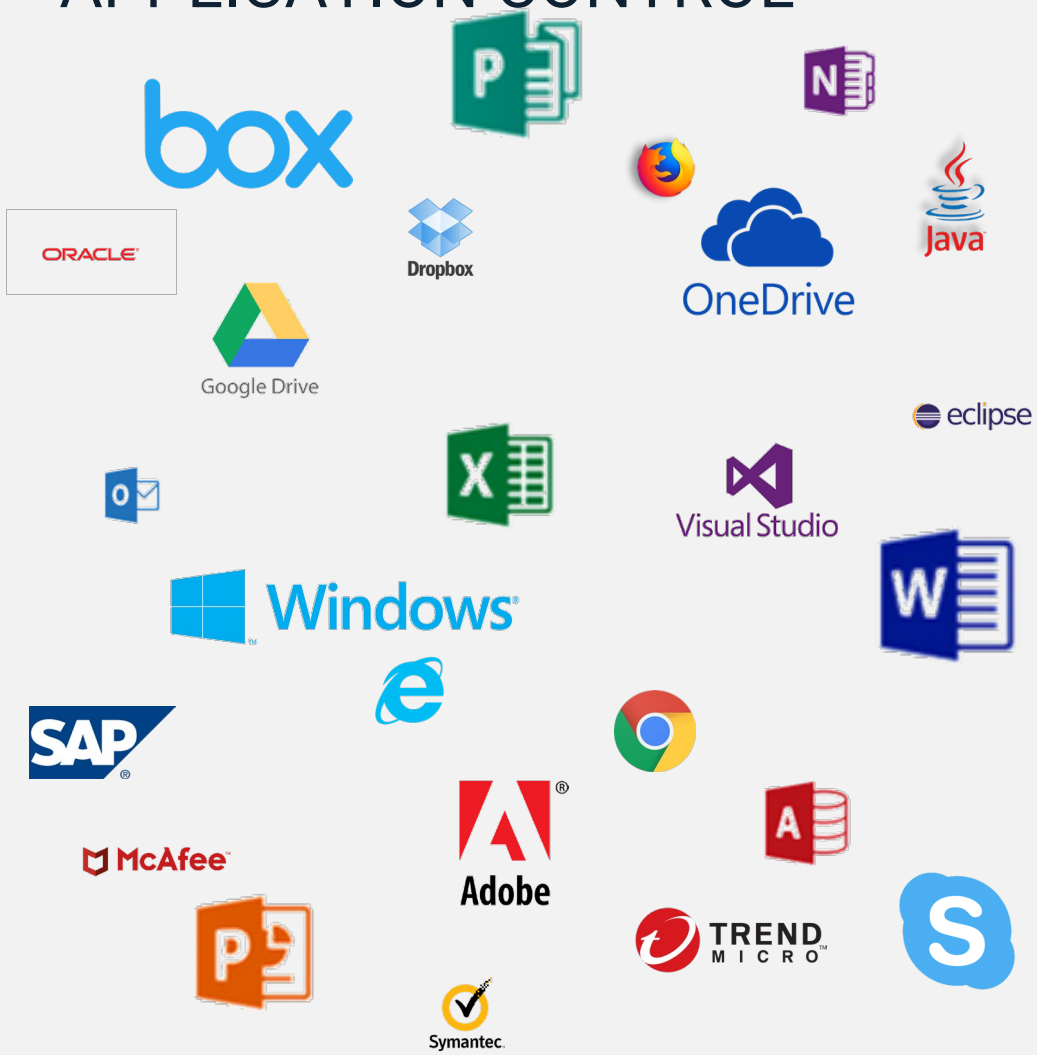
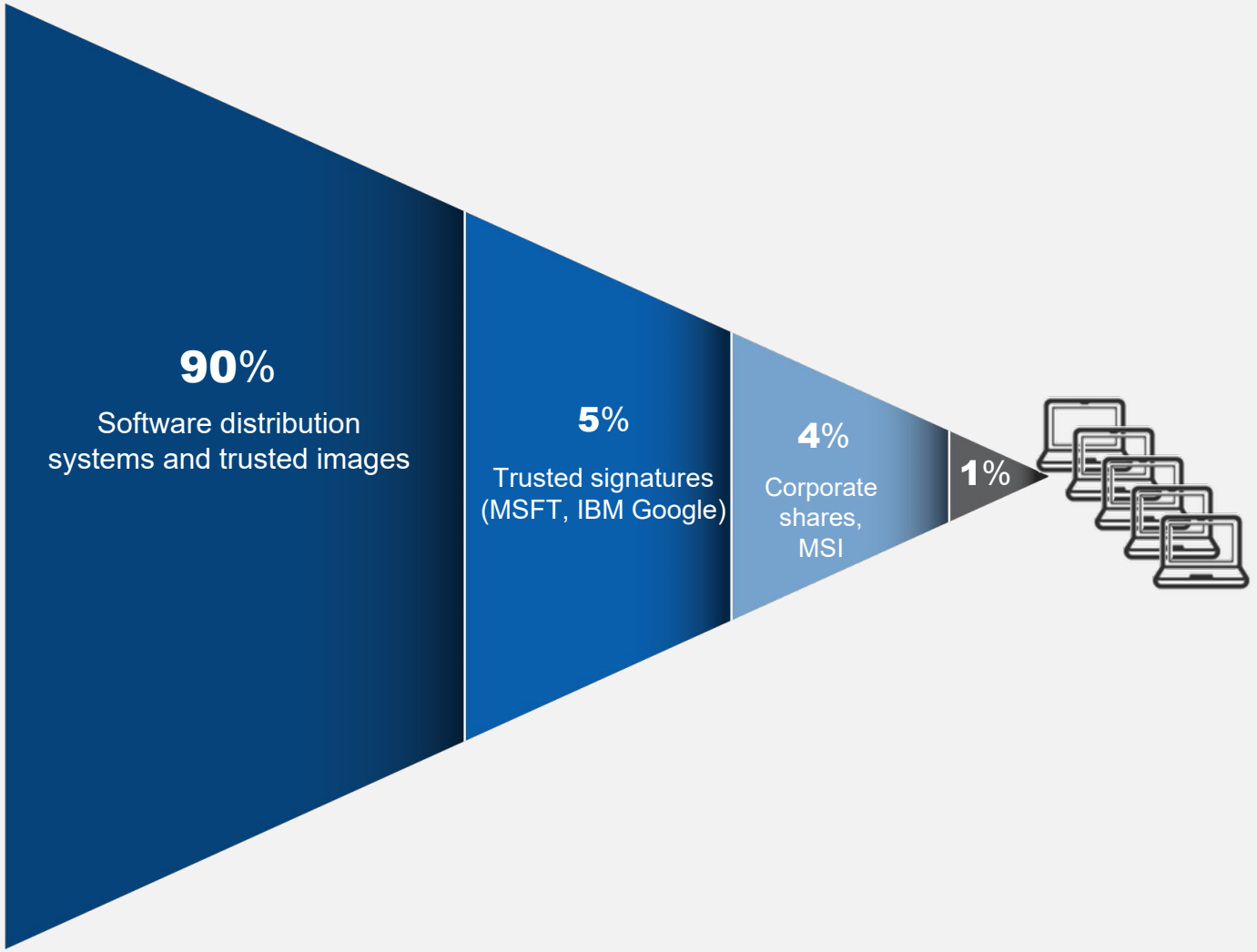
ATTACK + DEFEND

LAB 3 – TRUSTED PUBLISHERS

Setting up policies for Least Privilege

TRUSTED SOURCES REMOVES THE BARRIERS TO APPLICATION CONTROL

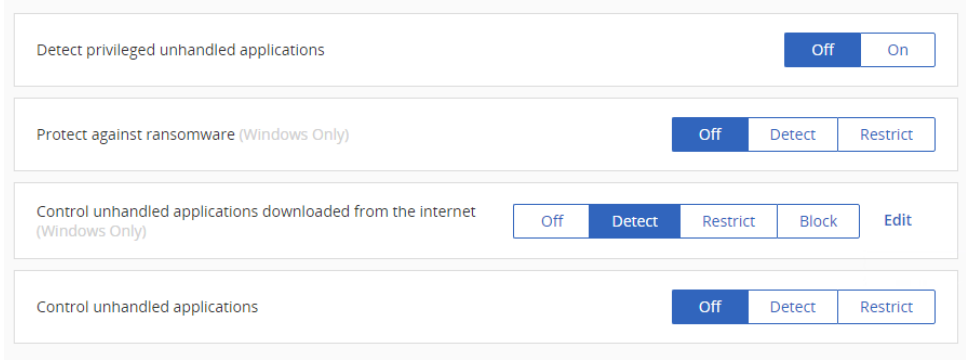


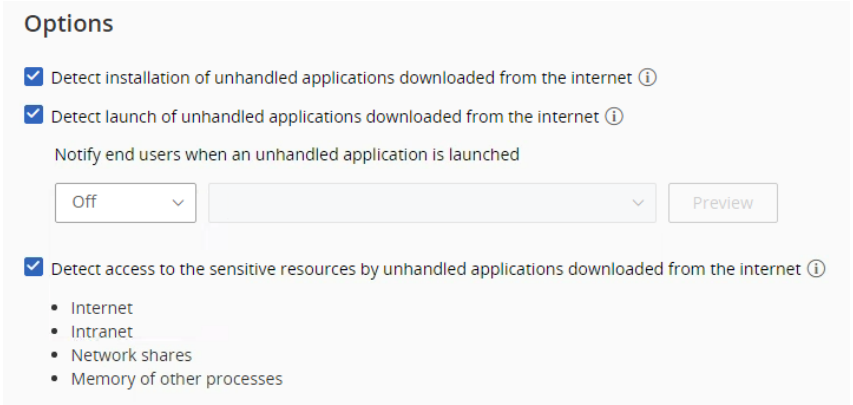


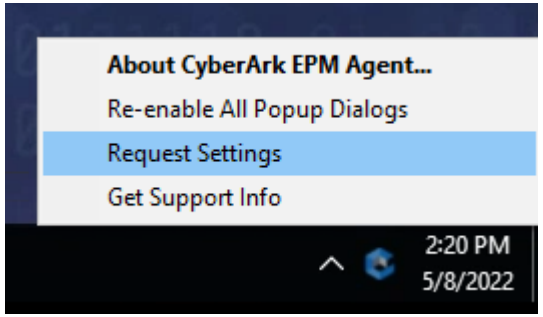
CyberArk automates policy creation for **over 99%** of application and system software

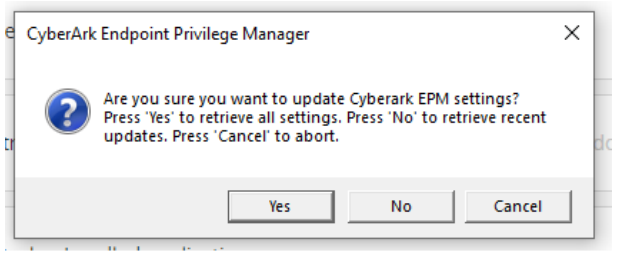
Detecting Internet Applications.

- Go back to Policies…Default Policies and set Control unhandled applications downloaded from the internet. To Detect. Click Edit policy settings.
- Under options, make sure all three check boxes are checked. Click save and confirm the policy changes.
- Refresh the EPM policy on the agent.



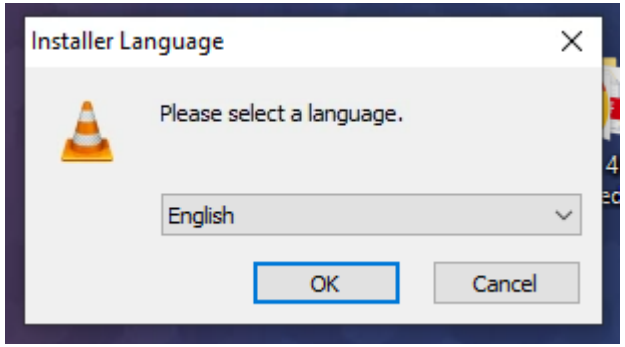






Executing Code

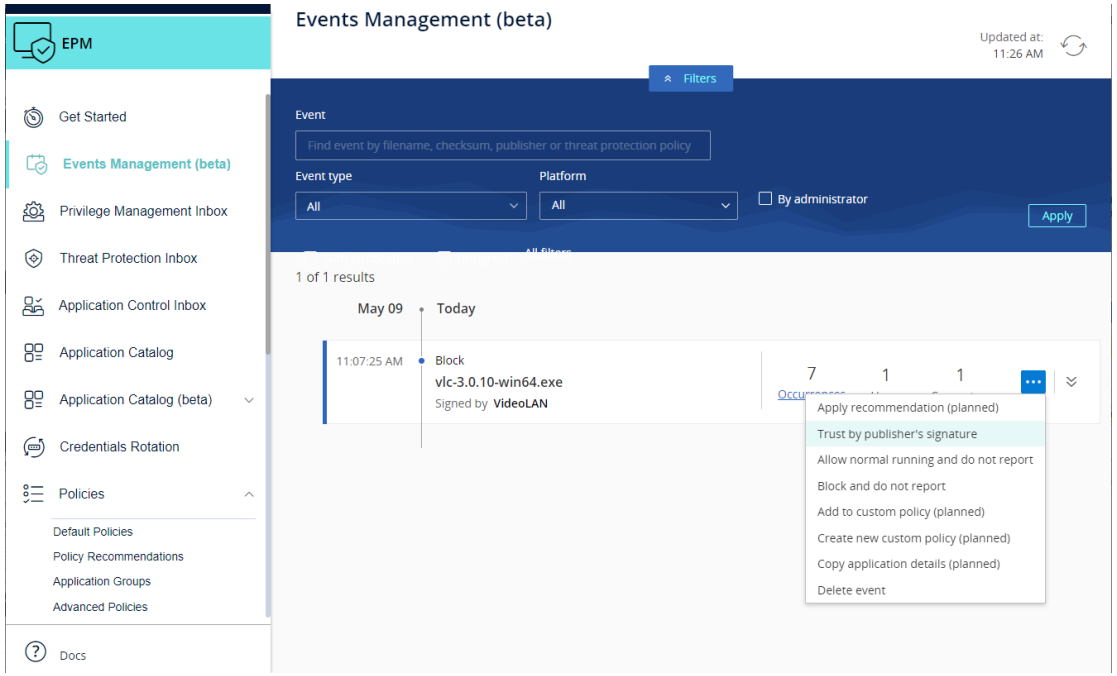
- From the ‘Lab 3 – Trusted Publishers’ folder, click the vlc-3.0.10-win64.exe shortcut and note how it is also runs. Immediately close the installer.

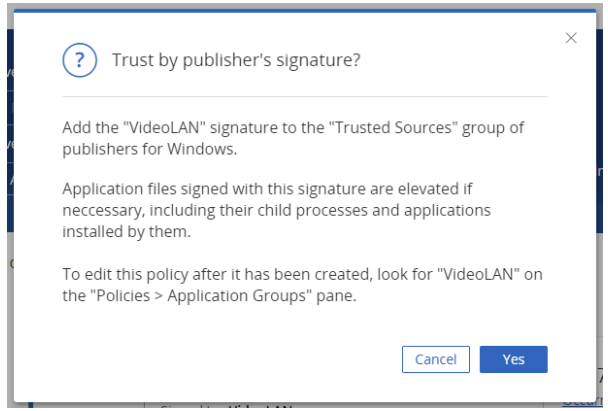


- From the ‘Lab 3 – Trusted Publishers’ folder, click the Download vlc-3.0.09-win64.exe shortcut
- Run vlc-3.0.09.exe and observe the result.

Configure trusted source policy

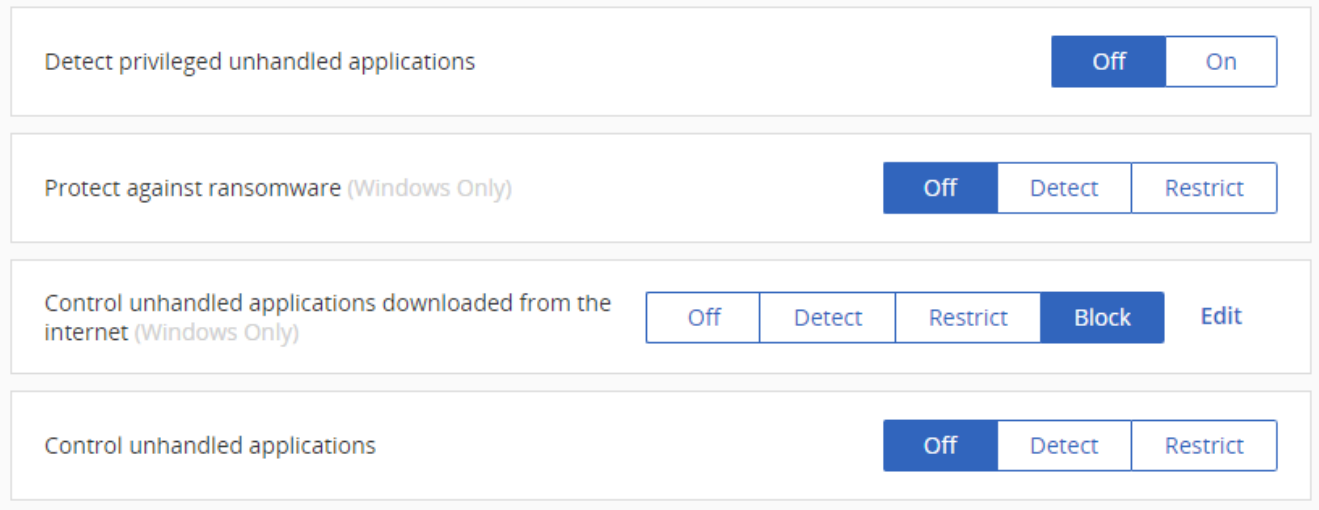
- Go to Events Management (beta)
- Find vlc-3.0.10-win64.exe
- Click … and select Trust by publisher's signature. Click Yes to confirm.



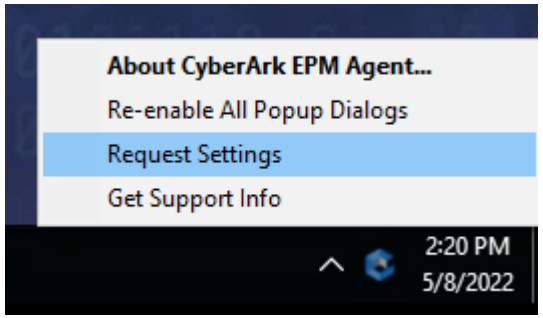


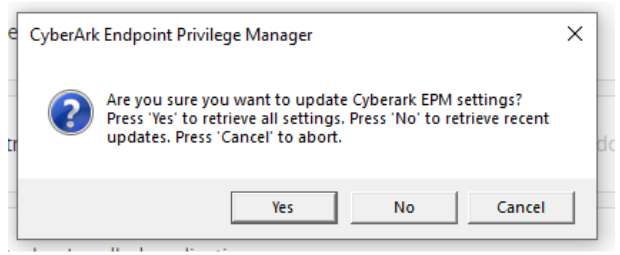
Locking it down.

- Go back to Policies…Default Policies.
  Set ‘ Control unhandled applications downloaded from the internet’ back to Block.
  Click Yes to confirm.



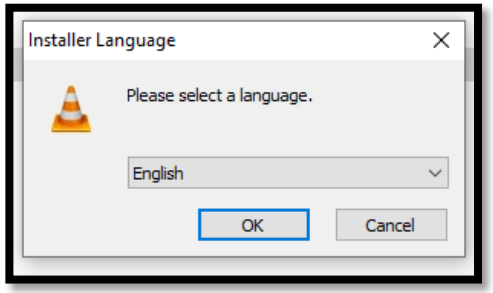
- Refresh EPM Agent Policy.





Executing 7zip Installer

- Navigate to ‘Lab 4 – Trusted Sources’.
- Examine the two files and their properties.
- Run vlc-3.0.09-win64.exe and observe the result.
- Run vlc-3.0.10-win64.exe and observe the result.



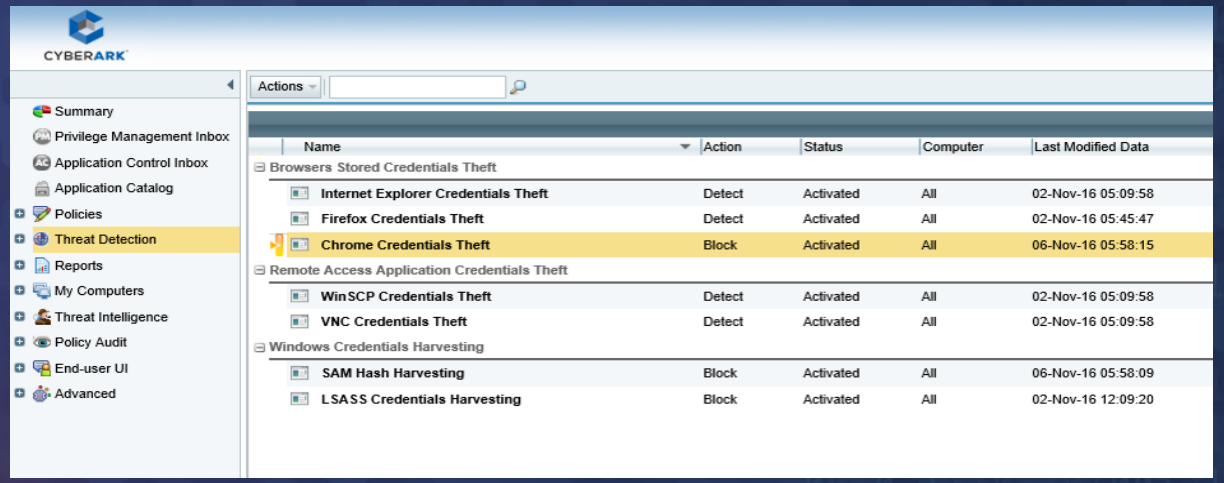
ATTACK + DEFEND

LAB 4 – CREDENTIAL THEFT PROTECTION

Protected applications from Credential Theft

THINK LIKE AN ATTACKER WITH CREDENTIAL THEFT PROTECTION

- The endpoint is the entry point for attacks
- Credentials are the main target of malware and non–malware–based attacks
- Contain the attack on the endpoint



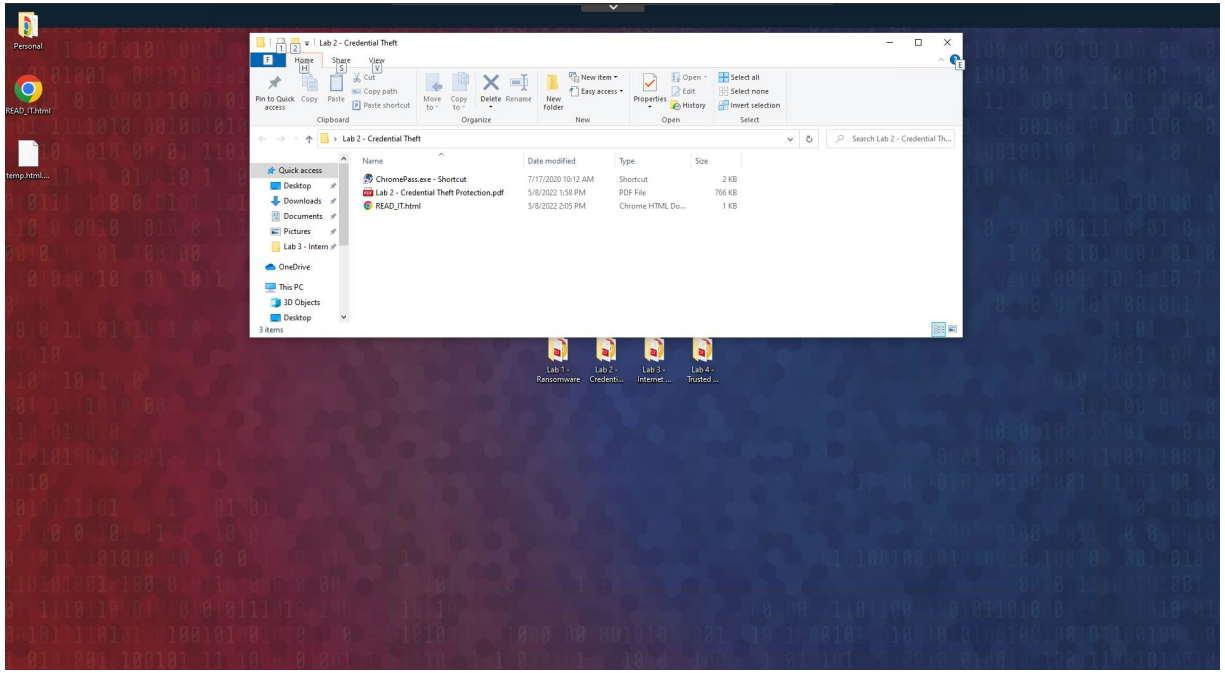
LAB 3 CREDENTIAL THEFT PROTECTION

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

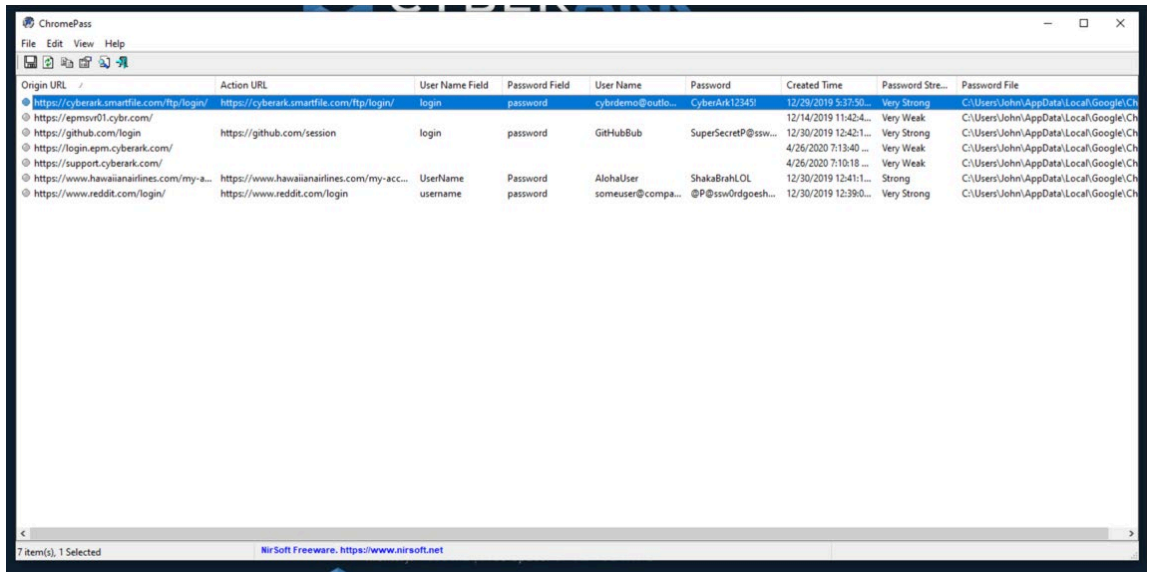
- What is ChromePass?
  - https://www.nirsoft.net/utils/chromepass.html
- What is Lazagne?
  - https://github.com/AlessandroZ/LaZagne

Getting started with ChromePass

- Open the ‘Lab 4 – Credential Theft’ folder on the desktop. Double click on ChromePass.exe - Shortcut

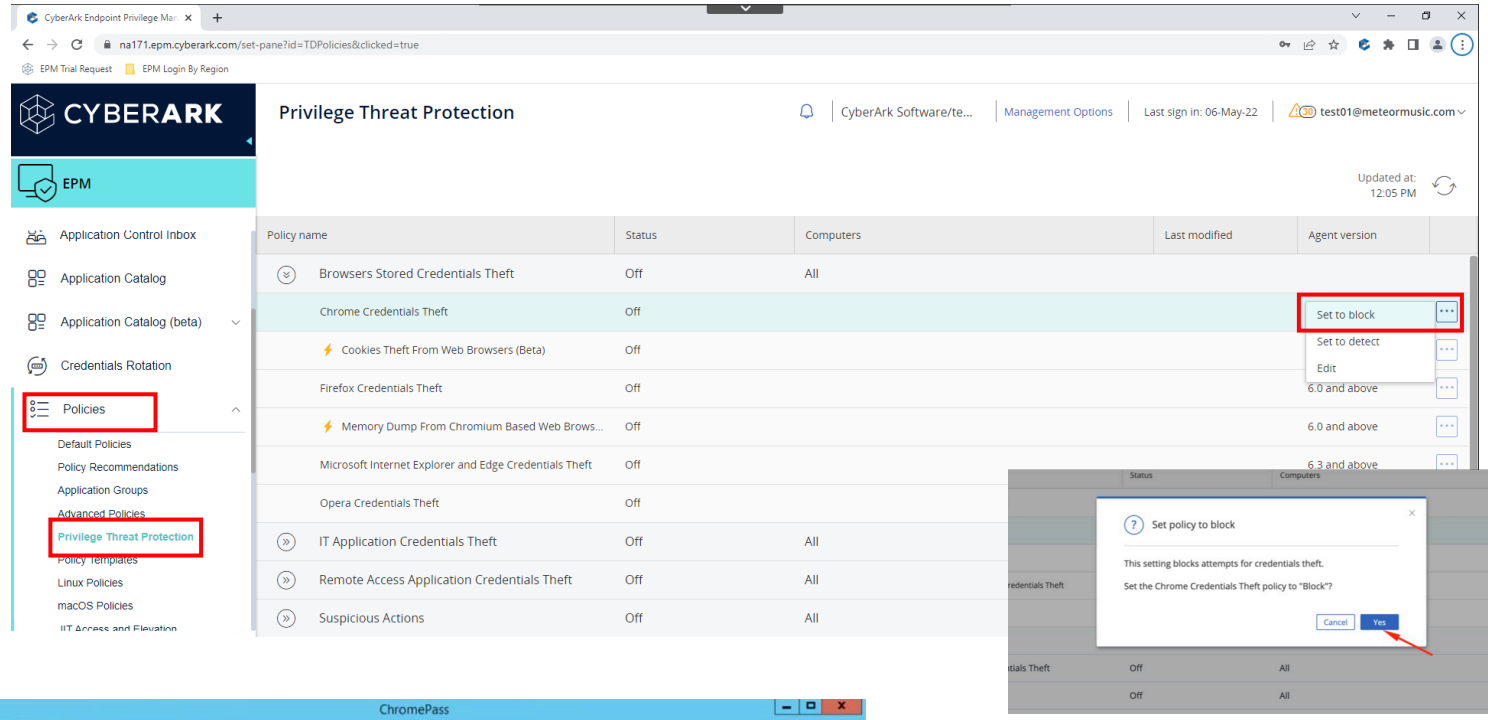


- The utility will be seen immediately



Enable Threat Protection Policies

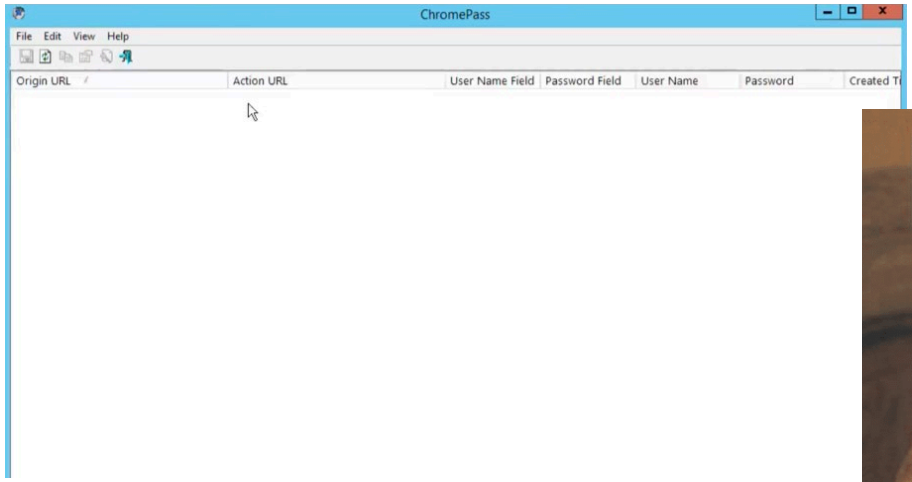
- Drop down Policies
- Open Privilege Threat Protection
- Expand on Browsers Stored Credential Theft



- Set Chrome Credentials Theft to Block

Run Chromepass again

- What is visible now?
- NOTHING!



- Click on Threat Protection Inbox to view more data about the event.