jamk

Koventaminen – Labra 2

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Harjoitustyö

Helmikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

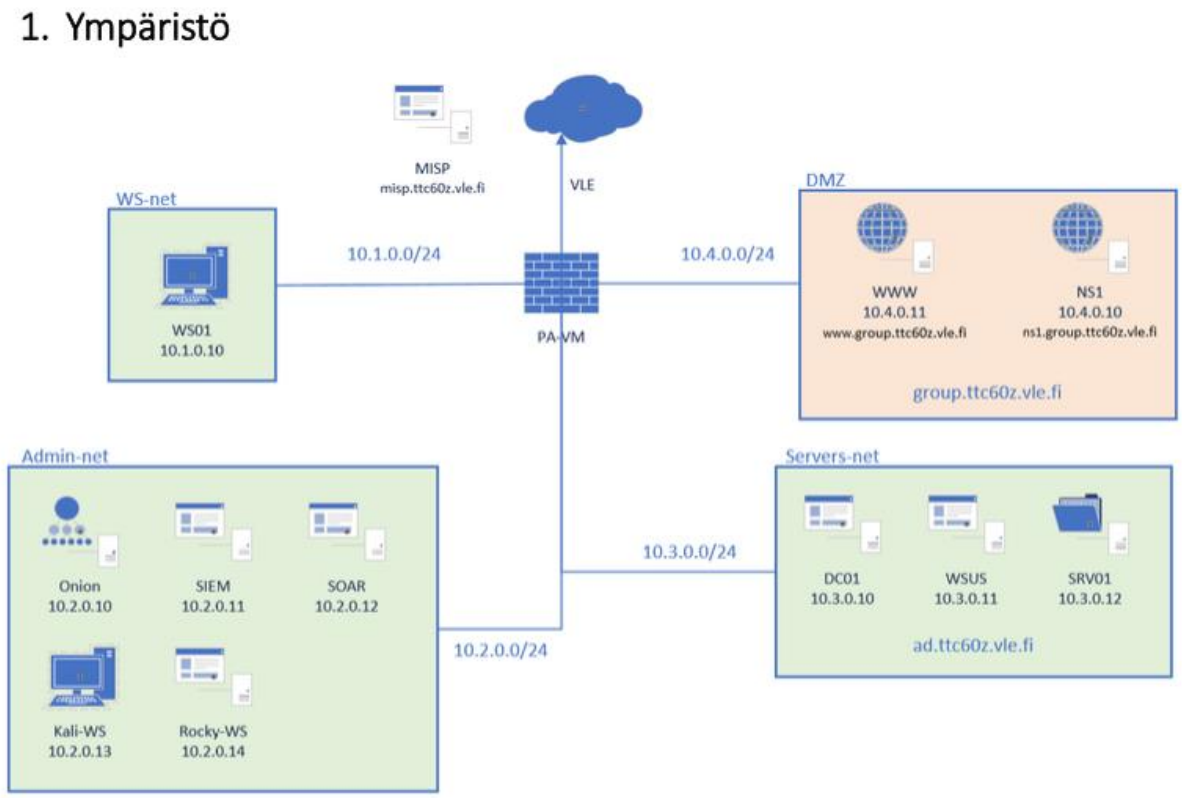
jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Tämän labran tehtävänantona oli työaseman Windows 11 koventaminen, jota lähdimme suorittamaan suositellulla Security Compliance Toolilla, koska kyseinen työkalu ei ollut meille tuttu. Tehtävässä lähdimme ohjeen mukaisesti ensin katsomaan nykyisen työaseman kautta minkälaista suositusta Security Compliance Tool meille antaa, jonka jälkeen teimme saman DC01 –koneella, jossa määritimme baselinen mukaiset GPO:t kyseisen työkalun scriptin avulla, ja teimme samassa muutaman oman kovennuksen GPO -käytänteisiin käyttäen apuna CIS Microsoft Windows 11 Stand-alone Bencmark –ohjetta. Raportissa käsitellään teoriaa, työaseman koventamista, Security Compliance Toolia, GPO:n määrittelyä sekä ryhmän kolme pohdintaa harjoituksen kokonaisuudesta. Harjoitus suoritetaan VLE -ympäristössä, ja käytetty topologia on esitetty (ks. Kuvio 1).



Kuvio 1. VLE ympäristö

2 Teoria

2.1 Windows 11 työaseman koventaminen

Windows työaseman koventamiseen löytyy monta erilaista kovennusohjetta, ja tässä harjoituksessa käytimme Windowsin Security Compliance Toolin avulla saatuja Baseline –kovennuksia, ja tästä ohjelmistosta lisäteoriaa seuraavissa luvuissa. Lisäksi käytimme CIS Microsoft Windows 11 benchmark kovennusohjetta ylimääräisissä kovennuksissa. Windows työaseman koventaminen tapahtuu pääsääntöisesti Domain Controller -työaseman kautta tehtyjen Group Policy Objectien kautta, koska näillä pystytään muuttamaan lähes kaikkia työaseman asetuksia.

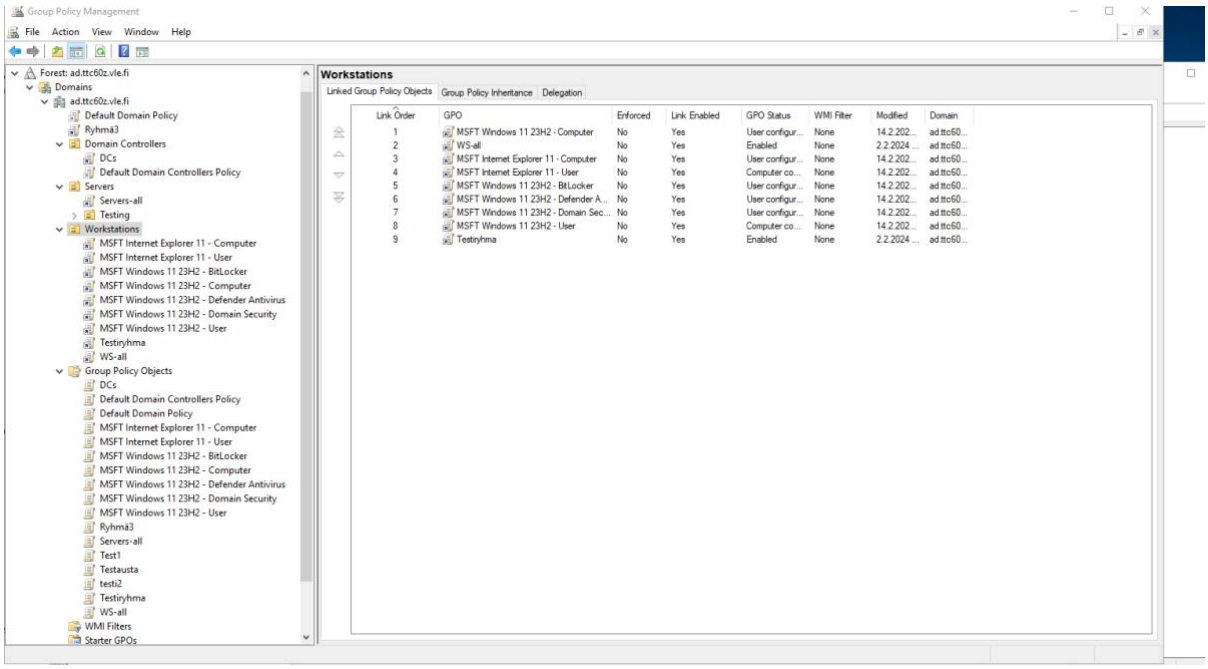
Group Policy Objectit jaetaan tietokoneeseen vaikuttaviin ja käyttäjään vaikuttaviin käytäntöasetuksiin. Tietokoneeseen liittyvissä käytännöissä määritetään mm. järjestelmän käyttäytyminen, sovellusasetukset, suojausasetukset, määritetyt sovellukset ja tietokoneen käynnistys- ja sammutusohjelmat. Käyttäjään liittyvissä käytännöissä määritetään mm. järjestelmän käyttäytymisen, sovellusasetukset, suojausasetukset, määritetyt ja julkaistut sovellukset, käyttäjän kirjautumis- ja uloskirjautumisskriptit sekä kansioiden uudelleenohjauksen. Tietokoneeseen liittyvät asetukset ohittavat käyttäjään liittyvät asetukset. (Group Policy Objects. 2018).

Työaseman koventamisessa voidaan käyttää esimerkiksi CIS Microsoft Windows 11 Stand-alone Bencmark –ohjetta, joka pitää sisällään hyvin laajalla skaalalla erilaisia koventamiskohteita. CIS Microsoft Windows Benchmark on kirjoitettu itsenäisille järjestelmille, ja sen benchmark-suosituksiin voidaan tehdä mukautuksia useilla eri tavoilla esimerkiksi paikallisen ryhmäkäytäntöeditorin, ryhmäkäytäntöjen hallintakonsolin ja Windows Server (GPMC) ja Microsoft Local Group Policy Objet -työkalun (LGPO) kautta (CIS Microsoft Windows 11 Stand-alone Benchmark 2023, 23.).

2.2 GPO:n lajittelu ja järjestys

GPO:n järjestys ja miten se vaikuttaa riippuu mihin kohtaan kyseinen GPO on sijoitettu tai linkitetty. AD:n ylimmällä tasolla olevat OU:hin linkitetyt GPO:t käsitellään ensimmäisenä ja sen jälkeen GPO:t, jotka on linkitetty sen alaiseen OU:hin ja niin edelleen. Lyhkäisyydessään tämä tarkoittaa, että GPO:t, jotka ovat linkitetty suoraan OU:hin, joka sisältää käyttäjä- ja tietokoneobjekteja käsitellään viimeisenä, joten ne ovat etusijalla. (Group Policy Order of Precedence FAQ. 2016)

Asiaa pyritään vielä avaamaan alla olevan esimerkin avulla, jossa käytetty apuna labrassa tehtyjä GPO:ja.



Kuvio 2. GPO -ympäristö

Kuvio 2:ssa (ks. Kuvio 2) näkyy Group Policy Management, jolla hallittaan GPO -käytänteitä ja miten ne toimivat missäkin osa-alueessa. Suoraan AD:n alla olevat Default Domain Policy ja Ryhmä3 GPO:t luetaan ensimmäisenä, ja ne koskevat koko AD:n aluetta. Kuitenkin, kun mennään

OU:n sisään, kuten kuviossa esimerkiksi Workstationin alle, jossa on monta erilaista GPO:ta. Kyseiset GPO:t ohittavat tärkeysjärjestyksessä AD:n omat, ja koska WS:n alla on monta GPO:ta niin linkitysjärjestyksellä pystytään määrittämään näiden järjestys, eli mitä ylempänä listassa sen tärkeämpi ja kyseisen GPO:n asetukset tulevat voimaan, vaikka alemmalla olevassa listassa tulisi samoihin käytäntöihin liittyviä säännöksiä.

2.3 Microsoft Security Baseline

Security Baseline sisältää Microsoftin, turvallisuustiimin kuratoimia, ennalta määrittämiä ja suositeltuja tietoturvakonfiguraatioita ohjelmistoille, käyttöjärjestelmille ja sovelluksille. Ne toimivat perustana tietoturvajärjestelmien suojaamiseksi ja on suunniteltu vähentämään kokonaisuudessaan hyökkäyspintaa sekä lieventämään yleisiä tietoturvauhkia. Turvallisuusperusteet ovat erityisen tärkeitä organisaatioille, jotka joutuvat noudattamaan tiettyjä turvastandardeja ja noudattamaan sääntelyvaatimuksia. Erilaisilla organisaatiolla on erilaiset tarpeet turvallisuusuhkiin vastaamiseksi. Microsoftin Security Baseline pyrkii tarjoamaan selkeän ”tiekartan” ja lähtökohdan organisaation tietoturvan vahvistamiseksi. Security baseline tarjoaa suuren määrän turva-benchmarkeja, johon administraattori voi verrata omaa ympäristöään. Security baseline avaa, jokaisen tekemänsä suosituksen taustoja, jotta adminilla/organisaatiolla on mahdollisimman selkeä käsitys tekemistään valinnoista. (Mehta. 2024).

2.4 Security Compliance Toolkit – Policy Analyzer

Security Compliance Toolkit (SCT) on kokoelma työkaluja, joilla yrityksen adminit, voivat ladata, testata, analysoida, muokata sekä tallettaa Microsoftin suosittamia tietoturvakonfiguraatioita Windowsille ja Microsoftin muihin tuotteisiin. SCT:n avulla voidaan tehokkaasti hallinnoida yrityksen Group Policy Objecteja (GPO), verrata niitä Microsoftin suosittelemaan baselineen ja jakaa niitä laajasti Active Directoryn kautta tai yksittäin local policyinä.

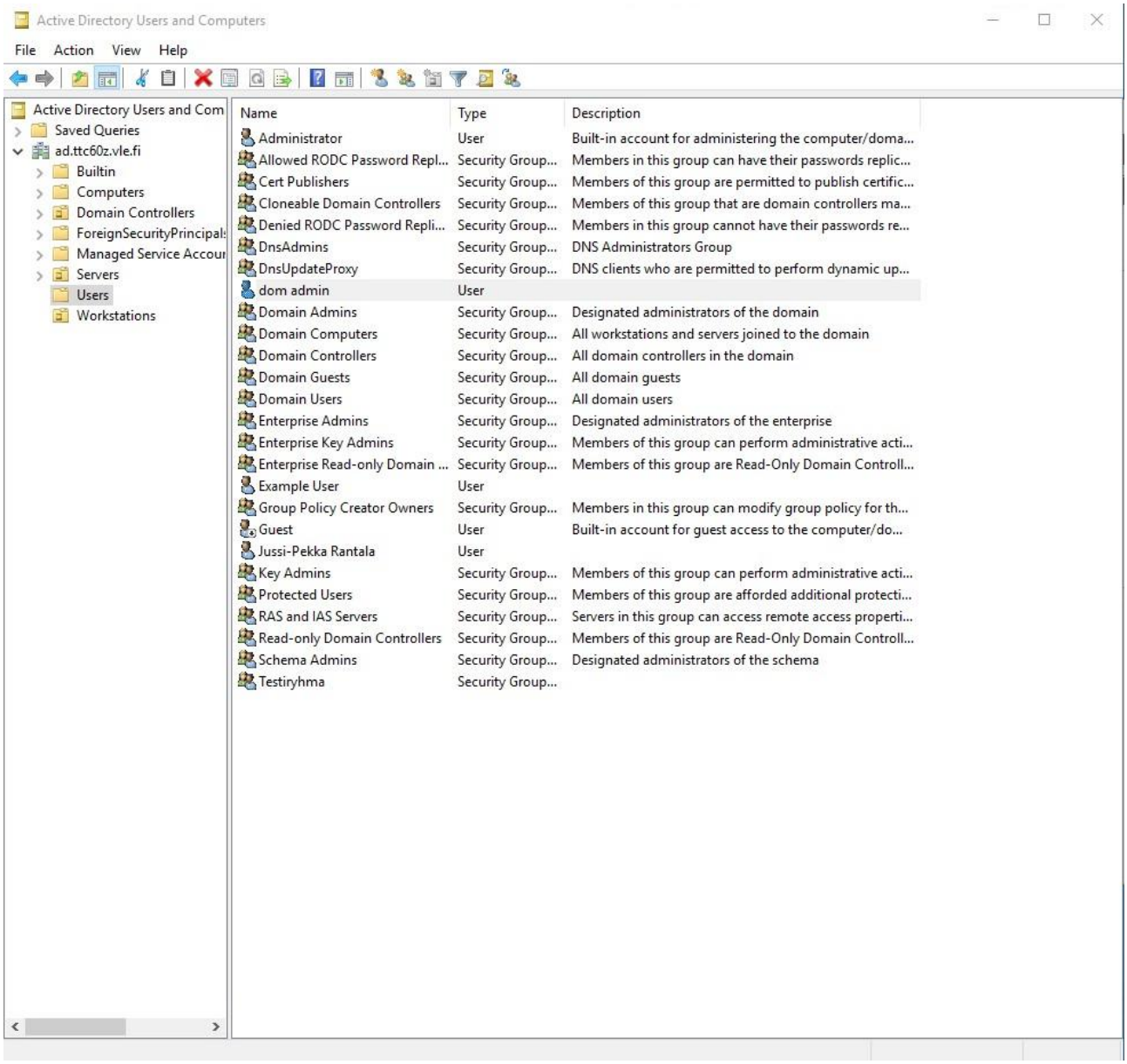
Policy Analyzer on työkalu, jolla voidaan analysoida ja vertailla GPO- sääntöjä laajana kokonaisuutena. Sen pääominaisuuksia ovat:

- korostaa tarpeettomia asetuksia tai sisäisiä ristiriitoja
- korostaa GPO-verisoiden välisiä eroja
- verrata GPO-sääntöjä tämänhetkisiin local policy ja local registry asetuksiin
- viedä GPO:t exel-taulukoihin

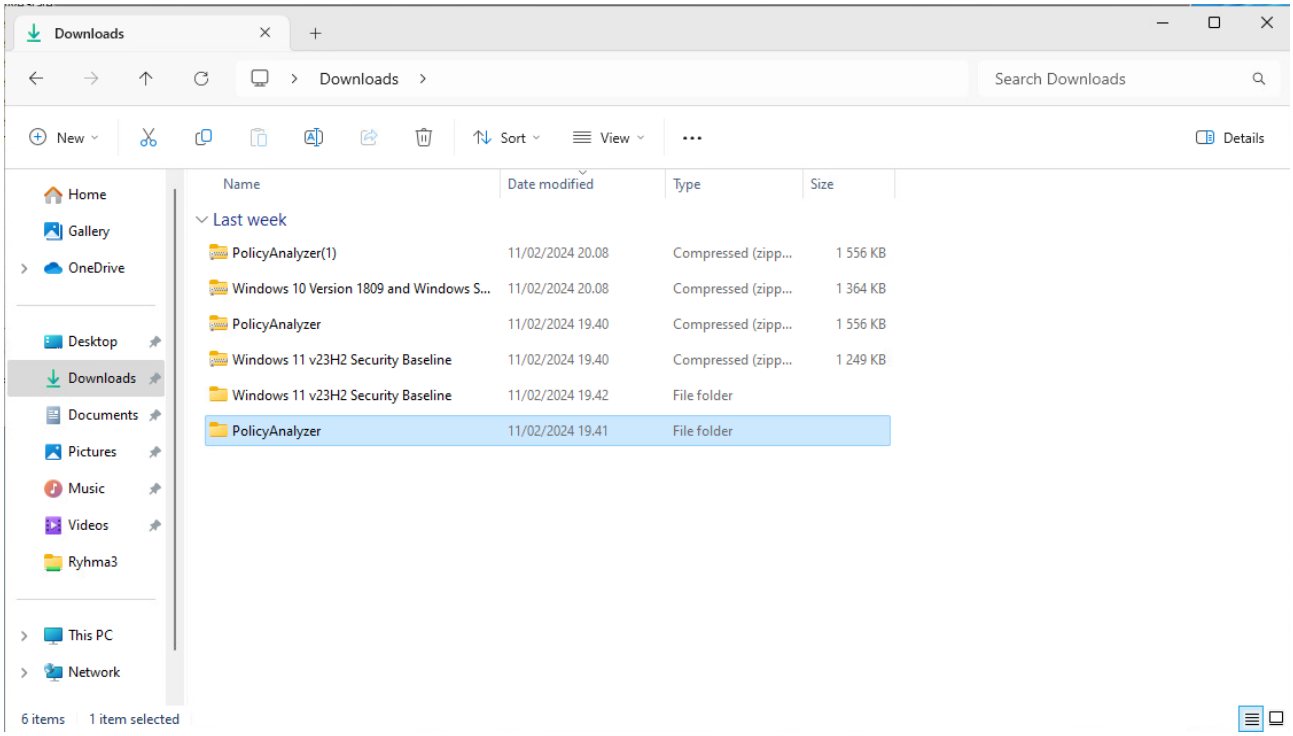
Policy analyzerin avulla useita GPO:ta voidaan käsitellä yhtenä yksikkönä. Tämän pohjalta on helppoa määrittää ovatko tietyt asetukset määritetty samalla tavalla käyttäjän ympäristössä, vai onko niissä ristiriidassa olevia asetuksia. Policy analyserin avulla baseline on helppo tallentaa ja myöhemmin verrata siihen ympäristössä tehtyjä muutoksia. (Microsoft Security Compliance Toolikit- How to use. 2023).

3 Toteutus

Aloitimme luomalla käyttäjän DC-koneella, joka kuuluu domain admins ryhmään (ks. Kuvio 3). Tällä käyttäjällä kirjauduimme myös WS01-koneelle ja latasimme Windows 11 v23H2 Security Baselinen ja Policy Analyzerin (ks. Kuvio 4).

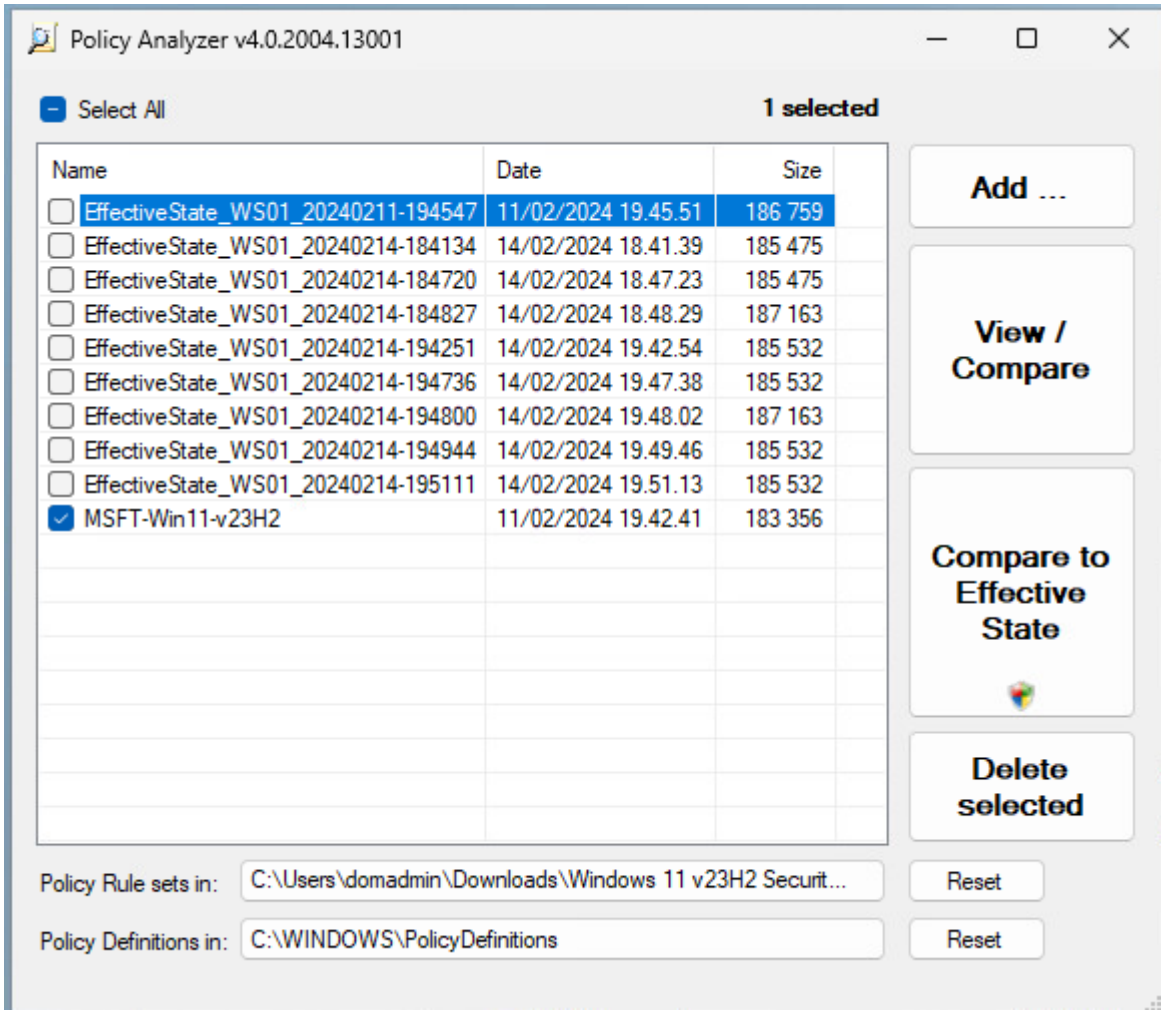


Kuvio 3. Domain admin käyttäjä



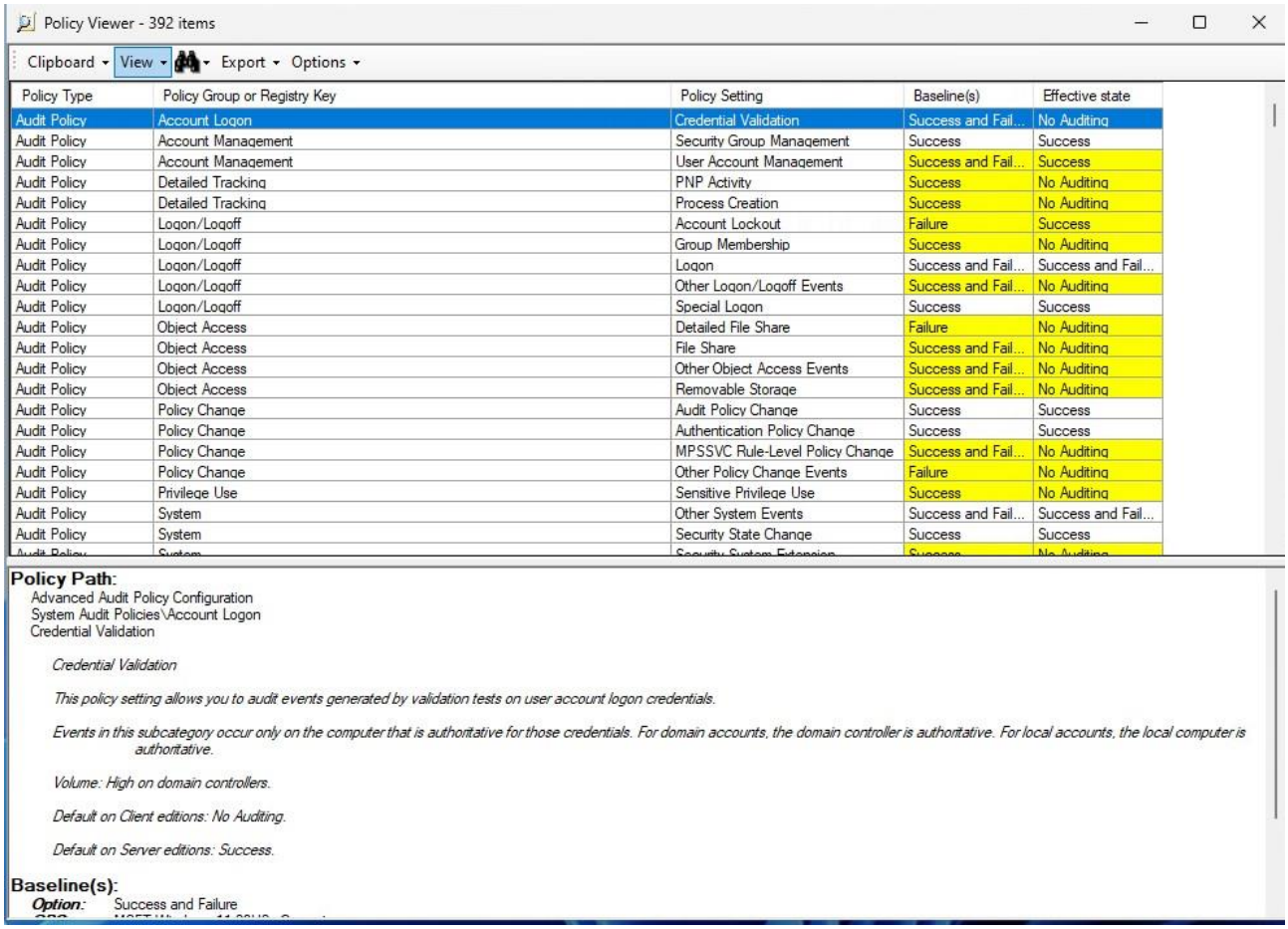
Kuvio 4. Security Baseline ja Analyzer ladattu

Kun zip-kansiot olivat purettu, avasimme Policy Analyzerin ja valitsimme Policy Rule sets in: kohtaan Security Baselinesta Documentation kansion. Kansion valinnan jälkeen, Policy Analyzeriin ilmestyi MSFT-Win11-v23H2 (ks. Kuvio 5).



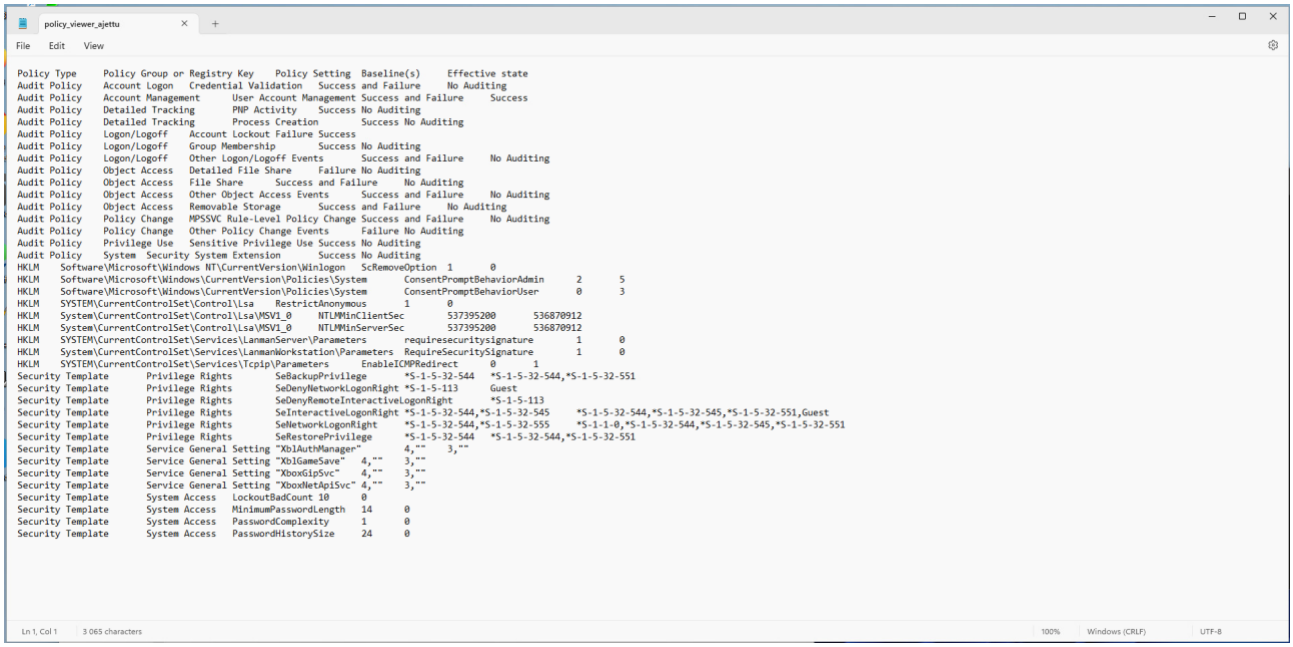
Kuvio 5. Policy Analyzerissä MSFT Policy Rules valittuna

Ajoimme Policy Analyzerin klikkaamalla Compare to Effective State, jolloin se vertasi meidän Effective Statea Baselineihin (ks. Kuvio 6). Tuloksista voidaan nähdä, että Analyzer suosittelee kovennuksien tasoa sarakkeessa Baseline ja sarakkeessa Effective state voidaan nähdä voimassa oleva kovennuksen taso.



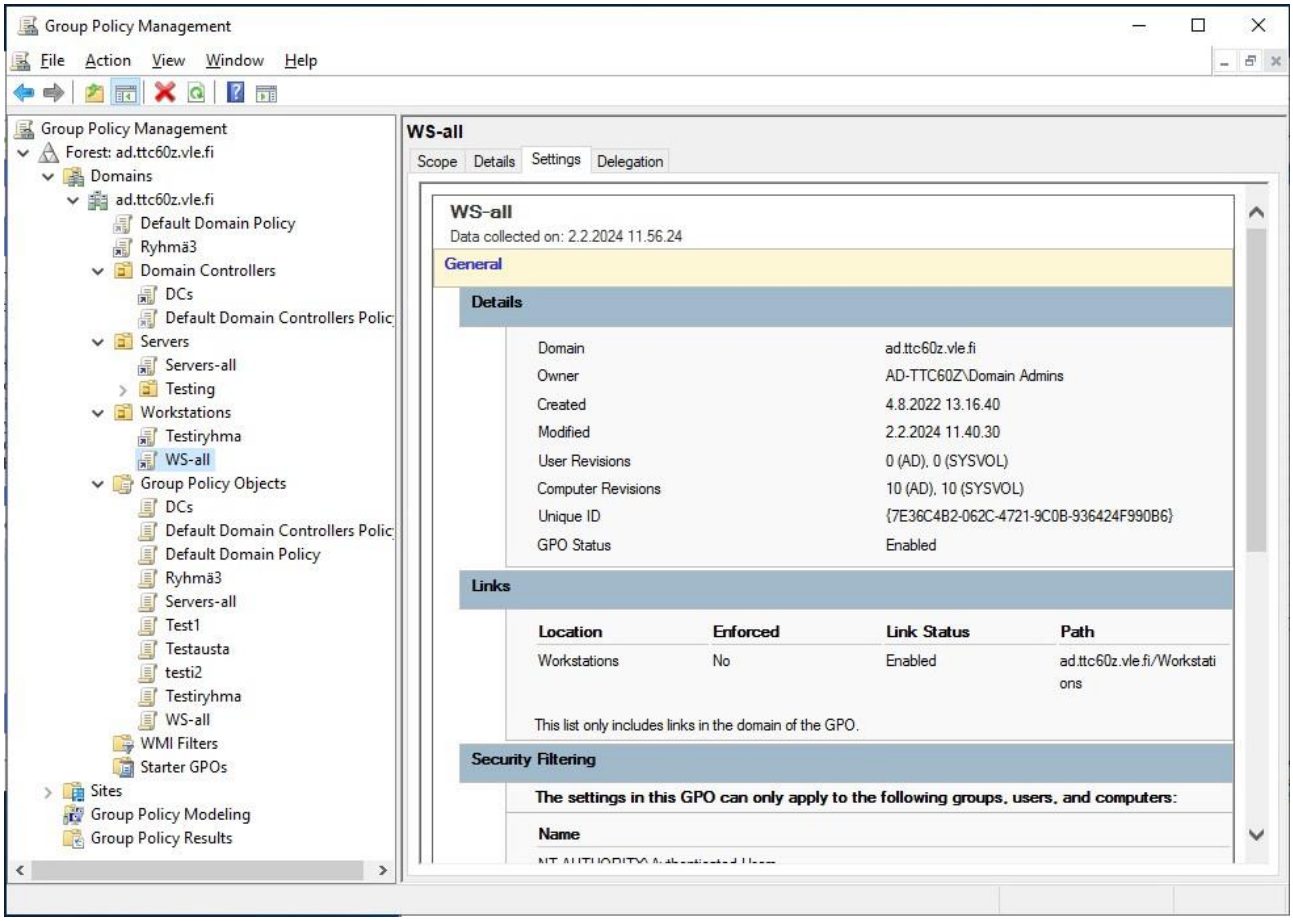
Kuvio 6. Policy Analyzer ajettu

Valitsimme Show only Conflicts ja tallensimme ne Notepadiin (ks. Kuvio 7).



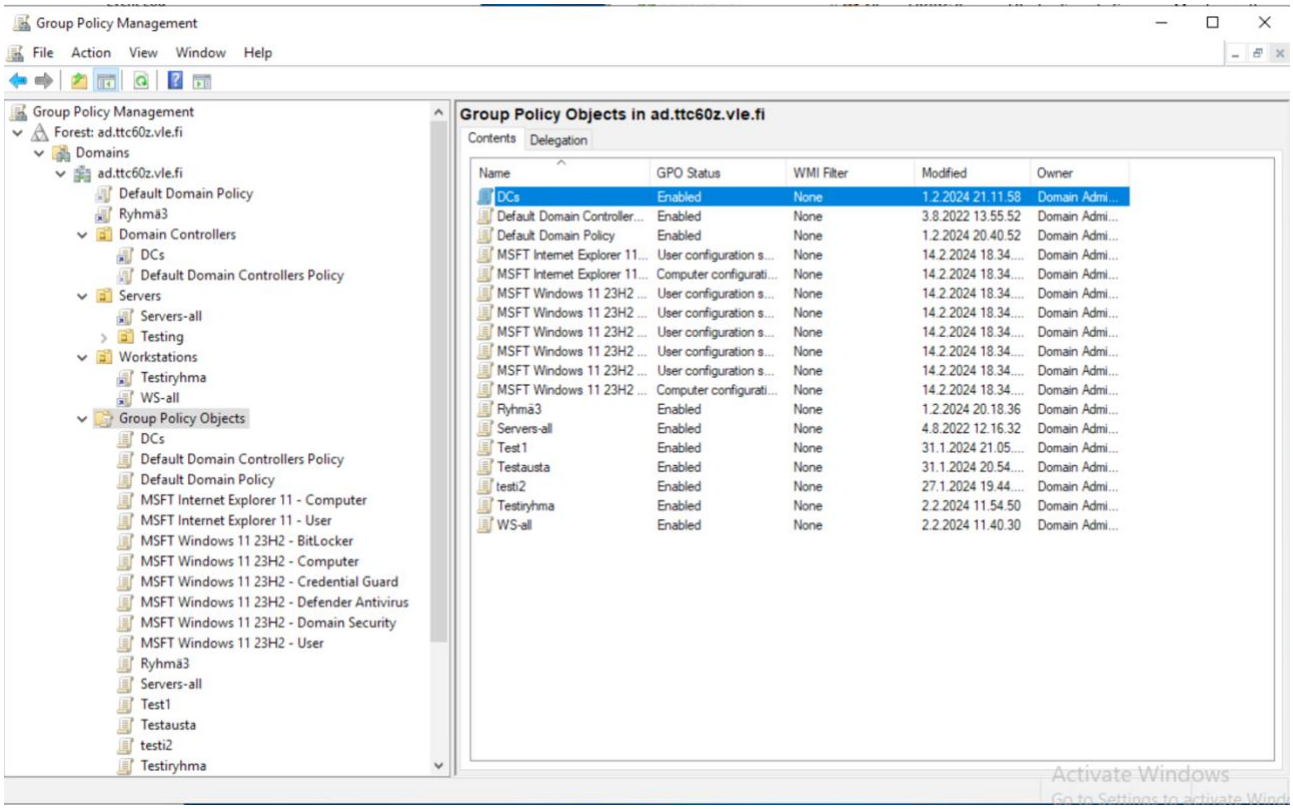
Kuvio 7. Konfliktit tallennettu

Latasimme ja asensimme myös DC-koneelle Policy Analyzerin ja saman Security Baselinen kuin WS01-koneelle. Alhaalla vielä kuva ennen asetusten tiputtamista (ks. Kuvio 8).



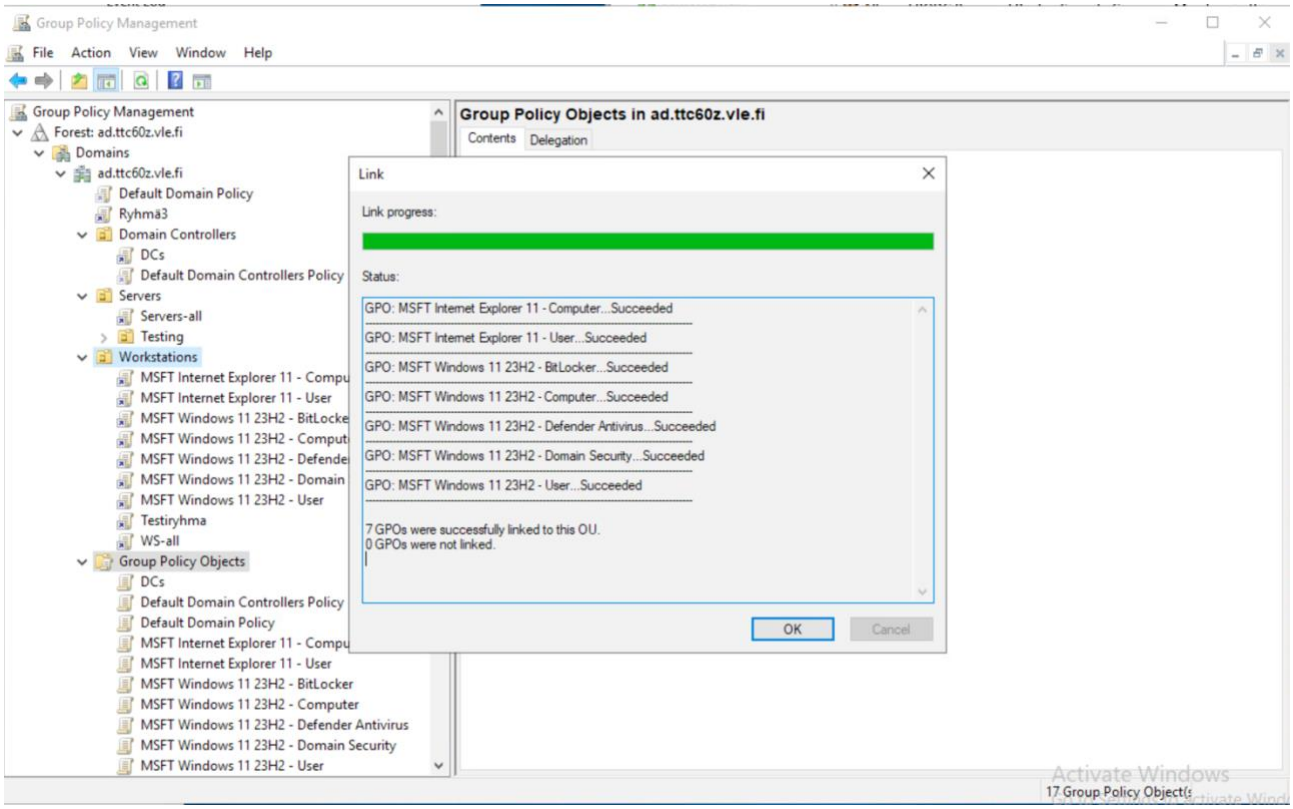
Kuvio 8. Group Policy Management ennen asetusten tiputtamista

Tämän jälkeen tuodaan kovennukset baseline:sta Active Directoryn Group policy:yn. Aloitetaan asennus etsimällä tiedosto: Baseline-ADImport ja tuodaan se komennolla run with powershell. Komento löytyy, kun tiedoston kohdalla painaa hiiren oikealla. Tuonnin jälkeen päivitetään group policy management näkymää, joka löytyy Action – refresh polusta. Group polizy management näkymän päivittämisen jälkeen uudet kovennukset näkyvät Group polizy objects kansiossa (ks. Kuvio 9).



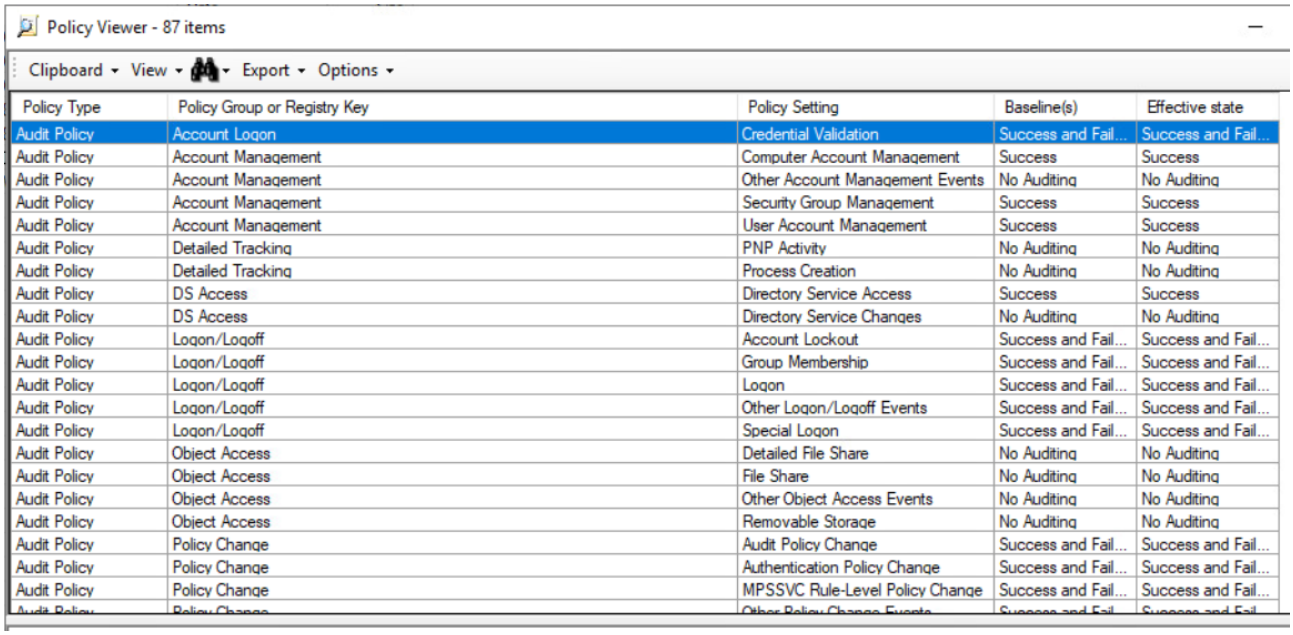
Kuvio 9. Kovennuksien tuonti

Koska tarkoitus on koventaa työasemia pitää kovennukset linkittää Workstations kansion alle. Ennen linkitystä pitää poistaa credential guard -niminen sääntö. Tämä sääntö aiheuttaa työasemien jumiutumisen joissakin olosuhteissa, jota ei haluta (ks. Kuvio 10). Jotta säännöt tulevat voimaan pitää ajaa gpupdate /force komento.



Kuvio 10. Sääntöjen linkitys

Tämän jälkeen tarkastetaan, että kovennukset ovat tulleet voimaan ja että ne ovat vaikuttaneet halutulla tavalla. Voidaan verrata tilannetta alkutilanteeseen (ks. Kuvio 6) ja tilanteeseen kovennuksen jälkeen (ks. Kuvio 11). Tuloksista voidaan nähdä, että Baseline:n kovennukset ovat tulleet onnistuneesti käyttöön työasemille.



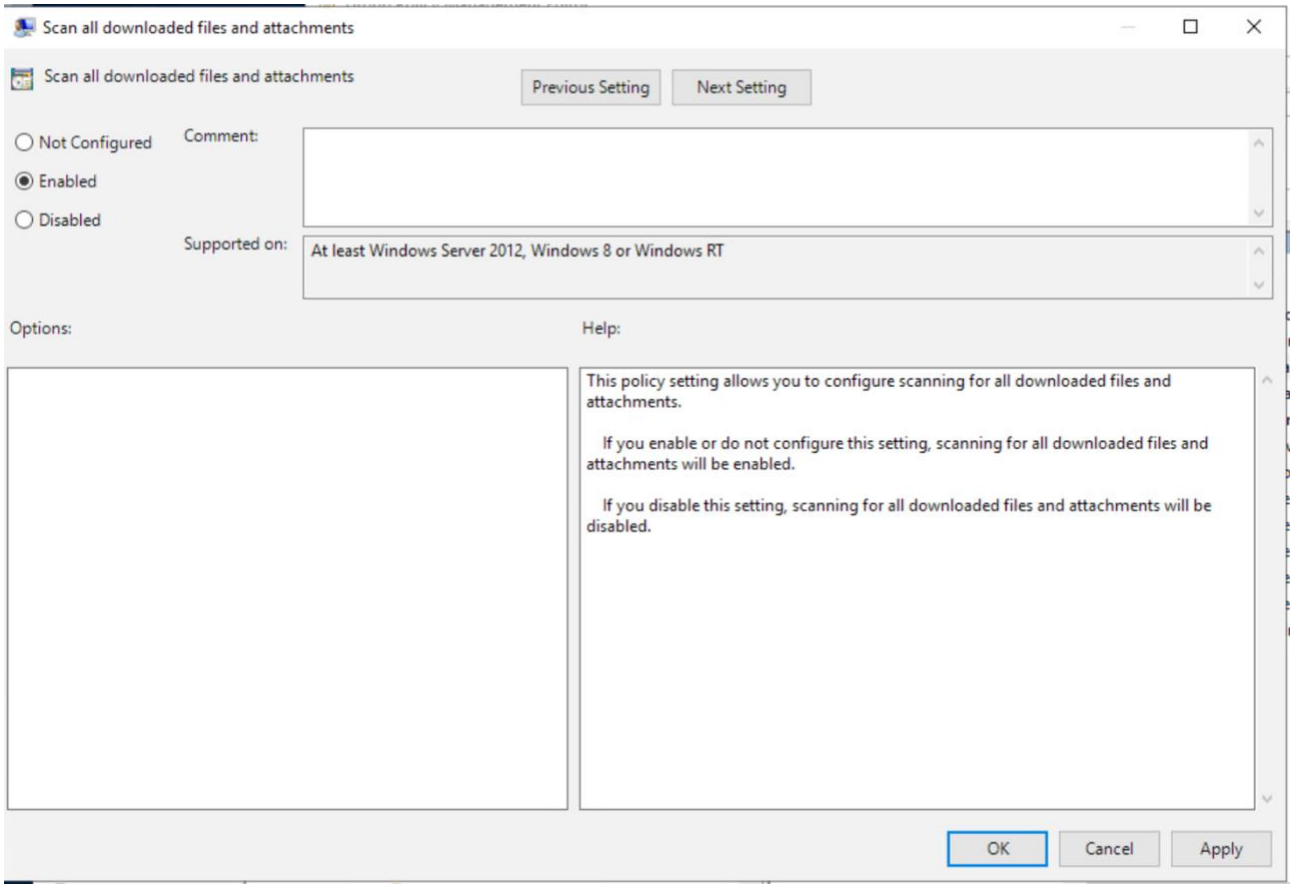
Policy Viewer - 87 items

Clipboard ▾ View ▾ Export ▾ Options ▾

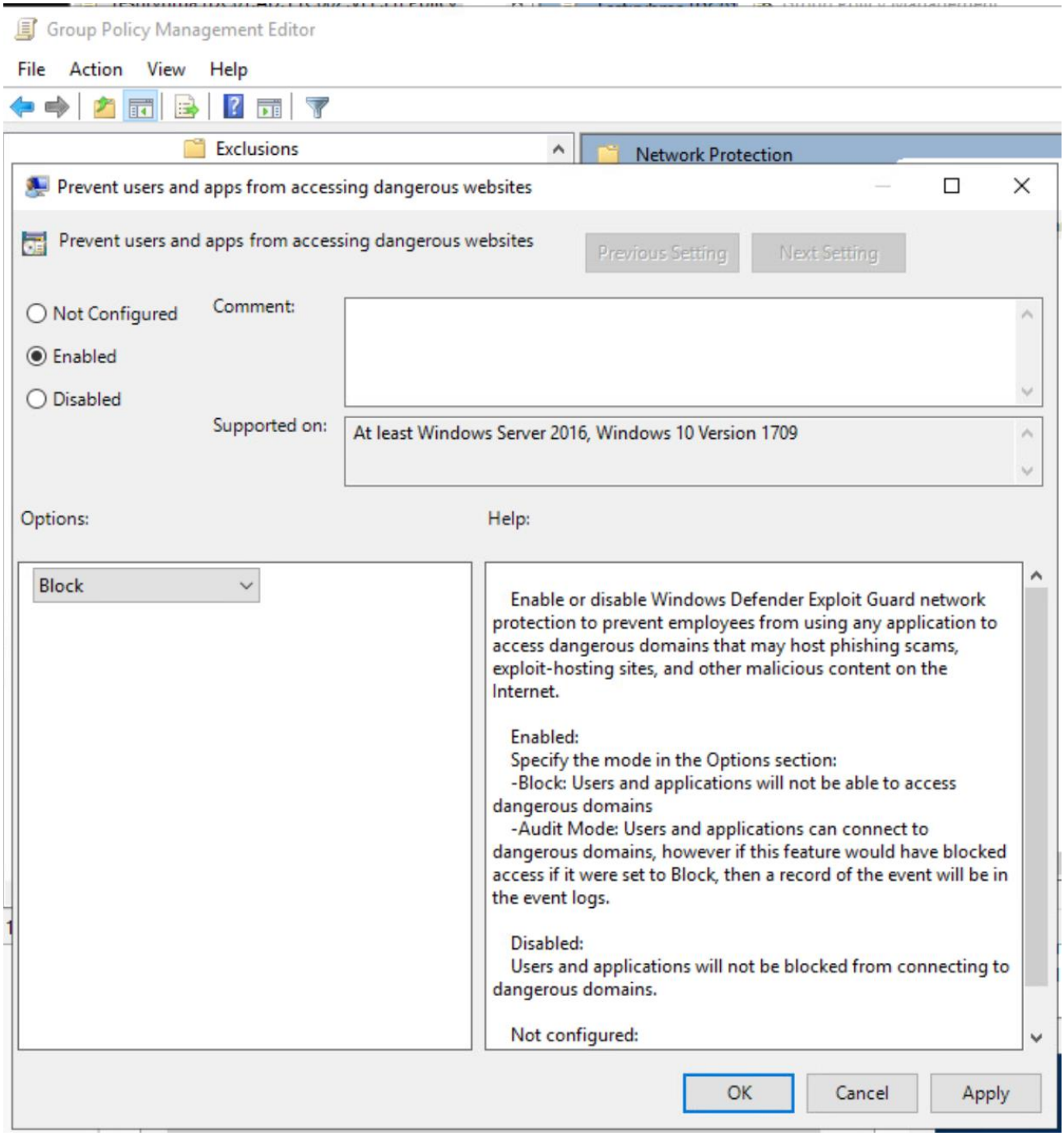
Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	No Auditing	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success	Success
Audit Policy	Detailed Tracking	PNP Activity	No Auditing	No Auditing
Audit Policy	Detailed Tracking	Process Creation	No Auditing	No Auditing
Audit Policy	DS Access	Directory Service Access	Success	Success
Audit Policy	DS Access	Directory Service Changes	No Auditing	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Group Membership	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Special Logon	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Detailed File Share	No Auditing	No Auditing
Audit Policy	Object Access	File Share	No Auditing	No Auditing
Audit Policy	Object Access	Other Object Access Events	No Auditing	No Auditing
Audit Policy	Object Access	Removable Storage	No Auditing	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Authentication Policy Change	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	Success and Fail...

Kuvio 11. Analyzer ajon tulokset

Labra:ssa piti myös valita jokin kovennusohje ja ottaa sieltä muutama kovennus käyttöön. Ryhmämme päätti valita kovennusohjeeksi CIS Microsoft Windows 11 Stand-alone Benchmark ohjeen, jonka versio on v2.0.0 – 05.17.2023. Valitsimme seuraavat kovennukset, koska ne ovat peruskovennuksia ja suojaavat kaikkia käyttäjiä: Ensure scan all downloaded files and attachments' is set to 'enabled'. Tämä sääntö tarkastaa kaikki ladatut tiedostot ja liitteet Microsoftin Defender Antivirus -ohjelmalla. Ensure 'prevent users and apps from accessing dangerous websites' is set to 'enabled: block'. Tämä sääntö suojaa käyttäjää menemästä vaaralliselle domainille, joka voi sisältää huijaussivustoja, haittaohjelmia tai haitallista sisältöä sisältävät sivustot. Asennuksien todennukset on esitetty kuvioissa 10 ja 11 (ks. Kuvio 12 ja Kuvio 13). (CIS 2023.)



Kuvio 12. Scan all downloaded files and attachments



Kuvio 13. Prevent users and apps from accessing dangerous websites

Tämän jälkeen piti taas ajaa gpudate /force komento, jotta säännöt tulevat voimaan (ks. Kuvio 14).

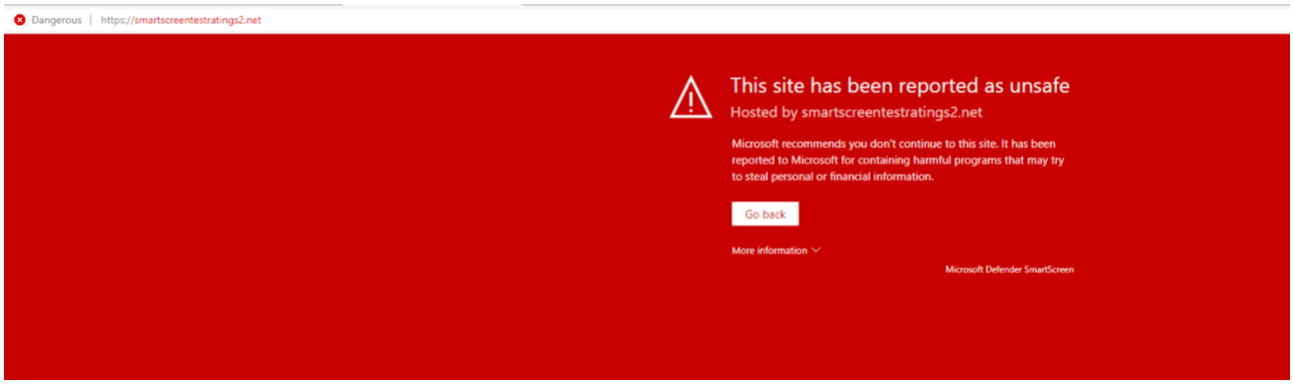
```
C:\Users\domadmin>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\domadmin>
```

Kuvio 14. Päivitys jotta säännöt tulevat voimaan

Testasimme sääntöjen toimivuutta lopuksi. Oli vaikea löytää oikea huijaussivustoa, jolla testi voidaan suorittaa, joten käytimme Microsoftin sivuilta löytyvää evaluate network protection fake malicious domain -sivustoa. Sääntö toimi hienosti (ks. Kuvio 15). (Evaluate network protection 2023.)

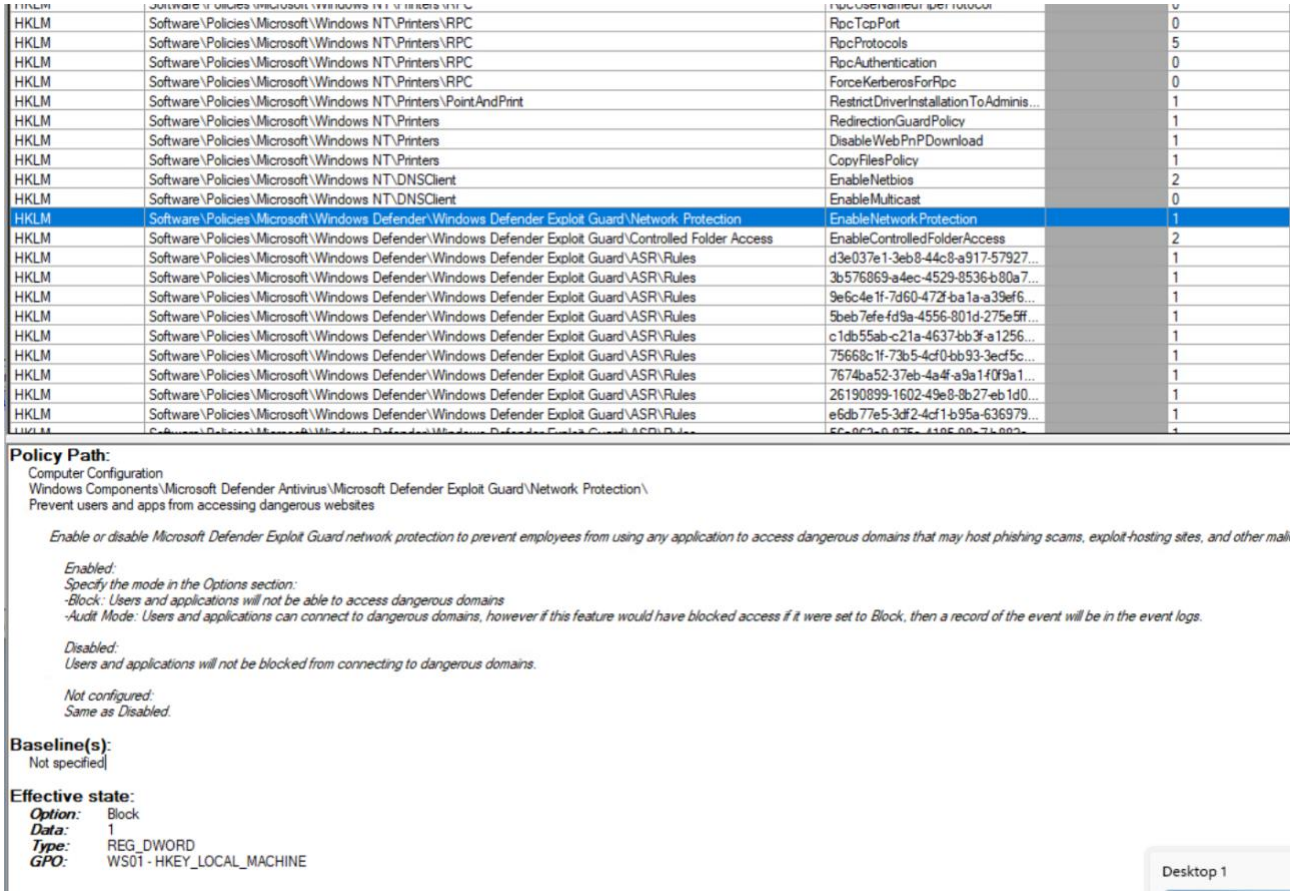


Kuvio 15. Todennus kovennuksen toimivuudesta

4 Pohdinta

Lisä kovennuksien suunnittelussa tuotti ylimääräistä vaivaa ymmärtää mihin kaikkiin kovennuksiin verrattuna CIS-ohjetta oli baseline tehnyt kovennuksen ja mitä kovennuksia kannattaisi käyttää sen jälkeen, kun baseline:n kautta saatavat kovennukset on asetettu. Tulimme siihen tulokseen,

että kun tarkastelemme Analyzerin tuloksia, voidaan todeta, että jos baseline on tilassa not specified, ei baselinen kovennuksiin ole kuulunut ko. kovennus. Ja kun olemme tehneet kovennuksen, näkyy haluttu lopputulema effective state kohdassa (ks. Kuvio 16).



HKLM	Software\Policies\Microsoft\Windows NT\Printers\RPC	RpcTcpPort	0
HKLM	Software\Policies\Microsoft\Windows NT\Printers\RPC	RpcProtocols	5
HKLM	Software\Policies\Microsoft\Windows NT\Printers\RPC	RpcAuthentication	0
HKLM	Software\Policies\Microsoft\Windows NT\Printers\RPC	ForceKerberosForRpc	0
HKLM	Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint	RestrictDriverInstallationToAdminis...	1
HKLM	Software\Policies\Microsoft\Windows NT\Printers	RedirectionGuardPolicy	1
HKLM	Software\Policies\Microsoft\Windows NT\Printers	DisableWebPnPDownload	1
HKLM	Software\Policies\Microsoft\Windows NT\Printers	CopyFilesPolicy	1
HKLM	Software\Policies\Microsoft\Windows NT\DNSClient	EnableNetbios	2
HKLM	Software\Policies\Microsoft\Windows NT\DNSClient	EnableMulticast	0
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection	EnableNetworkProtection	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access	EnableControlledFolderAccess	2
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	d3e037e1-3eb8-44c8-a917-57927...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	3b576869-a4ec-4529-8536-b80a7...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	9e6c4e1f-7d60-472f-ba1a-a39ef6...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	5beb7efe-fd9a-4556-801d-275e5ff...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	c1db55ab-c21a-4637-bb3f-a1256...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	75668c1f-73b5-4cf0-bb93-3ecf5c...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	7674ba52-37eb-4a4f-a9a1-f0f9a1...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	26190899-1602-49e8-8b27-eb1d0...	1
HKLM	Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules	e6db77e5-3df2-4cf1-b95a-636979...	1

Kuvio 16. Pohdintaa kovennuksista

Lähteet

CIS. 2023. Microsoft Windows 11 Stand-alone Benchmark. CIS Center of Internet Security.

Evaluate network protection. 2023. Microsoft. Viitattu 17.2.2024. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluate-network-protection?view=o365-worldwide

Group Policy Objects. 2018. Viitattu 18.2.2024. https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects

Mehta Janki. 2024. Windows Security: Detailed Guide to Understand Security Baselines. 2024. SignMyCode. Viitattu 16.2.2024. https://signmycode.com/blog/windows-security-detailed-guide-to-understand-security-baselines

Microsoft Security Compliance Toolkit- How to use 31.10.2023. Microsoft. Viitattu 16.2.2024. https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10