

# Attack Surface Reduction Rules

Workplace Ninja User Group Finland

20.12.2024





- Mikä on ASR?
- Konfliktinäkymät
- Raportit
- Event Viewer
- Jotain muuta?



# Miksi tämä pitäisi kiinnostaa?

[www.wpninjas.fi](http://www.wpninjas.fi)



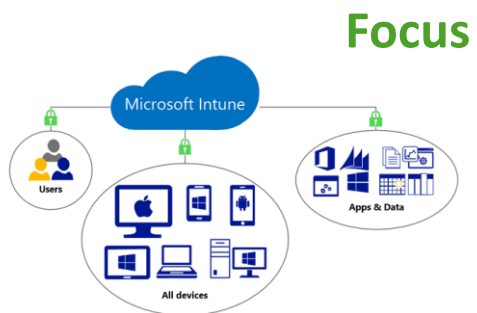
Tietoturva myy, osa Zero Trustia

DFE Security Recommendationsissa esillä



# Pavel Mirochnitchenko

[www.wpninjas.fi](http://www.wpninjas.fi)



**From**



**User Group Finland**



*Workplace Ninja*  
*User Group Finland*



&



**Microsoft  
Intune**

**Hobbies**



- IT company of 600 professionals
- Cloud Services, corporate networks, security solutions
- Subsidiary of Telia Company, Nordic telecommunication solutions



# Mitä emme käsittele tänään

---

Attack Surface Reduction sisältää myös:

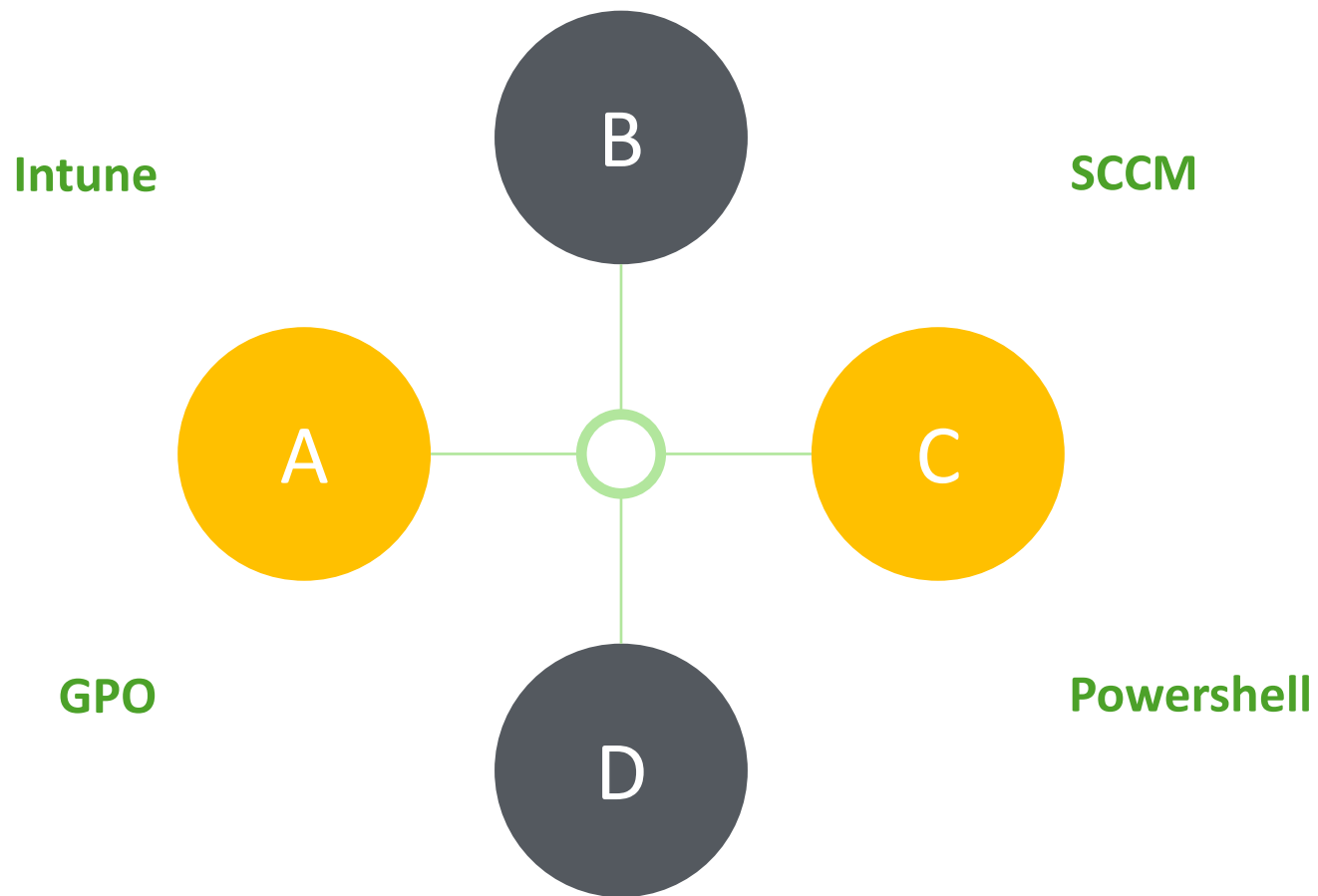
- Hardware-based isolation for Edge
- Application Control (WDAC, Application Control for Business)
- Web Protection
- Exploit Guard
- Network Protection, Firewall

Muista: *"the full attack surface reduction feature-set is only available with a Windows enterprise license."*



# Hallintatavat

[www.wpninjas.fi](http://www.wpninjas.fi)






- Intunessa on useita mahdollisuuksia
  - Endpoint Security \ ASR \ ASR Rules
  - Windows Security Baseline, Defender for Endpoint Security Baseline
  - Settings Catalog

Pavelin suositus -> ota muualta pois, käytä vain ASR Rules.
- Ensin AUDIT, sitten BLOCK



- Block vs. Warn vs. Audit = ei välttämättä muodosta konfliktia yksittäisessä tapauksessa
- Enable vs. Disable (Controlled Folders) = muodostavat
- Näkymä yksittäisen Device -> Configuration

Device Windows Security Attack Surface Reduction Rules v3	System account	Settings Catalog	⚠ Conflict
	pauli@yannara.net	Settings Catalog	⚠ Conflict
Device Windows Security Attack Surface Reduction Rules v3	pauli@yannara.net	Settings Catalog	⚠ Conflict
Device ASR Test	System account	Settings Catalog	⚠ Conflict
Device ASR Test	pauli@yannara.net	Settings Catalog	⚠ Conflict

Name	Status
ASR Only Per Rule Exclusions	✓ Succeeded
Attack Surface Reduction Rules	✓ Succeeded
Enable Controlled Folder Access	⚠ Conflict





# Konflikti näkymä

www.wpninjas.fi

## W365-H3X7B - Policy Settings ...

Recently updated information can take up to 20 minutes to be available in this report.

Refresh Columns

Search



Add filters

Name

Status

Error code

Attack Surface Reduction Rules

Conflict

Enable Controlled Folder Access

Succeeded

### Setting - Details

#### SETTING

Attack Surface Reduction Rules

#### STATE

Conflict

#### SOURCE PROFILES

Source Profile



Device Windows Security Attack Surface R...

ASR test block



ASR test audit

Source Profiles näkyy vain jos molemmat policyt ovat ASR Ruleja, muuten arvataan itse mistä konflikti tulee





# Voi jeesus sentään

- Satunnaisia virheitä luonnin yhteydessä, ei merkkää mitään. Ilmeisesti jos tekee objektin ilman assignmenttia, niin menee läpi. Jos samaan aikaan assigmentin kanssa niin feilaa

 **Create policy** 

Something went wrong. Unable to successfully create Device Windows Security Attack Surface Reduction PSEXEC test.

a few seconds ago

 **Create policy** 

Something went wrong. Unable to successfully create Device Windows Security Attack Surface Reduction PSEXEC test.

a few seconds ago



Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT administrator. For more information please contact your IT administrator.  
ID: 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2

Detected file	Detected on	Blocked/Audited?	Rule	Source app	Device
<input type="checkbox"/> svchost.exe	Dec 9, 2024 7:30 AM	Blocked	Block credential stealing from the Windows local security authority subsystem (lsass.exe)	svchost.exe	lb2ce2491sws
<input type="checkbox"/> svchost.exe	Dec 8, 2024 10:40 PM	Blocked	Block credential stealing from the Windows local security authority subsystem (lsass.exe)	svchost.exe	lbasus

## Block credential stealing from the Windows local security authority subsystem (lsass.exe)

Remediation required

Human operated ransomware   User impact assessment   Internet facing

Open software page   Report inaccuracy

General   Remediation options

Follow these steps:

1. Ensure that [Microsoft Defender Antivirus is turned on](#) as the **primary** antivirus solution, with [Real-Time Protection](#) enabled.
2. Enable [this ASR rule](#) in **Block** mode using either [Intune \(Windows 10 only\)](#), [Group Policy](#) or [MDM](#)



# Custom lokinäkymä (event viewer)

[www.wpninjas.fi](http://www.wpninjas.fi)

[Understand and use attack surface reduction - Microsoft Defender for Endpoint | Microsoft Learn](#)





# 'Block credential stealing from the Windows local security authority sub system'

[www.wpninjas.fi](http://www.wpninjas.fi)

## Case Esimerkki

I recently enabled the attack surface reduction rule, 'Block credential stealing from the Windows local security authority subsystem (lsass.exe)', and I'm getting a large number of notifications. What is going on?

A notification generated by this rule doesn't necessarily indicate malicious activity; however, this rule is still useful for blocking malicious activity, since malware often targets lsass.exe to gain illicit access to accounts. The lsass.exe process stores user credentials in memory after a user has logged in. Windows uses these credentials to validate users and apply local security policies.

Because many legitimate processes throughout a typical day are calling on lsass.exe for credentials, this rule can be especially noisy. If a known legitimate application causes this rule to generate an excessive number of notifications, you can add it to the exclusion list. Most other attack surface reduction rules generate a relatively smaller number of notifications, in comparison to this one, since calling on lsass.exe is typical of many applications' normal functioning.

Device
lb5cg91225f8
lb5cg91225f8
lb5cg9491plc
lbasus
lb5cg9491plc
w365-h3x7b
lb5cg91225f8
lb5cg9491plc
lbasus
lb5cg9491plc
w365-h3x7b
lb2ce2491sww

Block



C:\Windows\System32\lsass.exe



# Case esimerkki 2

www.wpninjas.fi

Event 1121, Windows Defender

General Details

Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT administrator.  
For more information please contact your IT administrator.

ID: D1E49AAC-8F56-4280-B9BA-993A6D77406C  
Detection time: 2024-12-18T15:40:31.029Z  
User: NT AUTHORITY\SYSTEM  
Path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
Process Name: C:\Windows\PSEXESVC.exe  
Target Commandline: "powershell.exe"  
Parent Commandline: C:\WINDOWS\PSEXESVC.exe  
Involved File:  
Inheritance Flags: 0x00000000  
Security intelligence Version: 1.421.859.0  
Engine Version: 1.1.24090.11  
Product Version: 4.18.24090.11

Block process creations originating from Block  
PSEXec and WMI commands ⓘ

ASR Only Per Rule Exclusions ⓘ

C:\Intune\psexec.exe, C:\Intune\psexec64.exe,  
C:\Windows\System32\cmd.exe, C:\Windows\PSEXESVC.exe



# Lisää tutkittavaa

---

[www.wpninjas.fi](http://www.wpninjas.fi)

- Advanced Hunting ->

```
DeviceEvents  
| where ActionType startswith 'Asr'
```

- Powershell -> Get-MPPreference | Select-Object -ExpandProperty AttackSurfaceReductionRules\_Ids