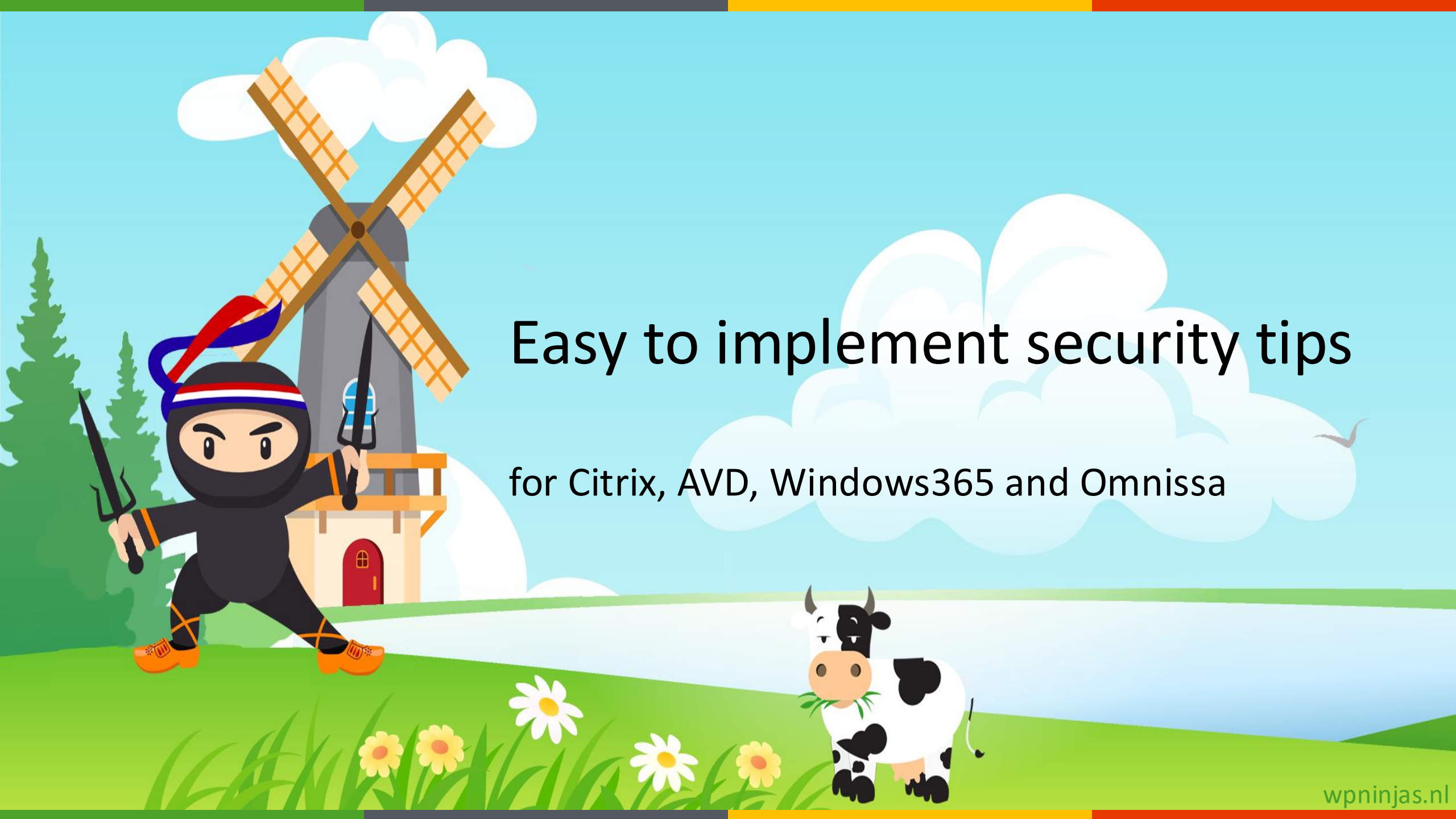

Easy to implement security tips
for Citrix, AVD, Windows365 and Omnissa
wpninjas.nl

Stefan Dingemanse

BRAINPULSE IT
CONSULTANCY & TRAINING

Microsoft® MVP Most Valuable Professional

Focus

Modern Workplace
Consultant/Architect at Brainpulse IT

From

The Netherlands

My blog

https://stefandingemanse.cm

Communities

Azure Thursday

Dutch Virtual Desktop User Group

Hobbies

Hyrox / Crossfit

HYROX

Contact

Stefan@brainpulse.it

Patrick van den Born

Focus

End User Computing

DevOps way of working

From

The Netherlands

My blog

www.detechnischejongens.nl

www.go-euc.com

Communities

GO-EUC

Dutch Virtual Desktop User Group

Microsoft and Citrix

Hobbies

CrossFit

Weightlifiting

Sim racing

Contact

patrick@detechnischejongens.nl

Agenda

- Real World Scenarios
- What are the risks
- Easy to implement security tips
- Recap
- Questions


Personal – Real world scenario

Personal – Real world scenario

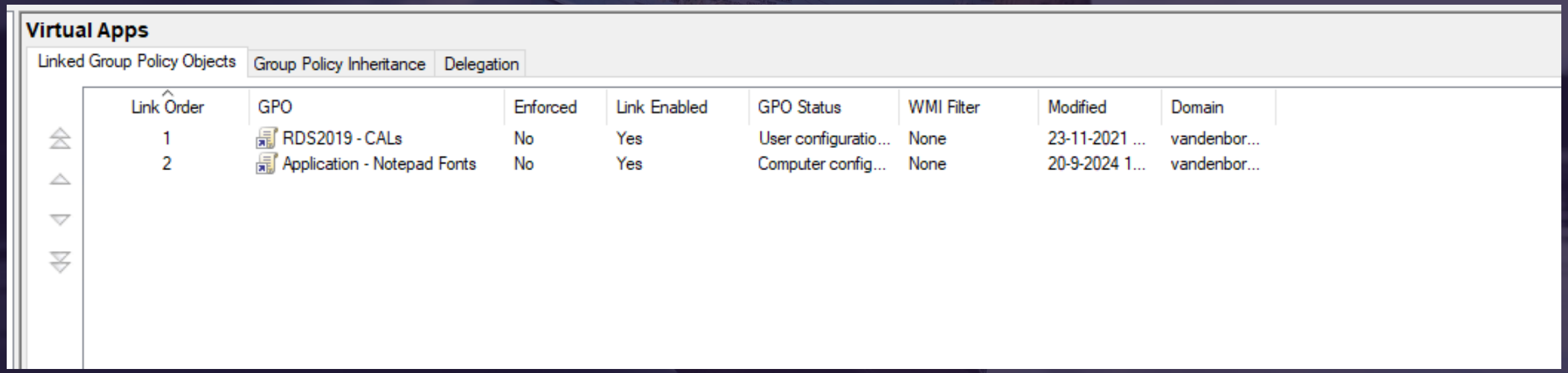
EUC Environments

Application configuration

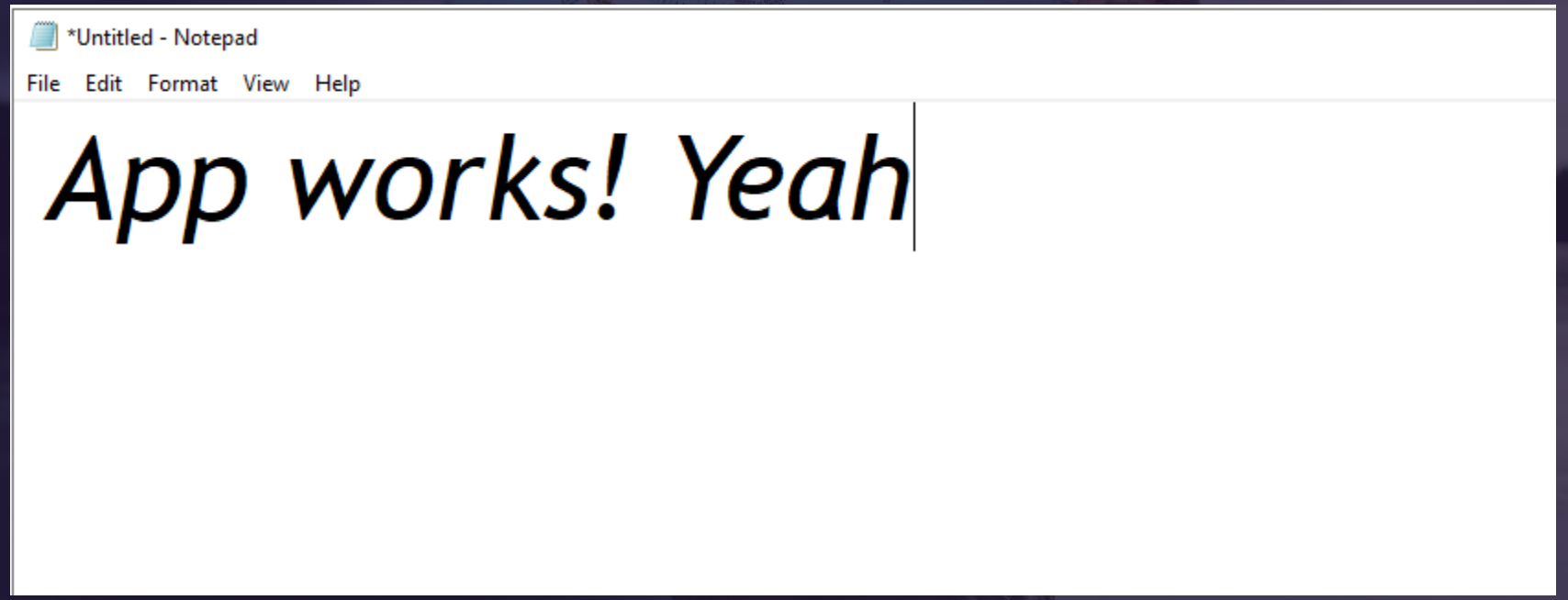
Easy tips

Session Host defense

Customer example

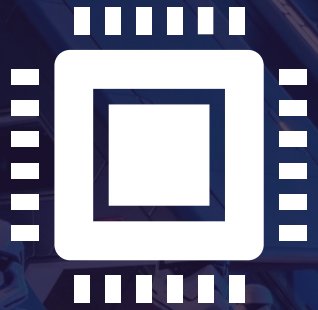


Customer example



Security findings from the field

Scripting



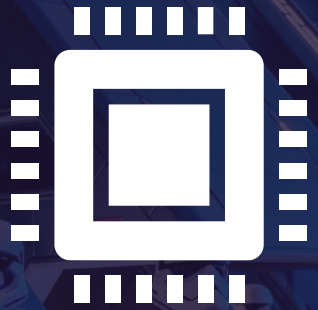
OS

Applications

Security findings from the field

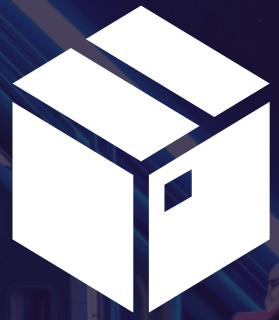
Scripting

Powershell v2 enabled
Powershell full language mode



OS

Cached credentials
User write rights
Identical local admin passwords
Network communication
Outbound internet firewall
Windows updates strategy



Applications

No application whitelisting
Outdated applications
Internet Explorer 11
No virus scanners or EDR/XDR

What are the risks?

Cyber war

Internet facing

Lateral movement

Ransomware Delivery Protocol

Windows Privilege Escalation Awesome Scripts

https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS

Product Solutions Resources Open Source Enterprise Pricing

Search or jump to... Sign in Sign up

peass-ng / PEASS-ng Public

Sponsor Notifications Fork 3.1k Star 15.8k

Code Issues 24 Pull requests 1 Actions Projects Security Insights

Files

master

Go to file

- .github
- build_lists
- linPEAS
- metasploit
- parsers
- winPEAS
  - winPEASbat
  - winPEASexe
  - winPEASps1
  - README.md
- .gitignore
- CONTRIBUTING.md
- LICENSE
- README.md
- TODO.md

PEASS-ng / winPEAS /

carlospolop f2 b3bcfa4 · 3 weeks ago History

Name	Last commit message	Last commit date
..		
winPEASbat	WinPEASS Big Update	3 weeks ago
winPEASexe	f2	3 weeks ago
winPEASps1	WinPEASS Big Update	3 weeks ago
README.md	WinPEASS Big Update	3 weeks ago

README.md

Windows Privilege Escalation Awesome Scripts

Check the **Local Windows Privilege Escalation checklist** from book.hacktricks.xyz

Check more **information about how to exploit** found misconfigurations in book.hacktricks.xyz

Quick Start

Find the **latest versions of all the scripts and binaries in** the releases page.

WinPEAS Flavours

- Link to WinPEAS C# .exe project (.Net >= 4.5.2 required)

Windows Privilege Escalation Awesome Scripts

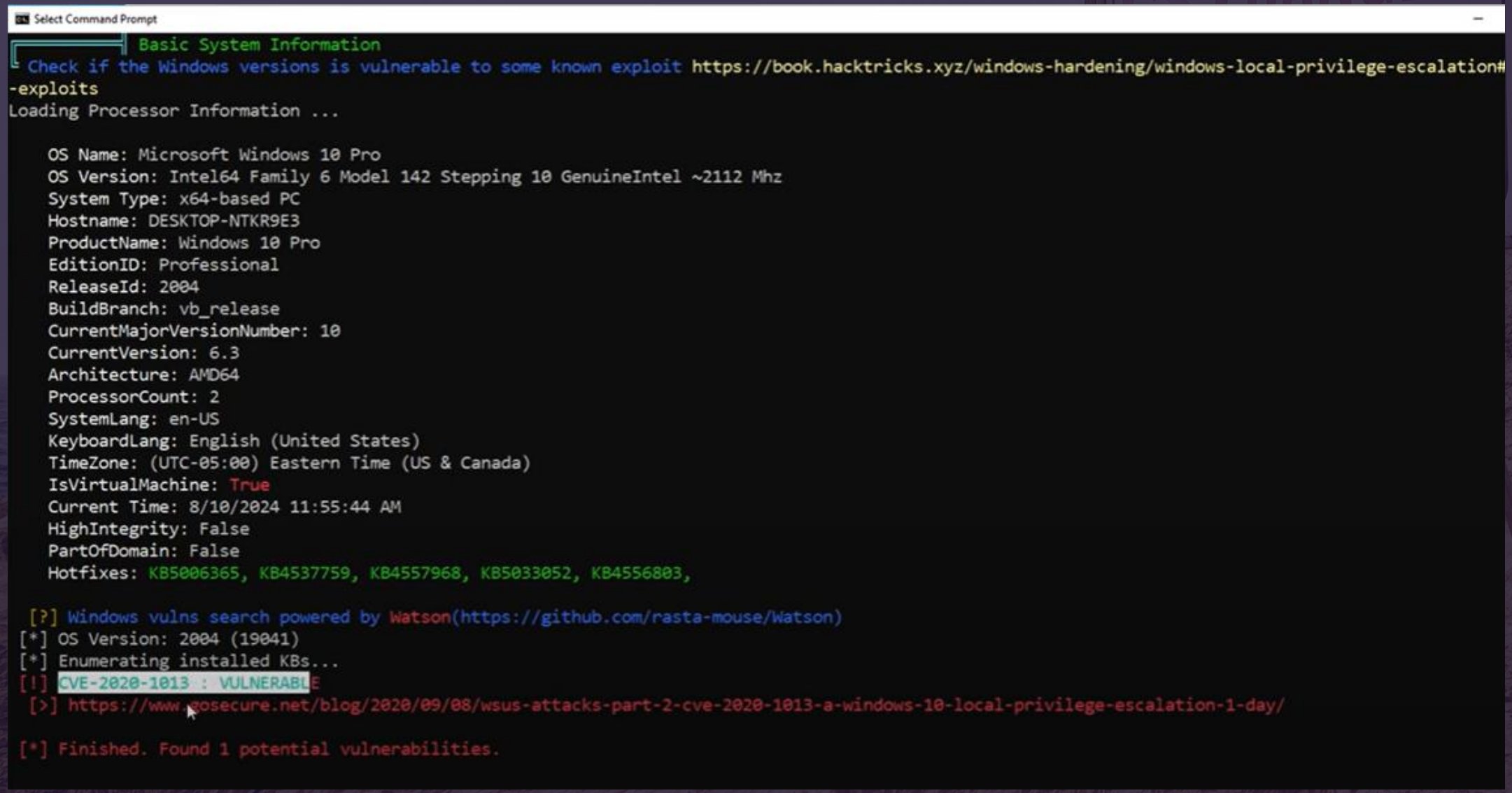
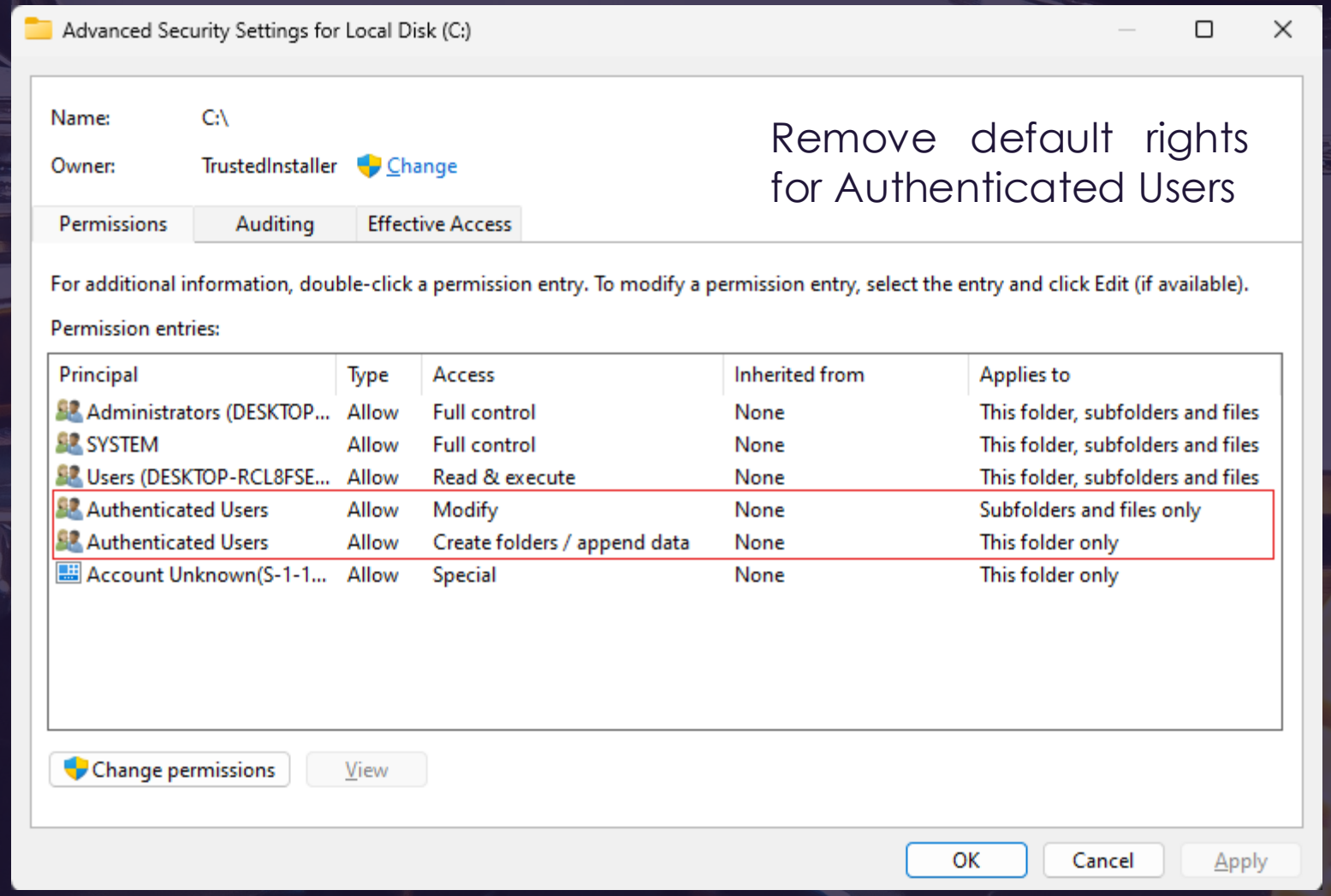



Image adjustments

Image adjustments



Remove default rights for Authenticated Users

Image adjustments

```
# Adjust C-drive permissions
Write-Host "##[C-Drive]Retrieving security principal for SID S-1-5-11 (NT AUTHORITY\Authenticated
Users)"
$SID = New-Object System.Security.Principal.SecurityIdentifier("S-1-5-11")
$User = $SID.Translate([System.Security.Principal.NTAccount])
Write-Host "##[C-Drive]NT AUTHORITY\Authenticated Users group name is ($($User.Value))"
Write-Host "##[command][C-Drive]Setting C-Drive permissions"

$aclroot = Get-Acl -Path "C:\"
$accessToRemove = @('AppendData', '-536805376')

foreach ($access in $accessToRemove) {
    $removeAcl = $aclroot.Access | Where-Object { $_.IdentityReference -like $User.Value -and
$_.FileSystemRights -like $access }
    if ($removeAcl) {
        $aclroot.RemoveAccessRule($removeAcl)
        Write-Host "##[C-Drive]Removed [$($User.Value)] with access [$access]"
    }
}

Write-Host "##[C-Drive]Start applying new ACL on C-Drive - This might take a while"
$null = Set-Acl -Path "C:\" -AclObject $aclroot
Write-Host "[C-Drive]Done!"
```

Image adjustments

```
#Disable Cached Logons on server
Write-Host "##[command][Cached-Credentials] Disabling Cached Credentials"
$securityCachedLogonsCount = [ordered] @{
    RegistryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
    RegistryName = "CachedLogonsCount"
    RegistryValue = "0"
    RegistryType = "String"
}
$securityCachedLogonsCount | Format-Table -AutoSize | Write-output
Set-RegistryValue @securityCachedLogonsCount
Write-Host "[Cached-Credentials] done"
```

Image adjustments

```
$featureVariables = [ordered]@{
    Online      = $true
    FeatureName = "MicrosoftWindowsPowershellV2Root"
}

#Logging
Write-Host "Disable: $($featureVariables.FeatureName)"
$featureVariables | Format-Table -AutoSize | Write-output

#Disable Windows Feature
Disable-WindowsOptionalFeature @featureVariables
```

Image adjustments

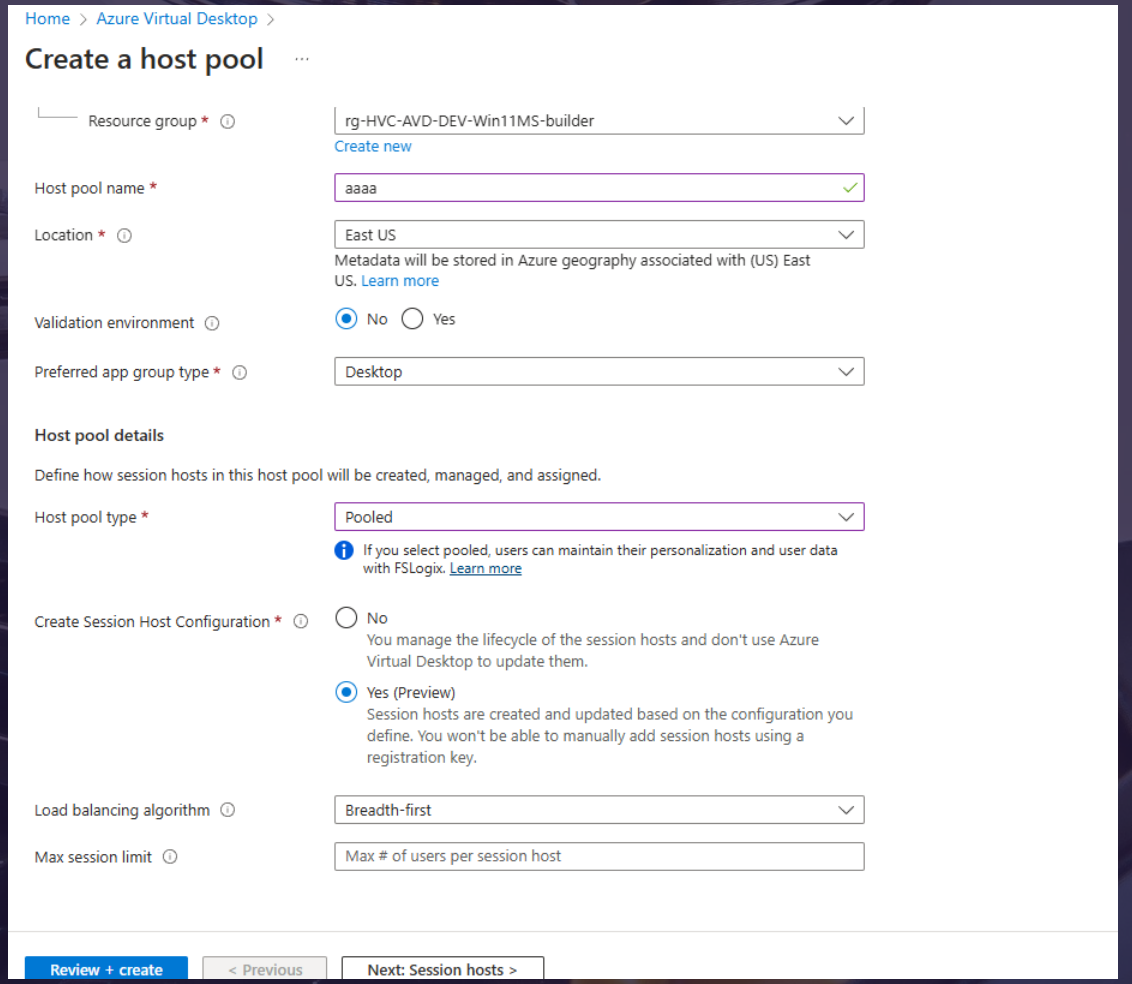
```
$featureVariables = [ordered]@{
    Online      = $true
    FeatureName = "Internet-Explorer-Optional-amd64"
}

#Logging
Write-Host "Disable: $($featureVariables.FeatureName)"
$featureVariables | Format-Table -AutoSize | Write-output

#Disable Windows Feature
Disable-WindowsOptionalFeature @featureVariables
```

Consistent Image Release Strategy

Citrix Machine Creation Services
Citrix Provisioning Services

Azure Virtual Desktop Session Host Configuration

Omnissa Linked Clones



Creating Confidence in the Connected World™

At CIS®, we're harnessing the power of the global IT community to safeguard public and private organizations against cyber threats. Join us.

World-Renowned Best Practices and Expert Communities

CIS Benchmarks™

The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

Microsoft

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

against cybersecurity threats.

Lower the attach surface

The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.

CIS benchmarks provide two levels of security settings:

- **Level 1** recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- **Level 2** recommends security settings for environments requiring greater security that could result in some reduced functionality.

CIS Benchmarks™

The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

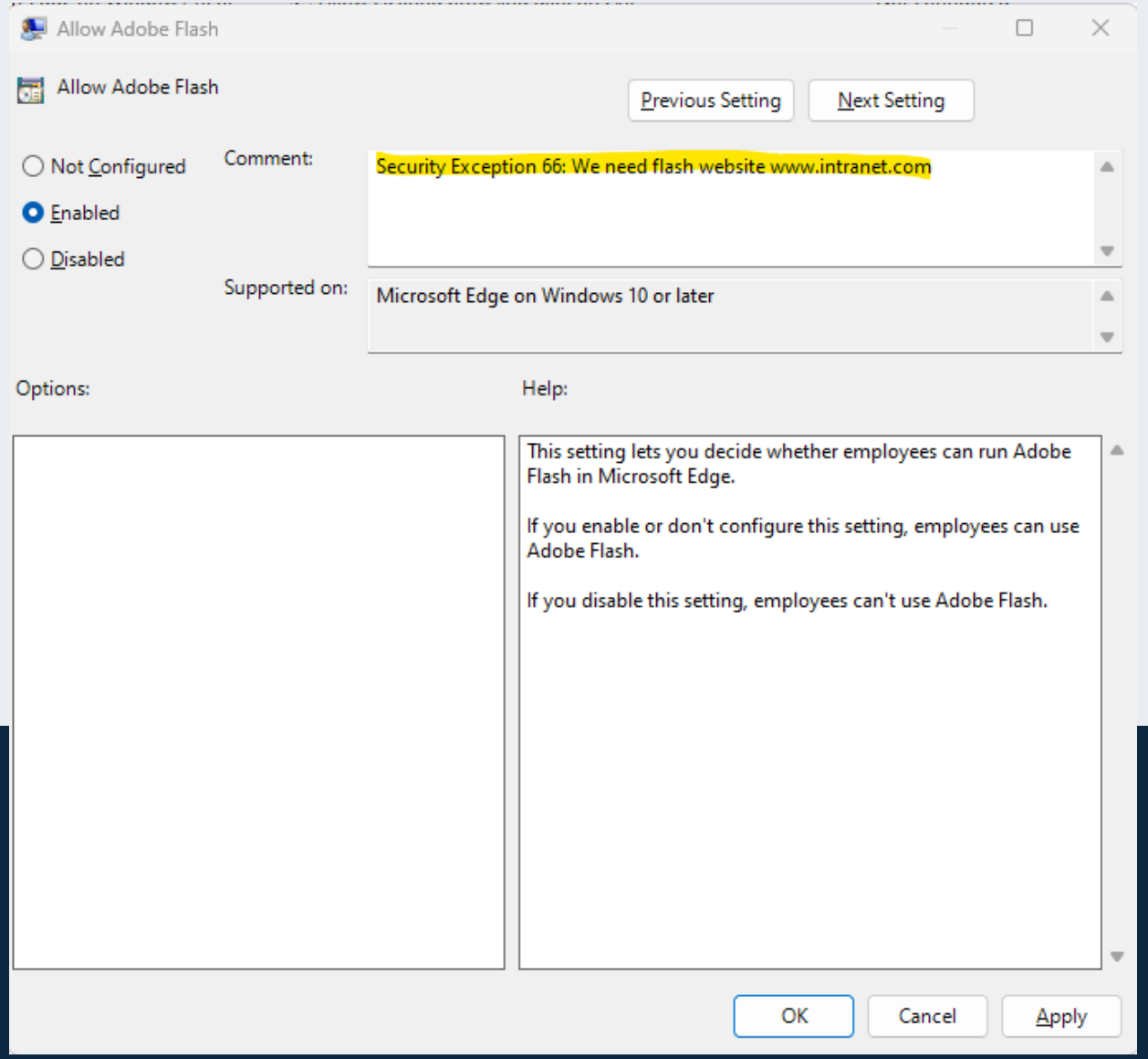
Microsoft

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

DoD CYBER EXCHANGE PUBLIC

STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.

1	AVD_PROD_COMP_Settings	All Computer related policy settings combined	
2	AVD_PROD_USER_Settings	All User related policy settings combined	
3	AVD_PROD_AppLocker	AppLocker Policy	
4	**AVD_PROD_CIS_Exceptions**	**User/Computer Exceptions on General Cis**	**Enforced**
5	AVD_PROD_CIS	CIS Policy Microsoft Windows, Office, Edge, RemoteApps (unchanged)	


Allow Adobe Flash
Allow Adobe Flash
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Security Exception 66: We need flash website www.intranet.com
Supported on:
Microsoft Edge on Windows 10 or later
Options:
Help:
This setting lets you decide whether employees can run Adobe Flash in Microsoft Edge.
If you enable or don't configure this setting, employees can use Adobe Flash.
If you disable this setting, employees can't use Adobe Flash.
OK
Cancel
Apply




Microsoft Security Baselines and CIS Remote Desktop Protocol

CIS Benchmarks™

The CIS Benchmarks™ are prescriptive configuration recommendations. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

Microsoft

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implication. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

DoD CYBER EXCHANGE PUBLIC

STIGs are developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). They offer a set of guidelines for various operating systems, including Windows and Linux, to secure an organization's assets against cybersecurity threats.

Validate and test

scipag/
HardeningKitty

HardeningKitty - Checks and hardens your Windows configuration

3 Contributors · 9 Issues · 1k Stars · 169 Forks

)SCIP(

tenable®

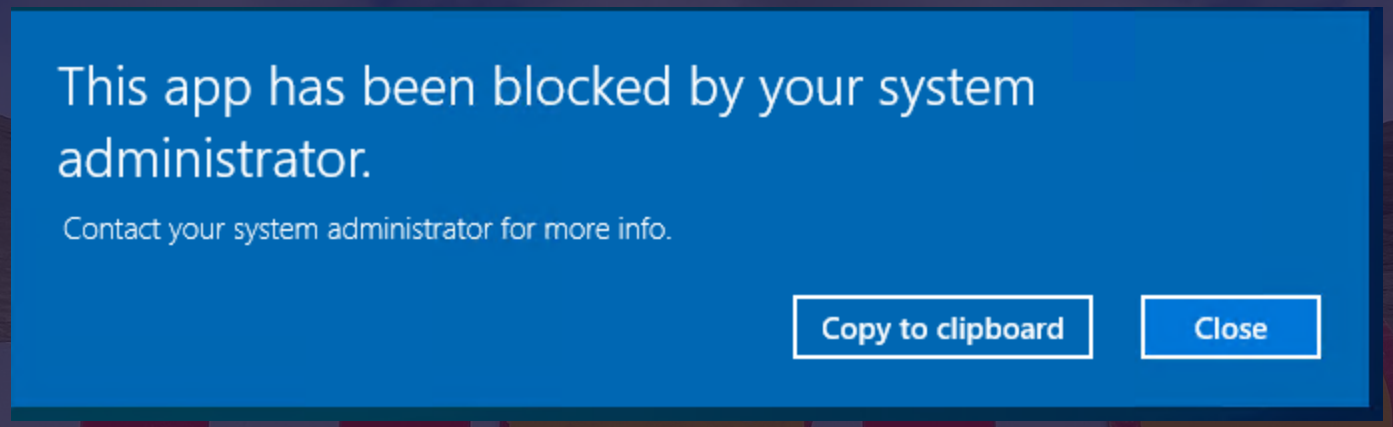
https://github.com/scipag/HardeningKitty

Good Old PolicyAnalyzer

Vulnerability Scanner

Application whitelisting the easy way

Application whitelisting the easy way



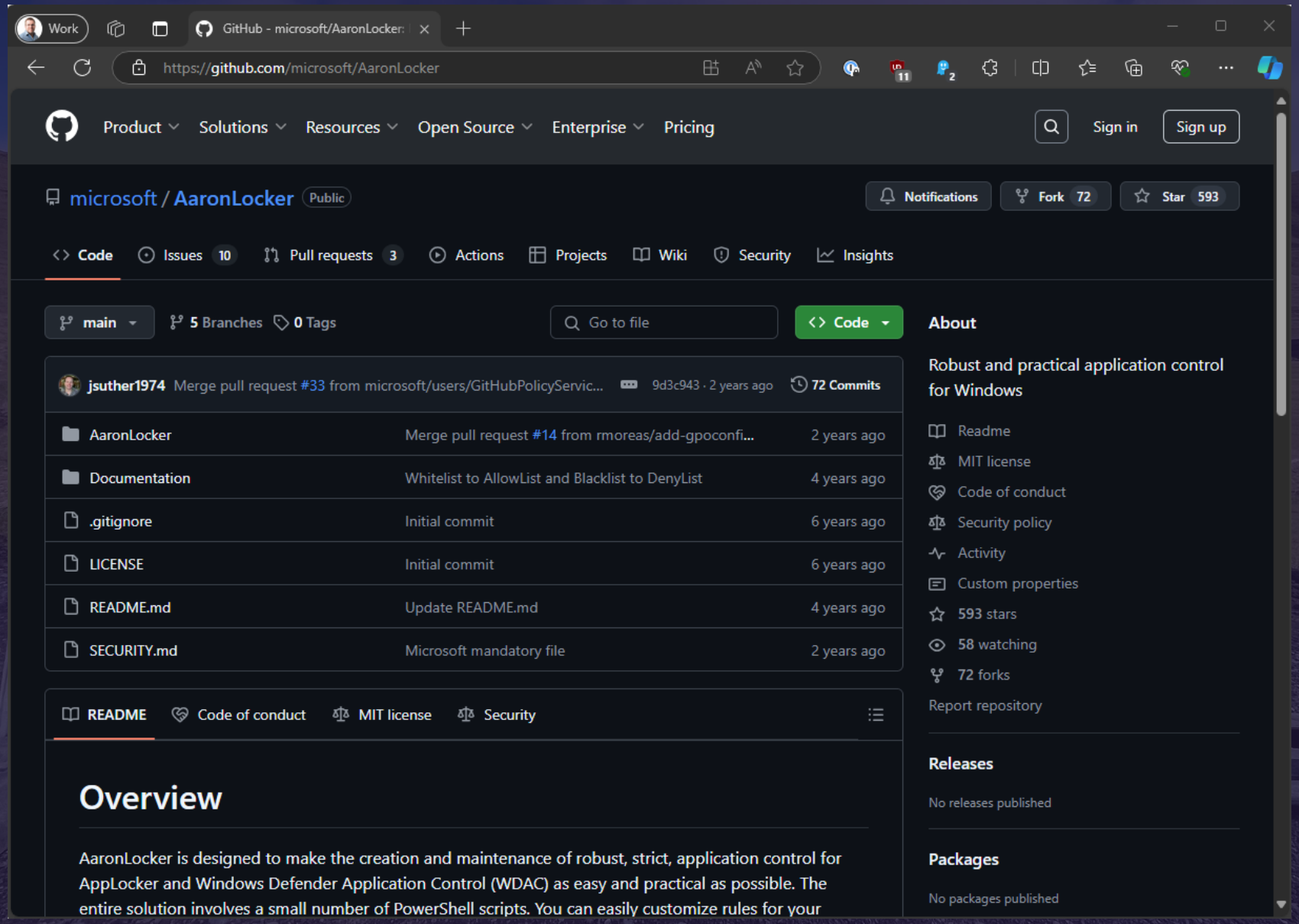
Allow applications

Pen testers

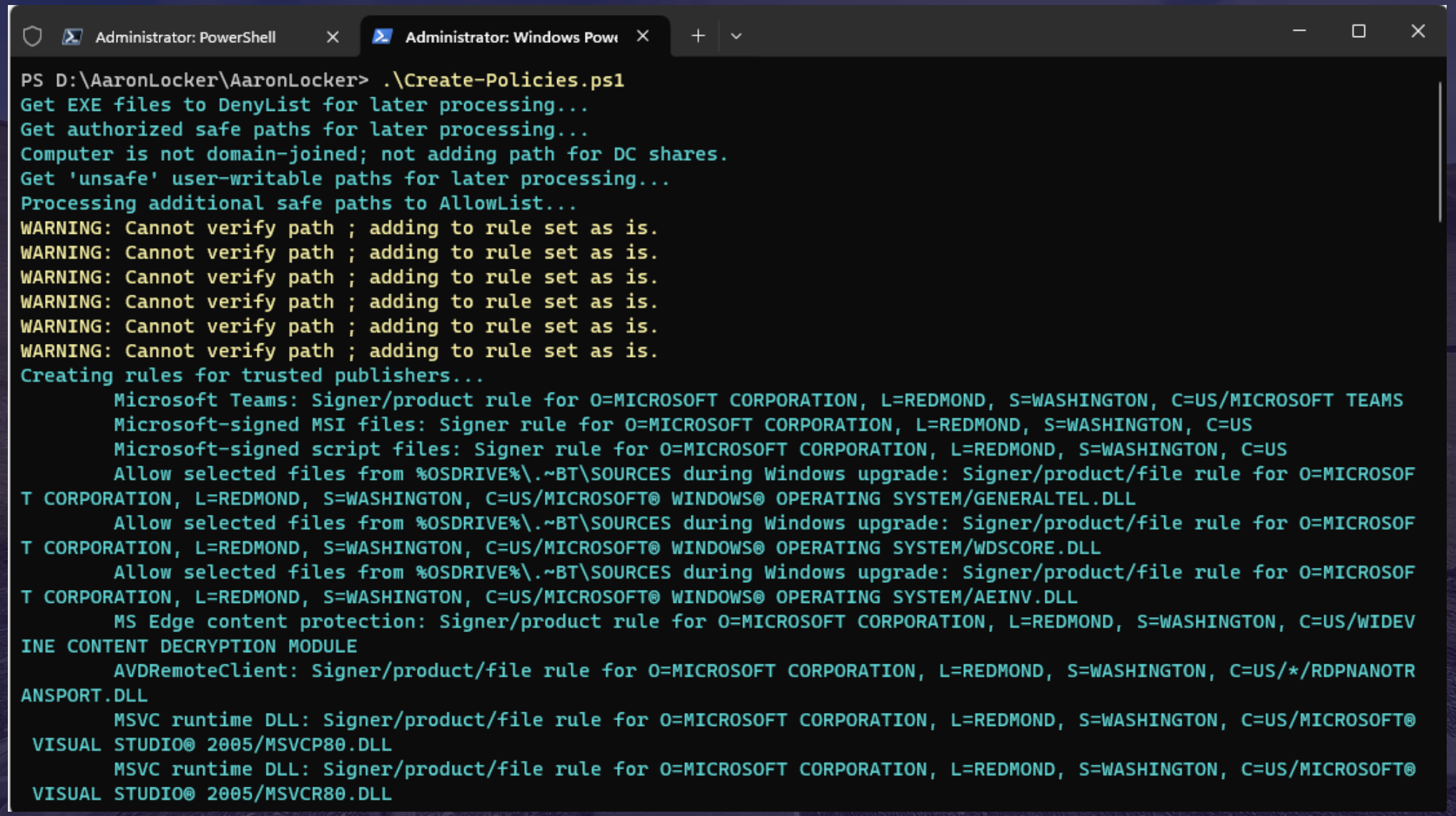
Abnormally detection

User writable folders

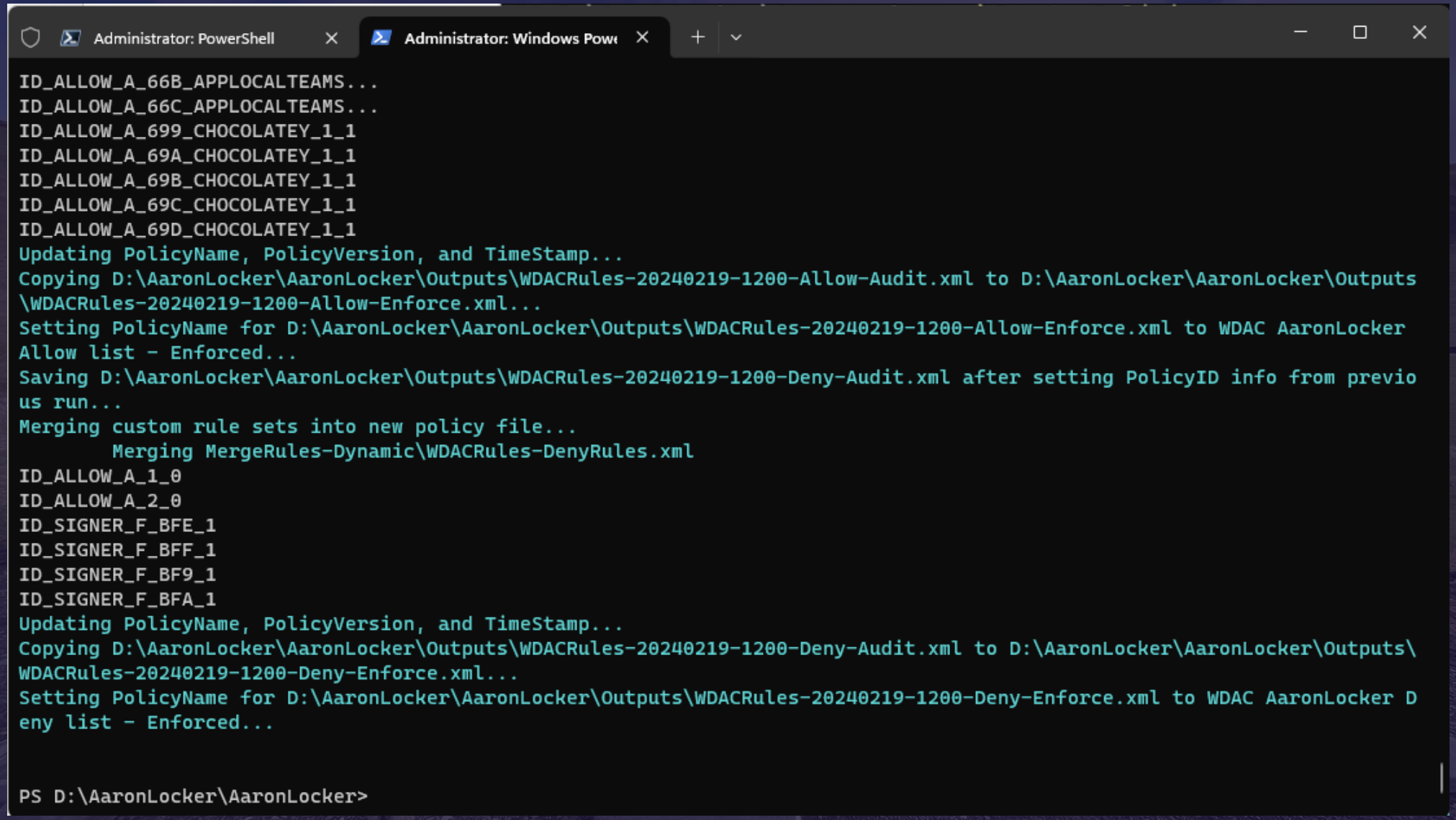
Application whitelisting the easy way



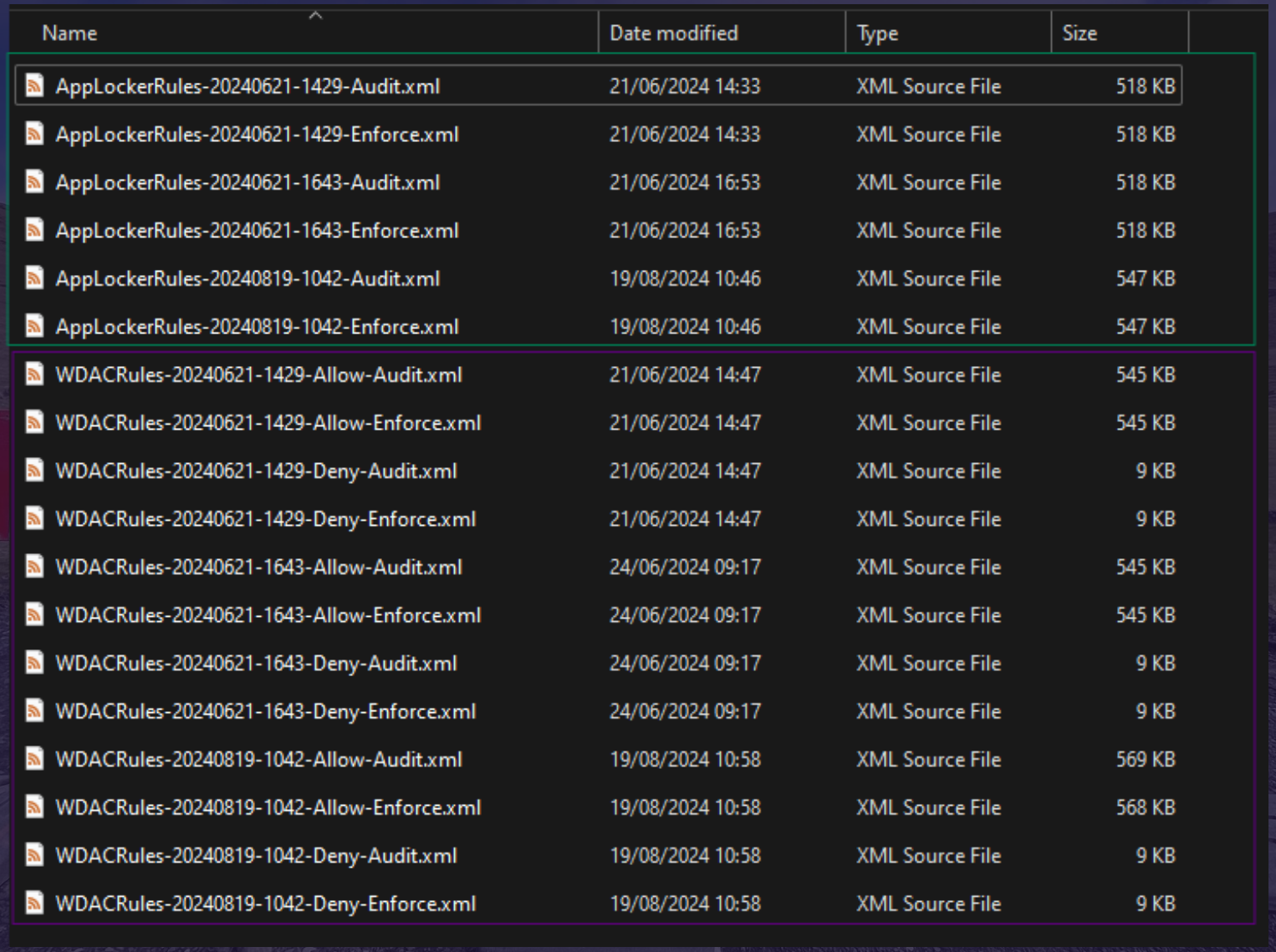
Application whitelisting the easy way



Application whitelisting the easy way

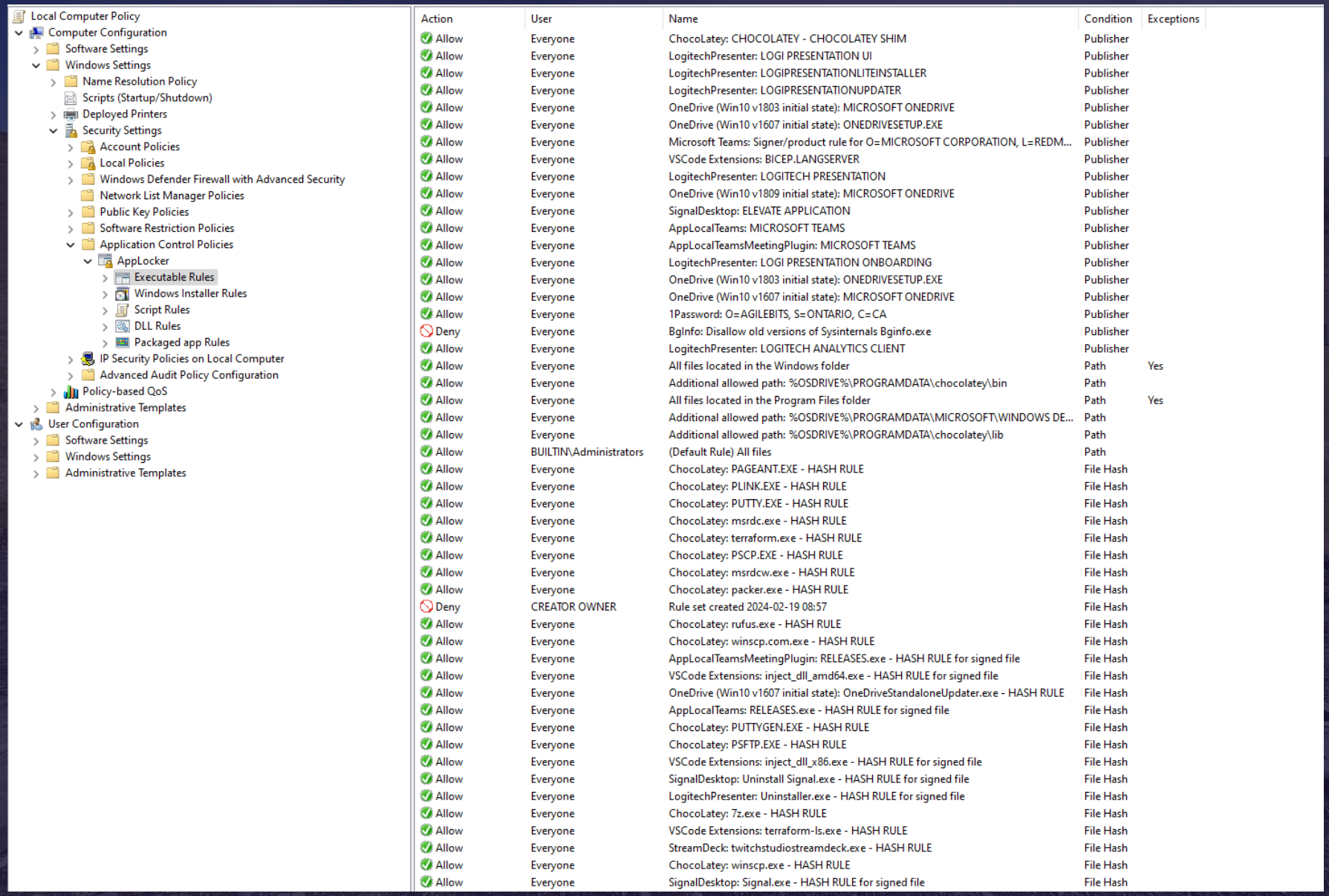


Application whitelisting the easy way



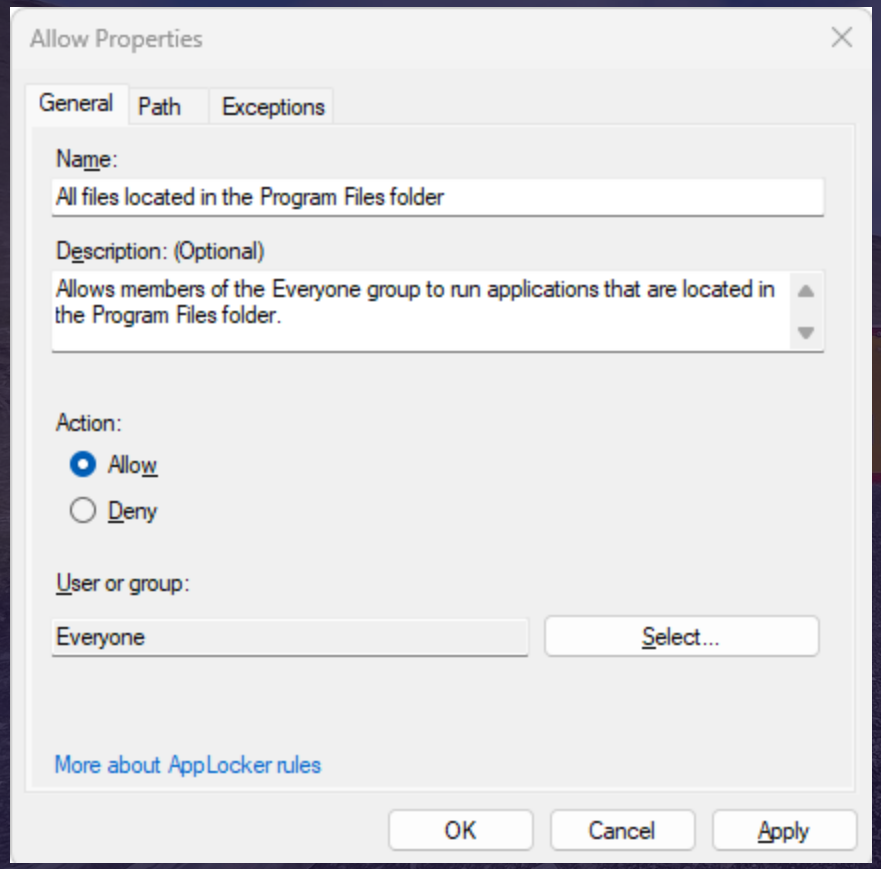
Name	Date modified	Type	Size
AppLockerRules-20240621-1429-Audit.xml	21/06/2024 14:33	XML Source File	518 KB
AppLockerRules-20240621-1429-Enforce.xml	21/06/2024 14:33	XML Source File	518 KB
AppLockerRules-20240621-1643-Audit.xml	21/06/2024 16:53	XML Source File	518 KB
AppLockerRules-20240621-1643-Enforce.xml	21/06/2024 16:53	XML Source File	518 KB
AppLockerRules-20240819-1042-Audit.xml	19/08/2024 10:46	XML Source File	547 KB
AppLockerRules-20240819-1042-Enforce.xml	19/08/2024 10:46	XML Source File	547 KB
WDACRules-20240621-1429-Allow-Audit.xml	21/06/2024 14:47	XML Source File	545 KB
WDACRules-20240621-1429-Allow-Enforce.xml	21/06/2024 14:47	XML Source File	545 KB
WDACRules-20240621-1429-Deny-Audit.xml	21/06/2024 14:47	XML Source File	9 KB
WDACRules-20240621-1429-Deny-Enforce.xml	21/06/2024 14:47	XML Source File	9 KB
WDACRules-20240621-1643-Allow-Audit.xml	24/06/2024 09:17	XML Source File	545 KB
WDACRules-20240621-1643-Allow-Enforce.xml	24/06/2024 09:17	XML Source File	545 KB
WDACRules-20240621-1643-Deny-Audit.xml	24/06/2024 09:17	XML Source File	9 KB
WDACRules-20240621-1643-Deny-Enforce.xml	24/06/2024 09:17	XML Source File	9 KB
WDACRules-20240819-1042-Allow-Audit.xml	19/08/2024 10:58	XML Source File	569 KB
WDACRules-20240819-1042-Allow-Enforce.xml	19/08/2024 10:58	XML Source File	568 KB
WDACRules-20240819-1042-Deny-Audit.xml	19/08/2024 10:58	XML Source File	9 KB
WDACRules-20240819-1042-Deny-Enforce.xml	19/08/2024 10:58	XML Source File	9 KB

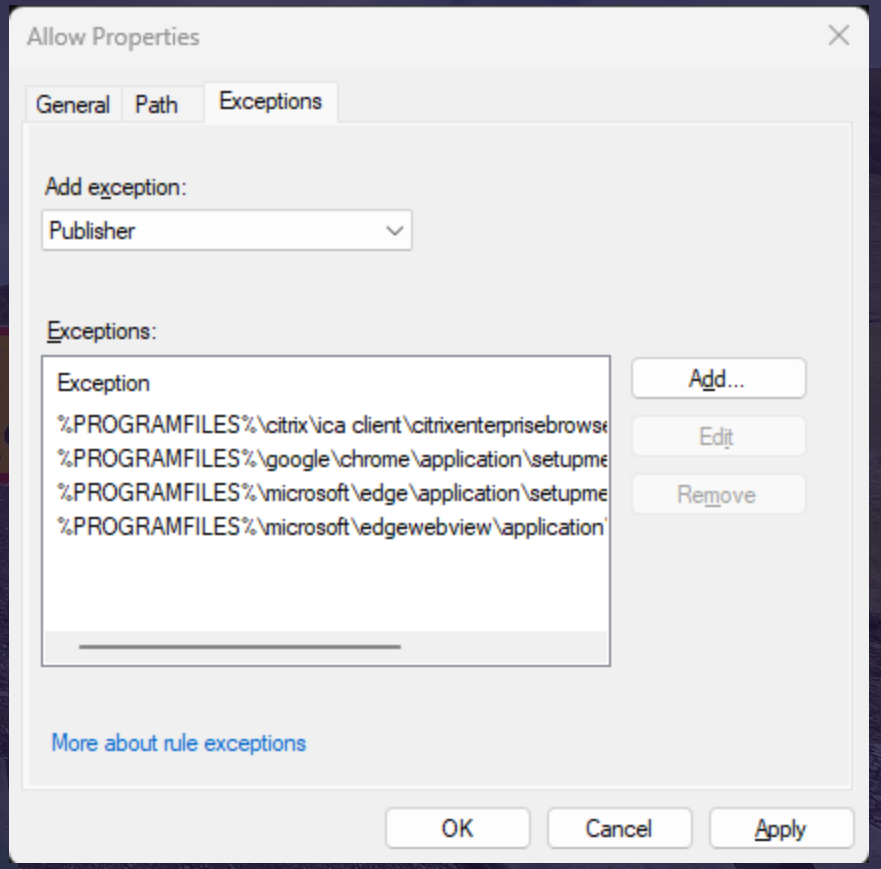
Application whitelisting the easy way



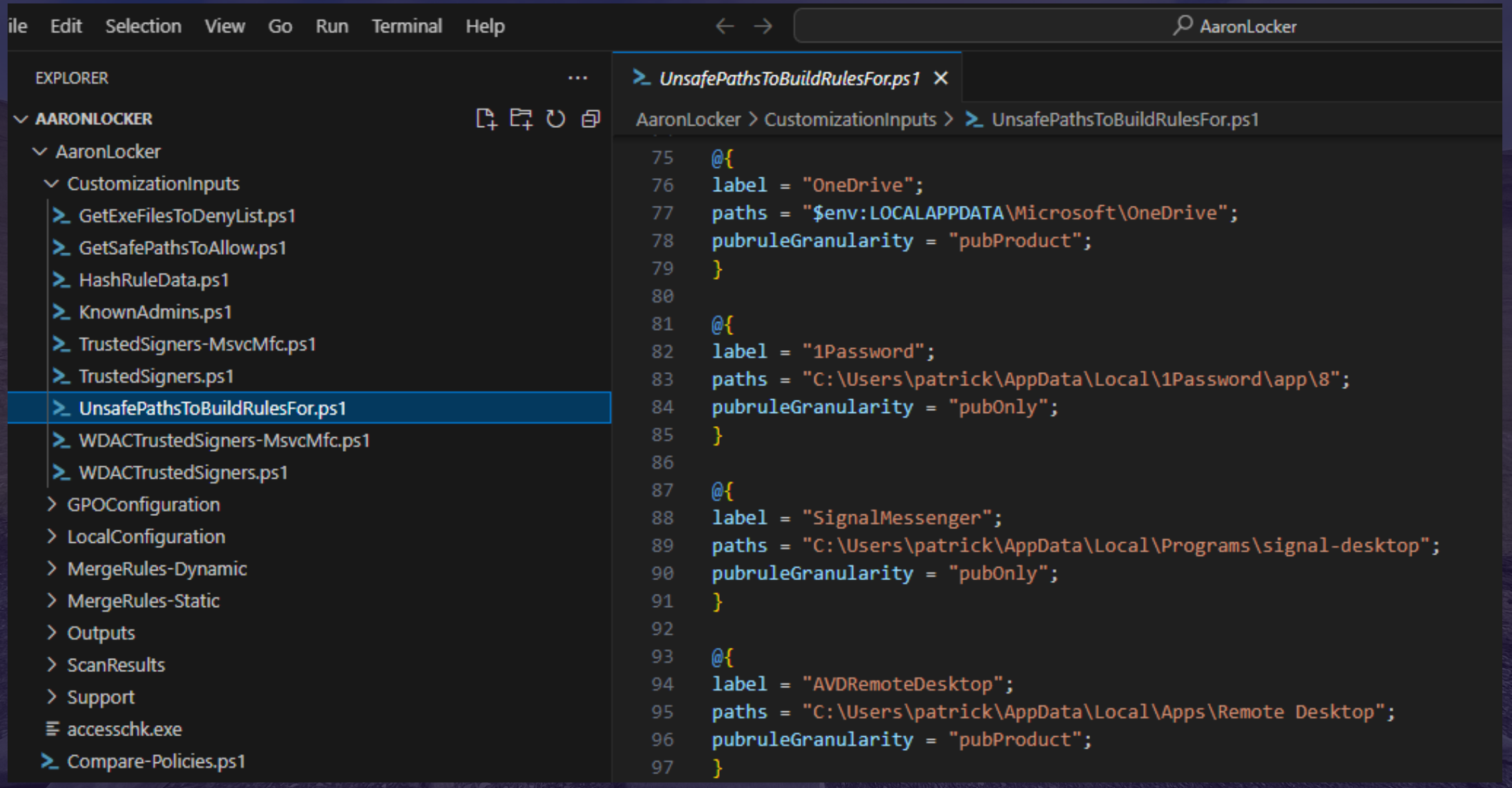
Action	User	Name	Condition	Exceptions
Allow	Everyone	ChocoLatey: CHOCOLATEY - CHOCOLATEY SHIM	Publisher	
Allow	Everyone	LogitechPresenter: LOGI PRESENTATION UI	Publisher	
Allow	Everyone	LogitechPresenter: LOGIPRESENTATIONLITEINSTALLER	Publisher	
Allow	Everyone	LogitechPresenter: LOGIPRESENTATIONUPDATER	Publisher	
Allow	Everyone	OneDrive (Win10 v1803 initial state): MICROSOFT ONEDRIVE	Publisher	
Allow	Everyone	OneDrive (Win10 v1607 initial state): ONEDRIVESETUP.EXE	Publisher	
Allow	Everyone	Microsoft Teams: Signer/product rule for O=MICROSOFT CORPORATION, L=REDM...	Publisher	
Allow	Everyone	VSCode Extensions: BICEP.LANGSERVER	Publisher	
Allow	Everyone	LogitechPresenter: LOGITECH PRESENTATION	Publisher	
Allow	Everyone	OneDrive (Win10 v1809 initial state): MICROSOFT ONEDRIVE	Publisher	
Allow	Everyone	SignalDesktop: ELEVATE APPLICATION	Publisher	
Allow	Everyone	AppLocalTeams: MICROSOFT TEAMS	Publisher	
Allow	Everyone	AppLocalTeamsMeetingPlugin: MICROSOFT TEAMS	Publisher	
Allow	Everyone	LogitechPresenter: LOGI PRESENTATION ONBOARDING	Publisher	
Allow	Everyone	OneDrive (Win10 v1803 initial state): ONEDRIVESETUP.EXE	Publisher	
Allow	Everyone	OneDrive (Win10 v1607 initial state): MICROSOFT ONEDRIVE	Publisher	
Allow	Everyone	1Password: O=AGILEBITS, S=ONTARIO, C=CA	Publisher	
Deny	Everyone	BgInfo: Disallow old versions of Sysinternals Bginfo.exe	Publisher	
Allow	Everyone	LogitechPresenter: LOGITECH ANALYTICS CLIENT	Publisher	
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	Everyone	Additional allowed path: %OSDRIVE%\PROGRAMDATA\chocolatey\bin	Path	
Allow	Everyone	All files located in the Program Files folder	Path	Yes
Allow	Everyone	Additional allowed path: %OSDRIVE%\PROGRAMDATA\MICROSOFT\WINDOWS DE...	Path	
Allow	Everyone	Additional allowed path: %OSDRIVE%\PROGRAMDATA\chocolatey\lib	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	ChocoLatey: PAGEANT.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PLINK.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PUTTY.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: msrdc.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: terraform.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PSCP.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: msrdcw.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: packer.exe - HASH RULE	File Hash	
Deny	CREATOR OWNER	Rule set created 2024-02-19 08:57	File Hash	
Allow	Everyone	ChocoLatey: rufus.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: winscp.com.exe - HASH RULE	File Hash	
Allow	Everyone	AppLocalTeamsMeetingPlugin: RELEASES.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	VSCode Extensions: inject_dll_amd64.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	OneDrive (Win10 v1607 initial state): OneDriveStandaloneUpdater.exe - HASH RULE	File Hash	
Allow	Everyone	AppLocalTeams: RELEASES.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	ChocoLatey: PUTTYGEN.EXE - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: PSFTP.EXE - HASH RULE	File Hash	
Allow	Everyone	VSCode Extensions: inject_dll_x86.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	SignalDesktop: Uninstall Signal.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	LogitechPresenter: Uninstaller.exe - HASH RULE for signed file	File Hash	
Allow	Everyone	ChocoLatey: 7z.exe - HASH RULE	File Hash	
Allow	Everyone	VSCode Extensions: terraform-ls.exe - HASH RULE	File Hash	
Allow	Everyone	StreamDeck: twitchstudiostreamdeck.exe - HASH RULE	File Hash	
Allow	Everyone	ChocoLatey: winscp.exe - HASH RULE	File Hash	
Allow	Everyone	SignalDesktop: Signal.exe - HASH RULE for signed file	File Hash	

Application whitelisting the easy way





Application whitelisting the easy way



Application whitelisting the easy way

Tips:

- Add your computer to domain if applicable
  - AaronLocker will scan UNC paths
- Add exception rules to the “CustomizationInputs” scripts
- Don’t add AppLocker rules manually
  - Do not exclude a complete user writeable folder, or your doomed!
- Rerun AaronLocker on updates (filehashes will change!)

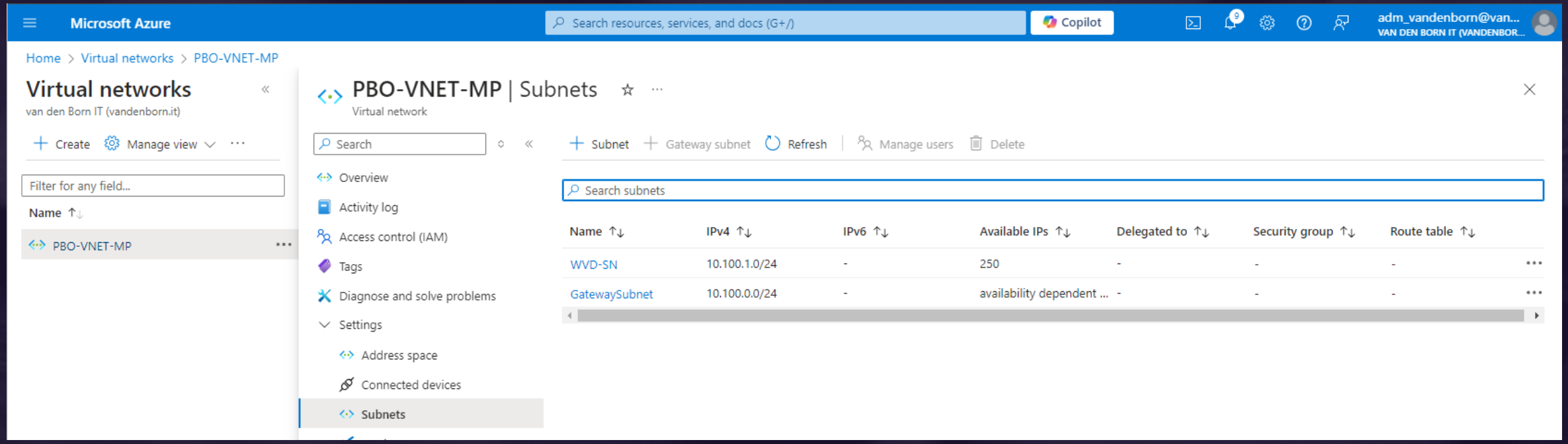
Local Admin Password Protection

Local Admin Password Protection

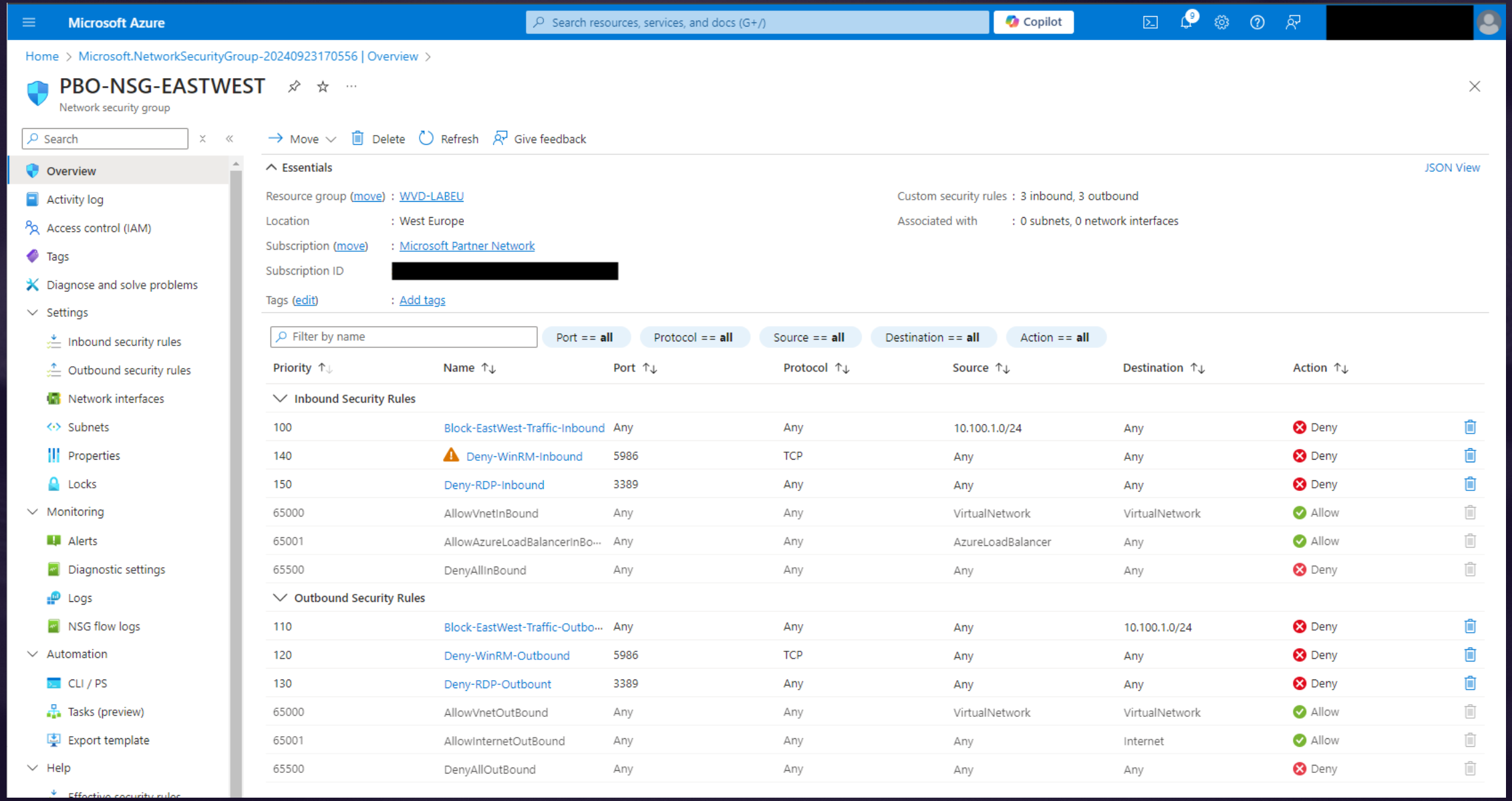
- Prevent identical local admin passwords on every session host
- Prevent pass the hash attacks
- Procedures for non-persistent images
  - CTX331247: Randomizing Local Admin Passwords in Non-persistent Environments


Block east-west network traffic

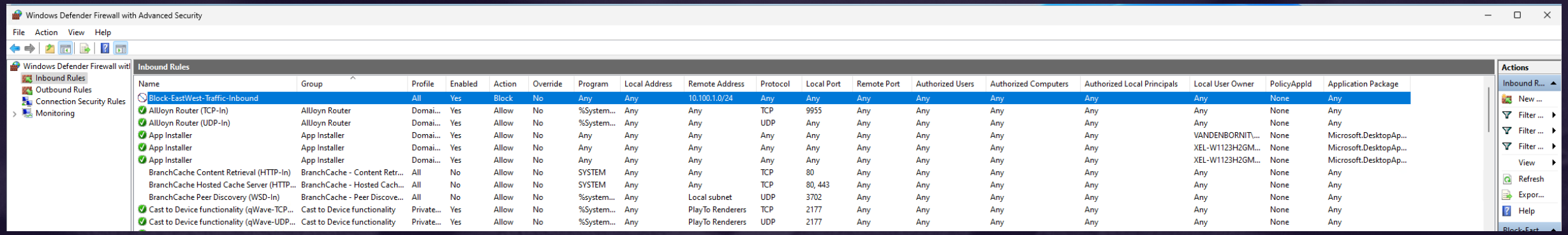
Block east-west network traffic

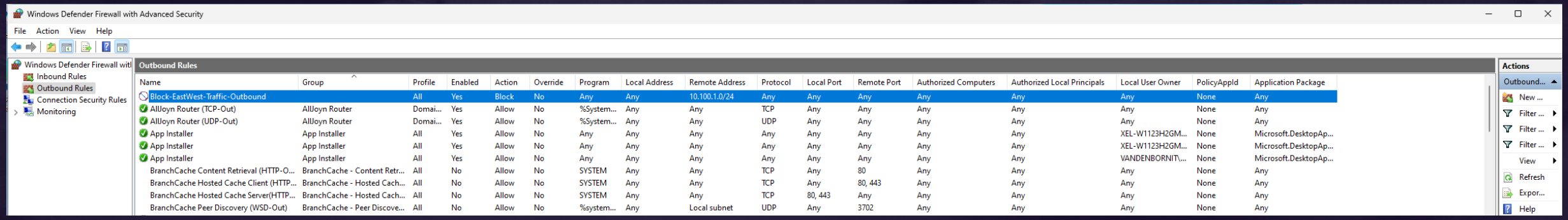


Block east-west network traffic



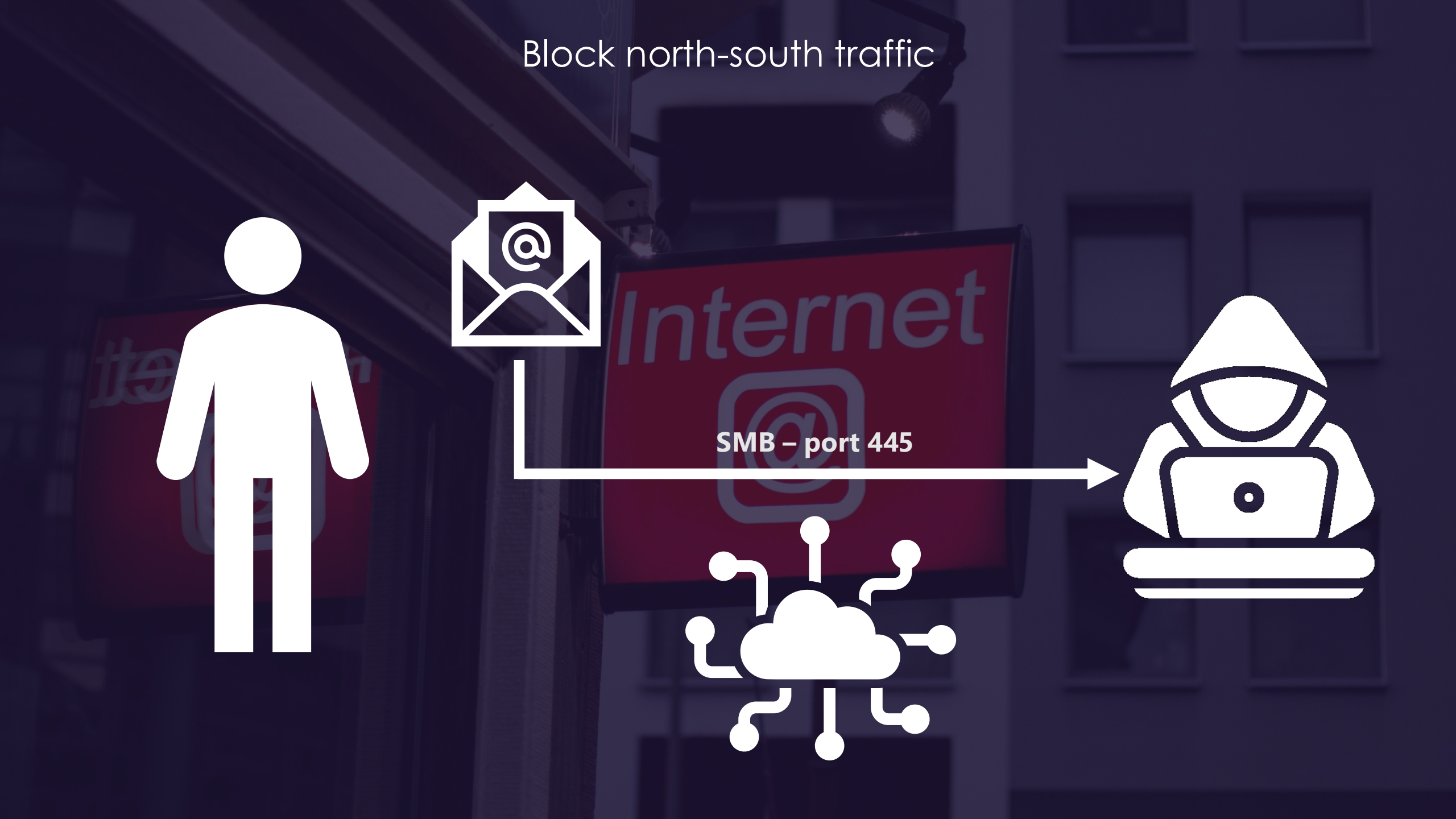
Block east-west network traffic





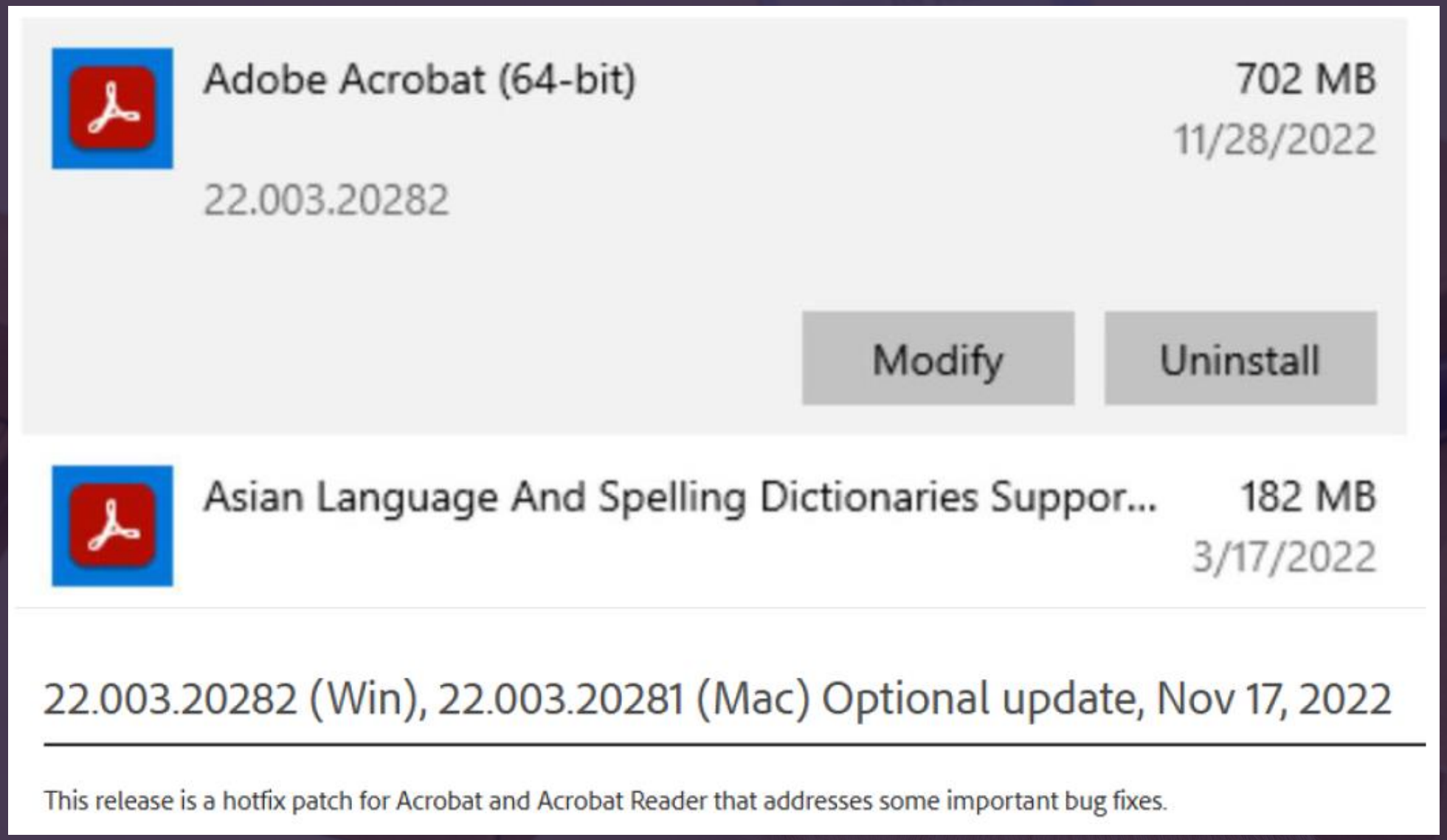
Block north-south network traffic

Block north-south traffic



Package manager

Package manager



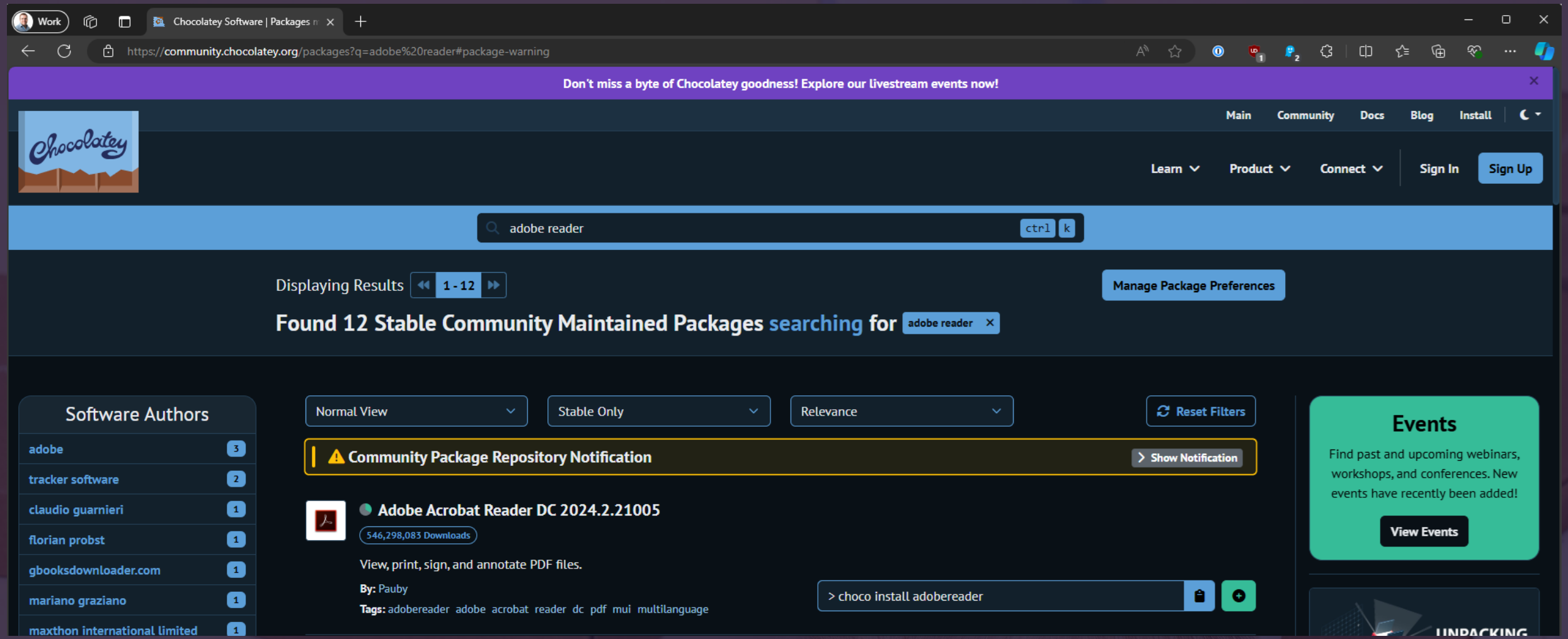
Package manager

WinGet

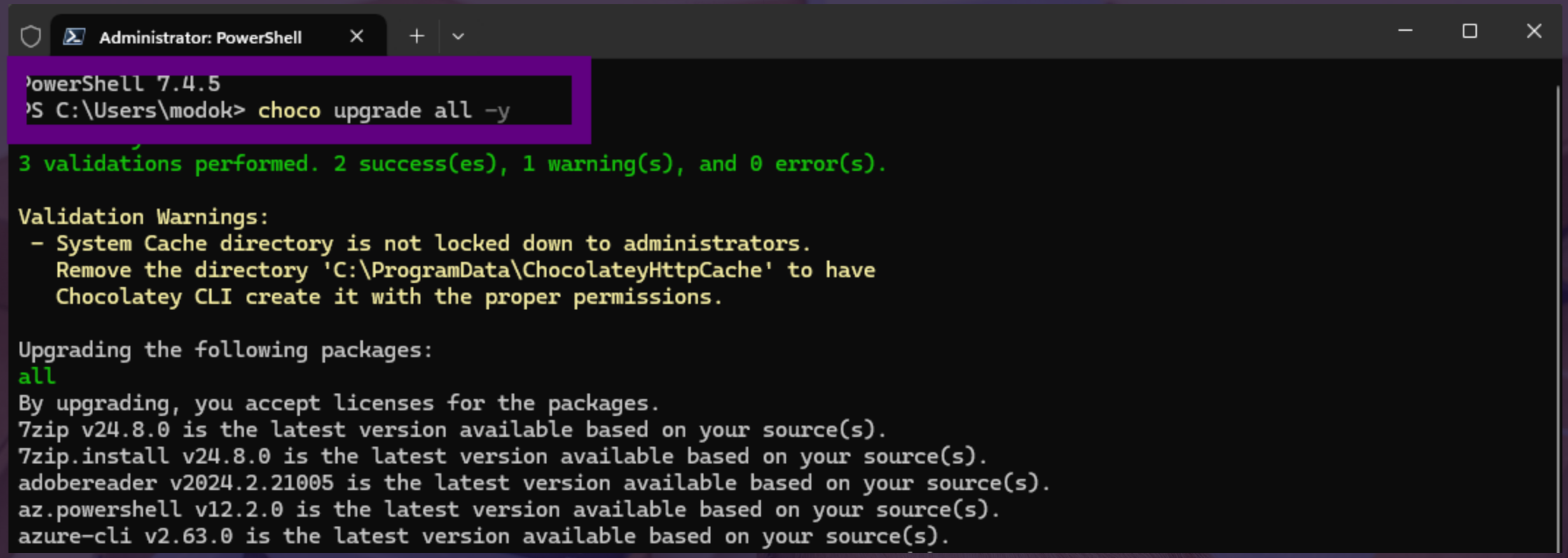
NeverRed

Evergreen

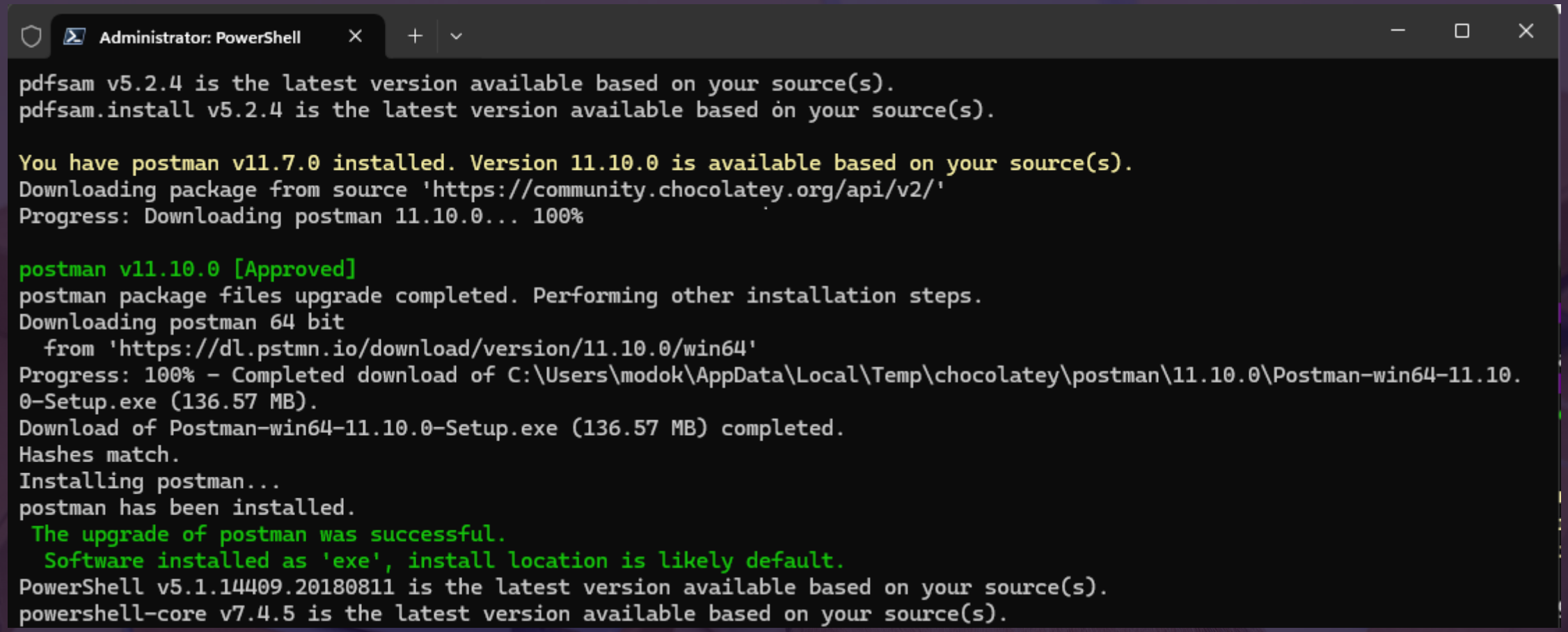
Package manager

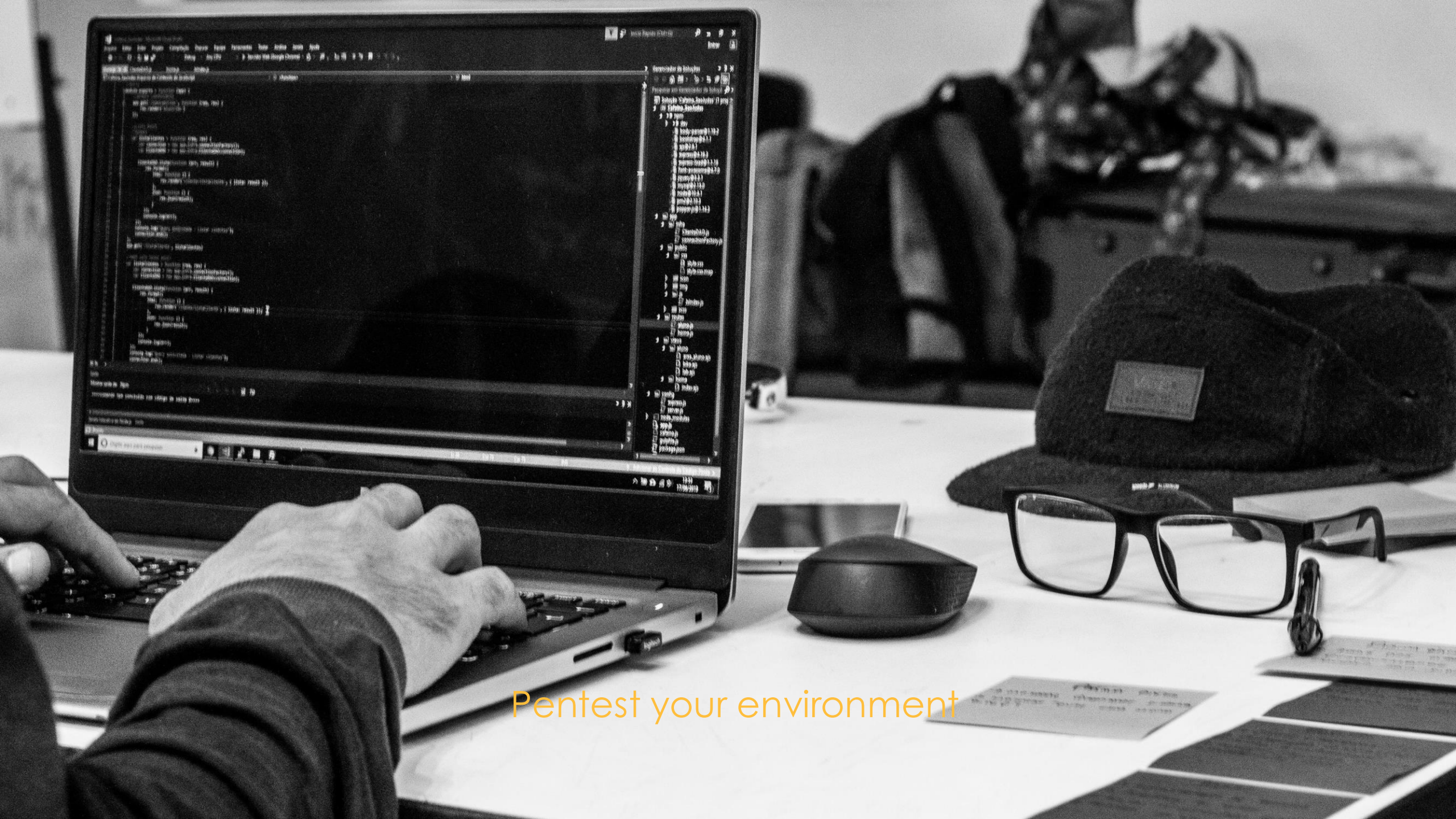


Package manager

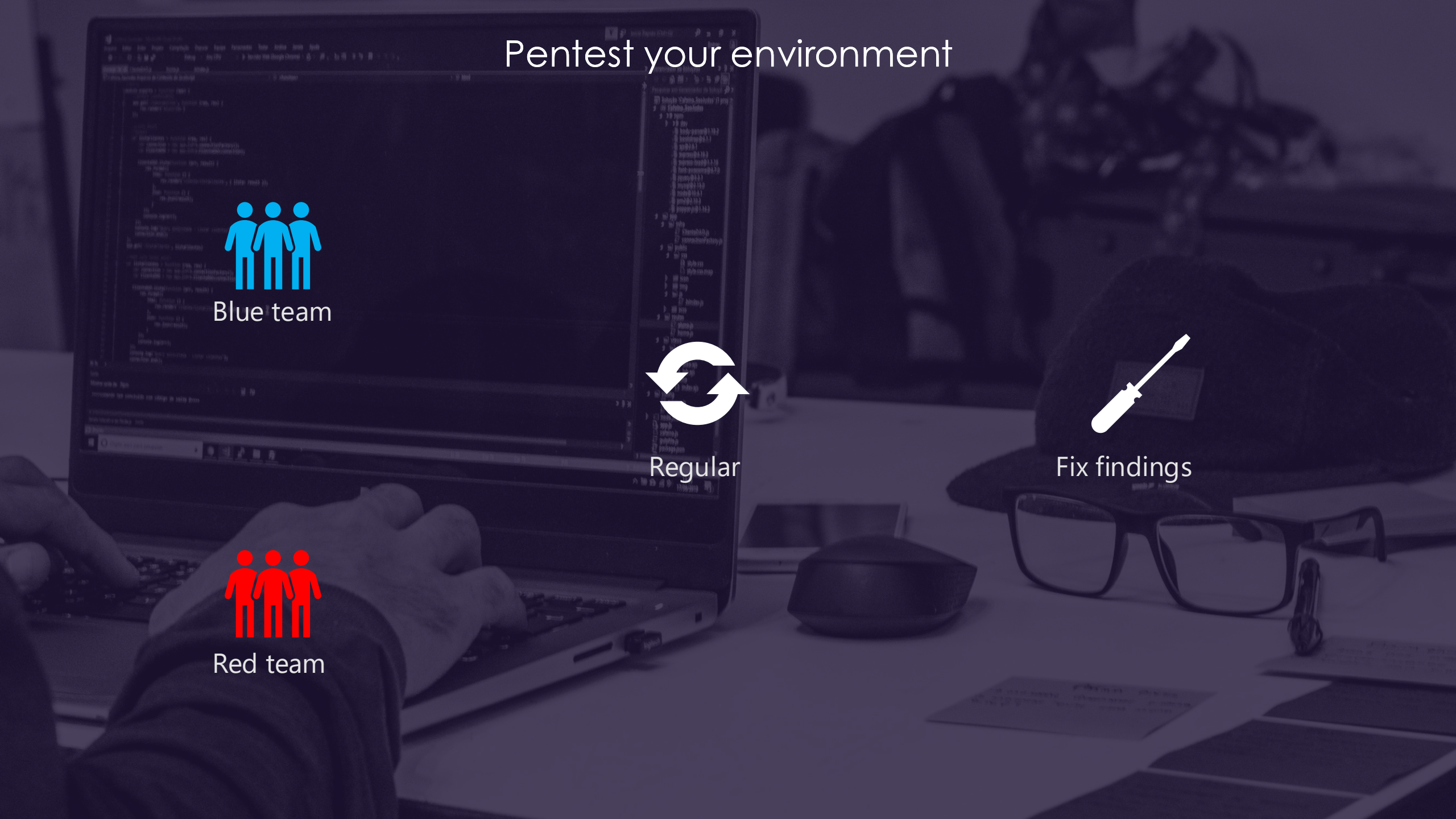


Package manager




Pentest your environment

Pentest your environment




Wrap up

Wrap up

Cyber war

Last line of defense

Harden golden image

CIS Policies

AaronLocker

East-West traffic
North-South traffic

Package manager

Penetration test