



Samen ICT *voor onderwijs*

Nota van Inlichtingen

Netwerkdetectie & Response
SOC-dienstverlening
(Marktconsultatiefase)

Aanbestedende dienst:	Coöperatie KIEN U.A.
Kenmerk:	NDR SOC 2023
TenderNed:	TN 420232
Versie:	1.0
Datum:	24 augustus 2023

Inhoudsopgave

Inhoudsopgave	2
1. Algemeen	3
2. Beantwoording vragen	4

1. ALGEMEEN

Op 12 juli 2023 heeft de Coöperatie KIEN U.A. (KIEN®) de marktconsultatie NDR SOC-dienstverlening gepubliceerd op TenderNed. Het document is op het platform bekend onder nummer: 420232.

Geïnteresseerde partijen hebben de gelegenheid gehad om tot 18 augustus 2023 vragen over de leidraad en procedure van de marktconsultatie te stellen. Dit document bevat de Nota van Inlichtingen (Nvl), behorende bij de marktconsultatie.

Een aantal partijen heeft vragen gesteld met als doel meer inzicht te krijgen in security maatregelen die KIEN al heeft genomen op de infrastructuur. Ook zijn er vragen gesteld over de omvang van de infrastructuur. KIEN beschouwt, zoals aangegeven in paragraaf 2.2 van de marktconsultatie, informatie over securitymaatregelen en informatie over de infrastructuur als gevoelige informatie. Daarom zal KIEN niet alle gevraagde informatie in de marktconsultatiefase delen. Tegelijkertijd snapt KIEN dat leveranciers bepaalde informatie nodig hebben om tot een passend aanbod te kunnen komen.

KIEN overweegt als vervolg op deze marktconsultatie een niet-openbare procedure omdat een dergelijke procedure de mogelijkheid biedt om onder voorwaarden de gevraagde informatie met een beperkt aantal partijen te delen.

Het valt op dat er ook vragen worden gesteld die wij in een Nvl binnen een aanbestedingsprocedure logisch vinden maar in een marktconsultatie niet kunnen beantwoorden. Het doel van de marktconsultatie is wat KIEN betreft juist van de markt te vernemen wat van meerwaarde is bij een NDR SOC-dienstverlening. Pas in een mogelijk vervolgtraject zal KIEN keuzes maken in wat voor KIEN belangrijk is en bijdraagt aan het realiseren van de beoogde kwaliteit.

2. BEANTWOORDING VRAGEN

Onderstaande vragen zijn ingediend door u of door een collega-marktpartij.

Nr.	Onderwerp	Vraag & antwoord
1.	Algemeen	Kunt u aangeven hoeveel lokale breakouts er zijn van en naar uw datacenter? <i>KIEN heeft één (redundante) breakout naar het internet vanuit het datacenter. Ook is er van het datacenter één breakout van het datacenter naar het achterliggende netwerk.</i>
2.	Algemeen	Wat is de gemiddelde load (troughput) per breakout? <i>Op doordeweekse dagen gaat gemiddeld 3 Gb/s via de centrale breakout naar het internet toe.</i> <i>De load vanaf de locaties naar de MER (main equipment room)/ datacenter heeft vergelijkbare waarden.</i>
3.	Vraag 7	Welke software bedoelt KIEN hier? Is dit de software die de aanbieder gebruikt in haar dienstverlening? Als dit zo is, hoe dienen wij deze vraag dan te interpreteren? Vraagt KIEN hier naar de eisen die wij stellen aan deze software? Indien het niet de software betreft die de aanbieder gebruikt in haar dienstverlening, welke software wordt dan wel bedoeld?" <i>KIEN bedoelt hier inderdaad de software mee die de dienstverlener gebruikt bij haar dienstverlening.</i>
4.	Vraag 12	Het is op basis van de thans door KIEN verstrekte informatie moeilijk zo niet onmogelijk om enige indicatie van het benodigde budget of een bandbreedte daarin te geven. Is het mogelijk dat KIEN – voor zover voorhanden – meer informatie deelt die in het kader van het benodigde budget relevant (kunnen) zijn. Te denken valt aan: •De gemiddelde hoeveelheid data per seconde die over (het relevante deel van) de netwerken gaat •Het aantal verwachte security events/alerts per dag

•Het aantal zelfstandige (niet gedeelde) netwerken binnen de verschillende locaties.

Met betrekking tot uw eerste sub vraag: zie het antwoord op de vragen #1 en #2.

Met betrekking tot het aantal te verwachten security events per dag heeft KIEN geen informatie beschikbaar.

KIEN levert één (gesegmenteerd) netwerk, wat beschikbaar is op de verschillende locaties. Iedere locatie heeft 10.x.0.0/16 toegewezen gekregen. Binnen deze reeks bestaan er standaard VLANs voor: werkplekken, printers, gebouwbeheersystemen, camera's, a-v. enzovoort.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

5.	Vraag 12	Hebben de afzonderlijke locaties break-out naar het internet of is dat centraal vanuit het SSC geregeld?
----	----------	---

KIEN heeft voor haar leden één Enterprise-netwerk met één breakout naar het internet. Daarnaast is er één (klein) speciaal netwerk wat volledig los staat van het Enterprise-netwerk met een eigen breakout.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

6.	Vraag 12	Indien de afzonderlijke locaties een local break-out hebben wordt deze voor als het netwerkverkeer gebruikt of is dit selectief?
----	----------	---

Zie het antwoord op vraag #1 en #2.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

7.	Vraag 12	Is er ruimte en mogelijkheid om op alle locaties met lokale break-out om een virtuele of fysieke sensor te plaatsen?
----	----------	---

N.v.t.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

8.	Vraag 12	Hebben alle leerlingen ook een AD account?
----	----------	---

Ja, (bijna) alle leerlingen hebben een AD-account.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|----|----------|--|
| 9. | Vraag 12 | Zitten de medewerkers en de leerlingen in een Aparte AD omgeving
<i>Neen, er is één AD met daarbinnen meerdere Azure AD's.</i> |
|----|----------|--|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|--|
| 10. | Vraag 12 | Hoeveel AD accounts zijn er in totaal?
<i>KIEN beheert in totaal circa 35.000 AD-accounts.</i> |
|-----|----------|--|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 11. | Vraag 12 | Kan er indicatief aangeven worden wat het gemiddelde volume van het totale ingaande en uitgaande netwerk verkeer is?
<i>Zie het antwoord op vraag #1 en #2.</i> |
|-----|----------|---|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|--|
| 12. | Algemeen | Wat voor looptijd van de dienst heeft KIEN voor ogen?
<i>Op deze vraag kan KIEN in deze fase nog geen concreet antwoord geven. De strategie die KIEN op dit domein zal kiezen is onder andere afhankelijk van de informatie die KIEN via deze marktconsultatie ontvangt.</i>

<i>Over het algemeen ziet KIEN meerwaarde in het aangaan van een partnerschap voor een langere periode met een leverancier. Uiteraard neemt KIEN hierbij beperkingen die het aanbestedingsrecht stelt aan de duur en omvang van opdrachten in acht. Daarnaast geldt dat bij KIEN op dit moment het beeld bestaat dat binnen het securitydomein er veel innovatie plaatsvindt. Dit kan mogelijk aanleiding zijn om de looptijd van de overeenkomst te beperken. Het afnemen van een dienst die niet langer een passende oplossing biedt is immers niet wenselijk.</i> |
|-----|----------|--|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 13. | Algemeen | Is het toegestaan dat de voertaal vanuit de te leveren dienst (de operatie) Engelstalig is?
<i>Hierover heeft KIEN nog geen definitief besluit genomen.</i> |
|-----|----------|---|

KIEN vindt het belangrijk dat de communicatie met een leverancier (ook in de operatie) duidelijk is. Op dit moment neigt KIEN naar het akkoord gaan met Engels als voertaal, mits dit niet met een zwaar accent wordt gesproken. Beide partijen moeten elkaar absoluut kunnen begrijpen.

Nr.	Onderwerp	Vraag & antwoord
14.	Algemeen	Is het toegestaan dat de eventuele SOC locatie buiten Nederland, maar binnen de EU is? <i>Hierover heeft KIEN zich nog geen mening gevormd. Wij kunnen ons voorstellen dat beide varianten kunnen bijdragen aan de kwaliteit van de dienstverlening. KIEN laat zich graag over de mogelijkheden informeren.</i>

Nr.	Onderwerp	Vraag & antwoord
15.	Algemeen	Nemen alle deelnemers (Scholen) altijd de NDR-dienst straks af of is dit een optionele dienst vanuit KIEN? <i>Het is de verantwoordelijkheid van KIEN om te zorgen voor een betrouwbare en veilige infrastructuur voor haar leden.</i> <i>De NDR SOC-dienstverlening zal dus onderdeel uitmaken van de standaard dienst van KIEN. Het is niet mogelijk voor een school om hierin een keuze te maken.</i>

Nr.	Onderwerp	Vraag & antwoord
16.	Algemeen	Kien vraagt een Netwerk Detectie & Response (NDR) dienst uit, beheerd vanuit een extern SOC. Tevens geeft Kien aan een groeistrategie te zien, waarbij NDR uiteindelijk evolueert naar een volwaardige SOC oplossing. Alleen een NDR oplossing bestrijkt een beperkt deel van het huidige dreigingslandschap. Een MDR oplossing, waarbij opdrachtnemers naast het netwerk ook de overige aspecten vanuit het SSC qua Cyber Security "Prevent-Detect-Response" meenemen is o.i. een betere oplossing. Het is hierbij de taak van de opdrachtnemer om de oplossing voldoende wendbaar te maken om effectief te zijn in het huidige dreigingslandschap. Hiervoor zijn zeer geschikte partijen en oplossingen in de markt. Ziet Kien mogelijkheden om een dergelijke dienst af te nemen?

Neen, KIEN ziet hier in deze fase geen mogelijkheid toe. Indien u mogelijkheden ziet binnen het door KIEN gestelde budget zijn wij uiteraard nieuwsgierig naar uw aanbeveling en zienswijze.

Daarbij merkt KIEN op dat er grote verschillen bestaan tussen marktpartijen over wat de definitie en scope van een NDR (-dienst) evenzo geldt dit voor MDR of XDR. De ene partij ziet MDR als een product, de ander als een (SOC)-dienst. Of TDR als een apart product of dienst wordt gezien wisselt eveneens per leverancier. Eerder eigen onderzoek laat ook grote verschillen zien met betrekking tot de (al dan niet AI-gedreven, geautomatiseerde) mate van 'Response' binnen een product of dienst. Deze verschillende zienswijzen zijn mede aanleiding voor deze marktconsultatie geweest.

KIEN legt de focus voornamelijk op NDR SOC-dienstverlening. De vragen uit de marktconsultatie blijven hiermee ongewijzigd.

Nr.	Onderwerp	Vraag & antwoord
17.	3.4 Technische middelen/ vraag 12	U geeft in 3.4 TECHNISCHE MIDDELEN aan dat u weinig technische gegevens deelt vanwege veiligheidsoverwegingen, wat begrijpelijk is. Voor een goede beantwoording van de MC als geheel, en specifiek vraag 12, zouden wij toch graag aanvullende informatie ontvangen met betrekking tot onder andere de omvang en inrichting van uw huidige netwerkinfrastructuur. Kunt u hier iets meer over vertellen en aangeven/schatten om hoeveel werkplekken en/of servers het gaat die beveiligd zouden moeten worden met de Managed Netwerk Detectie en Response oplossing. <i>KIEN beheert ongeveer 8000 Windows werkplekken (desktops & laptops), ongeveer 8000 Chromebook, < 500 Mac OS apparaten en 1600 iOS devices. Het aantal beheerde Android devices is nog laag maar hierin voorziet KIEN wel groei in de nabije toekomst.</i> <i>Deze aantallen zijn exclusief BYOD's (vo leerlingen en mbo-studenten hebben veelal eigen apparatuur.)</i> <i>Het aantal servers betreft ongeveer 300 (gevirtualiseerd).</i> <i>KIEN hoort graag van marktpartijen welke scope zij hierin aan zouden brengen bij de gevraagde NDR-oplossing.</i> <i>Zie ook het antwoord op vraag #1 en #2.</i>

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 18. | Algemeen | Welke beveiligingsoplossingen gebruikt u momenteel om bedreigingen te detecteren en aan te pakken? |
|-----|----------|---|

Op deze vraag willen wij niet antwoorden. U mag er van uitgaan dat KIEN met producten van gerenommeerde vendors werkt en dat firewalls, endpoint security, netwerksegmentatie, MFA enzovoort geïmplementeerd en operationeel zijn.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 19. | Algemeen | Bent u tevreden met de effectiviteit en prestaties van uw huidige beveiligingsoplossingen? |
|-----|----------|---|

Deze vraag is dermate algemeen geformuleerd dat het voor ons niet mogelijk is deze te beantwoorden.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 20. | Algemeen | Is uw organisatie op zoek naar een NDR-oplossing die kan integreren met bestaande beveiligingsproducten? |
|-----|----------|---|

KIEN is zeker geïnteresseerd in mogelijkheden die bijdragen aan automatisering en orkestratie binnen een SOC-dienstverlening. We kunnen ons goed voorstellen dat informatie afkomstig uit meerdere (waaronder al aanwezige) securityoplossingen hieraan bijdraagt.

In dat kader is KIEN voorstander van producten die werken met open standaarden.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 21. | Algemeen | Zijn er specifieke systemen of tools waarmee de NDR-oplossing moet kunnen samenwerken? |
|-----|----------|---|

Ja, dat is gewenst, bijvoorbeeld de aanwezige EDR-oplossingen.

Daarom heeft KIEN een voorkeur voor producten die werken op basis van open standaarden. In een eventuele vervolprocedure verwacht KIEN meer gedetailleerde informatie over de infrastructuur en de daarbinnen aanwezige componenten te kunnen delen.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

22.	Juridisch	Welke brancheregulering en wet- en regelgeving zijn van toepassing op uw organisatie met betrekking tot gegevensbeveiliging?
-----	-----------	---

"Met betrekking tot informatiebeveiliging wil KIEN uiteraard voldoen aan alle van toepassing zijnde relevante Nederlandse en Europese wet- en regelgeving waaronder:

- *Algemene Verordening Gegevensbescherming (AVG);*
- *Archiefwet;*
- *Auteurswet;*
- *Branchecode goed bestuur MBO, mbo raad;*
- *Databankenwet;*
- *Grondwet;*
- *Koppelingswet;*
- *Telecommunicatiewet;*
- *Wetboek van Strafrecht;*
- *Wet educatie en beroepsvorming WEB;*
- *Wet Computercriminaliteit III;*
- *Wet op het onderwijstoezicht;*
- *Wet op het voortgezet onderwijs;*
- *Wet op het primair onderwijs.*

Naast bovenstaande wet- en regelgeving zijn ook de normkaders voor informatiebeveiliging en privacy zoals deze in het funderend onderwijs en mbo worden toegepast (beide gebaseerd op het NBA-model) relevant.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

23.	Juridisch	Moet de NDR-oplossing voldoen aan specifieke compliance-vereisten?
-----	-----------	---

KIEN beschikt over een cybersecurityverzekering en voldoet derhalve aan de voorwaarden die de verzekeraar stelt.

Zie ook het antwoord op vraag #22.

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

24.	Algemeen	Heeft uw team specifieke training nodig om effectief gebruik te kunnen maken van de NDR-oplossing?
-----	----------	---

KIEN voert een actief kennisontwikkelingsbeleid. Om op deze vraag een passend antwoord te kunnen geven is het noodzakelijk dat KIEN

weet wat de mogelijkheden van een NDR SOC-dienstverlening er in de markt aanwezig zijn. KIEN kan zich, afhankelijk van de complexiteit van de geboden oplossing en de demarcatie van verantwoordelijkheden, voorstellen dat trainingen noodzakelijk zijn.

KIEN acht het waarschijnlijk dat in een mogelijk vervolgtraject expliciet naar de mogelijkheden van kennisontwikkeling zal worden gevraagd.

Nr.	Onderwerp	Vraag & antwoord
25.	Algemeen	Wat zijn uw verwachtingen met betrekking tot de aangeboden technische ondersteuning? KIEN heeft deze marktconsultatie gepubliceerd om inzicht te krijgen in de mogelijkheden bij een NDR SOC-dienst. In het algemeen geldt dat KIEN een SSC heeft met goed opgeleid personeel. Van partners wordt vooral tweedelijns en/of derdelijns support verwacht. Directe toegang tot het passende support level is een criterium wat voor KIEN van belang is.
26.	Algemeen	De hoofdaannemer wenst in te schrijven met de SOC dienstverlening van een partner. Is dit akkoord? KIEN houdt zich bij het inkopen van producten en diensten aan de geldende wet- en regelgeving, waaronder de Gids proportionaliteit. Zie vraag 13 van onze marktconsultatie. Wij zien uit naar uw antwoord.
27.	Algemeen	In hoeverre is “proven” technologie een vereiste? Denk aan erkenning in bijvoorbeeld Gartner’s NDR Marketguide of Forrester’s NDR wave. KIEN gebruikt deze marktconsultatie om meer inzicht te krijgen in de huidige stand van NDR-technologie. Op basis van de door de markt verstrekte informatie hoopt KIEN te kunnen bepalen in hoeverre er binnen dit domein sprake is van 'proven technology' en inzicht te krijgen in het huidige volwassenheidsniveau van de techniek. KIEN acht het waarschijnlijk dat er bij een mogelijke toekomstige aanbestedingsprocedure eisen gesteld zullen gaan worden aan de

techniek waaraan alleen enterprise level oplossingen kunnen voldoen."

Nr.	Onderwerp	Vraag & antwoord
28.	Algemeen	Hoeveel sites verwacht KIEN aan te sluiten binnen scope van dit project? <i>KIEN is geïnteresseerd in een centrale oplossing. Er is geen sprake van lokale breakouts.</i> <i>Zie ook het antwoord op vraag #1 en vraag #2.</i>

Nr.	Onderwerp	Vraag & antwoord
29.	Algemeen	Heeft KIEN reeds een beeld over welke verkeersstromen binnen scope moeten vallen voor dit project (denk aan het aantal sites, VLANs voor docenten, studenten, servers etc..)? <i>KIEN wil door deze marktconsultatie een beeld krijgen van wat de technische en organisatorische mogelijkheden zijn. Ook zijn we benieuwd naar de mogelijkheden zijn met betrekking tot de scope binnen het beschikbare budget. Beheerde devices en genoemde clouddiensten vallen sowieso binnen de beoogde scope.</i> <i>Zie ook de beantwoording van de andere vragen met betrekking tot vraag 12 uit de marktconsultatie.</i>

Nr.	Onderwerp	Vraag & antwoord
30.	Algemeen	Ziet KIEN meerwaarde voor haar beoordelingscriteria wanneer de aanbieder ook inspectie voor cloud diensten zoals M365 en Google workspace kan aanbieden binnen eenzelfde SOC dienstverlening? <i>Ja, inspectie van clouddiensten is gewenst.</i> <i>Zie ook vraag 3 in paragraaf 3.3 en paragraaf 3.4 van het marktconsultatiedocument.</i>

Nr.	Onderwerp	Vraag & antwoord
31.	Algemeen	Is er al een beeld van de hoeveelheid verkeer in Mbps per site? Zo ja, wat zijn de volumes? <i>Zie het antwoord op vraag #1 en vraag #2.</i>

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|--|---|
| 32. | | Welke third-party integraties zijn belangrijk voor KIEN?
<i>Zie het antwoord op vraag #30. Zie ook het antwoord op vraag #20.</i> |
|-----|--|---|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 33. | Algemeen | In hoeverre wil KIEN naast enkel netwerk metadata ook inspectie en analyse kunnen uitvoeren op (zero day) bestanden die via het netwerk getransporteerd worden middels sandboxing methodieken?
<i>KIEN verneemt graag van marktpartijen wat de mogelijkheden binnen het beschikbare budget zijn en wanneer het inzetten dergelijke technieken tot meerwaarde is voor de organisatie en haar dienstverlening.</i>

<i>KIEN is ook geïnteresseerd in deze en vergelijkbare methodieken wanneer dit in een groeiscenario kan worden toegepast.</i> |
|-----|----------|---|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 34. | Algemeen | Klopt het dat de verwachting van KIEN vanuit de dienstverlener zich beperkt tot de NDR oplossing?
<i>Ja, dit klopt. Echter, wij hebben gemerkt dat er in de markt grote verschillen bestaan over de definitie van NDR en wat binnen of buiten de scope van een NDR-oplossing valt. Ditzelfde geldt ook voor de definitie en gehanteerde scope van een SOC-dienst.</i>

<i>In dat kader voorziet KIEN een groeistrategie waarbij het ontwikkelen van een SOC-dienst (gezamenlijk met partners) waarbinnen NDR zich zal ontwikkelen tot bijvoorbeeld een XDR of MDR in de lijn der verwachtingen ligt.</i>

<i>Zie ook het antwoord op vraag #16.</i> |
|-----|----------|---|

Nr.	Onderwerp	Vraag & antwoord
-----	-----------	------------------

- | | | |
|-----|----------|---|
| 35. | Algemeen | Hoe ziet het vervolg traject er uit? Worden specifieke partijen uitgenodigd voor verdere toelichting, komt er een RFP via Tendered middels standaard europese aanbestedingseisen?
<i>Of er sprake zal zijn van een vervolgtraject en hoe een eventueel vervolgtraject eruit zal zien is afhankelijk van de resultaten van deze marktconsultatie. Een niet-openbare procedure ligt – gezien de</i> |
|-----|----------|---|

hoeveelheid vertrouwelijke informatie die geïnteresseerde partijen nodig hebben om tot een passend aanbod te komen – in de lijn der verwachtingen.

Zie ook paragraaf 2.2 en paragraaf 2.11 van het marktconsultatiedocument.

Nr.	Onderwerp	Vraag & antwoord
36.	Algemeen	Wanneer wenst KIEN een managed NDR oplossing geïmplementeerd te hebben? <i>Zo spoedig mogelijk. Uiteraard met in acht neming van geldende termijnen. Hierbij geldt ook dat de kwaliteit van het eindresultaat boven de snelheid van implementatie gaat.</i>

Nr.	Onderwerp	Vraag & antwoord
37.	1.3 Budget	Kan KIEN het budget verder toelichten? Betreft dit budget bijvoorbeeld enkel de SOC-dienstverlening, exclusief benodigde licenties voor securityproducten? <i>Betreft het beoogde budget voor de SOC-dienst, inclusief licenties voor de door u in te zetten securityproducten zoals sensoren en andere tooling. Het budget is exclusief kosten van reeds aanwezige securityproducten zoals firewalls, endpoint protectie enzovoort.</i>

Nr.	Onderwerp	Vraag & antwoord
38.	1.3 Budget	Kan KIEN verder uitweiden over mogelijke licenties en producten waarover al beschikking is? Dergelijke licenties/producten bevatten mogelijk al toegang tot securityfeatures en -tooling die helpen bij het effectief inzetten van het beschikbare budget. a) Heeft KIEN, als academische instelling, bijvoorbeeld de beschikking over een Microsoft E5 licentie? b) Zijn er bijvoorbeeld verschillen in de licenties tussen medewerkers en studenten?" <i>KIEN beschikt voor eigen medewerkers over A5-licenties, op de scholen hebben medewerkers en studenten een A3-licentie.</i> <i>Nadere details over aanwezige security-oplossingen zullen in een mogelijke vervolprocedure worden gedeeld.</i>

Nr.	Onderwerp	Vraag & antwoord
39.	1.4 Visie en doelstelling	In onze visie en ervaring is NDR 1 puzzelstukje. Daarnaast is namelijk ook zicht nodig op de hosts in uw IT landschap. a) Hoe kijkt KIEN aan tegen Endpoint Detection & Response (EDR)? b) Verwacht KIEN een totaaloplossing van het SOC, waarbij ook ruimte is voor bijv. EDR producten? Of heeft KIEN op dit moment wellicht bewust gekozen om met een kleine stap te beginnen om zichtbaarheid te creëren? <i>Wij begrijpen uw vraag. Afhankelijk van het type endpoint en positionering van het endpoint binnen het netwerk heeft KIEN securitymaatregelen genomen. De mate van 'response' binnen de oplossingen is mede afhankelijk van de fase van de life cycle waarbinnen de producten zich bevinden. Integratie, of verwerken van alerts vanuit de EDR is gewenst.</i> <i>Met betrekking tot het tweede deel van uw vraag klopt het dat KIEN waakt voor het aanschaffen van een mammoettanker. Het uitbouwen van het security portfolio in kleinere stappen - waarbij er oog is voor de security architectuur en dus de onderlinge samenhang van de elementen, heeft de voorkeur.</i> <i>Zie ook het antwoord op vraag #34.</i>

Nr.	Onderwerp	Vraag & antwoord
40.	1.4 Visie en doelstelling	Heeft KIEN de opzet (bijv. met de inrichting van het CERT) en ervaring om te reageren op cyberincidenten, op advies van en met de informatie verwacht van de SOC dienstverlener; of heeft KIEN ook behoefte aan 'boots-on-the-ground' tijdens (grote) incidenten (crisissituaties)? <i>Om in militair jargon te antwoorden: in geval van 'Defcon 1' geldt dat KIEN zeker behoefte heeft aan kennis en kunde, inclusief 'boots-on-the-ground' van haar partners.</i> <i>Uiteraard is dit afhankelijk van de ernst van het incident en de eventuele ontstane crisissituatie.</i>

Nr.	Onderwerp	Vraag & antwoord
41.	1.5 Strategie	KIEN heeft een duidelijke strategie voor ogen, die ons inziens getuigt van realistische groei om de beoogde doelen te halen. In het kader van deze strategie, kan KIEN verder uitweiden hoe het de samenwerking ziet tussen SOC dienstverlener en de eigen operationele organisatie om te reageren op een (kleiner) incident?

a) In dat kader, heeft KIEN bijvoorbeeld een piketdienst die een securityincident kan oppakken?

De verwachting is dat KIEN zeer goed in staat is om actie te ondernemen bij kleinere security incidenten. Bij dergelijke incidenten is onderlinge communicatie tussen KIEN en het SOC van belang.

Met betrekking tot sub vraag a geldt dat er zeker afspraken gemaakt kunnen worden over het reageren op incidenten door een piketdienst.

Nr.	Onderwerp	Vraag & antwoord
42.	1.5 Strategie	Ingrijpen op een securityincident heeft (waarschijnlijk) business impact tot gevolg. Daarvoor is het belangrijk om de organisatie context goed te doorgronden. In hoeverre wenst KIEN dat de eigen operationele organisatie ingrijpt tijdens incidenten? <i>U stelt een logische vraag die lastig te beantwoorden is buiten de context van een samenwerking waarin klant en leverancier elkaars organisatie en dienst kennen. Wanneer zich buiten kantoor tijden een situatie voordoet waarin acuut ingrijpen noodzakelijk is en het SOC kan dit doen dan is dat uiteraard wenselijk. Dit geldt ook voor een scenario waarin ingrijpen slechts een beperkte impact op de business heeft (bijvoorbeeld één device van een persoon of één locatie in quarantaine plaatsen). Bij andere scenario's kan het juist zo zijn dat KIEN de voorkeur geeft aan zelf ingrijpen omdat de eigen medewerkers (waarschijnlijk) beter de impact van de ingreep kunnen beoordelen.</i> <i>Onder welke omstandigheden het SOC ingrijpt of juist slechts detecteert en waarschuwt zou volgens KIEN onderwerp van gesprek moeten zijn en kunnen resulteren in een SLA. KIEN nodigt marktpartijen in hoofdstuk 3, vraag 5 ook uit om hun visie hierop te geven."</i>

Nr.	Onderwerp	Vraag & antwoord
43.	2.4 Planning	Op wat voor termijn wenst KIEN het NDR SOC geïmplementeerd te hebben? <i>Zie het antwoord op vraag 36.</i>
