AP HOGESCHOOL ANTWERPEN

OCTWISE

Bachelor in de

Elektronica – ICT/TI

Documentatie – Implementatie Van CyberArk EPM

Luka Wynants

Begeleider: Similon Andie
Mentor: Verreth Jelle

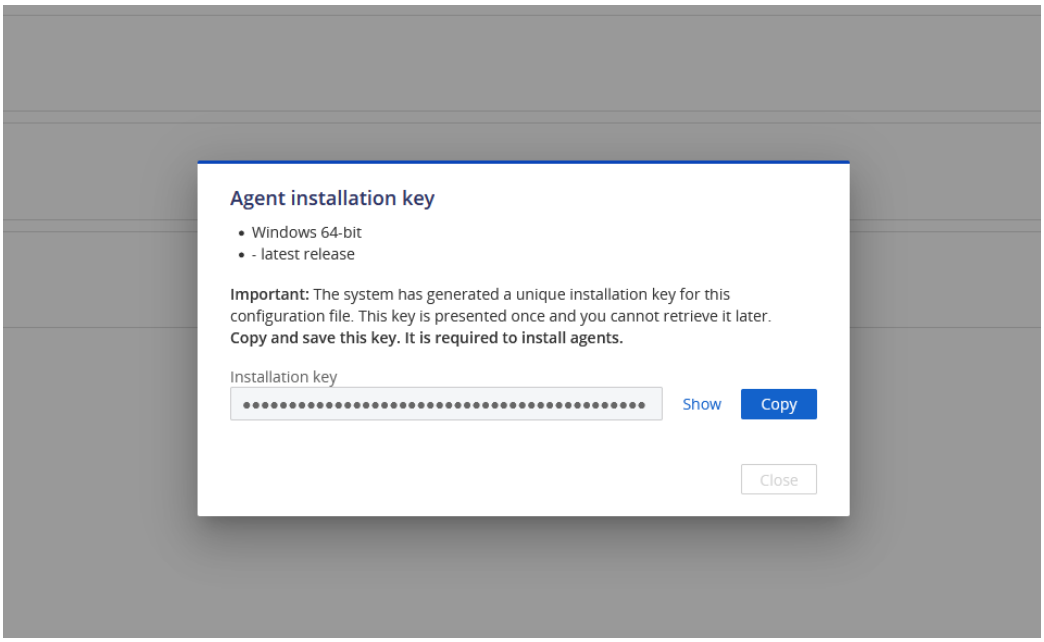
Academiejaar 2024-2025
2de semester

Contents

1.0 EPM-installatie

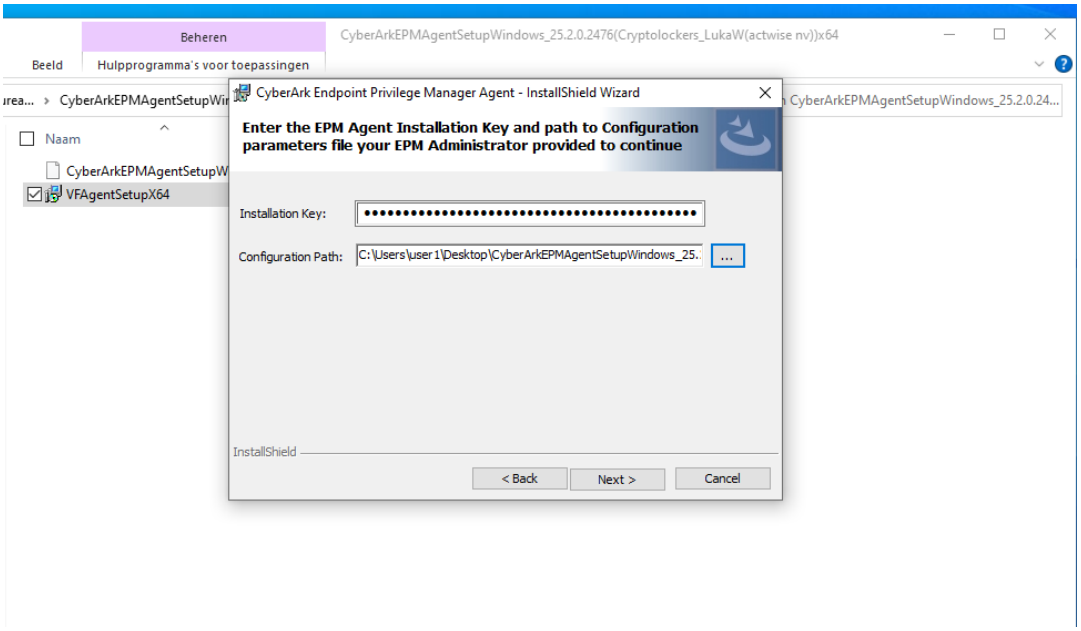
1.1 EPM-Agent installatie

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 1Agent installatie sleutel

Tijdens de installatie op de endpoint wordt er gevraagd achter de installation key:

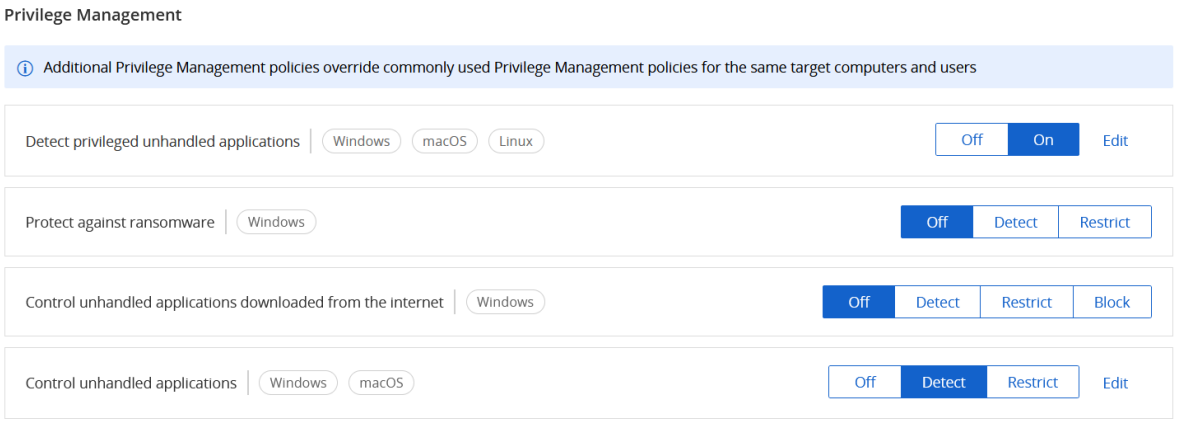


Figuur 2 Agent installatie op windows 10

2.0 EPM-configuratie

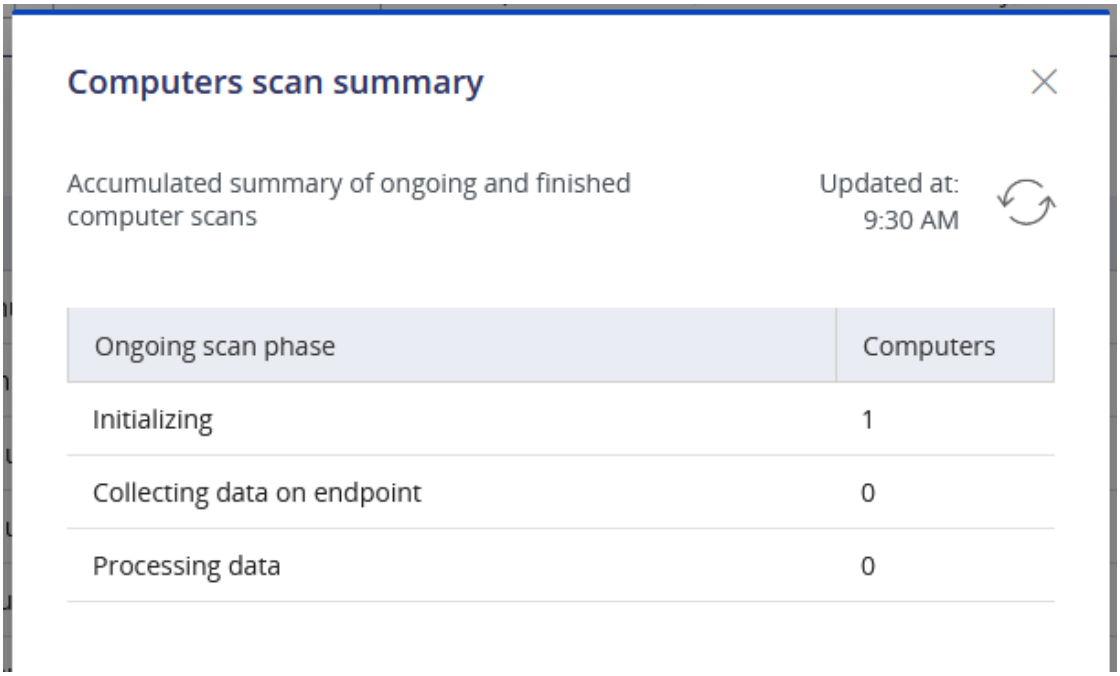
2.1 Monitoring fase

De eerste stap in EPM is de monitoringsfase. Hier wordt 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.



Figuur 3 Default Policies

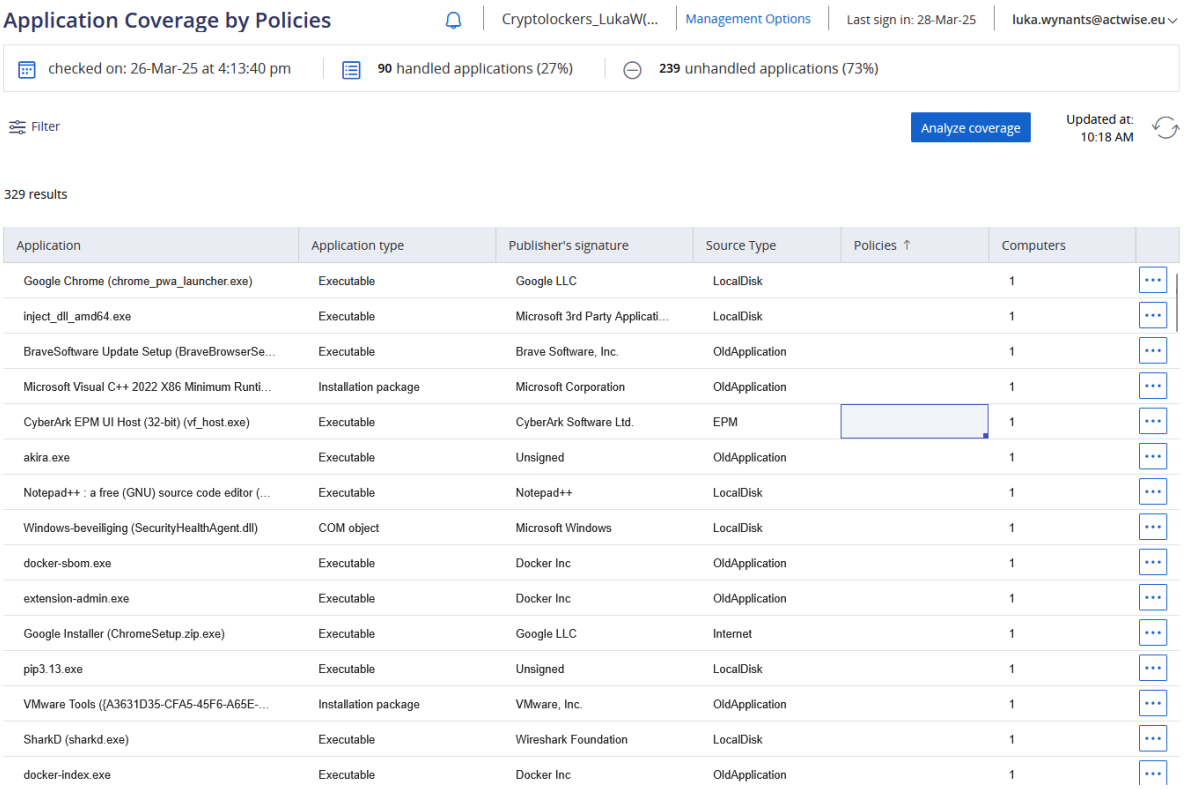
Om ongecontroleerde applicaties te detecteren, moet je de policy "Detect privileged unhandled applications" op "on" zetten en "Control unhandled applications" op "detect". Hierdoor worden events gegenereerd en worden nieuwe of bestaande applicaties gelogd in de *application catalogue*. Je kunt ook specifieke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



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	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

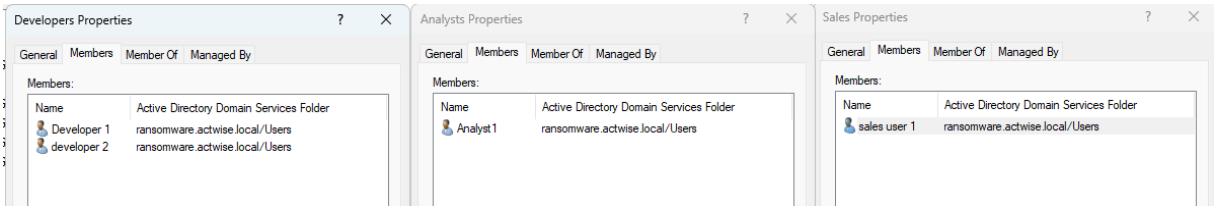
Figuur 5 Application catalogue

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 ontwikkelapplicaties gebruiken
- Malware Analysts – mogen analyst-applicaties gebruiken

In de onderstaande figuur kan je de Active Directory domeingroepen 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*. Best practice is 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.

De volgende *application groups* heb ik 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, Yahoomail
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,
Zipping	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 mogen worden gebruikt. Denk hierbij aan 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

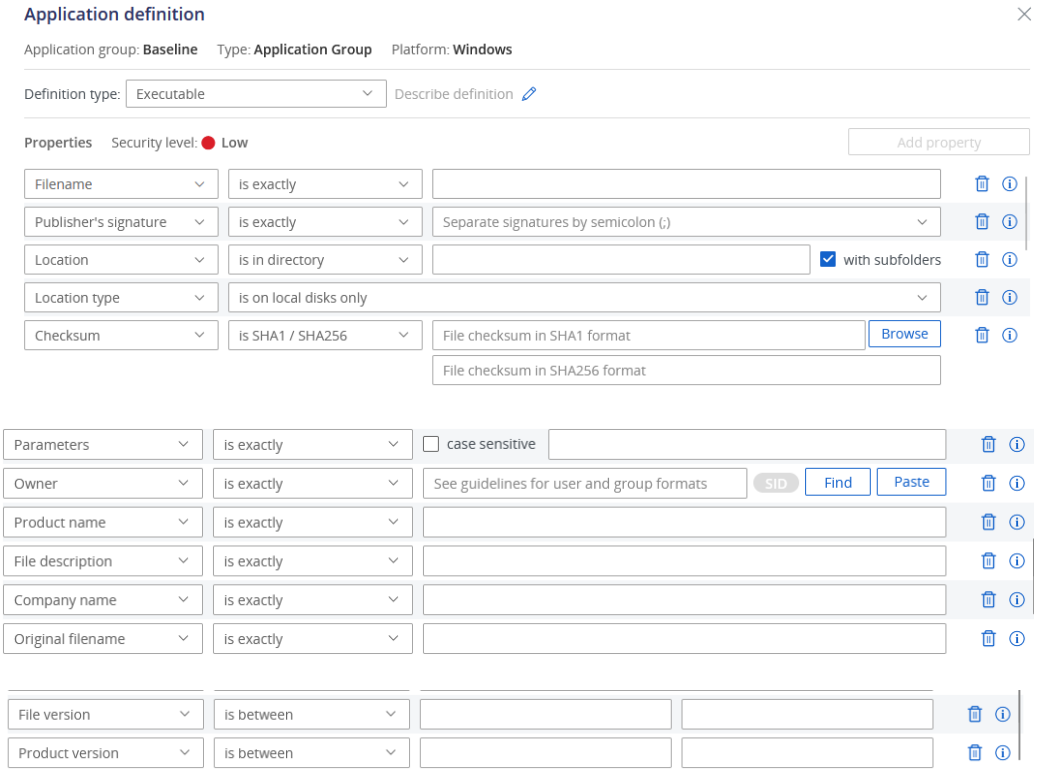
Malware Analysts application group – een groep van tools die uitsluitend door malware-analisten mogen worden gebruikt. Deze bevatten bijvoorbeeld tools voor procesanalyse, netwerkverkeerinspectie of reverse engineering.

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 defintition 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.



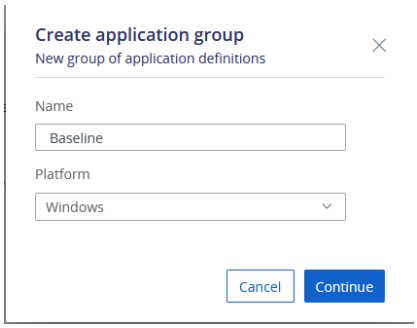
Figuur 10 Application definition opties

Voor mijn implementatie maak ik vooral gebruik van de volgende identificatiecriteria:

- *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 consistenter 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 aangepast wordt, en is dus een zeer nauwkeurige methode om specifieke versies van applicaties te identificeren.

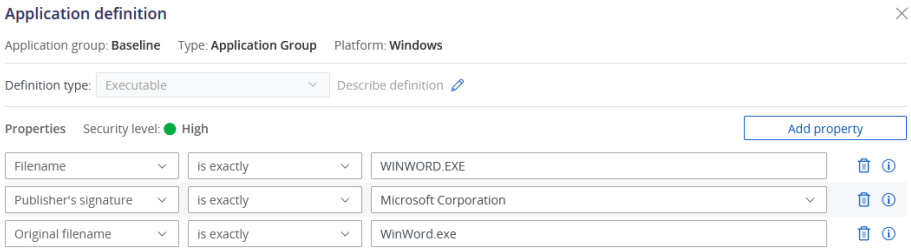
In mijn configuratie ga ik voornamelijk de Publisher Signature combineren met de Original Filename en Filename. De reden hiervoor is dat de Publisher Signature vrijwel onmogelijk te vervalsen is, aangezien deze is ondertekend door een Trusted Certificate Authority (CA) met een private key. Dit biedt een hoge mate van betrouwbaarheid bij het onderscheiden van legitieme software. In sommige gevallen heeft een legitieme applicatie echter geen digitale handtekening (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 wijzigt, waardoor deze methode minder flexibel is bij updates of 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:

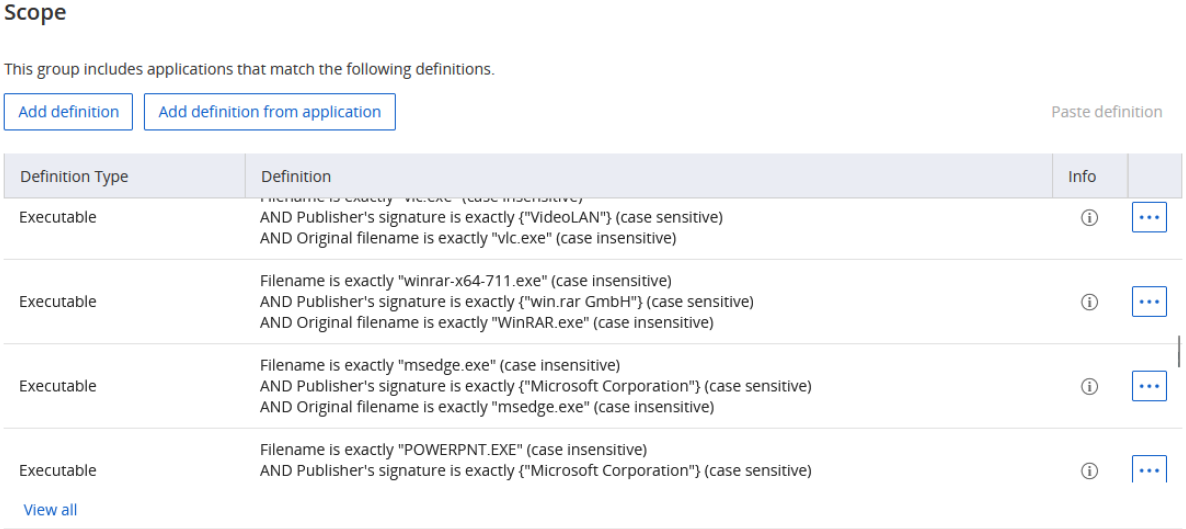


Figuur 12 Application definition van word

Zoals te zien in de eigenschappen van Word:

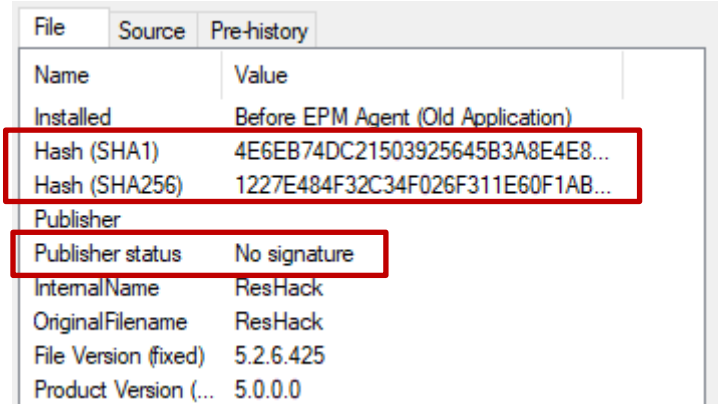
- *De Original Filename* is "WinWord.exe"
- De *Filename* is "WINWORD.EXE"
- De *Publisher Signature* moet overeenkomen met die van Microsoft

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

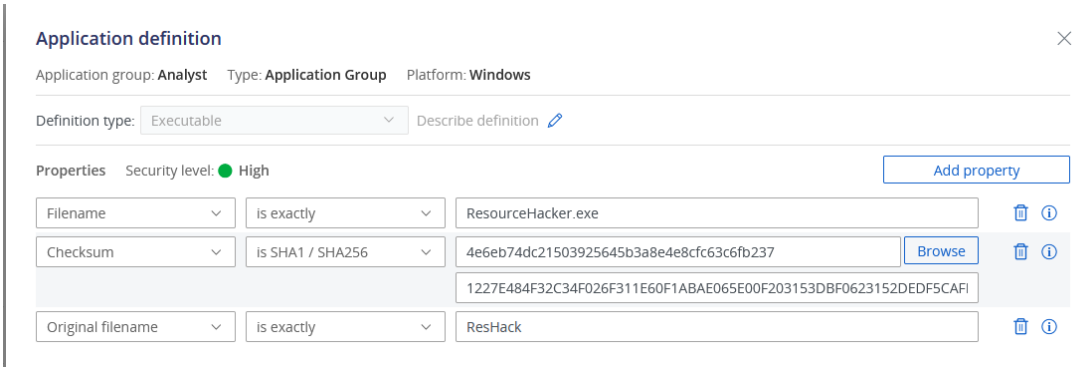


Figuur 13 Baseline Application group scope

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.

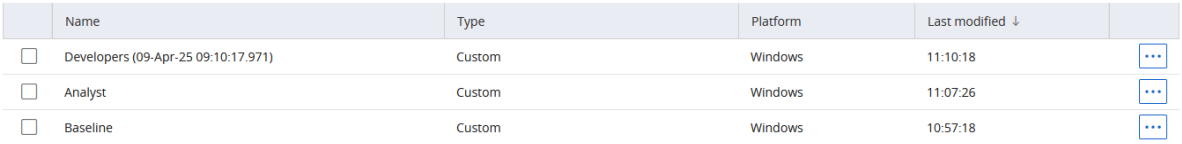


Figuur 14 SHA1 en SHA256 van een bestand en Publisher van resource hacker



Figuur 15 Application definition van resource hacker

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



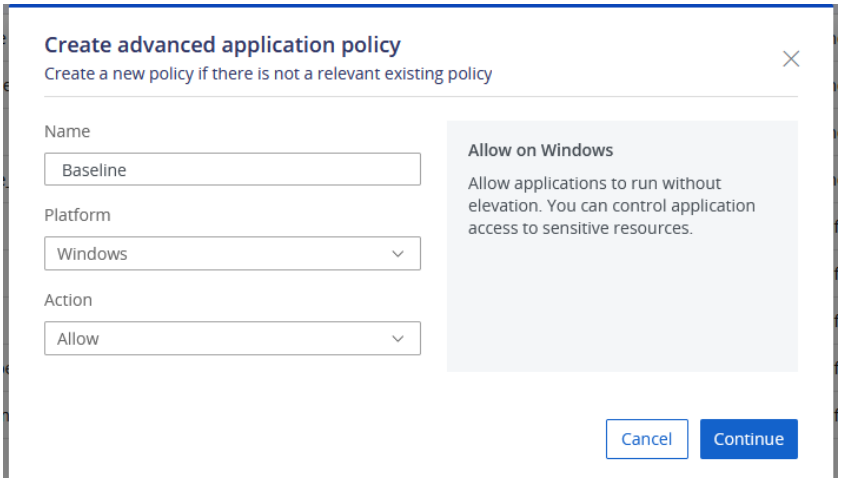
Figuur 16 Developers, Analyst en Basline application groups

4.0 Policies creëren

nu heb ik mijn basis apps gedefineert in application groups, de volgende stap is policies definieren voor deze application groepen en ze toewijzen aan een AD groep.

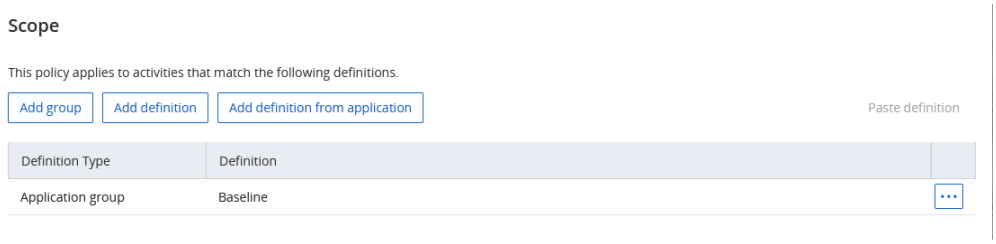
4.1 Baseline policy

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



Figuur 17 Baseline policy aanmaken

De scope is de *Baseline application group.*

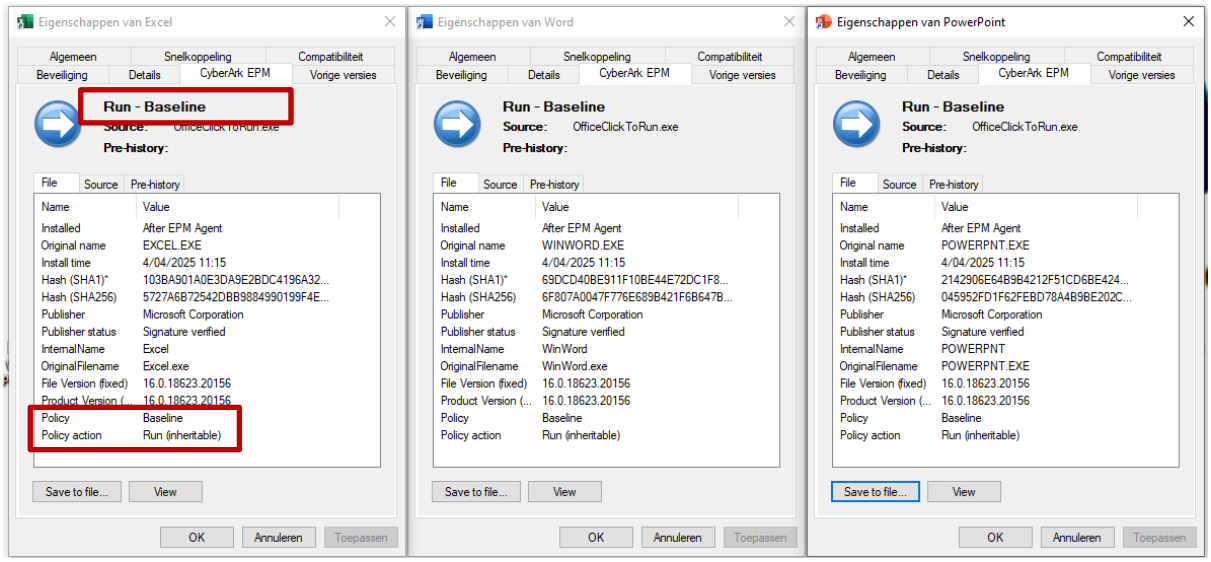


Figuur 18 Basline application groep koppelen aan de baseline policy

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

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

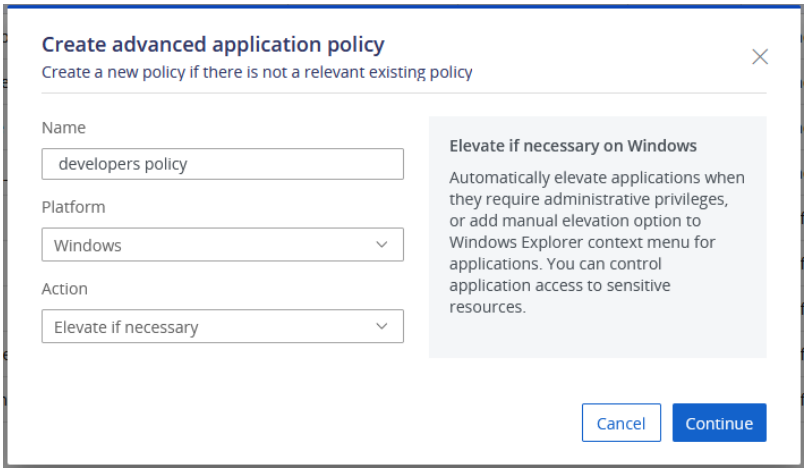
Zoals te zien in de eigenschappen van Word wordt nu onder “Policy” getoond dat de baseline policy is toegepast op deze applicatie. Je kunt ook zien dat deze applicatie mag worden uitgevoerd. Dit geldt voor alle applicaties in de *application group* “Baseline”.

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:

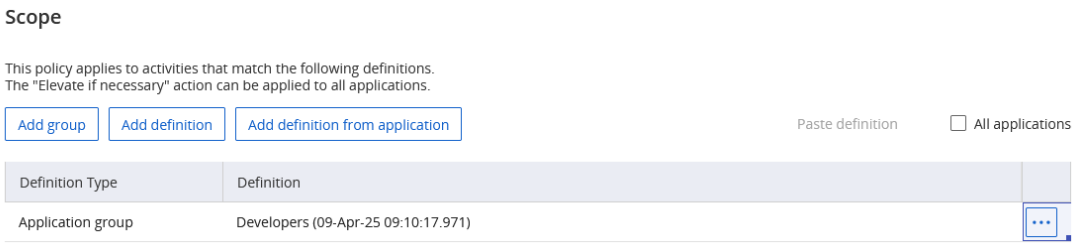
- De gebruiker zelf krijgt geen administratorrechten
- De applicatie krijgt tijdelijk de benodigde rechten
- EPM voert de elevation op de achtergrond uit, zonder dat het account van de gebruiker verandert
- Zodra de actie klaar is, verdwijnen de elevated rechten weer

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.

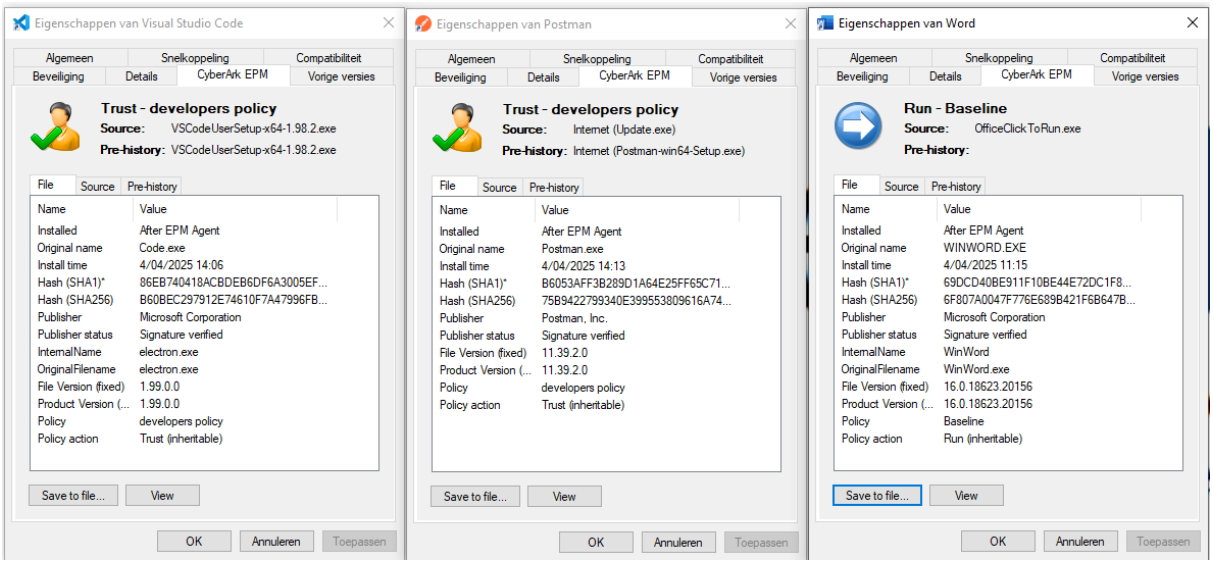


Figuur 22 Developers application group koppelen aan de developer's policy

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

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

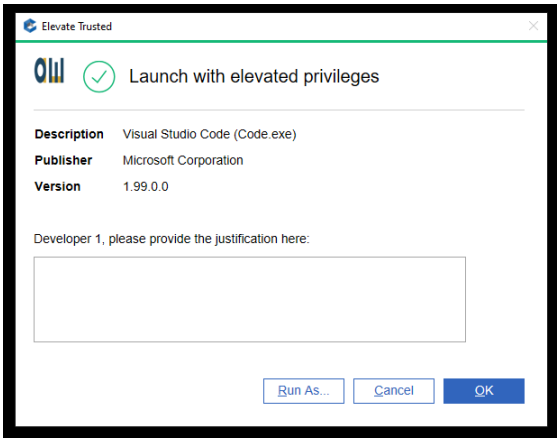
Als we dit testen op een gebruiker die in de developers AD groep zit zien we dat de applicaties van de developer application groep nu de Trust policy hebben gekregen van de developers policy.



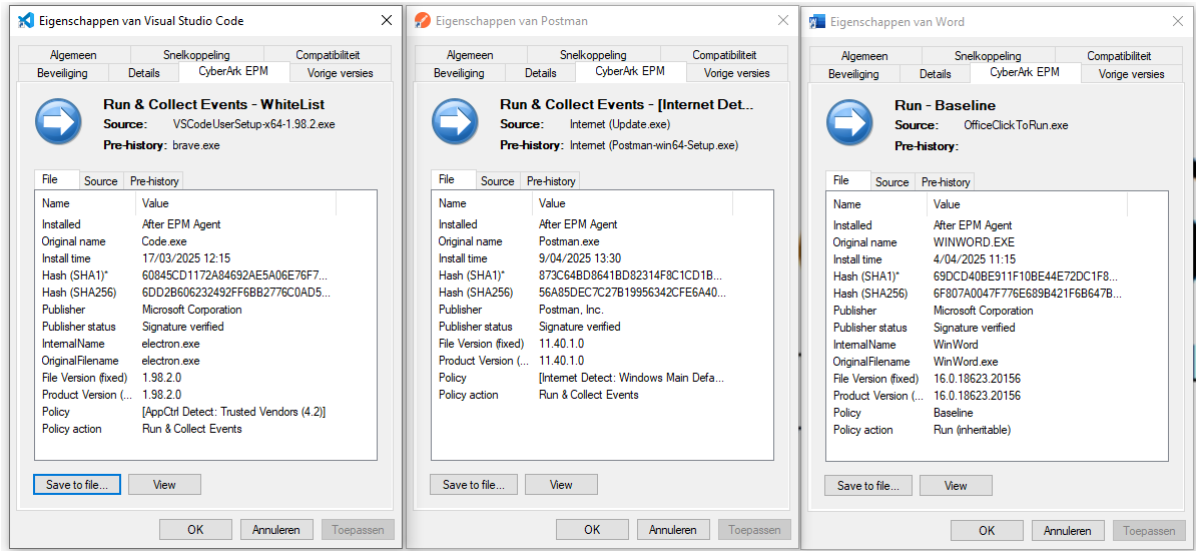
Figuur 24 VSCode, Postman en word CyberArk eigenschappen op developer1 user na de developer's policy te creëren

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.

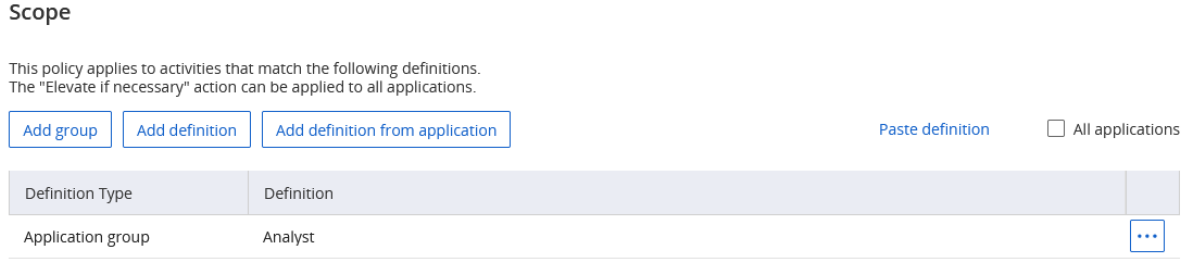


Figuur 25 VSCode, Postman en word CyberArk eigenschappen op salesuser1 user na de developer’s policy te creëren

We kunnen zien dat visual studio en postman die eerder op 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*.



Figuur 26 Analyst application group koppelen aan de Analysts policy

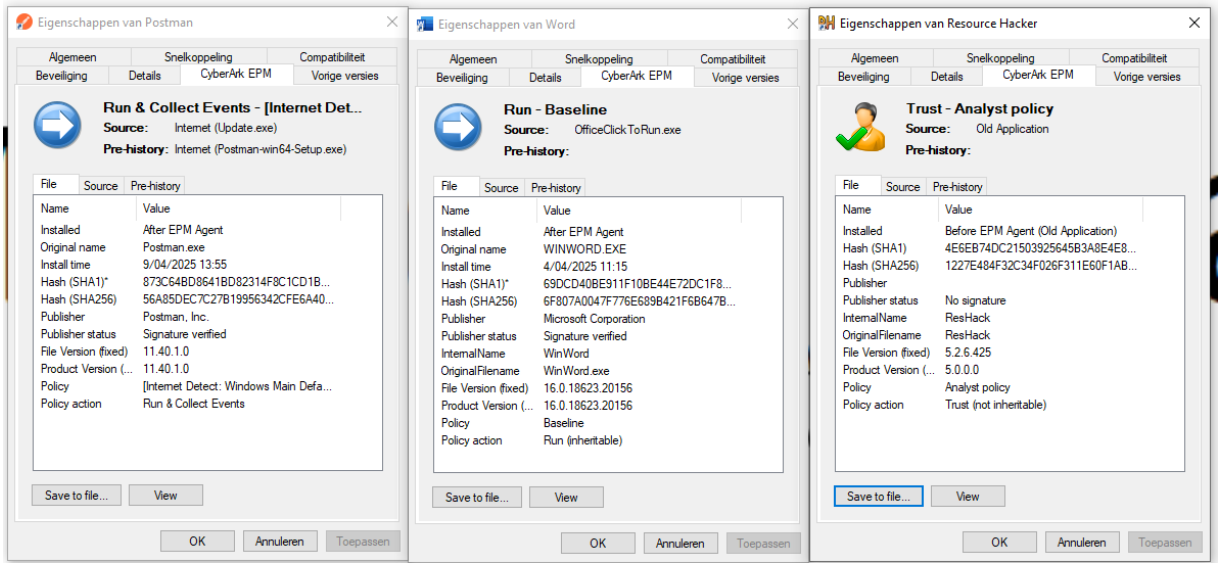
De target is de Analyst AD groep, dus deze policy geld alleen voor users in de analysts ad groep

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:

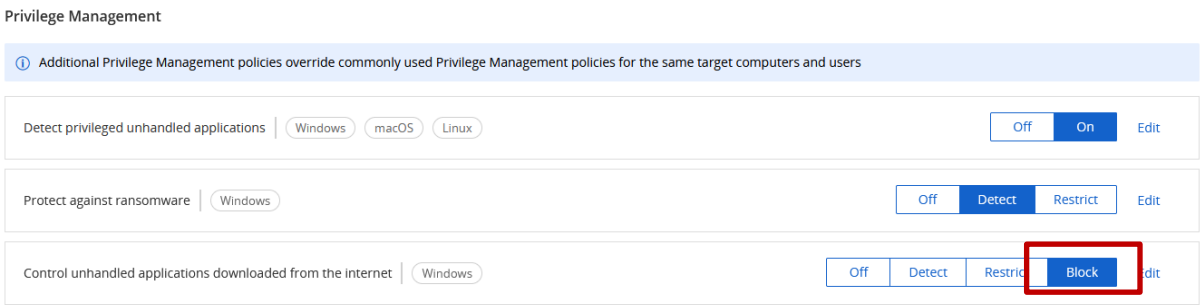


Figuur 28 Postman, Word en ResourceHacker CyberArk eigenschappen op Analyst1 user na de Analysts policy te creëren

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 betekend dat de applicatie unhandeled is voor de analyst user.

4.4 Block unhandled applicaties

De volgende stap is om de unhandled applicaties te blokkeren, als eerst willen we dit toepassen op applicaties gedownload van het internet:



Figuur 29 Default policies

Door de policy “control unhandled applications downloaded from the internet” op “block” te zetten zouden nu alle applicaties die unhandled zijn door een policy geblokkeerd worden, we kunnen dit testen door een postman uit te voeren op een gebruiker die niet in de “developers” AD groep zit. Postman is gedownload van het internet en is unhandled tenzij je in de AD groep developers zit.

Restrict vs Block

De volgende stap is om al de applicatie 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.

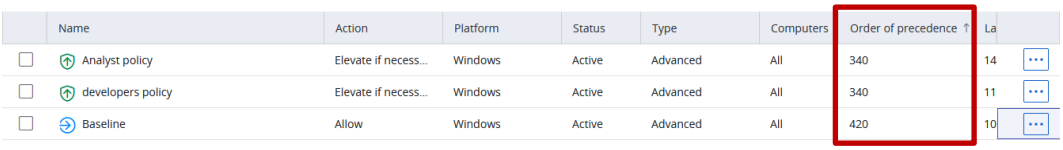
Block: applicaties worden volledig geblokkeert als ze unhandled zijn. Hier volg je de principle of zero trust, alleen applicaties die handled zijn voor gebruikers in de juiste AD met de juiste policy mogen die applicatie uitvoeren.

Voor de testfase heb ik ervoor gekozen om alle unhandled applicaties te blokkeren. 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 Prioraties

De lager de precedence number de hoger de prioriteit van de policy is: [Hier nog bijschrijven]

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



Name	Action	Platform	Status	Type	Computers	Order of precedence ↑	La
Analyst policy	Elevate if necess...	Windows	Active	Advanced	All	340	14
developers policy	Elevate if necess...	Windows	Active	Advanced	All	340	11
Baseline	Allow	Windows	Active	Advanced	All	420	10

Figuur 30 Analyst, Developers en Baseline policy prioriteiten

5.0 Tests

5.1 Test 1

- Gebruiker: salesuser1
- AD-groep: Sale

Testdoelen:

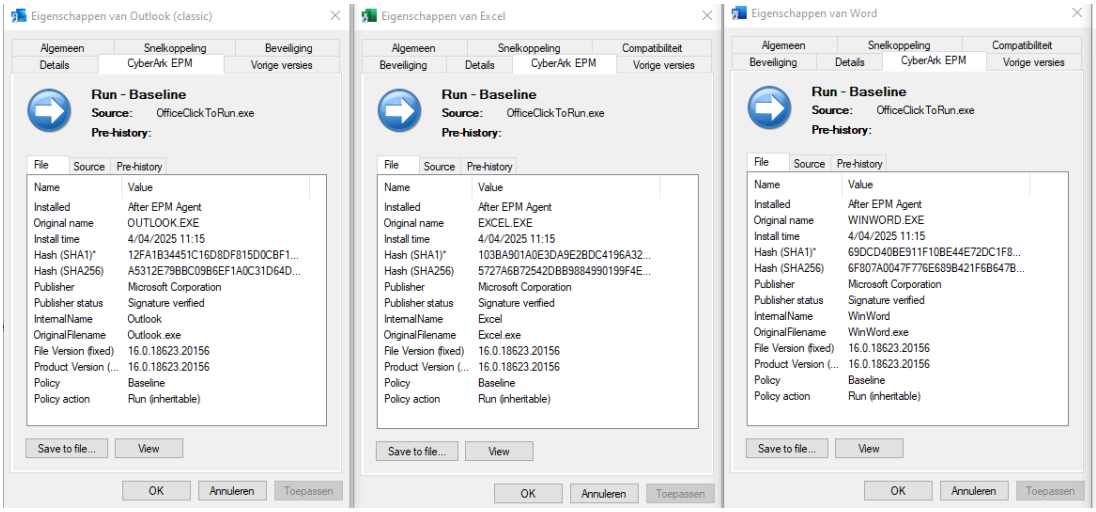
- Controleren of een gewone gebruiker nog steeds Office-apps kan gebruiken (Word, Excel, PowerPoint, etc.).
- Controleren of de *analyst* en *developer* applicaties geblokkeerd worden voor een gewone gebruiker.
- Controleren of *unhandled* applicaties worden geblokkeerd.

We gaan naar de volgende applicaties bekijken:

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

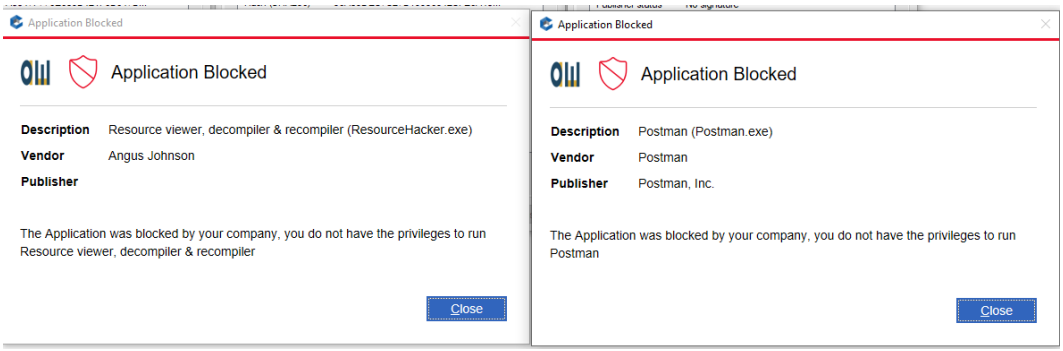
Daarnaast downloaden we Discord om te controleren of deze applicatie wordt geblokkeerd of nog uitvoerbaar is.

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



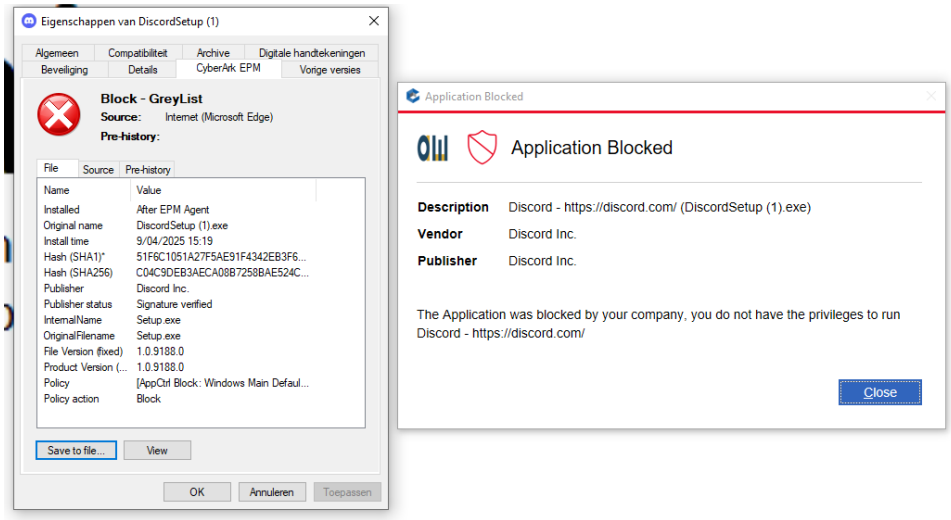
Figuur 31 Baseline policy test op de salesuser1user

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



Figuur 32 Unhandled applicaties test op salesuser1

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



Figuur 33 Applicatie van het internet testen

5.2 Test 2

- Gebruiker: developer1
- AD-groep: developers

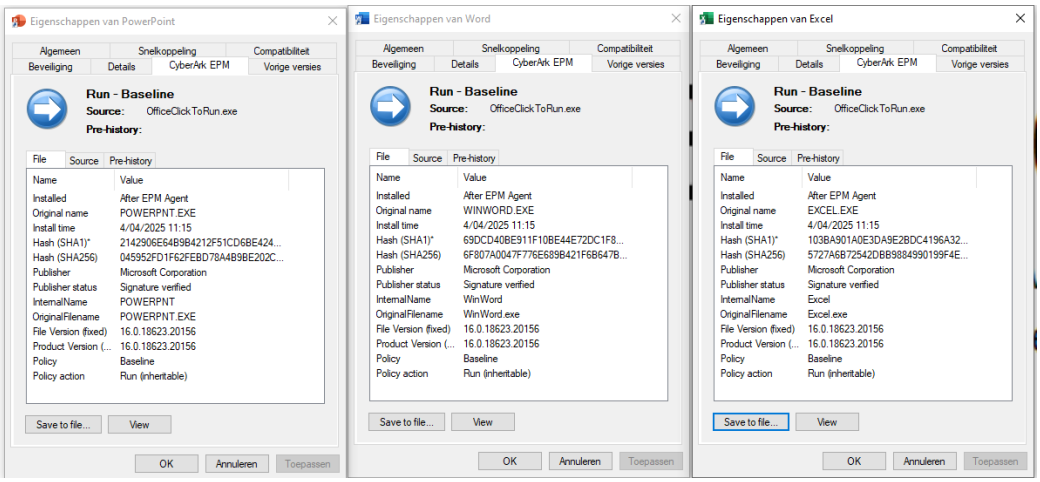
Testdoelen:

- 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, mongodbcompass, node.js ect.)
- Controleren of de *analyst* applicaties geblokkeerd worden voor een developer gebruiker.

We gaan naar de volgende applicaties bekijken:

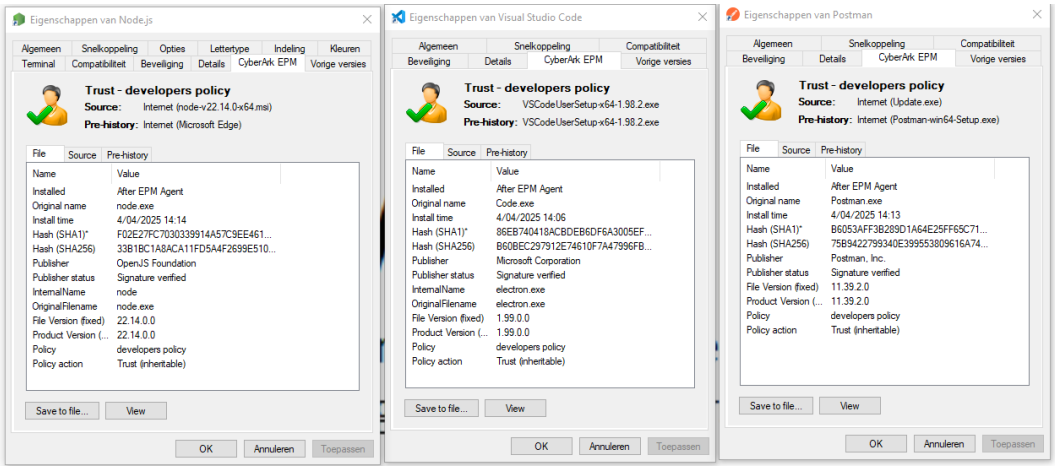
- Word, Excel, Powerpoint
- Visual studio code, node.js, postman (developer applications)
- Resource Hacker, wireshark (analyst applications)

Zoalste zien in figuur 31 kan de developer1 user alle baseline applicaties uitvoeren.



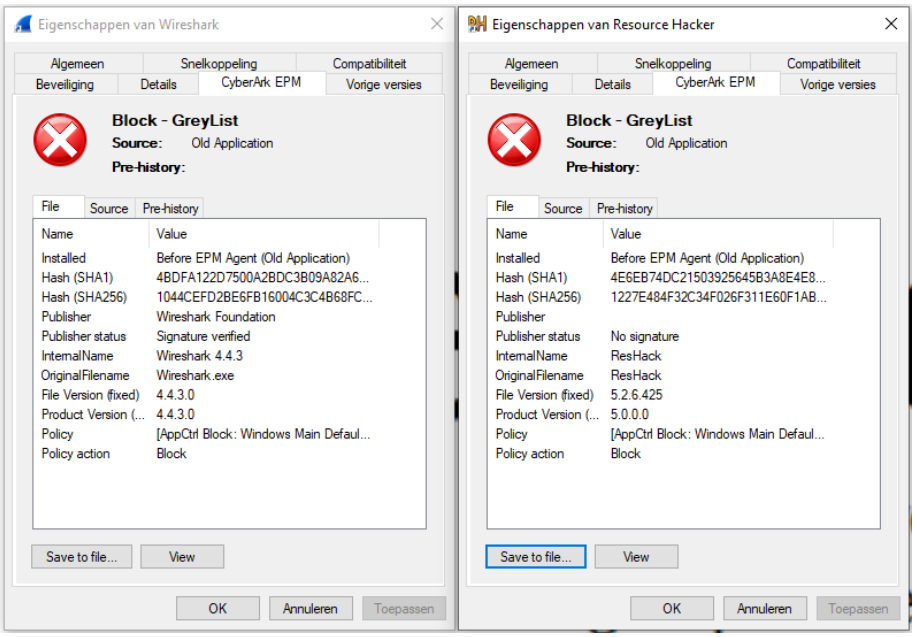
Figuur 34 Baseline policy test op de developer1 user

De developer1 user heeft ook de rechten om developer applicaties uit te voeren als adminitrator (zie figuur 35)



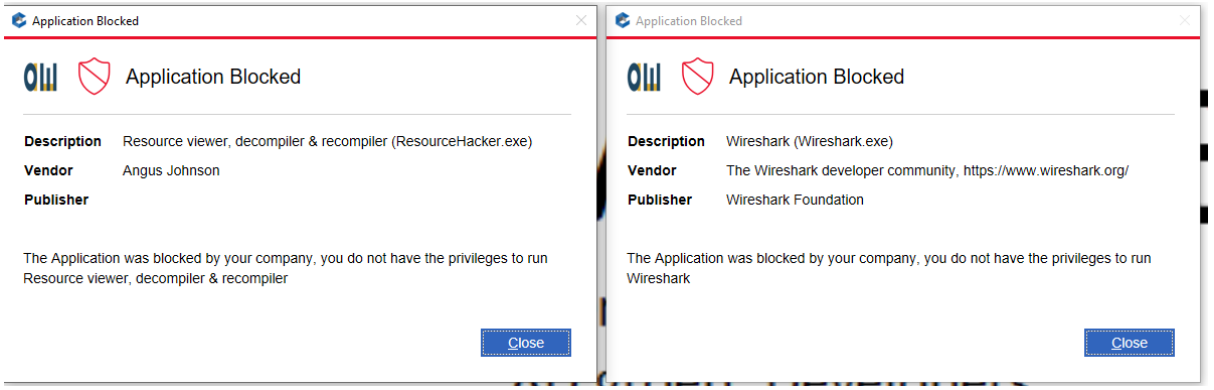
Figuur 35 Developers policy test op de developer1 user

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



Figuur 36 Unhandled applicaties test op de developer1 user

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



Figuur 37 Unhandled applicaties test op de developer1 user

5.3 Test 3

- Gebruiker: analyst1
- AD-groep: Analysts

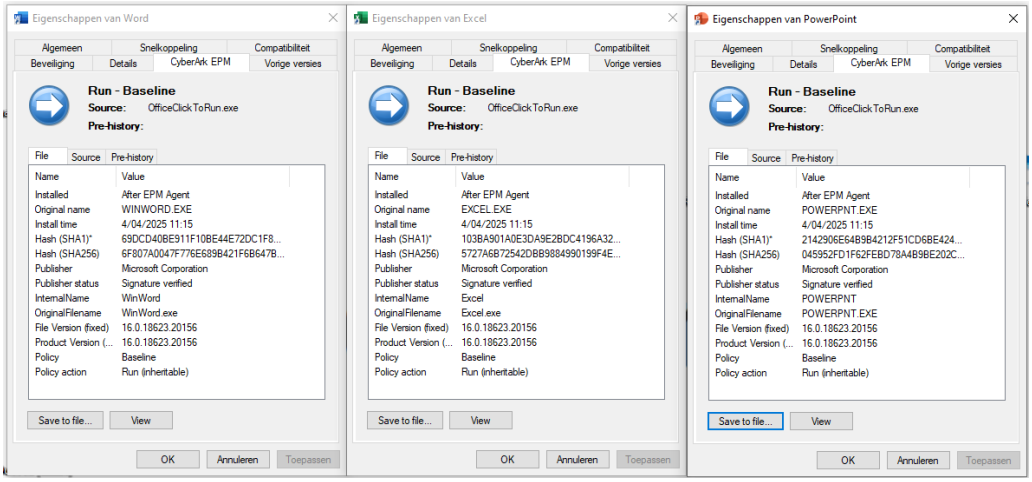
Testdoelen:

- 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 enalyst gebruiker.

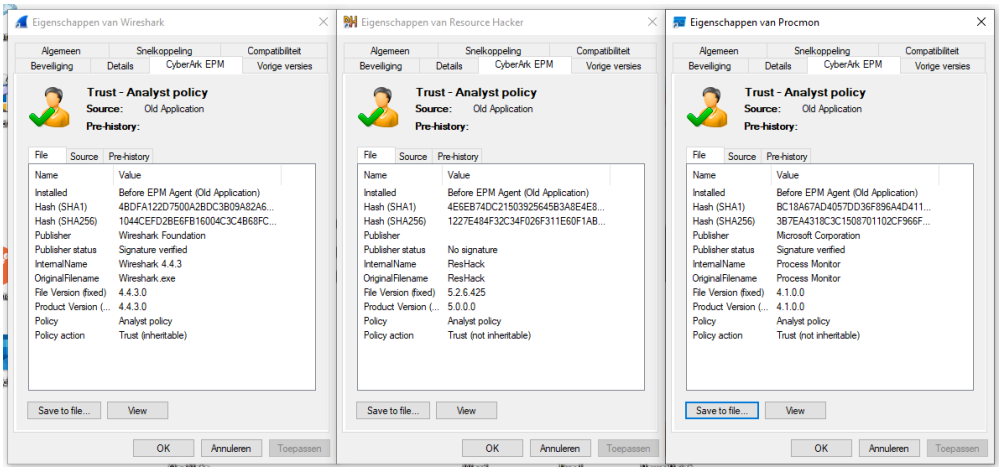
We gaan naar de volgende applicaties bekijken:

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

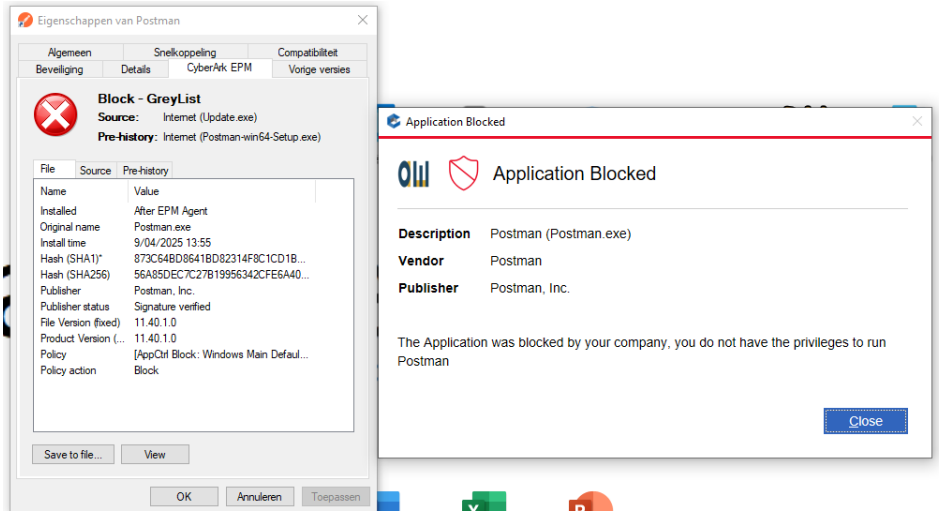
De baseline applicaties zijn uitvoerbaar op de analyst1 user (zie figuur 38).



Figuur 38 Baseline policy test op de analyst1 user



Figuur 39 Analyst policy test op de Analyst1 user



Figuur 40

Conclusie

De geteste policies werken zoals verwacht:

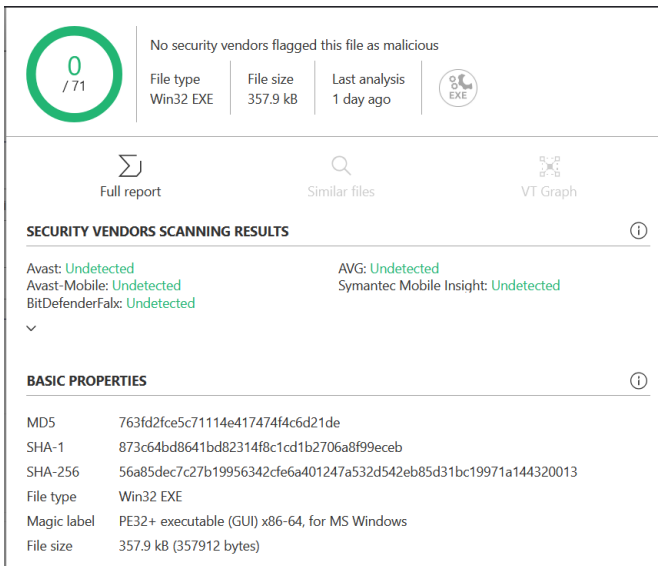
- Baseline apps zijn toegankelijk voor alle gebruikers.
- Developer apps zijn uitsluitend beschikbaar voor de developers.
- Analyst apps zijn uitsluitend beschikbaar voor de analysts.
- Onbekende applicaties worden op alle profielen correct geblokkeerd.

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 infrastructuur van de CyberArk SaaS omgevin. Wanneer een applicatie wordt gestart die nog niet gekend is binnen het beleid van EPM, wordt deze automatisch doorgestuurd naar de VirusTotal API. De hash van de executable wordt gecontroleerd

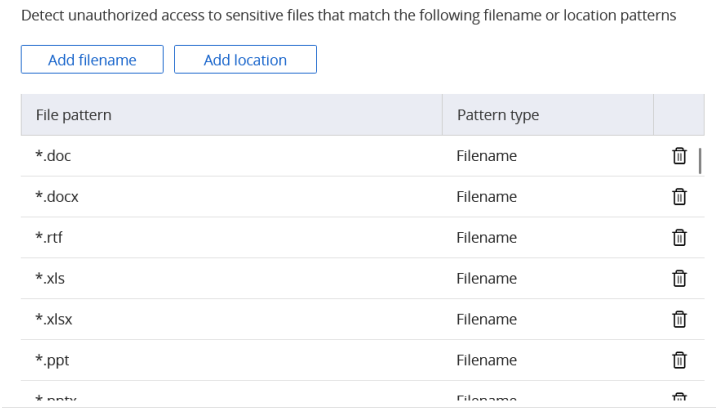


Figuur 41 VirusTotal report in CyberArk EPM SaaS

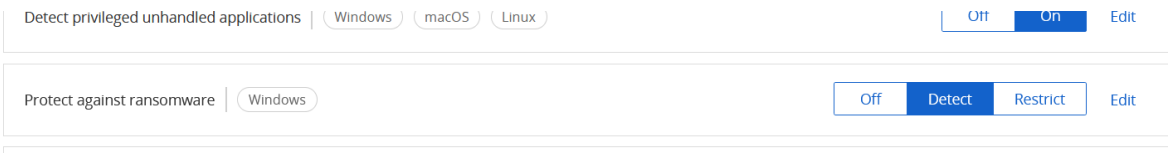
Op basis van de respons van VirusTotal – die informatie bevat over detectieratio's, gedrag, reputatie en mogelijke indicatoren van compromittering – wordt een automatisch rapport gegenereerd. Dit rapport kan vervolgens gebruikt worden om een weloverwogen beslissing te maken binnen EPM: zoals het automatisch 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 gevoelige bestanden en netwerkshares te detecteren of blokkeren wanneer deze wordt uitgevoerd door onbekende applicaties.



Figuur 42 Ransomware protection gevoelige bronnen



Figuur 43 Ransomware protection op detect

Detect Mode:

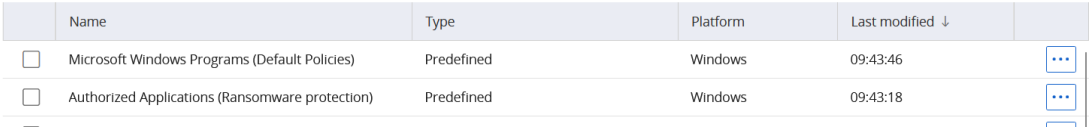
- Enkel logging – laat ransomware toe, maar registreert verdachte toegangspogingen.
- *Dit wordt gebruikt in de testfase om te zien wat geblokkeerd zou worden.*

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.*

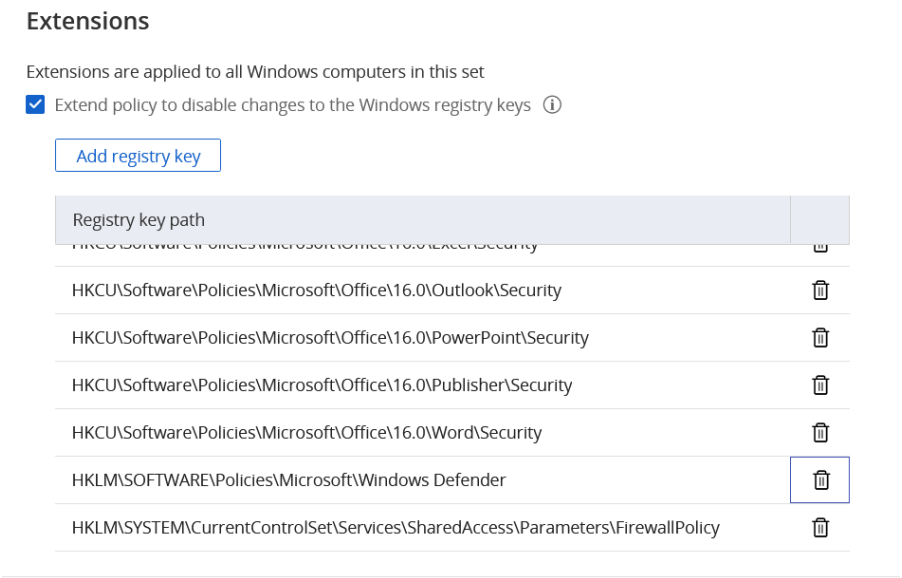
EPM maakt twee belangrijke groepen aan voor deze policy:

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



Figuur 44 Application groups aangemaakt door ransomware protection

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

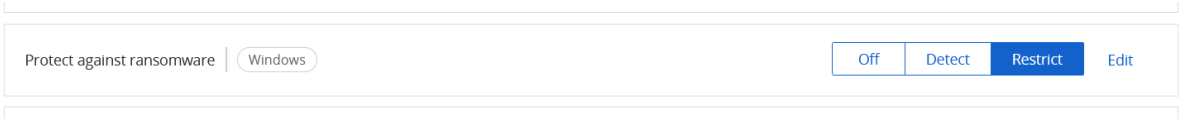


Figuur 45 Windows Registry protection

De policy biedt ook de mogelijkheid om wijzigingen aan specifieke Windows registry keys te blokkeren. Ik heb hiervoor de volgende sleutels toegevoegd (zie figuur 45):

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

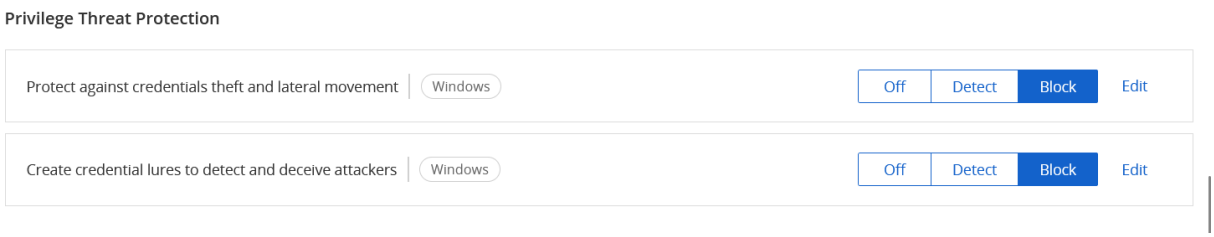
Deze registrybescherming voorkomt dat ransomware via registry-manipulatie Windows Defender of de firewall uitschakelt, wat een veelgebruikte techniek is om windows defender en firewall uit te zetten.



Figuur 46

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



Figuur 47

In de default policies in de cyberark EPM manager kun je ook privelage threat protection inschakelen, er zijn 2 policies in privelage threat protection, “protect against credential theft and lateral movement”, en “create credential lures to detect and decieve 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 48 "protect against credential theft and lateral movement" opties

Als je policies configureert voor credential diefstal en laterale beweging te vorkomen heb je verschillende opties, een aantal zijn te zien in de bovestaande figuur:

Optie naam	**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.

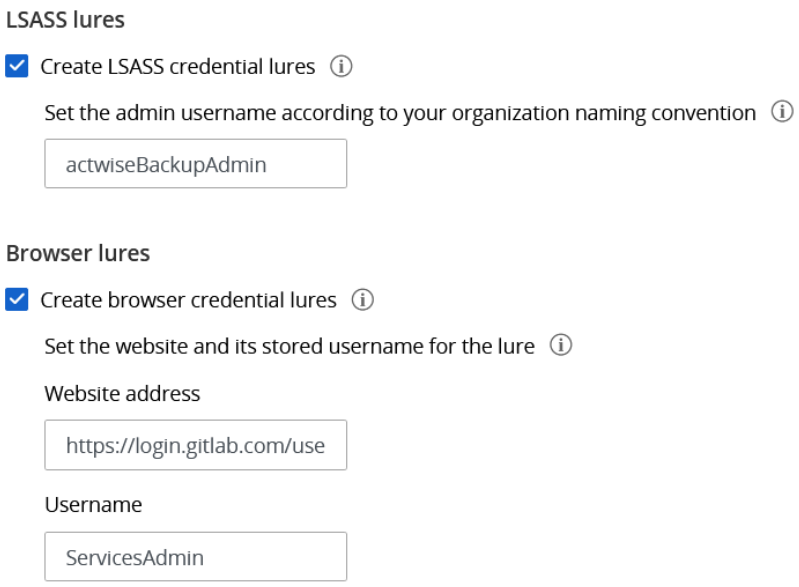
Windows Credentials Harvesting			All	
Credential Theft From Service Account	**Block**	Windows		02-Apr-2
Credential Theft From Windows Credential Manager	**Block**	Windows		02-Apr-2
Domain Credential Theft From Local Cache	**Block**	Windows		02-Apr-2
Local Security Authority (LSA) Secrets Harvesting	**Block**	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 49 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.

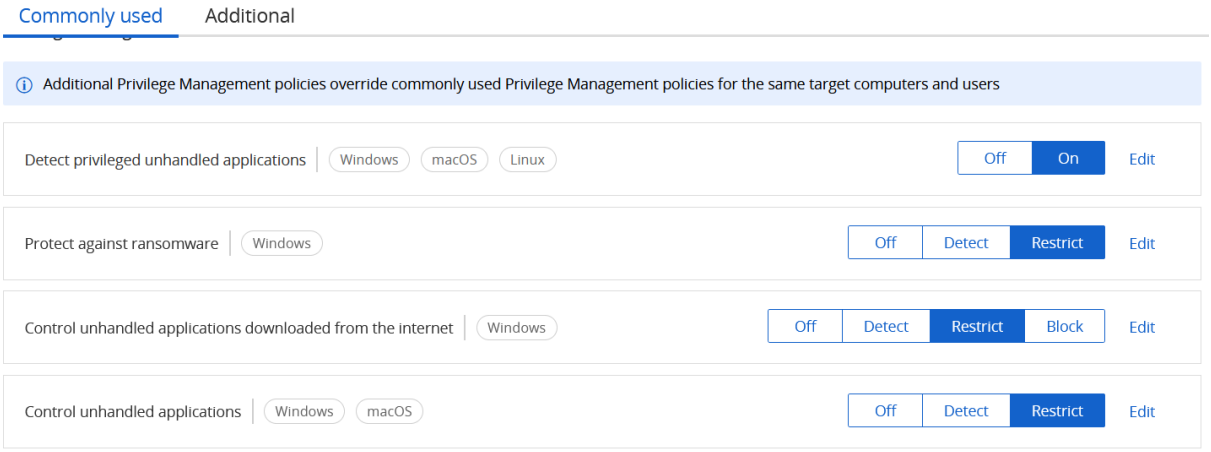
Met de policy ‘Create Credential Lures to Detect and Deceive Attackers’ kan je valse inloggegevens (“lures”) instellen op strategische locaties zoals LSASS of in browserprofielen. Deze techniek heeft als doel aanvallers te verleiden om deze credentials te gebruiken, wat leidt tot detectie en blokkering 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 nepbrowsercredentials op opgegeven websites (bijv. https://login.gitlab.com/use met gebruikersnaam ServicesAdmin). Dit detecteert pogingen om opgeslagen wachtwoorden te stelen.



Figuur 50 ‘Create Credential Lures to Detect and Deceive Attackers’ policy

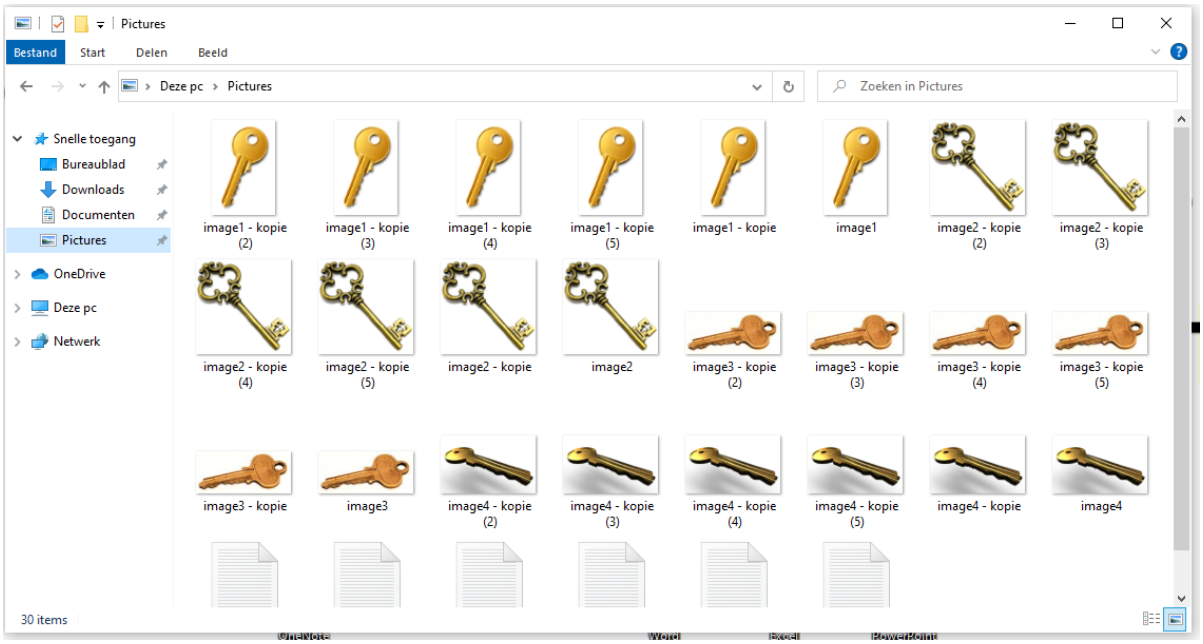
7.0 Finale Tests



Figuur 51

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.

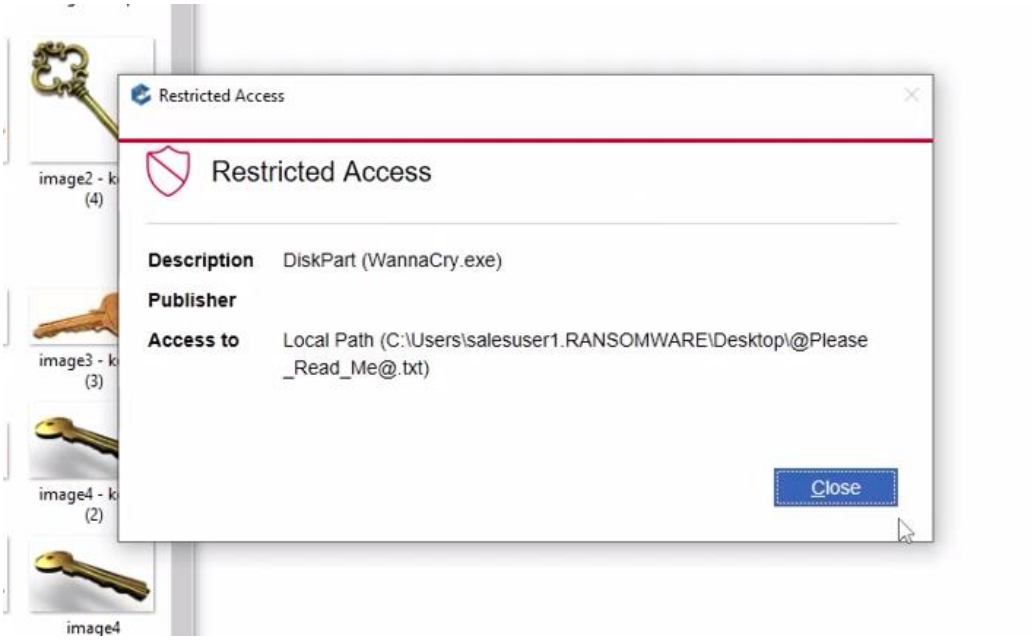
Vooraleer we de aanvallen opnieuw uitvoeren, zetten we het EPM-beleid op 'restrict' om de implementatie af te ronden — dit is hoe het ook in een reële bedrijfsomgeving zou gebeuren. Op elke gebruikersaccount worden enkele testbestanden, zoals foto's, geplaatst om te controleren of deze versleuteld worden. De testbestanden zien er als volgt uit:



Figuur 52 Files

7.1 WannaCry

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



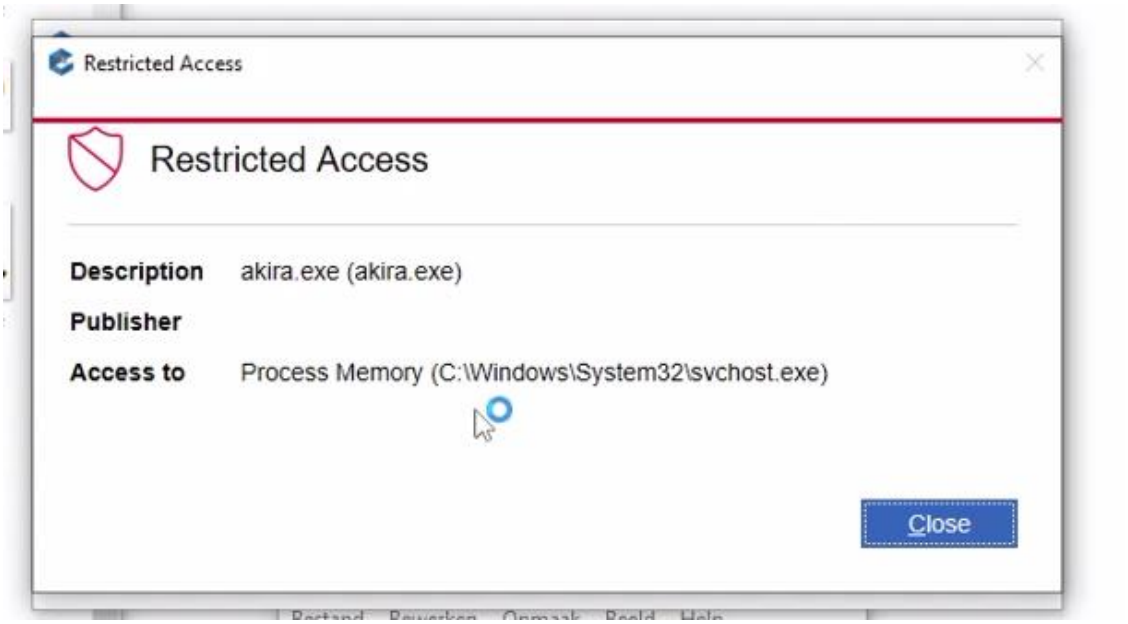
Figuur 53 WannaCry uitvoering na EPM implementatie

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 de ransomnote heeft aangemaakt 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 nog vóór de encryptiefase kan plaatsvinden.

Video:

7.2 Akira

- User: salesuser1
- ADgroep: Sales
- Toegepaste policies: ‘baseline policy’



Figuur 54 Akira uitvoering na EPM implementatie

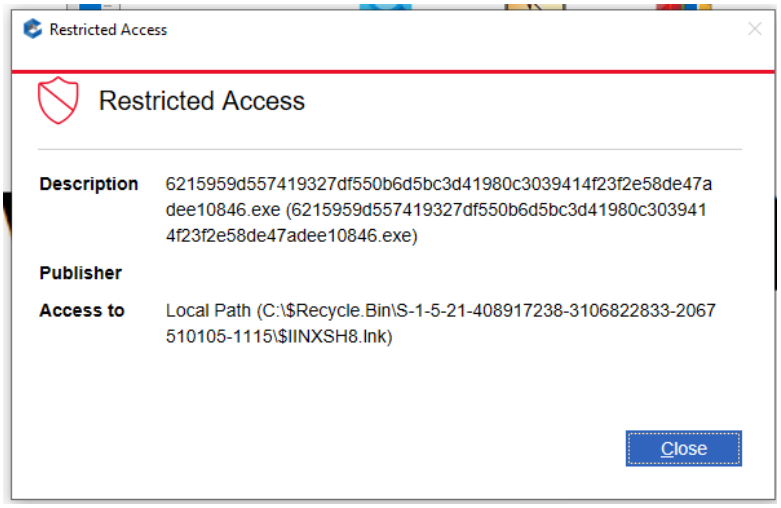
De volgende ransomware die we uitvoeren is de Akira-ransomware. Deze heb ik getest door deze uit te voeren met administratorrechten als *salesuser1*. Zelfs met deze verhoogde rechten slaagt Akira er niet in om het systeem succesvol te versleutelen.

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 plaatgevonden.

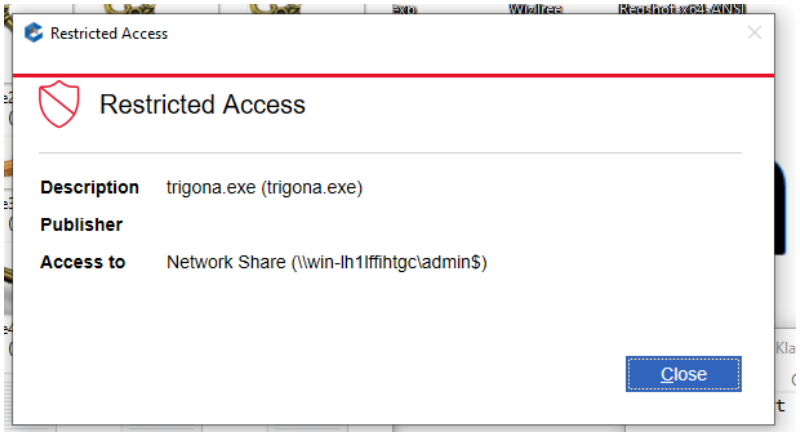
Video:

7.3 Trigona

- User: Analyst
- ADgroep: Analysts
- Toegepaste policies: ‘baseline policy’ en ‘analyst policy’



Figuur 55



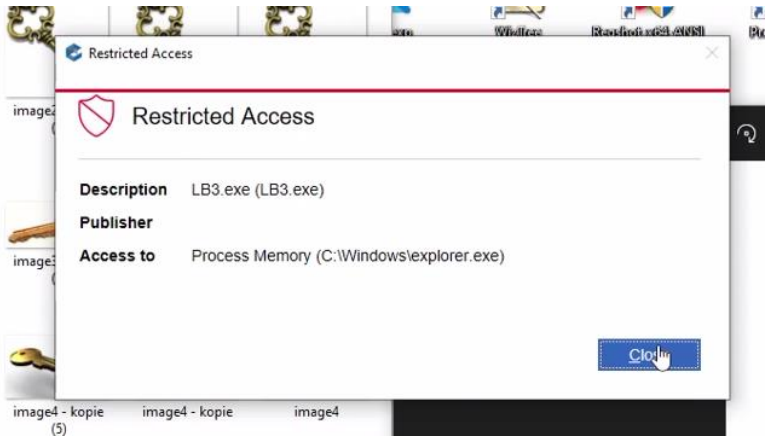
Figuur 56

Tijdens de uitvoering van Trigona onderneemt de ransomware meerdere pogingen om gevoelige locaties te benaderen. De eerste poging richt zich op een netwerkshare (\\win-lh1fl1fhtgc\admin$), die geblokkeerd wordt dankzij de toegepaste policies. Vervolgens probeert een willekeurig bestand 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: ‘basline’ en ‘developers’

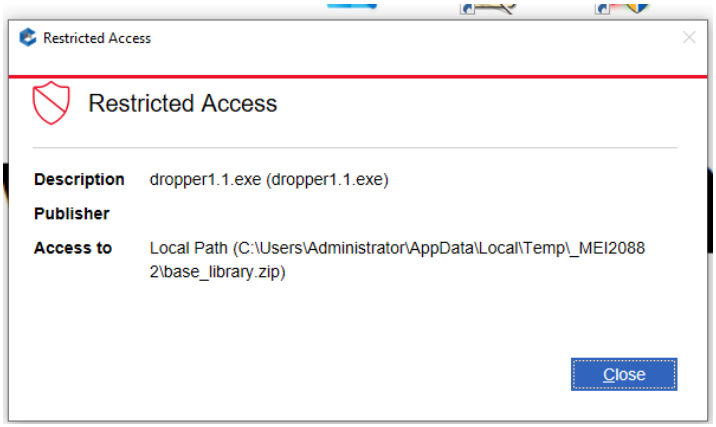


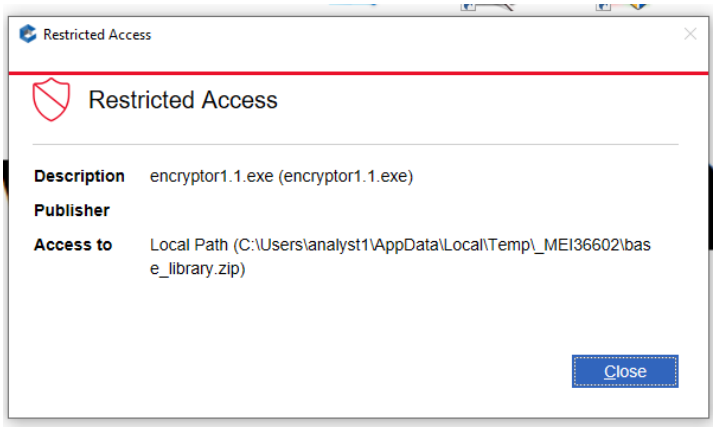
Figuur 57 LockBitV3 uitvoering na EPM-implementatie

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 het geheugen van systeemprocessen 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’ en ‘analysts’





8.0 Conclusie

9.0 Bronvermelding

[1] Jan, A. (2015-04-12). De titel van dit werk. Opgehaald van http://xxxxxxxxx.

[2] Peter, S. (2012). Titel van Peter's werk. *Journal of Infinitesimal Results 46*(2), 123-134.