# The road to Defender Application Control enforcement

- Kim Oppalfens
- EIEIO @ OSCC
- Twitter @TheWMIGuy
- MVP (for now)

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

# The road to Defender Application Control enforcement

- Tom Degreef
- XYZO @ OSCC
- Twitter @Tomdegreef
- MVP (for now)

Official sponsors

PATCH MY PC

RECAST SOFTWARE

NORDIC — VIRTUAL SUMMIT —

# The road

"Sell" the project

Pick your targets

Define your strategy

Build the base audit policy

Centralize your event logging

Pitfalls

T

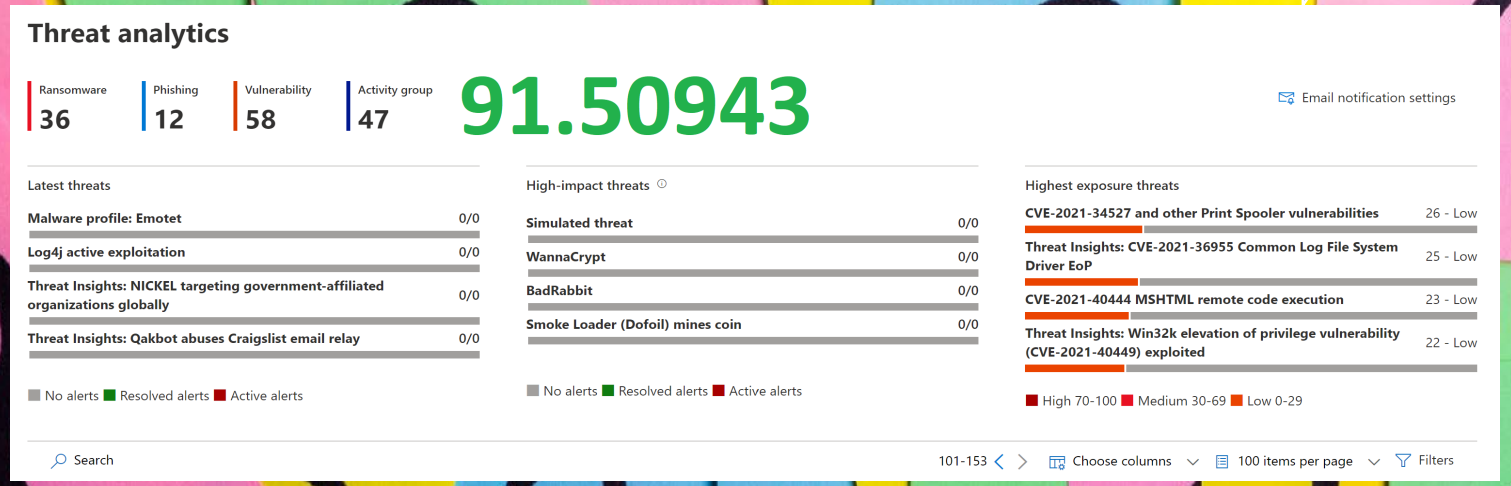
# Why? / Sell the project

The principle of least privilege is a guideline that states that users should have access to the resources they need to perform their tasks, but not more.

Windows code execution, in allowing any code to run, doesn't appear to follow that practice.

Proactive

Reactive



# Further Proof / Sell the project

**Actual Vulnerabilities**

- PrintNightmare (307.000)
- HiveNightmare/SeriousSAM(67.700)
- Windows Installer Privesc (20.700)
- Razer Mouse Driver install (944)
- Solarwinds supply chain attack? (72.400)
  - Powershell
  - C:\windows\idmu\common\ypprop.dll

# Applocker as an alternative / Sell the project


- DLL / Scripts?
  - Offensive security tooling exists entirely in PowerShell
    - Invoke-Mimikatz
  - Developing offensive tooling that results in .exe is just as usuable as tooling that results in a .dll
- No Managed Installer
- No ISG

T

# Targets

Information Workers

ICT Department

Servers

# Define your strategy – High Level

NORDIC
– VIRTUAL SUMMIT –

Strict Allow policy

Applocker like path rules Allow policy

- Automatically deny user writable folders

Application Control assistants

- Managed installers
- Intelligent security graph

Block Policy

T

# Define your strategy - Lowlevel

NORDIC
– VIRTUAL SUMMIT –

Security Catalogs

Intelligent security graph

Managed installer

Policy

- FilePublisher & Hash
- Path Rules

K

# Build the base audit policy

- Windows Default Audit policy
- Corporate Codesigning certificate / Codesigning certificate infra

```
$rules = New-CIPolicyRule -Level PcaCertificate -DriverFilePath C:\temp\signedfile.exe
```

- .net Native Images

```
$rules = New-CIPolicyRule -FilePathRule C:\Windows\assembly\NativeImages_v4.0.30319_32\*
$rules += New-CIPolicyRule -FilePathRule C:\Windows\assembly\NativeImages_v4.0.30319_64\*
New-CIPolicy -FilePath policy.xml -Rules $rules
```

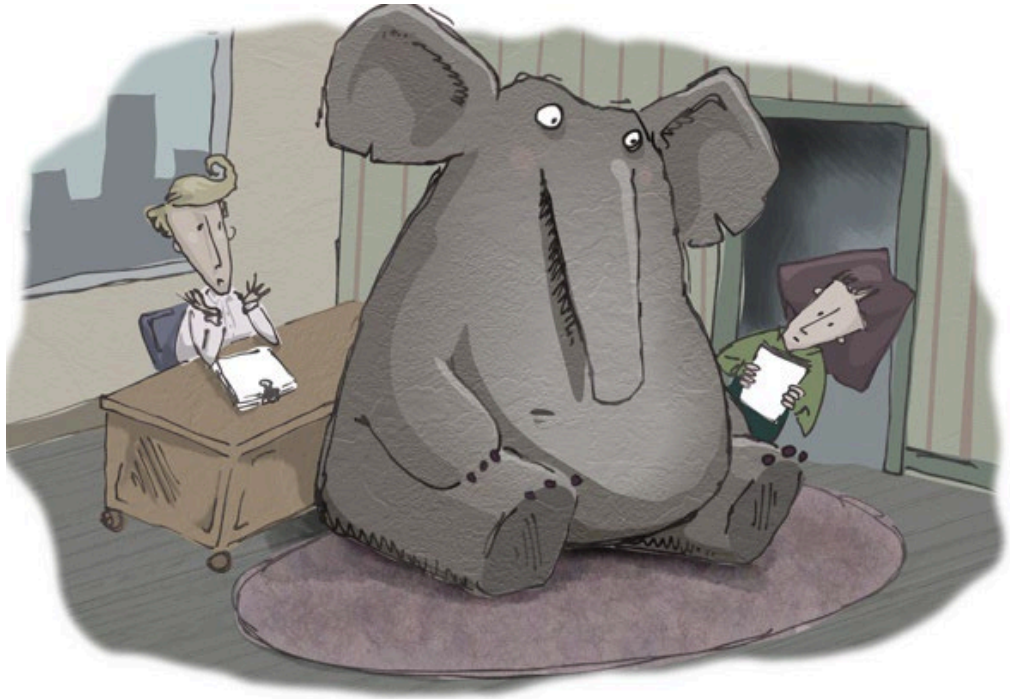
- Managed installers
  - `set-ruleoption -Option 13 -FilePath Policy.xml`
- Recommended block rules
  - Microsoft recommended block rules (Windows) - Windows security | Microsoft Docs
  - Microsoft recommended driver block rules (Windows) - Windows security | Microsoft Docs

# The unsurmountable challenge of code signing

```
//Create your own cert without a PKI
New-SelfSignedCertificate -Type CodeSigningCert `
-Subject 'Application control signing cert'


//Sign a file using that cert
$cert = gci Cert:\LocalMachine\My -CodeSigningCert

 Set-AuthenticodeSignature `
-Certificate $cert `
-TimestampServer http://timestamp.digicert.com -HashAlgorithm
sha256 `
-FilePath "file"
```

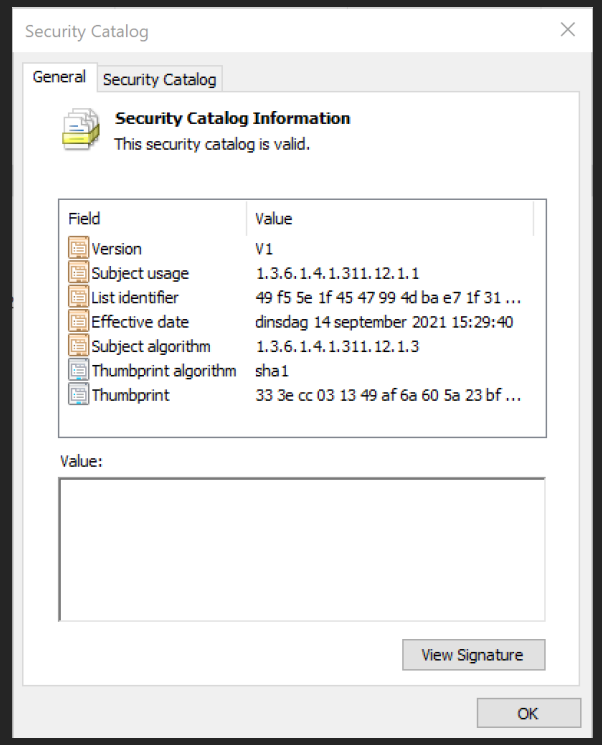


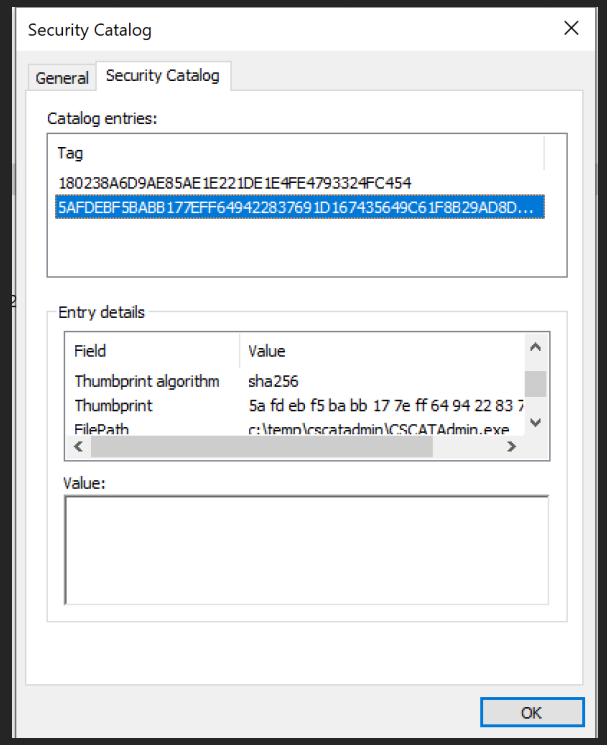
K

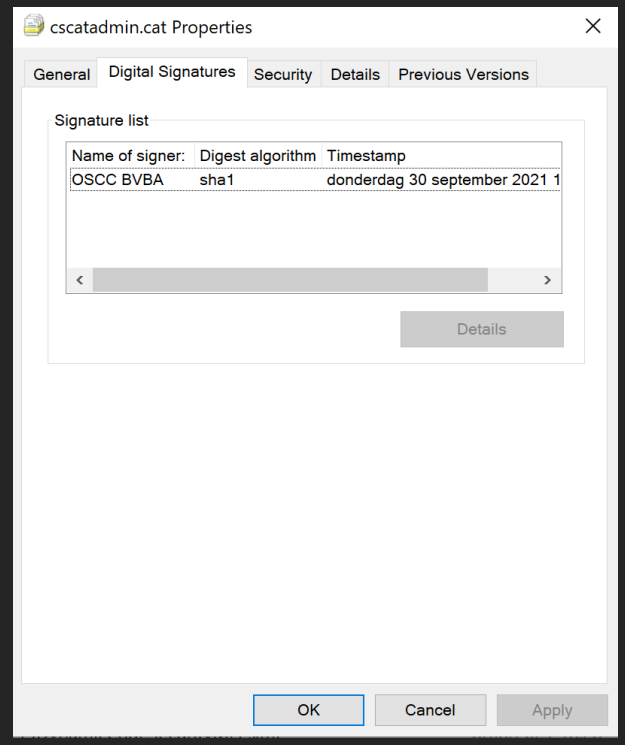
# Security catalogs & the backlog

NORDIC
– VIRTUAL SUMMIT –

- .cat files, Introduced 2 decades ago with Windows 2000
- Enforcement started in Windows XP
  - Driver signing is Kernel Mode Code Integrity
- Windows Defender Application Control adds User mode Code Integrity



# Centralized reporting

- Microsoft Defender for Endpoint
  - Plan 1 included in Microsoft 365 E3
  - Plan 2 included in Microsoft 365 E5
  - The Applocker logging Caveats
- Azure Log Analytics – MSEndpointMgr style
- Windows Event Forwarding
  - CodeIntegrity 3076, 3077 & 3089

# Pitfalls

NORDIC
– VIRTUAL SUMMIT –

- Intune accidental reboots!
  - Use the AppControl CSP custom OMA-URI
- Software during OSD
- Auto-updating software
- ISG & Invalidate EAs on reboot
- Applocker Logging & Managed installer

T

# A big thanks to our sponsors

NORDIC
– VIRTUAL SUMMIT –

PATCH MY PC

RECAST SOFTWARE

# Thank you!

**Please remember to fill out the evals!**

https://stream.nordicvirtualsummit.com/feedback