

Bijlage 01b

Specificatie van de Prestatie | Architectuur

Programma van Eisen

Behorend bij

Raamovereenkomst Security Operations Center (SOC)

Status : Concept
Versie : 260429-1
Datum : 29-04-2026

Inhoudsopgave

1	Inleiding	3
2	Architectuur	3
2.1	Scope, doel en uitgangspunten	3
2.2	Architectuurprincipes	4
2.2.1	Architectuurkaders	4
2.2.2	Eigenaarschap en datasoevereiniteit	4
2.2.3	Integratie via open standaarden	4
2.2.4	Overdraagbare dienstverlening	4
2.2.5	Schaalbaarheid en toekomstvastheid	4
2.2.6	Security by design en Zero Trust	4
2.2.7	Transparantie en auditability	4
2.2.8	Herbruikbaarheid en standaardisatie	4
2.3	Sectoraal SOC	5
2.4	Provinciale SIEM-SOC Architectuur	6
2.5	SIEM en SOC	6
2.6	Databronnen – Security Tooling	7
2.7	Databronnen – Audit Logs	7
2.8	Datamanagement	7
2.9	Data Enrichment	8
2.10	Beheer van Security Policies binnen Microsoft Security Stack	8

1 Inleiding

Deze bijlage beschrijft de Eisen en randvoorwaarden met betrekking tot de architectuur en technische inrichting van de SOC-dienstverlening. Deze Eisen hebben tot doel te waarborgen dat de dienstverlening veilig, schaalbaar, interoperabel en beheersbaar kan worden geleverd en passend is binnen de bestaande en toekomstige IT-landschappen van Opdrachtgever en Deelnemers.

De in deze bijlage opgenomen Eisen zijn in beginsel generiek van aard. Dit betekent dat deze Eisen van toepassing zijn op de volledige architectuur en technische inrichting van de dienstverlening binnen de scope van de Raamovereenkomst, tenzij expliciet anders is aangegeven of de aard van een specifieke Eis anders vereist.

De architectuureisen omvatten onder meer de logische en technische opbouw van de oplossing, integraties met bestaande systemen, gegevensverwerking, beveiligingsmaatregelen en uitgangspunten ten aanzien van openheid en het beperken van afhankelijkheden van specifieke leveranciers, voor zover dit redelijkerwijs mogelijk is.

Opdrachtnemer dient de dienstverlening zodanig te ontwerpen, implementeren en beheren dat wordt voldaan aan de in deze bijlage opgenomen architectuureisen, in samenhang met de diensteneisen (Bijlage 2a) en de kwaliteits- en prestatie-eisen (Bijlage 2c), zodat een samenhangende, duurzame en toekomstbestendige dienstverlening wordt gerealiseerd.

2 Architectuur

2.1 Scope, doel en uitgangspunten

Dit hoofdstuk beschrijft de architectuurprincipes, technische randvoorwaarden en integratie-eisen voor de levering van SOC-dienstverlening door de Opdrachtnemer. De architectuur is leidend voor de inrichting, implementatie, uitvoering, doorontwikkeling en overdracht van de dienstverlening.

Afwijkingen van de in dit hoofdstuk beschreven architectuur zijn uitsluitend toegestaan na schriftelijke goedkeuring van de Deelnemer.

Het uitgangspunt van deze aanbesteding is dat de Opdrachtnemer zijn dienstverlening levert door management van de SIEM-oplossing van de Deelnemer. De SIEM-omgeving van de Deelnemer vormt het centrale platform voor monitoring, detectie, analyse en incidentafhandeling.

De IT-infrastructuur van de Deelnemers is bij aanvang van de Raamovereenkomst hoofdzakelijk gebaseerd op Microsoft-technologie. Vrijwel alle Deelnemers beschikken over Microsoft E5-licenties en maken of gaan primair gebruik maken van Microsoft Sentinel als SIEM-oplossing. De Microsoft Cybersecurity Reference Architecture (MCRA) en de Security Operations Microsoft Reference Architecture worden gehanteerd als richtinggevend architectuurkaders. De Opdrachtnemer dient zijn dienstverlening aantoonbaar in lijn te brengen met MCRA-principes.

De Opdrachtnemer dient zijn dienstverlening zodanig in te richten dat deze aansluit op de SIEM-omgeving en beveiligingsarchitectuur van de Deelnemer.

Indien Deelnemers aanvullende of alternatieve beveiligingsoplossingen gebruiken, worden deze in beginsel gekoppeld aan de SIEM-omgeving van de Deelnemer, tenzij hierover expliciet andere afspraken worden gemaakt.

De Opdrachtgever onderkent dat de IT- en beveiligingsarchitectuur gedurende de looptijd van de Raamovereenkomst kan wijzigen. De Opdrachtnemer dient daarom in staat te zijn te integreren met gangbare SIEM-oplossingen en gebruik te maken van veilige, open en breed geaccepteerde standaarden en protocollen.

Ter voorkoming van vendor lock-in geldt als uitgangspunt dat:

- alle data, configuraties, detectieregels, automatisering (SOAR) en documentatie eigendom blijven van de Deelnemer;

- oplossingen binnen de infrastructuur en beheerdomeinen van de Deelnemer worden geïmplementeerd;
- configuraties en detectielogica exporteerbaar en overdraagbaar zijn;
- de dienstverlening overdraagbaar is naar een opvolgende opdrachtnemer zonder verlies van functionaliteit, kennis of kwaliteit.

2.2 Architectuurprincipes

De Opdrachtnemer dient bij het ontwerpen, implementeren en uitvoeren van de dienstverlening minimaal de volgende architectuurprincipes te hanteren.

2.2.1 Architectuurkaders

De Microsoft Cybersecurity Reference Architecture (MCRA) en de Security Operations Microsoft Reference Architecture worden gehanteerd als richtinggevend architectuurkaders. De Opdrachtnemer dient zijn dienstverlening aantoonbaar in lijn te brengen met MCRA-principes.

2.2.2 Eigenaarschap en datasoevereiniteit

Alle verzamelde beveiligingsdata, configuraties, use-cases, detectieregels, automatisering (SOAR) en documentatie blijven eigendom van de Deelnemer. De Opdrachtnemer dient te waarborgen dat deze informatie volledig beschikbaar, exporteerbaar en overdraagbaar is.

2.2.3 Integratie via open en verplichte standaarden

Koppelingen dienen te worden gerealiseerd op basis van open en breed geaccepteerde standaarden, waaronder waar relevant:

- REST API's
- Syslog
- STIX en TAXII
- JSON en CEF
- OAuth, SAML en OpenID Connect

2.2.4 Overdraagbare dienstverlening

De Opdrachtnemer richt de dienstverlening zodanig in dat overdracht naar een opvolgende opdrachtnemer aantoonbaar mogelijk is. Dit omvat minimaal overdracht van documentatie, configuraties, detectieregels, automatisering (SOAR) en procesbeschrijvingen. Hierbij dient Opdrachtnemer de inrichting, automatiseringen en afhandeling volledig binnen de omgeving van de Provincie in te richten, zonder technische of procedurele afhankelijkheden te introduceren. Exit-strategie perspectief, dient een eigen SOC of een andere opdrachtnemer de monitoring en support geruisloos over te kunnen nemen.

2.2.5 Schaalbaarheid en toekomstvastheid

De architectuur dient schaalbaar te zijn en wijzigingen in IT & OT-landschappen, dreigingsbeelden en beveiligingstechnologieën te kunnen ondersteunen.

2.2.6 Security by design en Zero Trust

De Opdrachtnemer dient beveiligingsprincipes zoals Zero Trust, least privilege en continue verificatie te ondersteunen.

2.2.7 Transparantie en auditability

Alle monitoring-, detectie- en analyseactiviteiten dienen volledig auditeerbaar te zijn.

2.2.8 Herbruikbaarheid en standaardisatie

Detectieregels, use-cases en integraties dienen herbruikbaar en gestandaardiseerd te worden ingericht.

2.2.9 Aanvullende eisen

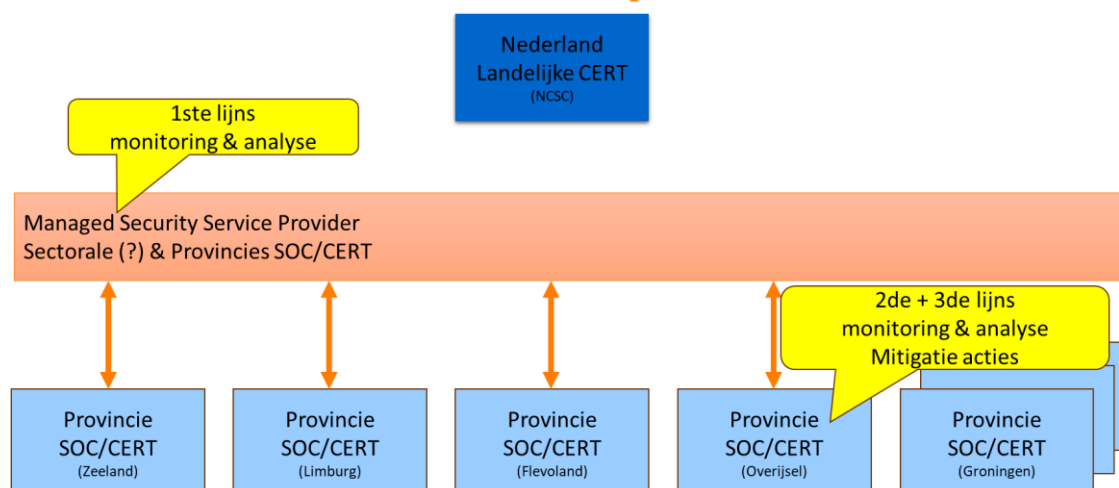
Eisen	
	MCRA-conformiteitsmatrix
2.9.1	Opdrachtnemer overlegt bij inschrijving een MCRA-conformiteitsmatrix waaruit blijkt hoe zijn dienstverlening aansluit op de relevante lagen van de MCRA (Identity & Access, Endpoint Security, Multi-Cloud Security, Security Operations). Afwijkingen worden gemotiveerd
3.1.2	Personeel heeft uitsluitend Just-In-Time (JIT) toegang via Privileged Identity Management (PIM)
3.1.3	Alle toegang wordt gelogd en is auditeerbaar (session recording)
3.1.4	Multi-factor authenticatie (MFA) is verplicht voor alle SIEM-toegang en gegevenstoegang bij de Deelnemers
3.1.5	Geen persistente service accounts met brede rechten; automatisering via service principals met minimale rechten

2.3 Sectoraal SOC

De basisarchitectuur gaat uit van aansluiting van de Opdrachtnemer op de individuele SIEM-omgevingen van de afzonderlijke Deelnemers.

De Opdrachtnemer dient sectorale dreigingsinformatie en relevante beveiligingsinzichten te delen met de andere Deelnemers, met inachtneming van geldende wet- en regelgeving, dataclassificatie, onderlinge afspraken en vertrouwelijkheidsvereisten. Waar noodzakelijk dient informatie te worden geanonimiseerd of gepseudonimiseerd.

Sectorale SOC Provincies (zonder centraal team)



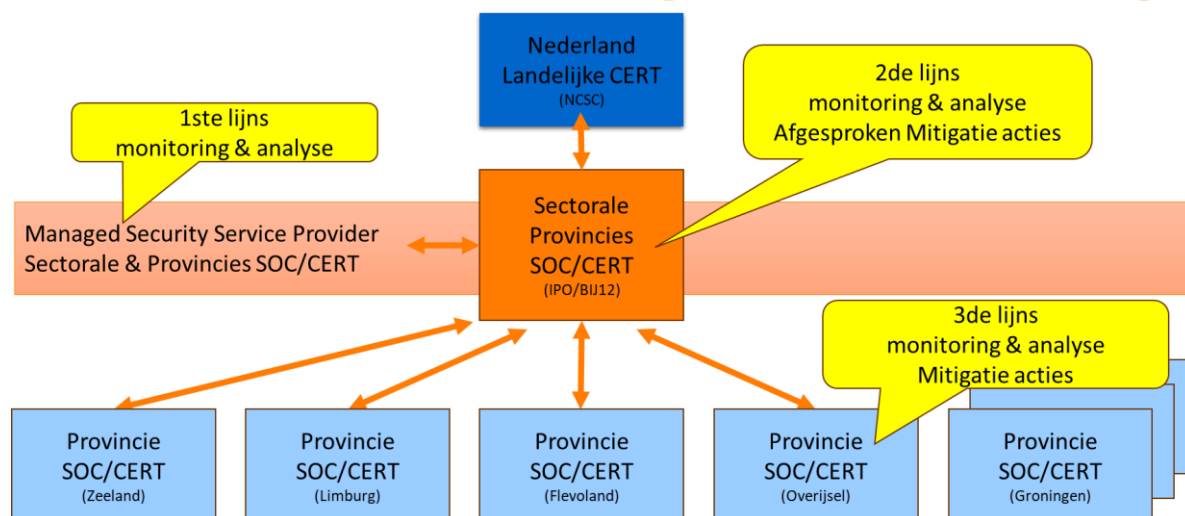
Opdrachtgever en Deelnemers onderkennen dat sectorale samenwerking kan worden ingericht in de vorm van een centraal SOC- of CERT-team. De Opdrachtnemer dient zijn dienstverlening zodanig in te richten dat integratie met een dergelijk centraal team gedurende de looptijd van de Raamovereenkomst mogelijk is.

De Opdrachtnemer dient ondersteuning te kunnen bieden bij:

- samenwerking tussen Deelnemers;
- sectorale dreigingsanalyse;

- kennisdeling;
- gezamenlijke responsactiviteiten.

Sectorale SOC Provincies (met centraal team)



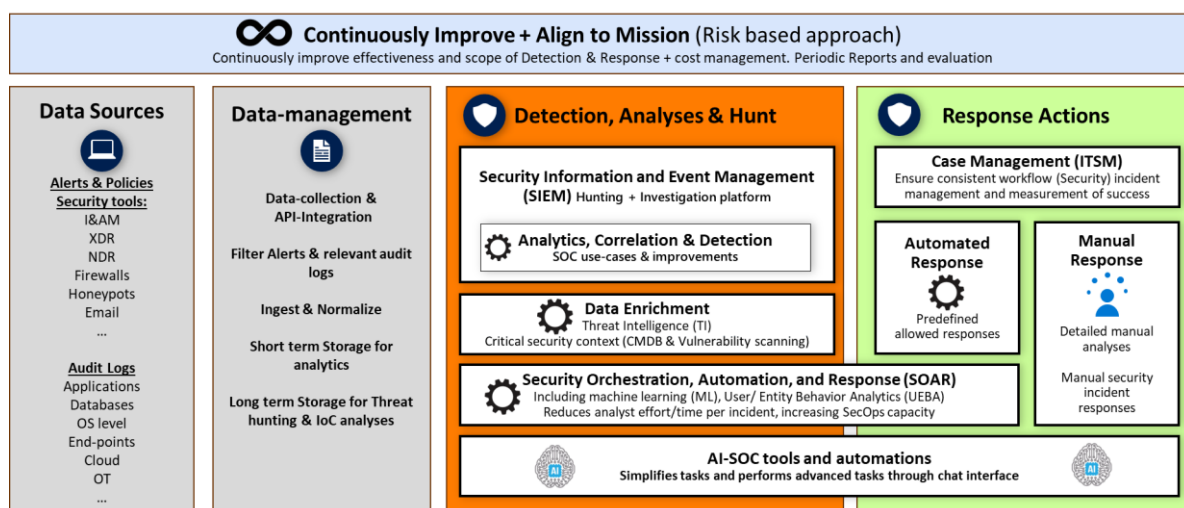
2.4 Provinciale SIEM-SOC Architectuur

De provinciale SIEM-SOC architectuur is gebaseerd op een gedistribueerd model waarbij:

- SIEM-omgevingen bij individuele Deelnemers zijn ingericht;
- SOC-dienstverlening centraal wordt geleverd door de Opdrachtnemer;
- samenwerking en informatie-uitwisseling tussen Deelnemers wordt gefaciliteerd.

De Opdrachtnemer dient de referentiearchitectuur van Opdrachtgever te ondersteunen en waar nodig verder uit te werken. Hierbij dient rekening te worden gehouden met scheiding van verantwoordelijkheden, datastromen en beveiligingsdomeinen.

Provinciale SIEM-SOC Architectuur - Conceptueel



2.5 SIEM en SOC

De SIEM-omgeving vormt het centrale platform voor het verzamelen, correleren en analyseren van beveiligingsinformatie. Het SOC omvat de processen, tooling en expertise voor monitoring, analyse, detectie en incidentafhandeling.

De Opdrachtnemer dient:

- gebruik te maken van de SIEM-omgeving van de Deelnemer als primaire monitoringomgeving;
- detectieregels, use-cases en automatisering (SOAR) te ontwikkelen, implementeren, onderhouden en te optimaliseren;
- monitoring- en incidentprocessen te beheren en te optimaliseren;
- rolgebaseerde toegangscontrole toe te passen;
- analistenactiviteiten te loggen en auditeerbaar te maken en bij te houden;
- zorg te dragen voor reproduceerbare en overdraagbare inrichting van detectie- en analysemethoden.

2.6 Databronnen – Security Tooling

De SIEM-omgeving wordt gevoed met meldingen en signalen uit beveiligingsoplossingen binnen de infrastructuur van de Deelnemer.

De Opdrachtnemer dient integratie te realiseren met onder andere:

- identity- en toegangsbeveiliging;
- endpoint- en serverbeveiliging;
- netwerkdetectie en firewalloplossingen;
- e-mail- en samenwerkingsbeveiliging;
- cloud security tooling.

De Opdrachtnemer dient:

- detecties en policies te benutten en waar nodig te optimaliseren;
- integraties te realiseren zonder negatieve impact op beschikbaarheid of prestaties van bronoplossingen;
- prioriteit te geven aan kritieke systemen en bedrijfsprocessen.

2.7 Databronnen – Audit Logs

De Opdrachtnemer dient audit- en activiteitslogs te verwerken afkomstig uit onder andere:

- applicaties;
- databases;
- besturingssystemen;
- endpoints;
- cloud-omgevingen;
- OT- en IoT-omgevingen, indien van toepassing.

Logverzameling dient te voldoen aan relevante wet- en regelgeving, beveiligingsrichtlijnen en bewaartermijnen. De Opdrachtnemer dient de integriteit, beschikbaarheid en vertrouwelijkheid van logdata te waarborgen.

Auditlogs dienen te worden ingezet voor:

- threat hunting / IoC analyses
- incidentonderzoek;
- forensische analyse;
- trendanalyse;
- compliance-doeleinden.

2.8 Datamanagement

Datamanagement omvat alle processen en voorzieningen voor het verzamelen, transporteren, filteren, normaliseren, classificeren, opslaan en beschikbaar stellen van beveiligingsdata.

De Opdrachtnemer dient:

- dataverzameling schaalbaar en efficiënt in te richten;

- filtering en normalisatie toe te passen om analyse te optimaliseren;
- dataclassificatie toe te passen;
- data versleuteld te transporteren;
- retentiebeleid te ondersteunen conform wettelijke en organisatorische eisen;
- datastromen te implementeren op basis van open integratiestandaarden;
- forensische bruikbaarheid en chain-of-custody van logdata te waarborgen;
- evaluatie en optimalisatie ook vanuit kosten perspectief.

De inrichting van datamanagement dient bij te dragen aan optimale detectiekwaliteit, prestaties en beheersbaarheid van kosten.

2.9 Data Enrichment

Data enrichment betreft het verrijken van beveiligingsmeldingen met contextinformatie om incidentanalyse en prioritering te verbeteren.

De Opdrachtnemer dient gebruik te maken van verrijgingsbronnen, waaronder:

- threat intelligence;
- configuratie- en assetinformatie;
- kwetsbaarheidsinformatie;
- bedrijfscontext en classificatie van systemen.

De Opdrachtnemer dient de kwaliteit en actualiteit van verrijgingsbronnen te borgen en verrijking geautomatiseerd en reproduceerbaar uit te voeren.

2.10 Beheer van Security Policies binnen Microsoft Security Stack

De Opdrachtnemer vervult een regisserende en uitvoerende rol bij het beheer en de optimalisatie van security detectie- en response policies binnen de Microsoft security stack van de Deelnemer.

Daarbij geldt dat:

- de Opdrachtnemer verantwoordelijk is voor inrichting, beheer en optimalisatie van security detectie policies en bijbehorende alerting;
- de Opdrachtnemer Deelnemer adviseert over preventieve security policies en wijzigingen daarop;
- de Opdrachtnemer verantwoordelijk is voor inrichting en beheer van response policies en escalatiemechanismen;
- de Deelnemer eindverantwoordelijk blijft voor beleidsbesluiten en risicobeoordeling.