GIBIT) bepaalt dat de in art. 16.3 en 16.4 (GIBIT) opgenomen beperkingen van aansprakelijkheid komen te vervallen bij schade door privacy schending.
Beide partijen dienen zich tevens te realiseren dat naast de bepalingen in de GIBIT, het Burgerlijk Wetboek (en andere relevante wetgeving) onverkort van toepassing is, tenzij daar in de GIBIT uitdrukkelijk van is afgeweken. Dit houdt o.m. in dat de regels uit boek 6 titel 1 afdeling 10 van toepassing zijn, waaronder begrepen de daarin opgenomen regels omtrent schadebegroting, causaliteit, eigen schuld, etc.
Zo kan Opdrachtgever pas schade claimen als er sprake is van een toerekenbare tekortkoming of onrechtmatig handelen van de Leverancier . Opdrachtgever kan dus bijvoorbeeld geen schade claimen voor zover zij daar

zelf debet aan is of voor zover de schade voortvloeit uit een niet-toerekenbare tekortkoming.
Naast de limitering van de hoogte van de aansprakelijkheid in artikel 16.3 en 16.4 (GIBIT), sluit AD dus 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 nu 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. Soms wordt met indirecte schade gedoeld op schade die in onvoldoende causaal verband staat tot de tekortkoming; de eis van causaal verband is echter al een algemene regel van Nederlands schadevergoedingsrecht.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
84

Onderwerp:
Inkoopvoorwaarden GIBIT 16.5

Vraag:
Het is leverancier niet toegestaan onbeperkte aansprakelijkheid voor schade te aanvaarden. Leverancier ziet graag dat de bepalingen onder i), iii) en iv) ook onder de aansprakelijkheidsbeperking van artikel 13.3 en 13.4 vallen. Bent u hiertoe bereid? Tekstvoorstel: De in dit artikel bedoelde beperking van aansprakelijkheid komt te vervallen indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel.

Antwoord:
Zie vraag en antwoord 83.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
85

Onderwerp:
Inkoopvoorwaarden GIBIT 16.4

Vraag:
Hoewel aansprakelijkheid voor overige schade beperkt is tot een bedrag per gebeurtenis met een maximum per jaar betreft het een erg forse aansprakelijkheid ten opzichte van de opdrachtwaarde. Daarnaast ziet de aansprakelijkheid op alle schade. Dit is in strijd met het beleid van leverancier Leverancier ziet deze bepaling graag dat aansprakelijkheid van Leverancier voor gevolgschade en/of indirecte schade is uitgesloten. Onder gevolgschade en/of indirecte schade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill en schade door bedrijfsstagnatie. Bent u daartoe bereid? Zo nee, waarom niet?

Antwoord:
Zie vraag en antwoord 83.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
86

Onderwerp:
Inkoopvoorwaarden GIBIT 16.3

Vraag:
Gezien de potentiele omvang van de contractwaarde stelt Leverancier voor deze bepaling naar redelijkheid aan te passen: De in lid 1 bedoelde aansprakelijkheid voor persoons- en zaakschade is beperkt tot een bedrag van € 750.000,– per gebeurtenis met een maximum van € 1.250.000,-. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. De aansprakelijkheid van partijen voor gevolgschade en/of indirecte schade is uitgesloten. Onder gevolgschade en/of indirecte schade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill en schade door bedrijfsstagnatie. Bent u daartoe bereid? Zo nee, waarom niet?

Antwoord:
Zie vraag en antwoord 83.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
87

Onderwerp:
Inkoopvoorwaarden GIBIT 6.6

Vraag:
Graag toevoegen dat indien leverancier de hiervoor gemaakte kosten kan factureren. Bent u akkoord?

Antwoord:
Zie vraag en antwoord 83.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
88

Onderwerp:
Inkoopvoorwaarden GIBIT 6.5

Vraag:
Graag toevoegen dat indien leverancier de hiervoor gemaakte kosten kan factureren. Bent u akkoord?

Antwoord:
AD begrijpt de strekking van deze vraag niet in relatie tot vraag en antwoord 87.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
89

Onderwerp:
Inkoopvoorwaarden GIBIT 4.3

Vraag:
Vraag: Leverancier ziet aan deze bepaling graag toegevoegd dat indien u de ontbinding van de overeenkomst inroept de reeds door leverancier uitgevoerde werkzaamheden, verrichte leveringen en diensten worden afgerekend naar de stand van het werk op het moment van ontbinding. Bent u hiertoe bereid?
Tekstvoorstel (toe te voegen aan artikel): Indien Opdrachtgever op het moment van de ontbinding reeds prestaties ter uitvoering van de Overeenkomst heeft ontvangen, zullen deze prestaties en de daarmee samenhangende betalingsverplichtingen geen voorwerp van ongedaanmaking zijn. Bedragen die Leverancier vóór de ontbinding heeft

gefactureerd in verband met hetgeen hij ter uitvoering van de overeenkomst reeds heeft verricht of geleverd, blijven onverminderd verschuldigd en worden op het moment van de ontbinding direct opeisbaar.

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
90

Onderwerp:
Inkoopvoorwaarden GIBIT 4.1

Vraag:
Leverancier acht het redelijk dat hij eerst in gebreke wordt gesteld voordat verzuim intreedt. Dit komt de rechtszekerheid ten goede. Bent u bereid hiermee in te stemmen?
Tekstvoorstel: Toevoegen: In alle gevallen, derhalve ook indien partijen schriftelijk en uitdrukkelijk een uiterste termijn zijn overeengekomen, komt Leverancier wegens tijdsoverschrijding eerst in verzuim nadat Opdrachtgever hem schriftelijk in gebreke heeft gesteld.

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.	**Onderwerp:**
91	Beschrijvend Document

Vraag:

3.9.6. In de 1 na laaste zin beggint met "de dat bij de leverancier…." : bedoelt Opdrachtgever hier "de data bij de leverancier"?
3.4. Zijn CERT diensten in- of exclusief de uitgevraagde scope?
3.9.3 Kan Opdrachtgever nader toelichten wat zij bedoelt met "current state of transactions" i.e. welke "transactions" bedoelt Opdrachtgever exact?
3.9.5 Kan Opdrachtgever nader toelichten wat zij bedoelt met "een Third Party Mededeling op de betrouwbaarheid van de dienstverlening"?
9.1.6 Wat cq welke optionele dienstverlening of consultancy bedoelt Opdrachtgever exact met "meerwerk"?
9.1.3 M.b.t. de eis dat de concrete SLA maximaal 6 A4 mag zijn, gaan wij er gemakshalve vanuit dat dit exclusief voor/achterblad en inhoudsopgave is?
Bijlage 1 Hier wordt Bijlage 4 niet expliciet genoemd: dient inschrijver er van uit te gaan dat de ingevulde bijlage 4 bij inschrijving moet worden ingedient?
Bijlage 7A Al19: Kunt u aangeven hoeveel van elke alert momenteel (gemiddeld per maand) gemeld worden?
Bijlage 7A Al19: Kunt u aangeven of "response tijd" inclusief triage en initiele analyse/classificatie tijd is? Oftewel start de responsetijd vanaf het moment dat een alert/event geclassificeerd is als een security incident door een analist en na uitsluiting van true negatives of start deze reeds vanaf het moment van genereren van een event/alert door de onderliggende technologie?
Bijlage 7A AL19: Indien met "responstijd" de tijd bedoelt wordt tussen classificatie en uiteindelijke escalatie naar Opdrachtgever; wat zijn dan de geeiste maximale tijden wat befreft de initiele pick up + classificatie tijd?
Bijlage 7A AL19: De huidige formulering in de uitvraag suggereert dat alle meldingen, ongeacht ernst of duiding, binnen maximaal 16 uur aan u moeten worden doorgegeven. Aanbieder is van mening dat het t.b.v. de efficiëntie en noodzaak niet gangbaar als ook voor Opdrachtgever niet gewenst is om P3 en P4 meldingen dermate snel 24/7 en ook in het weekend te rapporteren omdat met name P4 (informational) meldingen nooit directe opvolging behoeven en normaliter slechts in dashboarding en de standaard rapportages benoemd worden. Bent u bereid uw wens qua maximale responstijden aan te passen aan de in de markt gangbaar gehanteerde en meer logische tijden? Aanbieder wenst te benadrukken dat indien u vasthoudt aan de huidige maximale responstijden, inschrijven door Aanbieder(s) waarschijnlijk niet mogelijk gaat zijn omdat deze afwijkende en op maat in te richten SLA cq responstijden tot een dermate kostenstijging zou resulteren dat het maximale jaarbedrag niet haalbaar gaat zijn.
Bijlage 7A Al19 en TE10: hier lijken de tijden niet met elkaar in

overeenstemming te zijn: kunt u aangeven welke juist zijn? Indien Opdrachtgever beide als juist beschouwd: wat zijn de verschillen tussen deze reactie- cq responstijden?

Antwoord:
Allereerst wenst AD op te merken dat het indienen van meerdere vragen in één vraag onduidelijk en inefficiënt is. Verzoek is dan ook om bij de NVI-2 eventuele vragen 1 voor 1 te stellen in de vraag-antwoord-module van TenderNed;
3.9.6. DIt is een typefout, dit moet inderdaad data zijn.
3.4. Buiten Scope.
3.9.3. Een beschrijving van de huidige situatie van logstromen en gebeurtenissen die binnen de organisatie plaatsvinden en die naar een SIEM of SOC zouden moeten gaan.
3.9.5. Met een ""Third Party Mededeling op de betrouwbaarheid van de dienstverlening"" bedoelt Opdrachtgever een onafhankelijke assuranceverklaring, waarin wordt bevestigd dat de dienstverlening voldoet aan relevante normen op het gebied van betrouwbaarheid en beveiliging.
9.1.6. werkzaamheden die niet binnen de scope van de aanbesteding vallen
9.1.3 Akkoord
Bijlage 1: Correct
Bijlage 7AAL19: Opdrachtgever is van mening dat deze informatie niet relevant is voor de aanbesteding
Bijlage 7AAL19: zie vraag 74
Bijlage 7AAL19: Zie vraag 74
Bijlage 7AAL19: zie vraag 74
Bijlage 7AAL19: Zie vraag 74

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr. 92

Onderwerp:
BD 5.5

Vraag:
Deze paragraaf stelt dat bij een beroep op derden door deze derde een eigen

afzonderlijk UEA moet worden ingevuld. Verder in deze paragraaf staat inzake de continuïteitsparagraaf dat, indien deze derde een onderneming is die tot het concern van de inschrijver behoort, kan worden volstaan met het overleggen van een zogenaamde 2:403 verklaring. Kunt u bevestigen dat igv een moederorganisatie met een geconsolideerde jaarrekening er geen eigen UEA van de moederorganisatie wordt verwacht?

Antwoord:
Akkoord; Concernverklaring volstaat in deze.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
93

Onderwerp:
Onderwerp: Programma van Eisen AL. 7

Vraag:
Vraag: inschrijver eist dat de locatie van het SOC en de door de opdrachtnemer gebruikte software (o.a. SIEM), binnen de EER gevestigd moeten zijn.

Gaat de inschrijver ermee akkoord om de locatie-eisen te verruimen voor het SOC + de gebruikte software tot EER+UK, gezien de UK tot voor kort onderdeel was van de EER en gelijkwaardige regelgeving heeft rondom cybersecurity. Dataopslag kan wel binnen EER blijven.

Antwoord:
Akkoord, mits dataopslag aangetoond binnen de EER staat.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
94

Onderwerp:
Onderwerp: Programma van Eisen TE 14/15/16

Vraag:
Vraag: Inschrijver noemt in de gewenste situatie van het beschrijvend document op pagina 7 “verzamelen van beveiligingsgebeurtenissen en logs van verschillende bronnen binnen de IT-infrastructuur...”

Echter, in het programma van Eisen (TE 14/15/16) wordt ook de OT-omgeving genoemd.

1) Kan inschrijver bevestigen dat ook de OT-omgeving buiten de scope valt;
2) Indien het binnen de scope valt: kan inschrijver toelichten hoe de OT-omgeving eruitziet.

Antwoord:
De OT-omgeving valt niet volledig buiten de scope. Op basis van discovery ziet Defender welke OT-devices aanwezig zijn, zoals bijvoorbeeld Chromecasts, camera's en devices gerelateerd aan het toegansgbeheersysteem. Deze devices ziet opdrachtgever graag opgenomen worden in de SIEM en de SOC-dienstverlening.
Zie ook vraag en antwoord 20.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
95

Onderwerp:
Onderwerp: Programma van Eisen AL 11.

Vraag:
Vraag: Worden mobiele devices momenteel gemonitord in de huidige dienstverlening?

Antwoord:
Alle mobiele devices zijn onboarded in Defender.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
96

Onderwerp:
Onderwerp: Programma van eisen TE 25

Vraag:
Vraag: Eis TE 25 stelt dat SOC-dienst aantoonbaar in staat moet zijn om ten minste X vooraf opgestelde use cases te implementeren en onderhouden, kan inschrijver duiden om hoeveel uses cases het specifiek gaat?

Antwoord:
Zie vraag en antwoord 73.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 97

Onderwerp:
Onderwerp: Gunningscriterium K1 Aangeboden dienstverlening

Vraag:
Vraag: Gaat inschrijver ermee akkoord om het maximaal aantal pagina's dat gebruikt mag worden voor de uitwerking van gunningscriterium K1, gezien de hoeveelheid gevraagde informatie, te verruimen naar 8 a4 pagina's.

Antwoord:
Akkoord.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr. 98

Onderwerp:
Appendix 7B Use Cases - Item 16

Vraag:
Welke IoT-apparaten zijn momenteel in gebruik, waar bevinden ze zich op het netwerk en welke toegang hebben ze?

Antwoord:
Gebouwbeheersyste(e)m(en), Chromecast, Apple TV, Virtual Reality Brillen, Intercomsystemen, Telefoons (IP), Camera's (IP), Pinautomaten, UPS, Printers.
IOT devices zitten in een IOT netwerk met voornamelijk alleen toegang naar het internet.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
99

Onderwerp:
Appendix 7B, item 17.

Vraag:
Welke compliance-rapportages zijn vereist vanuit een use-caseperspectief?

Antwoord:
De opdrachtgever wenst dat compliance-rapportages worden ingericht op basis van de relevante use-cases, met als doel inzicht te verkrijgen in de naleving van beveiligings- en compliancebeleid binnen de organisatie. Deze rapportages dienen per systeem of logische groep beschikbaar te zijn. De opdrachtgever denkt hierbij aan rapportages die aansluiten op de binnen Microsoft 365 ingerichte compliance policies.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 4 sep 2025

Ref.nr.
100

Onderwerp:
3.3 Gewenste situatie

Vraag:
Aanbestedende Dienst geeft aan dat het maximale budget is gesteld op Eur 75.000 per jaar (excl BTW). Op basis van de gewenste scope acht Inschrijver het gereserveerde budget ruim ontoerijkend. Is Aanbestedende Dienst bereid om het maximaal jaarlijkse budget te verhogen met een factor 3 naar Eur 225.000 per jaar? Als Aanbestedende Dienst hier niet mee akkoord gaat, staat Aanbestedende Dienst er dan voor open om een subset van de scope uit te vragen? Als dit het geval is dan zien wij graag vanuit

Aanbestedende Dienst een prioriteitenstelling voor de aan de bieden subset.

Antwoord:
Zie vraag en antwoord 3.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
101

Onderwerp:
Beschrijvend Document, Bijlage 7A-Programma van Eisen (eis TE 35)

Vraag:
De eis stelt: “Opdrachtnemer krijgt geen beheerrechten binnen de infrastructuur van de opdrachtgever.” Voor gedegen incidentanalyse en –onderzoek menen wij dat (beperkte) leesrechten, zoals 'security reader' in Entra ID en Azure nodig zijn in de omgeving van opdrachtgever. Daarnaast gebruikt inschrijver service principals voor o.a. het pushen van nieuwe detectieregels naar de SIEM van Veiligheidsregio Twente. Deze service principals worden uitsluitend voor deze (geautomatiseerde) taak gebruikt, juist om beheerrechten op individuele accounts te voorkomen. Is het toekennen van dergelijke rollen en rechten bespreekbaar?

Antwoord:
Zie TE. 3. Noodzakelijk autorisaties voor het juist functioneren van de SIEM /SOC dienst zijn gewoon mogelijk en bespreekbaar.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025

Ref.nr.
102

Onderwerp:
Beschrijvend Document, Referentieopdrachten (par. 7.4 / bijlage 6)

Vraag:
U vraagt om referentieopdrachten met SIEM/SOC-diensten aan een (semi-) overheidsorganisatie. Mogen de referenties ook uit de private sector komen of uitsluitend uit de publieke sector?

Antwoord:
Zie vraag en antwoord 34.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 SIEM/SOC

Beantwoord op: 3 sep 2025