



Bachelor in de
Elektronica – ICT/TI

Documentatie – Implementatie Van
CyberArk EPM

Luka Wynants

Contents

Termen en Afkortingen	3
1.0 EPM-installatie	4
1.1 EPM-Agent installatie.....	4
2.0 EPM-configuratie.....	5
2.1 Monitoring fase.....	5
2.2 Application catalogue	6
2.3 AD groepen aanmaken.....	6
3.0 Application groups	7
3.1 Application defintition toevoegen.....	8
3.2 Application groups creëren	9
4.0 Policies creëren	11
4.1 Baseline policy.....	11
4.2 Developer policy	12
4.3 Analyst policy	14
4.4 Block/restrict unhandled applicaties.....	15
4.5 Prioraties	16
5.0 Tests	16
5.1 Test 1	16
5.2 Test 2	18
5.3 Test 3	20
6.0 Extra Implementatie.....	22
6.1 Virus total integration	22
6.2 Protect against ransomware.....	23
6.3 Privilege Threat protection.....	24
Configuratie Samenvatting	26
7.0 Finale Tests	27
7.1 WannaCry.....	28
7.2 Akira	28
7.3 Trigona	29
7.4 LockBit	29
7.5 PoC ransomware	30
8.0 Conclusie	31

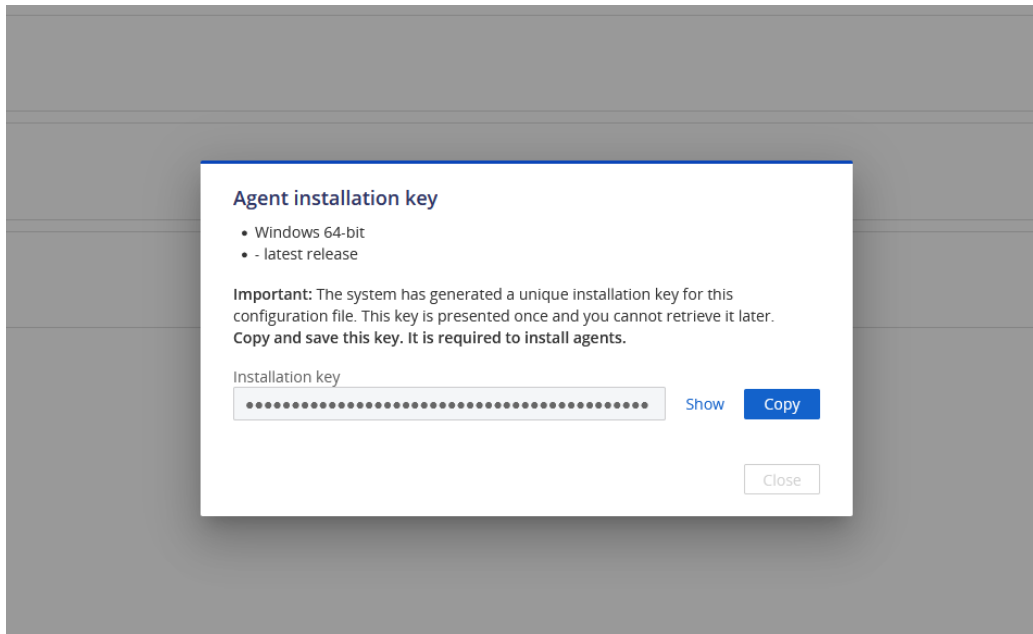
Termen en Afkortingen

Term	Omschrijving
AD	Een systeem gebruikers, computers en andere resources binnen een netwerk te beheren.
Analyst	Een user die verantwoordelijk is voor het analyseren van malware.
API	Een code waarmee software met andere software kan praten.
Application Catalogue	Lijst van bekende applicaties binnen EPM.
Application Definition	Instellingen die bepalen welke applicaties worden behandeld.
Application Group	Verzameling applicaties met gelijkaardige regels.
Baseline policy	Standaardbeleid dat op alle systemen wordt toegepast.
Certificate Authority (CA)	Vertrouwde instantie die digitale certificaten uitgeeft.
Checksum	Een hash waarde van data om te controleren of de data ongewijzigd is.
Credential Lure	Valse inloggegevens die aanvallers misleiden.
Credential Theft	Diefstal van gebruikersnamen en wachtwoorden.
CyberArk	Beveiligingsbedrijf met oplossingen voor het beheren van beheerdersrechten (PAM/EPM).
Default policy	Basisregels die standaard op applicaties worden toegepast.
Detect mode	Een modus dat gedrag Logt zonder blokkering.
Developer	Een user die software ontwikkeld.
Endpoint	Een apparaat zoals een computer of laptop.
EPM	Endpoint Privilege Manager
EPM-Agent	Software op een endpoint die CyberArk EPM-beleid uitvoert.
Elevate if necessary	Een EPM-optie dat verhoogde rechten geeft aan applicaties maar alleen als het nodig is.
Events	Alerts of meldingen op endpoints die naar de event viewer worden gestuurd.
Executable	Uitvoerbaar bestand zoals .exe.
Explorer.exe	File explorer van Windows.
Hashwaarde	Unieke digitale waarde van een bestand.
Handled application	Applicatie die onder een EPM-policy valt.
Indicator of Compromise (IoC)	Bewijsstuk dat een systeem mogelijk is gecompromitteerd.
Lateral Movement	Beweging van een aanvaller tussen systemen binnen hetzelfde netwerk.
LSASS	Windows-proces dat authenticatie beheert.
Metadata	Informatie over een bestand, zoals aanmaakdatum.
Monitoring phase	Periode waarin gedrag gelogd.
Network Share	Gedeelde map op een netwerk.
NTDS.dit dumping	Uitlezen van AD-database voor gebruikersgegevens.
Pass-the-Hash	Privilege escalation aanval met opgeslagen wachtwoord-hashes te gebruiken
Policy	(Beleid) Regels die bepalen hoe applicaties behandeld worden.
Windows proces	Systeemtaak of applicatie die draait in het Windows-besturingssysteem.
Publisher Signature	Digitale handtekening van software dat door de officiële developer is getekend
Ransomware	Malware die bestanden versleutelt en losgeld eist.
Restrict Mode	Modus waarin applicaties beperkte rechten krijgen.
ransomnote	
Safe Mode	Veilige opstartmodus van Windows voor herstel.
SAM harvesting	Uitlezen van Windows gebruikersdatabase.
SHA-1, SHA-256	Veelgebruikte hash-algoritmes.
Unhandled Applications	Applicatie die niet onder een EPM-policy valt.
VirusTotal	Onlinedienst die bestanden scant met meerdere antivirusprogramma's.

1.0 EPM-installatie

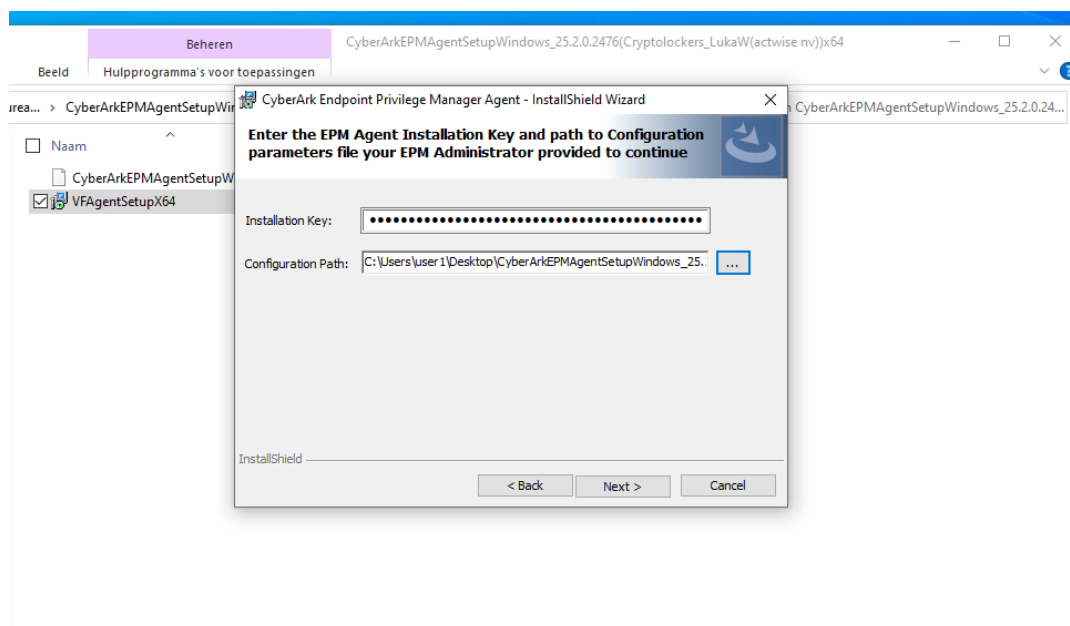
1.1 EPM-Agent installatie

Om EPM te installeren op een endpoint, moet je een agent installeren. De agent verzamelt events die worden gebruikt om policies aan te maken. Je kunt de EPM-agent downloaden; deze krijgt een willekeurige installatiecode die je slechts één keer kunt bekijken, kopiëren en gebruiken. Bij het downloaden ontvang je een installatiescript dat je moet uitvoeren op je endpoint.



Figuur 1 Agent installatie sleutel

Tijdens de installatie op de endpoint wordt er gevraagd om de installatiecode in te voeren:



Figuur 2 Agent installatie op windows 10

Hierna is de agent succesvol geïnstalleerd.

2.0 EPM-configuratie

2.1 Monitoring fase

De eerste stap in de implementatie van EPM is de monitoringsfase. Hier wordt er nagegaan welke applicaties op welke computers worden gebruikt en welke privileges deze applicaties vereisen. Het uiteindelijke doel is om deze applicaties in een *application group* te plaatsen waarop vervolgens policies worden gedefinieerd. Deze policies worden gekoppeld aan een Active Directory-groep en bepalen welke gebruiker wat mag.

Privilege Management

① Additional Privilege Management policies override commonly used Privilege Management policies for the same target computers and users

Detect privileged unhandled applications	Windows macOS Linux	Off On Edit
Protect against ransomware	Windows	Off Detect Restrict
Control unhandled applications downloaded from the internet	Windows	Off Detect Restrict Block
Control unhandled applications	Windows macOS	Off Detect Restrict Edit

Figuur 3 Default Policies

Om ongecontroleerde applicaties te detecteren, moet je de policy "*Detect privileged unhandled applications*" op "*on*" zetten en "*Control unhandled applications*" op "*detect*". Hierdoor worden events gegenereerd en worden nieuwe of bestaande applicaties gelogd in de *application catalogue*. Je kunt ook specifieke computers waarop de EPM-agent is geïnstalleerd, scannen op applicaties:

Computers scan summary	
Accumulated summary of ongoing and finished computer scans	
Updated at: 9:30 AM	
Ongoing scan phase	Computers
Initializing	1
Collecting data on endpoint	0
Processing data	0

Figuur 4 Computer scan summary

2.2 Application catalogue

In de onderstaande figuur is de *application catalogue* te zien. Hier kun je alle applicaties zien, zowel ‘unhandled’ als ‘handled’:

Application Coverage by Policies | Cryptolockers_LukaW... | Management Options | Last sign in: 28-Mar-25 | luka.wynants@actwise.eu

checked on: 26-Mar-25 at 4:13:40 pm | 90 handled applications (27%) | 239 unhandled applications (73%)

Filter Analyze coverage Updated at: 10:18 AM

329 results

Application	Application type	Publisher's signature	Source Type	Policies ↑	Computers	
Google Chrome (chrome_pwa_launcher.exe)	Executable	Google LLC	LocalDisk		1	...
inject_dll_amd64.exe	Executable	Microsoft 3rd Party Applicati...	LocalDisk		1	...
BraveSoftware Update Setup (BraveBrowserSe...	Executable	Brave Software, Inc.	OldApplication		1	...
Microsoft Visual C++ 2022 X86 Minimum Runti...	Installation package	Microsoft Corporation	OldApplication		1	...
CyberArk EPM UI Host (32-bit) (vf_host.exe)	Executable	CyberArk Software Ltd.	EPM		1	...
akira.exe	Executable	Unsigned	OldApplication		1	...
Notepad++ : a free (GNU) source code editor (...)	Executable	Notepad++	LocalDisk		1	...
Windows-beveiliging (SecurityHealthAgent.dll)	COM object	Microsoft Windows	LocalDisk		1	...
docker-sbom.exe	Executable	Docker Inc	OldApplication		1	...
extension-admin.exe	Executable	Docker Inc	OldApplication		1	...
Google Installer (ChromeSetup.zip.exe)	Executable	Google LLC	Internet		1	...
pip3.13.exe	Executable	Unsigned	LocalDisk		1	...
VMware Tools ([A3631D35-CFA5-45F6-A65E-...)	Installation package	VMware, Inc.	OldApplication		1	...
SharkD (sharkd.exe)	Executable	Wireshark Foundation	LocalDisk		1	...
docker-index.exe	Executable	Docker Inc	OldApplication		1	...

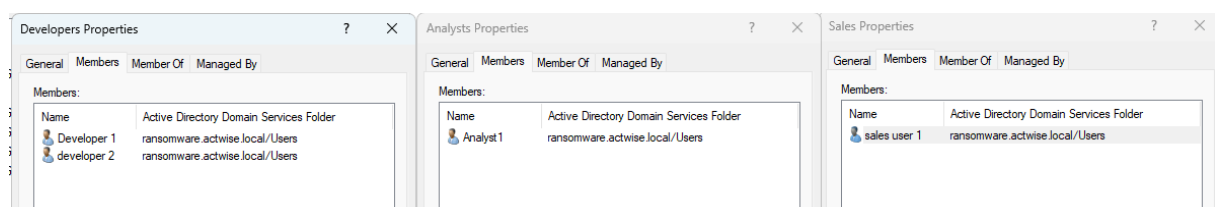
Figuur 5 Application catalogue

2.3 AD groepen aanmaken

Om policies toe te passen, moet je deze toewijzen aan een AD-groep of gebruiker. Daarom heb ik nieuwe gebruikers en AD-groepen aangemaakt:

- Normale gebruikers (bijv. sales) – mogen baseline-applicaties gebruiken
- Developers – mogen developer applicaties gebruiken
- Malware Analysts – mogen analyst-applicaties gebruiken

In de onderstaande figuur kun je de Active Directory groepen zien die ik heb aangemaakt. In elke groep worden vervolgens gebruikers geplaatst.



Figuur 6 Active directory groepen: ‘Developers’, ‘Analysts’, ‘Sales’

3.0 Application groups

De volgende stap in het proces is het groeperen van applicaties in *application groups*. In een echte implementatie voor een bedrijf is het de bedoeling om samen met het bedrijf een tabel op te stellen waarin per afdeling wordt bepaald welke applicaties en rechten vereist zijn. Ik heb zelf een kleine catalogus van applicaties samengesteld, maar in een echte situatie zouden er veel meer *application groups* en applicaties zijn.

Ik heb de volgende *application groups* aangemaakt:

Baseline application group – een groep van applicaties die alle gebruikers mogen gebruiken. Deze groep definieert bijvoorbeeld welke browser, documenteditor en communicatie-applicaties zijn toegestaan binnen de organisatie.

Application type	Allow	Block
Messaging/video conferencing	Microsoft Teams	Discord, Zoom, Skype, googlemeet, whatsapp, telegram
Browsers	Edge	Chrome, Safari, Opera, Brave, Vivaldi, Firefox
Mail	Outlook	ThunderBird, Gmail, Yahooemail
Social media apps	Not allowed	Instagram, Facebook, Twitter, Snapchat,
games	Not allowed	Steam, epic games launcher
filesharing	OnDrive	Dropbox
Entertainment	Not allowed	Netflix, Disney, Twitch, HBOMax, Prime, Hulu
Documents	Word, Excel, powerpoint, onenote	LibreOffice, GoogleDocs
VPN	Not allowed	NordVPN, ProtonVPN, ExpressVPN, OpenVPN
AI	Not allowed	ChatGPT, deepseek
Hobbies	Not allowed	GarageBand, audacity,
Zippping	WinRAR	FileZilla, 7zip, BreeZip
Multimedia Viewing	VLC media player	OBS studio

Figuur 7 Baseline application group

Developers application group – een groep applicaties die enkel door developers mag worden gebruikt. Voorbeelden hiervan zijn programmeertalen of command-line tools zoals PowerShell, die niet toegankelijk mogen zijn voor gewone gebruikers.

Application type	Allow	Block
IDE	Vscode	Sublime, Pycharm, Notepad++, Arduino IDE
Languages	Python, JavaScript, Node.js	Ruby, PHP, Rust
Databases	MongoDb	MySQL, SQLite,
Virtualization/containers	Docker, Vmware	Vbox, Kubernetes, vagrant
Version management	git	
installation tools	Postman, pip, npm	
commandline	WSL, CMD, Powershell	

Figuur 8 Developers application group

Malware Analysts application group – een groep van tools die uitsluitend door malware-analisten mogen worden gebruikt. Deze bevatten bijvoorbeeld tools voor procesanalyse, netwerkverkeerinspectie of reverse engineering.

Application type	Allow	Block
Network	Wireshark, zenmap(nmap gui), tcp view	
Application Monitoring	processExplorer, ProcMon	
Analysis	ProcessHacker	
Registry	RegShot	
Exe analysis	ResourceHacker	
Presistance checking	Autoruns	
Tools	Psexec	
Storage Analysis	WizTree	

Figuur 9 Analyst application groep

3.1 Application definition toevoegen

Om applicaties toe te voegen aan *application groups* in CyberArk Endpoint Privilege Manager (EPM), zijn er verschillende parameters beschikbaar om applicaties op een betrouwbare manier te identificeren.

Application definition X

Application group: **Baseline** Type: **Application Group** Platform: **Windows**

Definition type: Executable [Describe definition](#)

Properties Security level: Low Add property

Filename	is exactly		🗑️ ℹ️
Publisher's signature	is exactly	Separate signatures by semicolon (;)	🗑️ ℹ️
Location	is in directory	<input type="checkbox"/> with subfolders	🗑️ ℹ️
Location type	is on local disks only		🗑️ ℹ️
Checksum	is SHA1 / SHA256	File checksum in SHA1 format Browse File checksum in SHA256 format	🗑️ ℹ️
Parameters	is exactly	<input type="checkbox"/> case sensitive	🗑️ ℹ️
Owner	is exactly	See guidelines for user and group formats SID Find Paste	🗑️ ℹ️
Product name	is exactly		🗑️ ℹ️
File description	is exactly		🗑️ ℹ️
Company name	is exactly		🗑️ ℹ️
Original filename	is exactly		🗑️ ℹ️
File version	is between		🗑️ ℹ️
Product version	is between		🗑️ ℹ️

Figuur 10 Application definition opties

Enkele voorbeelden die ik gebruik in mijn implementatie:

- **Filename:** De bestandsnaam van de applicatie zoals die op het systeem voorkomt. Dit is een basisparameter, maar kan eenvoudig worden gewijzigd en is dus minder betrouwbaar als enige criterium.
- **Original Filename:** De originele naam van het bestand zoals vastgelegd in de metadata van het uitvoerbare bestand. Dit is vaak consistentere dan de zichtbare bestandsnaam.
- **Publisher's Signature:** De digitale handtekening van de uitgever. Deze parameter verhoogt de betrouwbaarheid van de identificatie omdat het moeilijker is om een legitieme handtekening te vervalsen. Dit is vooral nuttig voor bekende softwareleveranciers.
- **Checksum:** Een hashwaarde (SHA-1, SHA-256) van het bestand. Deze unieke waarde verandert zodra het bestand ook maar minimaal wordt aangepast, en is dus een zeer nauwkeurige methode om specifieke versies van applicaties te identificeren.

In mijn configuratie ga ik voornamelijk de *publisher signature* combineren met de *original filename* en *filename*. De reden hiervoor is dat de *publisher signature* onmogelijk te vervalsen is, aangezien deze is ondertekend door een *Trusted Certificate Authority* (CA) met een private key. Dit biedt een hoge mate van betrouwbaarheid bij het identificeren van legitieme software. In sommige gevallen heeft een legitieme applicatie geen *publisher signature* (bijvoorbeeld oudere of custom software). In zulke situaties maak ik gebruik van de *checksum* om de applicatie toch uniek te kunnen identificeren. Het nadeel van deze aanpak is dat de *checksum* bij elke kleine wijziging van de applicatie verandert, waardoor deze methode minder flexibel is bij updates of meerdere versies.

3.2 Application groups creëren

Figuur 11 'Baseline' Application group aanmaken

Ik heb een *application group* "baseline" aangemaakt waarin ik alle applicaties heb geplaatst die in de Excel onder "allow" vallen. Bijvoorbeeld:

Figuur 12 Application definition van word

Zoals te zien in de eigenschappen van Word:

- De *Original Filename* is "WinWord.exe"
- De *Filename* is "WINWORD.EXE"
- De *Publisher Signature* moet overeenkomen met die van Microsoft

Dit verifieert dat het de "echte" Word is. Deze stappen heb ik herhaald voor alle baseline-applicaties (zie fig).

This group includes applications that match the following definitions.

Add definition
Add definition from application

Paste definition

Definition Type	Definition	Info	
Executable	Filename is exactly "vlc.exe" (case insensitive) AND Publisher's signature is exactly {"VideoLAN"} (case sensitive) AND Original filename is exactly "vlc.exe" (case insensitive)		
Executable	Filename is exactly "winrar-x64-711.exe" (case insensitive) AND Publisher's signature is exactly {"win.rar GmbH"} (case sensitive) AND Original filename is exactly "WinRAR.exe" (case insensitive)		
Executable	Filename is exactly "msedge.exe" (case insensitive) AND Publisher's signature is exactly {"Microsoft Corporation"} (case sensitive) AND Original filename is exactly "msedge.exe" (case insensitive)		
Executable	Filename is exactly "POWERPNT.EXE" (case insensitive) AND Publisher's signature is exactly {"Microsoft Corporation"} (case sensitive)		

View all

Figuur 13 Baseline Application group scope

Sommige applicaties, zoals Resource Hacker, hebben geen signature. In dat geval gebruik ik SHA1 en SHA256 om ze te identificeren. Aangezien deze applicatie niet geüpdatet hoeft te worden, blijven de hashes geldig.

File	Source	Pre-history
Name	Value	
Installed	Before EPM Agent (Old Application)	
Hash (SHA1)	4E6EB74DC21503925645B3A8E4E8...	
Hash (SHA256)	1227E484F32C34F026F311E60F1AB...	
Publisher		
Publisher status	No signature	
InternalName	ResHack	
OriginalFilename	ResHack	
File Version (fixed)	5.2.6.425	
Product Version (...)	5.0.0.0	

Figuur 14 SHA1 en SHA256 van een bestand en Publisher van resource hacker

Application definition
×

Application group: **Analyst** Type: **Application Group** Platform: **Windows**

Definition type: Executable Describe definition [🔗](#)

Properties Security level: ● High Add property

Filename	is exactly	ResourceHacker.exe	🗑️ ℹ️
Checksum	is SHA1 / SHA256	4e6eb74dc21503925645b3a8e4e8cfc63c6fb237 Browse	🗑️ ℹ️
		1227E484F32C34F026F311E60F1ABAE065E00F203153DBF0623152DED5CAFI	
Original filename	is exactly	ResHack	🗑️ ℹ️

Figuur 15 Application definition van resource hacker

Deze stappen heb ik herhaald voor zowel de *developers* en *analyst application groups*, hierin heb ik de applicaties van de excel toegevoegd. Zoals te zien in figuur 16 zijn er nu 3 *application groups*.

	Name	Type	Platform	Last modified ↓	
<input type="checkbox"/>	Developers (09-Apr-25 09:10:17.971)	Custom	Windows	11:10:18	⋮
<input type="checkbox"/>	Analyst	Custom	Windows	11:07:26	⋮
<input type="checkbox"/>	Baseline	Custom	Windows	10:57:18	⋮

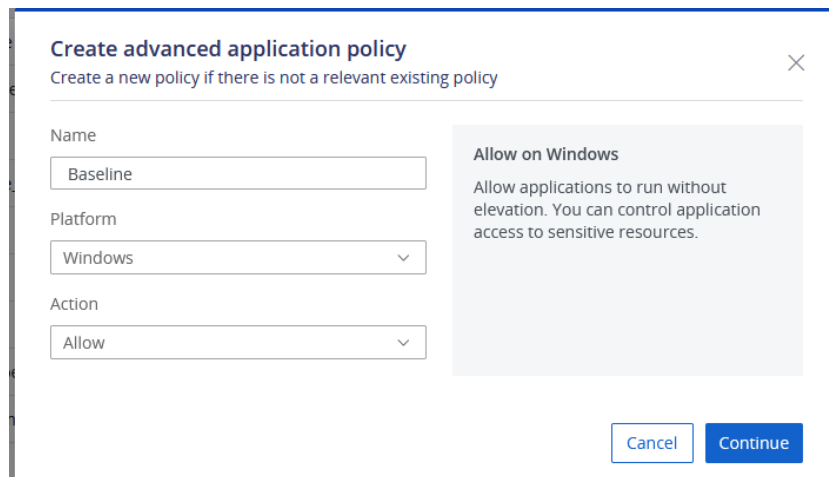
Figuur 16 Developers, Analyst en Baseline application groups

4.0 Policies creëren

Nu heb ik mijn basis apps gedefinieerd in *application groups*, de volgende stap is policies definiëren voor deze application groepen en ze toewijzen aan een AD groep.

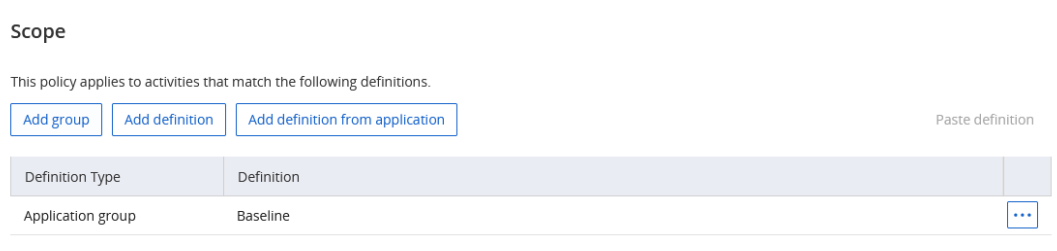
4.1 Baseline policy

De eerste policy die ik heb gemaakt is de *baseline policy*.



Figuur 17 Baseline policy aanmaken

De scope is de *Baseline application group*.



Definition Type	Definition
Application group	Baseline

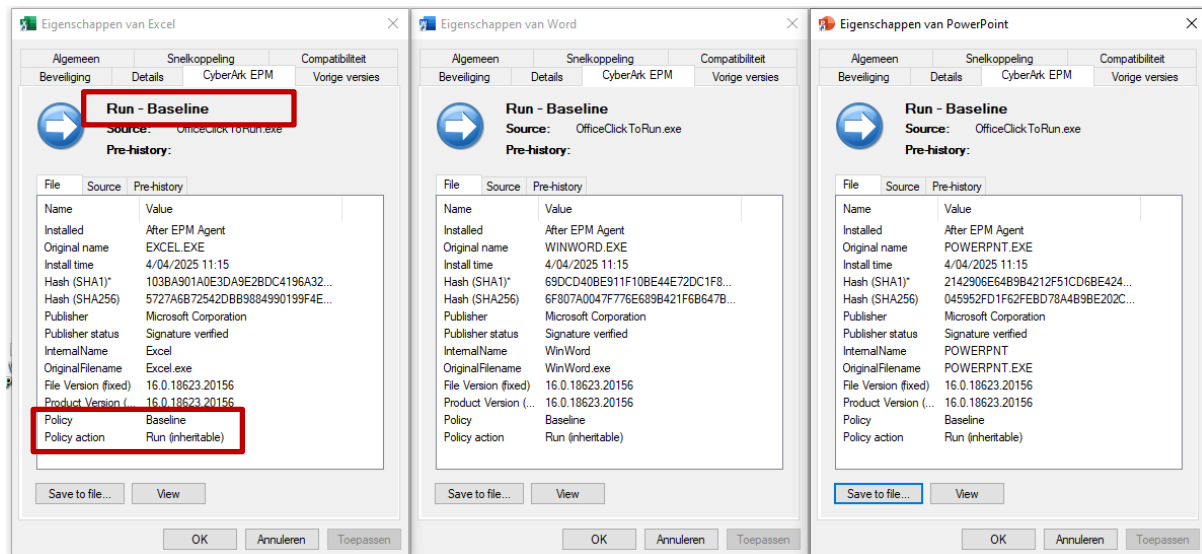
Figuur 18 Baseline application groep koppelen aan de baseline policy

De target is op alle endpoints sinds deze policy de baseline is voor elke user.

Targets		
Apply policy to	Selected	
Computers in this set	All	<button>Edit</button>
Computers in AD security groups	All	<button>Edit</button>
Users and groups	All	<button>Edit</button>

Figuur 19 Targets definiëren voor Baseline policy

Als we nu inloggen met eender welke gebruiker, zou de policy zijn toegepast op de applicaties die in de groep zitten. Als voorbeeld Excel, Word en PowerPoint:



Figuur 20 Excel, Word en PowerPoint CyberArk eigenschappen na de Baseline policy is gecreëerd

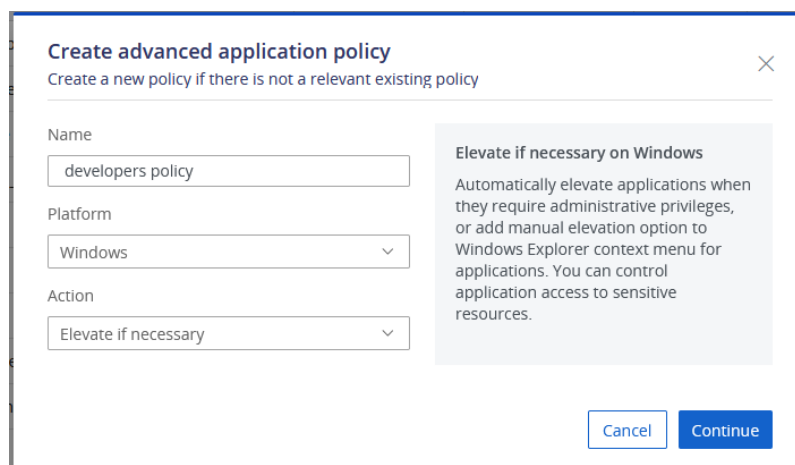
Zoals te zien in de eigenschappen van Word wordt nu onder "Policy" getoond dat de *baseline policy* is toegepast op deze applicatie. Je kunt ook zien dat deze applicatie mag worden uitgevoerd. Dit geldt voor alle applicaties in de *application group* "Baseline".

4.2 Developer policy

Nu ga ik de developer's policy creëren, deze policy krijgt "elevate if necessary" permissions. Bij "Elevate if necessary" in CyberArk EPM:

- De gebruiker zelf krijgt geen administratorenrechten
- De applicatie krijgt tijdelijk de benodigde rechten
- EPM voert de elevation op de achtergrond uit, zonder dat het account van de gebruiker verandert
- Zodra de actie klaar is, verdwijnen de elevated rechten weer

Met andere woorden: EPM "leent" de rechten alleen aan het proces, niet aan de gebruiker. Dit is ideaal voor het veilig uitvoeren van applicaties die soms hogere rechten nodig hebben, zoals installers, updates of configuratietools.



Figuur 21 Developers policy creëren

De scope van de developers policy is de *application group* van de *developers* die eerder is aangemaakt.

Scope

This policy applies to activities that match the following definitions.
The "Elevate if necessary" action can be applied to all applications.

Paste definition ☐ All applications

Definition Type	Definition
Application group	Developers (09-Apr-25 09:10:17.971)

Figuur 22 Developers application group koppelen aan de developer's policy

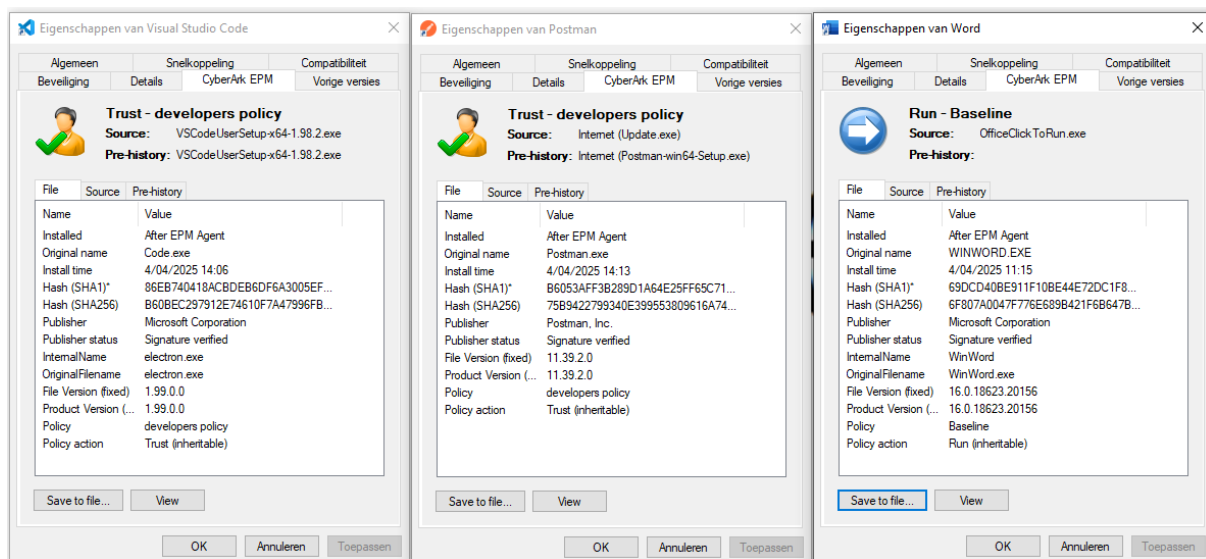
De targets zijn alleen de users in de *developers* Active Directory groep.

Targets

Apply policy to	Selected	
Computers in this set	All	<input type="button" value="Edit"/>
Computers in AD security groups	All	<input type="button" value="Edit"/>
Users and groups	Developers	<input type="button" value="Edit"/>

Figuur 23 Developers AD groep koppelen aan de developer's policy

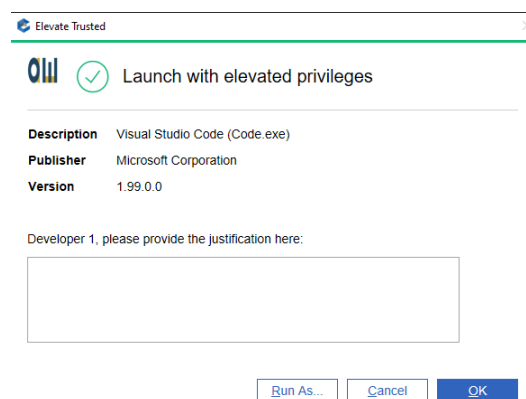
Als we dit testen op een gebruiker die in de developers AD groep zit zien we dat de applicaties van de developer application groep nu de Trust policy hebben gekregen van de developers policy.



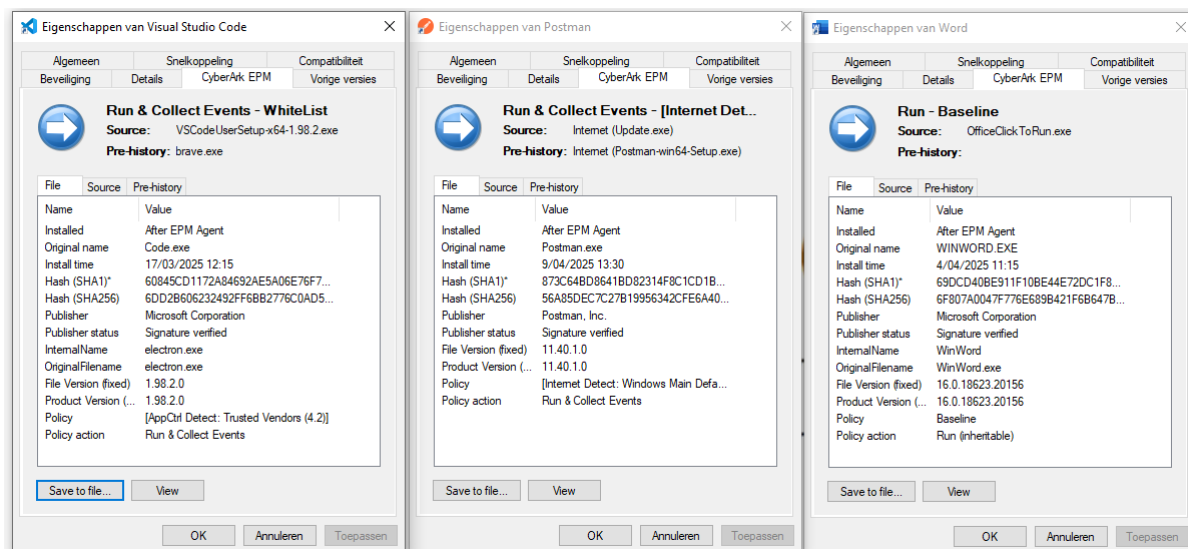
Figuur 24 VSCode, Postman en word CyberArk eigenschappen op developer1 user na de developer's policy te creëren

Bij het testen met de developer1 user die in de developers groep zit zien we dat Visual Studio en Postman elevated rechten krijgen. Word blijft deel van de *Baseline Policy*, maar "Developer1" mag extra applicaties uitvoeren dankzij de Developer Policy.

Als we een developer applicatie openen met admin rechten krijgen we de volgende prompt:



Gebruikers buiten de groep (zoals “Sales”) kunnen dit niet. Zij krijgen slechts de “Run & Collect Events”-rechten.



Figuur 25 VSCode, Postman en word CyberArk eigenschappen op salesuser1 user na de developer's policy te creëren

We kunnen zien dat visual studio en postman die eerder bij de developer1 user elevation rights kregen nu in de “run & collect events” zitten wat betekent dat de policy van de developers niet applied op de sales gebruiker, het werkt al zoals verwacht.

4.3 Analyst policy

Als laatste maken we de ‘analyst policy’ aan. Ook deze krijgt “Elevate if necessary” maar dan toegepast op de Analyst application group.

This policy applies to activities that match the following definitions.
The "Elevate if necessary" action can be applied to all applications.

☐ All applications

Definition Type	Definition
Application group	Analyst

Figuur 26 Analyst application group koppelen aan de Analysts policy

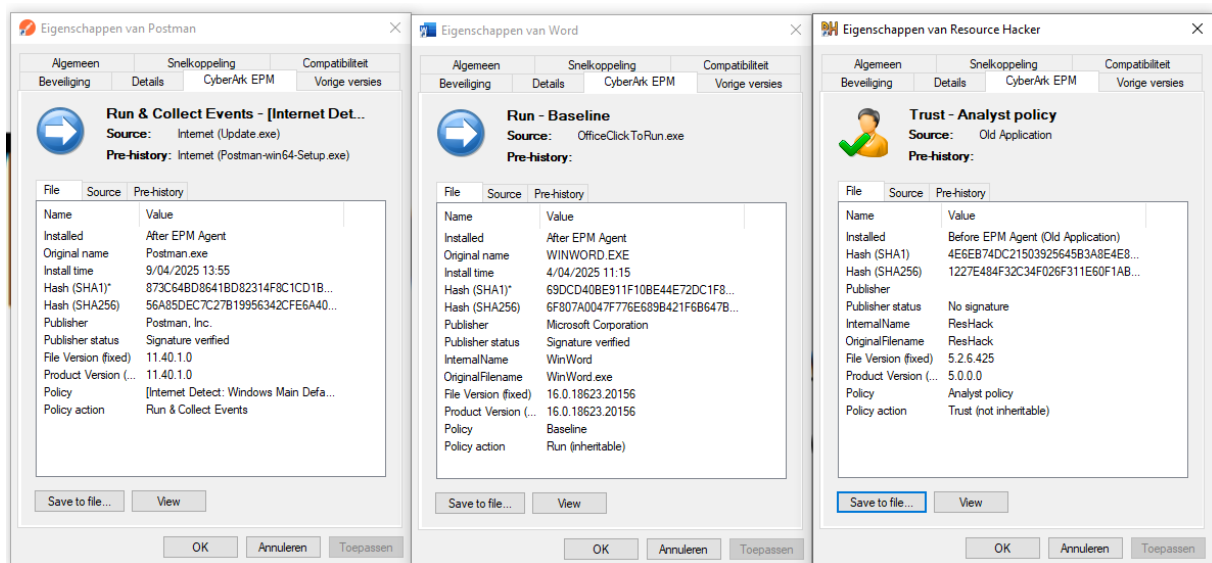
De target is de Analyst AD groep, deze policy geldt alleen voor users in de analysts active directory groep.

Targets

Apply policy to	Selected	
Computers in this set	All	Edit
Computers in AD security groups	All	Edit
Users and groups	Analysts	Edit

Figuur 27 Analysts AD groep koppelen aan de analysts policy

Als we op de analyst1 gebruiker inloggen kunnen we dit testen:

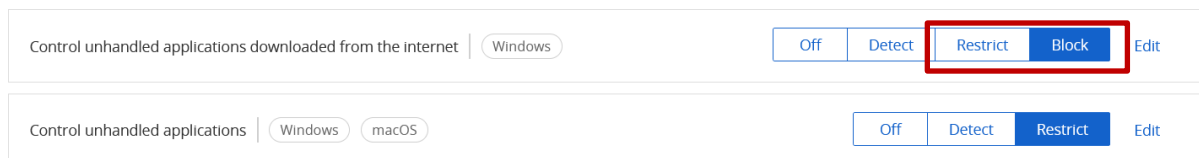


Figuur 28 Postman, Word en ResourceHacker CyberArk eigenschappen op Analyst1 user na de Analysts policy te creëren

Zoals te zien wordt word toegelaten door de "baseline" policy, Resource hacker een applicatie die in de analyst application groep zit mag worden uitgevoerd met elevated rechten indien nodig doordat de analyst policy hierop wordt toegepast, en postman heeft de "run & collect events" policy wat betekent dat de applicatie unhandled is voor de analyst user.

4.4 Block/restrict unhandled applicaties

De volgende stap is om de *unhandled applications* te blokkeren of te beperken. Als eerst heb ik dit toegepast op applicaties gedownload van het internet:



Figuur 29 Default policies



Figuur 30 Additional policies

Restrict vs Block

De volgende stap is om al de applicaties die *unhandled* zijn te restricten of blokkeren:

Restrict: Applicaties worden gelimiteerd wanneer ze *unhandled* zijn. Ze kunnen nog wel worden uitgevoerd, maar krijgen beperkte toegang tot bijvoorbeeld het internet, systeembestanden of adminrechten.

Block: applicaties worden volledig geblokkeert als ze *unhandled* zijn. Hier volg je de principle of zero trust, alleen applicaties die handled zijn voor gebruikers in de juiste AD met de juiste policy mogen die applicatie uitvoeren.

Voor de testfase heb ik ervoor gekozen om alle *unhandled applicaties* te blokkeren (zie figuur 30). Zo kunnen we controleren of onbekende applicaties correct worden herkend. In de finale fase, wanneer alles correct is geïmplementeerd, zal ik deze instelling terugzetten op Restrict, aangezien dit de standaardpraktijk is in realistische omgevingen.

4.5 Priorities

De lager de precedence number de hoger de prioriteit van de policy is:

- De *analyst* en *developers* policy hebben de hoogste prioriteit
- De *baseline* policy geldt voor alle gebruikers dus die heeft de laagste prioriteit

	Name	Action	Platform	Status	Type	Computers	Order of precedence ↑	La	
<input type="checkbox"/>	Analyst policy	Elevate if necess...	Windows	Active	Advanced	All	340	14	...
<input type="checkbox"/>	developers policy	Elevate if necess...	Windows	Active	Advanced	All	340	11	...
<input type="checkbox"/>	Baseline	Allow	Windows	Active	Advanced	All	420	10	...

Figuur 31 Analyst, Developers en Baseline policy prioriteiten

5.0 Tests

5.1 Test 1

- Gebruiker: salesuser1
- AD-groep: Sale

Testdoelen:

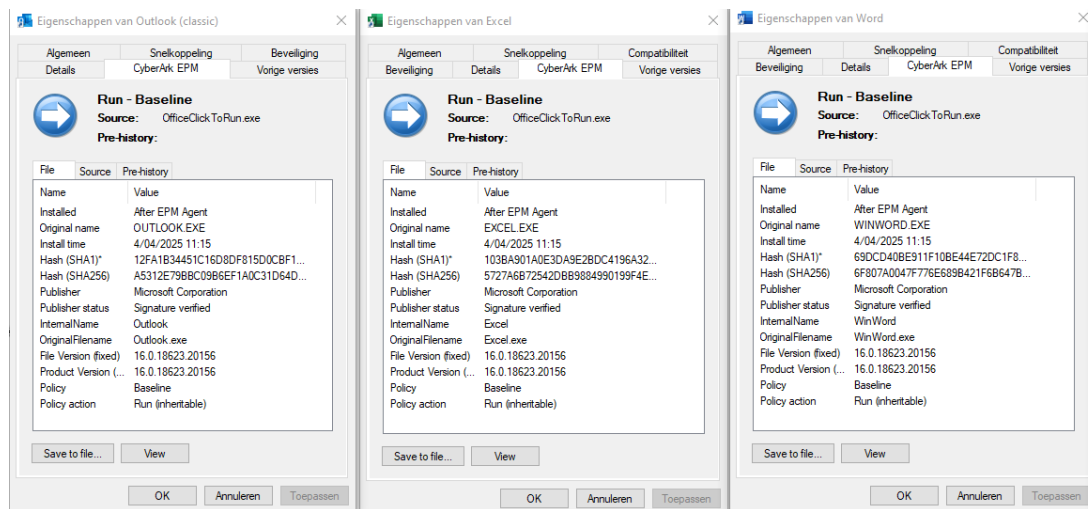
- Controleren of een gewone gebruiker nog steeds Office-apps kan gebruiken (Word, Excel, PowerPoint, etc.).
- Controleren of de *analyst* en *developer* applicaties geblokkeerd worden voor een gewone gebruiker.
- Controleren of *unhandled* applicaties worden geblokkeerd.

We gaan naar de volgende applicaties bekijken:

- Word, excel, outlook (baseline applicatie)
- Postman (developer applicatie)
- Resource Hacker (analyst applicatie)

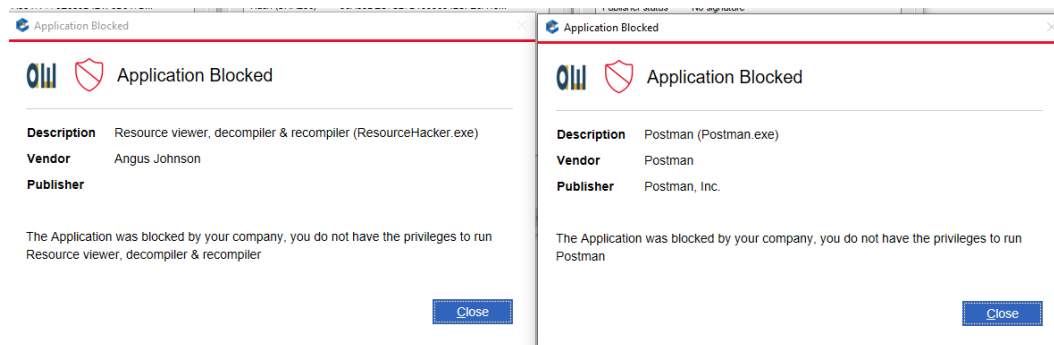
Daarnaast downloaden we Discord om te controleren of deze applicatie wordt geblokkeerd of nog uitvoerbaar is.

Zoals te zien in de onderstaande screenshot zijn al de apps in de *baseline policy* toegelaten:



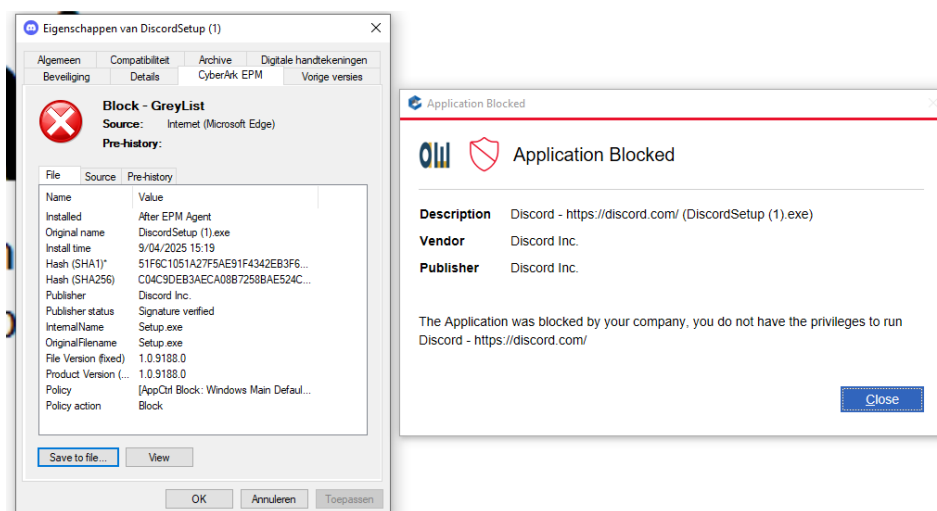
Figuur 32 Baseline policy test op de salesuser1user

Beide postman (developer application) en resource hacker (analyst application) worden geblokkeerd:



Figuur 33 Unhandled applicaties test op salesuser1

De discord installer wordt ook geblokkeerd sinds het een onbekende applicatie is:



Figuur 34 Applicatie van het internet testen

5.2 Test 2

- Gebruiker: developer1
- AD-groep: developers

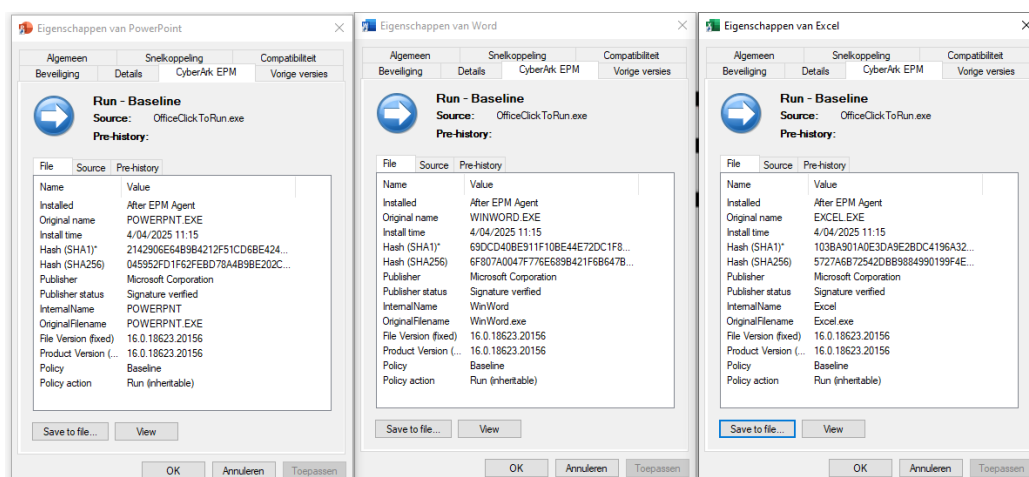
Testdoelen:

- Controleren of een developer gebruiker nog steeds Office-apps kan gebruiken (Word, Excel, PowerPoint, etc.).
- Controleren of een developer gebruiker developer-apps kan gebruiken (visual studio code, postman, mongodcompass, node.js ect.)
- Controleren of de *analyst* applicaties geblokkeerd worden voor een developer gebruiker.

We gaan naar de volgende applicaties bekijken:

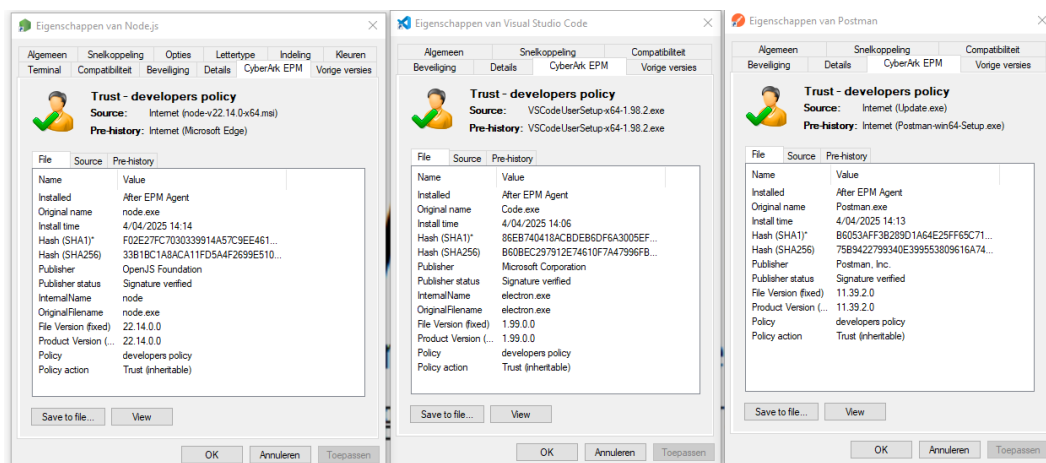
- Word, Excel, Powerpoint
- Visual studio code, node.js, postman (developer applications)
- Resource Hacker, wireshark (analyst applications)

Zoalste zien in figuur 35 kan de developer1 user alle baseline applicaties uitvoeren.



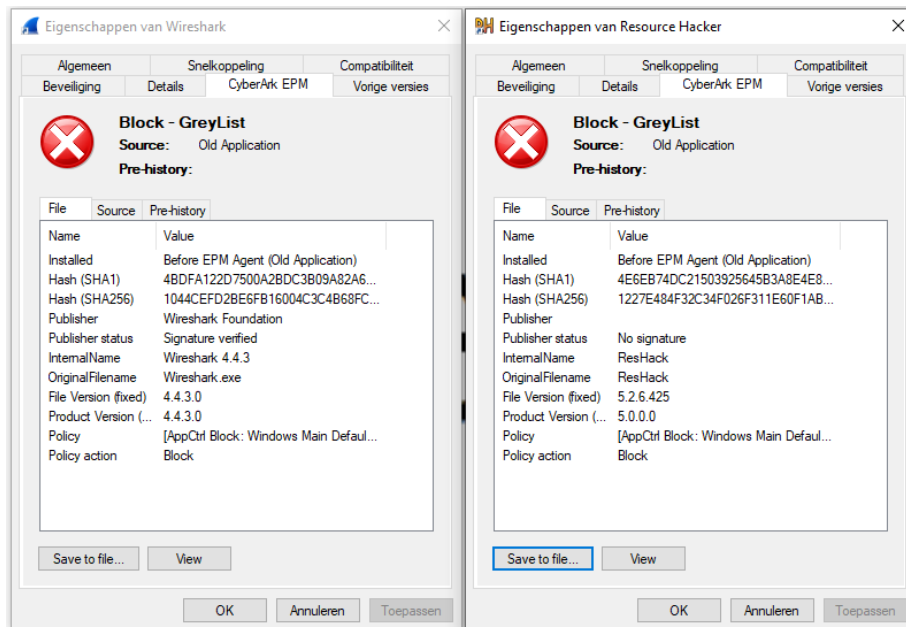
Figuur 35 Baseline policy test op de developer1 user

De developer1 user heeft ook de rechten om developer applicaties uit te voeren als administrator (zie figuur 36)



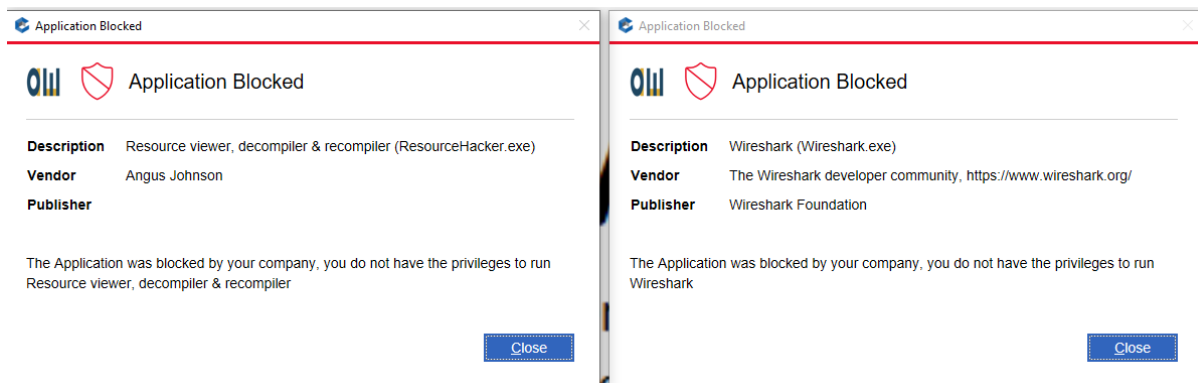
Figuur 36 Developers policy test op de developer1 user

Analyst applicaties worden ook geblokkeerd, zoals te zien in de onderstaande figuur zijn wireshark en resource hacker (beide analyst applications) op blocked.



Figuur 37 Unhandled applicaties test op de developer1 user

Als je deze probeert uit te voeren lukt het niet meer:



Figuur 38 Unhandled applicaties test op de developer1 user

5.3 Test 3

- Gebruiker: analyst1
- AD-groep: Analysts

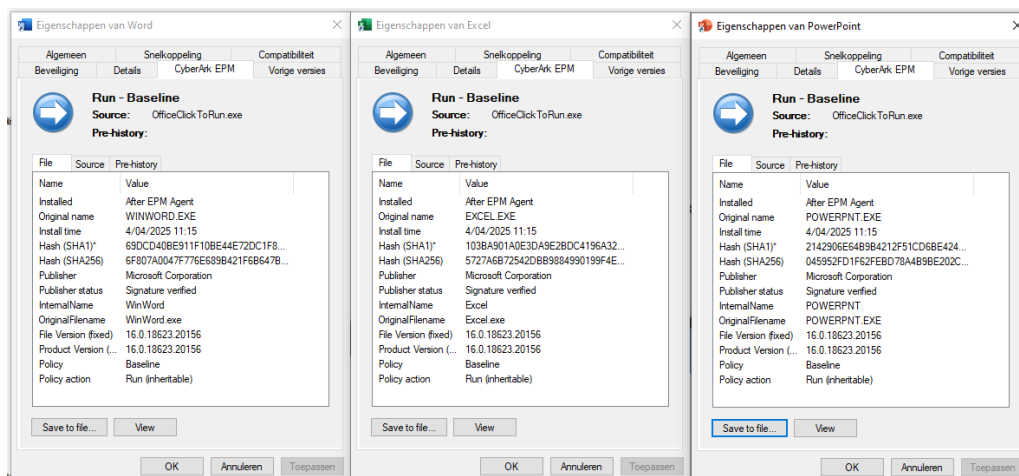
Testdoelen:

- Controleren of een analyst gebruiker nog steeds Office-apps kan gebruiken (Word, Excel, PowerPoint, etc.).
- Controleren of een analyst gebruiker analyst-apps kan gebruiken (Resource hacker, wireshark, procmon ect.)
- Controleren of de *developer* applicaties geblokkeerd worden voor een analyst gebruiker.

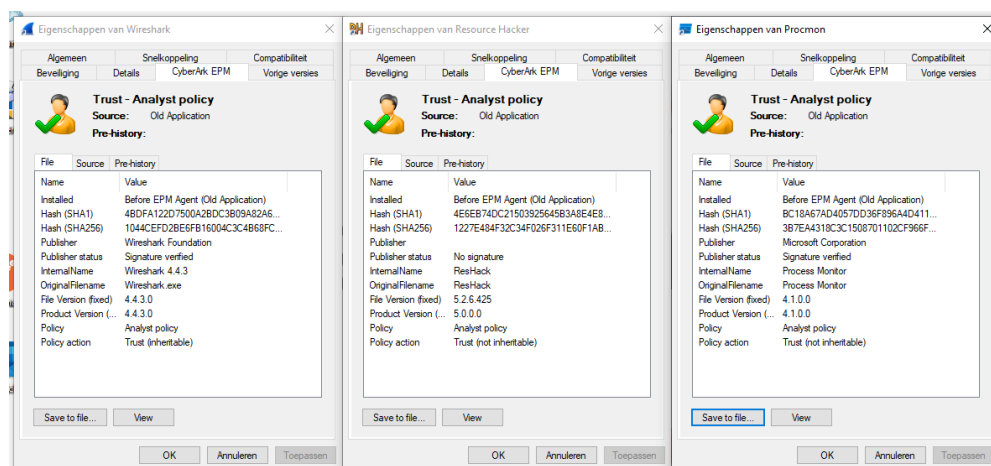
We gaan naar de volgende applicaties bekijken:

- Word, Excel, Powerpoint
- Resource Hacker, wireshark, procmon (analyst applications)
- postman (developer applications)

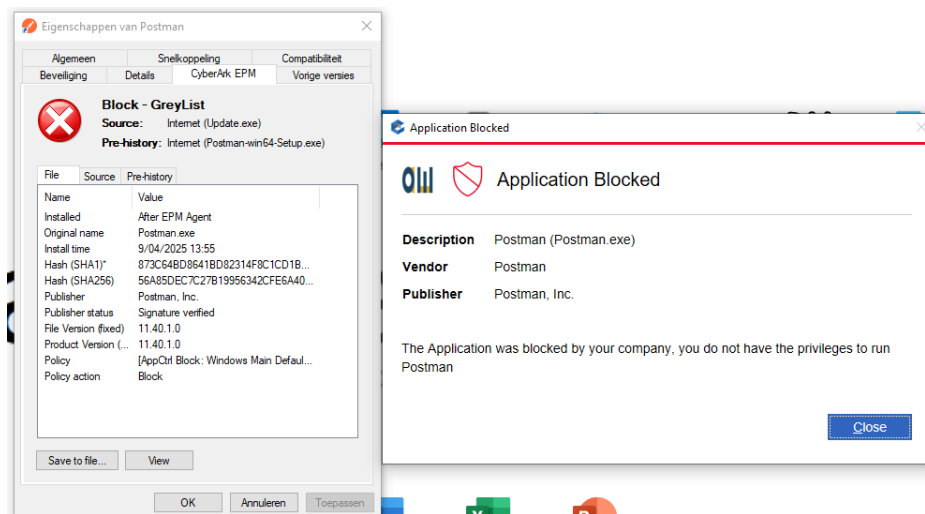
De baseline applicaties zijn uitvoerbaar op de analyst1 user (zie figuur 39).



Figuur 39 Baseline policy test op de analyst1 user



Figuur 40 Analyst policy test op de Analyst1 user



Figuur 41

Conclusie

De geteste policies werken zoals verwacht:

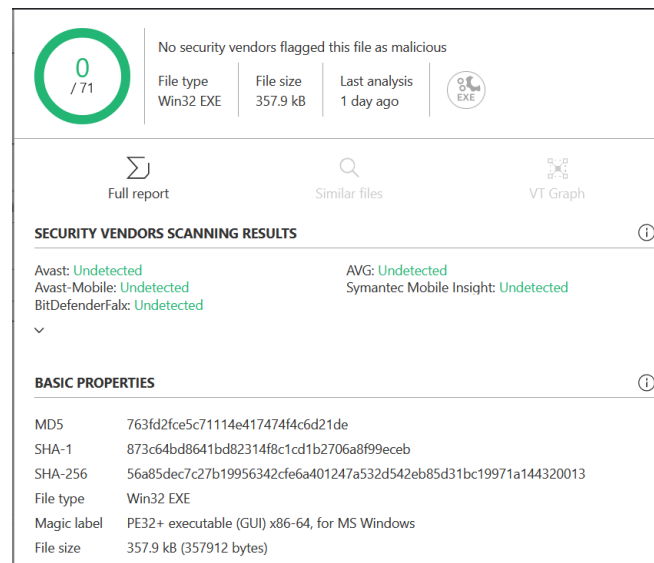
- Baseline apps zijn toegankelijk voor alle gebruikers.
- Developer apps zijn uitsluitend beschikbaar voor de developers.
- Analyst apps zijn uitsluitend beschikbaar voor de analysts.
- Onbekende applicaties worden op alle profielen correct geblokkeerd.

6.0 Extra Implementatie

6.1 Virus total integration

VirusTotal is een online tool die verdachte bestanden, URL's, IP-adressen en domeinen analyseert aan de hand van meer dan 70 antivirus-engines en diverse tools. Door gebruik te maken van de API van VirusTotal kan deze analyse geautomatiseerd worden binnen een beveiligingsomgeving.

In mijn project heb ik VirusTotal geïntegreerd met de CyberArk SaaS-omgeving. Wanneer een applicatie wordt gestart die nog niet gekend is binnen het beleid van EPM, wordt deze automatisch verzonden naar VirusTotal via een API en wordt de hash van de executable gecontroleerd.



Figuur 42 VirusTotal report in CyberArk EPM SaaS

Op basis van de respons van VirusTotal – die informatie bevat over detectieratio's, gedrag, reputatie en mogelijke indicatoren van compromittering – wordt een automatisch rapport gegenereerd. Dit rapport kan vervolgens gebruikt worden om een weloverwogen beslissing te maken binnen EPM: zoals het automatisch blokkeren van de applicatie, het plaatsen in een grijze zone voor verdere analyse, of het toestaan met beperkingen (zoals zonder netwerktoegang of zonder administratorrechten).

6.2 Protect against ransomware

De *CyberArk EPM Protect Against Ransomware*-policy is ontworpen om ongeautoriseerde toegang tot bestanden, netwerkshares en Windows processen te detecteren of blokkeren wanneer deze worden gebruikt door een onbekende applicatie.

Detect unauthorized access to sensitive files that match the following filename or location patterns

[Add filename](#) [Add location](#)

File pattern	Pattern type	
*.doc	Filename	
*.docx	Filename	
*.rtf	Filename	
*.xls	Filename	
*.xlsx	Filename	
*.ppt	Filename	
*.pptx	Filename	

Figuur 43 Ransomware protection gevoelige bronnen

Detect privileged unhandled applications | [Windows](#) [macOS](#) [Linux](#) [Off](#) [On](#) [Edit](#)

Protect against ransomware | [Windows](#) [Off](#) [Detect](#) [Restrict](#) [Edit](#)

Figuur 44 Ransomware protection op detect

Detect Mode:

- Enkel logging – laat ransomware toe, maar registreert verdachte toegangspogingen.
- *Dit wordt gebruikt in de testfase om te zien wat geblokkeerd zou worden.*

Restrict Mode:

- Blokkeert toegang van niet-goedgekeurde apps tot gevoelige bestanden én netwerkshares.
- *Dit wordt gebruikt in productie of tijdens de eindfase van mijn test om te bewijzen dat ransomware wordt gestopt.*

EPM maakt twee belangrijke groepen aan voor deze policy:

- Microsoft Windows Programs (*Default Policies*): Programma's die wél toegang mogen hebben (bv. verkenners, Word, cmd, PowerShell)
- Authorized Applications (*Ransomware Protection*): Andere vertrouwde apps die uitgesloten zijn van de policy (bv. eigen scripts/tools)

	Name	Type	Platform	Last modified ↓	
<input type="checkbox"/>	Microsoft Windows Programs (Default Policies)	Predefined	Windows	09:43:46	...
<input type="checkbox"/>	Authorized Applications (Ransomware protection)	Predefined	Windows	09:43:18	...

Figuur 45 Application groups aangemaakt door ransomware protection

In mijn setup heb ik alle applicaties van de baseline, developers en analysts *application groups* hier ook aan toegevoegd aangezien deze toegang moeten behouden tot resources.

Extensions

Extensions are applied to all Windows computers in this set

☒ Extend policy to disable changes to the Windows registry keys ⓘ

Add registry key

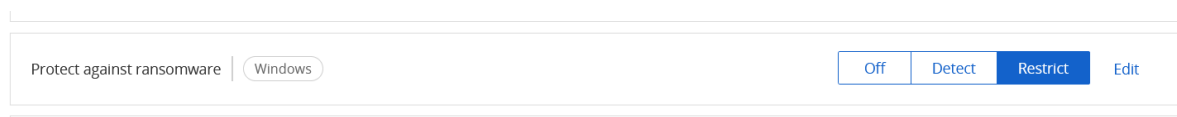
Registry key path	
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\16.0\Excel\Security	
HKCU\Software\Policies\Microsoft\Office\16.0\Outlook\Security	
HKCU\Software\Policies\Microsoft\Office\16.0\PowerPoint\Security	
HKCU\Software\Policies\Microsoft\Office\16.0\Publisher\Security	
HKCU\Software\Policies\Microsoft\Office\16.0\Word\Security	
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy	

Figuur 46 Windows Registry protection

De policy biedt ook de mogelijkheid om wijzigingen aan specifieke Windows registry keys te blokkeren. Ik heb hiervoor de volgende sleutels toegevoegd (zie figuur 46):

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy

Deze registrybescherming voorkomt dat ransomware via registrymanipulatie Windows Defender en Windows Firewall uitschakelt, wat een veelgebruikte techniek is.

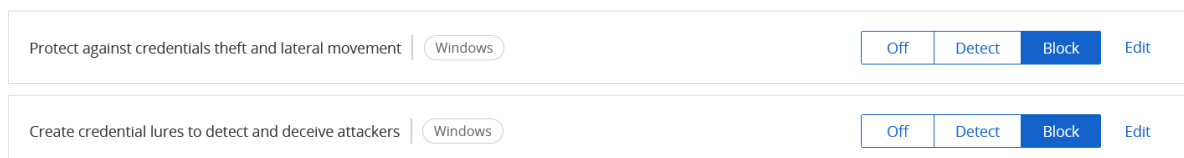


Figuur 47 Protect against ransomware policy

De volgende stap in mijn testprocedure was verifiëren of de Authorized Applications nog correct functioneren wanneer de policy in detect mode staat. Nadien heb ik de policy op restrict Mode gezet om de implementatie te finaliseren en voorbereid te zijn op de finale ransomwaretests.

6.3 Privilege Threat protection

Privilege Threat Protection



Figuur 48 privilege threat protection policies

In de *default policies* in de Cyberark EPM Manager kun je ook privilege threat protection inschakelen, er zijn 2 policies in privilege threat protection, “*protect against credential theft and lateral movement*”, en “*create credential lures to detect and deceive attackers*”, ik ga eerst credential theft en lateral movement configureren.

Name	Action	Platform	Computers
» Browsers Stored Credentials Theft	Block		All
» IT Application Credentials Theft	Block		All
» Remote Access Application Credentials Theft	Block		All
» Threat Protection	Block		All
» Windows Credentials Harvesting	Block		All

Figuur 49 “protect against credential theft and lateral movement” opties

Als je policies configureert om credential diefstal en laterale beweging te voorkomen heb je verschillende opties, een aantal zijn te zien in de bovenstaande figuur:

Optienaam	Beschrijving
Browsers Stored Credentials Theft	Detecteert diefstal van opgeslagen wachtwoorden in browsers zoals Chrome, Firefox en Edge.
IT Application Credential Theft	Detecteert diefstal van inloggegevens uit IT-tools zoals AWS, FileZilla, SQL en andere.
Remote Access Application Credential Theft	Detecteert credential diefstal uit toepassingen voor externe toegang zoals VNC, WinSCP en RDP.
Threat Protection	Beschermt tegen verdachte opstartverzoeken zoals safe modus of debugmodus.
Windows Credential harvesting	Detecteert technieken zoals SAM harvesting, NTDS.dit dumping, Pass-the-Hash (PtH) aanvallen, en LSASS credential harvesting.

» Windows Credentials Harvesting	All		
Credential Theft From Service Account	Block	Windows	02-Apr-2 ...
Credential Theft From Windows Credential Manager	Block	Windows	02-Apr-2 ...
Domain Credential Theft From Local Cache	Block	Windows	02-Apr-2 ...
Local Security Authority (LSA) Secrets Harvesting	Block	Windows	02-Apr-2 ...
LSASS Credentials Harvesting	Block	Windows	02-Apr-2 ...
Pass The Hash Attack	Block	Windows	02-Apr-2 ...
SAM Hash Harvesting	Block	Windows	02-Apr-2 ...

Figuur 50 Voorbeeld: “windows credential harvesting”

Een voorbeeld van enkele van deze policies is te zien in figuur 49. Deze policies zijn ingericht voor bescherming tegen *Windows Credential Harvesting*.

Met de policy *'Create Credential Lures to Detect and Decieve Attackers'* kan je valse inloggegevens (*lures*) instellen op strategische locaties zoals LSASS of in browserprofielen. Deze techniek heeft als doel aanvallers te verleiden om deze credentials te gebruiken, wat leidt tot detectie en blokkering van hun acties. Wanneer je deze policy configureert, zijn er verschillende soorten lures die je kunt inschakelen. De instellingen van deze policy zijn te zien in figuur 50 en de volgende tabel:

Soort Lure	Beschrijving
LSASS Lures	Maakt valse LSASS credentials aan die eruitzien als gevoelige accounts. Wanneer een aanvaller deze probeert uit te lezen (bijv. via Mimikatz), wordt dit gedetecteerd.
Browser Lures	Creëert nep-browsercredentials op opgegeven websites (bijv. https://login.gitlab.com/use met gebruikersnaam ServicesAdmin). Dit detecteert pogingen om opgeslagen wachtwoorden te stelen.

LSASS lures

☒ Create LSASS credential lures ⓘ

Set the admin username according to your organization naming convention ⓘ

actwiseBackupAdmin

Browser lures

☒ Create browser credential lures ⓘ

Set the website and its stored username for the lure ⓘ

Website address

<https://login.gitlab.com/use>

Username

ServicesAdmin

Figuur 51 *'Create Credential Lures to Detect and Decieve Attackers'* policy

Configuratie Samenvatting

- Baseline-applicaties zijn correct toegankelijk voor alle gebruikersgroepen.
- Developer-applicaties zijn enkel toegankelijk voor leden van de developers-groep.
- Analyst-applicaties zijn enkel toegankelijk voor leden van de analysts-groep.
- Onbekende en niet-goedgekeurde applicaties worden op consistente wijze geblokkeerd voor alle gebruikersgroepen.
- De VirusTotal-integratie zorgt voor een geautomatiseerde controle van onbekende bestanden.
- De *Ransomware Protection-policy* detecteert en verhindert pogingen om bestanden te versleutelen, Windows Processen te misbruiken en kritieke registersleutels aan te passen.
- De Privilege Threat Protection-polices zorgen voor detectie en preventie van credential harvesting en laterale beweging binnen het netwerk, met behulp van zowel bescherming als misleiding via credential lures.

7.0 Finale Tests

Commonly used

Additional

① Additional Privilege Management policies override commonly used Privilege Management policies for the same target computers and users

Detect privileged unhandled applications | Windows macOS Linux Off On Edit

Protect against ransomware | Windows Off Detect Restrict Edit

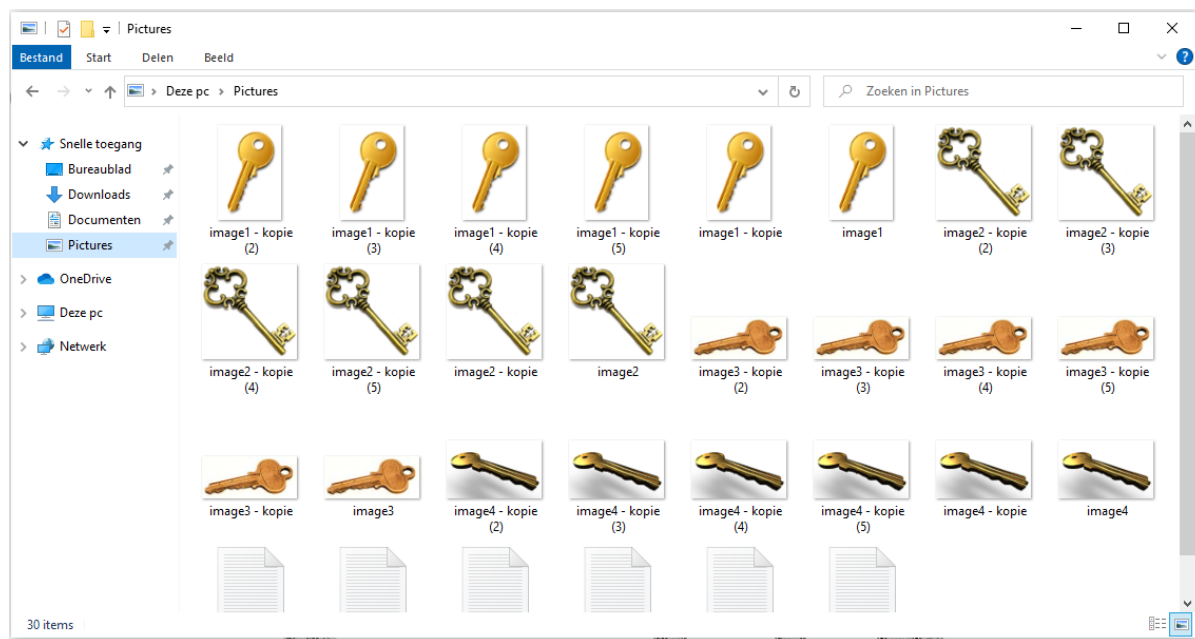
Control unhandled applications downloaded from the internet | Windows Off Detect Restrict Block Edit

Control unhandled applications | Windows macOS Off Detect Restrict Edit

Figuur 52 Default policies

Tijdens de finale tests wordt geëvalueerd of de implementatie van EPM effectief is in het tegenhouden van de ransomware-aanvallen die eerder in dit onderzoek zijn uitgevoerd zonder EPM. Daarnaast wordt nagegaan of onze zelfontwikkelde ransomware Proof of Concept (PoC) gedetecteerd wordt.

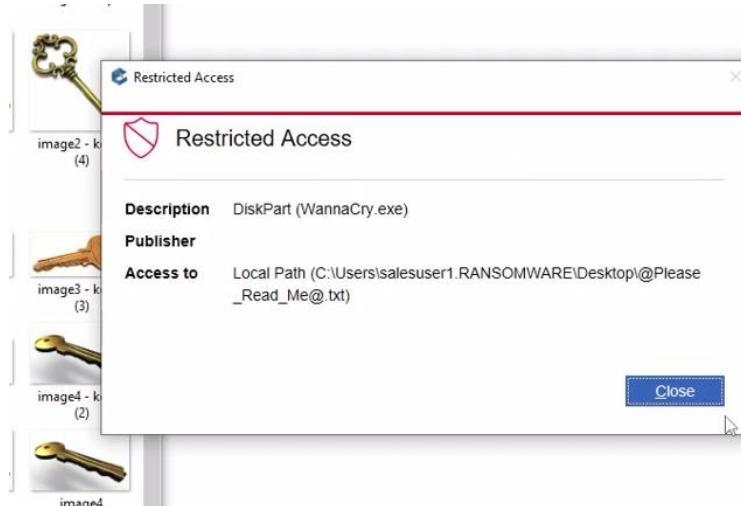
Voordat we de aanvallen opnieuw uitvoeren, heb ik het EPM-beleid op 'restrict mode' gezet om de implementatie af te ronden, dit is hoe het in productie zou gebeuren tijdens een implementatie. Op elke gebruikersaccount heb ik testbestanden aangemaakt, zoals foto's, geplaatst om te controleren of deze versleuteld worden. De testbestanden zien er als volgt uit:



Figuur 53 Files

7.1 WannaCry

- User: salesuser1
- ADgroep: Sales
- Toegepaste policies: 'baseline policy'



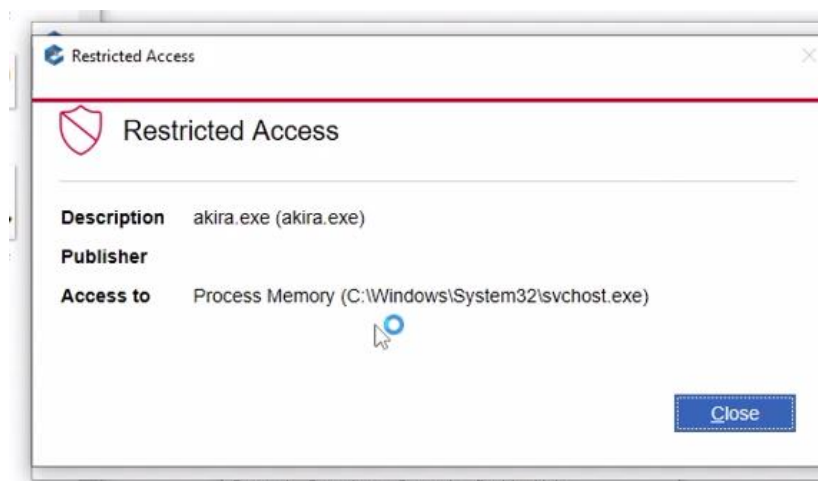
Figuur 54 WannaCry uitvoering na EPM implementatie

We starten met het uitvoeren van de WannaCry-ransomware. Zodra de ransomware wordt gestart, verschijnt er onmiddellijk een pop-upmelding van CyberArk EPM. Deze melding geeft aan dat de applicatie probeert toegang te krijgen tot een pad waarvoor geen toestemming is verleend. Uit de observatie blijkt dat WannaCry op dat moment een ransomnote aanmaakt en vervolgens probeert deze te wijzigen. De EPM-policy "protect against ransomware" grijpt echter in en blokkeert toegang tot alle soorten bestanden wanneer de applicatie als *unhandled* wordt beschouwd. Hierdoor wordt de aanval effectief onderbroken voordat de encryptiefase kan plaatsvinden.

Video:

7.2 Akira

- User: salesuser1
- ADgroep: Sales
- Toegepaste policies: 'baseline policy'



Figuur 55 Akira uitvoering na EPM-implementatie

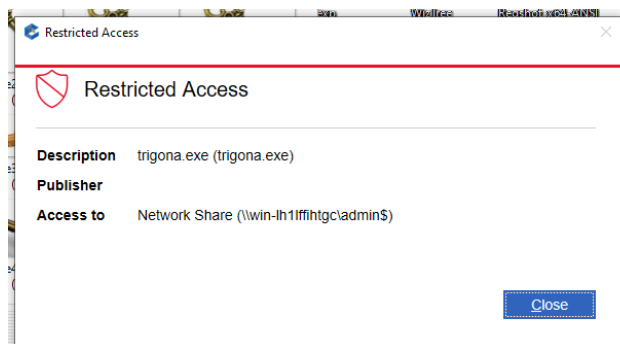
De volgende ransomware die we uitvoeren is de Akira-ransomware. Deze heb ik getest door deze uit te voeren met administratorrechten als *salesuser1*. Zelfs met deze verhoogde rechten slaagt Akira er niet in om het systeem succesvol te versleutelen.

Bij uitvoering verschijnt onmiddellijk een melding van CyberArk EPM waarin wordt aangegeven dat de applicatie probeert toegang te krijgen tot een Windows-proces (zie figuur 54). Aangezien Akira nog niet door een specifieke policy is behandeld, wordt deze als *unhandled* beschouwd. Volgens de policy die ik heb ingesteld mogen *unhandled* applicaties geen toegang krijgen tot Windows processen, waardoor de aanval wordt geblokkeerd. Als gevolg hiervan blijven alle bestanden intact en is er geen encryptie plaatsgevonden.

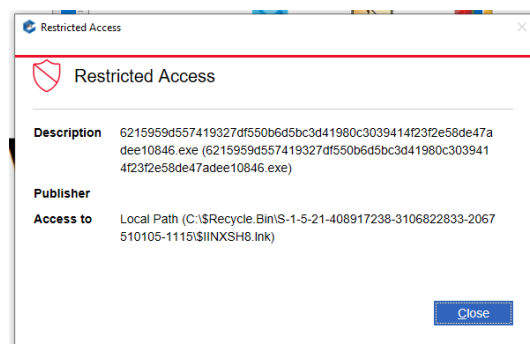
Video:

7.3 Trigona

- User: Analyst
- ADgroep: Analysts
- Toegepaste policies: *'baseline policy'* en *'analyst policy'*



Figuur 56 Trigona uitvoering na EPM-implementatie



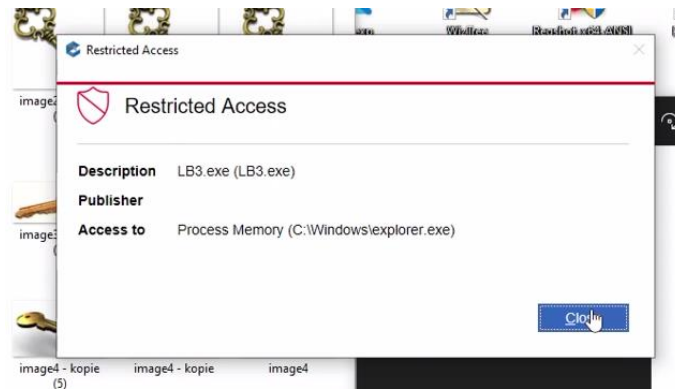
Figuur 57 Trigona uitvoering na EPM-implementatie

Tijdens de uitvoering van Trigona onderneemt de ransomware meerdere pogingen om toegang te krijgen tot gevoelige locaties. De eerste poging richt zich op een netwerkshare (\\win-lh1fl1fhtgc\admin\$), die geblokkeerd wordt dankzij de toegepaste policies. Vervolgens probeert een willekeurig proces toegang te krijgen tot de Recycle Bin (C:\\$Recycle.Bin). Beide pogingen worden door EPM herkend als verdacht gedrag van een *unhandled application*, en worden effectief tegengehouden. Dit voorkomt dat Trigona zijn kwaadaardige activiteiten kan voortzetten. Alle bestanden blijven onaangetast, en er is geen encryptie opgetreden.

Video:

7.4 LockBit

- User: Developer1
- AD groep: developers
- Toegepaste policies: *'baseline policy'* en *'developers policy'*

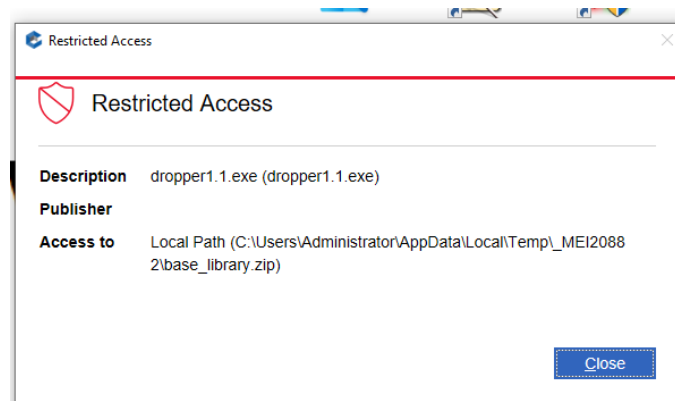


Figuur 58 LockBitV3 uitvoering na EPM-implementatie

Bij het starten van LockBitV3 wordt onmiddellijk een poging ondernomen om toegang te krijgen tot het geheugen van het proces explorer.exe. CyberArk EPM detecteert deze actie direct en toont een “Restricted Access”-melding. Omdat LB3.exe wordt beschouwd als een *unhandled application*, wordt de toegang tot systeempromessen geweigerd. Deze blokkade verhindert verdere verspreiding of encryptie door de ransomware. Uit systeemcontrole blijkt dat alle bestanden onaangetast zijn gebleven.

7.5 PoC ransomware

- User: Analyst1
- AD groep: Analysts
- Toegepaste policies: ‘baseline policy’ en ‘analyst policy’



Figuur 59 PoC ransomware uitvoering na EPM-implementatie

Tijdens de uitvoering van onze zelfontwikkelde Proof of Concept (PoC) ransomware wordt een poging ondernomen om toegang te krijgen tot een tijdelijk bestand (base_library.zip) in de lokale gebruikersmap. CyberArk EPM detecteert deze poging onmiddellijk en toont een “Restricted Access”-melding (zie figuur 58).

Het executable bestand dropper1.1.exe is gemaakt met PyInstaller, een tool waarmee Python-scripts worden omgezet naar standalone .exe-bestanden. Tijdens de uitvoering van een PyInstaller-executable wordt een tijdelijke werkomgeving aangemaakt in de map AppData\Local\Temp_MEIxxxx, waarin onder andere de Python-runtime en vereiste bibliotheken worden uitgepakt. Omdat dropper1.1.exe niet expliciet wordt vertrouwd en als een *unhandled application* wordt beschouwd door het ingestelde EPM-policy, wordt de toegang tot deze bestanden direct geblokkeerd. Hierdoor wordt de uitvoering van de PoC ransomware stopgezet nog vóór deze schadelijke acties kan ondernemen, zoals encryptie of antivirus uitschakelen.

Uit controle blijkt dat alle testbestanden intact zijn gebleven en dat geen enkele versleuteling of wijziging heeft plaatsgevonden. Dit toont aan dat de ingestelde EPM-politcies ook effectief zijn tegen nieuwe, onbekende dreigingen zoals onze zelfontwikkelde PoC.

8.0 Conclusie

Uit dit onderzoek blijkt dat CyberArk Endpoint Privilege Manager (EPM) een goede oplossing is voor het detecteren en blokkeren van ransomware-aanvallen binnen een bedrijfsomgeving. Door verschillende ransomwarevarianten — WannaCry, Akira, Trigona en LockBitV3 — uit te voeren onder verschillende Active Directory-gebruikers, werd aangetoond dat EPM telkens vroeg tussenkomt om kwaadaardige acties te blokkeren, nog vóór de encryptiefase kan plaatsvinden. Daarnaast werd ook mijn zelfontwikkelde Proof of Concept (PoC) ransomware effectief tegengehouden. De resultaten tonen aan dat EPM:

- zelfs nieuwe, onbekende ransomware wordt geblokkeerd;
- gebruikersdata blijft volledig intact;
- aanvallen met verhoogde rechten worden zelfs geblokkeerd;

Besluit: CyberArk EPM vormt een robuuste verdedigingslaag tegen ransomware-aanvallen, zonder de gebruikservaring van eindgebruikers onnodig te beperken. Door nauwkeurige beleidsconfiguraties te combineren met krachtige detectie- en blokkeermogelijkheden, biedt EPM een evenwichtige oplossing tussen veiligheid en gebruiksgemak. Dit onderzoek toont aan dat een correcte implementatie van EPM het risico op dataverlies en systeemcompromittering aanzienlijk vermindert, en bijgevolg een waardevolle meerwaarde biedt voor organisaties die hun endpoints willen beschermen tegen geavanceerde bedreigingen.

Bronvermelding