Workplace Ninja
User Group Finland

Windows työasemien tietoturva ja kovennukset 31.10.2025

Tietoturvasta ei voi puhua liikaa, varsinkaan nyt!

Katso Sami Laihon esitys

Sisältö

- Käyttäjien tekemät virheet
- Ylläpidon tekemät virheet
- Admin väliaikaisesti - työkalut
- Security Baseline & Firewall vinkit
- The End

Käyttäjien virheet (Zero Trust)

www.wpninjas.fi

Kotona

- Yrityksen fyysinen palomuuri ei ole käytössä
- Työt tehdään ilman VPN yhteyttä
- Kuitu liittymän kaapeli suoraan koneeseen
- Lapset konffaa reitittimen pelejä varten (siltaa)

Operaattori

- 4G/5G yhteys puhelimesta ilman NAT
- Reitittimet vanhenee nopeasti

Julkisissa paikoissa

- WIFI ilman salasanaa
- Julkinen WIFI jaetulla salasanalla myös riski

Ylläpidon virheet

- Tietoturvapäivityksiä viivästytetään liikaa
- Käyttäjät ajaa koneitaan admin oikeuksilla

Ratkaisuja väliaikaiseen adminiin

LAPS

Salasana Intune konsolissa

PLENTICS

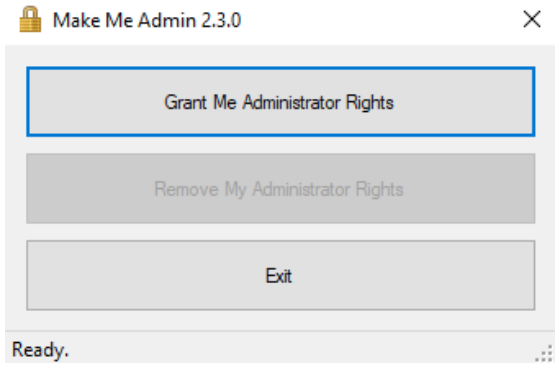
- Netoxin kumppani
- Myöntää 60min admin oikeudet Company Portaalin kautta

Make Me Admin

Asennetaan työasemalle

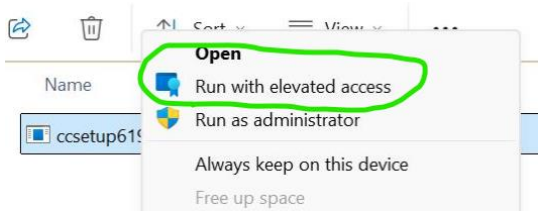
Open Source / Github

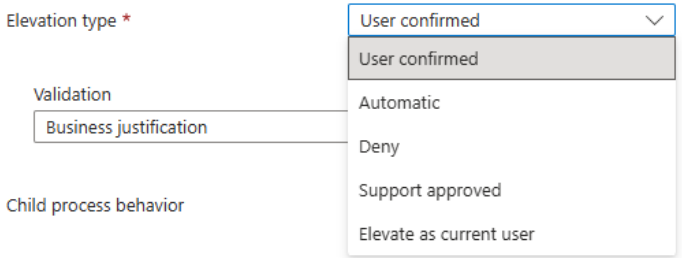
10 minuuttia

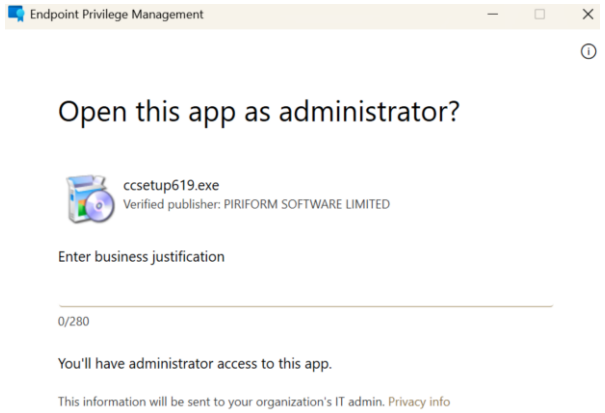


Intune Endpoint Privilege Management

www.wpninjas.fi







- **Vain sovellus asennuksiin**
- **Raportit ja audit**

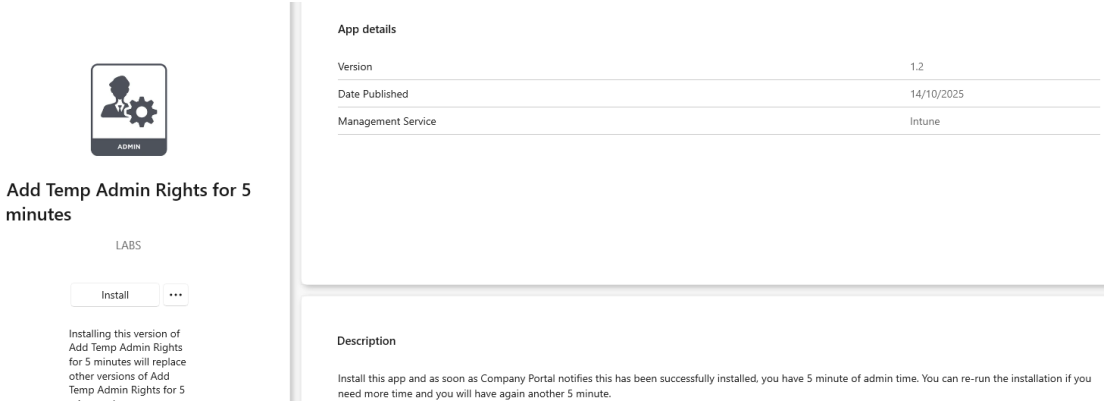
Uutta – käyttäjäprofiilissä evaluointi virtuaalisen sijaan.

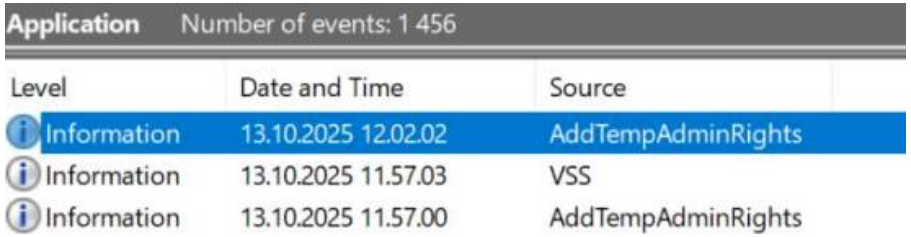
Add Temp Admin Rights

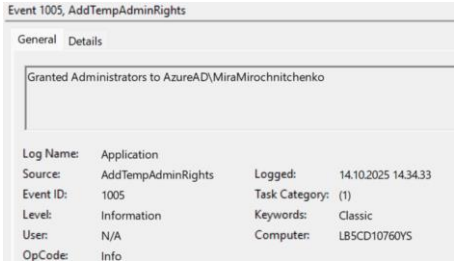
www.wpninjas.fi

(Chat GTP + Pavel + Github Copilot)

- Powershell pohjainen
- Käyttää Detection Methodia päälle ja pois
- Lokitus Event Vieweriin
- Piilotettu, ei pääse helposti väliin
- Ei erillistä pop-up promptia, vain CP
- Poistaa myös muulla tavalla lisätyt adminit, mutta vaatii bootin







MS Security Baseline vs. CIS

Microsoft

- Helppo ottaa käyttöön
- Microsoftin ylläpitämä, seuraa Windows 11 build julkaisuja

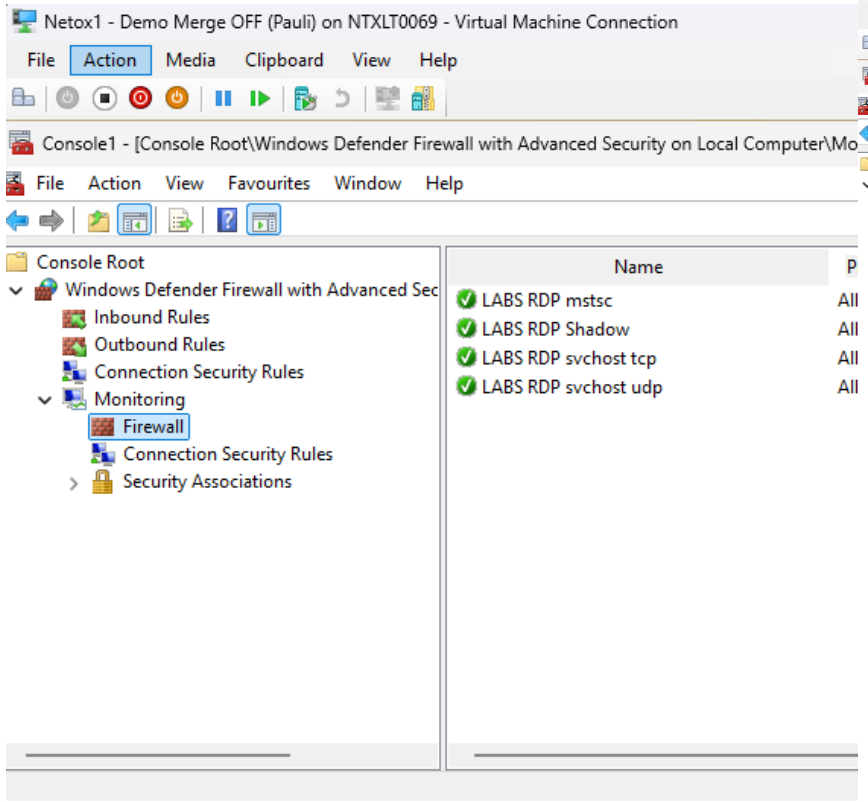
Voivat toimia myös yhdessä

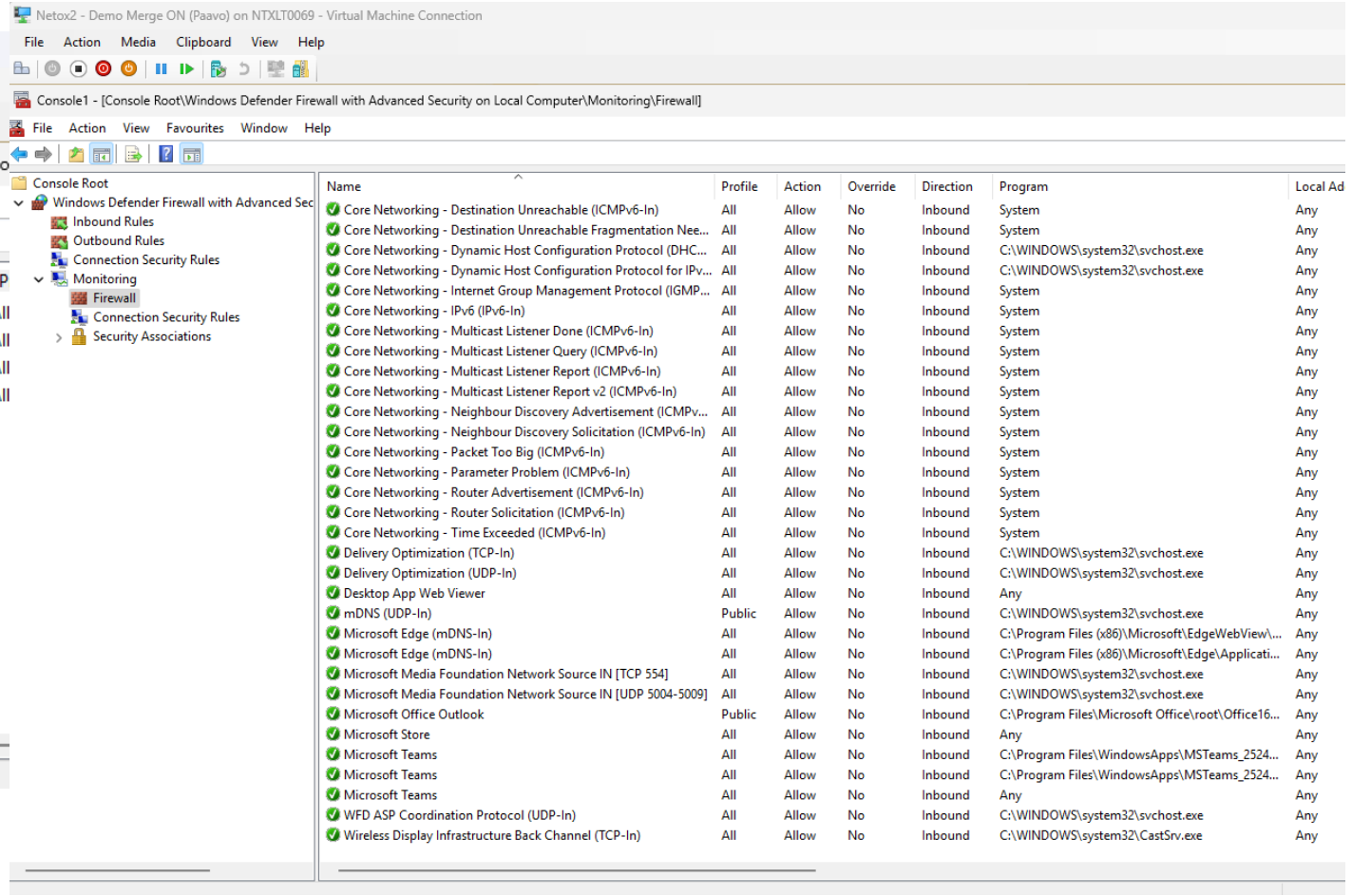
CIS

- Tiukempi
- Eri tasoja (TIER)
- Yksityiskohtaisempi, tarkempi
- Takana on yhteisö (Center of Internet Security)
- Päivitykset ja oma versiointi (ei ilmesty yhteen Windows 11 building kanssa)
- Muitakin tuotteita, (Apple, AWS)

Vinkki 1

- Windows Firewall Local Policy Merge Off/Disabled = Paikalliset säännöt eivät ole enää voimassa





Merge or not Merge

Merge On

- Vähemmän tietoturvaa
- Sovellukset tekee omia sääntöjä asennuksen yhteydessä

Merge OFF

FW rule kontrolli sinulla

Tietoturvallisempi

Vinkki 2

- Firewall sääntöihin Protokolla on määriteltävä!

- (help-teksti virheellinen)

Kiitos

Workplace Ninja
User Group Finland