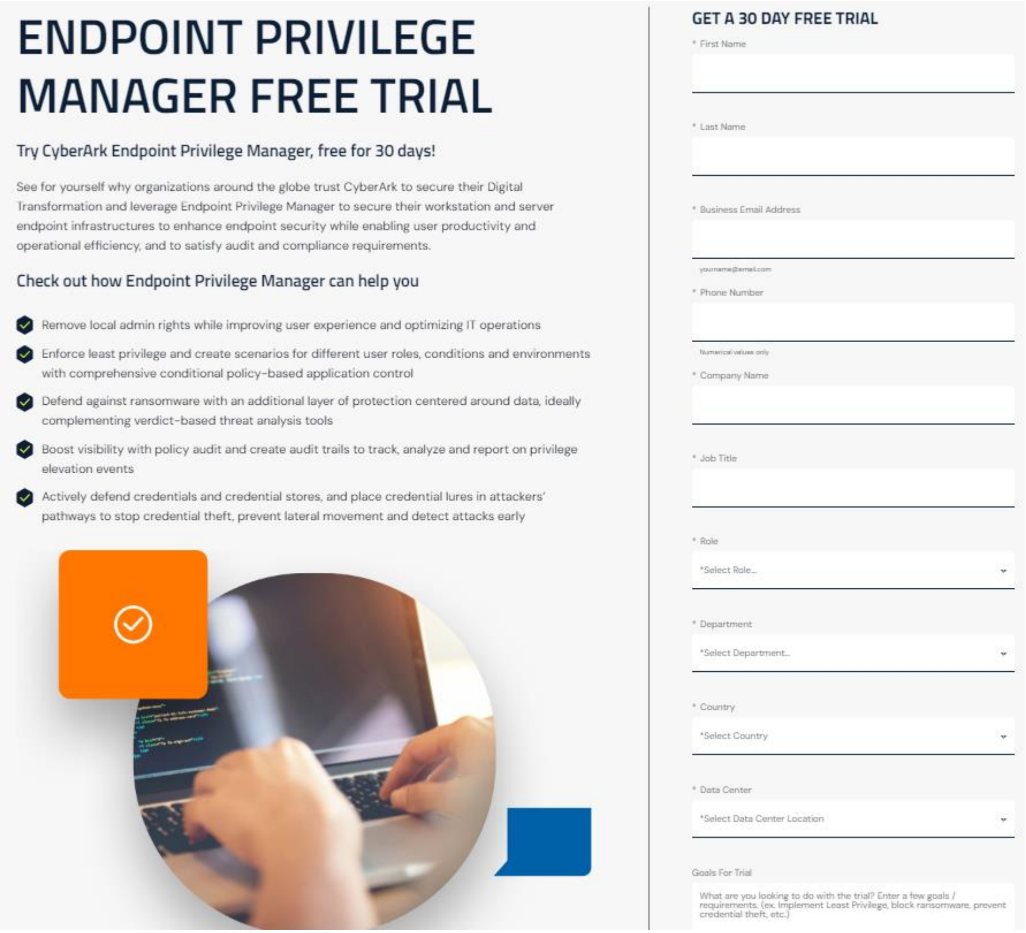
LAB – 0
AGENT INSTALL

- Request Trial
- Email Confirmation
- Registration
- Agent Download
- Installation

REGISTER FOR TRIAL



ENDPOINT PRIVILEGE MANAGER FREE TRIAL

Try CyberArk Endpoint Privilege Manager, free for 30 days!

See for yourself why organizations around the globe trust CyberArk to secure their Digital Transformation and leverage Endpoint Privilege Manager to secure their workstation and server endpoint infrastructures to enhance endpoint security while enabling user productivity and operational efficiency, and to satisfy audit and compliance requirements.

Check out how Endpoint Privilege Manager can help you

- ✓ Remove local admin rights while improving user experience and optimizing IT operations
- ✓ Enforce least privilege and create scenarios for different user roles, conditions and environments with comprehensive conditional policy-based application control
- ✓ Defend against ransomware with an additional layer of protection centered around data, ideally complementing verdict-based threat analysis tools
- ✓ Boost visibility with policy audit and create audit trails to track, analyze and report on privilege elevation events
- ✓ Actively defend credentials and credential stores, and place credential lures in attackers' pathways to stop credential theft, prevent lateral movement and detect attacks early

GET A 30 DAY FREE TRIAL

* First Name

* Last Name

* Business Email Address

yourname@email.com

* Phone Number

Numerical values only

* Company Name

* Job Title

* Role

*Select Role...

* Department

*Select Department...

* Country

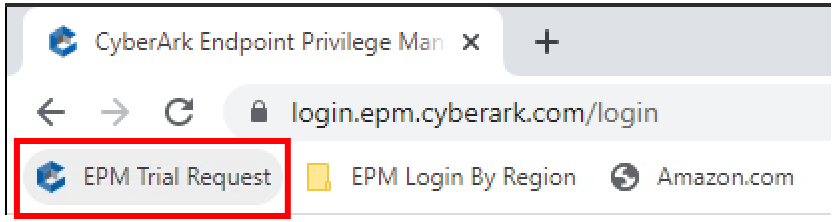
*Select Country

* Data Center

*Select Data Center Location

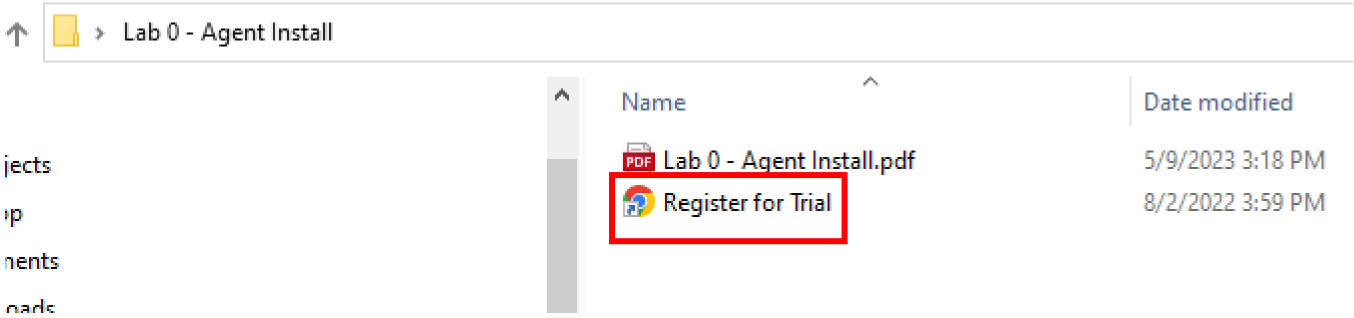
Goals For Trial

What are you looking to do with the trial? Enter a few goals / requirements. (ex. Implement Least Privilege, block ransomware, prevent credential theft, etc.)



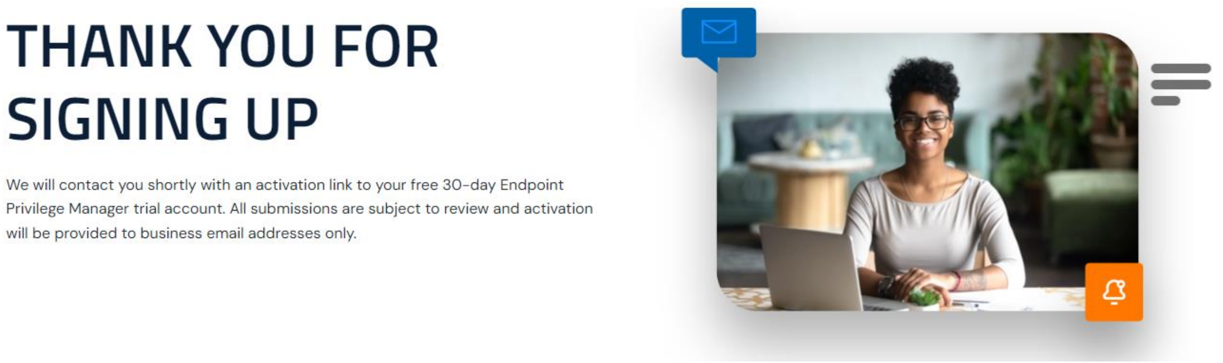
CyberArk Endpoint Privilege Man

login.epm.cyberark.com/login



Lab 0 - Agent Install

Name	Date modified
Lab 0 - Agent Install.pdf	5/9/2023 3:18 PM
Register for Trial	8/2/2022 3:59 PM

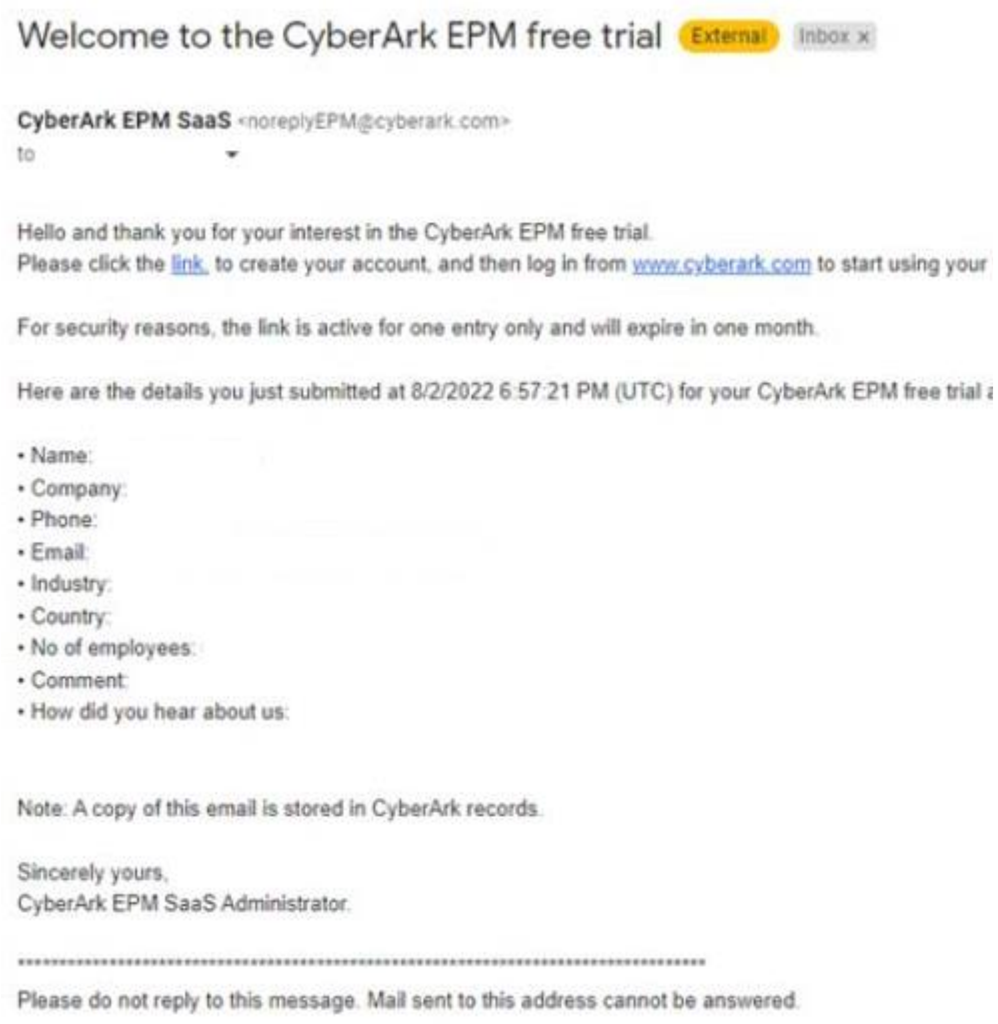


THANK YOU FOR SIGNING UP

We will contact you shortly with an activation link to your free 30-day Endpoint Privilege Manager trial account. All submissions are subject to review and activation will be provided to business email addresses only.

https://www.cyberark.com/try-buy/endpoint-privilege-manager-trial/

ACTIVATION



Welcome to the CyberArk EPM free trial

CyberArk EPM SaaS <noreplyEPM@cyberark.com>
to

Hello and thank you for your interest in the CyberArk EPM free trial.
Please click the link to create your account, and then log in from www.cyberark.com to start using your

For security reasons, the link is active for one entry only and will expire in one month.

Here are the details you just submitted at 8/2/2022 6:57:21 PM (UTC) for your CyberArk EPM free trial a

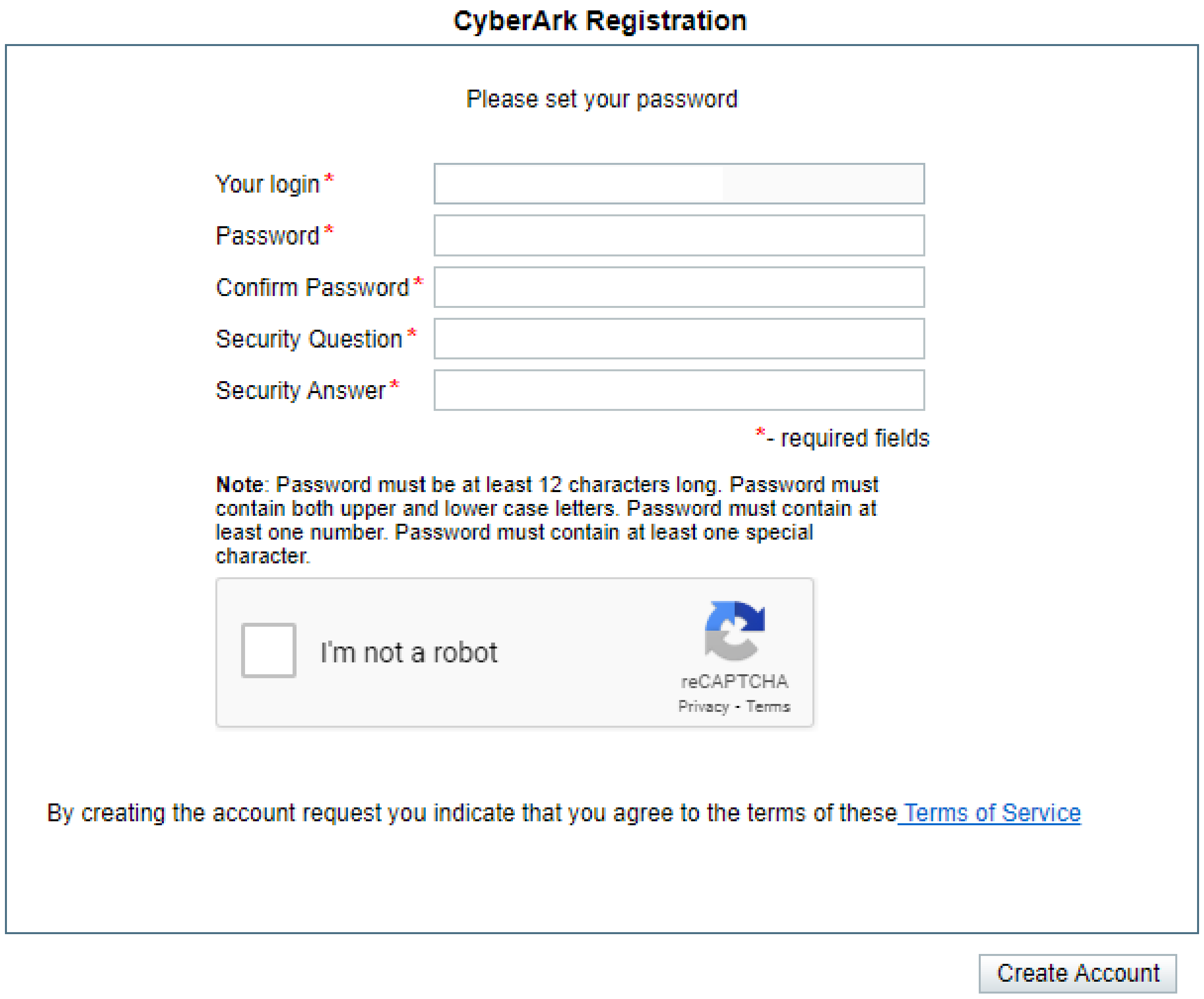
- Name:
- Company:
- Phone:
- Email:
- Industry:
- Country:
- No of employees:
- Comment:
- How did you hear about us:

Note: A copy of this email is stored in CyberArk records.

Sincerely yours,
CyberArk EPM SaaS Administrator.

****

Please do not reply to this message. Mail sent to this address cannot be answered.



CyberArk Registration

Please set your password

Your login*	
Password*	
Confirm Password*	
Security Question*	
Security Answer*	

*- required fields

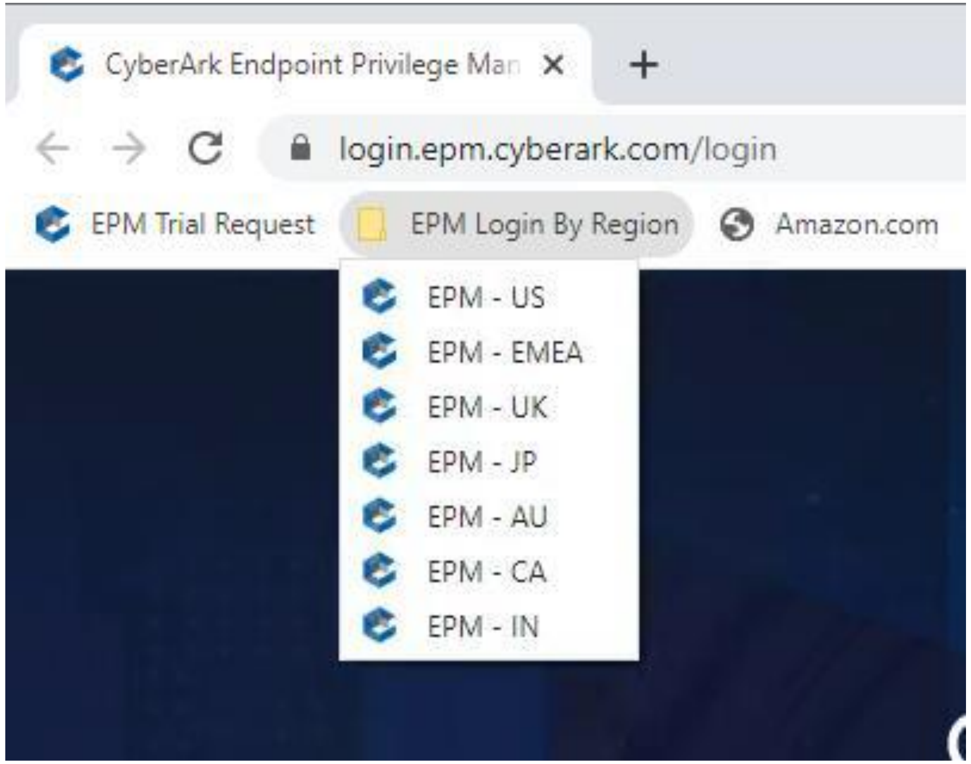
Note: Password must be at least 12 characters long. Password must contain both upper and lower case letters. Password must contain at least one number. Password must contain at least one special character.

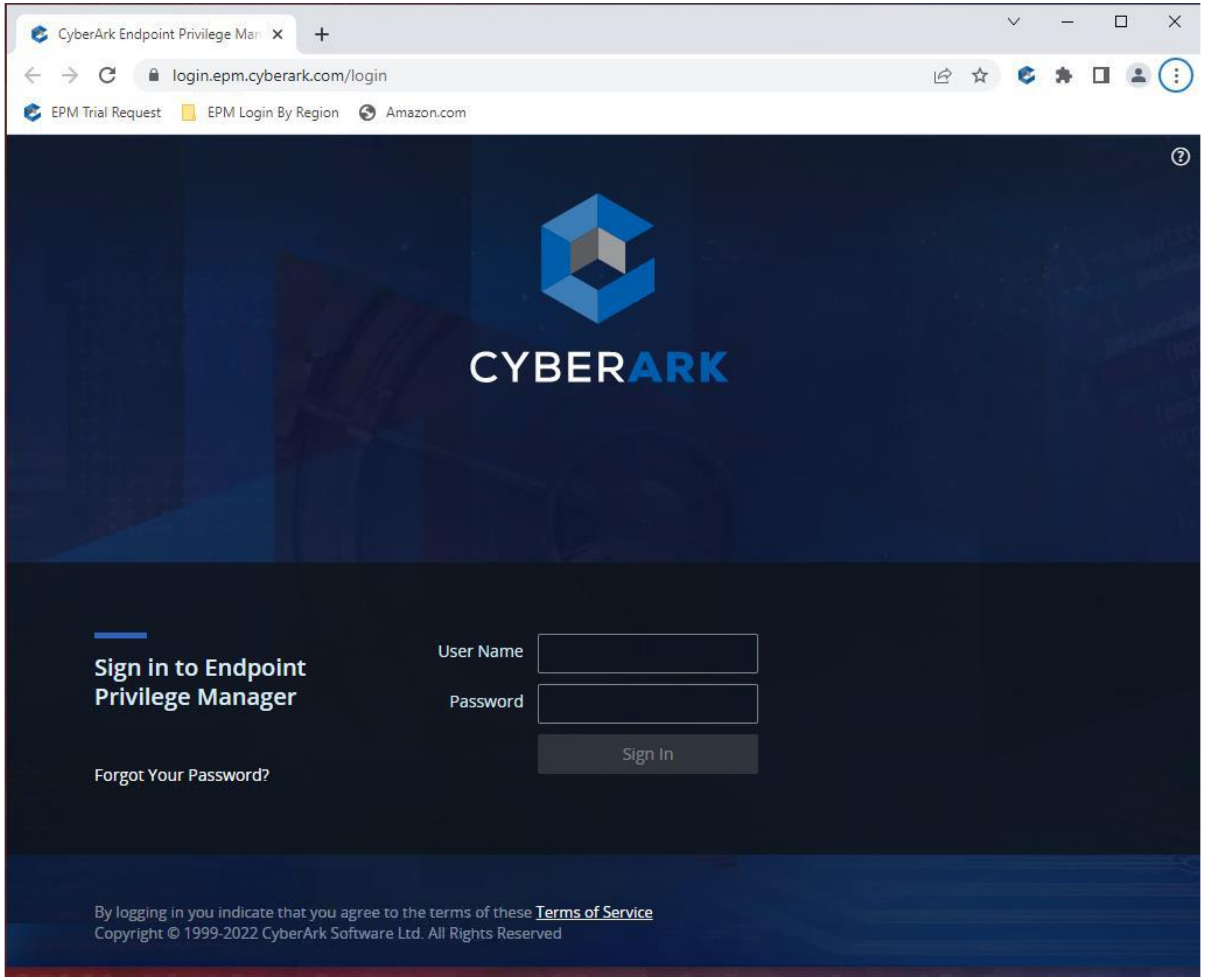
□ I'm not a robot

By creating the account request you indicate that you agree to the terms of these Terms of Service

Upon clicking 'Create Account' it may take a moment to continue
It's building the instance

AUTHENTICATING TO THE EPM PORTAL

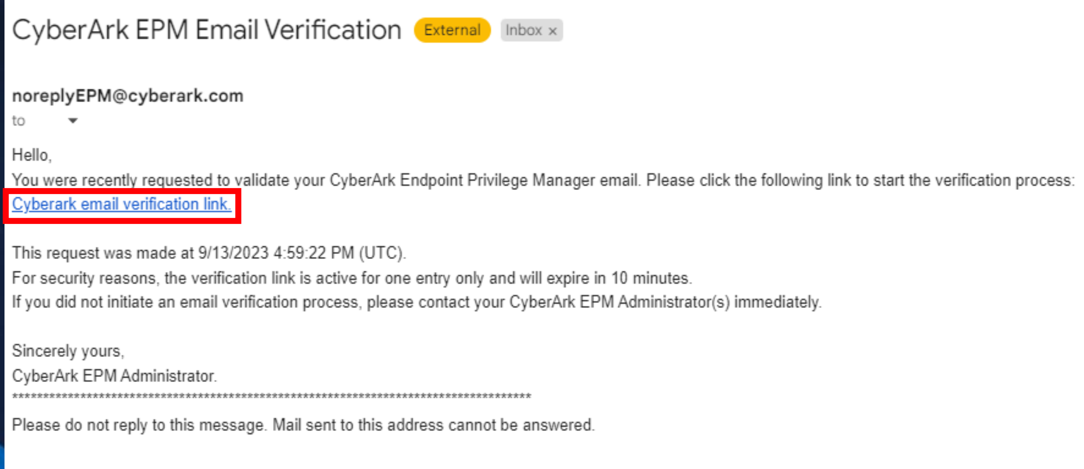




CyberArk Endpoint Privilege Man
login.epm.cyberark.com/login
EPM Trial Request
EPM Login By Region
Amazon.com
CYBERARK
Sign in to Endpoint Privilege Manager
User Name
Password
Sign In
Forgot Your Password?
By logging in you indicate that you agree to the terms of these Terms of Service
Copyright © 1999-2022 CyberArk Software Ltd. All Rights Reserved

EMAIL VERIFICATION

- ○ Once verified, from within the VM login to the EPM portal
- ○ Use the bookmarks tab to select the correct instance



CyberArk EPM Email Verification

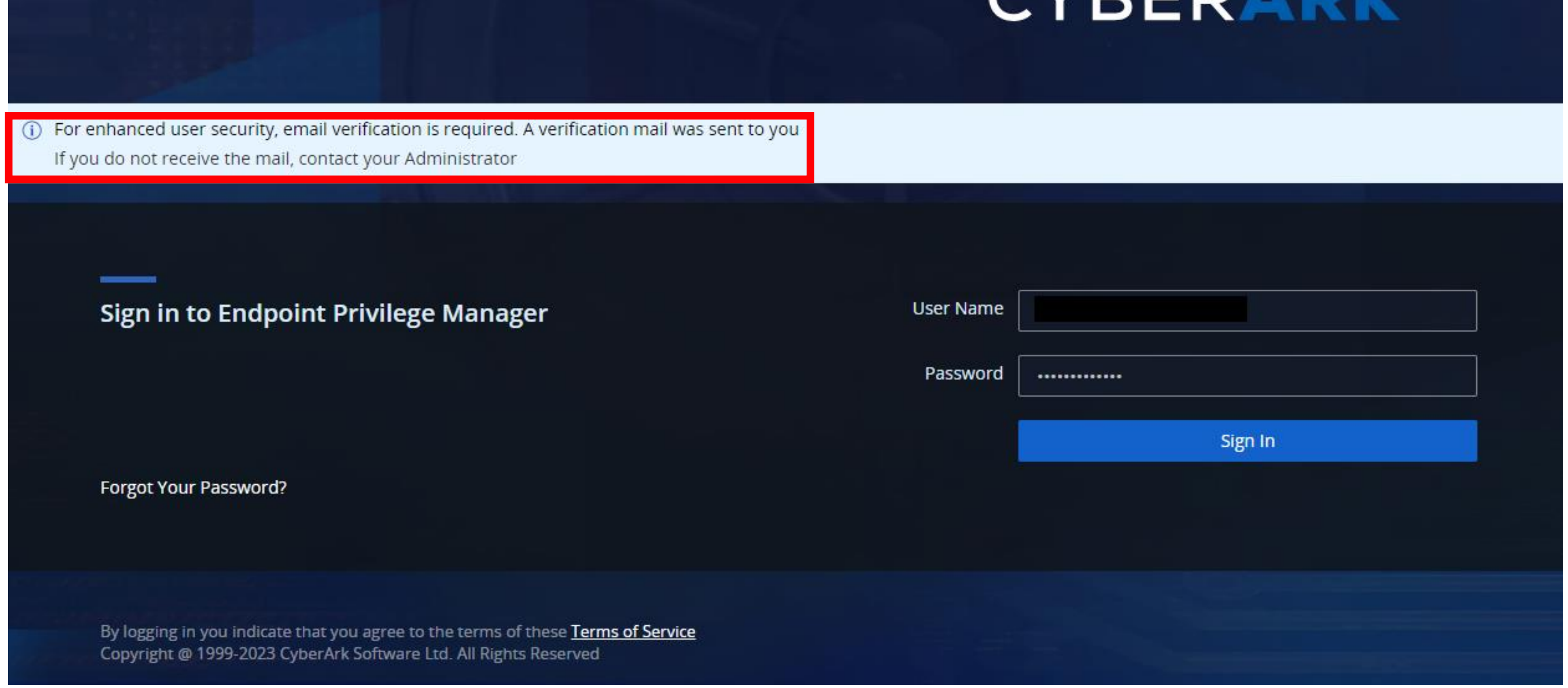
noreplyEPM@cyberark.com
to

Hello,
You were recently requested to validate your CyberArk Endpoint Privilege Manager email. Please click the following link to start the verification process:
Cyberark email verification link.

This request was made at 9/13/2023 4:59:22 PM (UTC).
For security reasons, the verification link is active for one entry only and will expire in 10 minutes.
If you did not initiate an email verification process, please contact your CyberArk EPM Administrator(s) immediately.

Sincerely yours,
CyberArk EPM Administrator.
****

Please do not reply to this message. Mail sent to this address cannot be answered.



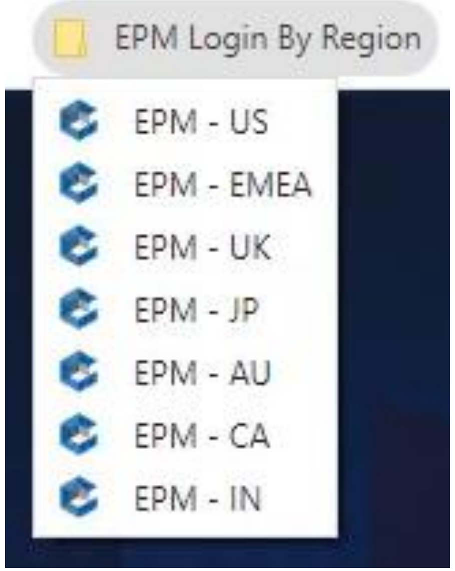
ⓘ For enhanced user security, email verification is required. A verification mail was sent to you
If you do not receive the mail, contact your Administrator

Sign in to Endpoint Privilege Manager

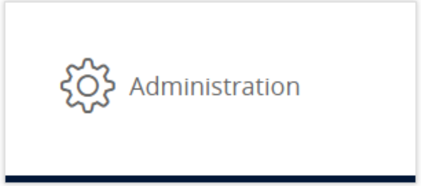
User Name: [redacted]

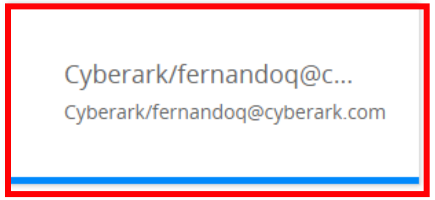
Password: ••••••••••••••

By logging in you indicate that you agree to the terms of these Terms of Service
Copyright @ 1999-2023 CyberArk Software Ltd. All Rights Reserved

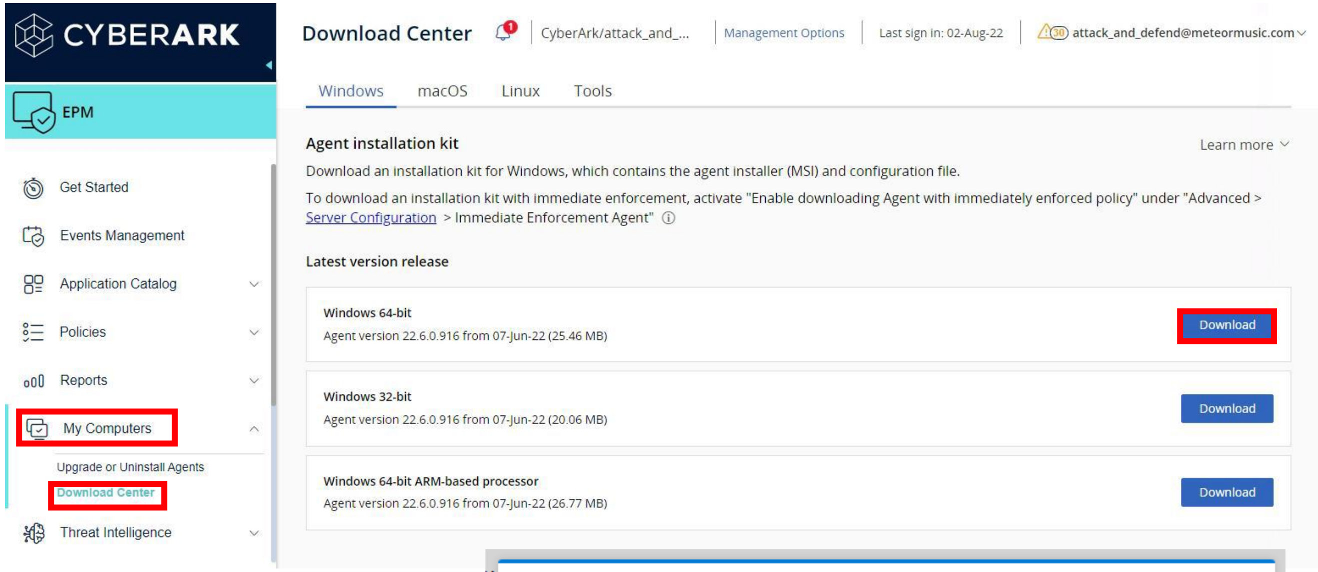


AGENT INSTALL





- Select the platform /cyberark/<<YourTenant>>
- Navigate to My Computers\Download Center
- Download the 64-bit platform agent



Agent installation kit

Download an installation kit for Windows, which contains the agent installer (MSI) and configuration file.

To download an installation kit with immediate enforcement, activate "Enable downloading Agent with immediately enforced policy" under "Advanced > Server Configuration > Immediate Enforcement Agent"

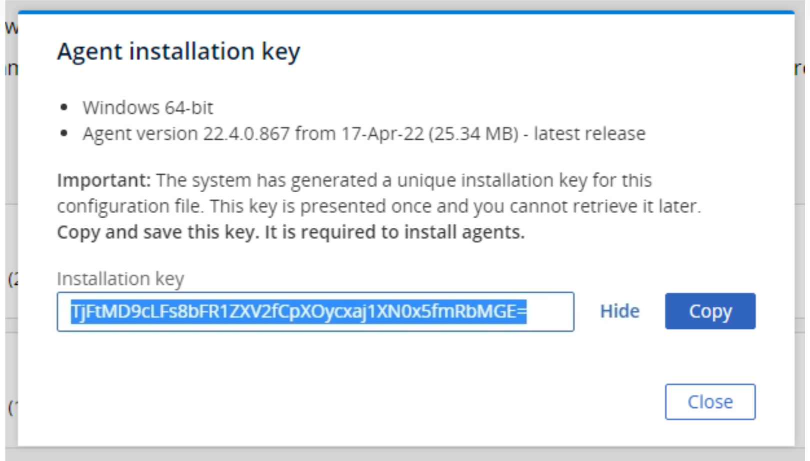
Latest version release

Windows 64-bit
Agent version 22.6.0.916 from 07-Jun-22 (25.46 MB) Download

Windows 32-bit
Agent version 22.6.0.916 from 07-Jun-22 (20.06 MB) Download

Windows 64-bit ARM-based processor
Agent version 22.6.0.916 from 07-Jun-22 (26.77 MB) Download

- Copy the installation key to <u>your VM's</u> clipboard for later use. Extract/Unzip the CyberArkEPMAgentSetupWindows.zip file
  There will be 2 files, the MSI and a .config file



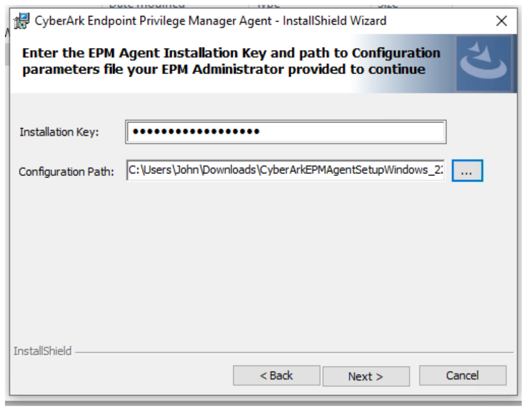
Agent installation key

- Windows 64-bit
- Agent version 22.4.0.867 from 17-Apr-22 (25.34 MB) - latest release

Important: The system has generated a unique installation key for this configuration file. This key is presented once and you cannot retrieve it later. **Copy and save this key. It is required to install agents.**

Installation key: TjFtMD9cLFs8bFR1ZXV2fCpXOycxaj1XN0x5fmRbMGE=

- Install the MSI file.
  - Paste the installation key from the clipboard and select the config file



CyberArk Endpoint Privilege Manager Agent - InstallShield Wizard

Enter the EPM Agent Installation Key and path to Configuration parameters file your EPM Administrator provided to continue

Installation Key: ••••••••••••••••••

Configuration Path: C:\Users\John\Downloads\CyberArkEPMAgentSetupWindows_2:

<u>DOWNLOAD THE MSI TO THE LAB ENVIRONMENT</u>

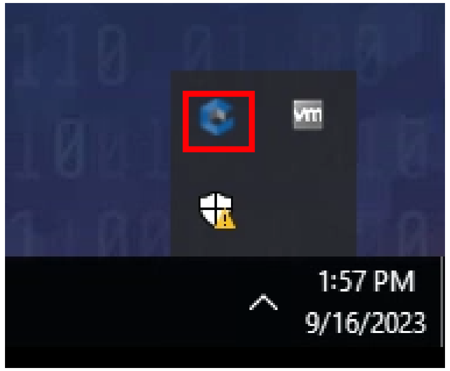
<u>DO NOT INSTALL THE AGENT ON YOUR LOCAL COMPUTER</u>

DOWNLOAD THE MSI TO THE LAB ENVIRONMENT

IF YOU INSTALL THE AGENT LOCALLY
INSTRUCTOR
YOU'RE GOING TO HAVE A BAD TIME

DO NOT INSTALL THE AGENT ON YOUR LOCAL COMPUTER

AGENT INSTALL CONFIRMATION



- Click Complete_Agent_Install.bat
  The system will reboot
- Upon successful reboot, look in the CyberArk logo in the system tray/notification area
  It should automatically log you on as John
- This confirms the agent is properly installed

At this point, the agent is installed and running
You can proceed to any of the labs.

ATTACK + DEFEND

LAB 1 – RANSOMWARE PROTECTION

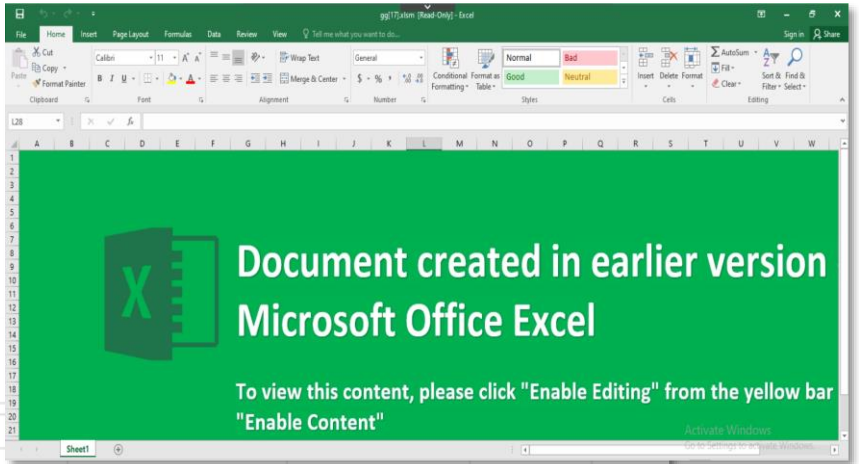
Protect from ransomware compromise

LAB 1 RANSOMWARE PROTECTION

- Open an infected file
- Survey the damage
- Reset and decrypt
- Create Ransomware policy
- Replay attack scenario

EXECUTING RANSOMWARE

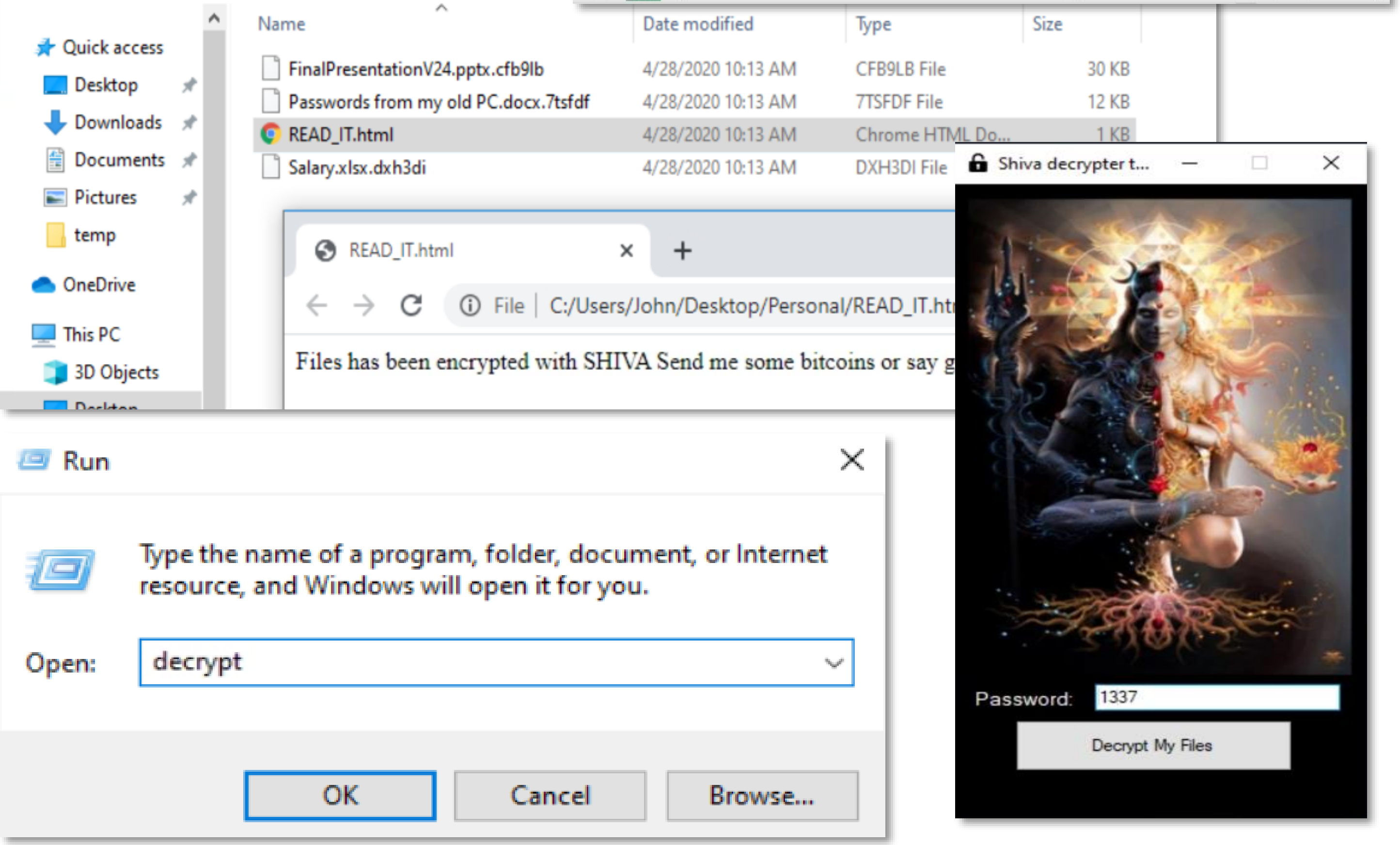
- Open \Lab 1 – Ransomware\Totally_Not_Ransomware.xlsm **(OPEN THE FILE ONLY ONCE)**



Document created in earlier version Microsoft Office Excel

To view this content, please click "Enable Editing" from the yellow bar "Enable Content"

- Go back to Personal Folder
- Read the HTML file
- Oooops ! 🔒 🔑



Personal

File Home Share View

This PC › Desktop › Personal

Name	Date modified	Type	Size
FinalPresentationV24.pptx.cfb9lb	4/28/2020 10:13 AM	CFB9LB File	30 KB
Passwords from my old PC.docx.7tsfdf	4/28/2020 10:13 AM	7TSFDF File	12 KB
READ_IT.html	4/28/2020 10:13 AM	Chrome HTML Do...	1 KB
Salary.xlsx.dxh3di	4/28/2020 10:13 AM	DXH3DI File	

READ_IT.html

File | C:/Users/John/Desktop/Personal/READ_IT.ht

Files has been encrypted with SHIVA Send me some bitcoins or say g

Shiva decrypter t...

Password: 1337

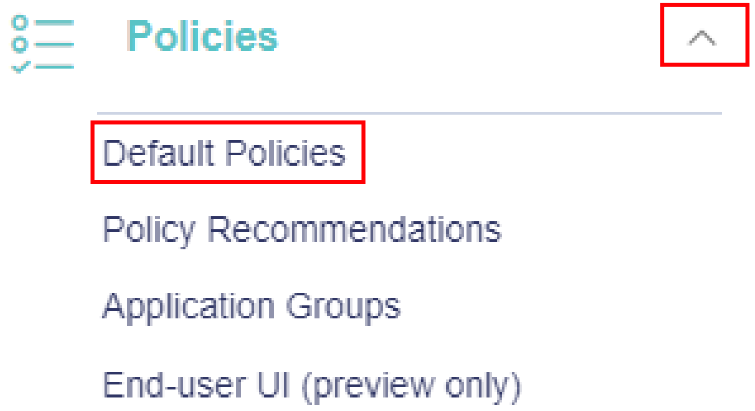
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

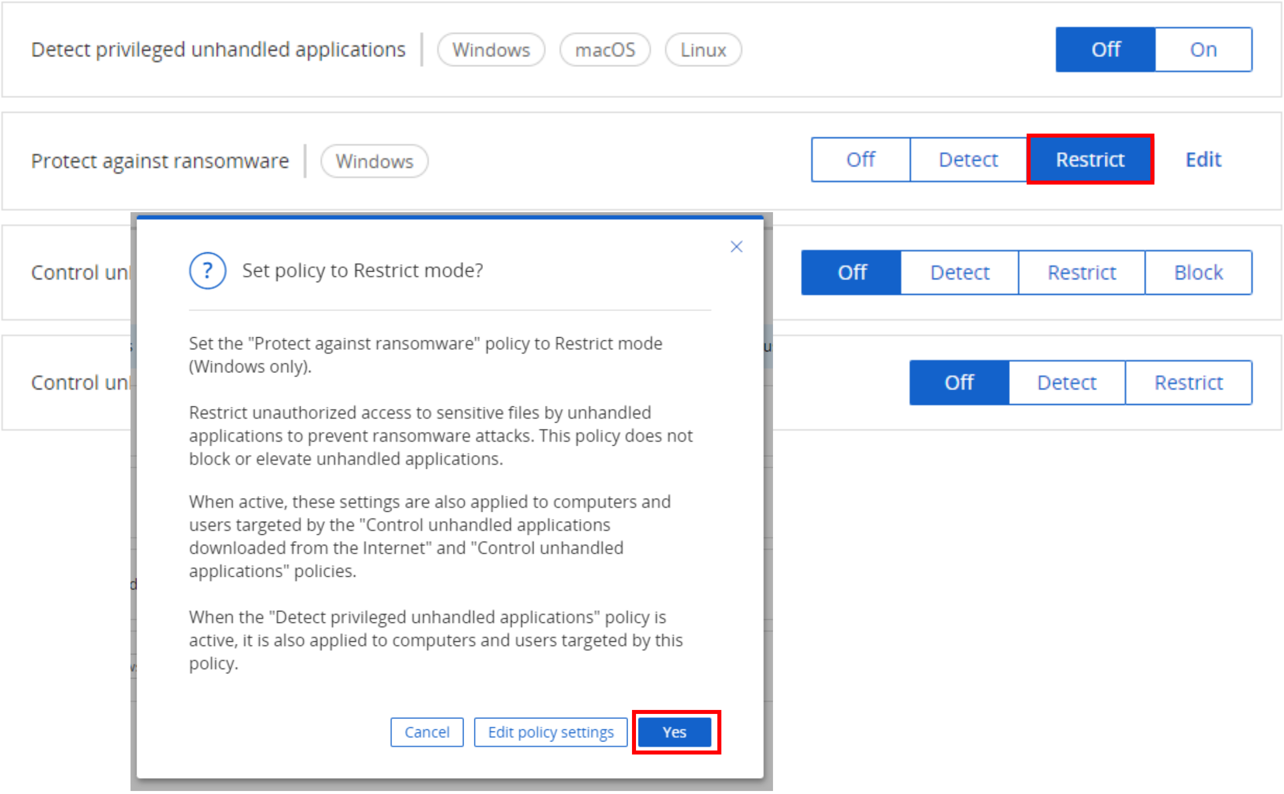
Open: decrypt

- Run \Lab 1 – Ransomware\decrypt.bat
- The password to decrypt: 1337
- Check your personal folder

ENABLE RANSOMWARE PROTECTION



- On the left menu, expand Policies by clicking ^
- Select Default Policies



Detect privileged unhandled applications | Windows macOS Linux — Off On

Protect against ransomware | Windows — Off Detect Restrict Edit

Control un — Off Detect Restrict Block

Control un — Off Detect Restrict

Set policy to Restrict mode?

Set the "Protect against ransomware" policy to Restrict mode (Windows only).

Restrict unauthorized access to sensitive files by unhandled applications to prevent ransomware attacks. This policy does not block or elevate unhandled applications.

When active, these settings are also applied to computers and users targeted by the "Control unhandled applications downloaded from the Internet" and "Control unhandled applications" policies.

When the "Detect privileged unhandled applications" policy is active, it is also applied to computers and users targeted by this policy.

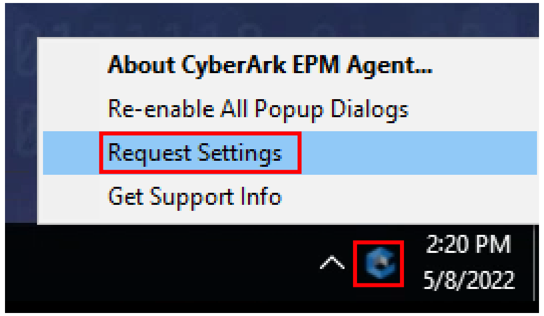
- Set ‘Protect against ransomware’ to **Restrict**
- Click Yes to confirm the policy

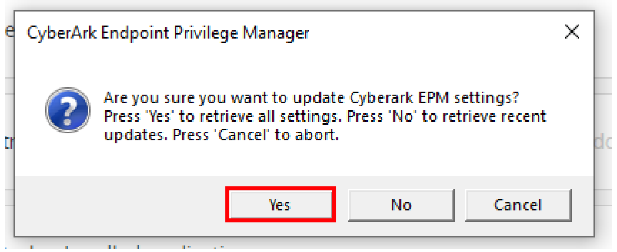
REATTEMPTING THE ATTACK

RESET POLICY

(You'll be doing this a lot throughout the lab exercises)

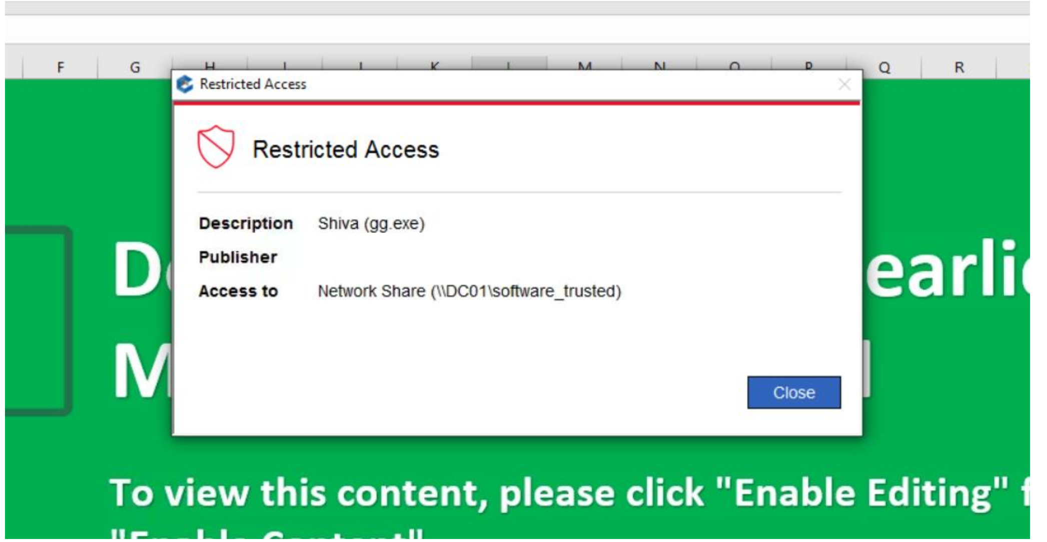
- Right-click on the CyberArk EPM icon in the system tray and select 'Request Settings'.
- Click Yes to confirm.




CyberArk Endpoint Privilege Manager

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.

- Open \Lab 1 – Ransomware\Totally_Not_Ransomware.xlsm **(PLEASE OPEN THE FILE ONLY ONCE)**
- Click Close for the Restricted Access Popups


Restricted Access

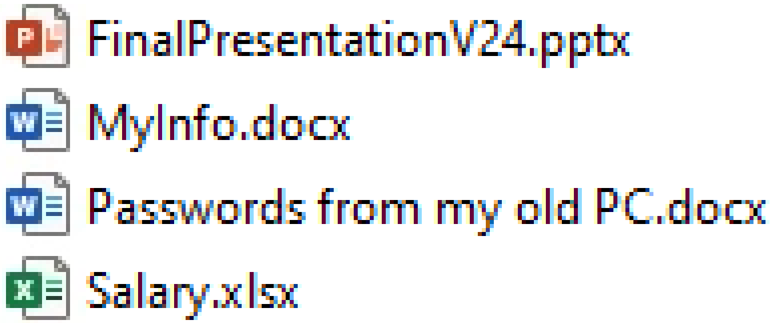
Restricted Access

Description: Shiva (gg.exe)

Publisher:

Access to: Network Share (\\DC01\software_trusted)

- Go back to Personal Folder
- Open your personal files


FinalPresentationV24.pptx

MyInfo.docx

Passwords from my old PC.docx

Salary.xlsx

ATTACK + DEFEND

LAB 2 – INTERNET DOWNLOADS

Configure policy limit access for applications downloaded from the internet

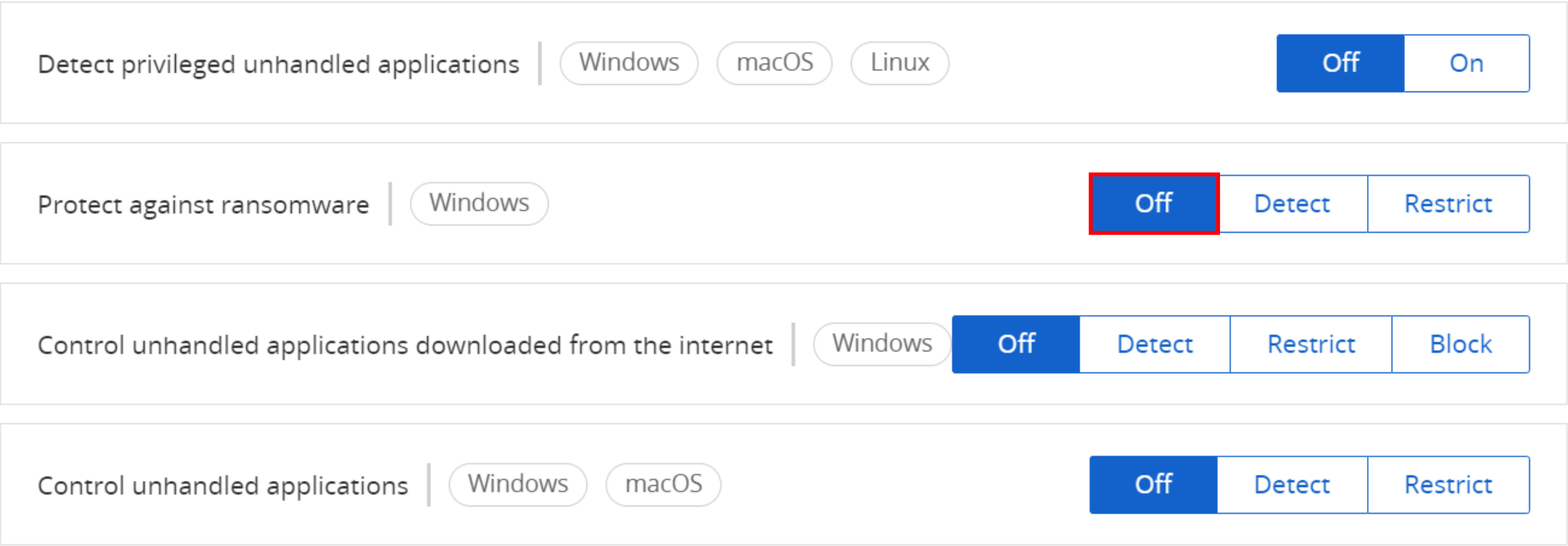
LAB 2 INTERNET DOWNLOADS

- Download and run malicious program
- Enable block policy
- Replay attack scenario

RESETTING THE CONFIGURATIONS

Some of the policies overlap. For labs to properly work correctly, it's important to reset the policies.

- Open the Default policies page
- Under Privilege Management, set all settings to Off
- Request Settings via agent

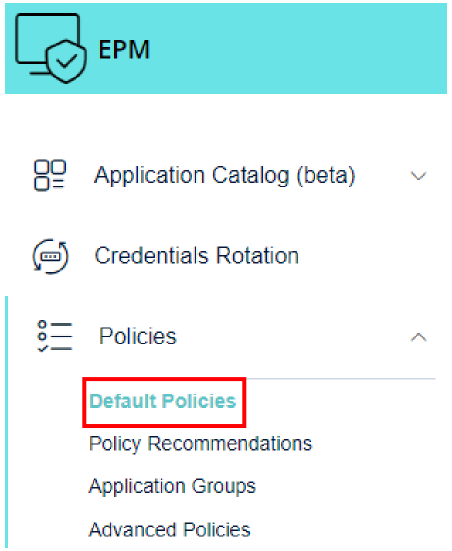


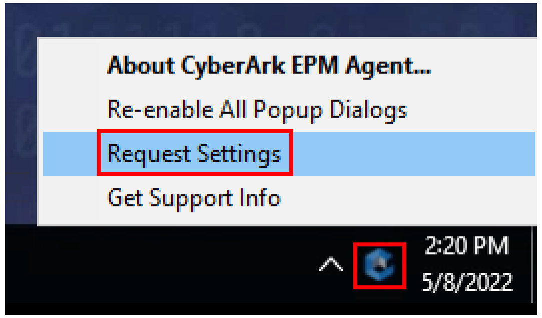
Detect privileged unhandled applications | Windows | macOS | Linux | [✓ Off] On

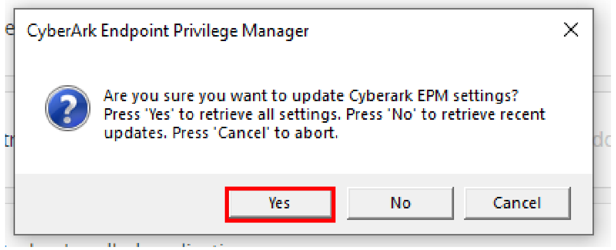
Protect against ransomware | Windows | [✓ Off] Detect Restrict

Control unhandled applications downloaded from the internet | Windows | [✓ Off] Detect Restrict Block

Control unhandled applications | Windows | macOS | [✓ Off] Detect Restrict





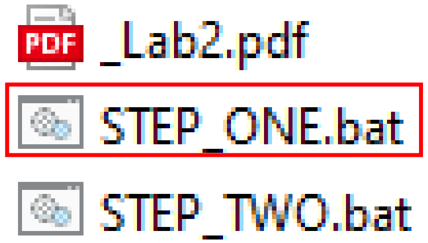


CyberArk Endpoint Privilege Manager

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.

LAUNCHING CRYPTOMINER

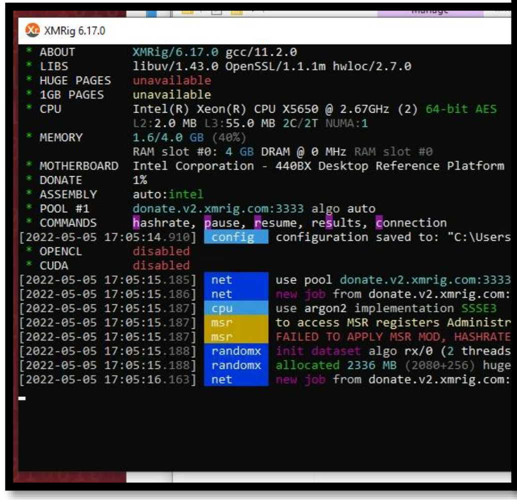
- From the ‘Lab 2 - Internet Downloads’ folder, click STEP_ONE.bat.
  - This will download and launch a cryptominer by the name of xmrig.exe and open the task manager
- Click on the Performance tab and monitor the system processes *(CPU performance should start to run at 100%)*
- Close the window or press Ctrl+C to stop mining



_Lab2.pdf

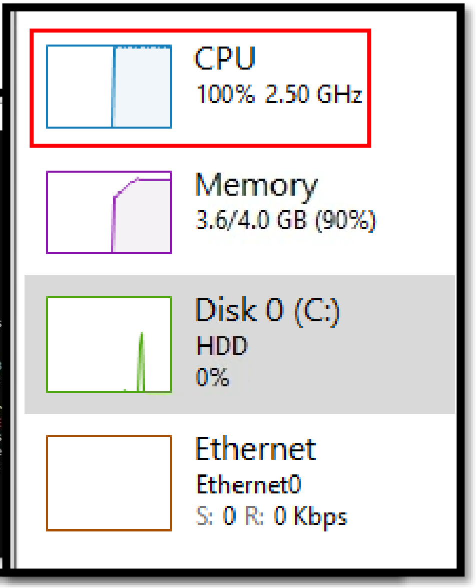
STEP_ONE.bat

STEP_TWO.bat



XMRig 6.17.0

```
 * ABOUT        XMRig/6.17.0 gcc/11.2.0
 * LIBS         libuv/1.43.0 OpenSSL/1.1.1m hwloc/2.7.0
 * HUGE PAGES   unavailable
 * 1GB PAGES    unavailable
 * CPU          Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2) 64-bit AES
                L2:2.0 MB L3:55.0 MB 2C/2T NUMA:1
 * MEMORY       1.6/4.0 GB (40%)
                RAM slot #0: 4 GB DRAM @ 0 MHz RAM slot #0
 * MOTHERBOARD  Intel Corporation - 440BX Desktop Reference Platform
 * DONATE       1%
 * ASSEMBLY     auto:intel
 * POOL #1      donate.v2.xmrig.com:3333 algo auto
 * COMMANDS     hashrate, pause, resume, results, connection
[2022-05-05 17:05:14.910]  config   configuration saved to: "C:\Users
 * OPENCL       disabled
 * CUDA         disabled
[2022-05-05 17:05:15.185]  net      use pool donate.v2.xmrig.com:3333
[2022-05-05 17:05:15.186]  net      new job from donate.v2.xmrig.com:
[2022-05-05 17:05:15.187]  cpu      use argon2 implementation SSSE3
[2022-05-05 17:05:15.187]  msr      to access MSR registers Administr
[2022-05-05 17:05:15.187]  msr      FAILED TO APPLY MSR MOD, HASHRATE
[2022-05-05 17:05:15.188]  randomx  init dataset algo rx/0 (2 threads
[2022-05-05 17:05:15.188]  randomx  allocated 2336 MB (2080+256) huge
[2022-05-05 17:05:16.163]  net      new job from donate.v2.xmrig.com:
```



CPU
100% 2.50 GHz

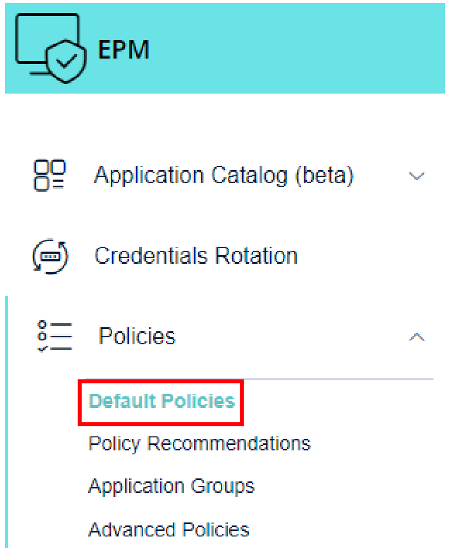
Memory
3.6/4.0 GB (90%)

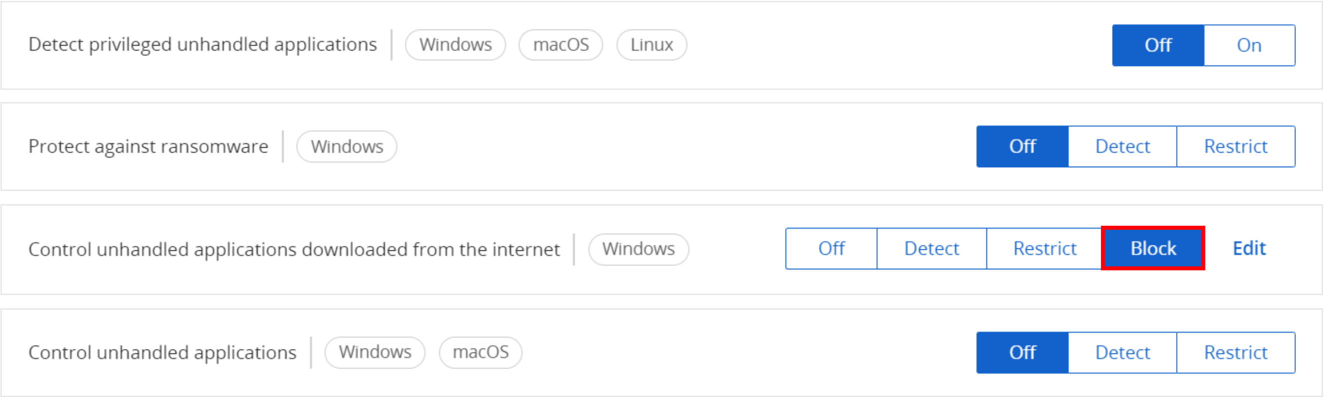
Disk 0 (C:)
HDD
0%

Ethernet
Ethernet0
S: 0 R: 0 Kbps

PREVENTING DOWNLOADED APPLICATIONS TO RUN

- Open the Default policies page
- Set 'Control unhandled applications downloaded from the internet' to Block. Click yes to confirm



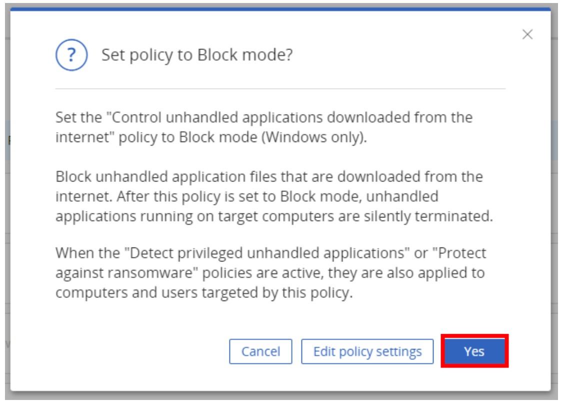


Detect privileged unhandled applications | Windows | macOS | Linux — Off | On

Protect against ransomware | Windows — Off | Detect | Restrict

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

Control unhandled applications | Windows | macOS — Off | Detect | Restrict



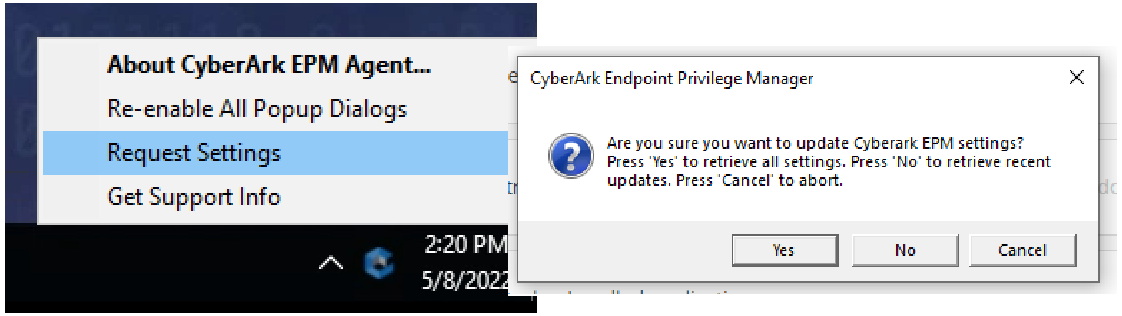
Set policy to Block mode?

Set the "Control unhandled applications downloaded from the internet" policy to Block mode (Windows only).

Block unhandled application files that are downloaded from the internet. After this policy is set to Block mode, unhandled applications running on target computers are silently terminated.

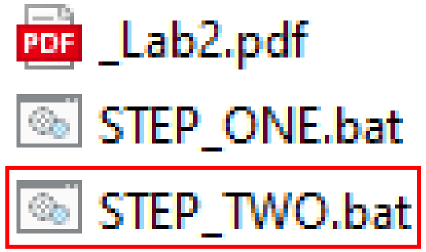
When the "Detect privileged unhandled applications" or "Protect against ransomware" policies are active, they are also applied to computers and users targeted by this policy.

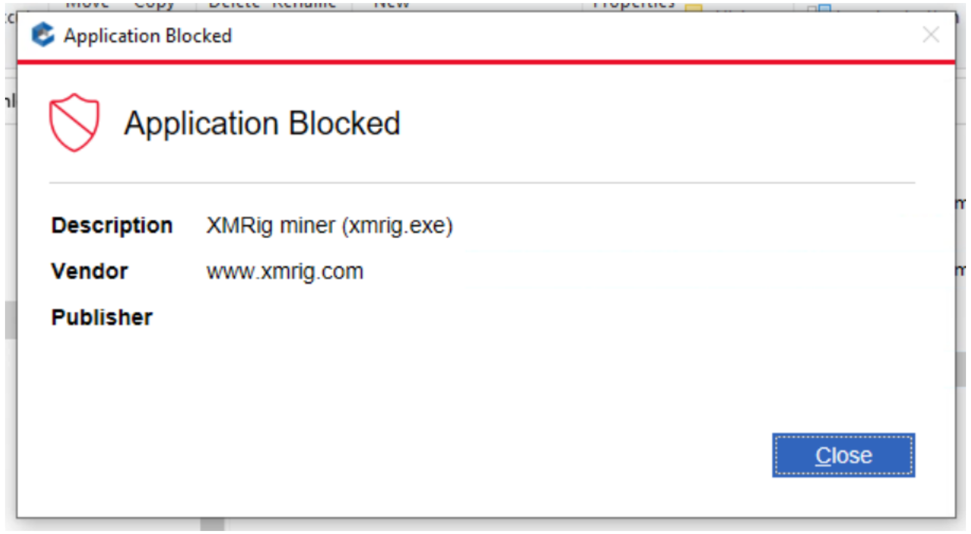
LAUNCHING CRYPTOMINER (AGAIN)


About CyberArk EPM Agent...
Re-enable All Popup Dialogs
Request Settings
Get Support Info
2:20 PM
5/8/2022
CyberArk Endpoint Privilege Manager
Yes
No
Cancel

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.

- Request latest settings/policy from EPM
- From the ‘Lab 2 - Internet Downloads’ folder, click STEP_TWO.bat
- This will re-download xmrig.exe, execute the file, and open the task manager
- Note the results





Application Blocked

Description XMRig miner (xmrig.exe)

Vendor www.xmrig.com

Publisher

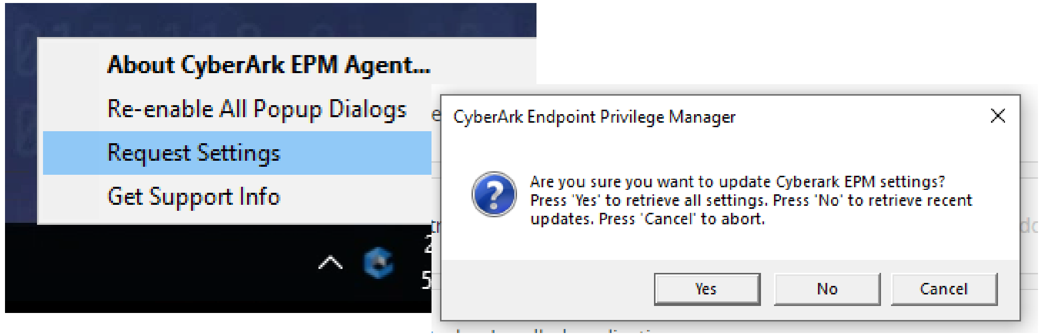
ATTACK + DEFEND

LAB 3 – TRUSTED PUBLISHERS

Setting up policies for Application Control

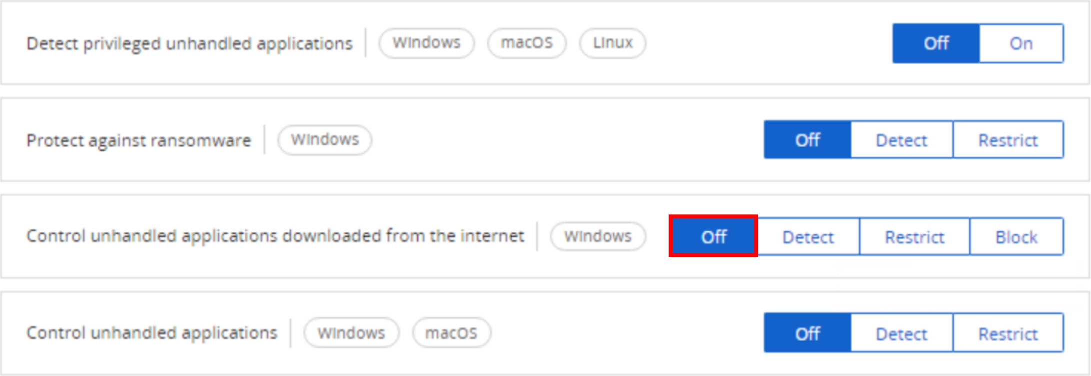
RESET POLICY

- Go back to Policies…Default Policies and set ‘Control unhandled applications downloaded from the internet’ back to Off.
- Refresh the EPM policy on the agent.



CyberArk Endpoint Privilege Manager

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.



Detect privileged unhandled applications	Windows, macOS, Linux	Off, On
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

EXECUTING UNKNOWN FILES

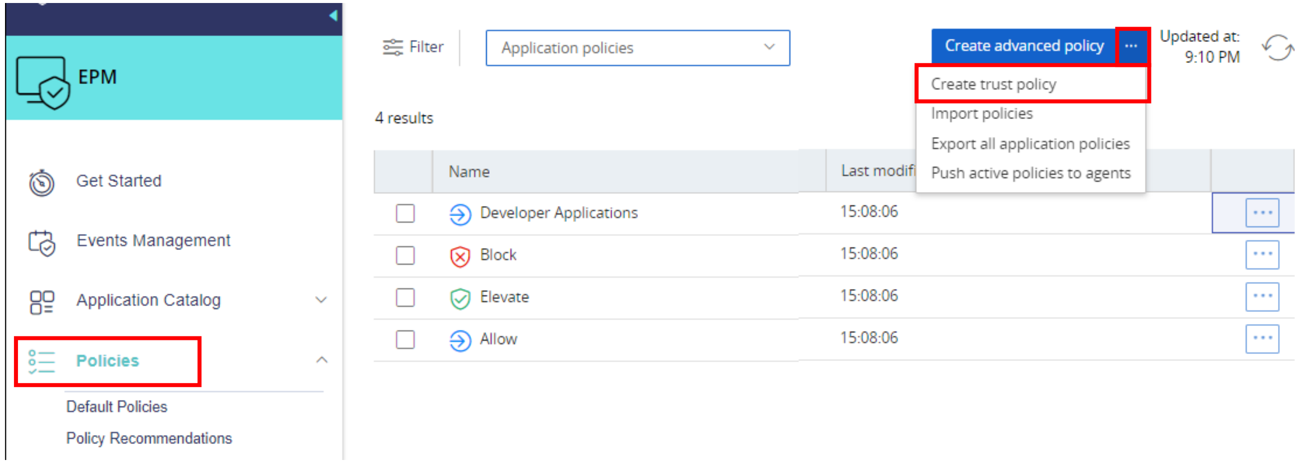
- From the ‘Lab 3 – Trusted Publishers’ folder, double-click and run ‘vlc-3.0.09-win64.exe’
Turn up the volume and enjoy! ♫

This is why you don’t want end users to download and install untrusted files!

vlc-3.0.09-win64.exe

CREATING A TRUSTED SOURCE POLICY

- Click on Policies
- Expand the menu under ‘Create advanced policy’
- Select Create trust policy



EPM

Get Started

Events Management

Application Catalog

Policies

Default Policies

Policy Recommendations

Filter

Application policies

Create advanced policy ···

Updated at: 9:10 PM

Create trust policy

Import policies

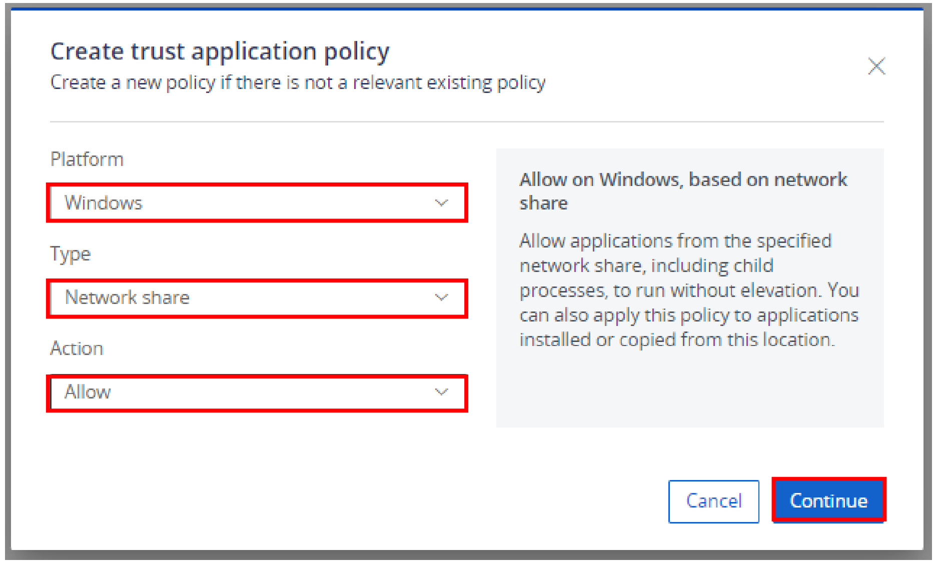
Export all application policies

Push active policies to agents

4 results

	Name	Last modifi
□	Developer Applications	15:08:06
□	Block	15:08:06
□	Elevate	15:08:06
□	Allow	15:08:06

- Set Platform to Windows.
- Set Type to Network share.
- Set Action to Allow
- Press Continue



Create trust application policy

Create a new policy if there is not a relevant existing policy

Platform: Windows

Type: Network share

Action: Allow

Allow on Windows, based on network share

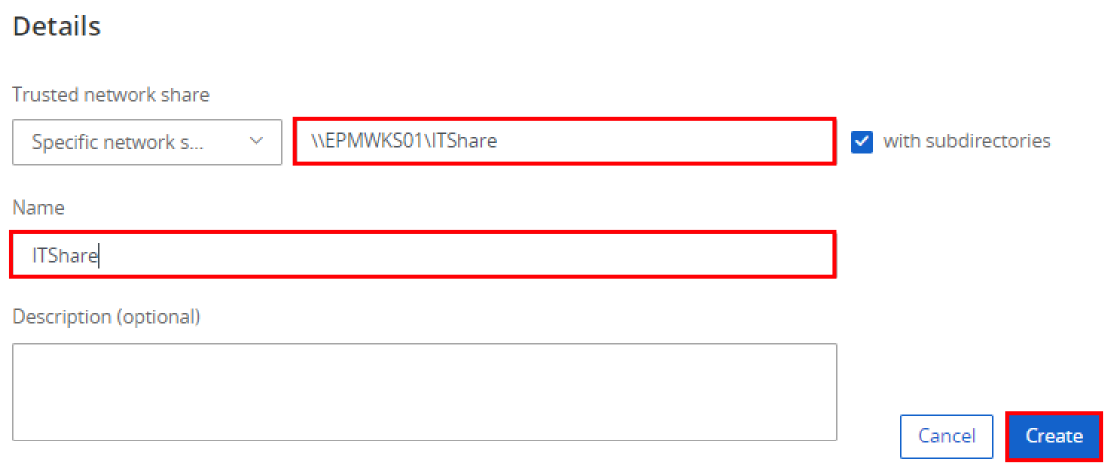
Allow applications from the specified network share, including child processes, to run without elevation. You can also apply this policy to applications installed or copied from this location.

Cancel

Continue

CREATING A TRUSTED SOURCE POLICY

- Set the Specific Network share to \\EPMWKS01\ITShare and the name to ITShare
- Click Create and click Yes to confirm.



Details

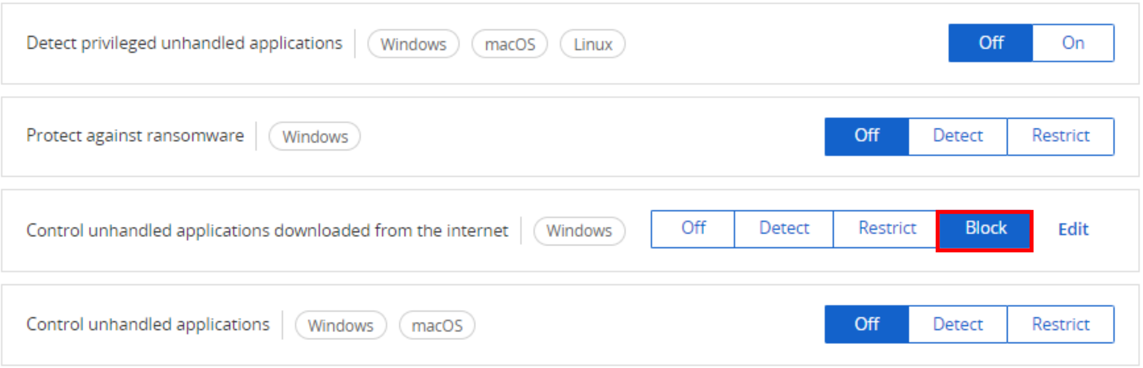
Trusted network share: Specific network s... | \\EPMWKS01\ITShare | ☑ with subdirectories

Name: ITShare

Description (optional):

LOCKING IT DOWN (AGAIN)

- Go back to Policies…Default Policies and set ‘Control unhandled applications downloaded from the internet’ back to Block.
- Refresh the EPM policy on the agent.

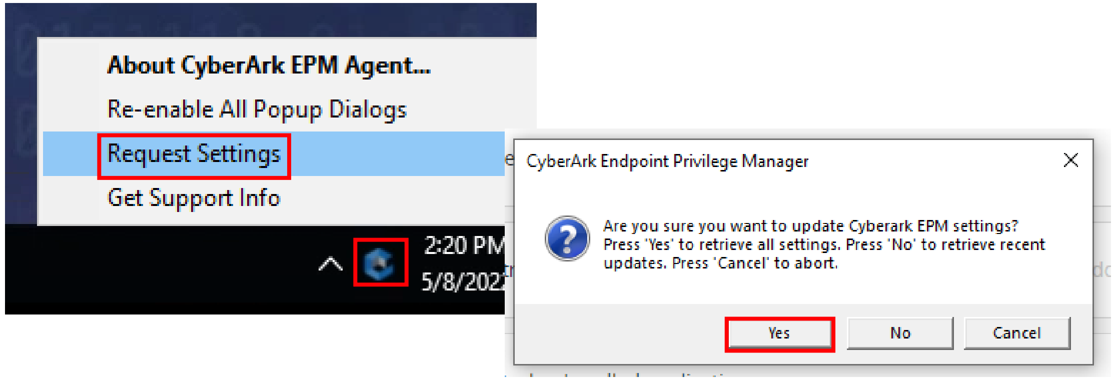


Detect privileged unhandled applications | Windows | macOS | Linux | [✓ Off] On

Protect against ransomware | Windows | [✓ Off] Detect Restrict

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

Control unhandled applications | Windows | macOS | [✓ Off] Detect Restrict

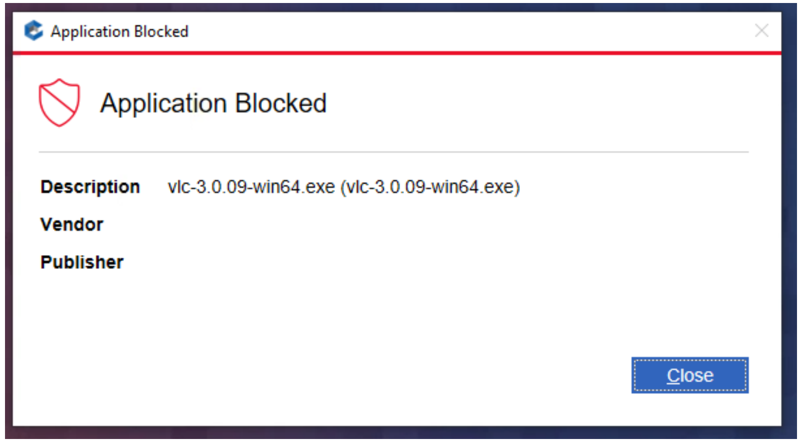


CyberArk Endpoint Privilege Manager

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.

TESTING TRUSTED SOURCE POLICY

- From the ‘Lab 3 – Trusted Publishers’ folder, double-click and run ‘vlc-3.0.09-win64.exe’
- Observe the result



Application Blocked

Application Blocked

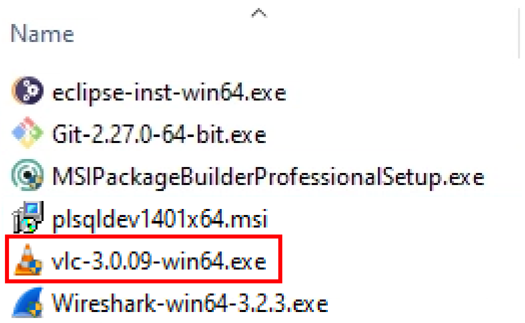
Description vlc-3.0.09-win64.exe (vlc-3.0.09-win64.exe)

Vendor

Publisher

- Double click on the ITShare shortcut or go to //EPMWKS01\ITShare directly.

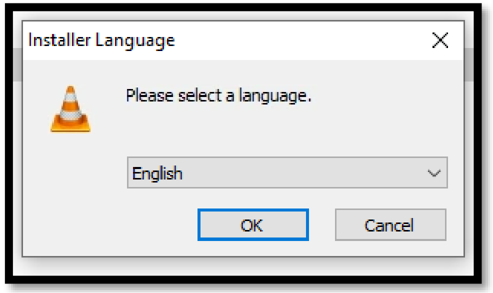
ITShare



Name

eclipse-inst-win64.exe
Git-2.27.0-64-bit.exe
MSIPackageBuilderProfessionalSetup.exe
plsqldev1401x64.msi
vlc-3.0.09-win64.exe
Wireshark-win64-3.2.3.exe

- Double-click and run ‘vlc-3.0.09-win64.exe’ from the ITShare folder.
- Observe the result.



Installer Language

Please select a language.

English

ATTACK + DEFEND

LAB 4 – CREDENTIAL THEFT PROTECTION

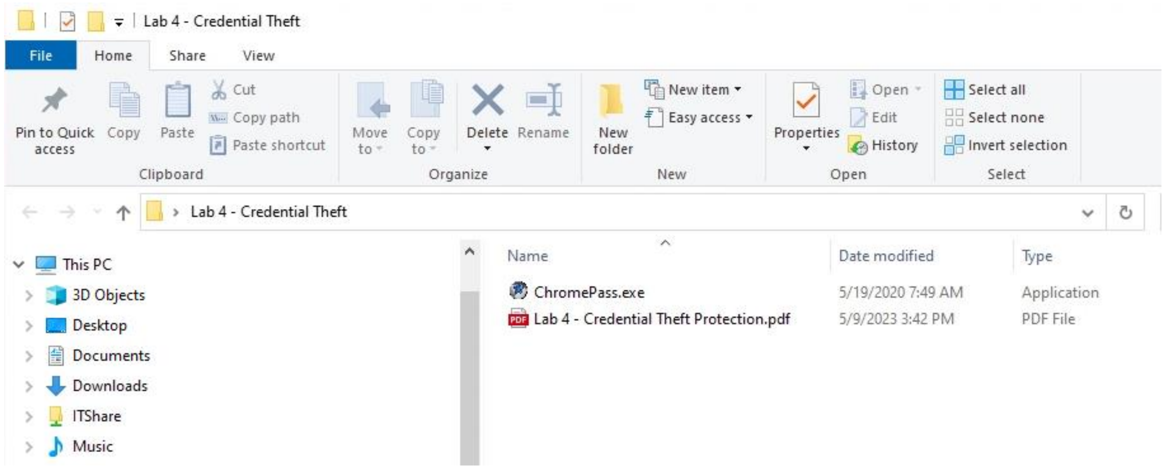
Protected applications from credential theft

LAB 3 CREDENTIAL THEFT PROTECTION

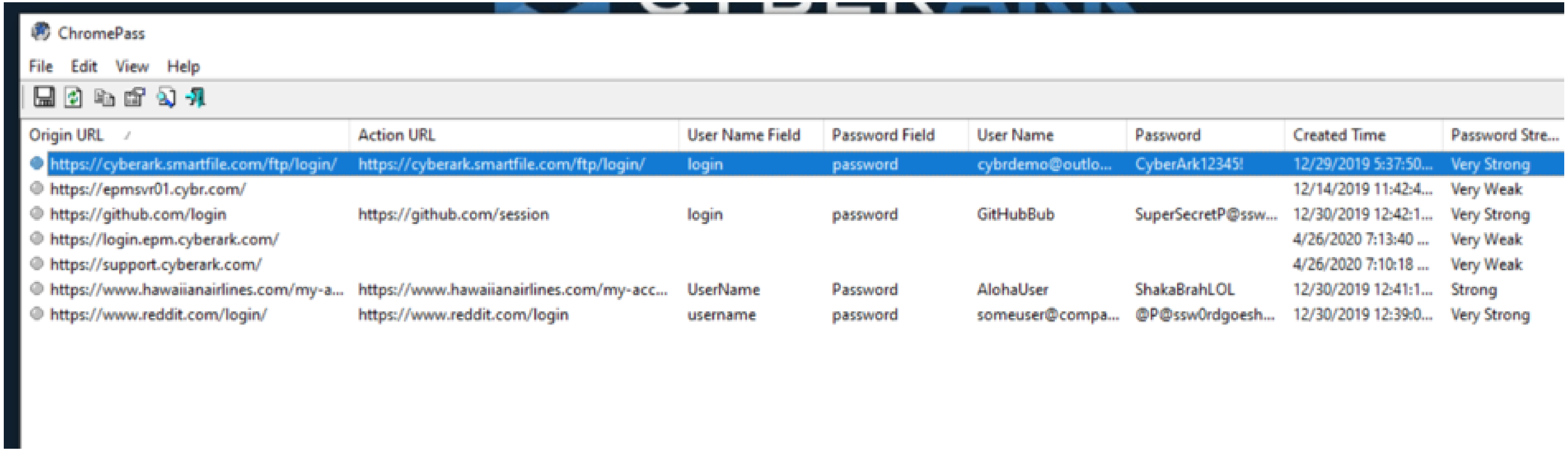
- Run Chromepass
- See the credentials in plain text
- Create a Credential Theft Protection policy
- Replay attack scenario

GETTING STARTED WITH CHROMEPASS

- Open the ‘Lab 4 – Credential Theft’ folder on the desktop
- Double click on ChromePass.exe
- The utility launch and credentials will be seen immediately



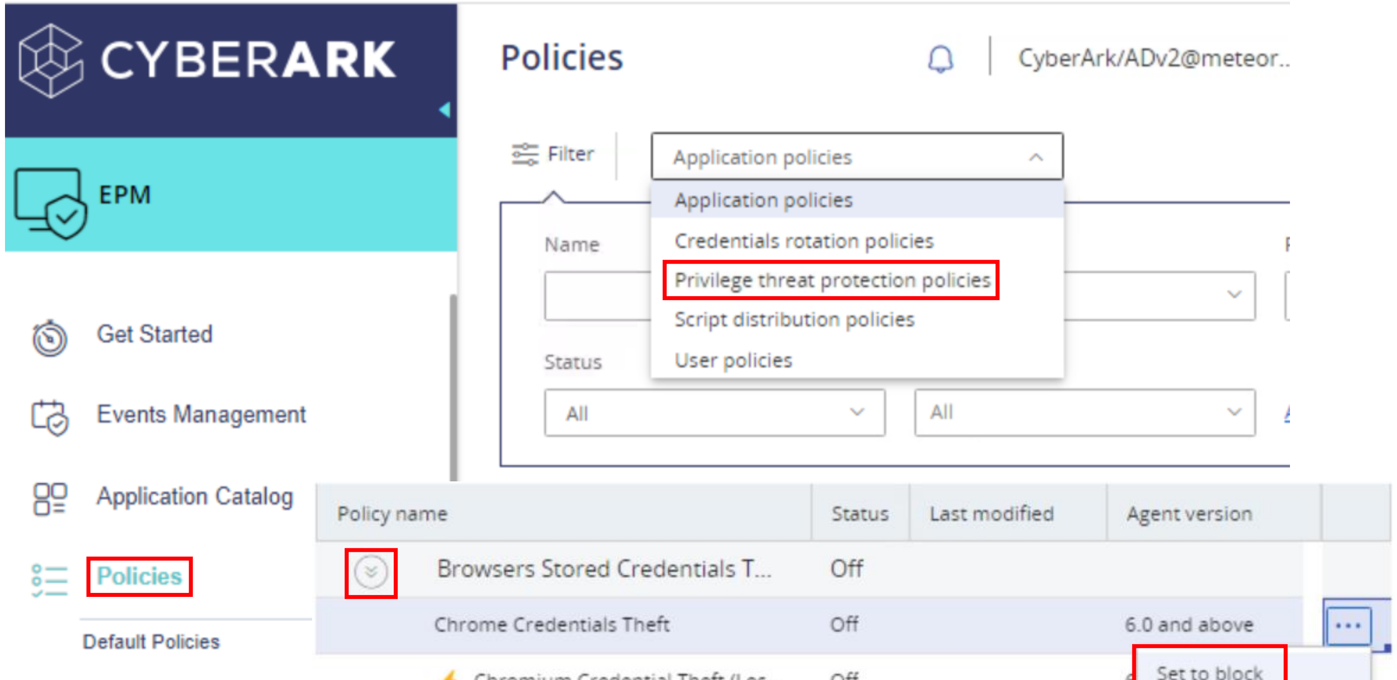
Name	Date modified	Type
ChromePass.exe	5/19/2020 7:49 AM	Application
Lab 4 - Credential Theft Protection.pdf	5/9/2023 3:42 PM	PDF File



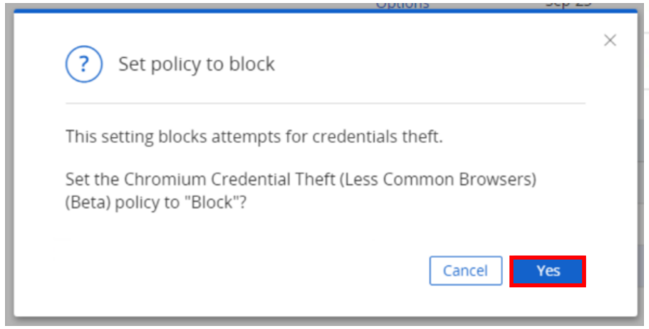
Origin URL	Action URL	User Name Field	Password Field	User Name	Password	Created Time	Password Stre...
https://cyberark.smartfile.com/ftp/login/	https://cyberark.smartfile.com/ftp/login/	login	password	cybrdemo@outlo...	CyberArk12345!	12/29/2019 5:37:50...	Very Strong
https://epmsvr01.cybr.com/						12/14/2019 11:42:4...	Very Weak
https://github.com/login	https://github.com/session	login	password	GitHubBub	SuperSecretP@ssw...	12/30/2019 12:42:1...	Very Strong
https://login.epm.cyberark.com/						4/26/2020 7:13:40 ...	Very Weak
https://support.cyberark.com/						4/26/2020 7:10:18 ...	Very Weak
https://www.hawaiianairlines.com/my-a...	https://www.hawaiianairlines.com/my-acc...	UserName	Password	AlohaUser	ShakaBrahLOL	12/30/2019 12:41:1...	Strong
https://www.reddit.com/login/	https://www.reddit.com/login	username	password	someuser@compa...	@P@ssw0rdgoesh...	12/30/2019 12:39:0...	Very Strong

ENABLE THREAT PROTECTION POLICIES

- Drop down Policies
- Expand Application Policies and select Open Privilege threat protection policies
- Expand on Browsers Stored Credential Theft
- Set Chrome Credentials Theft to Block



Policy name	Status	Last modified	Agent version
Browsers Stored Credentials T...	Off		
Chrome Credentials Theft	Off		6.0 and above
Chromium Credential Theft (Les...	Off		6
Cookies Theft From Web Brows...	Off		6
Firefox Credentials Theft	Off		6.0 and above



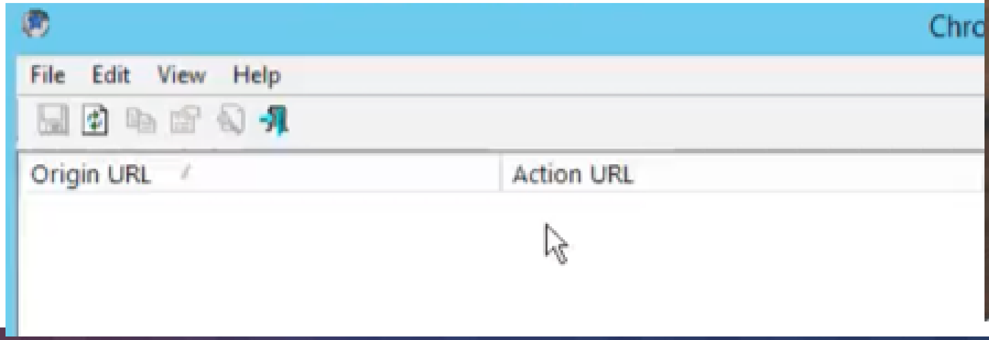
Set policy to block

This setting blocks attempts for credentials theft.

Set the Chromium Credential Theft (Less Common Browsers) (Beta) policy to "Block"?

CREDENTIAL HARVEST RETRY

- Run Chromepass again
  It might take a minute for the policy to push
  Try a few times if necessary
- What is visible now?
  - NOTHING!



ATTACK + DEFEND

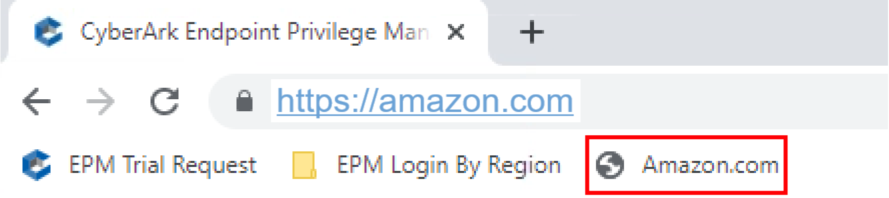
LAB 5 – POLICY IMPORT

Making your job easy.

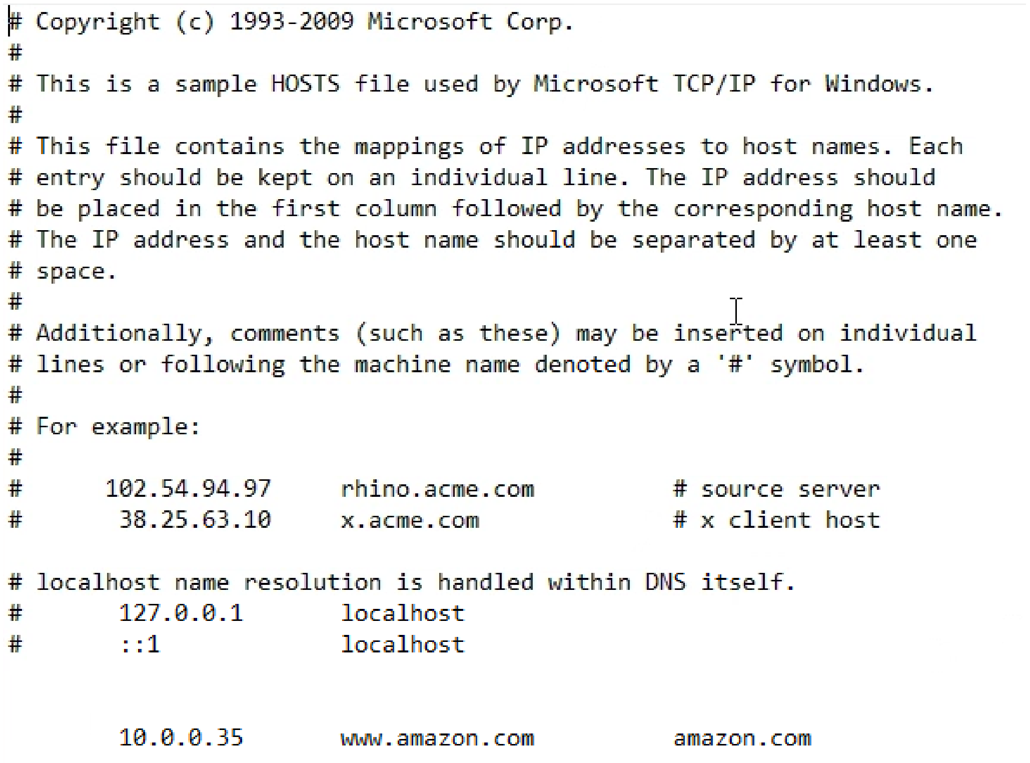
LAB 5
POLICY IMPORT

- View DNS Poisoned Site
- Attempt to edit HOSTS file
- Import Policy
- Edit HOSTS file

HOSTS FILE POISONED



- Click on the Amazon.com shortcut, bookmark, or go to http://amazon.com
  (if you type in the url, note it's http vs https)
- Notice anything different?
- Someone has poisoned the local HOSTS file to re-direct the domain name
- From within the 'Lab 5 – Policy Import' folder, open 'HOSTS – shortcut' with Notepad
- Attempt to edit and save the file
  - You can't!
  - You are unable to do so as the current user is not a local administrator



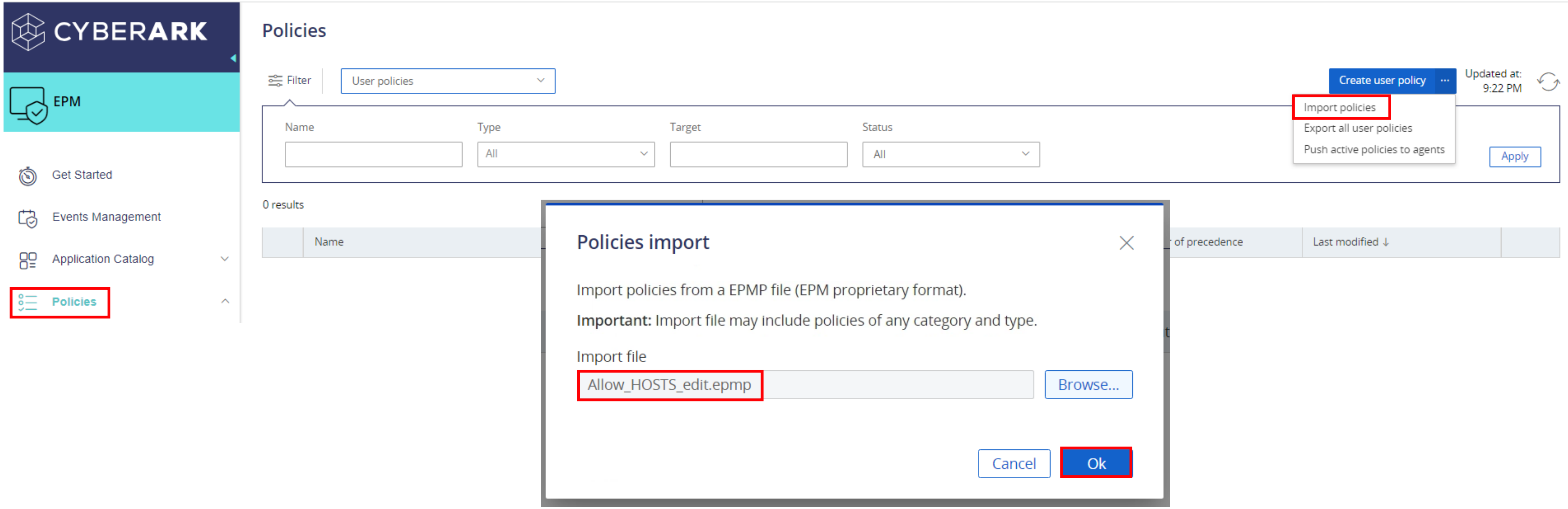
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


        10.0.0.35       www.amazon.com          amazon.com
```

IMPORT A POLICY ALLOWING HOSTS FILE EDITING

- Click on Policies, Select User Policies from the drop-down menu
- Expand the Create user policy and select ‘Import policies’
- Select the Allow_HOSTS_edit.epmp file within the ‘Lab 5 – Policy Import’ folder
  Click Ok



Policies

Policies import

Import policies from a EPMP file (EPM proprietary format).

Important: Import file may include policies of any category and type.

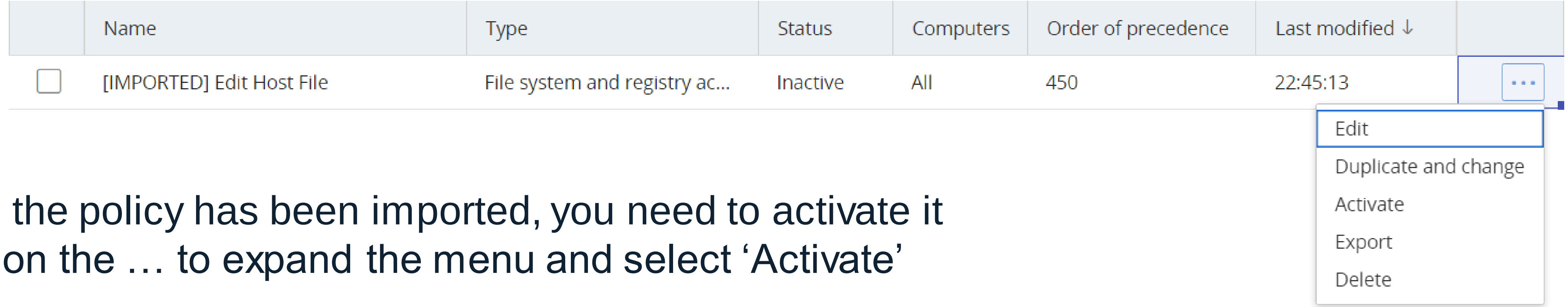
Import file: Allow_HOSTS_edit.epmp

Browse...

Cancel

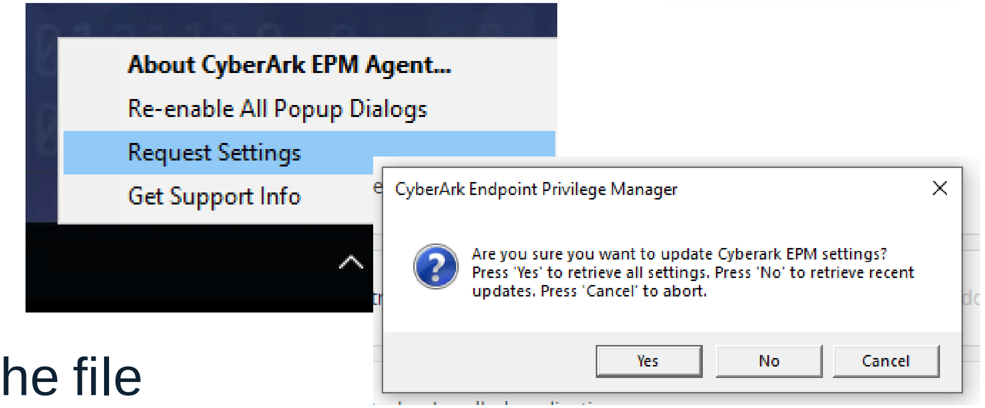
Ok

POLICY ACTIVATION



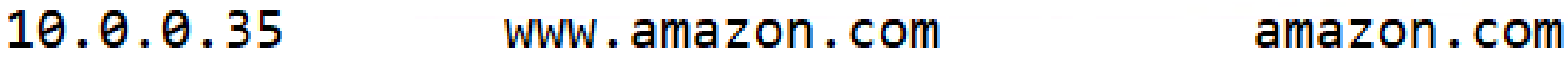
	Name	Type	Status	Computers	Order of precedence	Last modified ↓	
□	[IMPORTED] Edit Host File	File system and registry ac...	Inactive	All	450	22:45:13	...

- Once the policy has been imported, you need to activate it Click on the … to expand the menu and select ‘Activate’
- Click Yes to Activate the policy
- Request Settings from the agent
- Reopen the HOSTS file
- Remove line 24 or comment out the line and save the file
- Launch Amazon.com again



CyberArk Endpoint Privilege Manager

Are you sure you want to update Cyberark EPM settings? Press 'Yes' to retrieve all settings. Press 'No' to retrieve recent updates. Press 'Cancel' to abort.



```
10.0.0.35        www.amazon.com        amazon.com
```