www.wpninjas.eu
#WPNinjaS

Workplace Ninja User Group Edition 2406

Entdecken Sie die Möglichkeiten von

Windows **D**efender **A**pplication **C**ontrol (WDAC)

About Fabrizio Gobeli

Focus

Endpoint Security

Work

baseVISION

Senior Endpoint Security Consultant

From

Hobbies

My Blog

www.gobisweb.ch

Contact

https://gobisweb.ch/about

- Key takeaways:
- **Top 10 Erkenntnisse:** Was Sie über WDAC wissen sollten bevor Sie ein Deployment starten
- **Erfahrungen aus der Praxis:** Aus aktuellen 5 WDAC Projekten

Thank you Sponsors

www.wpninjas.eu
#WPNinjaS

Microsoft

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

EPIC FUSION
BRING IT ALL TOGETHER

01 – Die Grundlagen

- Application Control

  - Schutz vor aktuellen Bedrohungen, wenn der Angriffsvektor ausführbarer Code ist
  - Verhinderung, dass nicht genehmigte/schädliche Programme ausgeführt werden, einschliesslich
    - EXE
    - DLL
    - Skripten
    - Installationsprogrammen

  - Eine der wirksamsten Strategien, um die Sicherheit von Systemen zu gewährleisten.

01 – Die Grundlagen

- Strategien zur Eindämmung von Cybersicherheitsvorfällen (Cyber Security Incidents)

  - Effectiveness Rating: Limited, Very Good, Excellent, Essential

  1. Patch operating systems
  2. Patch applications
  3. Restrict administrative privileges
  4. Multi-factor authentication
  5. Regular backups (Immutable)
  6. Application Control
  7. Configure Microsoft Office macro settings
  8. Application hardening

  Quelle: Australien Cyber Security Centre - Strategies to Mitigate Cyber Security Incidents | Cyber.gov.au

01 – Die Grundlagen

MDE Threat analytics
April/Mai 2024
Threats: 20
WDAC Block: 14 (70%)

Threat Analytics	Attack chain/Analyst report	Published	Would have been blocked by WDAC
Activity Profile: Recent OSINT trends in malvertising	Malvertising campaigns have showcased a diverse range of malware payloads, including MetaStealer, Danabot, FakeBat, and PikaBot, each serving distinct malicious purposes such as data theft and system compromise. MSIX installers packaged with heavily obfuscated PowerShell code	01.04.2024	YES
Vulnerability Profile: CVE-2023-48788 - in Fortinet FortiClient EMS	Observed threat actors exploiting this vulnerability in FortiClient SQL Servers. In one case, this exploitation led to deployment of INC ransomware.In the observed case, after successful exploitation, an unknown actor managed to download and install a renamed instanced of the Atera remote monitoring and management (RMM) tool. (setup.msi)	01.04.2024	YES
Vulnerability Profile: CVE-2024-3094 - XZ Utility vulnerability	vulnerability caused by a supply chain compromise in which a threat actor managed to install a backdoor in the open-source Linux utility xz.	02.04.2024	NO, no Support for Linux
Activity Profile: Remote code execution exploit chain in OpenVPN	A threat actor could exploit these vulnerabilities to launch arbitrary code with SYSTEM privileges in kernel mode on a target system running a vulnerable version of OpenVPN.	09.04.2024	YES
Vulnerability Profile: CVE-2024-3400 - command injection vulnerability	This vulnerability stems from two weaknesses in the PAN-OS code with overlapping scopes. PAN-OS is a Linux-based operating system running on Palo Alto Networks firewalls.	12.04.2024	NO, no Support for Linux
Activity Profile: Grandoreiro banking trojan campaign expands target regions	Microsoft tracks the recently observed campaigns under a different cluster, which involves delivery of .zip files followed by .exe files	25.04.2024	YES
Tool Profile: GooseEgg	GooseEgg is a bespoke tool that exploits a vulnerability in the Windows Print Spooler service where a modified JavaScript constraints file can be executed with elevated permissions. GooseEgg is typically deployed with a batch script, which we have observed using the name execute.bat and doit.bat.	25.04.2024	YES
Activity Profile: Seashell Blizzard exploiting vulnerabilities to install Atera Agent for post-compromise activities	Atera installation via ScreenConnect Remote Support & Access Software (setup.msi)	06.05.2024	YES
Tool Profile: PlugX	DLL side-loading	07.05.2024	YES
Technique Profile: Exchange mailbox exfiltration	SMTP Forwarding, Email rules, Power Automate, Mail Flow Rules	08.05.2024	NO, can't be stopped by application control technologies Not applicable.
Activity Profile: Recent OSINT trends in Linux malware	Researchers identified an emerging Linux malware campaign targeting misconfigured servers running web-facing services	10.05.2024	NO, no Support for Linux
Activity Profile: Threat actors misusing Quick Assist in social engineering attacks leading to ransomware	Once the user complies and allows access, the threat actor runs a scripted cURL command to download a series of batch files or ZIP files used to deliver malicious payloads.	13.05.2024	YES
Vulnerability Profile: CVE-2024-30051 - Desktop Window Manager EoP vulnerability	A malicious application can pass a crafted value that causes dwm.exe to run arbitrary shellcode with SYSTEM privileges, which can in turn cause dwm.exe to load an arbitrary dynamic link library (DLL).	14.05.2024	YES
Activity Profile: Star Blizzard spearphishing campaign targets US think tanks	Adversary-in-the-middle (AiTM) phishing	14.05.2024	NO, can't be stopped by application control technologies Not applicable.
Vulnerability Profile: CVE-2024-30040	Downloads a malicious Java archive (JAR), and runs that file using the Java Runtime Environment (JRE) installed on the targeted system with the permissions of the user currently signed in.	14.05.2024	YES
Technique Profile: Golden SAML	Allow a threat actor to impersonate specific users to (1) obtain elevated or any other privileges; (2) attain persistence by indefinitely creating an arbitrary number of valid authentication tokens; and (3) evade defenses by using or impersonating legitimate authentication infrastructure.	16.05.2024	NO, can't be stopped by application control technologies Not applicable.
Activity Profile: Seashell Blizzard stealing interactive logon credentials using HighCount	HighCount typically manifests as a Windows executable, and its malicious functionality is enabled by unique configurations within the Windows Registry.	20.05.2024	YES
Technique Profile: Malicious use of PowerShell	Threat actors run PowerShell on compromised hosts to conduct many malicious activities, such as taking advantage of living-off-the-land binaries (LOLBins) for collections and persistence, file transfer activities, and for deployment of additional malicious code or files.	20.05.2024	YES
Vulnerability Profile: CVE-2023-2071	An unauthenticated threat actor can upload a malicious dynamic link library (DLL) to a vulnerable device, which allows the actor to bypass security checks and run any code in the functions exported from the DLL.	20.05.2024	YES
Vulnerability Profile: CVE-2024-4040	By exploiting CVE-2024-4040, an unauthenticated threat actor can achieve remote code execution (RCE) with administrative privileges on a vulnerable system.	30.05.2024	YES

Quelle: Microsoft Defender for Endpoint Threat Analytics - https://security.microsoft.com/threatanalytics3

01 – Die Grundlagen

- Windows Defender Application Control
  - Neueste und sicherste Application Control Technologie von Microsoft.
  - Ermöglicht Unternehmen die Kontrolle darüber, welche Anwendungen und Treiber auf ihren Windows-Clients/Servern ausgeführt werden dürfen.
  - Eingeführt mit Windows 10 / Windows Server 2016

01 – Die Grundlagen

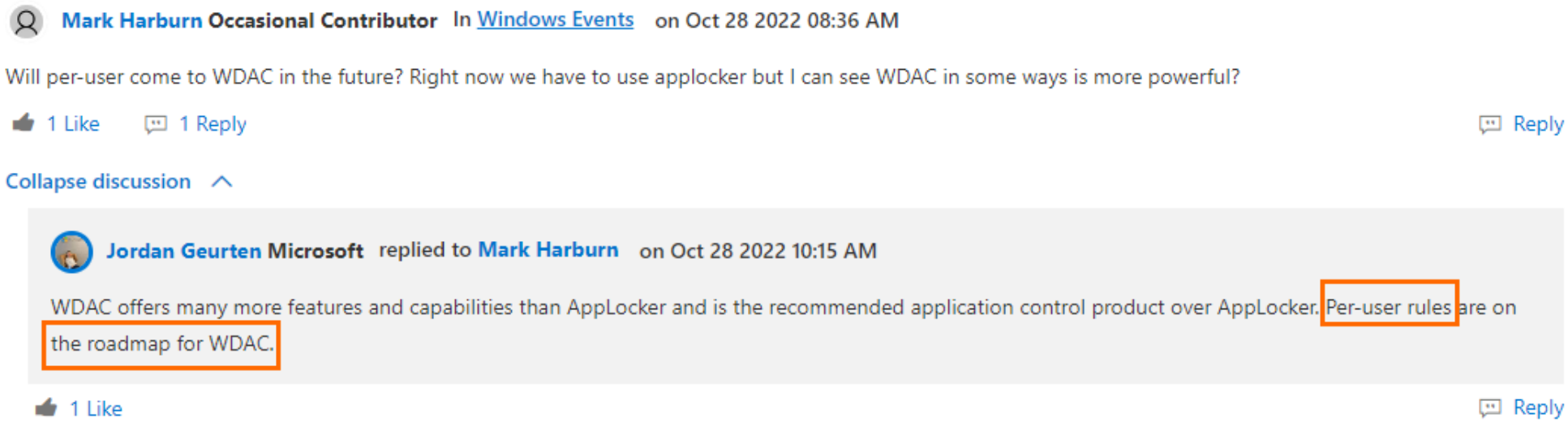
- Windows Defender Application Control
  - Früher bekannt als Configurable Code Integrity (CCI) und Device Guard.
  - Umbenennung in Windows Defender Application Control (WDAC) mit Windows 10 1903.
  - Wird in Zukunft umbenannt in App Control for Business?

01 – Die Grundlagen

- Windows Defender Application Control
  - Unterstützt die folgenden Betriebssysteme
    - Windows 10 Build 1903+ (Beliebige Client-Edition)
    - Windows 11 (Beliebige Client-Edition)
    - Windows Server 2016 oder höher

02 – Es gibt nur Device Policies

- WDAC kennt nur Devices Policies
  - Richtlinien gelten für den verwalteten Computer als Ganzes und betreffen alle Benutzer des Geräts.
  - Es gibt keine Per-User Richtlinien, wie bei AppLocker
  - Dies ist der grösste Nachteil, den WDAC im Vergleich zu AppLocker noch hat



03 – WDAC vs. AppLocker

	AppLocker	WDAC
Policies Applicability	• Can apply to all users of a computer or to individual users and groups	• Applies to the managed computer as a whole and affects all users of the device
Further Development	• Will continue to receive security fixes • Will not undergo new feature improvements	• Undergoing continual improvements
Enforceable file types	• Enforcement of Untrusted DLLs is optional • Driver files (.sys) are not supported	• Untrusted DLLs are blocked by default • Driver files (.sys) are supported

Important Features only supported by WDAC		• Managed Installer (MI)
		  ◦ Allow applications installed by a designated software distribution solution, such as Microsoft Intune
		• Reputation-Based intelligence
		  ◦ Authorize reputable apps with the Intelligent Security Graph (ISG)
		• Multiple Policy support
		  ◦ Supports up to 32 active policies on a device at once.
		• Runtime FilePath Rule Protection
		  ◦ Apps allowed based on file path rules must come from a file path that's only writable by an administrator

Platform support	• Windows 8 and Windows Server 2012 R2 or later.	• Windows 10, Windows 11, and Windows Server 2016 or later.

04 – Managed Installer

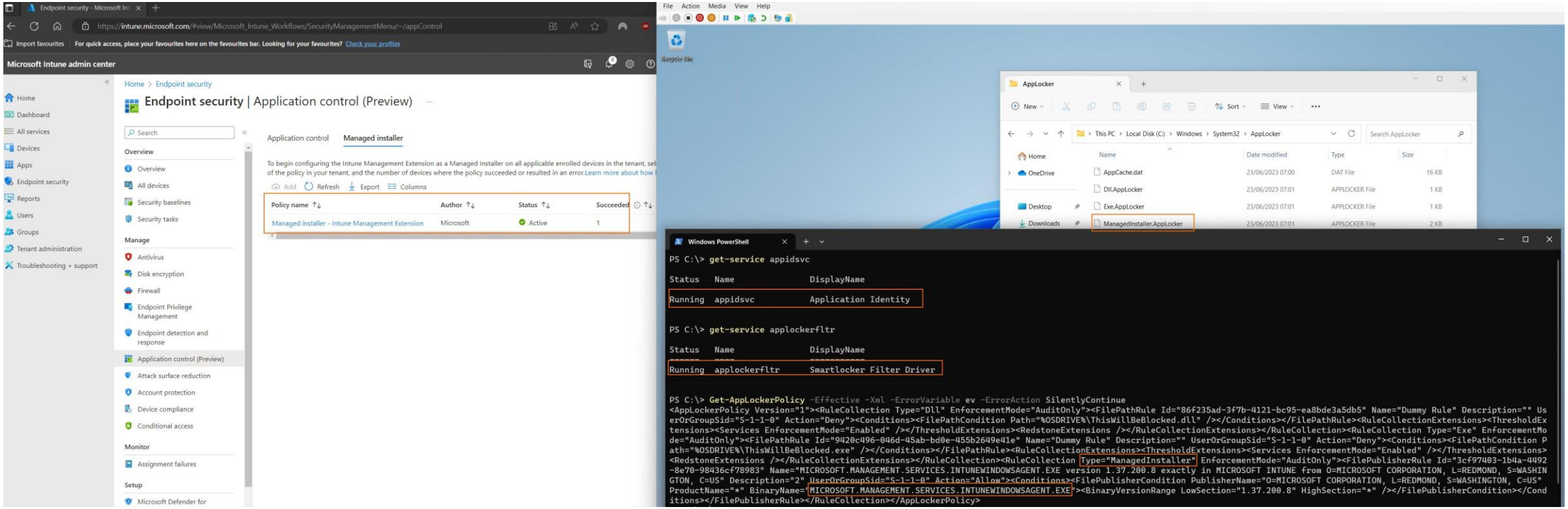
- Um Managed Installer (MI) mit WDAC zu verwenden, müssen Sie AppLocker Rules implementieren.

Administrator: Windows Powe

```
PS C:\> Get-AppLockerPolicy -Effective -Xml -ErrorVariable ev -ErrorAction SilentlyContinue
<AppLockerPolicy Version="1"><RuleCollection Type="Dll" EnforcementMode="AuditOnly"><FilePathRule Id="86f235ad-3f7b-4121
-bc95-ea8bde3a5db5" Name="Benign DENY Rule" Description="" UserOrGroupSid="S-1-1-0" Action="Deny"><Conditions><FilePathC
ondition Path="%OSDRIVE%\ThisWillBeBlocked.dll" /></Conditions></FilePathRule><RuleCollectionExtensions><ThresholdExtens
ions><Services EnforcementMode="Enabled" /></ThresholdExtensions><RedstoneExtensions /></RuleCollectionExtensions></Rule
Collection><RuleCollection Type="Exe" EnforcementMode="AuditOnly"><FilePathRule Id="9420c496-046d-45ab-bd0e-455b2649e41e
" Name="Benign DENY Rule" Description="" UserOrGroupSid="S-1-1-0" Action="Deny"><Conditions><FilePathCondition Path="%OS
DRIVE%\ThisWillBeBlocked.exe" /></Conditions></FilePathRule><RuleCollectionExtensions><ThresholdExtensions><Services Enf
orcementMode="Enabled" /></ThresholdExtensions><RedstoneExtensions /></RuleCollectionExtensions></RuleCollection><RuleCo
llection Type="ManagedInstaller" EnforcementMode="AuditOnly"><FilePublisherRule Id="55932f09-04b8-44ec-8e2d-3fc736500c56
" Name="MICROSOFT.MANAGEMENT.SERVICES.INTUNEWINDOWSAGENT.EXE version 1.39.200.2 or greater in MICROSOFTï¿½ INTUNEï¿½ fro
m O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="" UserOrGroupSid="S-1-1-0" Action="Allow"><Condit
ions><FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="*" Bina
ryName="MICROSOFT.MANAGEMENT.SERVICES.INTUNEWINDOWSAGENT.EXE"><BinaryVersionRange LowSection="1.39.200.2" HighSection="*
" /></FilePublisherCondition></Conditions></FilePublisherRule></RuleCollection></AppLockerPolicy>
PS C:\>
```

04 – Managed Installer

- Um Managed Installer (MI) mit WDAC zu verwenden, müssen Sie AppLocker Rules implementieren.



04 – Managed Installer

www.wpninjas.eu
#WPNinjaS

Home > Endpoint security | App Control for Business (Preview) > Managed installer - Intune Management Extension

Managed installer - Intune Management Extension | Properties

Managed Installer

Search

- Overview
- Manage
  - Properties
- Monitor
  - Device status

Basics

Name	Managed installer - Intune Management Extension
Description	Managed installer - Intune Management Extension
Publisher	Microsoft
Version	4

Settings

Set managed installer	Intune Management Extension

Scope tags Edit

Default

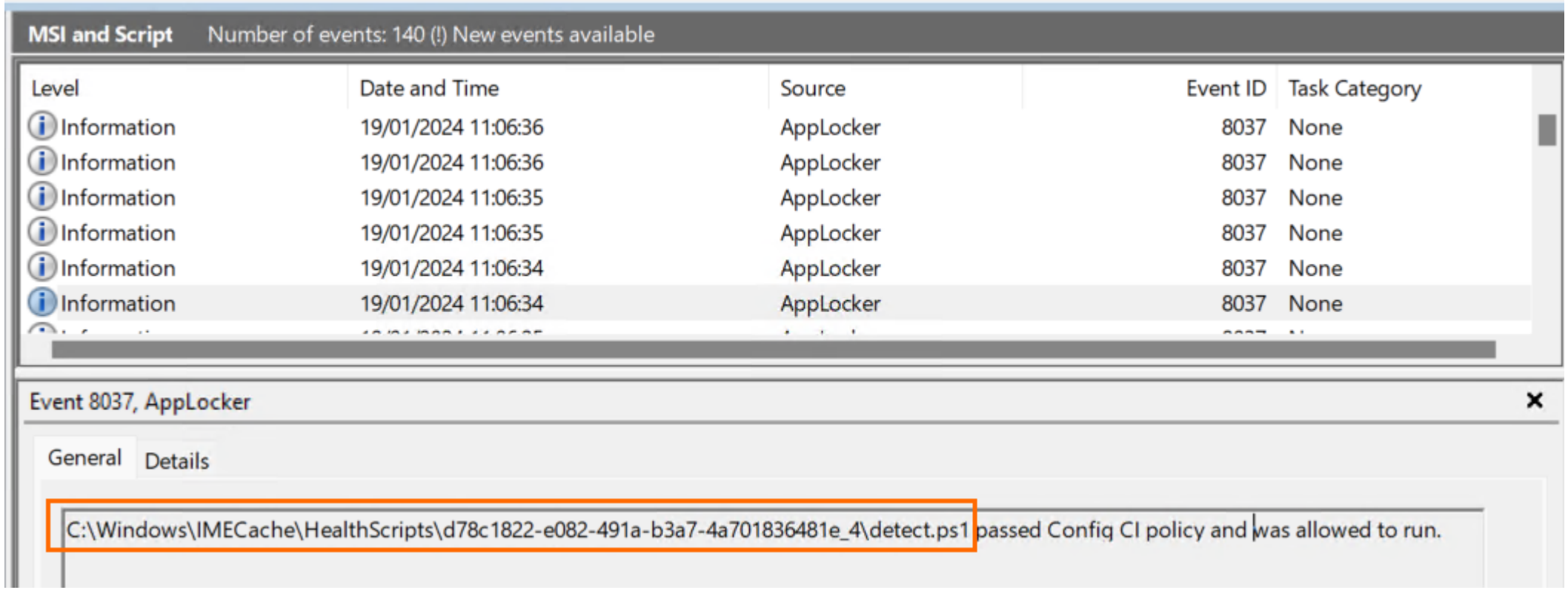
Assignments

Included groups

Selected groups
All devices

04 – Managed Installer

- Microsoft verwendet für die Managed Installer Intune Management Extension Remediation Scripts:
  - C:\Windows\IMECache\HealthScripts

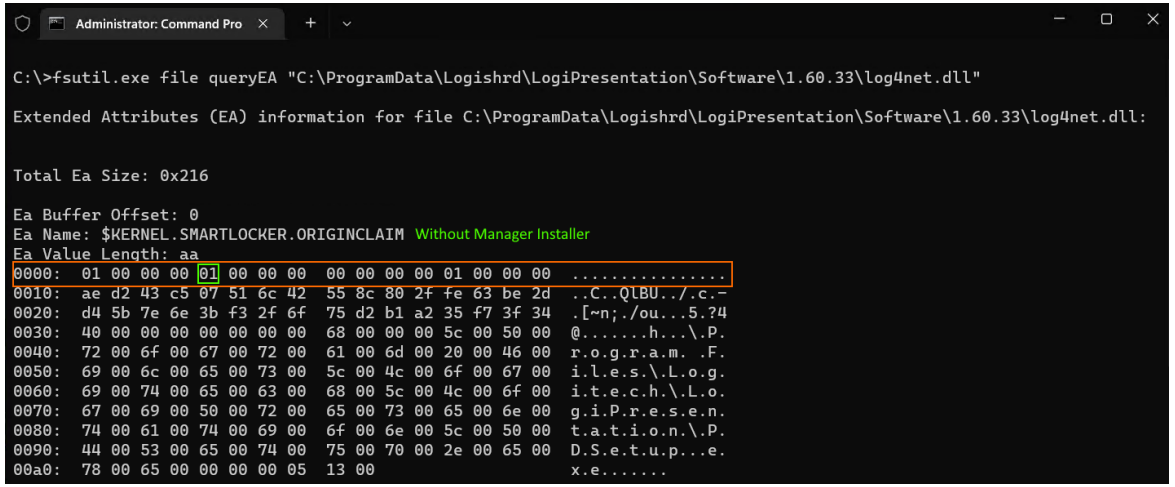


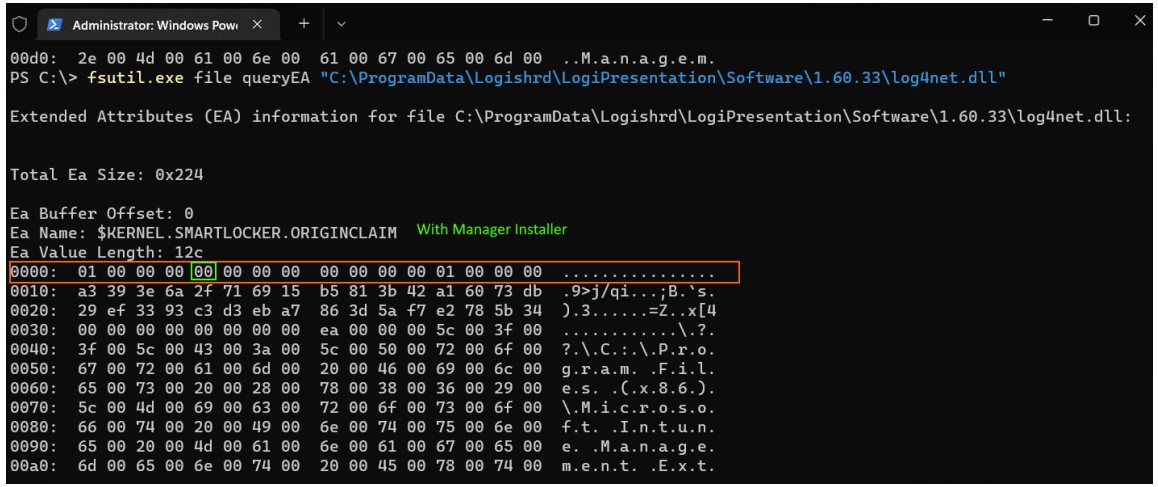
04 – Managed Installer


```
<RuleCollection Type="ManagedInstaller" EnforcementMode="AuditOnly">
    <FilePublisherRule Id="3cf97403-1b4a-4492-8e70-98436cf78983" Name="MICROSOFT.MANAGEMENT.SERVICES.INTUNEWINDOWSAGENT.EXE version 1.37.200.8 exactly in MICROSOFT INTUNE from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="2" UserOrGroupSid="S-1-1-0"
        <Conditions>
            <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="MICROSOFT.MANAGEMENT.SERVICES.INTUNEWINDOWSAGENT.EXE">
                <BinaryVersionRange LowSection="1.37.200.8" HighSection="*" />
            </FilePublisherCondition>
        </Conditions>
    </FilePublisherRule>
    <FilePublisherRule Id="6ead5a35-5bac-4fe4-a0a4-be8885012f87" Name="CMM - CCMEXEC.EXE, 5.0.0.0+, Microsoft signed" Description="2" UserOrGroupSid="S-1-1-0" Action="Allow">
  <Conditions>
    <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="CCMEXEC.EXE">
      <BinaryVersionRange LowSection="5.0.0.0" HighSection="*" />
    </FilePublisherCondition>
  </Conditions>
</FilePublisherRule>
<FilePublisherRule Id="8e23170d-e0b7-4711-b6d0-d208c960f30e" Name="CCM - CCMSETUP.EXE, 5.0.0.0+, Microsoft signed" Description="2" UserOrGroupSid="S-1-1-0" Action="Allow">
  <Conditions>
    <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="CCMSETUP.EXE">
      <BinaryVersionRange LowSection="5.0.0.0" HighSection="*" />
      </FilePublisherCondition>
    </Conditions>
  </FilePublisherRule>
   <FilePublisherRule Id="2ab8fa52-c4bb-4578-b272-d7bb4a9b175d" Name="EPMSERVICESTUB.EXE version 6.2312.31.1000 exactly in MICROSOFT INTUNE from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" Description="2" UserOrGroupSid="S-1-1-0" Action="Allow">
        <Conditions>
            <FilePublisherCondition PublisherName="O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="*" BinaryName="EPMSERVICESTUB.EXE">
            <BinaryVersionRange LowSection="6.2312.31.1000" HighSection="*" />
            </FilePublisherCondition>
        </Conditions>
    </FilePublisherRule>
</RuleCollection>
```

04 – Managed Installer

- Extended Attributes (EA)
  - KERNEL.SMARTLOCKER.ORIGINCLAIM EA
  - fsutil.exe file queryEA “C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\log4net.dll”





05 – Design / Policies Überlegungen

1 Allow Microsoft

- Windows OS components
- Microsoft Store applications
- Office 365, OneDrive, Teams
- WHQL signed kernel drivers
- All Microsoft signed applications

2 Microsoft Recommended Block Policies

- Since there are some bypasses methods that are exploited via signed Microsoft applications (such as Msbuild.exe), Microsoft's Recommended Block Policies will be implemented:
  - Microsoft's Recommended Block Rules
  - Microsoft's Recommended Driver Block Rules

3 Allow Trusted File Path

- C:\Program Files
- C:\Program Files (x86)

4 Verify write permissions in trusted file paths

- If write permission exists on the trusted file paths, we use the WDAC feature "Runtime Filepath Rules" to prevent users from copying and executing applications in the trusted file path.

5 Allow Trusted Publishers

- Trust all applications signed by your hardware manufacturer like e.g., Lenovo
- We trust our used and signed remote support application like e.g., TeamViewer

6 Allow Managed Installer (MI)

- All approved applications that are distributed via Microsoft Intune (Required/Available/ Uninstall) should not be blocked

7 Reputation-Based intelligence

- Authorize reputable apps with the Intelligent Security Graph (ISG).
- If you want to block installations that do not require administrator rights because they are installed via the user context (%LocalAppData%), ISG should not be used.

8 Block everthing else

- Everything else is blocked. We block all malicious, untrusted or unsigned applications.

05 – Design / Policies Überlegungen

1 ACfB-01-BP-Allow-Microsoft

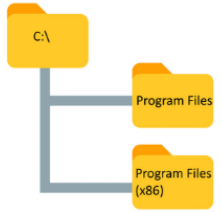
- Windows OS components and Microsoft Store applications
- Office 365, OneDrive, Teams
- WHQL signed kernel drivers
- All Microsoft signed applications
- Microsoft's Recommended Block Rules
- Microsoft's Recommended Driver Block Rules

2 ACfB-02-SP-Allow-Trusted3rdPublishers

- Allow Publisher Rules
  - All applications signed by your hardware manufacturer like e.g., Lenovo
  - Used and signed remote support application like e.g., TeamViewer
  - Other trusted 3rd party publishers that do not run applications in the default program files directories

3 ACfB-03-SP-Allow-TrustedPaths

- Allow Default Trusted Path Rules
  - %OSDRIVE%\Program Files*
  - %OSDRIVE%\Program Files (x86)*



06 – Corporate Codesigning

- Erwäge Corporate Codesigning für WDAC Policies
  - Individual certs (External Code Signing Certificate)
  - Corporate PKI (Internal Code Signing Certificate)
  - Azure Trusted signing
    - https://learn.microsoft.com/en-us/azure/trusted-signing/

07 – Monitoring

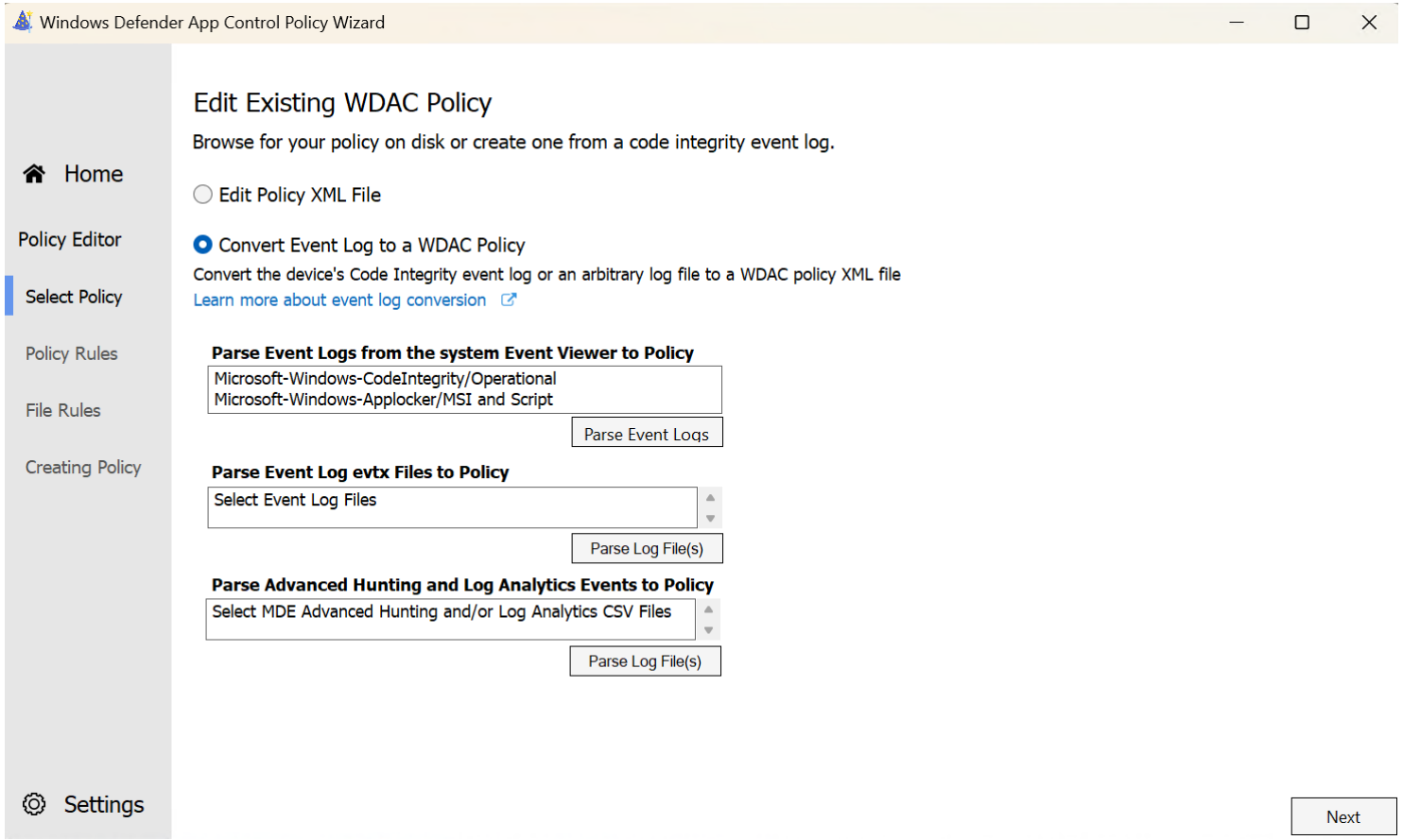
- Die Ereignisse der Windows Defender Application Control-Richtlinienprotokolle werden an zwei Orten erzeugt:
  - Applications and Services logs > Microsoft > Windows > CodeIntegrity > Operational
  - Applications and Services logs > Microsoft > Windows > AppLocker > MSI and Script

07 – Monitoring

1. Microsoft Defender for Endpoint - Advanced Hunting Queries
2. Azure Log Analytics
3. Configuration Manager – CMPivot
3. Microsoft Intune – Device query
4. Event Log Forwarding
5. Third Party (Splunk)

08 – Deployment

- WDAC Wizard
  - Erstellen, Bearbeiten und Zusammenführen von WDAC Policies

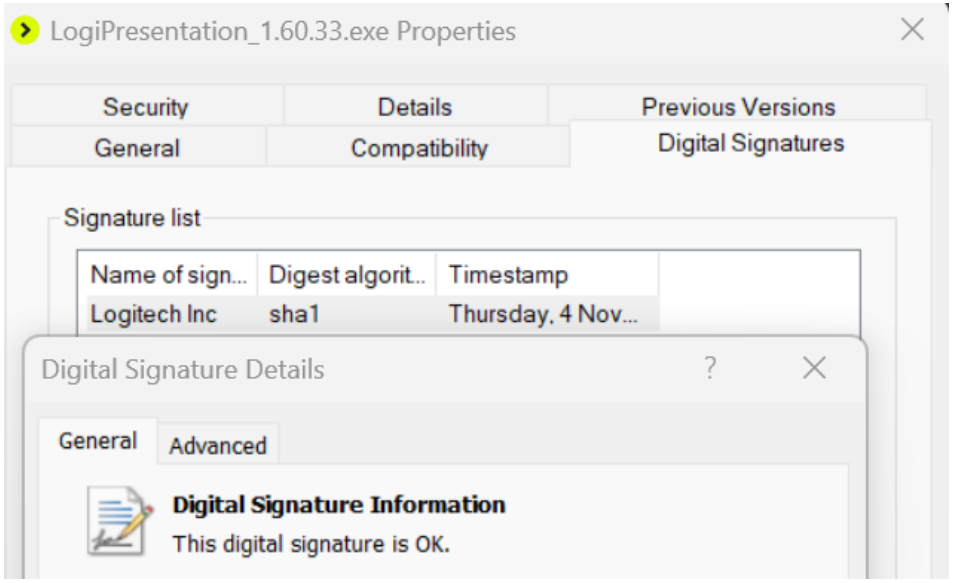


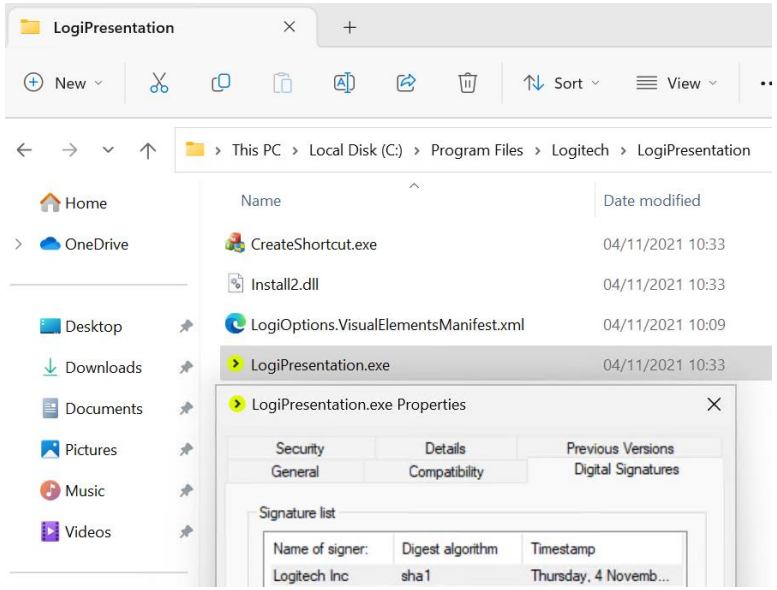
08 – Deployment

- Management Solutions
  - Microsoft Intune (Empfohlen)
  - Microsoft Configuration Manager (Nicht empfehlenswert)
  - Group policy (nicht empfehlenswert)
  - PowerShell (nicht empfehlenswert)

09 – Die grösste Herausforderung

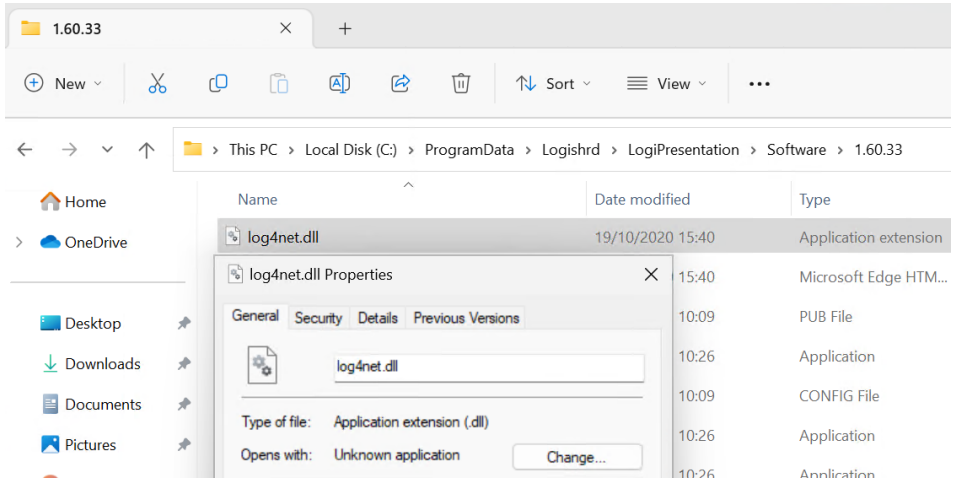
- Nicht signierte Applikationen

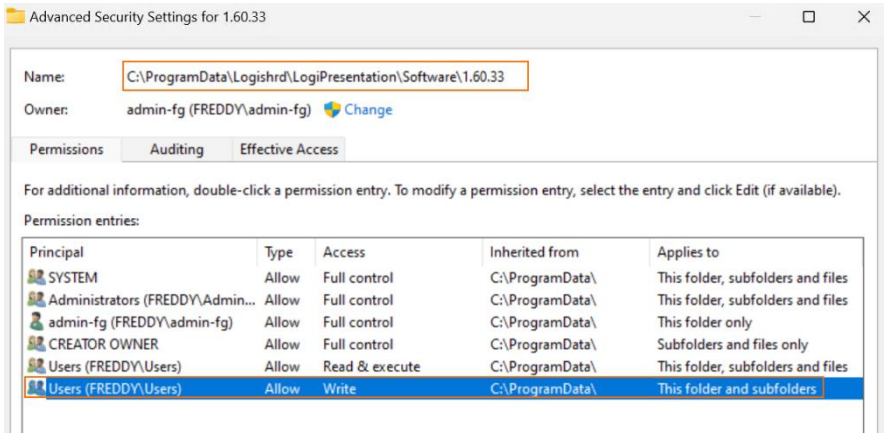




09 – Die grösste Herausforderung

- Nicht signierte Applikationen





- C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\log4net.dll
- C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\Ninject.dll
- C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\GalaSoft.MvvmLight.dll
- C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\Hardcodet.Wpf.TaskbarNotification.dll
- C:\ProgramData\Logishrd\LogiPresentation\Software\1.60.33\Newtonsoft.Json.dll

10 – Empfehlungen aus der Praxis

1. Definieren Sie Anwendungsfälle!

   Entscheidung WDAC / AppLocker -> Killerkriterium werden User Rules benötigt?

2. Analysieren Sie, welche Anwendungen keine digitale Signatur haben (Managed Installer)

3. Ohne ein Konzept und ein gut geplantes Basic Rule Set wird es nicht funktionieren

4. Die Überwachung ist der wichtigste Teil

5. Ein WDAC Deployment ist am einfachsten mit Windows 11, Microsoft Intune und Microsoft Defender for Endpoint

Best Case Szenario: Migration von Windows 10 auf Windows 11

Thank you

Session Feedback

www.wpninjas.eu
#WPNinjaS