TLP:GREEN

OR-3 PROCESMODEL

Monitoring & Detectie – SOC Operational Readiness - Identitymanagement

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	29-01-2025	Initiële versie
V1.1	05-02-2025	Aanpassingen document opmaak
V1.2	19-02-2025	Toevoeging document context
V1.3	07-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Implementatieplan	Zie "OR-3, Implementatieplan" onder SOC Operational Readiness - Producten
Accountoverzicht	Zie "OR-3, Accountoverzicht" onder SOC Operational Readiness - Producten
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

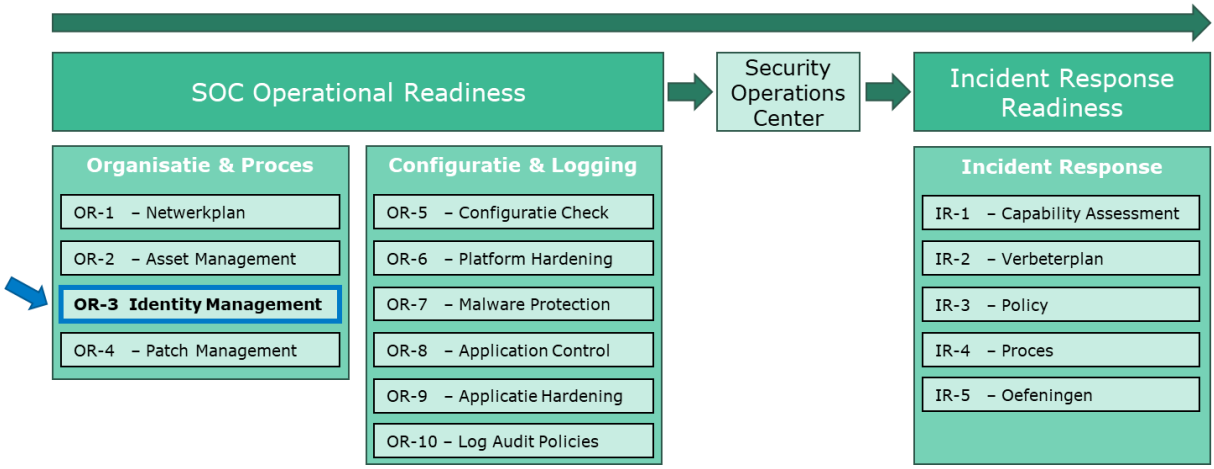
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **Identity Management** (OR-3), binnen **Organisatie & Proces**, behandelt.

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

Tabel 1: Miniproducten breakdown

3 Identity Management

In dit document wordt een voorbeeld identity managementproces beschreven. Hierbij worden zeven verschillende onderdelen benoemt. Bepaalde onderdelen worden extra belicht aangezien deze van groot belang zijn voor het Security Operations Center (SOC) en voor de "***identity management implementatie"*** en het "***account overzicht"***.

3.1 Inleiding

Effectieve Identity Management (IdM) is cruciaal voor een organisatie omdat het een centraal punt biedt voor het beheren en monitoren van gebruikersaccounts, wat helpt bij het voorkomen van ongeautoriseerde toegang. Voor kleine tot middelgrote organisaties zorgt het gebruik van een IdM-proces ervoor dat alleen geautoriseerde personen toegang hebben tot de middelen van de organisatie en inzicht in de verschillende accounts die worden gebruikt. Dit proces heeft dus ook betrekkingen op de BIO (Baseline Informatiebeveiliging Overheid) paragraaf 9.2 aangezien het beheer van wijzigingen van invloed heeft op toegangsrechten en autorisaties binnen systemen. Het doel is om wijzigingen gecontroleerd en veilig door te voeren om de continuïteit en veiligheid van systemen te waarborgen.

Als het IdM-proces goed is ingericht, biedt dit de mogelijkheid om een SOC van de juiste informatie te voorzien voor het monitoren op speciale accounts en afwijking op gedrag van reguliere gebruikersaccounts. Daarnaast is de juiste informatie voor een SOC van belang bij het uitlopen van incidenten. Met de juiste contact informatie kan sneller en efficiënter contact worden gezocht met eigenaren van accounts.

Randvoorwaarden voor een succesvol IdM-proces:

- Het ontwikkelen of gebruik bestaande beleidslijnen die het Identity Management-beleid regelen. Voor een organisatie is het van belang omdat het duidelijke richtlijnen en regels biedt voor het beheren van accounts en toegangsrechten.
- De organisatie heeft richtlijnen opgesteld voor het gebruik en beheer van accounts.
- Verantwoordelijkheden en eigenaarschap voor accountbeheer zijn helder gedefinieerd.
- Periodieke controle en actualisatie van accounts en toegangsrechten worden uitgevoerd.
- Tools en systemen voor het beheren en monitoren van gebruikersaccounts zijn beschikbaar.
- Afstemming met relevante stakeholders, zoals IT, HR en het SOC, is gerealiseerd.

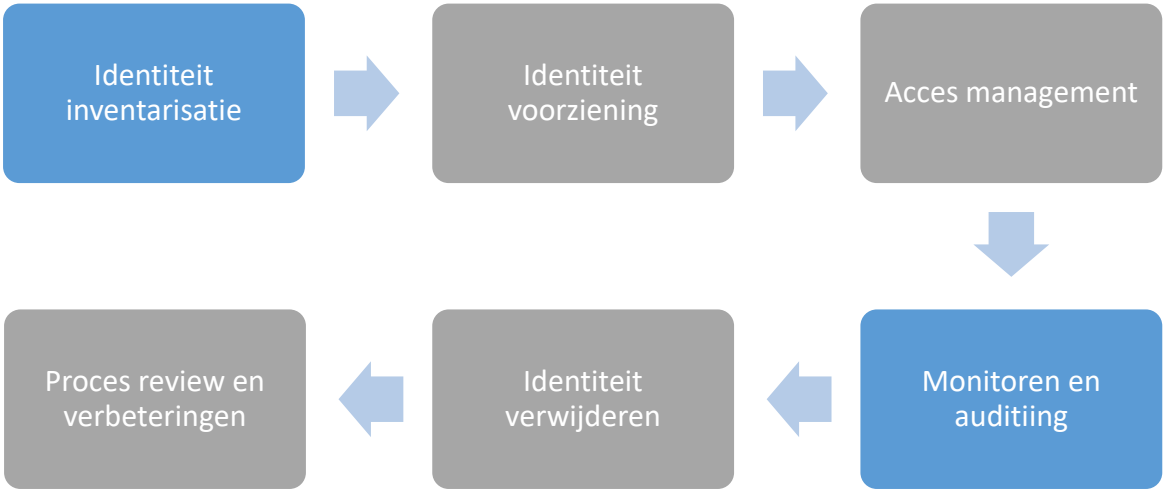
Dit document maakt onderdeel uit van een set van drie documenten: 1) "***IdM-Procesmodel"***; 2) ***"IdM-Implementatieplan"***; en, 3) ***"Account Overzicht"***. Deze drie documenten kunnen gezamenlijk worden gebruikt om eerst een proces voor de organisatie op te stellen om daarna het proces te implementeren, en om als laatste in het Account Overzicht alle informatie voor een SOC(-dienst) te verzamelen.

3.2 Beschrijving en uitleg van het proces

Het voorbeeld IdM-proces bevat zeven onderdelen. Van deze zeven procesonderdelen, zijn er drie van essentieel belang om een SOC-dienst van correcte informatie te voorzien: identiteit creatie, beleid ontwikkeling en monitoren en auditing. Deze processen zijn essentieel, omdat ze zorgen voor de juiste toegang, beveiliging en controle over wie welke acties mag uitvoeren binnen de organisatie. Deze drie onderdelen zijn in onderstaand diagram blauw gemarkeerd. Dit proces ondersteunt en zorgt voor een fundament bij het verder invullen van "***identity management implementatie"*** en "***account overzicht"***, wat van belang is voor het aansluiten aan een SOC.

3.2.1 Identity Management Proces Flowchart

Hieronder staat een flowchart van de zes stappen binnen het identity managementproces. Vervolgens volgt een uitleg per processtap, inclusief de beschrijving, het doel, de invoer, de activiteiten en de uitvoer. Hierbij zijn twee onderdelen blauw gekleurd aangezien ze van essentieel belang zijn voor de implementatie van security monitoring door een SOC



Figuur 1

3.2.2 Identiteit inventarisatie

- **Doel**: Een Inventarisatie opbouwen van alle bestaande identiteiten, hierdoor is het voor een organisatie gemakkelijk om zicht te krijgen in alle gebruikers.

- **Beschrijving**: Stel een uitgebreide lijst samen van alle identiteiten (gebruikers, service-accounts, applicatie-accounts, enz.) binnen de organisatie. De verschillende accounts kunnen worden opgenomen in het "***account overzicht"***.
- **Invoer**: De naamconventie van de verschillende vormen van accounts.

- **Activiteiten**:

  - Gegevens verzamelen uit verschillende bronnen.
  - Alle actieve en inactieve accounts identificeren.
  - Accounts categoriseren (bijv. admin, service, standaard).
  - Noteren in het "***account overzicht"***.

- **Uitvoer**: Gedetailleerd identiteitsinventarisatierapport.

3.2.3 Identiteit voorziening

- **Doel**: Zorgen dat identiteiten worden aangemaakt volgens gestandaardiseerde procedures.
- **Beschrijving**: Implementeer procedures voor het creëren en beheren van accounts.
- **Invoer**: Identity Managementbeleid en identiteitsinventarisatierapport.
- **Activiteiten**:
  - Gebruikersaccounts opzetten.
  - Geschikte toegangslevels toewijzen.
  - Acties voor provisioning documenteren.
- **Uitvoer**: Correcte gebruikersaccounts met de juiste toegang.

3.2.4 Acces management

- **Doel**: Zorgen dat gebruikers alleen toegang hebben tot de middelen die ze gedurende een bepaalde periode nodig hebben.
- **Beschrijving**: Beheer en controleer de toegangsrechten voor alle identiteiten.
- **Invoer**: Gebruikersrollen en verantwoordelijkheden en toegangscontrolebeleid
- **Activiteiten**:
  - Rollen en permissies toewijzen.
  - Toegangsrechten periodiek beoordelen.
  - Toegang bijwerken naarmate rollen veranderen.
- **Uitvoer**: Bijgewerkte toegangscontrolelijsten.

3.2.5 Monitoren en auditing

- **Doel**: de beveiliging en compliance binnen een organisatie te waarborgen.
- **Beschrijving**: Het SOC houdt toezicht op beveiligingsincidenten en afwijkingen, en kan signaleren wanneer toegangsrechten niet langer in lijn zijn met de actuele behoeften of rollen van gebruikers. In relatie met de BIO-9.2.5 kunnen organisaties ervoor zorgen dat toegangsrechten niet alleen correct worden toegewezen, maar ook regelmatig worden gecontroleerd en aangepast. Auditing daarentegen omvat een systematische evaluatie van identiteitsbeheerprocessen om te waarborgen dat deze voldoen aan beleidslijnen en regelgeving. Door regelmatig audits uit te voeren, kunnen organisaties afwijkingen identificeren en hun beveiliging verbeteren.
- **Invoer**: omvat het notuleren van gegevens over bepaalde accounts, toegangsrechten en activiteiten binnen systemen
- **Activiteiten**:
  - Inlogactiviteiten monitoren.
  - Toegangsrechten en wijzigingen auditen.
  - Nalevingsrapporten genereren.
- **Uitvoer**: Audit- en monitoringsrapporten.

3.2.6 Identiteit verwijderen

- **Doel**: De toegang van gebruikers tot systemen, applicaties en gegevens veilig en efficiënt in te trekken wanneer deze niet langer nodig is.

- **Beschrijving**: Verwijder toegangsrechten en deactiveer identiteiten of accounts wanneer ze niet langer nodig zijn.

- **Invoer**: Ontslagberichten en wijzigingen in rolmeldingen.

- **Activiteiten**:

  - Gebruikersaccounts deactiveren.
  - Toegangsrechten intrekken.
  - Acties voor deprovisioning documenteren.

- **Uitvoer**: Gedeactiveerde en/of verwijderde gebruikersaccounts en logging van de succesvolle acties.

3.2.7 Proces review en verbeteringen

- **Doel**: De efficiëntie en effectiviteit van identity management proces verbeteren.

- **Beschrijving**: Door regelmatige evaluaties kunnen inefficiënties, fouten of beveiligingslekken in de workflows worden geïdentificeerd en opgelost.

- **Invoer**: Auditrapporten en feedback van belanghebbenden.

- **Activiteiten**:

  - Auditbevindingen analyseren.
  - Procesknelpunten identificeren.
  - Verbeteringen implementeren.

- **Uitvoer**: Bijgewerkte identity managementproces documentatie.

3.2.8 RACI Matrix

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

Rol	IT Administrator	IT-Manager	Afdelingsmanagers	SOC (Security Operations Center)	Security Officer	Juridisch adviseur	Compliance Officer	HR-Vertegenwoordiger	Security Analist
Beleid ontwikkeling		C			R,A,C,I	C		I	
Identiteit creatie	R,C	A,C,I		C					
Identiteit voorziening	R	A,I						C	
Acces managment	R	A	C						A,I
Monitoren en auditing	C			A	A		C		R,A
Identiteit verwijderen	R		C					A	R,I
Proces review en verbeteringen		R,A,C,I			C		C	I	

Figuur 2

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.

3.3 Rol beschrijving

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

- **IT Manager**
  - **Beschrijving:** Toezicht te houden op de implementatie, werking en naleving van identity management proces binnen de organisatie.
  - **Belangrijkste verantwoordelijkheden:** Het beheren van risico's, zorgen voor compliance en optimaliseren processen om beveiliging en efficiëntie te waarborgen.
- **IT Administrator**
  - **Beschrijving:** Verantwoordelijk voor de operationele uitvoering van het identity management, zoals het aanmaken, beheren, en verwijderen van gebruikersaccounts en toegangsrechten.

- **Belangrijkste verantwoordelijkheden:** Het monitoren van activiteiten, lost technische problemen op, en voert beveiligingsmaatregelen uit om het identity managementproces soepel en veilig te laten verlopen.

- **AfdelingsManager**
  - **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.

- **SOC (Security Operations Center)**
  - **Beschrijving:** Verantwoordelijk voor het monitoren, detecteren en reageren op beveiligingsincidenten binnen de organisatie. Het team analyseert gegevens van verschillende bronnen om potentiële bedreigingen te identificeren en te mitigeren.
  - **Belangrijkste verantwoordelijkheden:** Reageert snel en adequaat op incidenten en zorgt voor continue bewaking van het identity managementsysteem.

- **Security Officer**
  - **Beschrijving:** Ontwikkelt en implementeert beveiligingsbeleid en procedures voor identity management om te voldoen aan beveiligingsstandaarden.
  - **Belangrijkste verantwoordelijkheden:** Zorgt voor de bescherming van gevoelige gegevens en ondersteunt het identity managementproces door veiligheidsmaatregelen te waarborgen..

- **Juridisch adviseur**
  - **Beschrijving:** Zorgt ervoor dat het identity managementsysteem voldoet aan wet- en regelgeving rond gegevensbescherming en privacy, zoals AVG/GDPR/BIO.
  - **Belangrijkste verantwoordelijkheden:** Adviseert over de juridische aspecten van identity management, zorgt ervoor dat het systeem voldoet aan privacywetten zoals de AVG en helpt bij het opstellen van contracten en beleidsdocumenten.

- **Compliance Officer**
  - **Beschrijving:** Toetst of identity 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.

- **Security Analist**
  - **Beschrijving:** Analyseert logs en activiteiten om risico’s of bedreigingen binnen het identity managementsysteem te detecteren en rapporteert hierover aan het SOC of management.
  - **Belangrijkste verantwoordelijkheden:** voert risicoanalyses uit en ondersteunt bij het oplossen van beveiligingsincidenten binnen het identity managementsysteem.

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

Identity Management - Procesmodel
Versie 1.3