TLP:GREEN

OR-10 IMPLEMENTATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Log audit policies**

Best Practice versie 1.1

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 Windows IT-beheerders, Systeemeigenaren, IT-Assetmanagers, Uitbestedingsmanagers, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	21-03-2025	Initiële versie
V1.1	08-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Log audit policies – Configuratiehandleiding (OR-10)	Zie "Log audit policies – Configuratiehandleiding (OR-10)" onder SOC Operational Readiness (Configuratie & Logging)
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

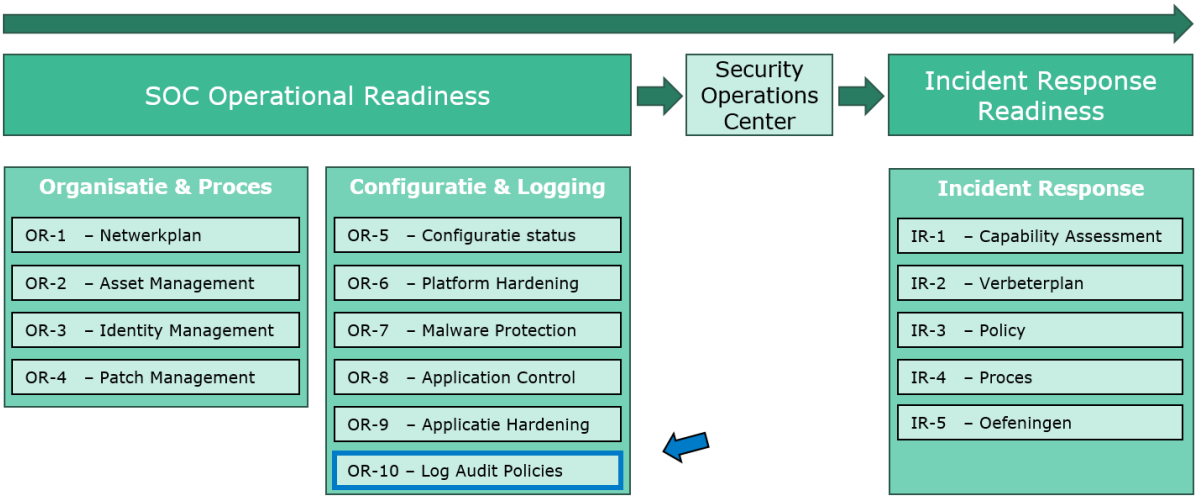
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **Configuratie & Logging** 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 figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document de implementatiehandleiding is voor Log audit policies (OR-10), binnen **Configuratie & Logging**, behandelt.

3 Inleiding

Audit logging policies bepalen welke systeemgebeurtenissen worden vastgelegd in de auditlogs en vormen een cruciaal onderdeel van beveiliging en compliance. Deze policies specificeren:

- Welke typen gebeurtenissen worden geregistreerd
- Het detailniveau van de logging
- De systemen en componenten waarop de logging van toepassing is

Een goed ingerichte audit policy kan onder andere het registreren van gebruikersaanmeldingen, toegang tot gevoelige bestanden, wijzigingen in systeemconfiguraties en beveiligingsgerelateerde gebeurtenissen omvatten. De vastgelegde informatie is van groot belang voor beveiligingsaudits, incidentonderzoek en naleving van regelgeving.

Een zorgvuldige implementatie van audit policies is noodzakelijk om inzicht te krijgen in gebruikers- en systeemactiviteiten, zonder onnodige belasting op systemen te veroorzaken. Een te hoog logvolume kan leiden tot prestatieproblemen en operationele verstoringen. Dit zijn de gevolgen van een te hoog logvolume. Anderzijds bestaat het risico van onvoldoende logging, waardoor potentiële incidenten niet of niet tijdig worden opgemerkt. Daarom is een evenwichtige aanpak vereist, waarbij logging effectief wordt ingezet zonder de continuïteit van de IT-omgeving in gevaar te brengen.

Dit stappenplan biedt een gecontroleerde methode om audit policies effectief uit te rollen binnen een organisatie. Door te starten met een kleine testgroep en het gefaseerd uitbreiden naar de volledige omgeving, wordt de impact geminimaliseerd.

3.1 Uitgangspunt en resultaat

Het uitgangspunt van dit stappenplan is om audit policies gecontroleerd en zonder verstoring van de productieomgeving te implementeren. Door een gefaseerde aanpak wordt de configuratie eerst getest binnen een beperkte groep systemen, zodat mogelijke impact inzichtelijk wordt.

Het resultaat is een gestandaardiseerde auditconfiguratie die voldoet aan compliance-eisen zoals de BIO. Deze configuratie is direct geschikt voor SOC-onboarding en biedt een solide basis voor een SOC (Security Operating Center) om hier vervolgens detectiemaatregelen op te bouwen en te implementeren.

3.2 Doel en Reikwijdte

Deze handleiding richt zich op het proces van gecontroleerde uitrol van audit policies binnen de organisatie. Dit omvat het opstellen van testscenario's, het uitvoeren van een gefaseerde uitrol en het waarborgen van de continuïteit en verbetering van het proces.

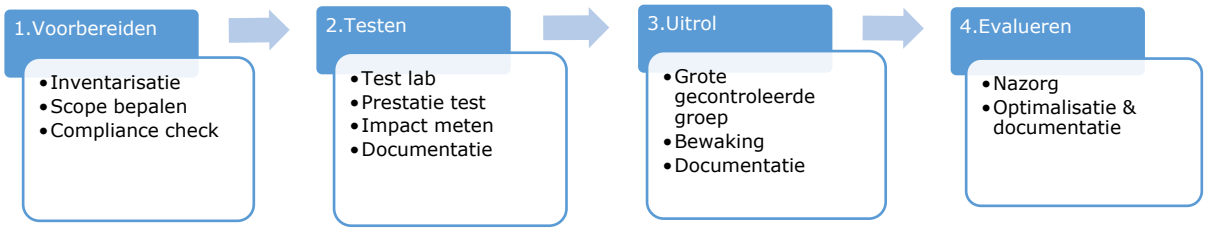
Dit document is geen technische configuratiehandleiding. Het richt zich op de praktische toepassing van de configuraties, met als doel ervoor te zorgen dat de audit policies correct worden geïmplementeerd en dat de continuïteit van de werking gewaarborgd blijft. De configuratiehandleiding is in een ander document opgenomen, zie paragraaf 1.2 voor de referentie.

3.3 Uitgangspunt en Resultaat

Het uitgangspunt is dat er een testomgeving beschikbaar is die de productieomgeving nauwkeurig nabootst waarop de audit policies eerst worden toegepast, voordat ze op grotere schaal in de productieomgeving worden uitgerold. Dit maakt het mogelijk om in elke fase te testen hoe de systemen reageren op de wijzigingen. Het uiteindelijke doel is ervoor te zorgen dat de systemen binnen de scope de juiste logs genereren, zodat een SOC in staat is om beveiligingsincidenten effectief te detecteren en aan te pakken.

4 Stappenplan voor implementeren Audit Policies

Het implementeren van audit policies via Windows Audit Policies en Linux Auditd is een efficiënte manier om een gestructureerde aanpak te volgen. Via Group Policies kunnen middels policies gecontroleerde wijzigingen worden uitgerold voor specifieke systemen. Daarnaast helpen de best practices die in dit hoofdstuk worden besproken organisaties om de uitrol op een gecontroleerde en systematische manier te realiseren, met nadruk op het monitoren van de impact tijdens het testen, het verzamelen van feedback en het documenteren van het proces.



Figuur 2 Stappenplan fasering

De flowchart (figuur 1) biedt een visueel overzicht van het stappenplan voor de implementatie van log audit policies. Het proces bestaat uit:

1. **Voorbereiden**, waarbij een inventarisatie van de huidige situatie wordt uitgevoerd en communicatie met de belanghebbenden plaatsvindt. Dit helpt om de scope van de uitrol te bepalen en verwachtingen te managen.
2. **Testen**, waarbij een testomgeving wordt opgezet om de impact van de instellingen te meten en te documenteren. Documentatie in deze fase is essentieel voor het traceren van de uitgevoerde wijzigingen, zodat deze in de toekomst eenvoudig kunnen worden bijgewerkt of aangepast. Dit stelt de beheerder in staat om mogelijke problemen vroegtijdig te identificeren zonder de productieomgeving te beïnvloeden.
3. **Uitrol**, Tijdens deze fase wordt de uitrol gestart met een beperkte, zorgvuldig geselecteerde groep van ongeveer 25 systemen. Deze systemen worden gekozen om de impact van de wijzigingen te monitoren en te documenteren, terwijl verstoring op de overige systemen tot een minimum wordt beperkt.
4. **Evalueren**, In de laatste fase worden de systeemprestaties van de systemen geëvalueerd. Het is essentieel om na te gaan of de nieuwe instellingen geen verstoringen veroorzaken in de werking van de systemen en daadwerkelijk bijdragen aan een verbeterde beveiliging. Daarnaast zorgt uitgebreide documentatie ervoor dat de aangebrachte wijzigingen goed traceerbaar zijn, wat toekomstige aanpassingen van de policies aanzienlijk vereenvoudigt.

De volgende paragrafen/secties behandelen de verschillende stappen zoals beschreven in Figuur 2 Stappenplan fasering.

4.1 Voorbereiden

De voorbereiding is een belangrijke fase in het implementatieproces, waarin de noodzakelijke stappen worden genomen om wijzigingen op een gecontroleerde manier door te voeren. Dit helpt om ervoor te zorgen dat de implementatie soepel verloopt en dat er geen onverwachte problemen ontstaan.

4.1.1 Inventarisatie

Voordat de audit policy wordt toegepast, is het belangrijk om een inventarisatie te maken van de benodigde vereisten voor de veranderingen. Dit omvat het identificeren van de systemen en of er overlapping is tussen het geadviseerde audit policy uit de configuratiehandleiding en GPO's die al actief zijn.

Taak	Actie
Identificeer systemen	Maak een lijst van systemen die de wijzigingen moeten ontvangen.
Analyseer de configuratiehandleiding	Controleer welke audit policies vanuit de handleiding geen directe waarde toevoegen aan de huidige infrastructuur. Richt speciale aandacht op de policies die als "IF" (voorwaardelijk) zijn gemarkeerd. Beoordeel of de omstandigheden waarin deze policies van toepassing zijn, overeenkomen met de huidige configuratie en beveiligingsdoelstellingen. Noteer irrelevante policies en motiveer waarom ze niet nodig zijn, bijvoorbeeld vanwege onverenigbaarheid of gebrek aan impact.
Identificeer overlapping	Controleer de huidige Group Policy Objects (GPO's) op instellingen die mogelijk overlappen met de voorgestelde audit policies. Werk aan een gestroomlijnde configuratie door overlappende settings samen te voegen of te elimineren, zodat er geen overbodige belasting ontstaat voor systemen of logbeheer.

4.1.2 Scope bepalen

Het bepalen van de scope betekent vaststellen welke systemen door de wijzigingen worden beïnvloed. Het is essentieel om duidelijk te definiëren op welke systemen de configuratiewijzigingen worden toegepast, bijvoorbeeld systemen van specifieke afdelingen, rollen of applicaties. Daarnaast moet worden vastgesteld welke systemen buiten de wijziging blijven om onbedoelde effecten te voorkomen en helpt bij het plannen van communicatie naar de betrokkenen.

Taak	Actie
Definieer doelgroepen	Bepaal welke systemen de wijziging moet ontvangen.
Communicatieplan opstellen (indien nodig)	Plan hoe de wijziging aan de betrokkenen wordt gecommuniceerd.
Evalueren van onbedoelde impact	Controleer of er systemen zijn die per ongeluk kunnen worden beïnvloed door de wijziging.

4.1.3 Compliance Check

Bij het doorvoeren van configuratiewijzigingen moet rekening worden gehouden met de geldende interne beveiligingsrichtlijnen van de organisatie. De compliance check helpt ervoor te zorgen dat de wijzigingen voldoen aan geldende richtlijnen of intern beleid.

Taak	Actie
Controleer richtlijnen en intern beleid	Beoordeel de relevante (interne) richtlijnen die van invloed kan zijn op de wijzigingen.

4.2 Testen

De testfase is een belangrijke stap om te controleren of de wijzigingen zoals beoogd functioneren, zonder negatieve gevolgen voor de systemen of gebruikers. Door deze fase zorgvuldig uit te voeren, kunnen beheerders er zeker van zijn dat de wijzigingen veilig en effectief kunnen worden uitgerold.

4.2.1 Test-lab

Het opzetten van een testomgeving is nodig om een gecontroleerde omgeving te hebben waarin de configuratiewijzigingen getest kunnen worden. De testomgeving moet zo dicht mogelijk bij de productieomgeving liggen om representatieve resultaten te verkrijgen. Binnen de testomgeving kunnen configuraties worden uitgeprobeerd om vast te stellen hoe de wijzigingen zich gedragen voordat ze daadwerkelijk worden geïmplementeerd.

Taak	Actie
Testomgeving opzetten	Stel een testomgeving in die lijkt op de productieomgeving.
Configuratie testen	Pas de geconfigureerde GPO’s toe zoals ze later in de productieomgeving zullen worden gebruikt.

4.2.2 Prestatietest

Door prestaties te meten en te vergelijken met een vooraf vastgestelde verwachting, kunnen beheerders bepalen of de wijzigingen positief, neutraal of negatief effect hebben op de systeemprestaties.

Taak	Actie
Bepaal de baseline voor de systeemprestaties	Bepaald wat de prestatiestandaarden zijn die nu voor de systemen geïmplementeerd zijn.
Test systeemprestaties	Voer prestatietests uit om de prestaties van systemen na de wijziging te controleren.
Vergelijk met baseline	Vergelijk de prestatiegegevens met de gegevens vóór de wijziging.

4.2.3 Impact meten

Het meten van de impact van de wijzigingen is nodig om te begrijpen hoe deze veranderingen de systemen en gebruikers beïnvloeden. Dit omvat zowel technische prestaties als gebruikservaringen, en helpt om een compleet beeld te krijgen van de gevolgen van de configuratiewijzigingen.

Taak	Actie
Identificeer de impact	Meet de invloed van de wijziging
Controleer op ongewenste effecten	Kijk of de wijziging onverwachte gevolgen heeft voor andere systemen of processen.

4.2.4 Documenteren

Documentatie speelt een belangrijke rol in het vastleggen van de resultaten en bevindingen van de testfase. Een gedetailleerd verslag van de testresultaten, bevindingen en eventuele problemen helpt bij toekomstige implementaties en zorgt voor transparantie naar alle betrokkenen.

Taak	Actie
Documenteer testresultaten	Leg de resultaten van de tests vast in een verslag waar de verwachte en werkelijke resultaten
Beschrijf bevindingen	Noteer gevonden problemen en bijzonderheden die tijdens de tests en de analyse zijn ontdekt.

4.3 Uitrol

Uitrol betreft de definitieve uitrol van de configuratiewijzigingen naar alle systemen die binnen de eerder gedefinieerde scope vallen. Deze fase bouwt voort op de ervaringen en resultaten van de testfase en is bedoeld om de wijzigingen in productie te brengen.

4.3.1 Uitrol volgens scope

Tijdens deze fase worden de configuratiewijzigingen uitgerold naar alle systemen die binnen de scope van de wijzigingen vallen.

Taak	Actie
Communiceren met betrokkenen	Informeer indien betrokkenen over de aanstaande wijziging.
Uitrol plannen	Bepaal een gedetailleerde planning voor de uitrol per systeemgroep.
Uitrollen change	Implementeer de configuratiewijzigingen zoals gepland.
Ondersteuning	Zorg voor ondersteuning tijdens de uitrol. Denk hierbij aan ondersteuning voor bijvoorbeeld systeembeheerders, applicatiebeheerders of andere medewerkers die hinder ondervinden.

4.3.2 Bewaking & Documentatie

Nadat de configuratiewijzigingen zijn uitgerold, is het belangrijk om een fase van bewaking en documentatie te volgen. De documentatie omvat alle relevante informatie voor toekomstige referentie en eventuele audits.

Taak	Actie
Gebruikersfeedback verzamelen	Verzamel feedback van personen die afhankelijk zijn van deze systemen, bijvoorbeeld applicatiebeheerders.
Bewaken consequenties	Bewaak de consequenties op de capaciteit van de logcollectors en de systeemprestaties als gevolg van de implementatie. Deze mogen niet veel afwijken van de testresultaten.
Resultaten documenteren	Documenteer alle bevindingen en leerpunten voor toekomstige referentie.

4.4 Evalueren

De evaluatiefase heeft tot doel te bepalen of de configuratiewijzigingen succesvol zijn geïmplementeerd. In deze fase wordt ook nazorg geleverd, en de evaluatie dient om lessen te trekken voor toekomstige wijzigingen. Indien de configuratieaanpassing niet succesvol is, moet er een nieuwe evaluatie van de risico's plaatsvinden. Evaluatie is niet alleen relevant voor toekomstige projecten, maar ook om vast te stellen welke van de beoogde configuratie-instellingen niet geïmplementeerd konden worden. Deze onvoltooide wijzigingen kunnen resulteren in blijvende cyberbeveiligingsrisico's, die in de evaluatie opnieuw moeten worden beoordeeld. Hierbij dient gekeken te worden of deze instellingen in de toekomst alsnog geïmplementeerd kunnen worden en of er compenserende maatregelen mogelijk zijn, bijvoorbeeld door deze extra met use cases door het SOC te laten monitoren.'

4.4.1 Nazorg

Nazorg is gericht op het ondersteunen van systeemeigenaren en het oplossen van eventuele problemen na de uitrol.

Taak	Actie
Gebruikersondersteuning	Bied extra ondersteuning aan systeemeigenaren bij problemen en vragen.
Kennisoverdracht	Zorg ervoor dat de helpdesk en supportteams goed geïnformeerd zijn over de wijzigingen en mogelijke problemen.

4.4.2 Optimalisatie & documentatie

Optimalisatie richt zich op het verbeteren van de configuraties op basis van de feedback en de verzamelde gegevens om de efficiëntie en effectiviteit te maximaliseren.

Taak	Actie
Implementeren van verbeteringen	Pas de configuraties indien mogelijk aan op basis van de analyse om problemen te op te lossen.
Evalueren van impact	Beoordeel de impact van de aangebrachte verbeteringen om ervoor te zorgen dat ze blijvend de gewenste resultaten opleveren.
Documenteer aanwezige risico's	Audit policies die niet geïmplementeerd konden en kunnen worden kunnen een risico veroorzaken op het systeem. Controleer met een deskundige of er nog compenserende maatregelen zijn om dit risico te mitigeren.
Bijwerken documentatie	Werk de documentatie bij met de aangebrachte wijzigingen en/of verbeteringen.

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)

Maart 2025