Marktconsultatie MDR+ dienstverlening

Digitale inlichtingenbijeenkomst
24 juni 2026 | 10:30–12:00

Ministerie van Financiën | CDIO | SOC

Welkom en werkwijze

- Welkom bij deze digitale inlichtingenbijeenkomst over de marktconsultatie MDR+ dienstverlening.
- Vandaag lichten wij de aanleiding, context, beoogde scope, planning en spelregels toe. De bijeenkomst is bedoeld om marktpartijen een gelijk beeld te geven van onze behoefte en aandachtspunten.
- Deze marktconsultatie is geen aanbesteding en leidt niet tot selectie of voorselectie.

Vragen tijdens deze bijeenkomst

- Om de bijeenkomst goed te laten verlopen vragen wij u om vragen bij voorkeur via de chat te stellen.
- De vragen worden tijdens de bijeenkomst genoteerd en aan het einde geclusterd behandeld. Korte verduidelijkende vragen kunnen tussentijds worden opgepakt als dat nodig is voor het vervolg van de toelichting.
- Vragen die uitzoekwerk vragen of relevant zijn voor alle marktpartijen, beantwoorden wij niet altijd direct. Deze worden waar nodig meegenomen in het verslag, via TenderNed of in de Nota van Inlichtingen.
- Alle relevante informatie wordt op gelijke wijze gedeeld met alle geïnteresseerde partijen.

Agenda

1. Opening en introductie
2. Aanleiding marktconsultatie
3. Context bestaand SOC
4. Beoogde scope MDR+
5. Belangrijkste consultatiethema’s
6. Proces, planning en vervolgstappen
7. Geclusterde vragen en afsluiting

Aanleiding

- Het ministerie van Financiën bereidt een mogelijke aanbesteding voor voor MDR+ dienstverlening.
- Deze dienstverlening is bedoeld als vervolg op en mogelijke verbreding van de huidige continuous monitoring dienstverlening, waarvan het contract eindigt op 31 december 2026.
- Met deze marktconsultatie willen wij toetsen wat haalbaar, proportioneel, marktconform en toekomstvast is voordat scope, kavelindeling en aanbestedingsstrategie definitief worden bepaald.

Context bestaand SOC

- Het ministerie beschikt over een bestaand intern Security Operations Center.
- Binnen deze SOC-architectuur is Splunk leidend voor centrale logging, correlatie, detectie, rapportage en opvolging van securitymeldingen.
- Het interne SOC ontwikkelt en beheert organisatie-specifieke detectie-use-cases en werkt met interne threat intelligence en use-case management.

Wat zoeken wij wel en niet?

Niet	Wel
Volledige uitbesteding SOC	Versterking intern SOC
Regie overnemen	Regie blijft MinFin
Losse meldingen zonder context	Verrijkte meldingen met handelingsperspectief

Beoogde scope MDR+

De marktconsultatie richt zich op:

- Managed Detection and Response
- XDR/EDR of vergelijkbare host monitoring
- Network Detection and Response
- Exposure management
- Integratie met Splunk, Topdesk, CMDB, CTI en rapportagevoorzieningen
- Forensische ondersteuning op afroep
- Soevereiniteit, gegevensbescherming, continuïteit en contractuele beheersbaarheid

Deze onderdelen worden in de marktconsultatie inhoudelijk getoetst en vormen nog geen definitieve scope of kavelindeling voor een eventuele aanbesteding.

Hybride SOC-model

- Het uitgangspunt is een hybride model.
- De externe dienstverlener(s) ondersteunen onder meer bij monitoring, triage, escalatie, endpointdetectie, netwerkdetectie, exposure management en forensische ondersteuning.
- Het interne SOC behoudt regie, contextkennis, prioritering, interne opvolging en verbinding met de organisatie.

Waar vragen wij marktinput op?

Wij vragen marktpartijen vooral om visie, praktijkervaring en concrete aanbevelingen over:

- scope en kavelindeling;
- geïntegreerde of modulaire dienstverlening;
- multivendor-interoperabiliteit;
- integratie met Splunk en bestaande SOC-processen;
- MDR, XDR/EDR, NDR en exposure management;
- CTI/TLP, soevereiniteit, prijsmodellen, implementatie en exit.

Aandachtspunten vanuit MinFin

- Splunk blijft leidend voor SOC-workflows en centrale logging.
- Meldingen moeten verrijkt zijn met voldoende context en handelingsperspectief.
- Dubbele detecties, dubbele triage en alert fatigue moeten worden voorkomen.
- De oplossing moet passen in een hybride en mogelijk multivendor omgeving.
- Vertrouwelijke IOC’s, detectieregels, telemetrie en onderzoeksbevindingen mogen niet ongecontroleerd worden gedeeld.
- Continuïteit tijdens incidenten is essentieel.

Verwachting richting marktpartijen

- Wij vragen geen aanbieding, demo of commerciële pitch, maar een inhoudelijke beantwoording van de vragen in Bijlage 1.
- Geef zo concreet mogelijk aan wat marktconform is, welke randvoorwaarden nodig zijn, welke risico's of afhankelijkheden u ziet en welke onderdelen volgens u basis, optioneel, modulair of afzonderlijk kavel zouden moeten zijn.

Proces en planning

- Inlichtingenbijeenkomst: 24 juni 2026, 10:30–12:00
- Zomervakantie: juli t/m 12 augustus 2026
- Indienen vragen via TenderNed: uiterlijk 13 augustus 2026, 12:00
- Publicatie Nota van Inlichtingen: 27 augustus 2026
- Indienen schriftelijke beantwoording: uiterlijk 10 september 2026, 12:00
- Eventuele individuele gesprekken: 15 t/m 21 september 2026
- Eindverslag beschikbaar: vanaf 22 september 2026

Vragen en afsluiting

- Wij behandelen nu de vragen die tijdens de bijeenkomst via de chat of mondeling zijn gesteld.
- Vragen worden waar mogelijk geclusterd per thema. Vragen die niet direct kunnen worden beantwoord, worden meegenomen in het verdere proces.
- Dank voor uw deelname en belangstelling.