

Nota van Inlichtingen – versie 2

Marktconsultatie ‘MDR/SOC dienstverlening ten behoeve van veiligheidsregio’s en het NIPV’.

Datum: 18 maart 2025

In deze Nota van Inlichtingen geeft de Aanbestedende Dienst antwoord op de gestelde vragen en wijzigingsvoorstellen die in het kader van de marktconsultatie ‘MDR/SOC dienstverlening ten behoeve van veiligheidsregio’s en het NIPV’ zijn geplaatst.

Algemene opmerkingen:

- Zie aanvullende vragen 39 – 49 en antwoorden.
- We merken dat het voor de markt onduidelijk is wat de rolverdeling is tussen het NIPV, het Versnellingsplan Informatieveiligheid en de Veiligheidsregio’s (VR’s). Deze marktconsultatie is ingezet door het Versnellingsplan Informatieveiligheid. Dit project ondersteunt de VR’s en het NIPV bij diverse onderwerpen aangaande informatieveiligheid, waaronder het verwerven van MDR/SOC diensten. In dit kader is ervoor gekozen een baseline te formuleren qua dienstverlening en de verwerving hiervan zoveel mogelijk voor te bereiden. Het opstellen van een PVE en het uitvoeren van een marktconsultatie is hier onderdeel van. Ook zullen vanuit het Versnellingsplan Informatieveiligheid de deelnemende VR’s en het NIPV verder worden begeleidt in het traject, met kennis en expertise. Omdat het Versnellingsplan geen formele basis heeft van waaruit het een marktconsultatie uit kan zetten, treedt het NIPV hierin als facilitator op. De uiteindelijke aanbestedingen zullen worden ingezet vanuit de VR’s en het NIPV, begeleidt door het Versnellingsplan Informatieveiligheid, waarbij gezamenlijke aanbestedingen niet worden uitgesloten als dit de meest logische optie is.
- We merken dat de markt ook vragen aan ons stelt die meer passen bij een nota van inlichtingen bij een aanbesteding. We zijn in deze marktconsultatie vooral op zoek naar input uit de markt die ons helpt om op de genoemde onderdelen een uitvraag te formuleren die niet alleen

past bij onze eisen of wensen, maar ook bij marktontwikkelingen, trends, gebruikelijkheden en beperkingen van de markt. Deze marktconsultatie heeft tot doel ons deze in te laten zien, om daar in de uitvragen rekening mee te gaan houden.

Vraag nr.	Verwijzing	Vraag	Antwoord
1.	Algemeen	De antwoorden dienen we in te vullen in de Word bijlage 1 in tabel-vorm. Gezien de type vragen is het ook toegestaan om bijlagen toe te voegen om zodoende een compleet antwoord of toelichting te kunnen geven?	Ja, dat is akkoord.
2.	Vragen marktconsultatie	Specificatie van de baseline: Hoewel de gebieden SOC-dienstverlening, SIEM, NDR en EDR als baseline worden genoemd, is de exacte functionele scope van deze baseline nog onduidelijk. Zou u meer details kunnen geven over de minimale functionaliteiten en dekkingsgraad die binnen elk van deze gebieden verwacht wordt? Denk hierbij aan specifieke use cases of detectiecapaciteiten die essentieel zijn.	De verwachting is dat de VR's en het NIPV individueel aanbestedingen zullen gaan uitvoeren. Het staat ze vrij om te bepalen welke van deze baseline onderdelen daadwerkelijk worden aanbesteed. Hierdoor kan er geen exacte functionele scope en minimale functionaliteiten en dekkingsgraad aangeven worden. De deelnemers zullen tijdens de aanbesteding verder in gaan op deze punten.
3.	Vragen marktconsultatie	Concrete voorbeelden regionaal maatwerk: Er wordt gesproken over ruimte voor regionaal maatwerk. Om beter inzicht te krijgen in de benodigde flexibiliteit van de dienstverlening, zouden we graag enkele concrete voorbeelden zien van de soorten aanvullingen of specifieke behoeften die de verschillende veiligheidsregio's mogelijk hebben bovenop de gedefinieerde baseline. Kunt u deze geven?	Maatwerk moet gezocht worden in het specifiek maken van use cases, wijzigingen in bereikbaarheid en tijden (zie ook 'optioneel' in het concept pve).
4.	Vragen marktconsultatie	Beslissingscriteria gezamenlijke vs. individuele aanbesteding: De keuze tussen een gezamenlijke of individuele aanbesteding is een cruciale strategische overweging (zie vraag 11 in bijlage 1). Kunt u nader toelichten welke criteria en afwegingen vanuit het perspectief van het NIPV en de VR's hierbij een rol spelen? Dit inzicht zou ons helpen om beter afgestemde adviezen en oplossingen te formuleren. Daarnaast	Niet het NIPV maar het Versnellingsplan Informatieveiligheid treedt in deze op als facilitator en ondersteuners naar deelnemende regio's én het NIPV. In principe zullen de uiteindelijke aanbestedingen individueel uitgevoerd worden, maar kan er de keuze wordt gemaakt om gezamenlijk een aanbesteding te doen. Bijvoorbeeld op basis van regionale samenwerking. Samenwerking wordt aangegaan als hier een logische grondslag voor te vinden is,

		horen we graag of het NIPV bijvoorbeeld een regiefunctie zou willen vervullen in dit proces.	deze marktconsultatie heeft mede tot doel om duidelijk te krijgen welke dit zouden zijn, rekening houdend met de mate van autonomie en vrijheid die regio's hebben.
5.	Vragen marktconsultatie	Rolverdeling VR-knooppunt: De term 'VR-Knooppunt' wordt genoemd (vraag 20 in bijlage 1, VR11.1-8 in bijlage 2). Zou u de specifieke rol, verantwoordelijkheden en beoogde interactie van dit knooppunt met de toekomstige MDR-dienstverlener kunnen toelichten? Dit is cruciaal om de meerwaarde van dreigingsinformatie en de samenwerking te begrijpen.	De specifieke rol, verantwoordelijkheden en gewenste interactie van het VR-Knooppunt moeten nog worden vastgesteld. In grote lijnen kan het volgende worden gesteld: • Het VR-Knooppunt zal (dreigings)informatie ontvangen vanuit sectorale partnerorganisaties en gremia. • Het zal primair een schakelfunctie vervullen, waarbij het dreigingsinformatie ontvangt en deelt met veiligheidsregio's, de MDR-dienstverlener en sectorale partners. • De rol voor leveranciers zou kunnen zijn dat bepaalde informatie met meerdere kanalen gedeeld moet worden (bijvoorbeeld primaire klant, maar ook met het knooppunt). We onderzoeken de eventuele impact hiervan op de dienstverlening (als die er al is).
6.	Concept Programma van Eisen	Verduidelijking logdata management: In bijlage 2 worden verschillende opties genoemd voor de verantwoordelijkheid van het verzamelen en opslaan van logdata (D4.2, D4.2.1, D4.2.2). Zou u meer kunnen toelichten over de voorkeuren of overwegingen die ten grondslag liggen aan deze verschillende modellen? Dit is van invloed op de architectuur van de dienstverlening.	Welke optie wordt gekozen zal mogelijk verschillend zijn per regio. De overwegingen zullen voornamelijk gebaseerd zijn op aanwezige infrastructuur (o.a. cloud vs. Hybride). De voors- en tegens van de verschillende opties proberen we ook in deze marktconsultatie verder duidelijk te krijgen. We zijn benieuwd of er in de markt voorkeuren zijn voor opties voor het verzamelen en opslaan van logdata en zo ja, waarom. Zijn er standaarden en zo ja, waarom? Is aanpassen op de standaard ingrijpend of goed mogelijk voor de markt, daar zijn we benieuwd naar. Vervolgens kunnen we in schatten waar de ruimte ligt aan onze kant om redelijke eisen en wensen te formuleren.
7.	Concept Programma van Eisen	Voorlopige service level expectations (SLEs): Hoewel een SLA na gunning wordt vastgesteld (A1.9 in bijlage 2), zijn er mogelijk al voorlopige verwachtingen ten aanzien van kritieke service level expectations (SLEs) , zoals bijvoorbeeld de responstijden op incidenten van verschillende prioriteiten (zie	Het is de vraag aan de markt wat reëel is om op te nemen in de aanbesteding. Hier kan dat bij het opstellen van de aanbestedingen rekening mee worden gehouden.

		D4.13 in bijlage 2), de beschikbaarheid van de dienst (T10.29 in bijlage 2), of de frequentie van rapportages (D4.11 in bijlage 2)? Inzicht hierin zou helpen bij het formuleren van een passende dienstverlening.	
8.	Concept Programma van Eisen	Integratie met bestaande security capabilities: Er wordt vermeld dat de Opdrachtnemer aansluit op de bestaande security capabilities (D4.3 in bijlage 2). Zou u meer kunnen specificeren over de belangrijkste bestaande security tools en platformen waarmee integratie verwacht wordt (naast de reeds genoemde SIEM, NDR en EDR)?	De securitytools en -platformen verschillen per veiligheidsregio. Wel kunnen we aangeven dat de gebruikte tools en platformen industrie-standaard producten zijn.
9.	Concept Programma van Eisen	Wensen rondom threat intelligence sharing: Met betrekking tot het delen van dreigingsinformatie (T10.3, D4.8 in bijlage 2, VR11.4, VR11.5 in bijlage 2), zijn er specifieke standaarden, formaten of platforms (buiten STIX/TAXII en MISP) die de voorkeur genieten of reeds in gebruik zijn binnen de VR's en het NIPV?	Wij zoeken in deze marktconsultatie naar de standaarden en eventuele flexibiliteit in de markt. Wij willen weten of hier wensen/eisen in te stellen zijn, of dat de markt hierin een aantal modellen voorziet (en zo ja, waarom en welke).
10.	Concept Programma van Eisen	Verwachtingen ten aanzien van playbooks: Eis T10.2 in bijlage 2 stelt dat de Opdrachtnemer Playbooks oplevert. Wat zijn de verwachtingen ten aanzien van de detailniveau, de scope en de verantwoordelijkheid voor het onderhoud van deze playbooks (ligt dit primair bij de dienstverlener of is dit een gezamenlijke inspanning)?	De verantwoordelijkheid voor het opstellen van de Playbooks is een gezamenlijke inspanning. Daarbij wordt van de MDR-dienstverlener verwacht dat deze zijn aanwezige kennis en expertise inzet om Playbooks voor te stellen en te optimaliseren.
11.	Concept Programma van Eisen Paragraaf 1.15 t/m 1.17	In deze paragrafen geeft u als eis dat mondelinge communicatie en documentatie in de Nederlandse taal dient te geschieden. Wij begrijpen heel goed dat de Nederlandse taal voor eindgebruikers nodig is, maar communiceren met beheerders binnen het IT domein in de Engelse taal is over het algemeen goed geaccepteerd. Wij willen u vragen of u de taaleis los kunt laten.	Het is aan de aanbestedende diensten om te bepalen of deze eis wordt losgelaten of niet. In de antwoorden op de vragen van de marktconsultatie kan een advies worden gegeven wat het de diensten kan opleveren als er ook in het Engels gecommuniceerd mag worden.

12.	Concept Programma van Eisen	Veel overheidsinstanties conformeren zich aan specifieke inkoopvoorwaarden (Arbit/Gibit). Geldt dit ook voor het NIPV en de veiligheidsregio's?	Ja, dat is correct.
13.	Hoofdstuk 1.3 Huidige situatie, pagina 5	NIPV geeft aan om met deelnemende VR's (10 stuks) samen te willen werken om MDR en SOC-diensten te verwerven. Welke rol speelt NIPV in deze? A: NIPV als facilitator: NIPV sluit centraal mantelcontract af voor SOC/MDR diensten/bouwblokken, waaronder de aangesloten deelnemers een specifieke uitvraag kunnen gaan doen? (Vergelijkbaar met bijvoorbeeld de VNG Mantel Monitoring en Response diensten) B: NIPV als inkoopbureau, eveneens voor de VR deelnemers? C: NIPV puur als informatievergaring tbv de aanbesteding uitvraag D: NIPV als beleidsbepalende entiteit en opstellen van baseline tbv de VR sector? E: Verwacht NIPV ook een rol te zullen gaan spelen in de operationele SOC en Incident en Response processen, buiten NIPV zelf om?	Zie het antwoord op vraag 4.
14.	Hoofdstuk 1.3 Huidige situatie, pagina 5	NIPV geeft aan om met deelnemende VR's (10 stuks) samen te willen werken om MDR en SOC-diensten te verwerven. Welke VR's maken onderdeel uit van deze uitvraag? En zijn deze VR's in deze uitvraag afnameplichtig?	Het is niet relevant voor deze marktconsultatie om de deelnemende VR's te benoemen. De VR's zijn niet afnameplichtig gezien de aanbestedingen in principe regionaal worden uitgevoerd, maar gezamenlijke aanbesteding ook mogelijk is.
15.	Hoofdstuk 1.1 Huidige situatie, pagina 4	NIPV geeft aan dat de implementatie van de BIO de laatste jaren de benodigde aandacht heeft gekregen. A: Geldt dat in dezelfde mate voor de implementatie van NEN7510?	A: NEN7510 is alleen van toepassing bij VR's met een GGZ functie. In die VR's is er constant afstemming hoe ver de normering reikt in relatie tot de VR. Daar waar dat zo is, zullen normeringen van toepassing zijn. Deze zullen dan naar verwachting in de uitvraag meegenomen worden.

		B: in hoeverre wordt in dat kader ook al naar de BIO2.0 gekeken?	B: De VR's gebruiken de BIO1.04. De BIO2 kan een rol gaan spelen, hoe is nog niet duidelijk.
16.	Hoofdstuk 1.4 Huidige situatie, pagina 6	NIPV geeft in paragraaf 1.4 aan welke type MDR diensten (bouwblokken) zij heeft gedefinieerd, (SOC, SIEM, EDR, NDR) als onderdeel van de baseline. Staat NIPV ook open voor additionele diensten zoals Vulnerability Management, Dark-/Deepweb monitoring, Third Party Monitoring, ...?	De keuze voor aanvullende dienstverlening is een individuele keuze die de VR's kunnen maken in hun aanbesteding.
17.	Hoofdstuk 1.4 Huidige situatie, pagina 6	NIPV geeft aan dat de geschatte waarde van de opdracht circa € 100.000,- a € 150.000,- excl. btw per jaar per deelnemer bedraagt. Kan NIPV aangeven op basis waarvan deze indicatie is bepaald?	Op basis van gespreken met de VR's en het NIPV zijn bedragen ter spraken gekomen en mede hierdoor is een indicatie gemaakt.
18.	Hoofdstuk 1.4 Huidige situatie, pagina 6	NIPV geeft aan dat de geschatte waarde van de opdracht circa € 100.000,- a € 150.000,- excl. btw per jaar per deelnemer bedraagt. Voor organisaties die meerdere beveiligingsoplossingen tegelijkertijd wensen in te zetten, wat vaak voorkomt, kan mogelijk, afhankelijk van de scope, het gestelde budget niet toereikend zijn. Hebben de VR's en NIPV een idee hoe hier mee om te gaan mocht zich dat voordoen? Is er bijvoorbeeld ruimte om boven de door NIPV geschatte waarde uit te komen? Is er bijvoorbeeld een platfondbedrag? En zo wat is deze dan?	De genoemde bedragen zijn slechts ter indicatie maar hier kan van worden afgeweken bij daadwerkelijke aanbestedingen. Door wensen, eisen, behoeften en mogelijkheden uit de markt samen te brengen komen we tot een inzicht qua begroting.
19.	Hoofdstuk 1.4 Huidige situatie, pagina 6	NIPV geeft aan dat de geschatte waarde van de opdracht circa € 100.000,- a € 150.000,- excl. btw per jaar per deelnemer bedraagt. Inschrijver gaat ervan uit dat dit alleen de geschatte waarde van de dienstverlening is dat de eenmalige kosten hier geen onderdeel van zijn. Is deze aanname correct?	Deze aanname is correct.
20.	PvE: A1.18	Kunt u aangeven welke landen NIPV definieert als landen met een offensief Cyberprogramma?	Conform de definitie van de AIVD: Rusland, China, Iran, Noord-Korea

21.	PvE: T10.29	Om 99,99% beschikbaarheid per maand te kunnen bieden is redundancy een veelal noodzakelijk in te vullen oplossingsrichting, wat ook additionele kosten met zich mee brengt. Heeft NIPV in haar budgetindicatie hier ook rekening meegehouden?	We begrijpen dat minder downtime meer kosten met zich meebrengt. We vragen de markt om ons te helpen begrijpen wat de verhouding is tussen kosten en uptime, waar een omslagpunt ligt en wat voor sectoren die met ons vergeleken kunnen worden gangbare uitgangspunten zijn.
22.	Algemeen	Hebben het NIPV en de bijbehorende veiligheidsregio's zelf een IT team met een 24/7 beschikbaarheid?	Dit verschilt per veiligheidsregio. Per regio zal in de aanbesteding gespecificeerd worden wat de behoefte is van de dienstverlener.
23.	Algemeen	Zijn er buiten kantoor tijden medewerkers beschikbaar om incidenten op te volgen?	Zie het antwoord op vraag 22.
24.	Pve	Uit onderzoek blijkt dat een retentietijd van 6 maanden niet altijd voldoende is om threat hunts in het verleden te kunnen doen (zie Solarwinds). Is het raadzaam om een retentie tijd van logging van minimaal 12 maanden uit te vragen?	Het is aan de aanbestedende diensten om dit te bepalen. In de antwoorden op de vragen van de marktconsultatie kan een advies worden gegeven wat het de diensten kan opleveren als de retentietijd 12 maanden is.
25.	Algemeen	Hebben jullie nagedacht over security automation (SOAR) rond de SOC dienstverlening? En zouden jullie deze software graag inclusief in de dienst willen zien?	Ja, zie Bijlage 2. T10.31
26.	Algemeen	Willen het NIPV en de bijbehorende veiligheidsregio's toegang hebben tot exact dezelfde SIEM software als het SOC team zodat er sprake is van volledige transparantie?	Ja, als dat mogelijk is, maar wel op basis van logica (need to know vs. nice to know afwegingen).
27.	Algemeen	Hebben het NIPV en de bijbehorende veiligheidsregio's behoefte aan de uitvoering van takedowns op malicious websites en phishing domains?	Dit betreft een aanvullende dienstverlening dus dit is een individuele keuze.
28.	Algemeen	Dient de MDR leverancier ook te alarmeren op gepubliceerde credentials op het (dark) web?	Dit betreft een aanvullende dienstverlening dus dit is een individuele keuze.

29.	Algemeen	Volstaat het voor het NIPV en de veiligheidsregio's dat de data binnen de EER blijft maar dat er voor de behandeling van een incident buiten lokale kantoor tijden kan worden uitgeweken naar een team buiten de EER volgens het follow the sun principe (Amerika, Australië)?	Nee, ook i.v.m. de Nederlandse taal eis. Zie tevens het antwoord op vraag 11.
30.	Algemeen	Op welke manier gaat het NIPV een kostenvergelijking maken tussen de verschillende aanbieders met verschillende licentiemodellen? (assets, dataverbruik, use-cases) <i>Voorbeeld: bij de uitvraag van de VNG hebben ze twee concrete use-cases beschreven zodat zij tot een duidelijk vergelijk van de kosten konden komen op basis van data verbruik, aantal assets en gekoppelde logbronnen.</i>	De beoordelingsmethoden zullen gekozen worden door de VRs en het NIPV tijdens het opstellen van de aanbestedingsdocumenten. Deze marktconsultatie is in eerste instantie gericht op het verkrijgen van informatie vanuit de markt. Advies met betrekking tot kostenvergelijking zien wij graag terug in het antwoord op 'prijsstelling algemeen'. De antwoorden worden gebruikt de VR's en het NIPV te adviseren bij het opstellen van hun aanbesteding. Wel vragen we de markt om mee te denken dit zoveel mogelijk vanuit 1 baseline in te richten. Dus bijvoorbeeld de suggestie van de markt om concrete use-cases in de aanbesteding mee te nemen, zouden we over kunnen nemen.
31.	Algemeen	In hoeverre is het belangrijk dat jullie op voorhand inzichtelijk hebben wat het totale kostenplaatje is, ongeacht het dataverbruik en het aantal use-cases?	Het is belangrijk om op voorhand te weten wat de deelnemers kunnen verwachten. De VR's en het NIPV zijn opzoek naar wat gangbaar is en willen ook kunnen bijstellen als dat nodig is.
32.	Algemeen	Dient in de aanbidding incident response inbegrepen te zijn of zijn de veiligheidsregio's zelf uitgerust met een incident response retainer?	Er is momenteel een incident response ingeregeld voor de VR's. Wel kunnen de VR's eventueel kiezen voor aanvullende incident response dienstverlening.
33.	Algemeen	Hebben het NIPV en de veiligheidsregio's grotendeels dezelfde IT infrastructuur componenten? Zo ja, dan is het raadzaam deze te vermelden in de uitvraag.	Zie Bijlage 2. T10.1

34.	Algemeen	Wat is de gemiddelde ideale implementatie tijd van de SOC dienst per locatie?	We zouden van de markt graag horen waar we rekening mee moeten houden. Ook zijn we benieuwd hoe de markt omgaat met meerdere trajecten tegelijk (achter elkaar aan cq. filevorming of gezamenlijk stappen zetten?).
35.	Algemeen	Is (managed) vulnerability management onderdeel van de uitvraag of is het mogelijk dit optioneel erbij aan te bieden?	Zie Bijlage 2. T10.15
36.	Algemeen	Dient de netwerk sensor onderdeel te zijn van de uitvraag of heeft uw organisatie hier al een oplossing voor?	Dat is geheel afhankelijk van de wens van deelnemer.
37.	Algemeen	Is het hebben van deception technologie (bijvoorbeeld honeypot of honey credentials) gewenst voor de SOC dienstverlening?	Dit betreft een aanvullende dienstverlening, dus is dit een individuele keuze.
38.	PvE	Gezien de begrippen bij punt D4.10 in het Engels, is het naast Nederlands ook toegestaan om in het Engels te communiceren in het geval van een incident?	Zie het antwoord op vraag 11.
39.	Bijlage 2 Concept Programma van Eisen v0.91 / A1.15	Betreffende tekst: <i>Mondelinge communicatie van de Opdrachtnemer naar de Opdrachtgever en Deelnemers vindt plaats in de Nederlandse taal.</i> Is de opdrachtgever bereidt naast Nederlands ook de Engelse taal toe te voegen? Eventueel met een demarcatie tussen technisch (EN) en operationeel (NL)?	Zie het antwoord op vraag 11.
40.	Bijlage 2 Concept Programma van Eisen v0.91 / C3.1	Betreffende tekst: <i>De door Inschrijver aangeboden tarieven zijn 'all-in', dat wil zeggen inclusief (niet gelimiteerd) salariskosten, overheadkosten, kosten voor gebruik apparatuur/software/hardware (die nodig zijn bij het in het kaart brengen en oplossen van een informatieveiligheid incident), verzekeringen, reis- en</i>	De behoefte van een one-size-fits-all is geheel afhankelijk van de individuele deelnemers. Mits zij met meerdere tegelijkertijd een uitvraag doen, is de verwachting dat Deelnemers individueel een verwervingstraject zullen bewandelen.

		<i>verblijfskosten, reistijd, belasting, heffingen, administratieve kosten, kosten voor overleg etc.</i> Is het de bedoeling van de opdrachtgever hiermee een one-size-fits-all propositie te creëren voor alle 10 deelnemers? Zo ja, impliceert opdrachtgever dat elke VR identiek is in zijn/haar behoefte?	
41.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.1	Betreffende tekst: <i>De Opdrachtnemer kan haar SOC-analisten classificeren volgens de marktdefinities voor SOC-Analisten niveau 1, niveau 2 of niveau 3.</i> Kan de opdrachtgever de specifieke marktdefinities per SOC analist Niveau 1,2 en 3 nader beschrijven?	Zie bijlage 1, vraag 19.
42.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.6	Betreffende tekst: <i>Opdrachtnemer implementeert, beheert en optimaliseert de te gebruiken security use cases en alle benodigde detectieregels. Indien [Deelnemer] over een lokale SIEM-oplossing beschikt, worden de use cases ook in dit lokale SIEM geïmplementeerd. Operationalisatie van deze uitrol vindt plaats in overleg met de betreffende Deelnemer. De security use cases bestaan minimaal uit:- Bescherming tegen bekende generieke aanvallen- Bescherming tegen specifieke aanvallen op Deelnemers- Bescherming tegen aanvallen die gedetecteerd zijn bij andere klanten van Opdrachtnemer en relevant zijn voor de Deelnemers.</i> Kan de opdrachtgever nader (technisch) toelichten op welke wijze de opdrachtnemer dient te voldoen aan de eis dat use cases ook in deelnemer (VR) specifieke omgeving geïmplementeerd dient te worden?	Wanneer een Deelnemer het verwervingstraject is gestart kan er een mogelijkheid worden geboden om meer toelichting te bieden.
43.	Bijlage 2 Concept Programma van	Betreffende tekst:	De feedback zal worden meegenomen en waar nodig aangepast.

	Eisen v0.91 / D4.8	<i>Opdrachtnemer heeft partnerships met diverse partijen om markt specifieke dreigingsinformatie te ontvangen, in ieder geval met het NCSC en een nog aan te wijzen VR-Knooppunt.</i> Is de opdrachtgever bekend met het feit dat sector specifieke dreigingsinformatie (NCSC) alleen beschikbaar gesteld mag worden via de opdrachtgever aan opdrachtnemer?	
44.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.13	Betreffende tekst: <i>Opdrachtnemer draagt zorg voor een tijdige prioritering van- en respons op- security incidenten door melding aan [Deelnemer]*. Hierbij voldoet Opdrachtnemer aan de volgende richtlijn: Time to respond:- Critical (P1). - 20 min- High (P2) - 1 uur- Medium (P3) - 4 uur- Low (P4). - 16 uur* En eventueel andere partijen zoals een nog aan te wijzen VR-Knooppunt. **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 desbetreffende Deelnemer.</i> Is de opdrachtgever bekend met het feit dat P4 incidenten een aanzienlijke verhoging op de werkdruk te weeg zal brengen bij de security organisatie van de betreffende deelnemer (VR)? Zo ja, is de opdrachtgever bereid om de time to respond aan te passen naar een periodieke rapportage vorm?	De feedback zal worden meegenomen, het is echter aan de Deelnemers of deze aanpassing gewenst is.
45.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.15	Betreffende tekst: <i>Opdrachtnemer dient op verzoek [Deelnemer] te kunnen ondersteunen bij het aansluiten op de SOC-dienstverlening. Dit omvat zowel de configuratie van de lokale componenten van een [Deelnemer] binnen haar eigen netwerkgrenzen als het aansluiten op de converged SOC-dienstverlening.</i> Bedoeld opdrachtgever daar waar SOC dienstverlening staat eigenlijk SOC/SIEM dienstverlening?	Correct.

46.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.23.1	Betreffende tekst: <i>Het SOC, de door de Opdrachtnemer gebruikte software (EDR) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).</i> Gaat de opdrachtgever ermee akkoord dat werkzaamheden aangaande SOC dienstverlening kan worden uitgevoerd conform het "follow the sun" principe. Zo ja, gaat de opdrachtgever ermee akkoord dat er een aanpassing zal moeten plaatsvinden van de "standard contractual clauses" conform de AVG?	Nee, bij een "follow the sun" aanpak wordt er niet voldaan aan de eis omtrent de Nederlandse taal en vestiging binnen de EER.
47.	Bijlage 2 Concept Programma van Eisen v0.91 / D4.23.2	Betreffende tekst: <i>Het SOC, de door de Opdrachtnemer gebruikte software (NDR) en de datacenters waar de data opgeslagen en verwerkt wordt, moeten binnen de EER gevestigd zijn (ook redundante systemen).</i> Gaat de opdrachtgever ermee akkoord dat werkzaamheden aangaande SOC dienstverlening kan worden uitgevoerd conform het "follow the sun" principe. Zo ja, gaat de opdrachtgever ermee akkoord dat er een aanpassing zal moeten plaatsvinden van de "standard contractual clauses" conform de AVG?	Nee, bij een "follow the sun" aanpak wordt er niet voldaan aan de eis omtrent de Nederlandse taal en vestiging binnen de EER.
48.	Marktconsultatie MDR SOC 1.3 Huidige situatie / aanleiding	Betreffende tekst: <i>"Het project waar deze marktconsultatie deel van uitmaakt is een samenwerking van 10 VR's en het NIPV."</i> Kunt u aangeven welke veiligheidsregio's hieraan meewerken?	Zie het antwoord op vraag 14.
49.	Marktconsultatie MDR SOC 1.3 Huidige situatie / aanleiding	Betreffende tekst: <i>"Het project waar deze marktconsultatie deel van uitmaakt is een samenwerking van 10 VR's en het NIPV."</i>	Zie het antwoord op vraag 4 en 14.

		Zijn de betreffende 10 veiligheidsregio's verplicht om de gecontracteerde dienstverlening af te nemen?	
--	--	--	--