

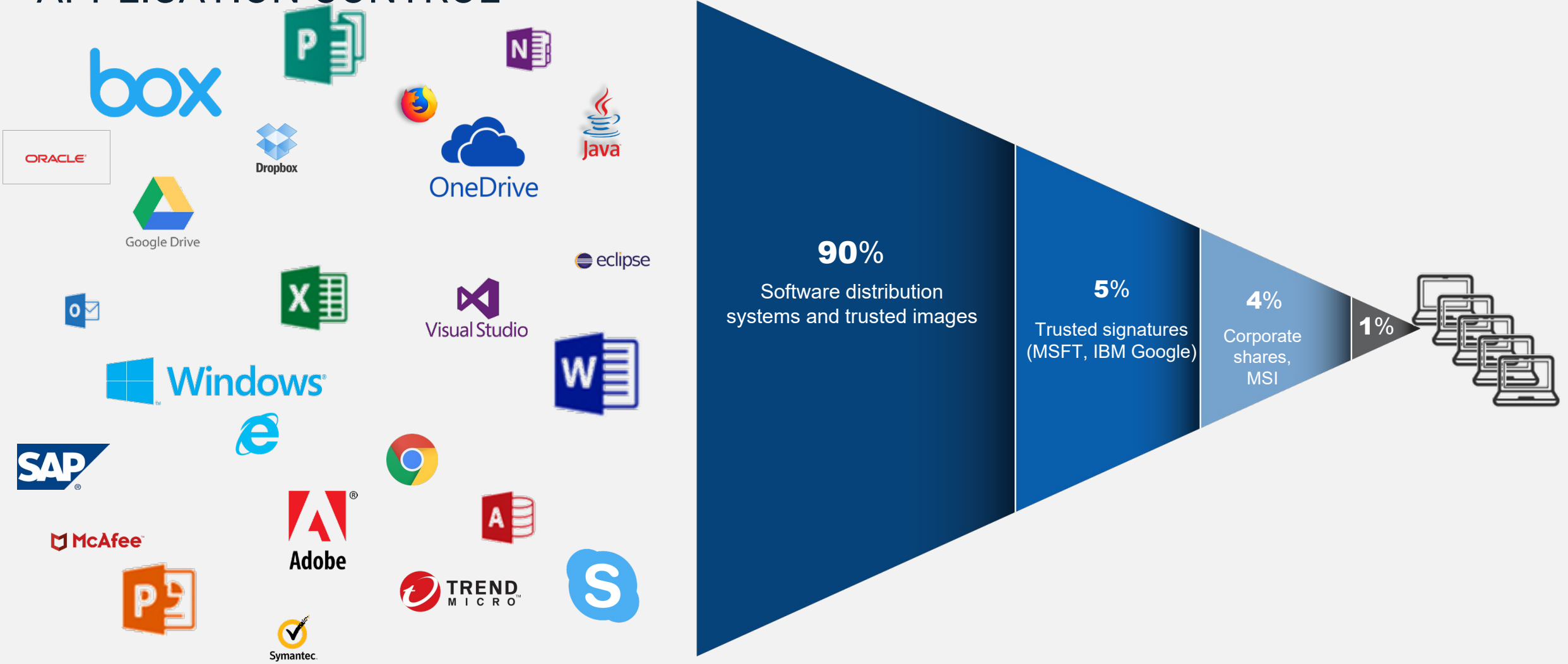


ATTACK + DEFEND

LAB 3 – TRUSTED PUBLISHERS

Setting up policies for Least Privilege

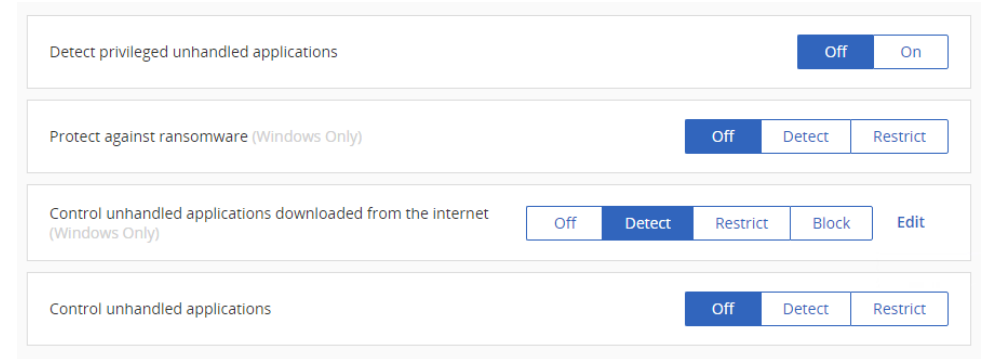
TRUSTED SOURCES REMOVES THE BARRIERS TO APPLICATION CONTROL



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

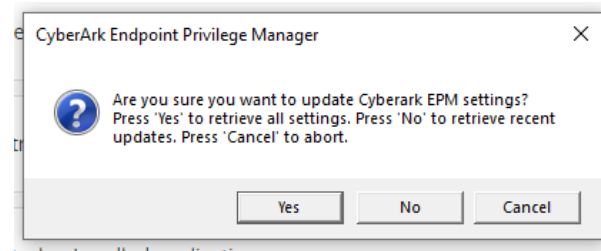
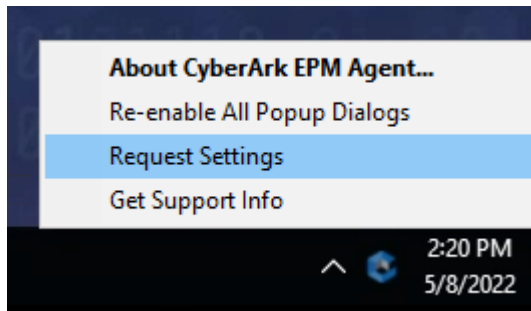
Detecting Internet Applications.

- 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.



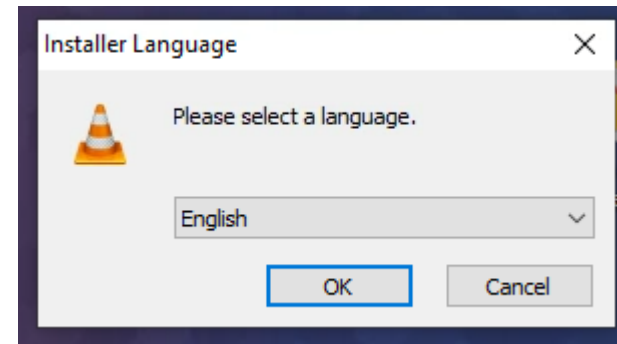
Options

- Detect installation of unhandled applications downloaded from the internet ⓘ
 - Detect launch of unhandled applications downloaded from the internet ⓘ
- Notify end users when an unhandled application is launched
- Off Preview
- Detect access to the sensitive resources by unhandled applications downloaded from the internet ⓘ
 - Internet
 - Intranet
 - Network shares
 - Memory of other processes



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.

Events Management (beta)

Updated at: 11:26 AM

Event

Find event by filename, checksum, publisher or threat protection policy

Event type: All Platform: All By administrator

1 of 1 results

May 09 Today

11:07:25 AM Block vlc-3.0.10-win64.exe Signed by VideoLAN

7 1 1

Trust by publisher's signature

- Apply recommendation (planned)
- Trust by publisher's signature
- Allow normal running and do not report
- Block and do not report
- Add to custom policy (planned)
- Create new custom policy (planned)
- Copy application details (planned)
- Delete event

Trust by publisher's signature?

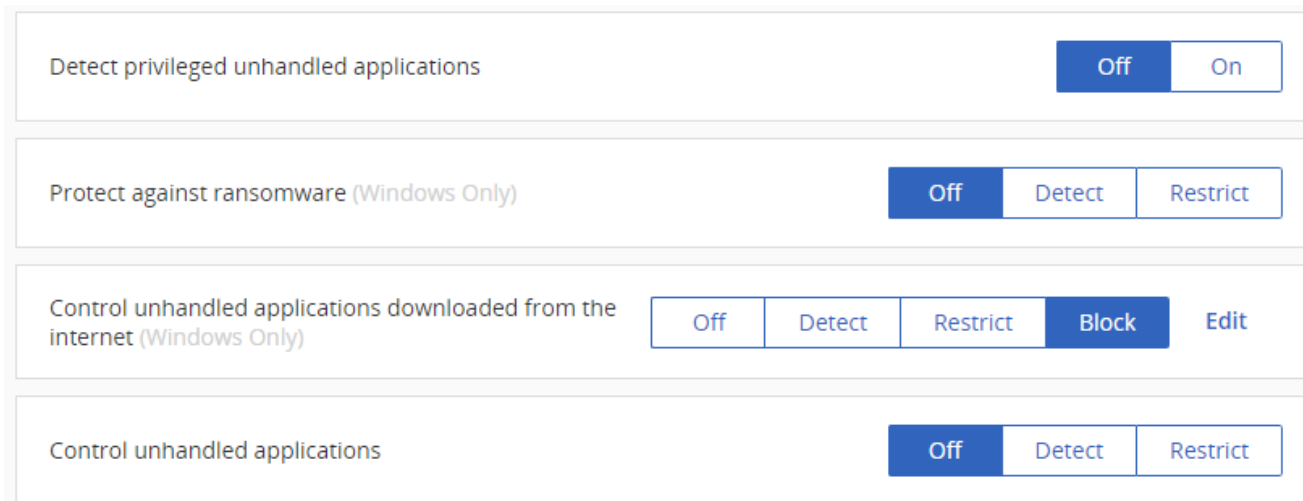
Add the "VideoLAN" signature to the "Trusted Sources" group of publishers for Windows.

Application files signed with this signature are elevated if necessary, including their child processes and applications installed by them.

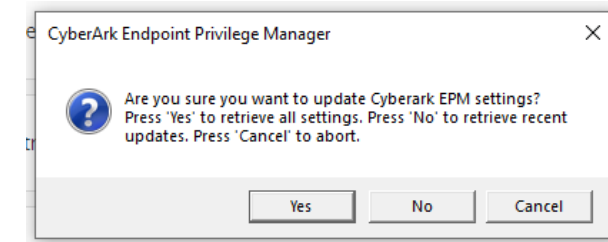
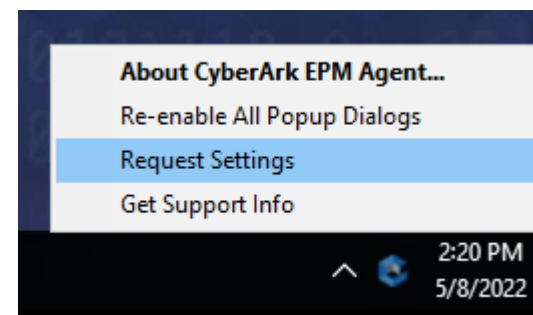
To edit this policy after it has been created, look for "VideoLAN" on the "Policies > Application Groups" pane.

Locking it down.

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

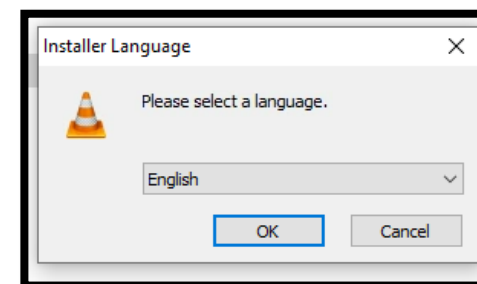


- Refresh EPM Agent Policy.



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



The screenshot shows the CYBERARK Threat Detection console. The left sidebar contains a navigation menu with options: Summary, Privilege Management Inbox, Application Control Inbox, Application Catalog, Policies, Threat Detection (highlighted), Reports, My Computers, Threat Intelligence, Policy Audit, End-user UI, and Advanced. The main area displays a table of policies under the 'Actions' dropdown.

Name	Action	Status	Computer	Last Modified Data
Browsers Stored Credentials Theft				
Internet Explorer Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58
Firefox Credentials Theft	Detect	Activated	All	02-Nov-16 05:45:47
Chrome Credentials Theft	Block	Activated	All	06-Nov-16 05:58:15
Remote Access Application Credentials Theft				
WinSCP Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58
VNC Credentials Theft	Detect	Activated	All	02-Nov-16 05:09:58
Windows Credentials Harvesting				
SAM Hash Harvesting	Block	Activated	All	06-Nov-16 05:58:09
LSASS Credentials Harvesting	Block	Activated	All	02-Nov-16 12:09:20

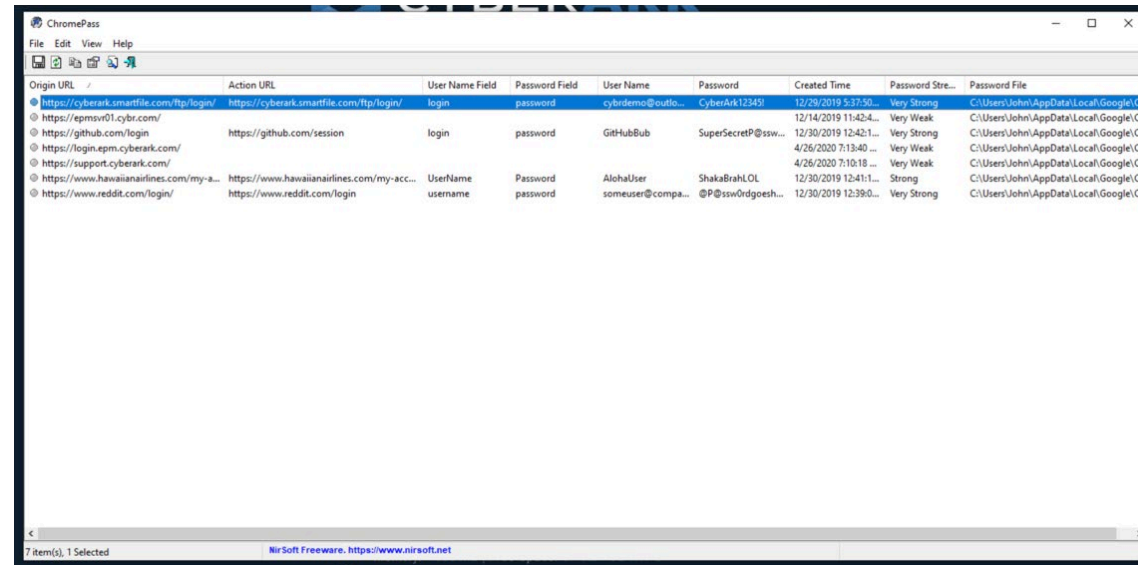
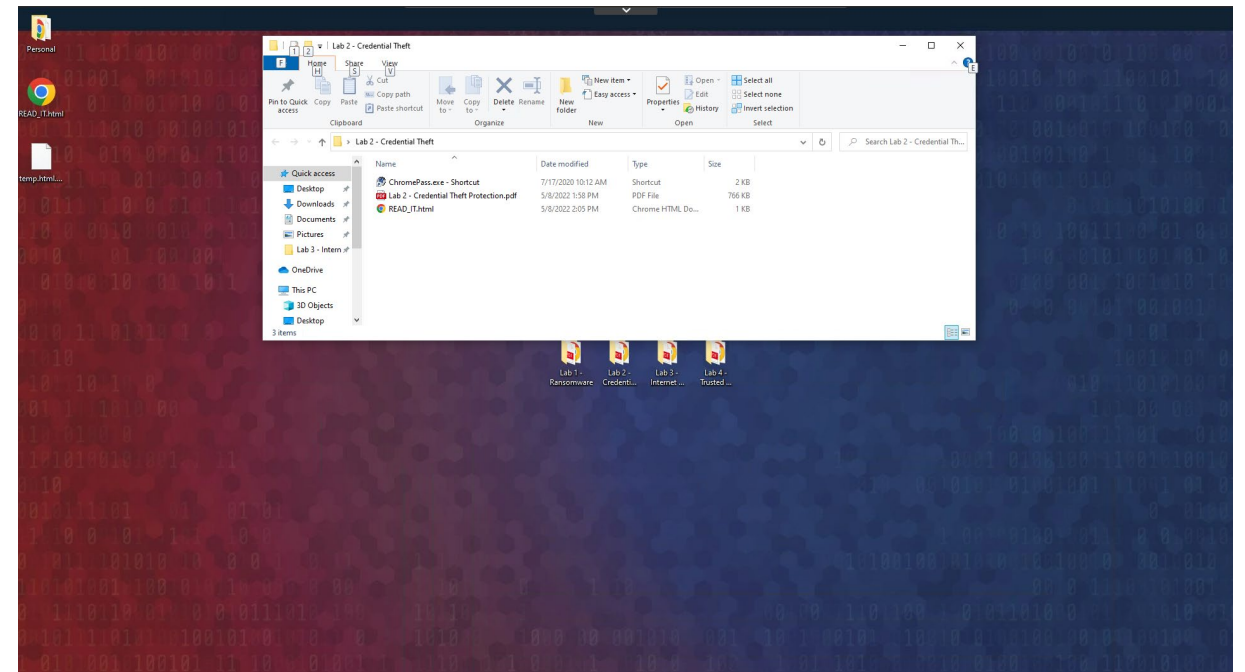
LAB 3 CREDENTIAL THEFT PROTECTION

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

- What is ChromePass?
 - <https://www.nirsoft.net/utills/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

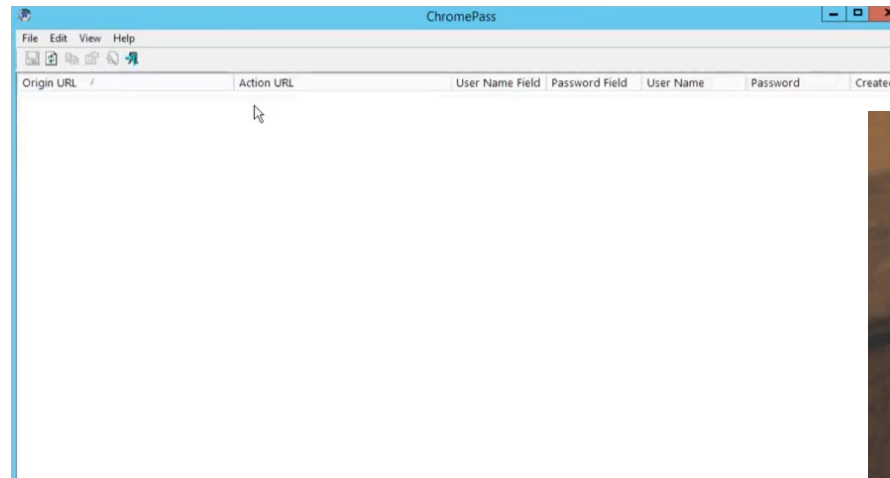
Run Chromepass again

- What is visible now?
- NOTHING!

The screenshot shows the CyberArk Privilege Threat Protection interface. On the left, the 'Policies' menu is expanded, and 'Privilege Threat Protection' is selected. The main area displays a table of policies:

Policy name	Status	Computers	Last modified	Agent version
Browsers Stored Credentials Theft	Off	All		
Chrome Credentials Theft	Off	All		
Cookies Theft From Web Browsers (Beta)	Off			
Firefox Credentials Theft	Off			
Memory Dump From Chromium Based Web Brows...	Off			6.0 and above
Microsoft Internet Explorer and Edge Credentials Theft	Off			6.3 and above
Opera Credentials Theft	Off			
IT Application Credentials Theft	Off	All		
Remote Access Application Credentials Theft	Off	All		
Suspicious Actions	Off	All		

A dialog box titled 'Set policy to block' is open, asking: 'This setting blocks attempts for credentials theft. Set the Chrome Credentials Theft policy to "Block"?'. The 'Yes' button is highlighted with a red arrow.



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

The screenshot shows the CyberArk Threat Protection Inbox interface. The left sidebar contains a navigation menu with items like 'Get Started', 'Events Management (beta)', 'Privilege Management Inbox', 'Threat Protection Inbox' (highlighted with a red box), 'Application Control Inbox', 'Application Catalog', 'Application Catalog (beta)', 'Credentials Rotation', 'Policies', and 'Docs'. The main content area displays a search bar and filters for 'Event Type' (All), 'Threat Type' (All), and 'Last Time' (Last month). Below the filters, a single result is shown for an event on May 06 at 12:10:35 PM. The event details include: 'Attack - Blocked Chrome Credentials Theft', 'Suspect process: C:\users\john\chromeapp\chrome\chrome.exe', 'File type: Executable', 'Hash (SHA1): 4105eb2d96b89b081a15b92595f3d97dadb62bdb', 'File first seen: 06-May-22 12:10:29', 'Event first occurrence: 06-May-22 12:10:29 - on EPMWKS01', 'Occurrences (Timespan): 2 (1 Day)', 'Affected Computers: 1 (EPMWKS01)', and 'Exposed Users: 0'. A 'Full Investigation >' link is available at the bottom right of the event details.