Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Beantwoording vragen Inlichtingenbijeenkomst

Rijksinkoopsamenwerking

Bezoekadres
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Beantwoording vragen Inlichtingenbijeenkomst

Marktconsultatie	
Titel marktconsultatie	Marktconsultatie Managed Detection and Response (MDR)+ dienstverlening
Opdrachtgever	het ministerie van Financiën, Concerndirectie Informatievoorziening & Openbaarmaking (CDIO)
Kenmerk	201865004.015.069
Datum	2-7-2026
Versie	1.0

Vragen

Vraag 1	
Vraag	Gezien het feit dat het huidige contract voor continuous monitoring afloopt per 31 december 2026, hebben jullie een indicatieve planning beschikbaar is voor de periode na de marktconsultatie, in het bijzonder ten aanzien van de beoogde publicatie van de aanbesteding (RFP) en de voorziene ingangsdatum van de nieuwe dienstverlening.
Antwoord	De genoemde einddatum van 31 december 2026 is indicatief en dient primair als uitgangspunt voor de planning. Op dit moment is de planning voor de periode na de marktconsultatie, waaronder de publicatie van een eventuele aanbesteding (inkooptraject) en de beoogde ingangsdatum van de nieuwe dienstverlening, nog niet definitief is vastgesteld. Indien de planning daartoe aanleiding geeft, kan worden bezien of de huidige dienstverlening gedurende een beperkte periode wordt voortgezet om een zorgvuldige overdracht naar de nieuwe dienstverlening in

	2027 mogelijk te maken. Hieraan kunnen op dit moment echter geen rechten of toezeggingen worden ontleend. De Opdrachtgever zal bij de verdere uitwerking van de planning rekening houden met de aanbestedingsrechtelijke kaders, zodat een eventuele overbruggingsperiode objectief, proportioneel en transparant kan worden vormgegeven. Nadere informatie hierover zal, indien van toepassing, worden opgenomen in de aanbestedingsstukken.

Vraag 2	
Vraag	Hoe kijken jullie naar automation vs human triage in het operating model.
Antwoord	Door het beperkt aantal analisten binnen het Financiën SOC en toename in dreigingen is het onvermijdelijk om te automatiseren. Mits daarmee dreigingen adequaat kunnen worden gedetecteerd en kan worden gewaarborgd dat dit geen invloed heeft op de betrouwbaarheid van de uitkomsten.

Vraag 3	
Vraag	Kunnen jullie iets verder uitwijden mbt de overheidspartijen die diensten leveren en hun eigen SOC hebben zoals SSC-ICT?
Antwoord	Binnen het ministerie van Financiën wordt het grootste deel van de kantoorautomatisering verzorgd door SSC-ICT. Zij hebben ook een eigen SOC waarmee het Financiën SOC nauw samenwerkt. Daarnaast heeft het ministerie van Financiën ook een commerciële leverancier, die een eigen securityteam heeft waarmee het Financiën SOC nauw samenwerkt.

Vraag 4	
Vraag	Wat voor screening verwachten jullie van de betrokken engineers en analysten ook ivm TLP Rood IOC?
Antwoord	Momenteel wordt er verwacht van de betrokken engineers en analisten dat zij minimaal over een VGB op niveau AIVD-B beschikken.

Vraag 5	
Vraag	Welke eisen stellen jullie aan de aanbieder zelf (ABRO)?
Antwoord	De Opdrachtgever onderzoekt momenteel welke eisen ten aanzien van de aanbieder noodzakelijk en proportioneel zijn. In dat kader zal een ABRO-toets worden uitgevoerd. Deze toets moet uitwijzen of de aard van de dienstverlening zodanig is dat sprake is van een relatie met de nationale veiligheid en of aanvullende eisen van toepassing zijn, zoals het beschikken over een ABRO-verklaring en/of het geheim verklaren van (delen van) het inkooptraject. De uitkomsten van deze toets worden, voor zover van toepassing, verwerkt in de aanbestedingsstukken. Op dit moment kunnen hierover nog geen definitieve uitspraken worden gedaan.

Vraag 6	
Vraag	Verwacht men deels directe actie/triage van MDR partij buiten kantoortijden?
Antwoord	Voor mogelijke prio-1/P-2 meldingen verwachten we een 24x7 dienstverlening (triage en escalatie), er zal dus ook een triage moeten plaatsvinden buiten kantoortijden. De daadwerkelijke vervolgactie of containment hangt vervolgens af van de ernst, het mandaat, de vooraf afgesproken procedures en de betrokken ketenpartijen.

Vraag 7	
Vraag	De nieuwe MDR+ Dienst behelst ongetwijfeld nieuwe diensten tov huidige SOC dienstverlening. Zijn er nieuwe of additionele diensten die in nieuwe MDR+ contract worden meegenomen. Zo ja, welke zijn dat?
Antwoord	Verwijzing naar de presentatie, waar genoemd wordt dat het Ministerie van Financiën op zoek is naar toekomst vaste oplossingen. Hier hebben wij zelf een beeld bij, maar horen graag via deze marktconsultatie hoe de markt dit ziet.

Vraag 8	
Vraag	u vermeldt dat u soevereiniteit belangrijk vind. Kunt u toelichten hoe we dat hier moeten interpreteren?

Antwoord	Opdrachtgever houdt zelf de regie, d.w.z. volledige zeggenschap/eigenaarschap van gegevens, controle over monitoring, maar ook borging van de continuïteit van de dienst gedurende de hele contractperiode en bij beëindiging daarvan

Vraag 9	
Vraag	In hoeverre verwacht u van de SOC partij dat hij zijn eigen gereedschapskist qua SOC-tooling (SIEM, EDR, NDR, ...) meeneemt in de MDR+ dienstverlening, en in hoeverre moet van de bestaande tooling gebruik gemaakt worden?
Antwoord	Voor de Opdrachtgever is Splunk het leidende platform voor de centrale zichtbaarheid en opvolging van beveiligingsmeldingen. De Opdrachtgever verwacht daarom dat tooling die wordt ingezet voor detectie, monitoring en response, zoals SIEM-, EDR-, NDR- of vergelijkbare oplossingen, waar mogelijk kan integreren met Splunk, zodat meldingen centraal kunnen worden weergegeven en opgevolgd. De Opdrachtgever sluit niet uit dat de leverancier aanvullende of eigen tooling inzet als onderdeel van de MDR+-dienstverlening. Wel is het van belang dat deze tooling goed aansluit op de bestaande omgeving en de operationele processen. Daarbij geldt als uitgangspunt dat meldingen niet op meerdere plekken afzonderlijk hoeven te worden beoordeeld, opgevolgd of afgesloten, om versnippering van het securityproces te voorkomen. Eén van de doelstellingen van deze marktconsultatie is om inzicht te verkrijgen in welke aanvullende tooling marktpartijen relevant achten voor een effectieve MDR+-dienstverlening en op welke wijze deze tooling kan samenwerken met de bestaande omgeving. De Opdrachtgever nodigt marktpartijen uit om hierover hun visie en aanbevelingen te delen.

Vraag 10	
Vraag	Staat u een hybride opzet toe waarbij een deel van de analisten Nederlandstalig en in Nederland gevestigd is, en aanvullende Engelssprekende analisten binnen de EU worden ingezet voor schaalbaarheid?
Antwoord	De Opdrachtgever staat terughoudend tegenover een hybride opzet waarbij een deel van de analisten buiten Nederland is gevestigd. Dit vanwege de aard van de werkzaamheden, waarbij toegang kan bestaan tot gevoelige gegevens, meldingen, systemen en informatie van de Nederlandse overheid, het Ministerie van Financiën en ketenpartners. Inzet van analisten buiten Nederland, maar binnen de EU-jurisdictie, kan onder voorwaarden bespreekbaar zijn. Oplossingen waarbij werkzaamheden buiten de EU plaatsvinden, zijn niet op voorhand uitgesloten, maar zullen uitsluitend worden beoordeeld indien de inschrijver overtuigend aantoont dat de daaraan verbonden risico's voldoende worden beheerst. Daarbij worden onder meer aspecten als juridische kaders, soevereiniteit, informatiebeveiliging, de aard van de werkzaamheden en de bescherming van de belangen van de Opdrachtgever betrokken.

Vraag 11	
Vraag	Kun je aangeven hoe in de huidige situatie de scheidslijn over de verschillende diensten tussen Ministerie en leverancier is?
Antwoord	Eén van de doelstellingen van deze marktconsultatie is om inzicht te verkrijgen in de wijze waarop marktpartijen de scheidslijn tussen de verantwoordelijkheden van het ministerie en de leverancier zien en welke verdeling van taken daarbij het meest effectief is. Het uitgangspunt is dat regie, eigenaarschap en de eindverantwoordelijkheid voor informatiebeveiliging en de dienstverlening bij het ministerie blijven liggen. Dit sluit aan bij de verantwoordelijkheden die voortvloeien uit onder meer de relevante wet- en regelgeving, zoals de NIS2-richtlijn en de Cyberbeveiligingswet. Waar de praktische afbakening van werkzaamheden en verantwoordelijkheden precies komt te liggen tussen het ministerie, een eventueel Security Operations Center (SOC), de leverancier en ketenpartners, is nadrukkelijk onderdeel van deze marktconsultatie. De Opdrachtgever nodigt marktpartijen uit om hierover hun visie, ervaringen en aanbevelingen te delen.