TLP:GREEN

OR-2 IMPLEMENTATIEPLAN

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	07-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Procesmodel	Zie "OR-2, Procesmodel" 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

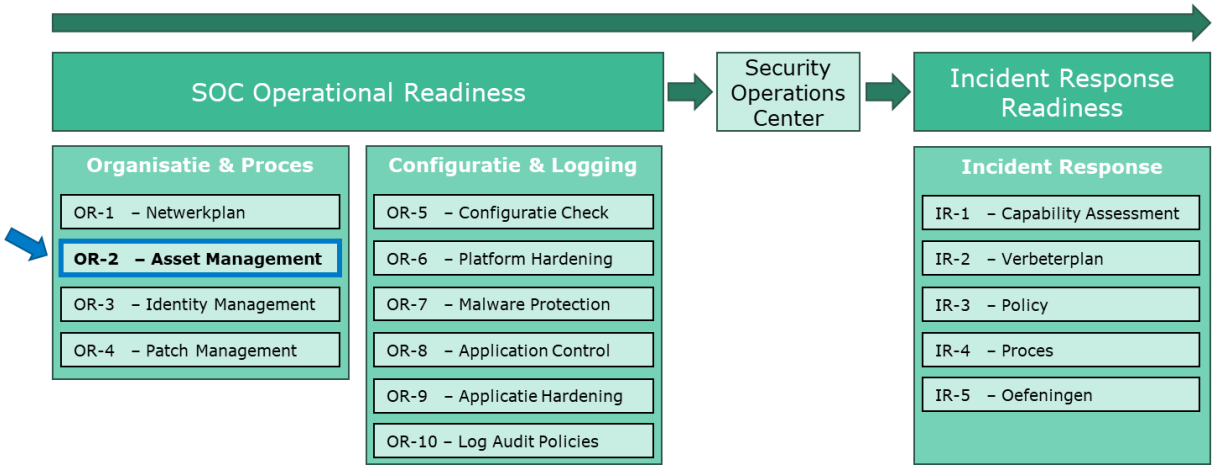
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **Implementatieplan** 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 Stappenplan voor Assetmanagement

Dit hoofdstuk bevat een implementatieplan voor effectief assetmanagement binnen de organisatie, een cruciale basis voor de SOC-dienstverlening.

3.1 Inleiding

Het Implementatie Stappenplan Assetmanagement biedt een gestructureerd kader om systematisch een assetmanagementproces in te zetten. Dit plan is ontworpen om het Assetmanagement-proces te implementeren en tegelijkertijd het "***Overzicht Kroonjuwelen***" excel-document volledig en correct in te vullen.

Kritieke assets zijn componenten die een essentiële rol vervullen in de bedrijfsprocessen van een organisatie. Dergelijke assets worden vaak aangeduid als 'kroonjuwelen'. Door middel van duidelijke, opeenvolgende stappen zorgt het plan ervoor dat elke fase van het assetmanagement - van de eerste inventarisatie en classificatie tot voortdurende monitoring en verwijdering - aansluit bij de prioriteiten en beveiligingsvereisten van de organisatie. Door de classificatie naar de BIV-classificering (Beschikbaarheid, Integriteit en vertrouwelijkheid) op te nemen, maakt het stappenplan een op risico's gebaseerde aanpak mogelijk. De BIV-classificering maakt onderdeel uit van Baseline Informatiebeveiliging Overheid (BIO).

Een belangrijk element binnen dit stappenplan is de koppeling tussen het ***"Assetmanagement beschrijving"*** Word-document en het bijbehorende ***"Overzicht Kroonjuwelen"*** Excel-document voor kroonjuwelenbeheer. Het procesdocument biedt de theoretische basis, richtlijnen en een beschrijving van de fasen binnen het assetmanagementproces. Het ***"Overzicht Kroonjuwelen"*** Excel-document fungeert daarbij als een operationeel hulpmiddel dat een praktische toepassing van deze richtlijnen mogelijk maakt. In het ***"Overzicht Kroonjuwelen"*** Excel-document worden alle kritieke assets, inclusief kroonjuwelen, systematisch geregistreerd, geclassificeerd en geprioriteerd. Hierbij wordt gebruik gemaakt van de risicobenadering volgens de BIV-classificering, waardoor het document direct aansluit op de doelstellingen uit het procesdocument.

Het ***"Overzicht Kroonjuwelen"*** Excel-document ondersteunt organisaties bij het vastleggen van details, zoals eigenaarschap, beveiligingsmaatregelen en risicobeoordelingen, en kan het dienen als input voor monitoringtools en rapportagesystemen. Door deze koppeling tussen het procesdocument en het ***"Overzicht Kroonjuwelen"*** Excel-document wordt een naadloze integratie gerealiseerd tussen beleidsvorming en uitvoering. Dit maakt het mogelijk om niet alleen kritieke assets te identificeren en te beheren, maar ook om data te gebruiken als input voor verbetercycli en om snel in te spelen op nieuwe bedreigingen en veranderingen in wet- en regelgeving.

Elke stap in het plan omvat goed gedefinieerde doelstellingen, rollen en verantwoordelijkheden, waardoor de verantwoording en een gestroomlijnde uitvoering in het hele team mogelijk wordt gemaakt. De gefaseerde aanpak stelt de organisatie in staat om het proces aan te passen en op te schalen naarmate het groeit, met continue optimalisatie om opkomende risico's en veranderende wettelijke vereisten aan te pakken. Door dit implementatieplan te volgen, kunnen organisaties kritieke assets effectiever beschermen, de toewijzing van middelen verbeteren en een weerbaar assetmanagementsysteem bouwen dat de operationele en strategische doelen op de lange termijn ondersteunt.

3.2 Implementatie stappenplan

Het stappenplan bestaat uit vijf hoofdfasen, van assetidentificatie tot veilige verwijdering, die logisch op elkaar aansluiten om een volledige lifecycle-benadering te waarborgen.

Structuur van dit hoofdstuk:

Stap 1: Asset Identificatie

Het vaststellen en registreren van alle organisatorische assets als basis voor verdere processen.

Stap 2: Asset Classificatie

Het beoordelen van de waarde en het belang van assets op basis van hun BIV-classificatie.

Stap 3: Asset Acquisitie & Registratie

Het documenteren en integreren van nieuwe assets in de SOC-monitoringsystemen.

Stap 4: Asset Beheer & Monitoring

Het waarborgen van continu beheer, beveiliging en monitoring van alle assets.

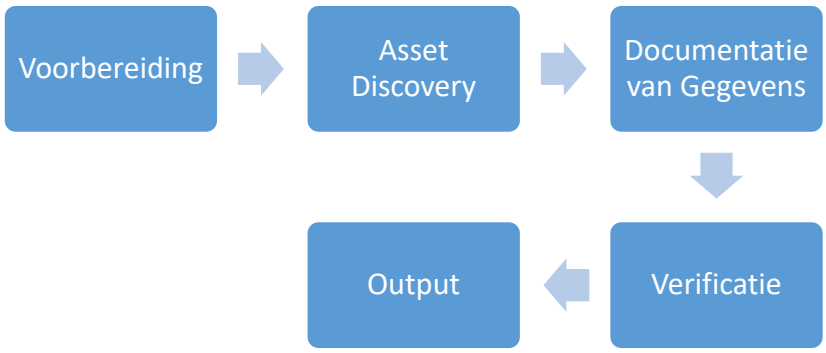
Stap 5: Asset Verwijdering

Het veilig en verantwoord afvoeren van assets aan het einde van hun levenscyclus.
Elke stap is onderverdeeld in implementatiestappen, met duidelijke doelen, activiteiten, en resultaten. Daarnaast bieden visuele weergaven ondersteuning om de processen beter te begrijpen.

Stap 1: Asset Identificatie Implementatieplan

Doel: Het identificeren en vastleggen van alle organisatorische assets om onder meer een solide basis te leggen voor SOC-operaties.

Implementatiestappen:



Figuur 1 Visuele weergave van de Asset Identificatie stappen

Voorbereiding:

- **Scope bepalen:** Maak een overzicht van alle relevante assettypen (hardware, software, netwerkcomponenten, enz.).
- **Betrokkenen identificeren:** Wijs rollen toe, zoals IT-managers en asset-eigenaren, die ondersteuning bieden bij het identificatieproces.
- **Invoer verzamelen:** Hergebruik de resultaten van de BIO-assessment om bestaande BIV-classificaties (Beschikbaarheid, Integriteit, Vertrouwelijkheid) toe te passen op assets.

Asset Discovery:

- **Scans uitvoeren:** Gebruik networkscanning tools om fysieke en virtuele assets in kaart te brengen.
- **Interviews afnemen:** Interview IT-medewerkers en afdelingshoofden om ervoor te zorgen dat er geen assets worden gemist.

Documentatie van Gegevens:

- **Invullen meegeleverde *"Overzicht Kroonjuwelen"* Excel-document:**
  Vul de Excel-sheet in met velden zoals assettype, eigenaar, locatie, enz.

Verificatie:

- **Controle op nauwkeurigheid:** Stem de inventarislijst af met betrokkenen om eventuele fouten te corrigeren.
- **Finaliseren:** Zorg ervoor dat de lijst compleet, geverifieerd en klaar is voor gebruik.

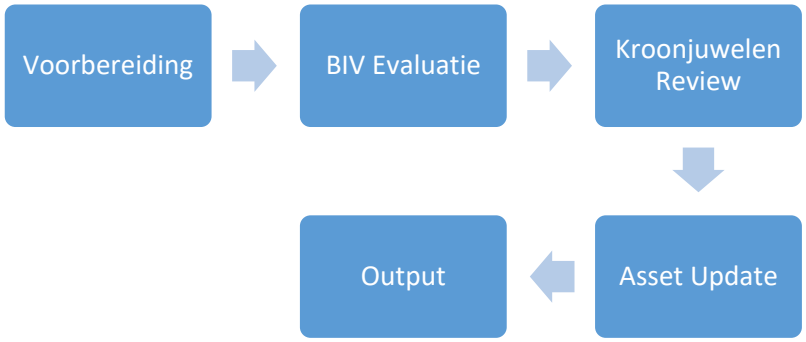
Output:

- Een geverifieerde en complete lijst van alle organisatorische assets, gereed voor de volgende fase: classificatie.
- Een volledig overzicht van de geïdentificeerde assets.

Stap 2: Asset Classificatie Implementatieplan

Doel: Creëer een helder overzicht van het belang van assets op basis van hun BIV-waarde, zodat beveiligingsmaatregelen strategisch kunnen worden ingezet.

Implementatiestappen:



Figuur 2 Visuele weergave van de Asset Classificatie stappen

Voorbereiding:

- Hanteer BIV-classificatiestandaarden (Hoog, Middel en Laag) overeenkomstig met de BIO-standaard (Baseline Informatiebeveiliging Overheid) om een solide basis te leggen.
- **Verzamel gegevens:** Breng alle geïdentificeerde assets en relevante risicobeoordelingsinformatie samen. Denk hierbij aan waardevolle input van asset-eigenaren die de dagelijkse bedrijfsprocessen goed kennen.
- Inventariseer bedrijf kritische processen.

BIV-Evaluatie:

- **Classificeer assets:** Gebruik de BIV-criteria (vertrouwelijkheid, integriteit, beschikbaarheid) om elk item te beoordelen en in te delen. Gebruik daarvoor als uitgangspunt uitkomsten van BIO-assessments.
- **Betrek de organisatie:** Werk samen met afdelingshoofden om het belang van assets te begrijpen en eventuele nuances mee te nemen in de classificatie.

Kroonjuwelen Review:

- **Identificeer kritische assets:** Gebruik de BIV-classificatie om de "kroonjuwelen" te bepalen—de cruciale assets die essentieel zijn voor de continuïteit van de organisatie.
- **Documenteer zorgvuldig:** Leg deze assets vast in het Excel-***"Overzicht Kroonjuwelen"***, inclusief alle relevante velden uit de meegeleverde template. Dit overzicht biedt het SOC een compleet beeld van de kroonjuwelen en ondersteunt effectieve beveiligingsmonitoring met verhoogde prioriteit voor de Kroonjuwelen van de organisatie.

Asset Update:

- **Actualiseer de Kroonjuwelen inventaris:** Voeg de BIV-classificatie toe aan het assetbeheersysteem om te zorgen voor een up-to-date overzicht.
- **Controleer de nauwkeurigheid:** Zorg ervoor dat alle kroonjuwelen correct en consistent zijn geclassificeerd.

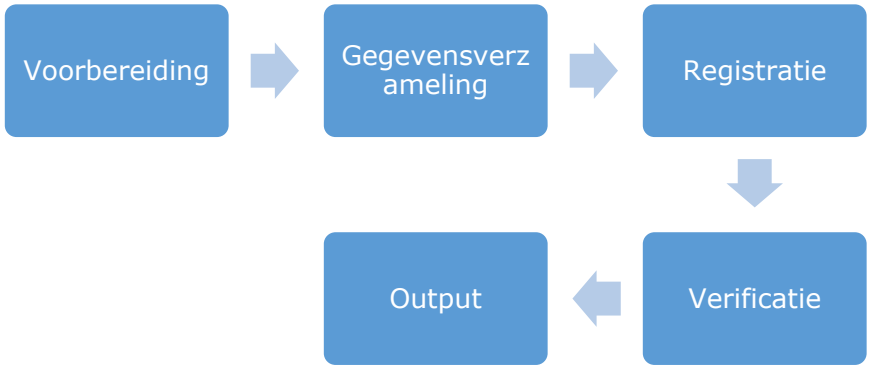
Output:

- Een geclassificeerde assetinventaris die de kroonjuwelen van de organisatie duidelijk identificeert. Dit overzicht vormt de basis voor gerichte SOC-operaties.
- Door deze aanpak te volgen, krijgt uw organisatie een sterkere grip op haar waardevolle assets en wordt beveiliging naar een hoger niveau getild.

Stap 3: Asset Acquisitie & Registratie Implementatieplan

Doel: Zorg voor een naadloze documentatie en onboarding van assets, zodat deze effectief worden geïntegreerd in de SOC-monitoringsystemen.

Implementatiestappen:



Figuur 3 Visuele weergave van de Asset Acquisitie & Registratie stappen

Voorbereiding:

- Selecteer en integreer een asset managementsysteem of andere manier van registratie: Stel de database, asset management of bestand in voor het centraal registreren van alle assets.

Gegevensverzameling:

- Verzamel cruciale assetinformatie: Zorg ervoor dat essentiële gegevens zoals OS-type, versie, hostnaam en IP-adres nauwkeurig worden vastgelegd.
- Bepaal de verantwoordelijkheden: Wijs een eigenaar toe aan elke nieuwe asset om verantwoordelijkheden te verduidelijken.

Registratie:

- Voeg assets toe aan het centrale systeem: Documenteer de asset in de database, inclusief de classificatie en andere relevante details.
- Informeer de SOC: Zorg ervoor dat nieuwe assets worden gedeeld met de SOC-teams, zodat ze correct worden geïntegreerd in de beveiligingsmonitoringsystemen.

Verificatie:

- Controleer op volledigheid en accuraatheid: Verifieer of de asset correct is geregistreerd en zichtbaar is in de SOC-monitoringtools.

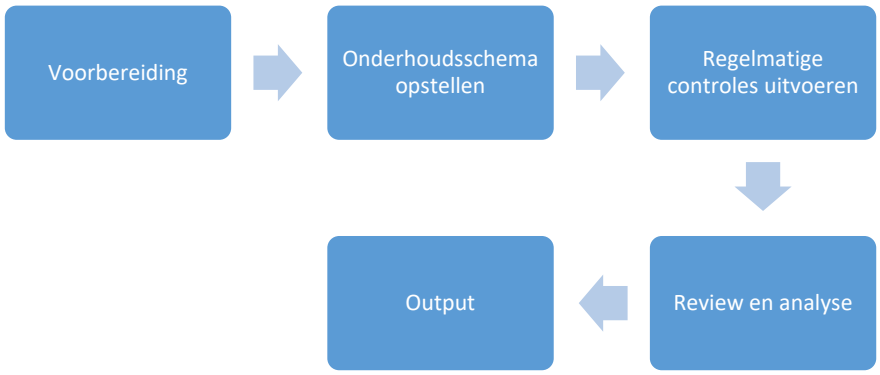
Output:

- Een bijgewerkte en betrouwbare assetinventaris waarin nieuwe toevoegingen volledig zijn gedocumenteerd en geïntegreerd in de SOC-monitoringsystemen.

Stap 4: Asset Beheer & Monitoring Implementatieplan

Doel: Zorg ervoor dat alle assets binnen de organisatie goed worden beheerd en beveiligd door middel van continue monitoring en onderhoud.

Implementatiestappen:



Figuur 4 Visuele weergave van de Asset Beheer & Monitoring stappen

Voorbereiding:

- **Bepalen van een Monitoringstrategie:** Ontwikkel een monitoringstrategie op maat, gebaseerd op de assetclassificatie met behulp van de BIV-classificaties (Beschikbaarheid, Integriteit, Vertrouwelijkheid).

Onderhoudsschema opstellen:

- **Creëren van een Onderhoudskalender:** Plan periodieke controles en updates voor elke asset, zodat deze altijd optimaal blijft functioneren.
- Toewijzen van Asseteigenaars: Zorg ervoor dat elke asset een specifieke eigenaar heeft die verantwoordelijk is voor onderhoud en updates.

Regelmatige controles uitvoeren:

- Bijwerken van Assetgegevens: Controleer regelmatig assetgegevens, zoals softwareversies en patchstatus, en werk deze waar nodig bij.
- Continu monitoren van de status van Assets: Gebruik monitoringtools om de prestaties en beveiligingsstatus van assets in real-time te volgen.
- **Beveiligingsbewaking:** Zorg ervoor dat de assets bewaakt worden vanuit beveiligingsoogpunt.

Review en analyse:

- Uitvoeren van periodieke Reviews: analyseer regelmatig de monitoringresultaten en assetregistratie om eventuele discrepanties of verbeterpunten te identificeren.

- Genereren van Rapporten: Maak heldere en inzichtelijke rapporten over de prestaties en beveiligingsstatus van assets. Deze rapporten ondersteunen bij naleving van regelgeving en het verminderen van risico's.

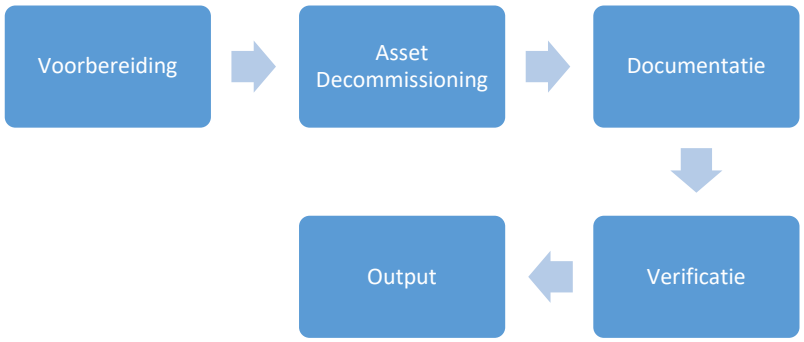
Output:

- Een effectieve en continu verbeterende aanpak voor assetbeheer:
  - Logboeken van onderhouds- en monitoringactiviteiten.
  - Uitgebreide rapporten die inzicht bieden in de status en prestaties van alle assets.

Stap 5: Asset Verwijdering Implementatieplan

Doel: Zorg voor een veilige en verantwoorde verwijdering van assets aan het einde van hun levenscyclus. Minimaliseer risico's, bescherm gevoelige gegevens, en waarborg naleving van regelgeving.

Implementatiestappen:



Figuur 5 Visuele weergave van de Asset Verwijdering stappen

Voorbereiding:

- **Ontwikkel een asset verwijderingsbeleid:** Stel een formeel beleid op dat gedetailleerde richtlijnen bevat voor veilige gegevensvernietiging en milieuvriendelijke fysieke verwijdering van assets.
- Toewijzing van Verantwoordelijkheden: Bepaal specifieke teams voor gegevensvernietiging, hardware afvoer en de coördinatie van het gehele decommissioningproces.

Asset Decommissioning:

- Gegevensveiligheid: Wis alle data op assets grondig en veilig met om ongeautoriseerde toegang te voorkomen.
- Milieuvriendelijke Verwijdering: Zorg ervoor dat fysieke assets worden verwijderd of gerecycled volgens geldende milieuregels en bedrijfsvoorschriften.
- Bijwerken van SOC Monitoring: Haal de gedecommissioneerde asset uit alle SOC-monitoringsystemen om onnodige meldingen te voorkomen.

Documentatie:

- Gedetailleerd Procesoverzicht: Houd volledige documentatie bij van het verwijderingsproces en verwijderingsverslagen.
- Auditlogs: Sla audit trails zorgvuldig op.

Verificatie:

- Controle van Verwijdering: Bevestig dat de asset volledig is verwijderd uit het asset beheersysteem en de SOC-monitoringsystemen.

Output:

- Leverbaar: Een compleet rapport van de verwijderde assets die deze verwijderingen weergeeft.

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: Implementatieplan
Versie 1.3