TLP:GREEN

OR-2 PROCESMODEL

Monitoring & Detectie – SOC Operational Readiness - Assetmanagement

Best Practice versie 1.3

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor IT-architecten, IT-beheerders, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	28-01-2025	Initiële versie
V1.1	05-02-2025	Aanpassingen document opmaak
V1.2	19-02-2025	Toevoeging document context
V1.3	06-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Implementatieplan	Zie "OR-2, Implementatieplan" onder SOC Operational Readiness - Producten
Overzicht Kroonjuwelen	Zie "OR-2, Overzicht Kroonjuwelen" onder SOC Operational Readiness - Producten
BIO	https://www.bio-overheid.nl/
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

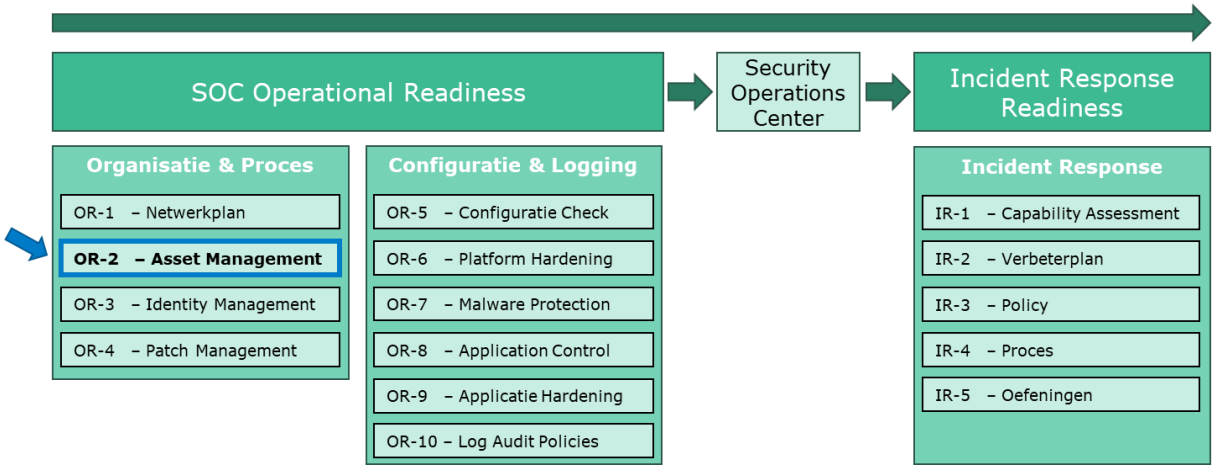
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Organisatie & Proces** in het VSSR-Minipoducten raamwerk.



Figuur 1: Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in *Tabel 1* per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document het **procesmodel** voor **asset management** (OR-2), binnen **Organisatie & Proces**, behandelt.

Organisatie & Proces	Configuratie & Logging
Procesmodel	Configuratiehandleiding
Implementatieplan	Implementatieplan (generiek of specifiek)
Inventarisatiesheet	Progressie checklist

Tabel 1: Miniproducten breakdown

3 Assetmanagement

Dit hoofdstuk beschrijft een generiek procesmodel voor het assetmanagementproces, met als doel een werkend proces binnen de organisatie te creëren. Dit proces dient als basis om het SOC (Security Operations Center) te voorzien van relevante informatie, waarmee detectiesystemen effectief kunnen worden ingericht.

Om een compleet beeld te geven, wordt eerst het algemene assetmanagementproces uitgelegd. Vervolgens wordt er specifiek ingezoomd op de vereisten die noodzakelijk zijn voor een effectieve SOC-dienstverlening. Hiermee wordt een solide fundament gelegd voor het optimaal ondersteunen van de SOC-activiteiten.

3.1 Inleiding

Asset Management is een gestructureerde aanpak om de assets van een organisatie, zoals gegevens, applicaties, hardware en software, te identificeren, classificeren en beheren. Het doel is om operationele efficiëntie, beveiliging en naleving van wet- en regelgeving te waarborgen. Met een risicogestuurde classificatie op basis van de BIO-standaard worden kritieke assets geïdentificeerd en beschermd. Voor een SOC (Security Operations Center) is inzicht in assets essentieel om detectieregels te definiëren en prioriteiten te stellen voor kroonjuwelen – de meest waardevolle assets. Hiervoor is gedetailleerde informatie nodig, zoals het type besturingssysteem, IP-adres, de locatie en het eigenaarschap van de assets.

Randvoorwaarden voor succes:

- Een vastgesteld Asset Management-beleid.
- BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) volgens organisatierichtlijnen.
- Identificatie en documentatie van kroonjuwelen zoals beschreven in de bijbehorende bijlagen *"Implementatieplan"* en *"Overzicht Kroonjuwelen".*
- Duidelijke scope en afbakening van processen.
- Periodieke evaluatie en verbetering.
- Afstemming met stakeholders en geschikte tools.
- Duidelijke verantwoordelijkheden en eigenaarschap.

Met deze aanpak kan een organisatie proactief reageren op bedreigingen, regelgeving naleven, belangrijke middelen beschermen en bedrijfscontinuïteit ondersteunen, terwijl verdere optimalisatie toekomstige verbeterpunten biedt. Meer informatie over BIO-standaarden is beschikbaar via de officiële BIO-pagina https://www.bio-overheid.nl/.

3.2 Beschrijving en uitleg van het proces

Het Asset Management Procesmodel wordt uitgevoerd door de organisatie om assets te identificeren, classificeren en beheren. Hieronder worden de belangrijkste stappen van het assetmanagementprocesmodel beschreven.

3.2.1 Asset Management Proces Flowchart

De flowchart bevat de volgende belangrijke fasen:

1. Start

2. **Asset Identificatie** – Deze stap is van essentieel belang voor een SOC om een goed beeld te krijgen van de aanwezige assets binnen een organisatie.

3. **Asset Classificatie** – Deze fase is van groot belang om assets te classificeren op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid, waarbij overheidstandaarden zoals

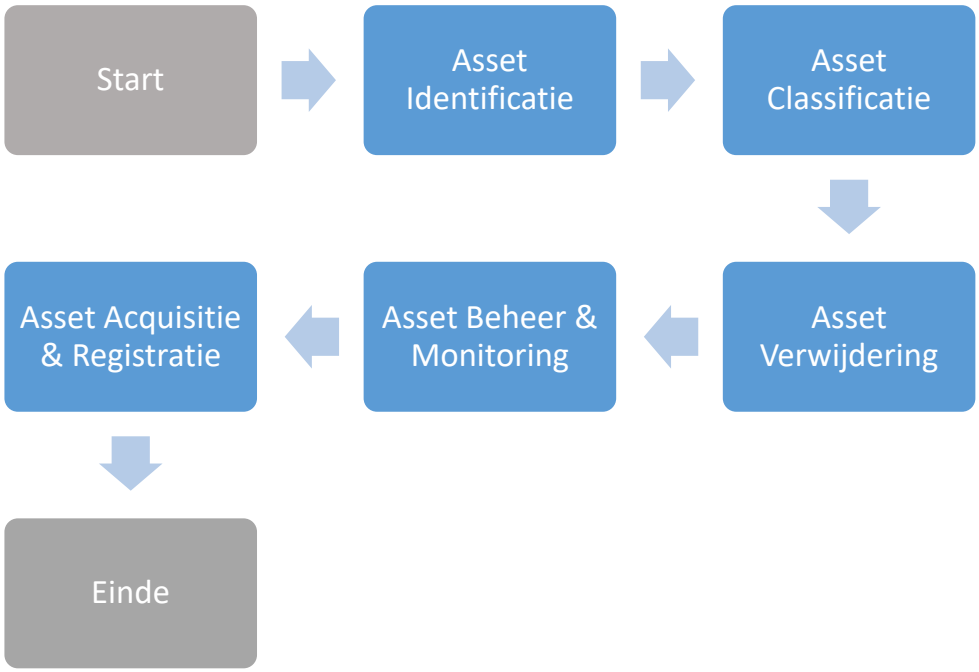
BIO als uitgangspunt gebruikt kan worden. Het resultaat van deze classificatie kan door het SOC gebruikt worden om de juiste prioriteit te geven aan assets van een organisatie.

4. **Asset Acquisitie & Registratie** – Deze fase is voor het SOC van groot belang om een nieuwe assets ook daadwerkelijk op te nemen in de beveiligingsmonitoring (Onboarding).

5. **Asset Beheer & Monitoring** – Deze fase is van belang voor het SOC om op de hoogte te blijven van veranderingen aan assets binnen een organisatie en daar adequaat veranderingen voor door te voeren in de beveiligingsmonitoring maatregelen.

6. **Asset Verwijdering** – Deze fase is voor het SOC van groot belang om assets ook daadwerkelijk te verwijderen in de beveiligingsmonitoring (Offboarding).

7. Einde



Figuur 1 Asset Management fases

3.2.2 Detail processtappen

Het Asset Management Procesmodel wordt uitgevoerd door de organisatie om assets te identificeren, classificeren en beheren. Hieronder worden de belangrijkste stappen van het assetmanagementprocesmodel in meer detail beschreven.

3.2.2.1 Asset Identificatie

Doel: Het ontdekken van alle assets binnen de organisatie om een solide basis te leggen voor efficiënte tracking, beheer en ondersteuning van SOC-diensten. Het stelt het SOC in staat om beter inzicht te krijgen in de infrastructuur, prioriteiten te stellen bij incidentrespons en beveiligingscontroles effectiever te implementeren.

Beschrijving: De stap Asset Identificatie brengt alle organisatorische middelen in kaart en documenteert belangrijke details zoals type, eigenaar en locatie. Een complete asset-inventaris is cruciaal voor risicoclassificatie, het identificeren van kroonjuwelen en effectieve SOC-monitoring. Het vormt de basis voor verbeterd risicobeheer, netwerkzichtbaarheid en strategische beveiliging.

Input:

Asset gegevens

Organisatie richtlijnen voor het bepalen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de assets op basis van gebruikte overheidstandaarden zoals Baseline Informatieveiligheid Overheid (BIO).

Activiteiten:

- Voer fysieke en/of virtuele scans uit om verborgen assets op te sporen,
- Creëer een gedetailleerde en complete lijst van alle assets

Output: Een geverifieerde lijst met alle assets, gereed voor classificatie en integratie in de SOC-processen.

3.2.2.2 Asset Classificatie

Doel: Classificeer assets op basis van BIV om beheers- en beveiligingsmaatregelen te prioriteren, zodat het Security Operations Center (SOC) effectief kan reageren op incidenten.

Beschrijving: Classificeer de organisatorische assets om de prioriteit voor beveiligingsmaatregelen en monitoring te bepalen, zodat het SOC zich kan richten op de meest kritieke assets in geval van een beveiligingsincident.

Input:

Lijst van Geïdentificeerde Assets: Een uitgebreide inventaris van alle assets binnen de organisatie.

BIV Classificaties: Beoordeling van elke asset op basis van Vertrouwelijkheid, Integriteit en Beschikbaarheid. Gebruik daarvoor als input bestaande overheidstandaarden zoals Baseline Informatiebeveiliging Overheid (BIO).

Activiteiten:

- Gebruik de BIO standaard als uitgangspunt voor het classificeren van assets op basis van BIV. De BIO standaard onderkent 3 niveaus voor de BIV-classificaties: Hoog, middel en laag.
- Werk de Assetregistratie Bij:
  - Werk de assetregistratie bij met de classificatie en risicobeoordeling, zodat het SOC deze kan gebruiken om prioriteit te geven aan monitoring en reactie-inspanningen.
- Identificeer de organisatie kroonjuwelen op basis van BIV-classificatie en risicoanalyse en leg deze vast in de bijlage Overzicht Kroonjuwelen t.b.v. SOC-operatie.

Output: Geclassificeerd Overzicht van Kroonjuwelen voor de SOC-operatie.

3.2.2.3 Asset Acquisitie & Registratie

Doel: Het doel van de stap Asset Acquisitie & Registratie is om ervoor te zorgen dat alle assets geïdentificeerd, geëvalueerd en op de juiste manier geïntegreerd worden in de asset registratie- en SOC-monitoringssystemen van de organisatie.

Beschrijving: Documenteer assets en voer ze op in het asset managementsysteem of andere gekozen vorm van asset registratie. Communiceer de asset toevoeging aan het SOC zodat de beveiligingsmonitoring hierop aangepast wordt.

Input: Inkoopgegevens, Leveranciersinformatie en basis configuratiestandaarden.

Activiteiten:

- Registreer assetgegevens (bijv. Operating Systeem Type en versie, hostname, IP-adres, Servicepoorten, Eigenaar, Applicatie en assetclassificatie (zie stap voor asset classificatie).
- Asset administratie bijwerken.
- Toevoegen van de asset aan de beveiligingsmonitoring.

Output: Bijgewerkte inventaris van assets met nieuwe toevoegingen.

3.2.2.4 Asset beheer & monitoring

Doel: De functionaliteit en beveiliging van assets behouden door middel van regelmatige monitoring en updates.

Beschrijving: Zorg ervoor dat alle assets regelmatig in de administratie worden bijgewerkt en gecontroleerd. Stel hiervoor periodieke controle momenten in en draag zorg voor administratie eigenaren (IT Asset managers) die verantwoordelijk gesteld worden voor een continue bijgewerkte asset registratie.

Input: Asset database, Onderhoudsschema.

Activiteiten:

- Voer regelmatig controles en updates uit,
- Gebruik en status van bedrijfsmiddelen bewaken.

Output: Logboeken van onderhouds- en monitoringacties, bijgewerkte rapporten over de status van de assets.

3.2.2.5 Asset verwijdering

Doel: Aan het einde van hun levenscyclus veilig verwijderen van assets.

Beschrijving: Verwijder assets uit actief gebruik, zorg ervoor dat gegevens worden gewist en vernietig fysieke assets op een veilige manier. Communiceer de asset toevoeging aan het SOC zodat de beveiligingsmonitoring hierop aangepast wordt.

Input: Asset verwijderingsbeleid, verwijderingsverslagen.

Activiteiten:

- Gegevens van apparaten wissen,
- Gooi hardware weg of recycle deze volgens de voorschriften,
- Documenteer de verwijdering voor auditdoeleinden.
- Verwijderen van de asset uit de beveiligingsmonitoring.

Output: Rapport over verwijderde assets, bijgewerkte asset database.

3.3 RACI Matrix

Hieronder is de RACI-matrix voor alle bovengenoemde stappen beschreven.

Rol	IT Asset Manager	IT-manager	Afdelingsmanagers	IT-beheer	Security Team/Compliance Officer	Asset Eigenaren	Risicomanager	IT Support	Eindgebruikers	IT Inkoop/IT Inkoop Manager	Financiële administratie
Asset Identificatie	R	A	C	I	I						
Asset Classificatie	R	A			C		C		I		
Asset Acquisitie & Registra	R		C						I	R,A	
Asset Beheer & Monitoring		A	C		R,C,I	I		R			
Asset verwijdering	R	A			R,C	I					I

Figuur 2 - RACI Matrix

Een RACI-model is een hulpmiddel voor het definiëren van rollen en verantwoordelijkheden binnen een project of proces. Het staat voor:

- **R** (Responsible): Degene die verantwoordelijk is voor de uitvoering van een taak of activiteit. Dit is de persoon die het werk uitvoert.
- **A** (Accountable): Degene die eindverantwoordelijk is. Deze persoon zorgt ervoor dat de taak correct en tijdig wordt uitgevoerd en geeft goedkeuring.
- **C** (Consulted): Personen of teams die geraadpleegd worden voor hun input of expertise. Dit zijn vaak belanghebbenden die adviseren.
- **I** (Informed): Personen of teams die geïnformeerd moeten worden over de voortgang of resultaten, maar geen directe betrokkenheid hebben.

3.4 Rol Beschrijvingen

Hier wordt de rolbeschrijving verder uitgewerkt, evenals de bijbehorende belangrijkste verantwoordelijkheden van de rol.

1. IT Asset Manager
    - Beschrijving: Verantwoordelijk voor het toezicht houden op de gehele levenscyclus van assets, inclusief identificatie, classificatie, verwerving, monitoring en verwijdering. Ze zorgen voor nauwkeurige assetregistraties, coördineren met andere afdelingen en handhaven het beleid voor assetmanagement.

- Belangrijkste verantwoordelijkheden: Het volgen van assets, het beheren van de assetdatabase, het waarborgen van de naleving van het assetbeleid en het coördineren van asset-activiteiten tussen afdelingen.

2. IT-Manager
    - Beschrijving: Toezicht te houden op de implementatie, werking en naleving van het asset management proces binnen de organisatie.
    - Belangrijkste verantwoordelijkheden: Het beheren van risico's, zorgen voor compliance en optimaliseren processen om beveiliging en efficiëntie te waarborgen.
3. Afdelingsmanagers
    - Beschrijving: Zorgt voor goedkeuring van toegangsverzoeken en waarborgt dat medewerkers alleen toegang hebben tot systemen die relevant zijn voor hun functie.
    - Belangrijkste verantwoordelijkheden: Bewaakt de naleving van de interne beleidsregels binnen de afdeling.
4. IT Inkoop
    - Beschrijving: Verantwoordelijk voor het werven en verwerven van assets volgens het beleid en de behoeften van de organisatie. Ze coördineren de aankoop van assets, onderhandelen met leveranciers en houden inkoopgegevens bij.
    - Belangrijkste verantwoordelijkheden: Het beheren van leveranciersrelaties, ervoor zorgen dat assets aan de vereisten voldoen en het faciliteren van de registratie en tracering van assets met de IT Asset Manager.
5. Security Team
    - Omschrijving: Verantwoordelijk voor het beoordelen van de beveiligingseisen voor assets en het implementeren van beschermende maatregelen, met name voor assets met een hoog risico. Ze werken samen met de IT Asset Manager om kritieke assets te identificeren en ervoor te zorgen dat de beveiligingsprotocollen worden nageleefd.
    - Belangrijkste verantwoordelijkheden: Assets bewaken op beveiligingskwetsbaarheden, toegangscontroles implementeren en veilige verwijdering van assets ondersteunen.
6. Risk Manager
    - Beschrijving: Geraadpleegd tijdens de classificatie van assets om de potentiële impact en risico's van verschillende soorten assets te beoordelen. Ze leveren input over risiconiveaus ter ondersteuning van prioritering in asset management.
    - Belangrijkste verantwoordelijkheden: Evaluatie van risiconiveaus voor assets, advies geven over de omgang met kritieke assets en ondersteunen van de naleving van het risicobeheerbeleid.
7. Compliance Officer
    - Beschrijving: Toetst of asset managementprocessen voldoen aan interne richtlijnen en externe regelgeving, en voert audits uit om naleving te waarborgen.
    - Belangrijkste verantwoordelijkheden: Zorgen voor naleving van regelgeving, herzien van beleid en ondersteunen bij auditvereisten.

8. IT Support

    - Beschrijving: Verantwoordelijk voor doorlopend beheer en monitoring van bedrijfsmiddelen, inclusief software-updates, patching en probleemoplossing. Ze zorgen ervoor dat assets functioneel blijven en ondersteunen de dagelijkse IT-activiteiten.

    - Belangrijkste verantwoordelijkheden: Het uitvoeren van regelmatig onderhoud, het oplossen van problemen met bedrijfsmiddelen en het bijwerken van activarecords na onderhoud.

9. Financiële administratie

    - Beschrijving: Geïnformeerd over acquisities en desinvesteringen om financiële gegevens, budgettering en afschrijving van assets te beheren. Ze zorgen ervoor dat de financiële implicaties van assetmanagement worden gevolgd en afgestemd op de begrotingsdoelstellingen.
    - Belangrijkste verantwoordelijkheden: Het bijwerken van financiële gegevens, het bijhouden van de afschrijving van assets en het ondersteunen van de budgettering voor het verwerven en afstoten van assets.

10. Asset eigenaren

    - Beschrijving: Medewerkers die zijn aangewezen om specifieke assets te gebruiken binnen hun functie. Zij zijn op de hoogte van de classificatie van assets en zijn verantwoordelijk voor het juiste gebruik en de basiszorg van de assets.
    - Belangrijkste verantwoordelijkheden: Zorgen voor een veilig en gepast gebruik van assets, eventuele problemen melden aan IT en ondersteunen van inspanningen voor het volgen van assets door het IT-beleid te volgen.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

januari 2025

Assetmanagement: Procesmodel
Versie 1.3