TLP:GREEN

OR-3 IMPLEMENTATIEPLAN

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

1.3 Definities

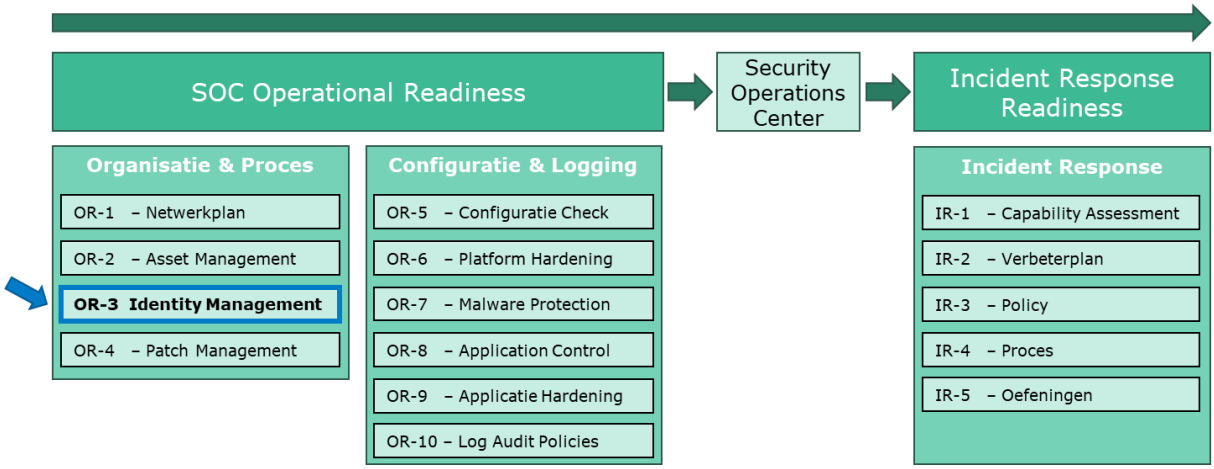
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **Implementatieplan** 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 Implementatie van identity management

In dit document wordt de implementatie van het "***identity managementproces" (IdM)*** beschreven. Hierbij zijn tien verschillende stappen beschreven voor een succesvolle implementatie van het identity management. Ook hierbij zijn er verschillende stappen die van groot belang zijn voor een Security Operations Center (SOC).

3.1 Inleiding

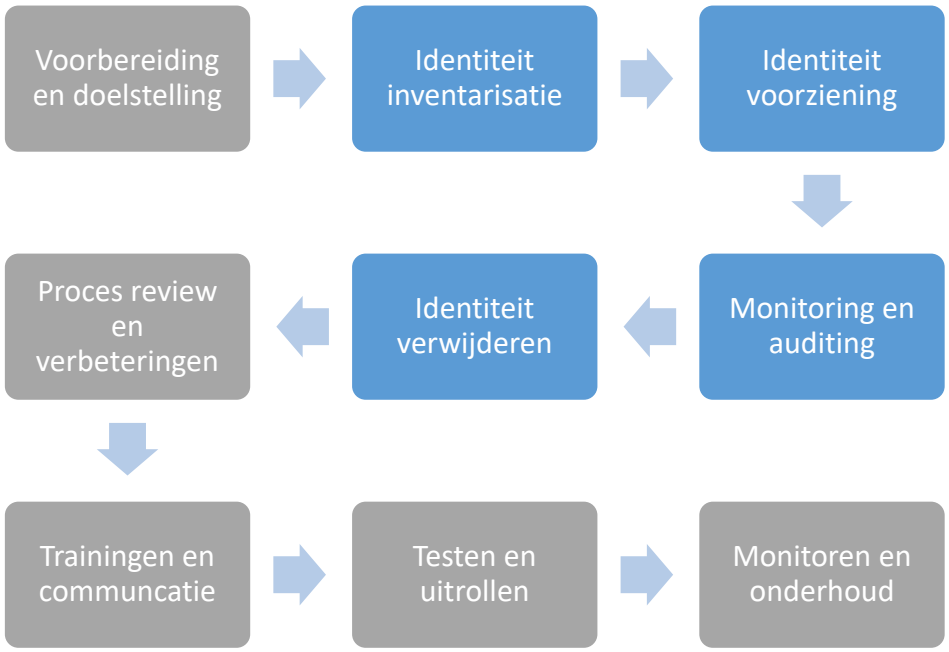
Het stappenplan is belangrijk omdat het zorgt voor een gestructureerde en efficiënte implementatie van het ***"identity managementproces"***. Het voorkomt overhaaste of incomplete implementaties door een duidelijke volgorde en aanpak te bieden, waardoor alle aspecten zoals beveiliging en compliance worden meegenomen. Het is ook van cruciaal belang voor een SOC omdat het een solide basis legt voor toegangsbeheer, dat essentieel is voor de beveiliging van systemen en gegevens.

3.2 Beschrijving en uitleg van de implementatie

Het stappenplan bestaat uit negen verschillende onderdelen waarbij vier onderdelen van essentieel belang zijn voor de implementatie van security monitoring door een SOC. Implementatie van identiteit creatie zorgt voor veilige en gestructureerde aanmaak van gebruikersaccounts, wat het bestaan van ongeautoriseerde accounts voorkomt. Configuratie van toewijzing en toegangsbeheer automatiseert het toekennen van de juiste toegangsrechten, minimaliseert fouten en biedt het SOC inzicht in wie toegang heeft tot welke systemen. Monitoring en auditing houdt zich bezig met 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. en compliance wordt ondersteund. Identity deprovisioning verwijdert snel toegangsrechten van vertrekkende medewerkers, wat risico's zoals ongeautoriseerde toegang minimaliseert en de beveiliging versterkt.

3.3 Identity management implementatie

Hieronder wordt in een flowchart de negen verschillende stappen voor de implementatie van identity management weergegeven. Hierna worden de individuele stappen beschreven, inclusief actiepunten en overwegingen. Hierbij zijn vier onderdelen blauw gekleurd aangezien ze van essentieel belang zijn voor de implementatie van security monitoring door een SOC.



Figuur 1

3.3.1 Stap 1: Voorbereiding en doelstelling

- **Actiepunten**:
  - Bepaal de scope en doelen op basis van de output die is geleverd in het "***identity management proces"***.
  - Documenteer het bereik, inclusief systemen, applicaties en gebruikersgroepen.

- **Overwegingen**: Zorg dat alle betrokken afdelingen, zoals IT, HR, en Compliance, zijn betrokken.

3.3.2 Stap 2: Identiteit inventarisatie

- **Actiepunten**:
  - Verzamel identiteitsgegevens uit beschikbare bronnen binnen de organisatie, inclusief systemen, applicaties en databases. Analyseer deze gegevens om actieve en inactieve accounts te identificeren en breng verschillen in kaart.
  - Het SOC speelt een cruciale rol door te zorgen voor het monitoren van toegangs- en identiteitsgerelateerde activiteiten om ongeautoriseerde toegang of verdachte activiteiten te detecteren.

- **Overwegingen**: Zorg voor het koppelen accounts (bijvoorbeeld management/HR) aan specifieke AD groepen en implementeer sterke wachtwoordbeveiliging bij de creatie.

3.3.3 Stap 3: Identiteit voorziening

- **Actiepunten**:
  - Automatiseer het toewijzen van toegangsrechten op basis van de rollen en functies van de gebruiker.
- **Overwegingen**: Zorg voor een duidelijke workflow voor goedkeuring van toegangsaanvragen.

3.3.4 Stap 4: Monitoring en auditing

- **Actiepunten**:
  - Zet tools in om activiteiten en toegangslogs in real-time te monitoren.
  - Hiervoor kan gekeken worden naar de ontwikkelde identity's die in kaart gebracht zijn bij het ***identity managementproces***.
  - Het SOC kan verdachte activiteiten zoals ongeautoriseerde toegangspogingen, afwijkende inlogpatronen of misbruik van toegangsrechten snel detecteren en reageren op potentiële beveiligingsrisico's. 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.

- **Overwegingen**: Zorg dat logs veilig worden opgeslagen en voldoen aan de regelgeving voor gegevensbeveiliging. Bekijk de BIO-9.2.5.

3.3.5 Stap 5: Identiteit verwijderen

- **Actiepunten**:
  - Automatiseer het proces voor het intrekken of verwijderen van toegang wanneer een gebruiker de organisatie verlaat of van functie verandert.
  - Zorg dat het deprovisioningproces volledig is geïntegreerd met HR- en andere relevante systemen.
  - Een HR-vertegenwoordiger zorgt dat gebruikers die de organisatie verlaten of van functie veranderen, onmiddellijk hun toegangsrechten verliezen of wijzigen. Het SOC is in staat om dit te monitoren. Dit vermindert het risico van ongeautoriseerde toegang tot systemen en gegevens na vertrek.

- **Overwegingen**: Zorg ervoor dat alle toegangsrechten worden ingetrokken, inclusief toegang tot externe systemen en applicaties en voer regelmatig controles uit om inactieve accounts te identificeren en te verwijderen.

3.3.6 Stap 6: Uitvoeren van proces review

- **Actiepunten**:
  - Voer regelmatig procesreviews uit om te beoordelen of het ***identity managementproces*** effectief is en voldoet aan de doelstellingen.
  - Verzamel feedback van gebruikers en IT-personeel om verbeterpunten te identificeren.

- **Overwegingen**: Begin met risicovolle systemen en rol MFA geleidelijk uit om de impact op gebruikers te minimaliseren.

3.3.7 Stap 7: Trainingen en communicatie

- **Actiepunten**:
  - Train medewerkers en gebruikers over de nieuwe procedures voor toegang, beveiliging en identity management.
  - Communiceer het belang van het nieuwe systeem en de beveiligingsmaatregelen aan alle betrokkenen.

- **Overwegingen**: Zorg dat gebruikers begrijpen waarom bepaalde procedures nodig zijn of het herzien van een ***identity managementproces***. Zorg voor voortdurende communicatie over updates of veranderingen in het systeem.

3.3.8 Stap 8: Testen en uitrollen

- **Actiepunten**:
  - Voer uitgebreide tests uit om te controleren of alle onderdelen van het systeem naar behoren werken.
  - Als er voor het eerst gebruik gemaakt wordt van een SOC, start met een pilot of gefaseerde uitrol om problemen in een gecontroleerde omgeving te identificeren voordat het systeem in de hele organisatie wordt uitgerold.

- **Overwegingen**: Betrek verschillende afdelingen bij de testfase om verschillende perspectieven te krijgen.

3.3.9 Stap 9: Monitoren en onderhoud

- **Actiepunten**:
  - Zet een monitoring- en onderhoudsstrategie op om het systeem continu te bewaken en te verbeteren
  - Dit kunnen bijvoorbeeld periodieke controles zijn om te kijken of het "***identity mangementproces"*** en het "***account overzicht"*** nog wel compleet zijn.

- **Overwegingen**: Zorg voor proactief beheer om beveiligingsincidenten te voorkomen en Blijf op de hoogte van veranderingen in de wet- en regelgeving en pas het systeem aan om compliant te blijven.

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