TLP:GREEN

OR-6 CONFIGURATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Basis platform hardening**

Best Practice versie 1.2

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

1. 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.

2. Documentgegevens

2.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	19-03-2025	Initiële versie
V1.1	31-10-2025	Toevoeging “Bijlage I – Configuratiestatus checklist”
V1.2	07-07-2026	Referenties geactualiseerd

2.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Generiek implementatieplan voor OR-6 t/m OR-9	Zie "Generiek implementatieplan” onder Platform/Applicatie Hardening & Malware bescherming (OR-6 t/m OR-9). Onderdeel van SOC Operational Readiness (Configuratie & Logging)
CIS Benchmark	https://www.cisecurity.org/cis-benchmarks
Microsoft Security baseline	https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
VSSR-kennisdocumenten	VSSR (ncsc.nl)

2.3 Definities

Term	Omschrijving
Entra ID	Microsoft cloudgebaseerde identiteits- en toegangsbeheeroplossing
Obfuscated scripts	Scripts waarvan de code opzettelijk moeilijk leesbaar is gemaakt vaak om detectie te voorkomen

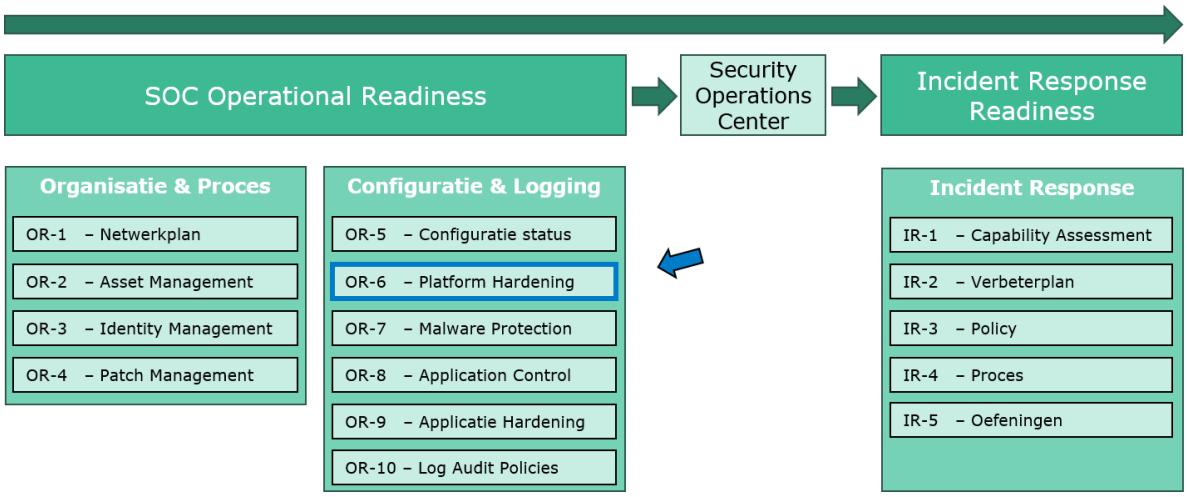
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

3. 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 configuratiehandleiding is voor Platform Hardening (OR-6), binnen **Configuratie & Logging**, behandelt.

4. Inleiding

In dit hoofdstuk wordt stilgestaan bij het doel van dit document, namelijk basis platform hardening. Daarnaast worden de randvoorwaarden besproken die nodig zijn om deze configuratiehandleiding te kunnen gebruiken en de geraadpleegde raamwerken.

4.1 Doel

Deze handleiding richt zich op de basismaatregelen die organisaties kunnen nemen om een Windows Enterprise-omgeving beter te beveiligen. De configuraties in deze handleiding zijn bedoeld om de meest basale zwakke plekken aan te pakken, maar bieden geen volledige bescherming. Voor een uitgebreide beveiliging zijn aanvullende maatregelen nodig, afgestemd op de specifieke risico's en behoeften van de organisatie. Met deze handleiding kunnen organisaties een begin maken met het opzetten van een IT-omgeving die beter voorbereid is op veelvoorkomende dreigingen. Deze handleiding beschrijft de aanbevolen configuratiewijzigingen, maar deze omvatten niet direct de uitrol. De deployment dient als een aparte stap te worden uitgevoerd. Voor een uitgebreide toelichting op het uitrolproces wordt verwezen naar de implementatiehandleiding. De configuratiehandleiding en de implementatiehandleiding dienen in combinatie te worden gebruikt. De configuratiehandleiding beschrijft de vereiste instellingen, terwijl de implementatiehandleiding de procedures voor een gecontroleerde uitrol van deze instellingen uitlegt.

4.2 Wat is platform hardening?

Platform hardening vormt een essentiële stap in het beveiligen van IT-systemen. In de huidige digitale wereld worden systemen voortdurend blootgesteld aan diverse dreigingen, waaronder malware, ransomware en andere vormen van cyberaanvallen. Hardening omvat het aanpassen van configuraties om veiligheidsrisico's minimaliseren. Platform hardening draagt bij aan een eerste stap om systemen minder kwetsbaar te maken voor veelvoorkomende risico's zoals schadelijke software en ongeautoriseerde toegang.

4.3 Randvoorwaarden

Om de configuratiehandelingen in deze handleiding te kunnen uitvoeren, dient aan een aantal essentiële randvoorwaarden te worden voldaan. Deze voorwaarden zijn belangrijk om ervoor te zorgen dat de hardeningsprocessen correct worden geïmplementeerd. De minimale vereisten zijn als volgt:

- **Toegang tot een Windows Enterprise omgeving:** Een licentie voor Windows 11 Enterprise is vereist om de beschreven hardeningsmaatregelen toe te passen.
- **Minimaal Microsoft E3 Licentie:** Deze licentie biedt de noodzakelijke beveiligings- en beheertools die essentieel zijn voor platform hardening.
- **Aanwezigheid van Microsoft Intune:** Microsoft Intune is vereist voor het beheer van apparaten en voor het afdwingen van beveiligingsbeleid op alle apparaten binnen de organisatie.
- **Basiskennis van Microsoft Intune:** Dit omvat het begrijpen van hoe je apparaten kunt onboarden, policies kunt opstellen en implementeren, en hoe je rapportages en monitoring kunt uitvoeren binnen Intune (bijvoorbeeld MD-102).
- **Apparaat management via Intune:** Dit is noodzakelijk voor het centraal beheren van beveiligingsinstellingen en voor de uitvoering van hardeningsmaatregelen voor Intune managed devices.
- **Onboarding van alle apparaten in Entra ID:** Apparaten moeten minimaal geregistreerd zijn in Entra ID, bij voorkeur Entra ID joined.
    - Bij gebruik van lokale Active Directory, moet Entra Connect of Cloud Sync ingeschakeld zijn.

4.4 Raamwerken

In deze handleiding is gebruikt gemaakt van de Center for Internet Security (CIS) Benchmark en de Microsoft Security Baseline for Windows 10 (en later). De CIS-Benchmarks bieden gedetailleerde, stapsgewijze richtlijnen voor het veilig configureren van IT-systemen. Het Microsoft-framework bevat aanbevelingen voor het configureren van Windows-systemen. Deze instellingen zijn in lijn met de beveiligingsaanbevelingen uit de Windows Security Baseline. Het is belangrijk te benadrukken dat, hoewel deze configuraties een belangrijke stap zijn in het versterken van de beveiliging, ze geen volledige bescherming bieden tegen alle mogelijke dreigingen. Door gebruik te maken van deze raamwerken kunnen organisaties beginnen met het implementeren van methoden en instellingen om hun IT-omgeving beter te beveiligen.

4.5 Leeswijzer

In deze handleiding is een keuze gemaakt om alleen de Windows end-user-computing platform instellingen te beschrijven. Dit is het meest gebruikte platform binnen de doelgroep voor deze handleiding.

Bij de instellingen is telkens aangegeven wat het niveau van hardening is (Level 1 t/m 5). Dit niveau geeft de mate van compleetheid waarin de basis hardening is geïmplementeerd en vormt een startpunt voor verdere beveiliging.

Daarnaast is aangeven op welk scherm de instelling gewijzigd kan worden. Naast de aanbevolen instelling is ook een onderbouwing aangegeven van de instelling.

5. Basis Platform Hardening

In dit hoofdstuk wordt uitgelegd welke configuratie veranderingen kunnen worden uitgevoerd binnen een organisatie, met als doel basis platform hardening.

5.1 Windows End-User Computing Settings

Windows End-User Computing (EUC) instellingen verwijzen naar de configuraties en beleidsinstellingen die specifiek de interactie van eindgebruikers met Windows-systemen beïnvloeden. Deze instellingen zijn essentieel voor het waarborgen van de beveiliging van werkplekken binnen een organisatie, aangezien zij bepalen hoe gebruikers toegang krijgen tot systemen en data, welke applicaties zij mogen uitvoeren, en hoe beveiligingsmaatregelen zoals encryptie en authenticatie worden afgedwongen. In Microsoft Intune kunnen beheerders EUC instellingen beheren, die specifiek de interactie van eindgebruikers met Windows-systemen beïnvloeden.

5.2 Intune Admin Center

De website https://admin.microsoft.com is het centrale beheerdersportaal voor Microsoft 365. Vanaf deze pagina kunnen beheerders toegang krijgen tot verschillende administratieve tools en services, waaronder gebruikers- en groepsbeheer, licentiebeheer, en beveiligingsinstellingen. Het portaal biedt een interface met dashboardweergaven, meldingen en rapporten om de status van de Microsoft 365-services binnen de organisatie te monitoren en beheren.
Https://intune.microsoft.com is de beheerconsole voor Microsoft Intune, een cloudgebaseerde tool die zich richt op het beheer van mobiele apparaten (MDM) en mobiele applicaties (MAM). Met Intune kunnen beheerders centraal de apparaten en applicaties van werknemers beveiligen en beheren. Om naar https://intune.microsoft.com te gaan vanaf de https://admin.microsoft.com pagina, volg je deze stappen:

1. Log in op *https://admin.microsoft.com* met je beheerdersaccount.
2. Klik in het linker navigatiemenu op "*Show all*" om alle beschikbare opties weer te geven.
3. Scroll naar beneden en klik onder het kopje "Admin centers" op "*Microsoft Intune*".
4. Je wordt nu doorverwezen naar https://*intune.microsoft.com*, waar je toegang hebt tot alle Intune-functionaliteiten en -beheeropties.

5.3 Gebruikersrechten

Bij basis platform hardening speelt het beheer van gebruikersrechten een belangrijke rol. Gebruikersrechten bepalen welke acties gebruikers mogen uitvoeren binnen een systeem. Dit omvat onder andere toegangsrechten tot bestanden en mappen, het installeren van software, en het uitvoeren van systeembeheer taken. Door zorgvuldig te definiëren en te beperken welke rechten aan welke gebruikers worden toegekend, wordt het risico op ongeautoriseerde toegang en potentiële beveiligingsinbreuken aanzienlijk verminderd.

Impersonate a Client after Authentication	
Configuratie-niveau	L3
Intune	Device > Windows > Configuration
Aanbevolen configuratie	• Maak een policy (kies voor settings category) • Zoek in de settings picker naar ‘Impersonate Client‘ • Beperk dit recht tot de volgende gebruikers: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE
Toelichting	Deze instelling bepaalt welke gebruikers of groepen de bevoegdheid hebben om taken uit te voeren namens een andere gebruiker na authenticatie. Het kan nodig zijn voor bepaalde administratieve functies of automatiseringstaken. Door deze rechten zorgvuldig toe te wijzen, kan het risico op misbruik worden beperkt.
Handleiding	Impersonate a client after authentication

5.4 Password Policies

Dit gedeelte richt zich uitsluitend op het wachtwoordbeleid voor het lokale administratoraccount van een apparaat. Dit account wordt doorgaans alleen door beheerders gebruikt en is niet hetzelfde als een eindgebruikersaccount. Om deze accounts te beveiligen, wordt LAPS (Local Administrator Password Solution) aanbevolen, waarmee de wachtwoorden van lokale beheerdersaccounts op apparaten veilig kunnen worden beheerd. Instellingen met betrekking tot eindgebruikerswachtwoorden worden beheerd via Entra ID en vallen buiten de scope van dit onderwerp.

Begin met het creëren van een policy in de **Settings Catalog**. Geef de policy een duidelijke titel, zoals "**Password-policy-doel**", en beschrijf in de omschrijving de belangrijkste instellingen van deze policy, bijvoorbeeld wachtwoordlengte, maximale en minimale wachtwoordleeftijd, en andere relevante wachtwoordinstellingen. Nadat de policy is aangemaakt, kan de optie **+ Add setting** worden geselecteerd om een nieuwe instelling toe te voegen. Gebruik de zoekbalk om de gewenste instelling te vinden, zoals **"Device Lock".** Na het vinden van de juiste instelling, kan deze geselecteerd worden om de configuratie verder in te stellen.

Belangrijk: Zorg ervoor dat de policies in Intune afgestemd zijn op de policies in Entra ID

Password Expiration	
Configuratie-niveau	L5
Intune	Device > Windows > Configuration
Aanbevolen configuratie	• Setting category: Local Administrator Password Solution (LAPS) • Password age: *Maximaal 90 dagen*
Toelichting	Het instellen van een maximale wachtwoordleeftijd zorgt ervoor dat gebruikers hun wachtwoorden periodiek moeten wijzigen. Dit helpt voorkomen dat wachtwoorden voor langere periodes hetzelfde blijven, wat de kans op een succesvolle aanval vergroot. Een korte maximale geldigheidsduur maakt dat gebruikers constant hun wachtwoord moeten wijzigen. Dit kan ertoe leiden dat gebruikers zwakkere wachtwoorden kiezen, wachtwoorden noteren of weerstand tegen de wijziging krijgen. Het is daarom van belang de periode niet te kort te maken.
Handleiding	Create Intune policies to configure and manage Windows LAPS | Microsoft Learn

Minimum Password Length	
Configuratie-niveau	L5
Intune	Device > Windows > Configuration
Aanbevolen configuratie	• Setting category: LAPS • *Password Length:* Minimaal 14
Toelichting	Het gebruik van langere wachtwoorden versterkt de beveiliging door het aanzienlijk moeilijker te maken voor aanvallers om een wachtwoord te raden of brute force-aanvallen uit te voeren. Microsoft beveelt minimaal 14 tekens aan voor een wachtwoord, aangezien langere wachtwoorden meer combinaties bieden en zodoende het risico op ongeautoriseerde toegang verminderen.
Handleiding	Create Intune policies to configure and manage Windows LAPS | Microsoft Learn

Password Complexity	
Configuratie-niveau	L5
Intune	Device > Windows > Configuration
Aanbevolen configuratie	• Setting category: LAPS • Password Complexity: Large letters + small letters + numbers + specials (5)
Toelichting	De instelling "Wachtwoordcomplexiteit" onder LAPS bepaalt de vereiste complexiteit voor wachtwoorden op apparaten, zodat deze voldoen aan specifieke criteria zoals lengte, teken types en andere beveiligingsvereisten ter versterking van de bescherming.
Handleiding	Device Compliance settings | Microsoft Learn

5.5 LSA-Protection

LSA-Protection (Local Security Authority Protection) is een belangrijke beveiligingsfunctie die is ontworpen om de kritieke authenticatiegegevens van een systeem te beschermen. Door LSA-Protection in te schakelen, worden gevoelige gegevens zoals wachtwoorden en beveiligingstokens beter beveiligd tegen aanvallen. Het inschakelen van LSA-Protection voorkomt dat niet-beveiligde processen toegang krijgen tot deze informatie, waardoor de kans op misbruik wordt verkleind.

LSA-Protected Process	
Configuratie-niveau	L5
Intune	Device > Windows > Configuration
Aanbevolen configuratie	Enabled with Unified Extensible Firmware Interface (UEFI) lock
Toelichting	Door Local Security Authority Subsystem Service (LSASS) als een beschermd proces in te stellen, wordt de beveiliging van LSASS verhoogd door te voorkomen dat kwaadwillende software de werking van het proces manipuleert. De UEFI-vergrendeling biedt extra bescherming door te eisen dat systeeminstellingen moeilijker aan te passen zijn zonder toegang tot de firmware-instellingen van de computer. **Belangrijk**: **Deze configuratie is alleen voor WHQL gecertificeerde drivers.**

5.6 Security Options

Security Options omvatten een reeks instellingen die de algehele beveiliging van een systeem versterken door controle te bieden over verschillende beveiligingsfuncties en -gedragingen. Deze opties bieden bescherming tegen zowel interne als externe dreigingen door zaken als gebruikersrechten, netwerkbeveiliging en toegangscontrole te configureren.

Enable Windows Firewall	
Configuratie-niveau	L1
Intune	Devices > Configuration
Aanbevolen configuratie	• Maak policy (Windows 10 en later) • Profile type: templates > zoek op 'Endpoint Protection' • Windows Firewall configuration settings openklappen • Network Settings > Windows Firewall > Enable • Indien mogelijk; Configureer de overige firewall settings onder het kopje Windows Firewall
Toelichting	Het configureren van Windows Firewall in Intune helpt bij het beschermen van het netwerk tegen beveiligingsdreigingen en aanvallen.
Handleiding	Intune endpoint security firewall settings | Microsoft Learn

Enable BitLocker Encryption	
Configuratie-niveau	L5
Intune	Devices > Configuration
Aanbevolen configuratie	• Maak policy (Windows 10 en later) • Profile type: templates > zoek op 'Endpoint Protection' • Windows Encryption configuration settings openklappen • Windows Settings > Encrypt devices > Require • Indien mogelijk; configureer overige bitlocker settings mbt Removable Media (USB-sticks, external disks, etc)
Toelichting	BitLocker Drive Encryption beschermt gegevens door ze te versleutelen, waardoor ongeautoriseerde toegang wordt voorkomen, zelfs als de computer verloren, gestolen of buiten gebruik gesteld is. De Microsoft Learn website bevat aanvullende artikelen over best practices voor sleutelbeheer, waaronder procedures voor verlies en herstel.
Handleiding	Enabling BitLocker with Microsoft Endpoint Manager - Microsoft Intune | Microsoft Community Hub

Enable Automatic updates for Windows OS and applications	
Configuratie-niveau	L2
Intune	Devices > Manage Updates > Windows Updates > Update rings
Aanbevolen configuratie	• Maak een profile • Configureer de gewenste update settings*
Toelichting	Deze configuratie zorg ervoor dat automatische updates zijn ingeschakeld om de veiligheid en functionaliteit van het Windows besturingssysteem en de applicaties te waarborgen. Dit vermindert het risico op kwetsbaarheden en zorgt ervoor dat de nieuwste functies en verbeteringen beschikbaar zijn. **Belangrijk: configureer auto reboot om ervoor te zorgen dat nieuwe updates in werking treden.**
Handleiding	Learn about using Windows Update for Business in Microsoft Intune | Microsoft Learn

*****Organisaties met 100-200 medewerkers kunnen de bovenstaande updateconfiguratie uitvoeren zonder het gebruik van update-ringen. Bij grotere organisaties is het echter aan te raden om update-ringen te gebruiken, zodat de uitrol van updates gecontroleerd en gefaseerd kan plaatsvinden. Een mogelijke indeling is als volgt: Ring 0 voor testsystemen, Ring 1 voor pilotgebruikers en de productiering voor alle overige medewerkers. Dit zorgt ervoor dat updates eerst gevalideerd worden voordat ze breed worden uitgerold. Voor een gedetailleerde instructie over het configureren van update-ringen in Intune, zie: Configure Update rings for Windows 10 and later policy in Intune | Microsoft Learn. Daarnaast is het belangrijk om de herstartinstellingen (reboot) goed te configureren, zodat geïnstalleerde updates daadwerkelijk in werking treden.

Enable Multi-Factor Authentication (MFA)	
Configuratie-niveau	L2
Intune	Devices > Conditional Access
Aanbevolen configuratie	Maak een policy aan binnen Conditional Access en stel de toegangsmethoden in op Grant > Require authentication strength > MFA om Multi-Factor Authentication af te dwingen voor gebruikers.
Toelichting	Multi-Factor Authentication (MFA) verhoogt de beveiliging door gebruikers te verplichten zich te verifiëren via twee of meer factoren. Dit vermindert het risico op ongeautoriseerde toegang, zelfs als een wachtwoord wordt gecompromitteerd. **Belangrijk: Definieer vooraf passende conditional access rules.**
Handleiding	Overview of Microsoft Entra authentication strength - Microsoft Entra ID | Microsoft Learn

Activate Credential Guard	
Configuratie-niveau	L4
Intune	Device > Windows > Configuration
Aanbevolen configuratie	• Maak een policy > Selecteer 'Setting catalog' • Voeg de setting 'Device Guard' toe • Credential Guard: Enabled without lock
Toelichting	Credential Guard beschermt inloggegevens door deze af te schermen in een geïsoleerde omgeving. Het inschakelen van Credential Guard voorkomt dat kwaadwillenden toegang krijgen tot deze gevoelige informatie, zelfs als zij beheerrechten verkrijgen op een apparaat. "Enabled with UEFI lock" biedt de hoogste beveiliging omdat het Credential Guard alleen kan worden uitgeschakeld via het UEFI. Gebruik deze setting alleen als uitschakelen op afstand niet nodig is. **Belangrijk: Credential Guard heeft impact op services die NTLMv1, MS-CHAPv2, Digest, en CredSSP gebruiken. Voer een analyse uit om te bepalen of deze configuratie-instelling geschikt is voor het bestaande organisatietype**.
Handleiding	**DeviceGuard Policy CSP | Microsoft Learn**

5.7 Exploit Protection & Attack Surface Reduction

Exploit Protection biedt een aanvullende laag van verdediging door kwetsbaarheden in software te identificeren en te blokkeren die door aanvallers kunnen worden misbruikt. Dit kan helpen bij het beschermen van systemen tegen veel voorkomende aanvalstechnieken. Het is belangrijk om ASR-regels eerst grondig te testen voordat je ze implementeert. Aangepaste instellingen kunnen invloed hebben op de werking van systemen. Daarom wordt aangeraden de instellingen in een testomgeving uit te proberen om eventuele negatieve impact te beoordelen. Daarnaast kunnen instellingen stapsgewijs worden toegepast, zodat de impact goed gemeten en gecontroleerd kan worden voordat alles op grote schaal wordt doorvoert[1].

Zie hier hoe ASR-regels het beste getest kunnen worden. ASR biedt de mogelijkheid om per regel uitsluitingen te configureren, wat betekent dat specifieke toepassingen of processen kunnen worden uitgesloten van de ASR-regels, zelfs wanneer ze normaal gesproken door deze beveiligingsmaatregelen zouden worden getroffen. Het gebruik van uitsluitingen kan noodzakelijk zijn wanneer bepaalde applicaties niet goed functioneren in combinatie met bepaalde ASR-regels.

Let op! Start bij het implementeren van ASR-regels altijd eerst in de audit mode om de impact per ASR-regel te analyseren.

Disallow Exploit Protection Override	
Configuratie-niveau	L3
Intune	Endpoint security > Attack surface reduction > Exploit Protection
Aanbevolen configuratie	Enable: Lokale gebruikers mogen geen wijzigingen aanbrengen in het gedeelte voor exploitbescherming.
Toelichting	Deze instelling voorkomt dat gebruikers wijzigingen kunnen aanbrengen in de exploitbeschermingsinstellingen in het Windows Defender Security Center. Als deze instelling wordt uitgeschakeld of niet is geconfigureerd, kunnen lokale gebruikers alsnog aanpassingen doen aan de exploitbescherming.
Handleiding	Turn on exploit protection to help mitigate against attacks - Microsoft Defender for Endpoint | Microsoft Learn

Block Execution of Potentially Obfuscated Scripts	
Configuratie-niveau	L2

[1] Voor meer details aangaande gecontroleerde implementatie kunt u de Implementatiehandleiding raadplegen.

Block Execution of Potentially Obfuscated Scripts	
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel detecteert verdachte eigenschappen binnen een obfuscerend script. Het blokkeren van obfuscerende scripts helpt bij het voorkomen van aanvallen die gebruik maken van complexe technieken om scripts onleesbaar te maken voor bijvoorbeeld antivirussoftware.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Win32 API Calls from Office Macros	
Configuratie-niveau	L3
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel voorkomt dat VBA-macro's Win32 API-aanroepen en uitvoeren. Dit wordt vaak misbruikt door aanvallers om schadelijke code te laden. Het blokkeren van deze toegang verkleint de kans dat malware via macro's toegang krijgt tot het systeem en wordt uitgevoerd.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Office Communication Application from Creating Child Processes	
Configuratie-niveau	L3
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel blokkeert alle Office-applicaties, zoals Word, Excel en PowerPoint, van het aanmaken van child-processen. Het voorkomt dat schadelijke code wordt uitgevoerd vanuit Office-applicaties, wat een belangrijke verdediging is tegen macro-aanvallen en andere soorten Office-kwetsbaarheden.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Adobe Reader from Creating Child Processes	
Configuratie-niveau	L2
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel voorkomt aanvallen door Adobe Reader, een veelgebruikte doelwittest voor aanvallers, van het creëren van child-processen. Dit voorkomt dat Adobe Reader wordt misbruikt om schadelijke processen te lanceren, een techniek die vaak worden ingezet voor het verspreiden van malware.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Credential Stealing from the Windows Local Security Authority Subsystem	
Configuratie-niveau	L3
Intune	Endpoint security > Attack surface reduction > ASR Rules

Block Credential Stealing from the Windows Local Security Authority Subsystem	
Aanbevolen configuratie	Block
Toelichting	Deze regel helpt bij het voorkomen van het stelen van inloggegevens door de Local Security Authority Subsystem Service (LSASS) af te schermen. Het blokkeert pogingen van aanvallers om LSASS te manipuleren en wachtwoorden en tokens van gebruikers te stelen Dit is essentieel voor het beschermen tegen credential stuffing en privilege escalation aanvallen.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block JavaScript or VBScript from Launching Downloaded Executable Content	
Configuratie-niveau	L3
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel voorkomt dat JavaScript- of VBScript-scripts gedownloade uitvoerbare bestanden lanceren. Veel malware gebruiken deze scripts als downloader om andere schadelijke payloads van het internet te halen. Door deze uitvoerbare inhoud te blokkeren, verklein je de kans op geïnfecteerde downloads die kunnen leiden tot ransomware of malware-infecties.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Persistence through WMI Event Subscription	
Configuratie-niveau	L4
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel voorkomt dat malware WMI (Windows Management Instrumentation) misbruikt om persistente toegang tot een systeem te behouden. Veel fileless malware maakt gebruik van WMI om zich te verbergen en automatisch opnieuw uit te voeren na een herstart, en deze regel helpt dergelijke dreigingen te blokkeren.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Process Creations Originating from PSExec and WMI Commands	
Configuratie-niveau	L4
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel blokkeert procescreaties die via PsExec of WMI zijn geactiveerd. Beide tools kunnen op afstand worden gebruikt om code uit te voeren, wat een risico vormt voor het verspreiden van malware door netwerken. Het blokkeren van deze processen helpt om kwaadwillende activiteiten te voorkomen die via netwerken kunnen worden verspreid.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Office Applications from Creating Executable Content	
Configuratie-niveau	L3

Block Office Applications from Creating Executable Content	
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel voorkomt dat Office-applicaties, zoals Word, Excel en PowerPoint, uitvoerbare inhoud aanmaken die mogelijk schadelijk kan zijn. Het blokkeert het schrijven van schadelijke code naar de schijf, wat het risico op geïnfecteerde bestanden vermindert.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Office Applications from Injecting Code into other Processes	
Configuratie-niveau	L4
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze regel blokkeert pogingen van Office-applicaties om code in andere processen te injecteren. Dit voorkomt dat aanvallers via kwetsbaarheden in Office-applicaties proberen andere programma's te manipuleren of aanvallen uit te voeren en tegelijkertijd detectie te omzeilen.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

Block Executable Content from Email Client and Webmail	
Configuratie-niveau	L2
Intune	Endpoint security > Attack surface reduction > ASR Rules
Aanbevolen configuratie	Block
Toelichting	Deze instelling blokkeert de uitvoering van uitvoerbare inhoud (zoals .exe, .dll, .scr bestanden) die via e-mailclients of webmail wordt ontvangen. Dit helpt te voorkomen dat schadelijke bijlagen, die vaak gebruikt worden bij phishing-aanvallen of verspreiding van malware, automatisch worden uitgevoerd. Door deze instelling in te schakelen, worden risico's op malware-infecties via e-mail verminderd.
Handleiding	Use attack surface reduction rules to prevent malware infection - Microsoft Defender for Endpoint | Microsoft Learn

5.8 Logging Settings

Logging Settings spelen een belangrijke rol in het vastleggen en monitoren van activiteiten binnen een systeem. Door gedetailleerde logbestanden bij te houden van systeem- en gebruikersactiviteiten, kunnen beheerders potentiële beveiligingsincidenten snel detecteren en hierop reageren. Het correct configureren van logginginstellingen zorgt ervoor dat belangrijke gebeurtenissen, zoals inlogpogingen, systeemfouten en wijzigingen in systeeminstellingen, nauwkeurig worden vastgelegd. Dit maakt het mogelijk om gedetailleerde audits uit te voeren en biedt een waardevolle bron voor onderzoek voor onder andere het SOC bij mogelijke incidenten.

1. Toegang tot het Intune-beheercentrum.
    a. Log in op het *Microsoft Endpoint Manager-beheercentrum* met uw beheerdersaccount.
    b. Navigeer naar *Devices* in het linker navigatiemenu.
2. Windows-configuraties openen
    a. Selecteer onder het menu *Devices* de optie *Windows*.
    b. Klik vervolgens op *Configuration* om een overzicht van bestaande configuratie profielen te zien.
3. Nieuw configuratieprofiel aanmaken
    a. Klik op *Create profile* om een nieuw configuratieprofiel aan te maken.
    b. Kies voor *Windows 10 and later* als platform.
    c. Selecteer als profieltype *Settings catalog.*
4. Configuratieprofiel instellen
    a. Geef het profiel een duidelijke naam en beschrijving zodat het later makkelijk te identificeren is.
    b. Klik op Next om verder te gaan naar de configuratie-instellingen.
5. Instellingen catalogus gebruiken
    a. In het Configuration settings scherm, klik op *Add settings.*
    b. Gebruik de zoekbalk en typ "Auditing" om de relevante auditinstellingen te vinden.
6. Maak een policy
7. Auditinstellingen configureren

Onderstaande loginstellingen vormen de basis van de Microsoft Baseline Recommendation. Voor geavanceerdere logopties en sterkere aanbevelingen kan het document "A10 Log Audit policies" worden geraadpleegd.

Audit Account Logoff	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: Yes • Failure: No
Toelichting	Het bijhouden van logoffs is belangrijk voor het monitoren van gebruikersactiviteiten. Het helpt beheerders inzicht te krijgen in wanneer gebruikers hun sessies beëindigen, wat nuttig kan zijn voor het opsporen van verdachte activiteiten.
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Account Logon	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: yes
Toelichting	Het registreren van succesvolle aanmeldingen biedt inzicht in wie wanneer toegang heeft verkregen tot het systeem. Dit is belangrijk voor het bijhouden van toegangsactiviteiten en het snel identificeren van ongeautoriseerde toegang.
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Authentication Policy Change	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: Yes • Failure: No
Toelichting	Het registreren van wijzigingen in het authenticatiebeleid is belangrijk om op de hoogte te blijven van beleidsaanpassingen (policies) die de beveiliging van het systeem beïnvloeden
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Security System Extension	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: yes
Toelichting	Het registreren van gebeurtenissen die verband houden met beveiligingssysteemextensies, zoals Kerberos en NTLM, wanneer ze worden geladen of geregistreerd.
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Changes to Audit Policy	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: yes
Toelichting	Het bijhouden van wijzigingen in het auditbeleid is belangrijk om te weten wanneer en door wie auditinstellingen worden aangepast.
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Security Group Management	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: no
Toelichting	Het registreren van gebeurtenissen in het beheer van beveiligingsgroepen helpt bij het monitoren van wijzigingen in groepslidmaatschappen en rechten
Handleiding	Audit Policy CSP | Microsoft Learn

Audit Special Logon	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: No
Toelichting	Het registreren van speciale aanmeldingen, zoals die met verhoogde privileges, is belangrijk voor het monitoren van beheerdersactiviteiten en andere gevoelige sessies.
Handleiding	Audit Policy CSP | Microsoft Learn

Audit User Account Management	
Configuratie-niveau	L1
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: no
Toelichting	Het registreren van gebeurtenissen in gebruikersaccountbeheer is belangrijk voor het volgen van wijzigingen in gebruikersaccounts. Dit helpt beheerders inzicht te krijgen in wie accounts aanmaakt, wijzigt of verwijdert,
Handleiding	Audit Policy CSP | Microsoft Learn

System Audit Security State Change	
Configuratie-niveau	L4
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: yes
Toelichting	Het registreren van beveiligingstoestandswijzigingen helpt bij het bewaken van belangrijke wijzigingen in de beveiligingsstatus van het systeem. Dit kan wijzigingen in de beveiligingsconfiguratie of andere belangrijke beveiligingsinstellingen omvatten.
Handleiding	Audit Policy CSP | Microsoft Learn

System Audit System Integrity	
Configuratie-niveau	L4
Intune	Devices > Windows > Configuration
Aanbevolen configuratie	• Success: yes • Failure: yes
Toelichting	Het registreren van zowel succesvolle als mislukte systeemintegriteitsgebeurtenissen is belangrijk voor het bewaken van pogingen om de systeemintegriteit te compromitteren.
Handleiding	Audit Policy CSP | Microsoft Learn

6. Bijlage I – Configuratiestatus checklist

Level	Configuration Control	Status
L1	Audit Account Logoff (H 4.8)	
	Audit Account Logon (H 4.8)	
	Audit Authentication Policy Change (H 4.8)	
	Audit Security System Extension (H 4.8)	
	Audit Changes to Audit Policy (H 4.8)	
	Audit Security Group Management (H 4.8)	
	Audit Special Logon (H 4.8)	
	Audit User Account Management (H 4.8)	
	Enable Windows Firewall (H 4.6)	
L2	Block Execution of Potentially Obfuscated Scripts (H 4.7)	
	Block Adobe Reader from Creating Child Processes (H 4.7)	
	Block Executable Content from Email Client and Webmail (H 4.7)	
	Enable Automatic updates for Windows OS and applications (H 4.6)	
	Enable Multi-Factor Authentication (MFA) (H 4.6)	
L3	Disallow Exploit Protection Override (H 4.7)	
	Block Win32 API Calls from Office Macros (H 4.7)	
	Block Office Communication Application from Creating Child Processes (H 4.7)	
	Block Credential Stealing from the Windows Local Security Authority Subsystem (H4.7)	
	Block JavaScript or VBScript from Launching Downloaded Executable Content (H 4.7)	
	Block Office Applications from Creating Executable Content (H 4.7)	
	Impersonate a Client after Authentication (H 4.3)	
L4	Block Persistence through WMI Event Subscription (H 4.7)	
	Block Process Creations Originating from PSExec and WMI Commands (H 4.7)	
	Block Office Applications from Injecting Code into other Processes (H 4.7)	
	System Audit System Integrity (H 4.8)	
	Activate Credential Guard (H 4.6)	
	System Audit Security State Change (H 4.8)	
L5	Enable BitLocker Encryption (H 4.6)	
	Password Expiration (H 4.4)	
	Minimum Password Length (H 4.4)	
	Password Complexity (H 4.4)	
	LSA-Protected Process (H 4.5)	

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