Bijlage 1 bij de Marktconsultatie SOC / MDR Dienstverlening

Invulinstructie vragenlijst	
1. Kolom Nr.	Betreft het aantal vragen per Deelnemer. Deelnemer dient zelf verder door te nummer bij meer dan 10 vragen.
2. Kolom Vraag MC	Geef aan op welke vraag uit de Marktconsultatie uw vraag betrekking heeft.
3. Kolom Par.	Geef aan op welke paragraaf en / pagina uit het document de vraag betrekking heeft.
4. Kolom V/O	Vermeld hier per regel één vraag of opmerking. **LET OP:** gebruik géén firmanamen en/of merknamen.

Nr.	Vraag MC	Par.	Vraag/opmerking	Antwoord
1	Marktconsultatie SOC MDR dienstverlening	2,1	Er wordt vanuit ons SOC standaard in het Engels gecommuniceerd met onze klanten. Staat de Hogeschool Rotterdam hiervoor open voor of wordt verwacht dat de dienstverlening volledig en uitsluitend in het Nederlands is?	Hogeschool Rotterdam verwacht dienstverlening volledig en uitsluitend in het Nederlands.
2	Marktconsultatie SOC MDR dienstverlening	2,3	Kunt u aangeven per wanneer Hogeschool Rotterdam zou willen starten met een nieuwe MDR dienstverlener?	Hogeschool Rotterdam wil in de eerste helft van 2025 starten met de nieuwe dienstverlener.
3	Marktconsultatie SOC MDR dienstverlening	1.2.	Het SurfSOC is al enige tijd actief met deelnermers uit de educative sector. Kunt u aangeven waarom niet gekozen wordt om aan te sluiten bij het SurfSOC?	SurfSOC richt zich niet op het monitoren van user-endpoints, maar meer op servers en delen van de infrastructuur, wat Hogeschool Rotterdam ontoereikend vindt. De door Surf gecontracteerde dienstverlening omvat het ontvangen van alerts en doorzetten naar de aansluitende onderwijsinstelling, maar biedt weinig analyse, interpretatie of oplossing.
4	1	2.2	Kunt u een meer gedetailleerde beschrijving geven van de medewerkers met de TISO (Technical Information Security Officer) rol of functie, welke werkzaamheden ze uitvoeren en waar ze in de organisatie (organigram) staan.	De TISO vervult een operationele adviesrol voor security. De TISO's vertalen beleid naar technische maatregelen en kijken of deze goed toegepast worden tijdens implementatietrajecten. Daarnaast monitoren TISO's het gehele IT landschap op dreigingen en inbreuken door middel van het analyseren van alerts uit onze security tooling.
5		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.2 Huidige omgeving	Hoe ziet u de samenwerking tussen het actieve security team, bestaande uit interne 3 TISO's (Technical Information Security Officers) en de externe partij die de externe SOC/MDR dienstverlening verzorgt.	Zie vraag 4. Hogeschool Rotterdam beoogt met de marktconsultatie advies te krijgen over de best wijze van samenwerken.
6	1,5,11,12,16	2.3	Hogeschool Rotterdam geeft aan dat het de Microsoft oplossingen in het vizier heeft. Wat bedoelt Hogeschool Rotterdam hiermee? Welke Microsoft producten en licenties heeft Hogeschool Rotterdam al in bezit en welke producten en onderdelen van Microsoft zijn al actief bij de Hogeschool?	Hogeschool Rotterdam is een gebruiker van het M365 aanbod van Microsoft als samenwerkingsomgeving (mail, teams, onedrive, etc.). Hiervoor maakt Hogeschool Rotterdam op dit moment gebruik van de Microsoft A3 licenties voor alle medewerkers en studenten. Daarnaast is Hogeschool Rotterdam bezig om alle integratievraagstukken in Azure onder te brengen met behulp van het Microsoft Integration Services (Azure Functions, API Gateway, Logic Apps, etc.). Tevens is het plan is om ook de gehele Identity & Access Management (IAM) processen onder te brengen in Microsoft Entra. Daarnaast worden alle beheerde apparaten (laptops, smartphones, tables) beheerd via de Microsoft Intune oplossing. Wat betreft security tooling wil Hogeschool Rotterdam, mede gezien het grote en almaar toenemende gebruik van Microsoft producten, Microsoft Defender en Sentinel gaan gebruiken zodat Hogeschool Rotterdam ook grip krijgt en op wat er gebeurt met onze identiteiten binnen de MS cloud en onze integratiekoppelingen.
7		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.3 Toekomstige omgeving	Hogeschool Rotterdam volgt de ontwikkelingen en heeft daarbij ook de oplossingen van Microsoft in het vizier. Wilt u dit verder specificeren?	Zie antwoord vraag 6.
8	1,6,10,18	2.3	In hoofdstuk 2.3 beschrijft Hogeschool Rotterdam dat het een SOC/MDR dienst verlening wil inrichten die aan de norm voldoet en past bij de ICT-organisatie. Welke norm gebruikt Hogeschool van Rotterdam voor de SOC/MDR dienstverlening.? Kan de Hogeschool toelichten wat zij verstaat onder 'passend'?	Hogeschool Rotterdam hanteert het SURF(norm)enkader. Hogeschool Rotterdam beoogt met deze marktconsultatie een beeld te krijgen wat passend is.
9		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.3 Toekomstige omgeving	Hogeschool Rotterdam heeft tot doel een SOC/MDR dienstverlening in te richten die aan de norm voldoet en past bij haar eigen IT-organisatie. Van welke norm wordt hierbij uitgegaan?	Zie antwoord vraag 8.
10	Marktconsultatie SOC MDR dienstverlening, 2. Beschrijving van de Opdracht	2.2	U geeft aan dat ON2IT zich specifiek gaat toeleggen op het monitoren van het Palo Alto firewall cluster. Wilt u hiermee zeggen dat ON2IT niet de SOC / MDR dienstverlening gaat uitvoeren?	Op dit moment neemt Hogeschool Rotterdam SOC dienstverlening af bij ON2IT op de smalle scope van de Palo Alto firewalls en het verkeer dat daar overheen gaat. Voor de uiteindelijke aanbesteding wil Hogeschool Rotterdam de scope veel breder trekken waardoor het een compleet andere vorm van dienstverlening wordt en ook de contractwaarde een stuk hoger (dan de drempelwaarde voor Europees aanbesteden).
11	Marktconsultatie SOC MDR dienstverlening, 2. Beschrijving van de Opdracht	2.2	"Hogeschool Rotterdam staat open voor mogelijke oplossingsrichtingen om dit onder te brengen in de mogelijke toekomstige dienstverlening". Staat Hogeschool Rotterdam open om het beheer van het Palo Alto cluster onder te brengen bij de SOC / MDR leverancier die de aanbesteding wint? Is managed firewall straks onderdeel van de aanbesteding voor SOC / MDR?	Hogeschool Rotterdam ziet de toegevoegde waarde van het loggen, monitoren en correleren van firewall-data en vraagt daarom ook naar "mogelijke oplossingsrichtingen in mogelijke toekomstige dienstverlening". Het dagelijks beheer (toevoegen/verwijderen van regels t.b.v. interne dienstverlening) van de firewall valt buiten de gevraagde dienstverlening.
12	Markconsultatie SOC MDR dienstverlening, 2. Beschrijving van de Opdracht	2.2	U geeft aan dat ESET thans de leverancier is van een EDR oplossing. Kunt u aangeven of EDR een onderdeel uit gaat maken van de aanbesteding?	Het monitoren van gedrag op endpoints (devices van eindgebruikers) en daarop in kunnen grijpen, zijn voor Hogeschool Rotterdam zeer belangrijke onderdelen van de scope voor SOC/MDR dienstverlening.
13	Marktconsultatie SOC MDR dienstverlening, 2. Beschrijving van de Opdracht	2.3	U geeft aan dat de Hogeschool Rotterdam de oplossingen van Microsoft in het vizier heeft. Kunt u aangeven of u al beschikt over een A3 of A5 Licentie?	Op dit moment neemt Hogeschool A3 licenties af voor alle medewerkers en studenten. Hogeschool Rotterdam realiseert zich dat voor uitbreiding van de dienstverlening A5 licenties nodig kunnen zijn.
14		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.3 Toekomstige omgeving	Heeft u voor elke gebruiker een Microsoft E5 licentie, indien niet het geval, welke licentie(s) heeft u dan wel?	Zie antwoord vraag 13.
15		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.2 Huidige omgeving	Indien u afscheidt neemt van ESET, staat u dan open om een andere EDR/XDR oplossing te implementeren of wenst Hogeschool Rotterdam dan so wie so over te gaan op Microsoft Defender (EDR/XDR)) for Endpoint?	Hogeschool Rotterdam wenst de richting van Microsoft Defender op te gaan vanwege de integratie met onder andere EntraID, M365. Hogeschool Rotterdam beoogt met deze marktconsultatie inzicht te krijgen in de best practice.
16		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.2 Huidige omgeving	Wie zal de regiefunctie vervullen, en op welke wijze, wanneer meerdere partijen diensten leveren aan Hogeschool Rotterdam. Met andere woorden hoe ziet u de samenwerking tussen partijen zoals Hogeschool Rotterdam (interne TISO's), ON2IT, de externe SOC/MDR dienstverlener en eventuele andere betrokken partij(en).	Hogeschool Rotterdam zal de regie voeren.
17		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 5, paragraaf 2.3 Toekomstige omgeving	Hogeschool Rotterdam is op zoek naar een passende prijsstructuur, vigerende kwaliteitsniveaus en alsmede flexibiliteit in de uitvoering in samenspraak en afstemming met de IT-organisatie van Hogeschool Rotterdam. Kunt u een toelichting geven op wat Hogeschool Rotterdam als een passende prijsstuctuur ziet en een toelichting geven welke flexibiliteit gezocht wordt in de uitvoering. Tevens hoe de afstemming met de SOC/MDR dienstverlener en de IT-organisatie van Hogeschool Rotterdam gewenst is.	Hogeschool Rotterdam voert de marktconsultatie uit mede om antwoord te krijgen op de gestelde vraag. Dit geldt ook voor de afstemming. Hogeschool Rotterdam verneemt graag van marktpartijen wat een gewenste afstemming zou kunnen zijn.
18		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 6, paragraaf 2.3 Toekomstige omgeving	Heeft u al een keuze gemaakt of u een XDR of SIEM oplossing wenst? Zo ja: welke oplossing heeft momenteel de voorkeur?	Hogeschool Rotterdam richt zich op de Sentinel oplossing van Microsoft, wetende dat deze oplossing van origine een SIEM oplossing is maar door het brede ecosysteem van Microsoft Securitytools bereikt het wel degelijk XDR functionaliteit.
19		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 6, paragraaf 2.4 Scope	Beheert en managed Hogeschool Rotterdam het netwerk, de werkplekken en alle server systemen of heeft zij daar een 3e partij cq 3e partijen voor?	Op dit moment beheert Hogeschool Rotterdam het netwerk, werkplekken en servers zelf.
20		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 6, paragraaf 2.4 Scope	In vervolg op vraag 9: Indien het een derde partij is cq derde partijen zijn: welke is/zijn dat dan?	Gezien het antwoord op vraag 19, is deze vraag niet van toepassing.
21		Marktconsultatie SOC MDR dienstverlening.pdf, Pagina 6, paragraaf 2.4 Scope,3e bullit	Indien bij Hogeschool Rotterdam 3e partijen op IT infrastructuur gebied actief zijn hebben wij additioneel nog de volgende vraag: -U geeft de wens aan "onmiddellijk reageren door het incident te onderzoeken, te mitigeren en te herstellen". Mitigeren en herstellen vereist handmatige toegang tot systemen op (bv. terugzetten naar herstelpunt, malware verwijderen, herconfigueren systemen, afsluiten endpoint van netwerk of blokkeren internet toegang: hoe kijkt uw IT/netwerk/werkplek leverancier die momenteel de systemen managed daar tegenaan cq staat deze partij open dat een security partij direct kan ingrijpen op systemen en zijn er met die partij afspraken gemaakt dat het mogelijk gaat zijn om constructieve demarcatie afspraken en een 3 partijen SLA overeen te komen?	Gezien het antwoord op vraag 19, is deze vraag niet van toepassing.