



**Vastgoed
en Facilitair**

**MARKTCONSULTATIE
MDR DIENSTVERLENING
PROJECTNUMMER 2024/003/IDT
DOCBASENUMMER UO233-2024/02986882**

Dienst
Naam auteur
Functie auteur
Verantwoordelijk directeur
Datum

IDT
Hans Velt
Senior Inkoopadviseur
Anjo van Kelckhoven
7 juni 2024

INHOUDSOPGAVE

1	Voorwoord	3
2	Verslaglegging marktconsultatie	4
2.1	Inrichting dienstverlening	4
2.2	Algemene ontwikkelingen	4
2.3	Ervaringen bij vergelijkbare klanten	5
2.4	Onderscheidend vermogen	5
2.5	Ontwikkelperspectief in de uitvoering	5
2.6	Kwaliteitsniveaus	6
2.7	Compliance en Certificeringen	6
2.8	Risico's	6
2.9	Opleiding en Expertise	6
2.10	Techniek	7
2.11	Omgeving	7
2.12	Implementatietraject	7
2.13	Detectie- en Responscapaciteit	7
2.14	Incident Response	7
2.15	Rapportage en Analyse	7
2.16	Prijsopbouw	8
2.17	Waardecreatie	8
2.18	Prestatiemanagement	8
2.19	Exit strategie	9
3	Nawoord	10

1 Voorwoord

Hogeschool Rotterdam heeft de marktconsultatie uitgevoerd als voorbereiding op een mogelijke aanbesteding voor Managed Detection & Response (MDR) dienstverlening.

Hogeschool Rotterdam wil de mogelijkheden van de markt optimaal benutten en luisteren naar aandachtspunten vanuit de markt.

Met deze marktconsultatie beoogt Hogeschool Rotterdam:

- inzicht te krijgen op welke manier de huidige markt voor security monitoring dienstverlening aansluit op de wensen binnen Hogeschool Rotterdam;
- input te vergaren voor de inrichting van de aanbestedingsstrategie, contractvorm en contractuitvoering en daarmee de kwaliteit van de aanbesteding verhogen;
- zoveel mogelijk partijen te bereiken, te interesseren en te stimuleren tot meedenken;
- inzicht te krijgen in de kostenopbouw van de security monitoring dienstverlening.

In hoofdstuk 2 is de verslaglegging van deze marktconsultatie weergegeven.

De aanbesteding zal naar verwachting in het vierde kwartaal van 2024 gepubliceerd worden op TenderNed.

2 Verslaglegging marktconsultatie

Deze samenvatting omvat globaal de antwoorden (uitspraken en meningen) die zijn verkregen uit de marktconsultatie zonder dat de antwoorden naar een marktpartij zijn te herleiden.

De marktconsultatie bestond uit totaal 19 inhoudelijke vragen.

Tien partijen hebben schriftelijk gereageerd op de marktconsultatie.

Twee partijen hebben aangegeven dat de inhoudelijke reactie volledig vertrouwelijk is.

De schriftelijke reacties bevatten naast beantwoording van de vragen van Hogeschool Rotterdam ook een toelichting en aanprijzing van de eigen dienstverlening.

In verband met de concurrentiegevoeligheid van de antwoorden wordt in deze samenvatting een algemeen beeld geschetst per onderdeel.

2.1 Inrichting dienstverlening

Hogeschool Rotterdam was op zoek naar inzichten vanuit de markt over hoe TISO's van HR worden aangesloten op de dienstverlening van de te contacteren partij.

Niet alle deelnemers aan de marktconsultatie zijn hier erg diep op ingegaan. Eén van de partijen geeft aan dat speciale aandacht vereist is voor de endpoints in zowel managed als byod vorm. Anderen noemen de rol van TISO's in de opvolging en het nadenken over operationele verbeteringen.

Eén partij geeft aan dat TISO's getraind moeten worden en dat de samenwerking nauw is in geval van incidenten.

2.2 Algemene ontwikkelingen

Hogeschool Rotterdam heeft de markt de volgende vragen gesteld:

- Welke ontwikkelingen en/of innovaties, nieuwe dienstverleningsconcepten, ziet u in de markt die van invloed kunnen zijn of bij kunnen dragen aan de aan te besteden dienstverlening?
- Op welke manier wenst u dat deze ontwikkelingen terugkomen in de aanbesteding?

Deelnemers aan de marktconsultatie zien verschillende ontwikkelingen. Van één partij krijgt Hogeschool Rotterdam het advies expliciet MITRE ATT&CK te eisen als framework maar wel met ruimte voor periodieke updates van dat framework. Dezelfde partij onderstreepte ook het belang van eisen aan capabilities op gebied van AI, ML, cloud, zero-trust principes.

Een andere partij onderstreepte de noodzaak van NDR gezien de grote hoeveelheid byod's. Ook was er een deelnemer aan de marktconsultatie die een ontwikkeling ziet waarin Machine Learning (ML) ingezet wordt om baselines te maken van normaal gedrag en afwijkingen daarop te detecteren en waarin Artificial Intelligence (AI) ingezet wordt in het afhandelingsproces voor incidenten.

Eén van de partijen ziet niet alleen een verschuiving van SIEM-only naar MXDR, maar ook verschuiving naar minder traditionele SIEMs zoals Sentinel. Deze partij ziet dat SOAR een onderdeel is van de dienstverlening.

Er is ook een partij die een marktontwikkeling ziet waarin SOC onderdeel is van een veel bredere MSP propositie.

2.3 Ervaringen bij vergelijkbare klanten

Uit de reacties heeft Hogeschool Rotterdam de volgende lessen opgehaald:

- Bewustzijn verhogen en security onder de aandacht brengen m.b.v. geboden dashboards;
- Implementatie duurt 2 maanden, neem daarna drie maanden voor "onboarding";
- Gebruik een risico-inventarisatie als basis voor de scope;
- Vergeet studentenaccounts en devices niet in die scope;
- Dienstverlening en maatregelen gefaseerd laten groeien op basis van de volwassenheid van de eigen organisatieklant;
- TISO's mee laten groeien en rol geven in dienstverlening evt. door extra training;
- Heroverweeg de eis voor volledige Nederlandse dienstverlening.

2.4 Onderscheidend vermogen

Dit bleek een lastig te beantwoorden vraag. Toch is een aantal inzichten te distilleren.

Onderscheidend vermogen zou kunnen zitten in de volgende aspecten:

- Ervaring hebben bij educatieve klanten;
- Het zijn van een Microsoft partner;
- Puur Nederlandse dienstverlening;
- Het niet alleen detecteren en notificeren maar ook daadwerkelijk optreden en ingrijpen bij incidenten;
- Het kunnen aanbieden van vulnerability management;
- De mate waarin de dienstverlening in staat is om Azure verbruik onder controle te houden;
- Het toepassen van Purview Data Loss Policies.

2.5 Ontwikkelperspectief in de uitvoering

Op de vraag hoe de uitvoering van de overeenkomst naar de mening van de markt georganiseerd moeten worden om optimaal in te kunnen spelen op toekomstige ontwikkelingen kreeg Hogeschool Rotterdam onderstaande adviezen:

- Evaluatie periodiek en organiseer verbetersessies o.l.v. security service consultant;
- Zorg voor flexibele contractstructuren;
- Kennissessies houden en trainingen verzorgen voor medewerkers van HR
- Hecht partnerschap tussen aanbieder en afnemer.
- Participatie in gebruikersgroep om ervaringen te delen.

2.6 Kwaliteitsniveaus

Lang niet alle deelnemers aan de marktconsultatie hanteren kwaliteitsniveaus.

Eén partij deelt de dienstverlening niet in op vaste servicelevel niveaus maar op basis van afspraken rond het MITRE ATT&CK framework.

Een andere partij kent verschillende abonnementsvormen, niet op basis van kwaliteitsniveau, maar op afgenomen (type) dienstverleningen.

Er is ook een partij die drie serviceniveaus onderscheidt.

2.7 Compliance en Certificeringen

De marktconsultatie levert geen extra inzichten op qua normen, zoals ISO 27001, en certificaten.

Een aantal partijen heeft een lijst van certificeringen aangeleverd, die het bedrijf zelf heeft.

2.8 Risico's

Deelnemers aan de marktconsultatie hebben de volgende risico's genoemd om rekening mee te houden in voorbereiding op de aanbesteding:

- Volwassenheidsniveau Hogeschool Rotterdam;
- Onduidelijkheid over verwachtingen en afspraken bij opvolging incidenten;
- Integratie met IT omgeving Hogeschool Rotterdam;
- Blinde vlek voor byod;
- Inschrijvers zonder ervaring met educatieve klanten;
- Gebrek aan flexibiliteit om in te springen op veranderende behoefte;
- Gebrek aan kennis en/of resources bij Hogeschool Rotterdam om gemelde incidenten op te lossen;
- Niet tijdig beschikbaar hebben van MS licenties;
- Security baseline niet tijdig ingericht;
- Onduidelijkheid mandaat ingrijpen door aanbieder;
- Krappe planning van aanbesteding waardoor partijen niet kunnen deelnemen;
- Onvoldoende gewicht aan kwaliteit in prijs/kwaliteitverhouding;
- Onvoldoende draagvlak bij Hogeschool Rotterdam;
- Gebrekkige integratie;
- Slechte samenwerking;
- Teveel focus op techniek t.o.v. proces;
- Teveel focus op reactieve detectie;
- Niet genoeg rechten om in te grijpen door aanbieder.

2.9 Opleiding en Expertise

Hogeschool Rotterdam was ook geïnteresseerd in de opleiding en expertise van medewerkers, met name gericht op nieuwe bedreigingen en technologieën.

Een aantal partijen heeft een uitgebreid programma voor scholing en standaardcertificeringen voor personeel. Andere hebben een trainingsbudget per medewerker of een vastgesteld trainingsprogramma.

2.10 Techniek

Hogeschool Rotterdam heeft een aantal specifieke vragen gesteld over techniek. Deze gingen over de infrastructuur en technologielandchap voor het monitoren van netwerken, endpoints en systemen en over de mogelijkheden om mee te groeien met de toenemende netwerk- en systeemvereisten. Heel specifiek was Hogeschool Rotterdam geïnteresseerd in de mate van aanpassing aan de Azure- en Defender-omgeving van Hogeschool Rotterdam.

De reacties lopen uiteen. In algemene zin kan gesteld worden dat aanpassing aan de Azure- en Defender-omgeving tot de mogelijkheden behoort.

2.11 Omgeving

Concreet wilde Hogeschool Rotterdam weten of het mogelijk is om de gevraagde dienstverlening aan te bieden zonder dat loggegevens de omgeving van Hogeschool Rotterdam verlaten.

Hierop heeft Hogeschool zowel positieve als negatieve (stellige) reacties gekregen. Inhoudelijk gaat het erom welke informatie door de contractant wordt geanalyseerd. Een partij analyseert alleen de informatie over het incident. Daar waar het niet mogelijk is heeft dit te maken met centrale data analyse.

2.12 Implementatietraject

De inschatting van de benodigde implementatietijd verschilt tussen de deelnemers aan de marktconsultatie: van enkele weken (4-6 weken) tot enkele maanden (2-3 maanden).

2.13 Detectie- en Responscapaciteit

Alle deelnemers aan de marktconsultatie geven een duidelijk beeld van het escalatie en response proces en geven daarbij vergelijkbare reactietijden.

2.14 Incident Response

De vragen over het incidentenresponse leveren nuttige inzichten op. Meeste deelnemers hebben het incident response proces uitgebreid beschreven. Soms is automatisch ingrijpen door de contractant ook mogelijk.

2.15 Rapportage en Analyse

Uit de antwoorden komt naar voren dat het gangbaar is om een realtime dashboard te hebben met informatie over detecties en opvolging. Daarnaast geven alle deelnemers maandelijkse rapportages waarbij in de meeste gevallen onderscheid gemaakt wordt tussen managementrapportage (tactisch) en technische rapportage (operationeel). Er is ook een partij die op maat rapportages kan leveren.

2.16 Prijsopbouw

Een belangrijke vraag in het kader van de voorbereiding op de aanbesteding heeft betrekking op de prijsopbouw: wat is de gangbare eenheid van afrekening?

Uit de reacties blijkt dat er niet één gangbare methode is. Deelnemers aan de marktconsultatie hanteren verschillende uitgangspunten.

Eén partij werkt met een menukaart voor de opbouw van kosten, waarbij het gebruikte platform een maandelijks terugkerende kostenpost is.

Implementatie en training zijn veelal vaste kostencomponenten.

Licentiekosten kennen verschillende eenheden:

- aantal BYOD's;
- aantal endpoints (werkstations en servers);
- aantal gebruikersaccounts;
- aantal en type logbronnen;
- aantal licenties aangesloten op Sentinel.

Er zijn ook partijen die werken met vaste (maandelijkse) kosten op basis van GB per dag ingestelde en afgenomen dienstverlening.

2.17 Waardecreatie

Op antwoord op de vraag hoe de aanbesteding in te richten om financieel gunstige Inschrijvingen te ontvangen heeft Hogeschool Rotterdam verschillende reacties ontvangen. Hieronder volgt een weergave van de gegeven adviezen:

- Hanteer een minimaal inschrijfbedrag voor de aanbesteding;
- Wees zo uitgebreid mogelijk in de beschrijving van de situatie en de scope zodat de inschrijver daar concreet rekening mee kan houden;
- Richt de uitvraag op gewenste resultaat en functionaliteit;
- Vraag 1 totaalprijs voor gehele dienstverlening (dit voorkomt verrassingen door groei in scope en omvang).

2.18 Prestatiemanagement

Deze vraag had betrekking op gangbare KPI's in de markt.

Verschillende partijen hebben lijsten met prestatie indicatoren gegeven, die goed bruikbaar zijn om in de aanbesteding op te nemen.

2.19 Exit strategie

De meeste partijen hebben een standaard exit procedure. Bij de beantwoording hebben partijen een al dan niet uitgebreide toelichting gegeven.

Data blijft eigendom van Hogeschool Rotterdam, wel zijn er verschillen in de overdracht. Kennisoverdracht en andere zaken worden nader uitgewerkt in de DAP.

3 Nawoord

Hierbij bedanken wij alle marktpartijen die antwoorden op onze vragen hebben ingediend.

Hogeschool Rotterdam kan op basis van deze informatie afwegingen maken bij het vormgeven van de inkoopstrategie en het opstellen van de aanbestedingsdocumenten.