Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Eindverslag marktconsultatie MDR+ dienstverlening

Betreft	**Marktconsultatie MDR+ dienstverlening**
Aanbestedende dienst	Ministerie van Financiën, Concerndirectie Informatievoorziening & Openbaarmaking (CDIO)
Kenmerk	201865004.015.069
Versie	1.0
Datum	12-10-2026

Inleiding

Het ministerie van Financiën, Concerndirectie Informatievoorziening & Openbaarmaking (CDIO), heeft via de Rijksinkoopsamenwerking (RIS) een marktconsultatie gehouden over mogelijke Managed Detection and Response (MDR)+ dienstverlening ter ondersteuning van het bestaande interne Security Operations Center (SOC). Dit eindverslag beschrijft het verloop, de geanonimiseerde inzichten uit de reacties van marktpartijen en de voorgenomen vervolgstappen.

Doel van de marktconsultatie

De marktconsultatie onderzoekt welke scope, kavelindeling, randvoorwaarden en aanbestedingsstrategie passend zijn. Het ministerie wil de haalbaarheid van mogelijke eisen toetsen en een eventuele uitvraag marktconform en proportioneel voorbereiden. De beoogde MDR+ dienstverlening ondersteunt het interne SOC; de centrale regie op logging, applicatieve use-cases, interne threat intelligence, prioritering en opvolging blijft bij het ministerie.

Verloop van de marktconsultatie

De marktconsultatie is op 15 juni 2026 via TenderNed gestart. De schriftelijke beantwoording was voorzien uiterlijk 10 september 2026. De Nota van Inlichtingen bevat 37 genummerde vragen en antwoorden. Voor dit verslag zijn 13 afzonderlijke schriftelijke marktbijdragen beoordeeld. Daarnaast zijn verdiepende interviewstukken van drie marktpartijen verwerkt.

De vragen en antwoorden uit de Nota van Inlichtingen verduidelijken onder meer dat de functionele onderzoeksscope nog geen verplichte basisdienst of definitieve kavelindeling vastlegt. De eventuele toepasselijkheid van ABRO-gerelateerde eisen hangt volgens de beantwoording af van een risicoanalyse. De schriftelijke reacties en interviewstukken zijn thematisch samengevat; leveranciersnamen, individuele oplossingen en commercieel gevoelige gegevens zijn buiten de vraaggewijze samenvatting gehouden.

Belangrijkste inzichten

De markt onderschrijft in hoofdzaak een co-managed MDR-model: externe 24/7 capaciteit, triage, specialistisch onderzoek en gezamenlijke verbetering van detecties, met centrale regie, risicoweging en besluiten met bedrijfsimpact bij het ministerie. Er is brede steun voor een duidelijke operationele kern met gefaseerd inzetbare onderdelen. De markt verschilt over de precieze basisomvang, de technische plek van detectie en casemanagement naast Splunk, de hoeveelheid telemetrie die naar Splunk moet en de mate van bundeling van NDR, exposure management en forensische ondersteuning. Een

functionele uitvraag met toetsbare integratie-, gegevens- en continuïteitseisen laat ruimte voor deze verschillende uitvoeringsmodellen.

Vraaggewijze samenvatting van de marktconsultatie

Hieronder worden de ontvangen antwoorden per vraag geanonimiseerd samengevat. De samenvatting bevat ook relevante inzichten uit de individuele gesprekken. Vertrouwelijke bedrijfsinformatie, herleidbare gegevens en individuele prijsopgaven zijn hierin niet opgenomen.

Vraag 1 – Scope en kavelindeling MDR+

Vraagstelling: Het ministerie onderzoekt een MDR+ dienstverlening bestaande uit Managed Detection and Response, XDR/EDR of vergelijkbare host monitoring, Network Detection and Response, exposure management en forensische ondersteuning op afroep. Welke rol ziet u voor MDR+ dienstverlening bij de doorontwikkeling van een middelgroot SOC binnen de rijksoverheid in de komende drie tot vijf jaar, in het bijzonder richting een hoger volwassenheidsniveau en meer threat-based werken? Herkent u deze scope als logisch en marktconform voor een organisatie met een bestaand intern SOC? Welke onderdelen moeten volgens u minimaal onderdeel zijn van de basisdienstverlening en welke onderdelen kunnen beter optioneel, modulair of als afzonderlijk kavel worden opgenomen? Adviseert u MDR, XDR/EDR, NDR, exposure management en forensische ondersteuning als één geïntegreerde dienst uit te vragen, of juist als afzonderlijke kavels of percelen? Licht uw antwoord toe.

Antwoorden

De reacties herkennen MDR+ als een logische versterking van een bestaand SOC. De terugkerende kern bestaat uit 24/7 monitoring, triage, escalatie, integratie met het interne SOC, operationele dreigingsinformatie en voortdurende verbetering van detecties. Meerdere partijen plaatsen EDR/XDR in die kern. Over NDR, exposure management, geavanceerde threat hunting en forensische inzet bestaat minder overeenstemming: sommige partijen nemen deze standaard op, andere adviseren modules of inzet op afroep. Een samenhangende operationele keten geniet brede steun, maar daarvoor hoeft niet ieder technisch onderdeel als één ondeelbare dienst te worden ingekocht.

Vraag 2 – Positionering ten opzichte van het bestaande SOC

Vraagstelling: Het ministerie beschikt over een bestaand intern Security Operations Center. De beoogde MDR+ dienstverlening moet dit SOC ondersteunen en versterken. Het ministerie zoekt geen volledige uitbesteding van het SOC. Waar ligt volgens u de natuurlijke knip tussen de externe MDR+ dienstverlener en het interne SOC van het ministerie? Welke verantwoordelijkheden moeten volgens u bij opdrachtgever blijven om regie, kennisbehoud, onafhankelijkheid en continuïteit te borgen? Welke informatie, processen en besluitvormingslijnen heeft u van opdrachtgever nodig om de dienstverlening effectief te kunnen leveren? Hoe ziet u de communicatielijnen en taakverdeling tussen de externe MDR+ dienstverlener, het interne SOC, de IBP/CISO-functie, IT-beheer, leveranciers en andere relevante organisatieonderdelen?

Antwoorden

De natuurlijke knip ligt volgens de meeste respondenten tussen externe 24/7 uitvoering en interne regie. De dienstverlener monitort, valideert, verrijkt, onderzoekt en escaleert; het ministerie blijft eigenaar van prioriteiten, kroonjuwelen, loggingstrategie, organisatiespecifieke use-cases, interne intelligence, risicoacceptatie en besluiten met substantiële bedrijfsimpact. Detection engineering en threat hunting worden vaak gezamenlijk ingericht. Voor effectieve samenwerking zijn een actuele CMDB en assetclassificatie, contactlijsten, escalatiematrix, toegang tot relevante data en een bevoegd 24/7 aanspreekpunt nodig.

Vraag 3 - Integratie met Splunk, SIEM en bestaande SOC-tooling

Vraagstelling: Binnen de bestaande SOC-architectuur is Splunk leidend voor centrale logging, correlatie, rapportage, use-case management en opvolging van securitymeldingen. De centrale regie op logging, applicatieve use-cases en interne threat intelligence blijft bij het ministerie. Hoe sluit uw dienstverlening aan op een Splunk-gedreven SOC-architectuur waarin Splunk leidend blijft voor

logging, correlatie, rapportage en interne SOC-workflows? Welke integratievorm adviseert u: meldingen naar Splunk, volledige telemetrie naar Splunk, bidirectionele koppeling, integratie via API's of een andere architectuur? Welke open standaarden, API's, exportformaten en datamodellen ondersteunt u voor koppeling met SIEM, ITSM/Topdesk, CMDB, CTI-platformen en rapportagevoorzieningen? Hoe past uw dienstverlening STIX en TAXII toe voor het uitwisselen en verwerken van dreigingsinformatie, en welke technische of procesmatige voorbereiding vraagt dit van opdrachtgever? In welke mate blijft uw dienstverlening effectief functioneren in een hybride of multivendor omgeving waarin MDR, SIEM, XDR/EDR, NDR en/of CTI van verschillende leveranciers afkomstig zijn? Welke technische, organisatorische en contractuele randvoorwaarden zijn daarvoor nodig? Hoe voorkomt u dubbele detecties, dubbele triage en alert fatigue wanneer bestaande SIEM-use-cases actief blijven binnen het interne SOC?

Antwoorden
Partijen kunnen in verschillende mate aansluiten op een Splunk-gedreven SOC. Veel reacties adviseren Splunk als centrale voorziening voor zichtbaarheid, rapportage en interne opvolging, met API-koppelingen, selectieve telemetrie en uitwisseling van verrijkte meldingen en incidentstatus. Volledige ruwe telemetrie naar Splunk wordt door meerdere partijen vanwege volume en kosten afgeraden, terwijl enkele partijen dat juist voor centrale controle adviseren. Sommige dienstverleners werken primair in hun eigen detectie- of casemanagementplatform en koppelen dit met Splunk en ITSM; anderen voeren detectie dichter bij of rechtstreeks in de Splunk-omgeving uit. Open API's, gangbare eventformaten en STIX/TAXII ondersteunen een multivendor inrichting.

Vraag 4 - 24/7 monitoring, triage en ketenopvolging
Vraagstelling: Het ministerie onderzoekt 24/7 monitoring en opvolging door een externe dienstverlener. Alleen monitoring is onvoldoende wanneer alarmering, triage, escalatie, overdracht en besluitvorming niet scherp zijn ingericht. Hoe ziet uw standaard operationele model eruit voor 24/7 monitoring, triage, escalatie en overdracht aan het interne SOC? Welke impact verwacht u van AI-gedreven dreigingen en AI-ondersteunde cybercapaciteiten op detectie, monitoring, triage en opvolging, en welke maatregelen acht u nodig om hierop voorbereid te zijn? Welke afspraken zijn volgens u nodig over P1/P2-incidenten, bereikbaarheid, escalatie, mandaat, reactietijden en eventuele on-site inzet? Hoe richt u de samenwerking in tussen leverancier, intern SOC, IBP/CISO-functie, IT-beheer en eventuele andere ketenpartijen? Welke informatie bevat een door u geëscaleerde melding minimaal, zodat interne analisten direct kunnen handelen?

Antwoorden

24/7 dienstverlening omvat volgens de reacties meer dan alertbewaking: validatie, prioritering, technische analyse, directe escalatie, heldere overdracht en aantoonbare opvolging. Voor P1/P2 zijn vooraf vastgestelde ernstcriteria, contact- en piketstructuur, bevoegdheden, reactietijden en terugvalroutes nodig. De interviews benadrukken één leidende incidentketen over leveranciersplatform, Splunk en ITSM heen. Een geëscaleerde melding bevat minimaal ernst, tijdlijn, betrokken assets, bewijs, context, verrichte acties, resterende onzekerheid en aanbevolen vervolgstappen. AI kan zowel dreigingen versnellen als analyse ondersteunen, maar vereist controle op kwaliteit en menselijk toezicht bij ingrijpende besluiten.

Vraag 5 - XDR/EDR en host monitoring
Vraagstelling: Het ministerie onderzoekt aanvullende host monitoring, bijvoorbeeld met XDR/EDR-functionaliteit, voor Windows- en Linux-systemen. Doel is het vergroten van detectie- en responscapaciteit op endpoints en servers, zonder onnodige verstoring van bestaande beheerprocessen of tooling. Welke endpointtelemetrie verzamelt uw oplossing op Windows- en Linux-systemen? Welke detectiemogelijkheden biedt uw oplossing voor onder meer lateral movement, credential abuse, PowerShell-misbruik, fileless malware, Linux persistence, privilege escalation en hands-on-keyboard gedrag? Hoe borgt u dat detecties aantoonbaar aansluiten op de belangrijkste risico's, dreigingen, kroonjuwelen en kritieke processen van opdrachtgever? Welke response-acties ondersteunt uw oplossing, en welke daarvan kunnen automatisch, semi-automatisch of uitsluitend na

expliciete toestemming van opdrachtgever worden uitgevoerd? Hoe voorkomt u verstoring van primaire bedrijfsprocessen bij response-acties zoals hostisolatie, procesblokkering, quarantaine of live response?

Antwoorden

Voor Windows en Linux noemen respondenten onder meer proces- en commandoregelactiviteiten, authenticaties, privileges, bestanden, netwerkverbindingen en gedragsindicatoren als bruikbare telemetrie. De detectie moet worden afgestemd op dreigingen voor kritieke processen en gezamenlijk worden getuned met endpoint-, identiteits-, netwerk- en SIEM-informatie. Responsemogelijkheden variëren van onderzoek en blokkeren tot quarantaine of hostisolatie. Partijen benadrukken dat automatisch handelen alleen binnen een vooraf vastgesteld mandaat passend is; acties op kritieke systemen vragen doorgaans expliciete autorisatie of zorgvuldig vooraf overeengekomen uitzonderingen.

Vraag 6 - NDR en netwerkzichtbaarheid

Vraagstelling: Het ministerie onderzoekt Network Detection and Response als aanvullende detectielaag naast endpointdetectie en SIEM-use-cases. Daarbij is niet alleen zicht op noord-zuid verkeer relevant, maar ook beter zicht op oost-west verkeer, onbeheerde systemen en afwijkend netwerkgedrag. Welke netwerkbronnen en sensortypen ondersteunt uw NDR-oplossing, zoals packet capture, metadata, NetFlow/IPFIX, DNS, proxy, firewall, cloudtelemetrie of andere bronnen? Welke minimale netwerkarchitectuur of sensorplaatsing acht u noodzakelijk voor effectief zicht op noord-zuid én oost-west verkeer? Hoe detecteert uw oplossing onbeheerde systemen, rogue devices, shadow IT of systemen waarop geen endpoint-agent aanwezig is? Hoe correleert uw NDR-oplossing netwerkdetecties met XDR/EDR, SIEM-use-cases en interne threat intelligence? Welke rol ziet u voor NDR of vergelijkbare netwerkdetectie bij wijzigingen in bestaande landelijke of sectorale netwerkdetectievoorzieningen, zoals het Nationaal Detectie Netwerk, en welke alternatieve inrichting adviseert u?

Antwoorden

NDR wordt gezien als aanvullende zichtbaarheid voor oost-west verkeer, onbeheerde systemen en gedrag dat endpointagenten niet zien. Mogelijke bronnen zijn pakket- of netwerkmetadata, NetFlow/IPFIX, DNS, proxy, firewall- en cloudgegevens. De bruikbaarheid hangt af van netwerkarchitectuur, sensorplaatsing, versleuteling, beschikbaarheid van bronnen en koppeling met assetinformatie. Correlatie met EDR, SIEM en interne intelligence is nodig om losse netwerkalerts te voorkomen. De reacties lopen uiteen over NDR als verplichte basisdienst of optionele uitbreiding.

Vraag 7 - Exposure management en bewaking van de buitenkant

Vraagstelling: Naast monitoring op interne bronnen onderzoekt het ministerie ook exposure management, waaronder bewaking van de buitenkant van het ministerie, domeinbewaking, merk- en domeinmisbruik, gelekte credentials, stealerlogs en vergelijkbare signalen. Hoe ziet u de ontwikkeling van exposure management en bewaking van de buitenkant binnen een SOC? Welke mogelijkheden biedt uw dienstverlening voor exposure management, externe aanvalsvlakmonitoring, domeinbewaking, merk-/domeinmisbruik, gelekte credentials en stealerlogs? Hoe worden bevindingen gevalideerd, geprioriteerd en voorzien van concreet handelingsperspectief? Hoe voorkomt u dat exposure management leidt tot veel losse signalen zonder duidelijke opvolging door SOC, IBP, IT-beheer of andere verantwoordelijke partijen?

Antwoorden

Exposure management kan het SOC eerder zicht geven op publiek bereikbare systemen, kwetsbaarheden, domeinmisbruik, gelekte inloggegevens en andere externe signalen. Respondenten benadrukken verificatie, relevantie voor eigen assets en risico’s, prioritering en toewijzing van een eigenaar voor herstel. Een deel ziet dit als onderdeel van de MDR-kern; andere partijen adviseren een module of afzonderlijke specialistische dienst. Zonder koppeling met IT-beheer en incidentopvolging ontstaat het risico van veel meldingen zonder handelingsperspectief.

Vraag 8 - CTI, IOC's, TLP en vertrouwelijkheid

Vraagstelling: Het ministerie werkt met interne threat intelligence, IOC's en mogelijk vertrouwelijke of geclassificeerde informatie. Het is van belang dat door het ministerie aangeleverde IOC's, detectieregels, telemetrie of onderzoeksbevindingen niet ongecontroleerd worden gedeeld met andere klanten, externe platformen, publieke cloudomgevingen of gebruikt voor modeltraining. Hoe gebruikt u CTI voor prioritering van monitoring, use-cases, threat hunting en incidentrespons? Hoe ondersteunt uw dienstverlening verwerking van IOC's vanuit een intern CTI-proces of CTI-platform? Hoe maakt uw oplossing onderscheid tussen publieke threat intelligence, leverancierseigen intelligence, interne IOC's en TLP-geclassificeerde informatie? Hoe voorkomt u dat door opdrachtgever aangeleverde IOC's, detectieregels, telemetrie of onderzoeksbevindingen worden gedeeld met andere klanten, externe platformen of publieke cloudomgevingen? Worden gegevens van opdrachtgever gebruikt voor training, tuning of verbetering van generieke modellen of leverancierseigen detecties? Zo ja, hoe is dit configureerbaar of uitschakelbaar?

Antwoorden

CTI moet volgens de markt worden vertaald naar detectie, threat hunting, verrijking en respons, met een duidelijk onderscheid tussen publieke, leveranciersgebonden en interne intelligence. Voor uitwisseling van IOC's worden onder meer gestandaardiseerde API's en STIX/TAXII genoemd. Interne IOC's, regels, telemetrie en onderzoeksbevindingen vragen classificatie, toegangsbeperking en afspraken over TLP, bewaren, delen met andere klanten en gebruik voor modeltraining. Leveranciers verschillen in de mate waarin intelligence in eigen platforms wordt verwerkt.

Vraag 9 - Soevereiniteit, gegevensverwerking, continuïteit en compliance

Vraagstelling: Het ministerie wil inzicht krijgen in de mate waarin dienstverlening, dataopslag, dataverwerking, support, beheer en onderaanneming passen binnen eisen op het gebied van gegevensbescherming, soevereiniteit, continuïteit en compliance. Waar worden data, metadata, telemetrie, meldingen, configuratie, back-ups, rapportages en supportinformatie verwerkt en opgeslagen? Welke onderaannemers, cloudproviders, supportpartijen of concernonderdelen worden ingezet, en vanuit welke landen hebben zij toegang tot gegevens of systemen van opdrachtgever? Hoe borgt u dat gegevensverwerking, beheer en support passen binnen eisen aan EU/EER-dataverwerking en gegevenssoevereiniteit, inclusief bescherming tegen ongewenste toegang vanuit derde landen? Welke onderdelen van uw dienstverlening blijven functioneren bij verstoringen in netwerkverbindingen, cloudplatformen, beheerportalen of verbindingen met uw centrale platform? Hoe ondersteunt uw dienstverlening aantoonbaarheid richting AVG, BIO, NIS2/Cyberbeveiligingswet en interne audit- of verantwoordingsprocessen?

Antwoorden

De antwoorden beschrijven uiteenlopende leveringsmodellen met verwerking in eigen omgevingen, klantomgevingen of cloudplatformen. Daarom kan uit een algemene toezegging van EU/EER-verwerking niet worden afgeleid waar alle supporttoegang, metadata, back-ups of onderaannemers zich bevinden. De markt noemt contractuele en technische maatregelen zoals dataminimalisatie, toegangsbeperking, versleuteling, logging, audits en continuïteits- en herstelplannen. Beschikbaarheid bij uitval van verbindingen of centrale platformen verschilt per architectuur. De Nota van Inlichtingen stelt dat mogelijke ABRO-eisen na een risicoanalyse worden bepaald.

Vraag 10 - Dienstmodel, prijsmodel (indicatieve kosten), implementatie en exit

Vraagstelling: Het ministerie wil een dienstverlening uitvragen die effectief, schaalbaar, proportioneel en beheersbaar is gedurende de looptijd van de overeenkomst. Daarbij zijn dienstmodel, prijsmodel, implementatie, transitie, overdraagbaarheid en exit belangrijke aandachtspunten. Welk dienstmodel en prijsmodel (indicatieve kosten) acht u passend voor deze MDR+ dienstverlening, en wat zijn volgens u de belangrijkste kostendrivers? Welke fasering adviseert u voor implementatie, bijvoorbeeld voor MDR-integratie, XDR/EDR, NDR, exposure management en aansluiting op bestaande SOC-processen? Hoe voorkomt u dat tijdens transitie een gat ontstaat tussen de huidige dienstverlening en de nieuwe

dienstverlening? Welke voorzieningen zijn nodig voor kennisoverdracht, documentatie, export van gegevens, overdraagbaarheid en exit aan het einde van de overeenkomst?

Antwoorden

Een terugkerend voorstel is een vaste prijs voor de operationele basis met variabele, transparant geprijsde modules. Kostendrijvers zijn onder meer aantallen endpoints en bronnen, logvolume en retentie, netwerkdekking, 24/7 capaciteit, implementatie, specialistische inzet en licenties. Marktpartijen adviseren gefaseerde onboarding, een nulmeting, parallelle dekking tijdens de overgang, acceptatiecriteria en overdracht van kennis, configuraties, data en incidenthistorie. De interviewstukken waarschuwen voor het te vroeg vastzetten van alle technologie en voor impliciete uitbreiding van MDR naar specialistisch Splunk-platformbeheer. Individuele indicatieve prijzen uit reacties zijn niet opgenomen in dit openbare verslag.