Bijlage A

Programma van eisen

Europese openbare aanbesteding

Managed Detection & Response

Aanbestedingsdossier	24.0000912
Tenderned referentie	467961
Versie	1.0
Datum	16 mei 2024

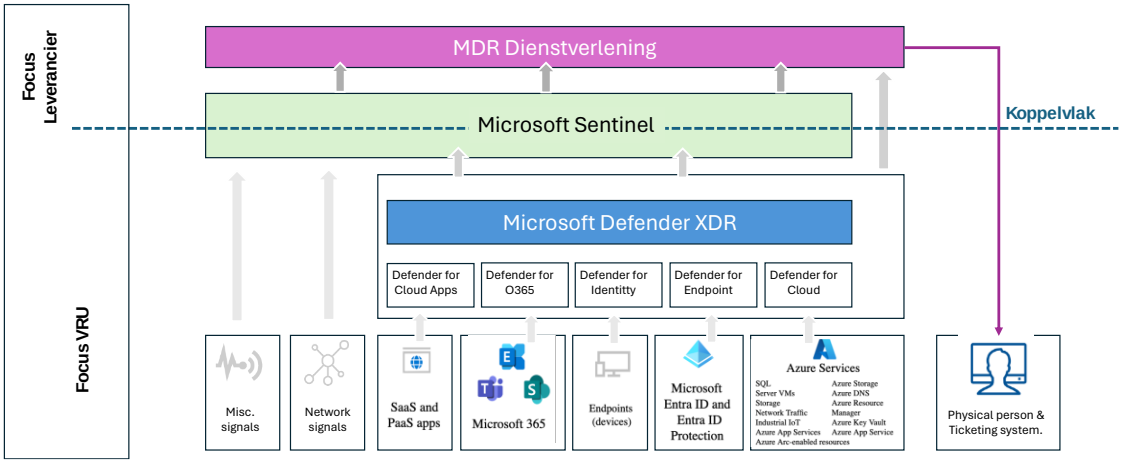
Veiligheidsregio Utrecht

vru.nl

Inhoud

* Alle eisen die met een asterisk zijn gemarkeerd, betreffen minimumeisen (ook wel inschrijvingseisen). Alle niet-gemarkeerde eisen zijn uitvoeringseisen (zie ook hoofdstuk 7 beschrijvend document)

1 Basis MDR Dienstverlening



Figuur 1: Illustratie logische opbouw MDR-omgeving VRU

De huidige omgeving van de VRU wordt gekenmerkt door de platforms van Microsoft en de daarbij behorende beveiligingsproducten uit de Microsoft Defender familie. De VRU is voornemens het XDR platform, welke automatisch gegevens verzamelt en correleert over meerdere beveiligingsvectoren, uit te breiden met de SIEM functionaliteit van Microsoft Sentinel. Deze combinatie van XDR/SIEM zal de basis vormen waarmee de Inschrijver zijn MDR-dienstverlening dient te integreren. Figuur één (1) illustreert hoe de omgeving logisch opgebouwd *kan* worden. Licenties, Configuratie, beheer van de Microsoft Defender XDR omgeving is de verantwoordelijkheid van de VRU. Dit is ook van toepassing voor de SIEM omgeving. Echter zal er voor configuratie en beheer van de SIEM omgeving altijd een gezamenlijk verantwoordelijkheid zijn, daar de effectiviteit en efficiëntie van de MDR dienstverlening sterk afhankelijk is van de inrichting en kwaliteiten van de SIEM oplossing. Voor aanvang van de MDR-dienstverlening zullen hier specifieke afspraken over worden gemaakt.

1.1 Algemene eisen

ID	EIS
1.1.1	De VRU gebruikt de Microsoft defender XDR suite voor proactieve bescherming en response. Inschrijver dient deze te integreren in de uitgevraagde dienstverlening.
1.1.2	De VRU is voornemens om, Microsoft Sentinel en Defender te gebruiken als Security Information and Event Management (SIEM) oplossing. Inschrijver dient deze te integreren in de uitgevraagde dienstverlening.
1.1.3	De VRU maakt gebruik van netwerkcomponenten met de mogelijkheid om bekende en onbekende bedreigingen en afwijkend gedrag te detecteren en hierop te alarmeren. Inschrijver dienen de deze (via de SIEM oplossing van de VRU) te integreren in de uitgevraagde dienstverlening
1.1.4	Eventuele voor de MDR dienstverlening benodigde specifieke hardware- en softwarecomponenten worden in abonnementsvorm geleverd. Eventuele logforwarders worden door de VRU geleverd.
1.1.5 *	Informatie over security incidenten en data mag niet verloren gaan, hiertoe heeft Inschrijver aantoonbaar afdoende maatregelen genomen om verlies van informatie te voorkomen.
1.1.6 *	Inschrijver levert de aangeboden MDR dienst met toepassing of configuratie van een uitgebreide bibliotheek met detectie mogelijkheden om bekende afwijkingen te detecteren die kunnen leiden tot een security incident.
1.1.7	Deze uitgebreide bibliotheek met detectie mogelijkheden dient door Inschrijver continu actueel volgens de dan toepasselijk stand der techniek, kennis, kunde en dreigingsbeeld te worden gehouden. Het moet mogelijk zijn om snel detectie (o.a. op basis van Threat Intelligence) van nieuwe dreigingen toe te voegen.
1.1.8	Voorts biedt de Inschrijver een Serviceportaal (voor de meldingen, standaard rapportages, etc.) welke eenvoudig voor de VRU bereikbaar is of een vergelijkbare laagdrempelige rapportagefunctionaliteit.

1.2 Eisen aan triage, onderzoeken, classificatie en reactie

ID	EIS
1.2.1 *	Van de Inschrijver wordt verwacht dat deze gebruik maakt van een eigen SOC-team binnen de Europese Economische Ruimte (EER+VK).
1.2.2 *	Van de Inschrijver wordt verwacht dat het eigen SOC-team 24x7 het “Eye on glass” principe hanteert. Dit principe vereist dat beveiliganalisten (mensen) actief XDR/SIEM dashboards en logs bekijken (en kunnen ingrijpen) op verdachte activiteiten, zowel vanuit MS Azure Sentinel als direct vanuit Defender.
1.2.3	De Inschrijver biedt een 24/7 telefonisch bereikbare Servicedesk met rechtstreeks contact met dan wel directe doorgeleiding naar ter zake kundig personeel voor vragen over meldingen en/of opvolgingsadviezen.
1.2.4	Op maandag t/m vrijdag, tussen 09:00 en 17:00 (CET, UTC+1, en UTC+2 in de zomermaanden) wordt van de servicedesk en ter zake kundig personeel van de Inschrijver, voor vragen over meldingen en/of opvolgingsadviezen, de Nederlandse taal verwacht. Buiten deze tijden, op zaterdag en zondag en feestdagen is Engels (Cambridge Engels of vergelijkbaar niveau) toegestaan.
1.2.5	Indien bij een prio-1 / high incident, op maandag t/m vrijdag, tussen 09:00 en 17:00 (CET, UTC+1, en UTC+2 in de zomermaanden) en buiten deze tijden, op zaterdag en zondag en feestdagen verdere opschaling nodig is, dient een Nederlandstalige specialist ingeschakeld te kunnen worden.
1.2.6	De Inschrijver is in staat om de analyse van security events binnen een realistische tijd – triage binnen enkele minuten na detectie, reactie en oplossing conform appendix 01) - uit te voeren en om het aantal false positives, die zowel door het SOC als in een periodieke rapportage gemeld worden tot een minimum te beperken. De Inschrijver dient daartoe o.a. de mogelijkheid te bieden om op aangeven van VRU specifieke false positives meldingen voor een bepaalde periode op ”mute” te zetten.
1.2.7	De VRU is verplicht om incidenten te delen met de sectorale CERT. De Inschrijver dient te faciliteren dat incidenten met een specifieke prioriteit na goedkeuring van de VRU met de CERT gedeeld worden.
1.2.8	De VRU kan in ieder geval notificaties ontvangen (bijv. via SMS, telefoon, email of andere ondersteunde optie; dit in overleg met de VRU) betreffende verschillende classificaties/prioriteiten van meldingen en bijbehorende systeem gegenereerde opvolgingsadviezen. Deze incidenten dienen bij voorkeur, en afhankelijk van de koppelingsmogelijkheden binnen de VRU, in het VRU ticketing ontvangen te kunnen worden.
1.2.9	In het geval van een prio-1/ high incident melding wordt de melding ook via SMS, telefoon of email (of andere ondersteunde opties) naar één of enkele contactpersoon/-personen worden gestuurd. Van de Inschrijver wordt verwacht dat deze monitort op ontvangstbevestiging vanuit de VRU. Hierover zullen bij aanvang van de dienstverlening nadere afspraken over worden gemaakt.

1.3 Eisen aan de log- en eventdata

ID	EIS
1.3.1 *	De door Inschrijver aangeboden MDR dienstverlening is voldoende robuust om het benodigde volume aan logdata en events te kunnen verwerken en bij inschrijver te kunnen opslaan voor de overeengekomen retentietijd. Bij het inrichten van de dienstverlening worden hier nadere afspraken over gemaakt.
1.3.2	Voor de aangeleverde log- en eventdata vanuit de XDR/SIEM oplossing geldt dat de Inschrijver een retentietijd van minimaal zes (6) maanden moet kunnen bieden. Bij het inrichten van de dienstverlening worden hier, binnen de wettelijke mogelijkheden, gezamenlijk nadere afspraken over gemaakt.
1.3.3 *	Voor de aangeleverde log- en eventdata vanuit de XDR/SIEM geldt dat deze bij de inschrijver zodanig opgeslagen moeten worden, dat de beschikbaarheid, integriteit en vertrouwelijkheid gegarandeerd is en deze beschikbaar is voor analyse van historische data (forensisch en post-mortem) en als bewijsmateriaal gebruikt kan worden in strafzaken.
1.3.4	Delen van de aangeleverde log- en eventdata dient door de VRU te kunnen worden geëxporteerd en archiveert buiten de systemen van de Inschrijver.
1.3.5	Bij exporteren en archivering van log- en eventdata wordt de meta-data meegeleverd.

1.4 Eisen aan de beveiliging

ID	EIS
1.4.1 *	Alle data dient te worden opgeslagen en verwerkt binnen de Europese economische ruimte (EER).
1.4.2 *	Alle data wordt versleuteld opgeslagen[1] en versleuteld verstuurd.[2]
1.4.3 *	Inschrijver past het principe van “least-privilege” en “need to know” toe en beperkt zo de toegang tot het noodzakelijke. Dit geldt ook voor serviceaccounts, machine-accounts, functionele accounts et cetera.
1.4.4	Inzage van logdata is alleen mogelijk voor de VRU en bevoegde medewerkers bij Opdrachtnemer, tenzij vooraf uitdrukkelijk en schriftelijk toestemming is gegeven door De VRU of als de rechter daar opdracht toe geeft. Bevoegde medewerkers: De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot logdata, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
1.4.5 *	Inschrijver gebruikt multi-factor authenticatie voor toegang tot alle rapportages/portalen voor zowel beheerders als gebruikers.

[1] Hierbij wordt minimaal gebruik gemaakt van AES-256

[2] Hierbij dienen de meest recentste ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC te worden gevolgd (op het moment van schrijven is het betreffende document versie 2.1)

1.5 Eisen aan de rapportage op hoofdlijnen

ID	EIS
1.5.1	Rapportages vanuit de geleverde dienst worden via een service portaal dan wel op een laagdrempelige, passende wijze aan de VRU beschikbaar gesteld. Via deze portal wil de VRU ook relevante dreigingsinformatie (threat intel) ontvangen.
1.5.2	De rapportages zijn opgesteld in de Nederlandse taal, waarbij het gebruik van Engelse termen incl. gegenereerde alerts in het Engels (korte berichten met dreigings- en technische informatie) zijn toegestaan.
1.5.3	De voorziening voor rapportages maakt het voor de VRU mogelijk om rapportages op te stellen op meerdere management niveaus alsmede trendrapportages.

1.6 Eisen aan de re-transitie

ID	EIS
1.6.1	Op eerste aangeven van de VRU stelt Inschrijver binnen tien (10) werkdagen een gedetailleerd exit-plan conform de GIBIT/artikel 22 op.
1.6.2	Gedurende de periode van retransitie dient de Inschrijver alle dienstverlening te continueren tegen de voorwaarden zoals overeengekomen.
1.6.3	Bij retransitie wordt alle bij Inschrijver opgeslagen VRU gerelateerde log- en event data in een voor de VRU bruikbaar format beschikbaar gesteld inclusief bijbehorende meta-data, exclusief intellectueel eigendom van desbetreffende Inschrijver.
1.6.4	De Inschrijver zal alle vertrouwelijke informatie van de VRU aan het einde van de overeenkomst c.q. aan het einde van de retransitie aan de VRU retourneren, zonder daar een kopie van te behouden, tenzij op basis van een (wettelijke) eis of verplichting, of op basis van aanvullende afspraken met de VRU, het langer aanhouden van een kopie van de informatie verplicht is gesteld. Als het langer aanhouden van een kopie van vertrouwelijke informatie verplicht is gesteld, dan zal deze informatie worden vernietigd vanaf het moment dat de termijn van het langer aanhouden is verstreken of als de informatie niet meer noodzakelijk is.

2 Onboarding

Onboarding diensten zijn alle activiteiten waarbij de VRU en de inschrijver de technische infrastructuur gereed maakt en configureert, en proces, procedures en werkinstructies afspreekt die nodig zijn om de dienstverlening of uitbreiding hiervan te realiseren.

2.1 Onboarding eisen

ID	EIS
2.1.1	De onboarding diensten moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.
2.1.2	Van de Inschrijver wordt verwacht dat betrokken projectleider(s) en servicemanager(s) de Nederlandse taal spreken en schrijven.
2.1.3	Van de Inschrijver wordt verwacht dat na definitieve gunning, de XDR omgeving binnen 14 dagen wordt gemonitord, dreigingen gedetecteerd en de VRU minimaal kan worden geïnformeerd of gealarmeerd. De gerelateerd kosten voor monitoring en detectie van de XDR omgeving kunnen naar ratio in rekening worden gebracht vanaf het moment van oplevering en acceptatie.
2.1.4	Van de Inschrijver wordt verwacht dat binnen 3 maanden na definitieve gunning de dienstverlening volledig operationeel is (inclusief formele acceptatie). De kosten van de volledige dienstverlening kunnen in rekening worden gebracht vanaf het moment van oplevering en acceptatie.
2.1.5	De scope en de impact van de dienstverlening gaat verder dan de CISO van de VRU. Het is dus van belang dat diverse geledingen binnen de VRU kennis maken met wat MDR dienstverlening is, wat de impact daarvan kan zijn op de organisatie en wat tactisch en operationeel gedaan moet worden om de inzet van dienstverlening effectief te doen zijn. Van de inschrijver wordt minimaal drie fysieke workshops van maximaal 2 uur (op een locatie van de VRU) verwacht.
2.1.6	De dienstverlening van de inschrijver dient te integreren met de Microsoft defender XDR suite van de VRU. Van de inschrijver wordt verwacht dat hij samen met de VRU, binnen drie maanden na definitieve gunning, de configuratie van de XDR suite doorloopt en aanbeveling doet om de detectie mogelijkheden te verbeteren en af te stemmen op het dreigingsbeeld van de VRU.
2.1.7	De VRU is voornemens om, Microsoft Sentinel te gebruiken als Security Information and Event Management (SIEM) oplossing. Van de inschrijver wordt verwacht dat hij de Microsoft Sentinel suite activeert en configureert zodat de detectiemogelijkheden van o.a. de netwerkcomponenten geïntegreerd worden.
2.1.8	Van de inschrijver wordt verwacht dat hij de Microsoft Sentinel suite configureert en daarmee integreert met de Microsoft defender XDR suite van de VRU.
2.1.9	Van de inschrijver wordt een implementatieplan verwacht conform artikel 5 GIBIT 2020.

3 Additionele diensten

In het portfolio zijn een aantal additionele diensten opgenomen, welke geen afnameverplichting kennen. Deze zijn beschreven in paragraaf 2.3 van het Beschrijvend document.

3.1 Kennis, advies en ondersteuning

De Inschrijver biedt naast de basisdienstverlening en de bijbehorende on-boarding de mogelijkheid voor aanvullende ondersteuning:

- Inhuur (consultancy) om de VRU te ondersteunen bij het inrichten van de beste-praktijk-voorwaarden voor MDR diensten in lijn met de aanbevelingen van het project VSSR van het Ministerie van Justitie en Veiligheid (SOC Readiness QuickScan versie 2.3).

- Nadere advisering (in retroperspectief) met betrekking tot gedetecteerde afwijkingen, incidenten en/of relevante dreigingen en ontwikkelingen in het beveiligingsdomein.

ID	EIS
3.1.1	De additionele diensten moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.

3.2 Ondersteuning bij door ontwikkelen use-cases en XDR/SIEM oplossing

De Inschrijver biedt (optioneel) de mogelijkheid voor aanvullende ondersteuning bij het opzetten van use-cases. Use-cases zijn cruciaal om specifieke dreigingen voor de VRU om te zetten in technische regelen. Van de Inschrijver wordt verwacht dat hij ondersteuning (consult) kan bieden bij het in kaart brengen van de specifieke dreigingen, risico's en regels afgestemd op MITRE ATT&CK, Lockheed Cyber Kill Chian of gelijkwaardig.

ID	EIS
3.2.1	De additionele diensten moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.

3.3 On-site ondersteuning bij grote beveiligingsincidenten

De Inschrijver biedt de VRU, als optionele dienstverlening, de mogelijkheid om ter zake kundig personeel (gespecialiseerd in het reageren op en het beheersen van beveiligingsincidenten) voor een beperkte duur af te nemen ter ondersteuning bij het feitelijk oplossen van het security incident.

ID	EIS
3.3.1	De additionele diensten moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.

3.4 Beheer van technische kwetsbaarheden

Beheer van technische kwetsbaarheden, ook bekend als vulnerability management omvat het identificeren, prioriteren en analyseren van kwetsbaarheden in het interne netwerk. *De VRU wil vulnerability-management, optioneel en as-a-service afnemen waarbij deze dienst geen deel uit van de beoordeling- en/of gunningscriteria.*

As-a-service betekent in deze dat de Inschrijver met eigen hardware, software en/of licenties de dienst levert. De inschrijver is in eerste instantie verantwoordelijk voor de installatie, configuratie en onderhoud. De Inschrijver voert minimaal één (1) keer per vier (4) weken een scan uit. De Inschrijver prioriteert de resultaten o.a. op basis van het daadwerkelijke risico en voorziet de VRU van advies om de kwetsbaarheid te verhelpen. Nadat de kwetsbaarheid is verholpen controleert de Inschrijver of de oplossing effectief is.

ID	Wens
Wens 4.4.1	De additionele dienst moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.
Wens 4.4.2	De additionele dienst wordt geleverd in lijn met de beste-praktijk-ervaring zoals beschreven in het document “Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO RIJK).

3.5 Monitoren digitale aanval oppervlak

Systemen die aan het internet verbonden zijn lopen een extra risico door misbruik van kwetsbaarheden door bijvoorbeeld onbedoeld open poorten, verouderde systemen of foutieve configuraties. *De VRU wil monitoring van het digitale aanval oppervlak (ook bekend als attack surface management), optioneel en as-a-service afnemen waarbij deze dienst geen deel uit van de beoordeling- en/of gunningscriteria.*

As-a-service betekent in deze dat de Inschrijver met eigen hardware, software en/of licenties de dienst levert. De Inschrijver is in eerste instantie verantwoordelijk voor de installatie, configuratie en onderhoud.

ID	Wens
Wens 4.4.1	De additionele dienst moeten geleverd worden door vakbekwaam personeel dat steeds voldoet aan de eisen die gelden in de branchestandaard.
Wens 4.4.2	De additionele dienst wordt geleverd in lijn met de beste-praktijk-ervaring zoals beschreven in het document “Handreiking kwetsbaarhedenscans Rijksoverheid (2021, CIO RIJK).

APPENDIX 01 - Reactietijd

Voor de prioritering van security incidenten wordt gebruik gemaakt van onderstaande tabel.

		Impact		
		Hoog	Midden	Laag
Urgentie	Hoog	1	2	3
	Midden	2	3	4
	Laag	3	4	5

Code/kleur	Omschrijving	Reactietijd	Oplossingstijd
1	Kritiek	15 minuten	1 uur
2	Hoog	30 minuten	4 uur
3	Medium	1 uur	8 uur
4	Laag	4 uur	24 uur
5	Zeer laag	1 dag	1 week

Colofon

Dit is een uitgave van
Veiligheidsregio Utrecht

Tekst: Erwin Bos
Fotografie: Beeldbank VRU
Ontwerp: Team communicatie

16 mei 2024

Veiligheidsregio Utrecht

vru.nl