



Samen ICT voor onderwijs

Bevindingen bij marktconsultatie

Netwerkdetectie & Response
SOC-dienstverlening

Aanbestedende dienst:	Coöperatie KIEN U.A.
Kenmerk:	NDR SOC 2023
Versie:	1.0
Datum:	15 december 2023

RESULTAAT MARKTCONSULTATIE

Op 14 juli 2023 heeft de Coöperatie KIEN U.A. (KIEN®) de markt uitgenodigd om informatie en zienswijzen aan te leveren over de mogelijkheden van Security Operation Center/ SOC-dienstverlening gebaseerd op Network Detection and Response (NDR) technologie.

In totaal hebben 28 partijen zich als geïnteresseerde gemeld waarvan 16 partijen actief hebben deelgenomen aan de marktconsultatie. Het aantal reacties heeft de verwachtingen van KIEN overtroffen. Dat geldt ook voor de (zeer) uitgebreide beantwoording van de door KIEN gestelde vragen. KIEN dankt alle partijen die de moeite hebben genomen om KIEN te informeren en het daarmee mogelijk te maken een weloverwogen vervolg te geven aan de marktconsultatie.

In dit document deelt KIEN de samengevatte resultaten.

ALGEMEEN

KIEN beoogde met de marktconsultatie antwoorden te krijgen op een aantal vragen die er binnen de organisatie speelden met betrekking tot SOC-dienstverlening. De marktconsultatie heeft veel van de aanwezige vragen beantwoord maar heeft ook nieuwe vragen opgeroepen.

Met betrekking tot technische maatregelen is er veel duidelijkheid gekomen. Dit geldt ook voor de visie die verschillende leveranciers hebben op samenwerking op dit domein. Met betrekking tot cloudplatformen in een vroeg stadium binnen scope van de SOC-dienst plaatsen blijven vragen bestaan. Vanuit de markt is bevestigend gereageerd op de keuze van KIEN om op dit moment in te zetten op het implementeren van NDR naast EDR en de telemetriedata die dit oplevert te laten analyseren door een SOC.

Omtrent innovaties op SOC-diensten is het beeld tweeslachtig: met name rondom het volwassenheidsniveau van een aantal dienstverleners, triage-technieken en rijkdom aan mogelijke diensten is er meer mogelijk dan KIEN had voorzien. Tegelijkertijd lijkt de mate van automatisering en orkestratie met betrekking tot *response*, in een minder vergevorderd stadium dan verwacht.

Het aantal partijen wat ervaring heeft binnen de onderwijssector en daar specifieke inzichten over deelt is klein. Dit geldt zeker voor ervaring in het funderend onderwijs.

Over de kostendrivers zijn duidelijke antwoorden vanuit de markt gekomen. Hierbij moet een voorbehoud worden gemaakt: zonder zeer duidelijk gemarkeerde scope van de opdracht bestaat het risico dat de verwachtingen tussen het gevraagde en geleverde niet overeenkomen. Het hebben van een duidelijk geformuleerde startsituatie en groeiscenario is daarom van groot belang.

DE MARKTPARTIJEN

Een divers pallet aan marktpartijen heeft gereageerd op de marktconsultatie. Onder de respondenten zijn producenten van NDR-sensoren en SOC-platformen die wereldwijd opereren, softwarebrokers die als makelaar in de markt opereren en resellers met een sterke lokale focus die gebruik maken van door vendors ontwikkelde tooling. Een enkele respondent gebruikt zelf ontwikkelde sensoren.

Ook in organisatiegrootte en omvang van het klantenbestand zijn grote verschillen waarneembaar. De grootste organisatie heeft honderden medewerkers op meerdere SOC-locaties en bedient duizenden klanten. Aan de andere kant zijn er partijen die minder dan vijf medewerkers op het SOC hebben werken en voor slechts een paar klanten SOC-dienstverlening leveren.

Ondanks het feit dat KIEN bij de marktconsultatie heeft aangegeven sterke bedenkingen te hebben bij een SIEM-gebaseerde oplossingen, zijn er toch een aantal respondenten die een SIEM binnen de scope van de geboden oplossing plaatsen. Soms wordt dit met motivatie gedaan, soms ook zonder verdere motivatie.

Het merendeel van de leveranciers biedt een SOC-dienst waarbij events geclassificeerd worden. Afhankelijk van de classificaties volgen vervolgacties. Ook werken de meeste SOC's volgens het 24/7 eyes-on-glass-principe en maken onderscheid tussen eerste, tweede, derdelijns en coördinatie functies binnen het SOC. Een beperkt aantal leveranciers is van mening dat een SOC-dienst kan worden geleverd zonder 24/7 bemensing en gaan niet in op de organisatorische inrichting van het SOC.

Van de leveranciers die een 24/7 bemensende SOC-dienst aanbieden hanteert een deel het follow-the-sun-principe waarbij wereldwijd SOC-locaties operationeel zijn. Daarnaast is er een aanzienlijk aantal leveranciers die vanuit één – veelal in Nederland gesitueerd SOC – de diensten levert.

Met betrekking tot ervaring en volwassenheid zijn eveneens grote verschillen waarneembaar. Een aantal organisatie heeft jarenlange ervaring binnen de security dienstverlening waarbij andere organisaties recent de SOC-dienstverlening aan het dienstenportfolio van de organisatie hebben toegevoegd aan het dienstenportfolio.

ARCHITECTUURMODELLEN

Het overgrote deel van de leveranciers maakt bij de inrichting van hun diensten gebruik van de SOC Visibility Triad, het Mitre&Att&ck framework of hanteert een Zero Trust Model architectuur.

In dat kader is een groot aantal leveranciers van mening dat voor KIEN, het implementeren van een NDR-oplossing een logische stap is in het continue verbeteren van de security. Met name de SOC Visibility Triad biedt perspectief in het formuleren van een groeiscenario voor KIEN.

LOGBRONNEN

De Aanbestedende dienst constateert dat er grote verschillen zijn tussen leveranciers met betrekking tot de keuze voor de technische oplossingen. Er zijn partijen die zeer duidelijk hun product- en dienstenportfolio vormgeven gecentreerd rondom de producten van één vendor met als argument dat dit de meest waardevolle data oplevert.

Enkele partijen geven aan praktisch gezien loggegevens van derde partijen niet, of slechts zeer beperkt te kunnen integreren in de dienstverlening. Aan de andere kant zijn er leveranciers die een uitgesproken agnostische benadering van techniek hebben en zodoende ook slechts de beperking van de kwaliteit van de aangeleverde loggegevens uit bronnen van derden als beperking zien.

Vrijwel alle leveranciers adviseren om naast de telemetriedata uit de NDR-sensor(en) ook in een vroeg stadium EDR-telemetriedata onderdeel te maken van de SOC-dienst. Hiermee wordt de bescherming van kroonjuwelen van een organisatie significant vergroot.

In een verder groeiscenario wordt de integratie van telemetriedata vanuit andere bronnen zoals cloudplatformen, email, firewall en IAM geadviseerd. Hierbij wordt door een aantal partijen aangegeven kritisch te zijn met betrekking tot de scope. Niet alle data vanuit een logbron hoeft aan inspectie te worden onderworpen. Het beperken van de te analyseren data zorgt voor minder false positives en houdt de kosten beheersbaar.

Met betrekking tot de positionering van BYOD lopen de visies uiteen. Er zijn partijen die adviseren deze apparatuur buiten scope te plaatsen terwijl andere partijen er belang aan hechten deze apparatuur binnen scope te plaatsen.

Voor de Aanbestedende dienst geldt dat, een keuze voor een oplossing die (grotendeels) gebaseerd is op de techniek van één vendor het risico van een desinvestering t.a.v. de huidige installed base en een vendor lock-in met zich meebrengt. Tegelijkertijd onderkent de Aanbestedende dienst het feit dat standaardisatie kan bijdragen aan het optimaliseren van securitymaatregelen.

TECHNIEK

Het merendeel van de respondenten heeft een voorkeur voor een technische oplossing van een beperkt aantal vendors. Hierbij zijn genoemd: Corelight, Extrahop, FortiNet, Palo Alto Cortex XDR, Sophos XDR, Trend Micro, Vectra AI, Zeek en intern ontwikkelde oplossingen op basis van open standaarden. Hierbij worden niet alleen NDR-sensoren maar ook platformen t.b.v. de SOC-dienst, bijvoorbeeld op basis van XDR, SIEM of SOAR genoemd.

Artificial Intelligence wordt nog niet door alle leveranciers toegepast. De partijen die AI inzetten doen dit vooral met Machine Learning technieken en verwachten dat de gebruikte technieken als laag-risico worden ingeschat.

CERTIFICERING

Als kwaliteitseis voor SOC-dienstverleners wordt door veel marktpartijen geadviseerd om naast de ISO27001 en ISO27002 ook een SOC type 2/3 certificering uit te vragen. Deze certificering richt zich specifiek op processen met betrekking tot securitydienstverlening. Ook ISAE 3402 inclusief Trust Service Criteria en HIPPAA certificering worden ter overweging gedeeld.

AFSPRAKEN RONDOM DIENSTVERLENING

Hoe en waarover gecommuniceerd wordt, wat wordt vastgelegd in een SLA en DAP en welke KPI's worden overeengekomen wisselt sterkt. Bij grote wereldwijd opererende organisaties ligt de focus op operationele afspraken. Bij middelgrote en kleinere organisaties wordt doorgaans meer aandacht gegeven aan communicatie op strategisch en tactisch niveau.

Reactietijd en oplostijd wordt door alle partijen genoemd als KPI maar hierop zijn wel verschillende visies hoe hiermee om te gaan. Dit geldt ook voor de manier waarop er gecommuniceerd wordt n.a.v. security events.

De antwoorden met betrekking tot samenwerking en dienstverlening lopen sterk uiteen: van een duidelijke visie op samenwerking, overlegstructuren, het belang van mandatering en verdeling van verantwoordelijkheden tot focus op wat de klant vooral op orde moet hebben en verwijzing naar de klachtenprocedure.

Bij alle partijen maakt ondersteuning in geval van een (major) incident tot de standaard dienstverlening. Hoe intensief de ondersteuning is wisselt.

AVG & AI ACT

Er is grote consensus in de markt dat het overeenkomen van een verwerkersovereenkomst noodzakelijk is om te kunnen voldoen aan de AVG. Eén partij heeft hier een andere visie op. Ook aanvullende maatregelen in het kader van privacy by design en privacy by default lijken gemeengoed te zijn in de sector. Dit geldt ook voor beleid met betrekking tot integriteit van medewerkers.

Met betrekking tot Artificial Intelligence is de inschatting van het merendeel van de leveranciers dat – indien er gebruik gemaakt wordt van AI – dit in het lichte regime gaat vallen binnen de AI Act.

DUURZAAMHEID

Daar waar partijen zich onderling nauwelijks lijken te onderscheiden als het om privacy gaat zijn er met betrekking tot duurzaamheid grote verschillen waarneembaar. Koplopers op dit onderwerp onderscheiden zich door een actief beleid, geaudit door externe partijen en heldere visie, bijvoorbeeld op basis van Social Development Goals. Tegelijkertijd zijn er partijen die verwijzen naar het beleid van de vendor waarmee wordt samengewerkt zonder

zelf beleid te hebben. Meerdere leveranciers in de sector zijn van mening dat ICT-producten en ICT-dienstverlening per definitie duurzaam zijn.

BUDGET EN KOSTENSTRUCTUUR

Een aantal partijen heeft aangegeven dat het budget van de Aanbestedende dienst niet toereikend is voor de beoogde dienstverlening. Tegelijkertijd zijn er een aantal partijen die aangeven meer dan het gevraagde te kunnen leveren voor het beschikbare budget. Het merendeel van de respondenten geeft aan te verwachten het gevraagde te kunnen leveren maar stellen dat een uitbreiding van het budget tot een significant betere dienstverlening leidt.

Marktpartijen bevestigen de veronderstelde kostenstructuur van eenmalige (implementatie)projectkosten en periodieke kosten. Binnen de periodieke kosten zijn de hoeveel te verwerken data (throughput) en aantal user accounts de kostendrivers. In geval van een hardware sensor zijn zowel koop als verrekening via een maandbedrag mogelijk. Geen van de partijen rekent extra kosten wanneer zij in actie moeten komen naar aanleiding van een (groot) incident.

IMPLEMENTATIE

Ook met betrekking tot de doorlooptijd van de implementatie lopen de antwoorden uiteen. Een enkele leverancier stelt dat de implementatie slechts enkele uren vergt en leveren geen verdere details. Gemiddeld wordt een implementatietijd van ongeveer acht weken genoemd waarbij het merendeel van de tijd wordt gereserveerd voor het finetunen van de dienstverlening.

Geen van de marktpartijen ziet risico's met betrekking tot leveringszekerheid of capaciteitsproblemen in de eigen organisatie. Voor zover er risico's onderkend worden zitten deze aan de zijde van de Aanbestedende dienst.

VOLLEDIGE OPDRACHT

De markt is eensgezind met betrekking tot de interesse in de volledige opdracht of een mogelijk perceel binnen de opdracht: het advies is om niet te splitsen en aan één leverancier te gunnen. Er wordt gewezen op het grote veiligheidsrisico wat met splitsen van de opdracht gepaard gaat. Bij incidenten zouden er conflicten kunnen ontstaan met betrekking tot de veronderstelde verdeling van verantwoordelijkheden.

GESPREKSRONDE

Naar aanleiding van de schriftelijke reacties vanuit de markt heeft KIEN een aantal partijen uitgenodigd om deel te nemen aan een gespreksronde. De selectie hiervoor is gemaakt langs de lijnen van verschillende technische oplossingen.

Dit met als doel om inzicht te krijgen in de vertaling van verschillende technische oplossingen binnen een SOC en om bij volgende stappen een betere scope aan te kunnen brengen en verschillende bouwblokken binnen de SOC-dienstverlening op een logische manier te

organiseren in een groeiscenario. Onder bouwblokken kan worden verstaan; telemetriedata uit andere bronnen dan NDR en EDR maar ook aanvullende diensten zoals gebruik van Threat Intelligence en Forensics diensten.

Uit de gesprekken is naast eerder genoemde zaken naar voren gekomen dat cloud-omgevingen nadrukkelijker om aandacht vragen. Gezien de grote vertegenwoordiging van Microsoft producten binnen het onderwijs (door een gunstige educatie-licentiemodellen) is het van belang hier bij de uitvraag rekening mee te houden. De mate waarin telemetriedata vanuit Microsoft producten kan worden gebruikt wisselt per leverancier.

VERVOLGTRAJECT

Naar aanleiding van de verkregen informatie in de marktconsultatie beraadt KIEN zich op een mogelijke vervolgprocedure. Hierbij wordt een niet-openbare aanbestedingsprocedure als logisch vervolg gezien. Hiervoor zal KIEN selectiecriteria bekendmaken. Bij het formuleren van de selectiecriteria zal KIEN gebruik maken van de verkregen informatie uit deze marktconsultatie en keuzes maken, onder meer met het doel om onderlinge vergelijkbaarheid van toekomstige aanbiedingen te kunnen waarborgen.

Het is zowel zaak om bij de uitvraag het groeiscenario te bewaken als ook duidelijk de scope van de dienstverlening per fase te beschrijven. Dit wordt mede veroorzaakt doordat er in de markt geen vaststaande scope bestaat voor termen zoals MDR, XDR, NDR enzovoort. Wordt dit niet goed gedaan dan bestaat het risico dat er na gunning geen juiste fit blijkt te zijn tussen de behoefte en beschikbare budget van KIEN en het aangeboden of dat het gewenste groeiscenario niet mogelijk blijkt te zijn.

KIEN verwacht een aankondiging van de opdracht in Q1 2024 te doen.