
CYBERARK
ATTACK & DEFEND
SERIES
THE ENDPOINT THREAT

LEGAL DISCLAIMER

This presentation contains materials that can be potentially damaging or dangerous.

These materials are for educational and research purposes only.

All tools provided are open source and CyberArk is not associated with any tools provided. Do not attempt to violate the law with anything contained here. If this is your intention, then **LEAVE NOW!** Neither the authors of this material, CyberArk, or anyone else affiliated in the content in any way, is going to accept responsibility for your actions.

We promote hacking, but do not promote CRIME! We are documenting the ways criminals steal and perform their nefarious acts, so you can defend yourself and your organization.

ANDY THOMPSON

Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

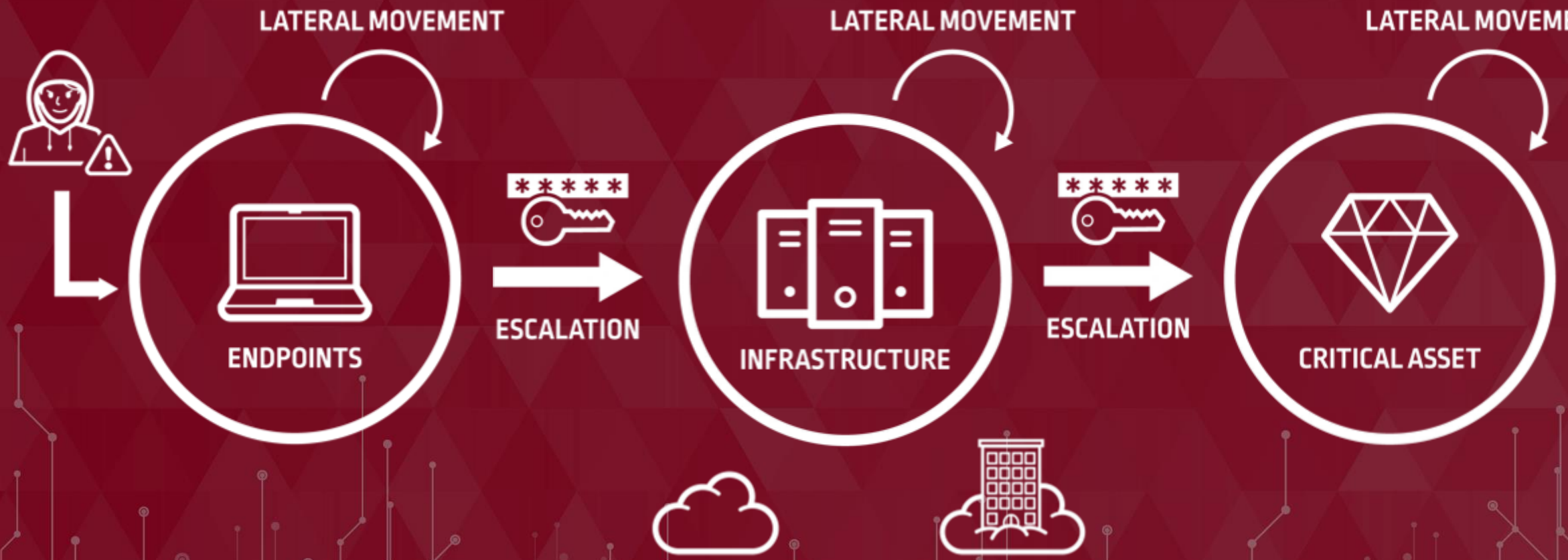
- Research Labs Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas TX Hacker Scene
- Travel-Hacker

IT IS ALL ABOUT THE ENDPOINT

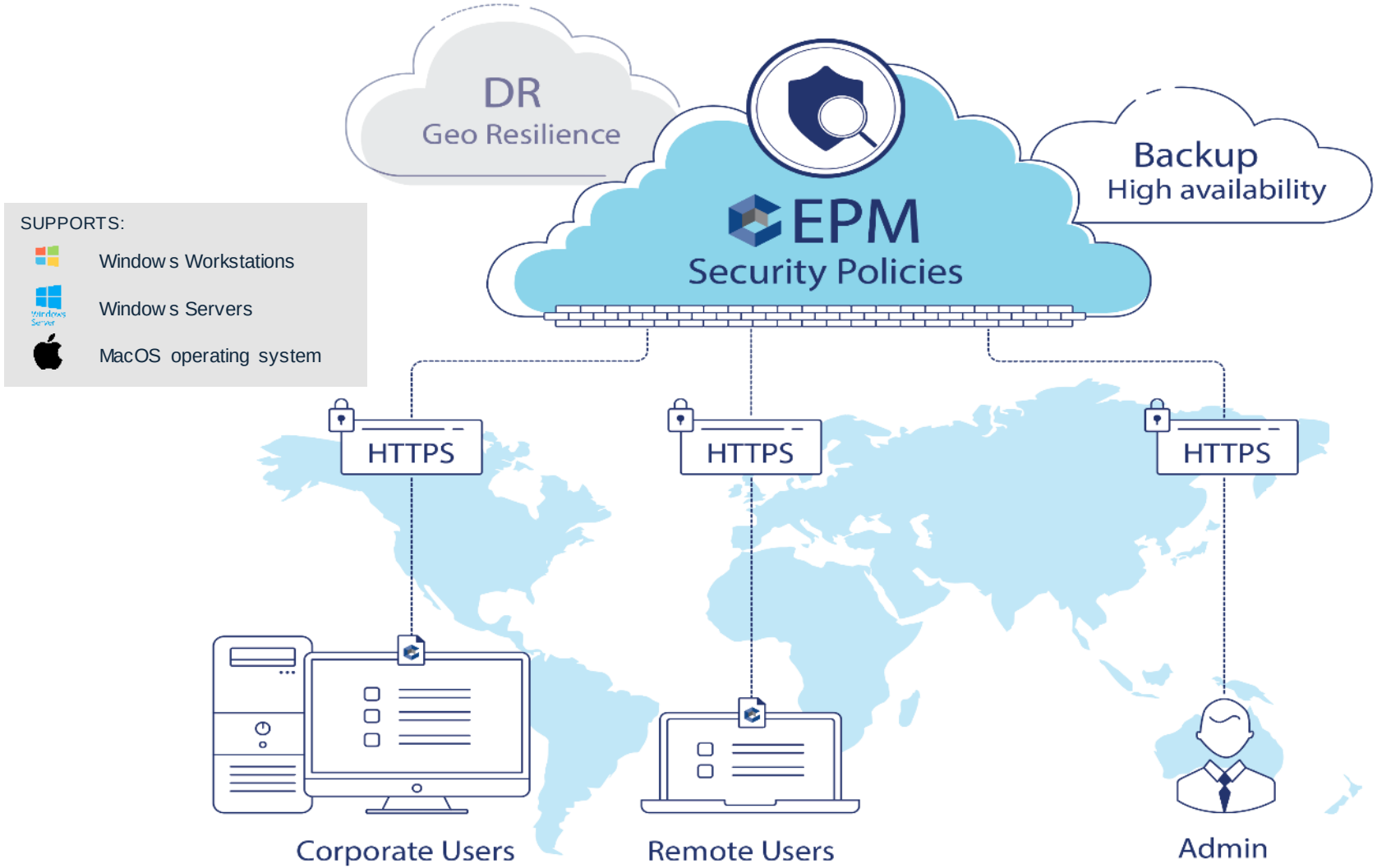
Most attacks start on the endpoints

Regardless of origin, attacker will typically have restricted rights and will need to elevate privilege to achieve goal (e.g. financial or data theft, disruption, vandalism)

ATTACK: THE PRIVILEGE PATHWAY



ENDPOINT PRIVILEGE MANAGER



AGENDA

- CrytpoVirology
  - Ransomware
    - Case Study
  - Crypto-Jacking
    - Case Study
- Endpoint security fundamentals
  - Least Privilege
  - Application Control
  - Deception technology
- Attack/Defense Demos
- Q&A

CYBERARK

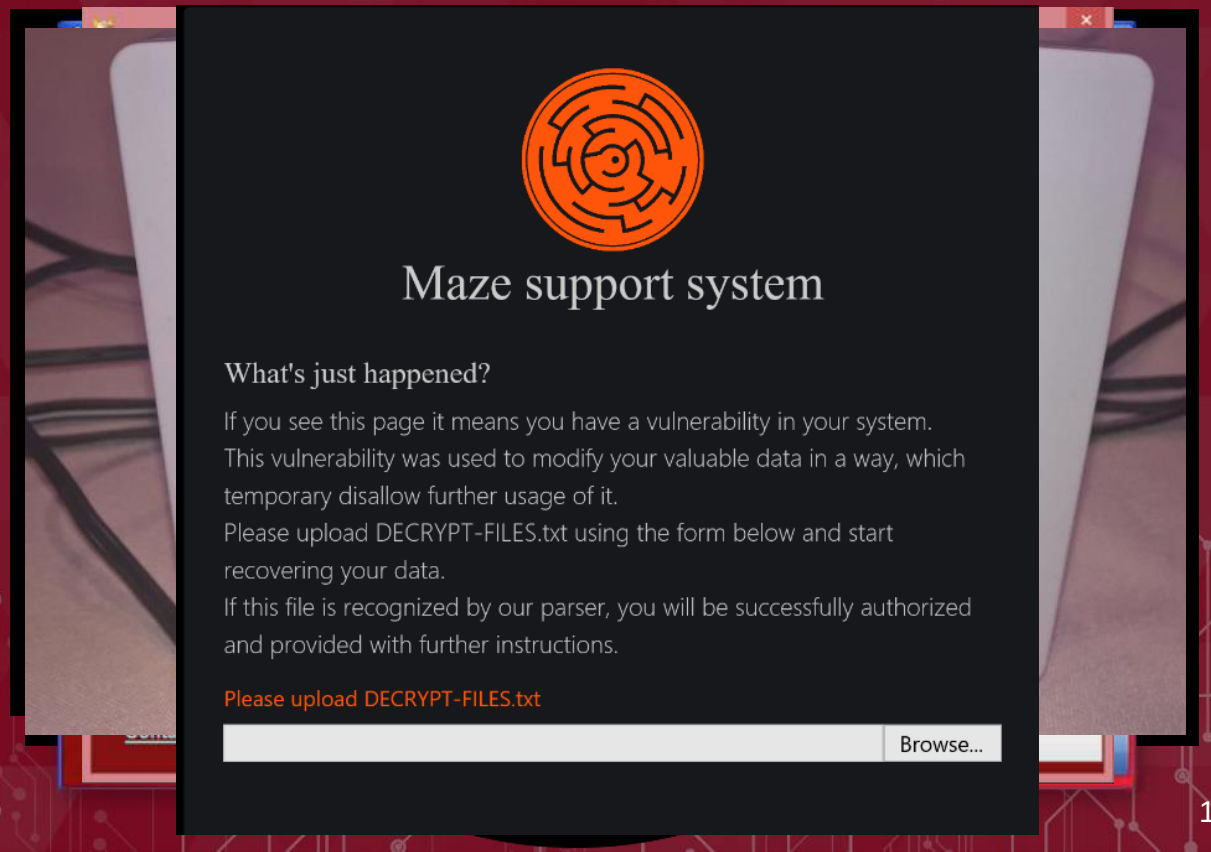
CRYPTO-VIROLOGY

RANSOMWARE

- Leveraging software to inhibits use of the system.
- Applies extortion on the assumption that the data is important enough to the user they are willing to pay for recovery.
- There is no guarantee of actual recovery, even after payment is made.

Evolution

- Non-Encrypting
- Encrypting
  - Self-Replicating
- IoT & Mobile Ransomware
- Exfiltration *(Leakware / DoxWare)*



RANSOMWARE PROTECTION

Ransomware is one of the most concerning cybersecurity threats today. Traditional Protection Is not enough

EVERYONE IS A TARGET

Endpoint Privilege Manager detect ransomware with certainty and respond before the attack can cause damage. Based on testing by CyberArk Labs, the removal of local administrator rights combined with application control was **100** percent effective in preventing ransomware from encrypting files.

CRYPTOJACKING

Unauthorized use of a resource to mine cryptocurrency

Scope:

- **Workstations (Windows, MacOS, Linux, etc)**
- **Mobile Devices (Android, iOS)**
- **Other Devices (routers, switches, IoT, etc)**
- **CI/CD Pipelines**

CRYPTOJACKING

Unauthorized use of a resource to mine cryptocurrency

Symptoms of CryptoJacking:

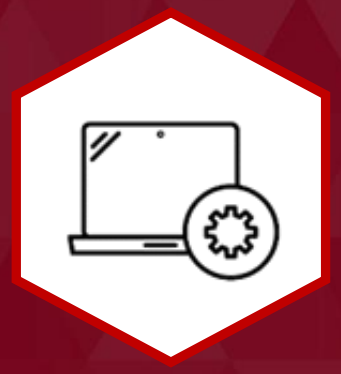
- **High resource utilization**
- **Slow system performance**
- **Device Overheating**
- **Ridiculously large bill.**

ENDPOINT SECURITY FUNDAMENTALS

SECURITY FUNDAMENTAL

Least Privilege – prevent attacks that start at the endpoint by removing local admin rights on Windows workstations, servers, and Macs.

THE PROBLEM: USERS WITH ADMIN RIGHTS CAN…



Change system configurations

Install malware

Access and change accounts

> “**87%** of organizations have not removed local admin rights which represents a significant increase YoY.”

Source: CyberArk Threat Landscape Survey, February 2018

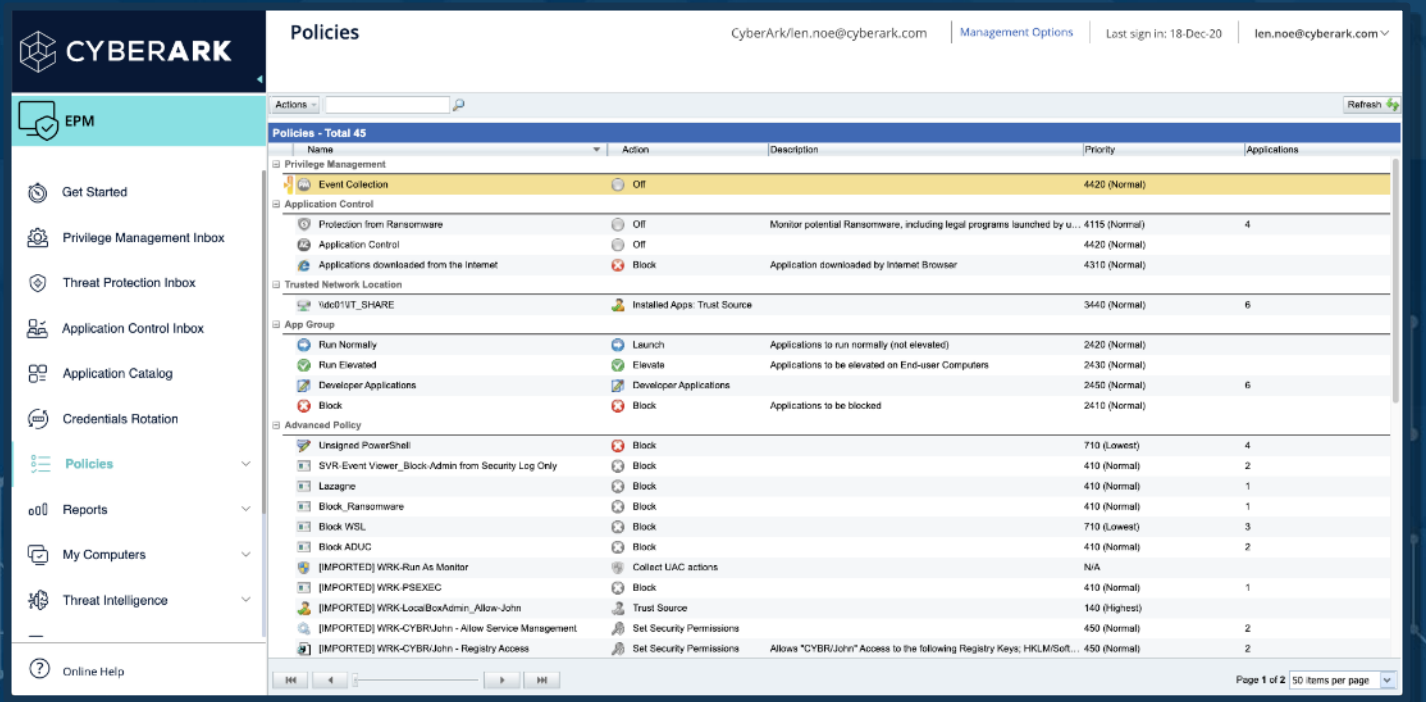
THE DILEMMA – SECURITY VS. OPERATIONAL IMPACT

	USERS HAVE LOCAL ADMIN RIGHTS	LOCAL ADMIN RIGHTS ARE REMOVED
OPERATIONS IMPACT	Happy, productive users 	Increased burden on the support team. Increased calls and costs. 
SECURITY IMPACT	Increased security incidents 	Contain attacks on the endpoint 

Enforce the **minimal** level of user rights, or lowest clearance level, that allows the user to perform their role

Endpoint Privilege Manager Privilege Management

- Remove local privileged accounts without the negative impact on the IT/helpdesk.
- Enforce granular least privilege policies for Windows administrators
- Seamlessly elevate user privileges as needed.
- Strengthen the protection and detection capabilities of your existing endpoint security



SECURITY FUNDAMENTAL

Application Control allows IT operations and security teams allow approved applications to run while restrict the unapproved ones..

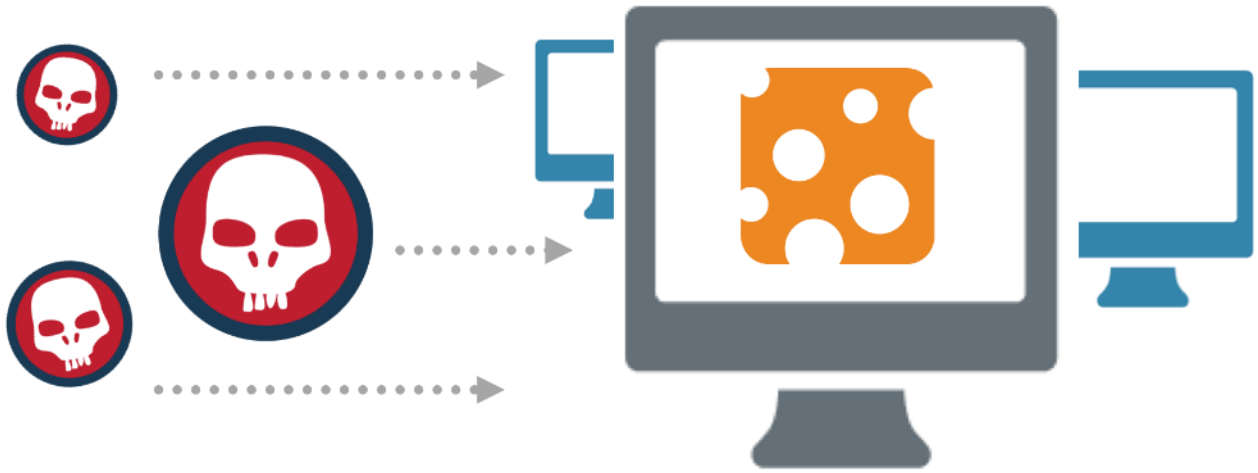
APPLICATION CONTROL

Endpoint Privilege Manager Application Control

- Allow approved applications to run while blocking malware, including Ransomware.
- Unknown applications, are run in ‘Restricted Mode’ which prevents them from accessing corporate resources, sensitive data or the internet.
- Application Risk Analysis service is provides additional insights about the risk.
- Trust business requirement sources such as SCCM, updaters, URL’s and more.

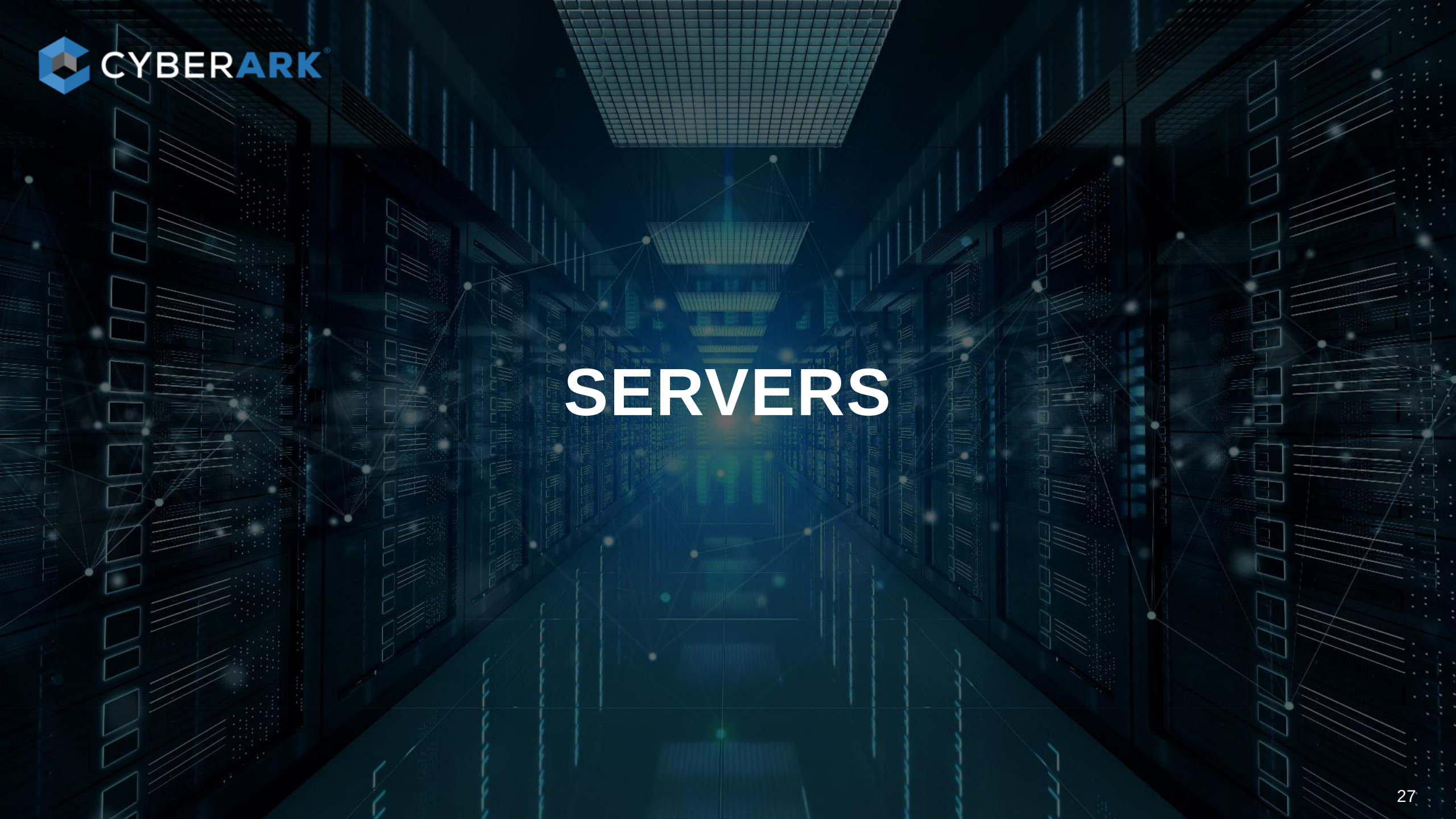
SECURITY FUNDAMENTAL

Privilege Deception feature enables defenders to quickly detect and proactively shut down in-progress attacks by placing deception components in the attack path.



Privilege Deception feature enables defenders to quickly detect and proactively shut down in-progress attacks by placing deception components in the attack path.

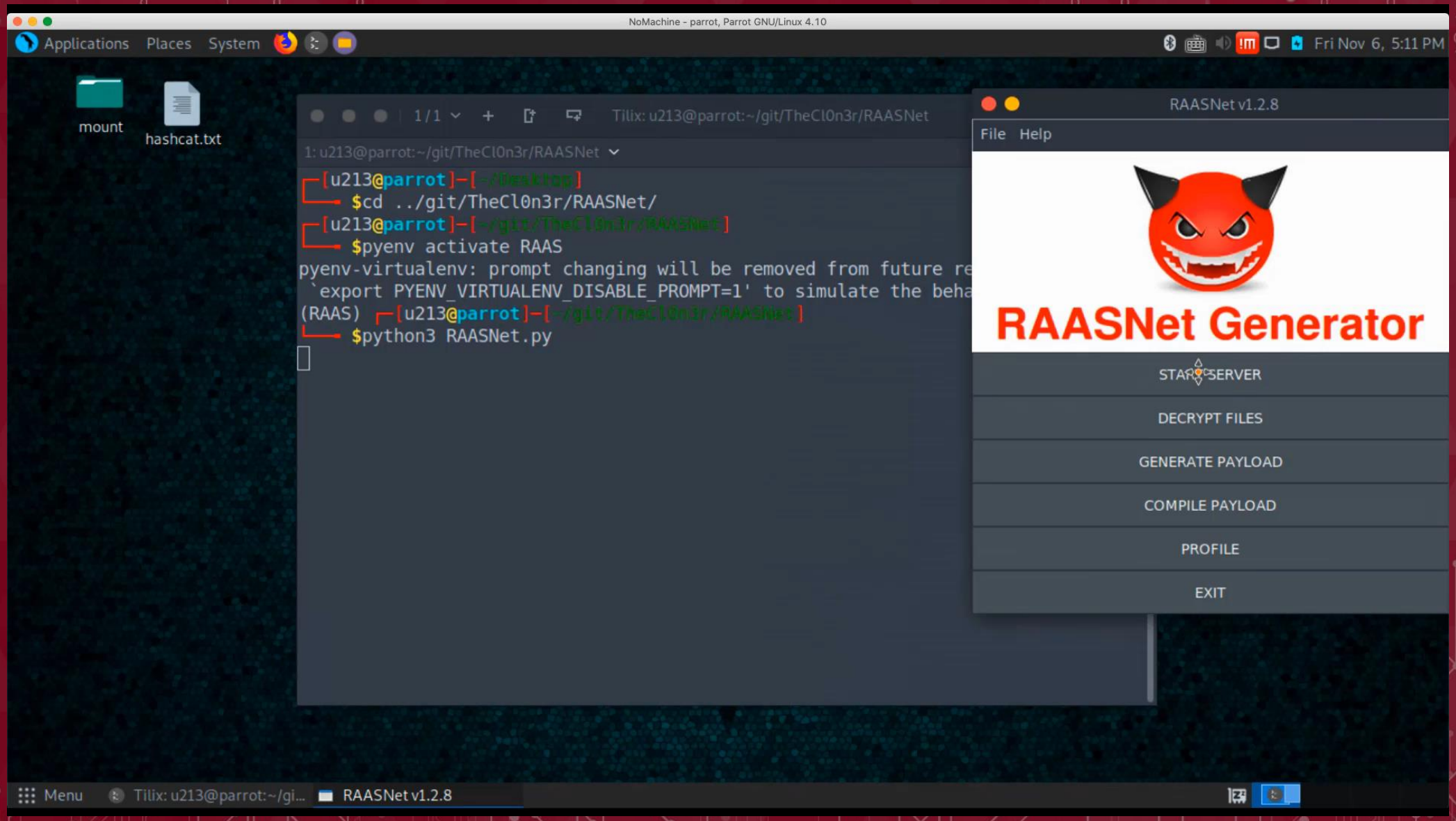
EPM helps break the attack chain at the initial point of entry by providing a deliberate and controlled way to track and mislead potential attackers, mitigate the exploitation of privileged credentials, and reduce dwell time.

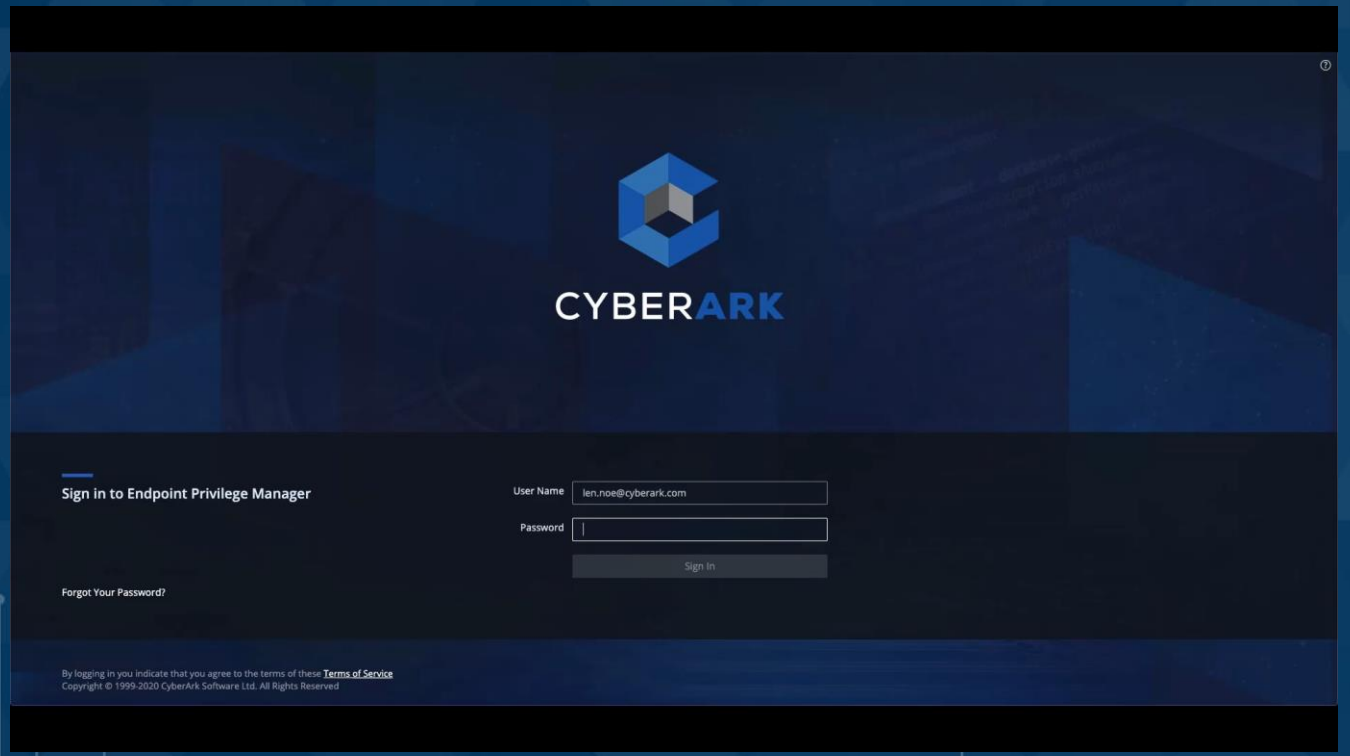

CYBERARK
SERVERS

CYBERARK

ATTACK DEMOS

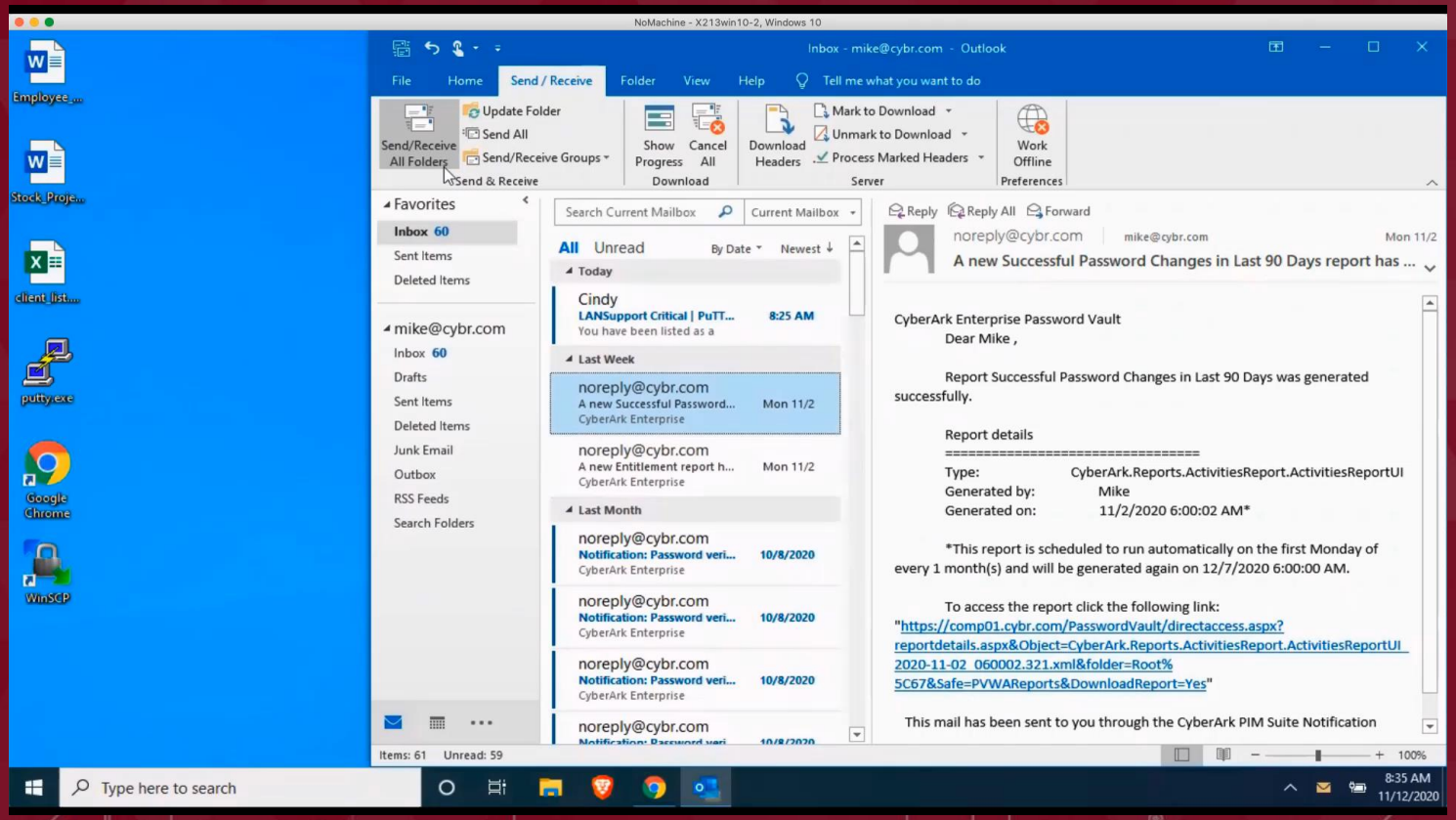
WHID CACTUS TO RANSOMWARE


NoMachine - parrot, Parrot GNU/Linux 4.10
Applications Places System
Fri Nov 6, 5:11 PM
mount
hashcat.txt
1 / 1
Tilix: u213@parrot:~/git/TheCl0n3r/RAASNet
1: u213@parrot:~/git/TheCl0n3r/RAASNet
[u213@parrot]-[~/Desktop]
$cd ../git/TheCl0n3r/RAASNet/
[u213@parrot]-[~/git/TheCl0n3r/RAASNet]
$pyenv activate RAAS
pyenv-virtualenv: prompt changing will be removed from future re
`export PYENV_VIRTUALENV_DISABLE_PROMPT=1' to simulate the beha
(RAAS) [u213@parrot]-[~/git/TheCl0n3r/RAASNet]
$python3 RAASNet.py
RAASNet v1.2.8
File Help
RAASNet Generator
START SERVER
DECRYPT FILES
GENERATE PAYLOAD
COMPILE PAYLOAD
PROFILE
EXIT
Menu
Tilix: u213@parrot:~/gi...
RAASNet v1.2.8

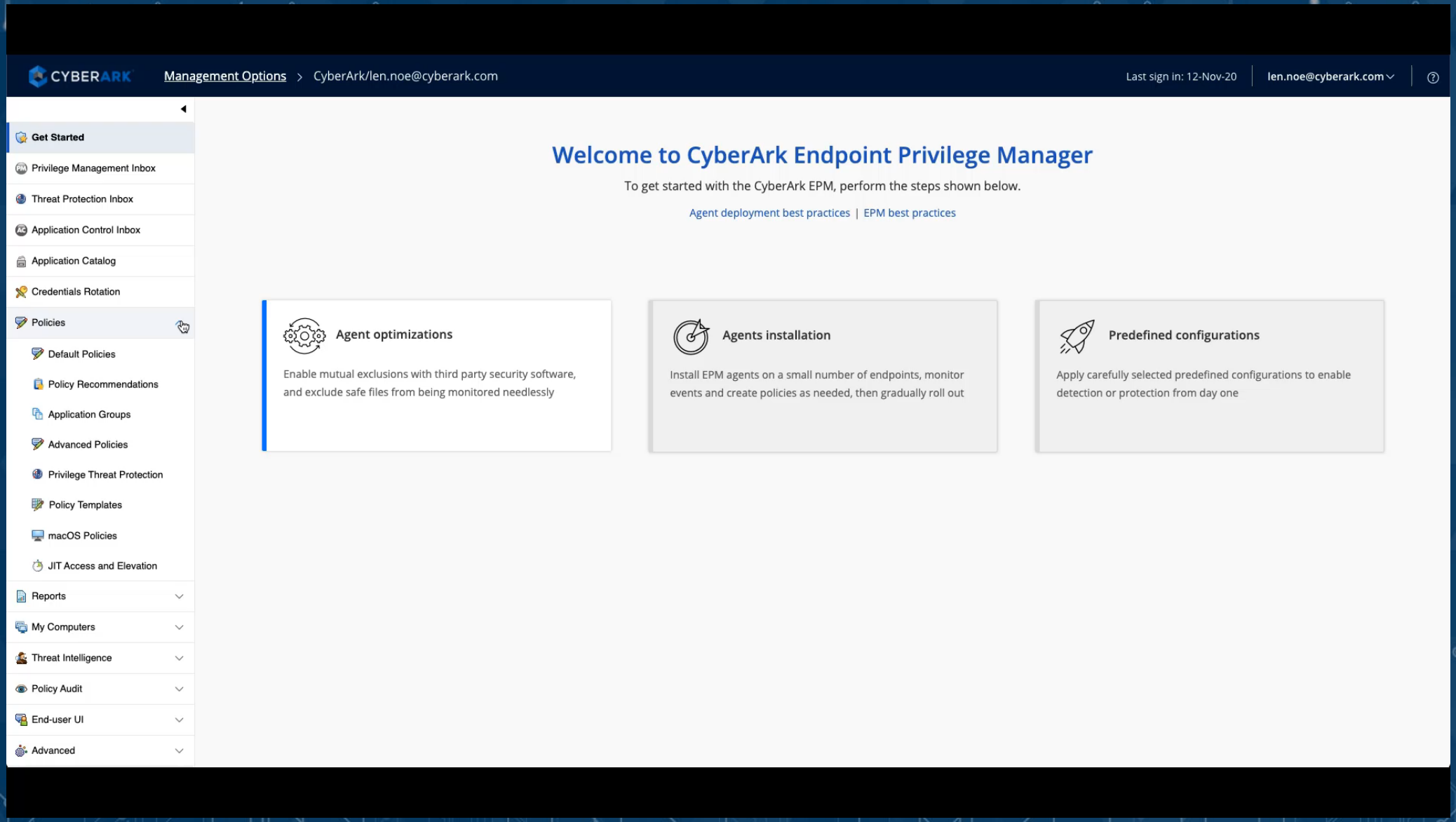

CYBERARK
Sign in to Endpoint Privilege Manager
User Name
len.noe@cyberark.com
Password
Sign In
Forgot Your Password?
By logging in you indicate that you agree to the terms of these Terms of Service
Copyright © 1999-2020 CyberArk Software Ltd. All Rights Reserved

CYBERARK

PHISH TO CRED DUMP

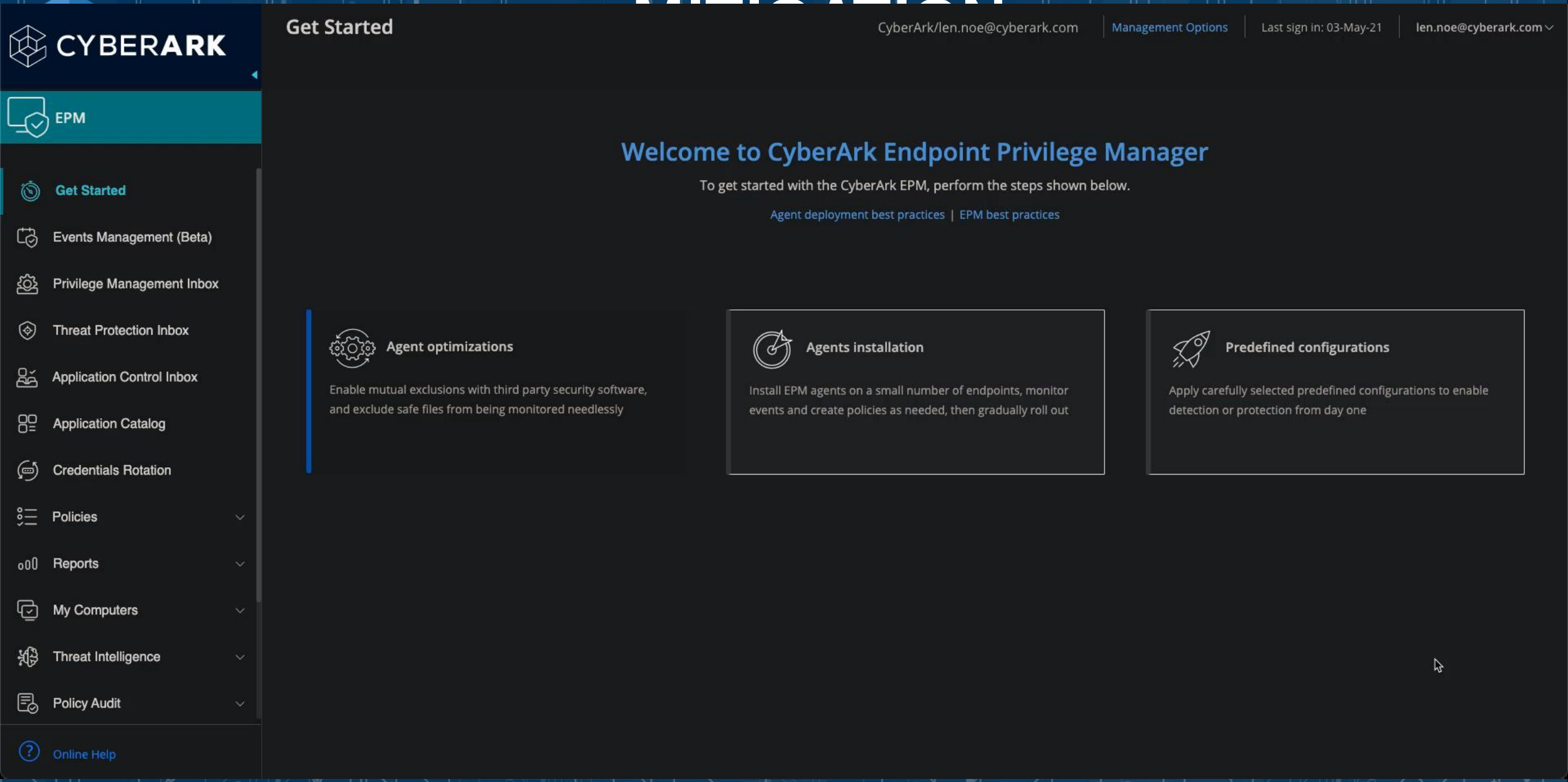

NoMachine - X213win10-2, Windows 10
Inbox - mike@cybr.com - Outlook
File
Home
Send / Receive
Folder
View
Help
Tell me what you want to do
Send/Receive All Folders
Update Folder
Send All
Send/Receive Groups
Send & Receive
Show Progress
Cancel All
Download
Download Headers
Mark to Download
Unmark to Download
Process Marked Headers
Server
Work Offline
Preferences
Favorites
Inbox 60
Sent Items
Deleted Items
mike@cybr.com
Inbox 60
Drafts
Sent Items
Deleted Items
Junk Email
Outbox
RSS Feeds
Search Folders
Search Current Mailbox
Current Mailbox
All
Unread
By Date
Newest
Today
Cindy
LANSupport Critical | PuTT...
8:25 AM
You have been listed as a
Last Week
noreply@cybr.com
A new Successful Password...
Mon 11/2
CyberArk Enterprise
noreply@cybr.com
A new Entitlement report h...
Mon 11/2
CyberArk Enterprise
Last Month
noreply@cybr.com
Notification: Password veri...
10/8/2020
CyberArk Enterprise
noreply@cybr.com
Notification: Password veri...
10/8/2020
CyberArk Enterprise
noreply@cybr.com
Notification: Password veri...
10/8/2020
CyberArk Enterprise
noreply@cybr.com
Reply
Reply All
Forward
noreply@cybr.com
mike@cybr.com
Mon 11/2
A new Successful Password Changes in Last 90 Days report has ...
CyberArk Enterprise Password Vault
Dear Mike ,
Report Successful Password Changes in Last 90 Days was generated successfully.
Report details
==========
Type: CyberArk.Reports.ActivitiesReport.ActivitiesReportUI
Generated by: Mike
Generated on: 11/2/2020 6:00:02 AM*
*This report is scheduled to run automatically on the first Monday of every 1 month(s) and will be generated again on 12/7/2020 6:00:00 AM.
To access the report click the following link:
"https://comp01.cybr.com/PasswordVault/directaccess.aspx?reportdetails.aspx&Object=CyberArk.Reports.ActivitiesReport.ActivitiesReportUI 2020-11-02_060002.321.xml&folder=Root%5C67&Safe=PVWAReports&DownloadReport=Yes"
This mail has been sent to you through the CyberArk PIM Suite Notification
Items: 61
Unread: 59
100%
Type here to search
8:35 AM
11/12/2020
Employee_...
Stock_Proje...
client_list...
putty.exe
Google Chrome
WinSCP

MITIGATION


CYBERARK
Management Options > CyberArk/len.noe@cyberark.com
Last sign in: 12-Nov-20
len.noe@cyberark.com
Get Started
Privilege Management Inbox
Threat Protection Inbox
Application Control Inbox
Application Catalog
Credentials Rotation
Policies
Default Policies
Policy Recommendations
Application Groups
Advanced Policies
Privilege Threat Protection
Policy Templates
macOS Policies
JIT Access and Elevation
Reports
My Computers
Threat Intelligence
Policy Audit
End-user UI
Advanced
Welcome to CyberArk Endpoint Privilege Manager
To get started with the CyberArk EPM, perform the steps shown below.
Agent deployment best practices | EPM best practices
Agent optimizations
Enable mutual exclusions with third party security software, and exclude safe files from being monitored needlessly
Agents installation
Install EPM agents on a small number of endpoints, monitor events and create policies as needed, then gradually roll out
Predefined configurations
Apply carefully selected predefined configurations to enable detection or protection from day one

CYBERARK

ICECAST TO CRYPTOJACK


CYBERARK
EPM
Get Started
Events Management (Beta)
Privilege Management Inbox
Threat Protection Inbox
Application Control Inbox
Application Catalog
Credentials Rotation
Policies
Reports
My Computers
Threat Intelligence
Policy Audit
Online Help
Get Started
CyberArk/len.noe@cyberark.com
Management Options
Last sign in: 03-May-21
len.noe@cyberark.com
Welcome to CyberArk Endpoint Privilege Manager
To get started with the CyberArk EPM, perform the steps shown below.
Agent deployment best practices | EPM best practices
Agent optimizations
Enable mutual exclusions with third party security software, and exclude safe files from being monitored needlessly
Agents installation
Install EPM agents on a small number of endpoints, monitor events and create policies as needed, then gradually roll out
Predefined configurations
Apply carefully selected predefined configurations to enable detection or protection from day one

CYBERARK

BASHBUNNY TO CRED DUMP

CYBERARK

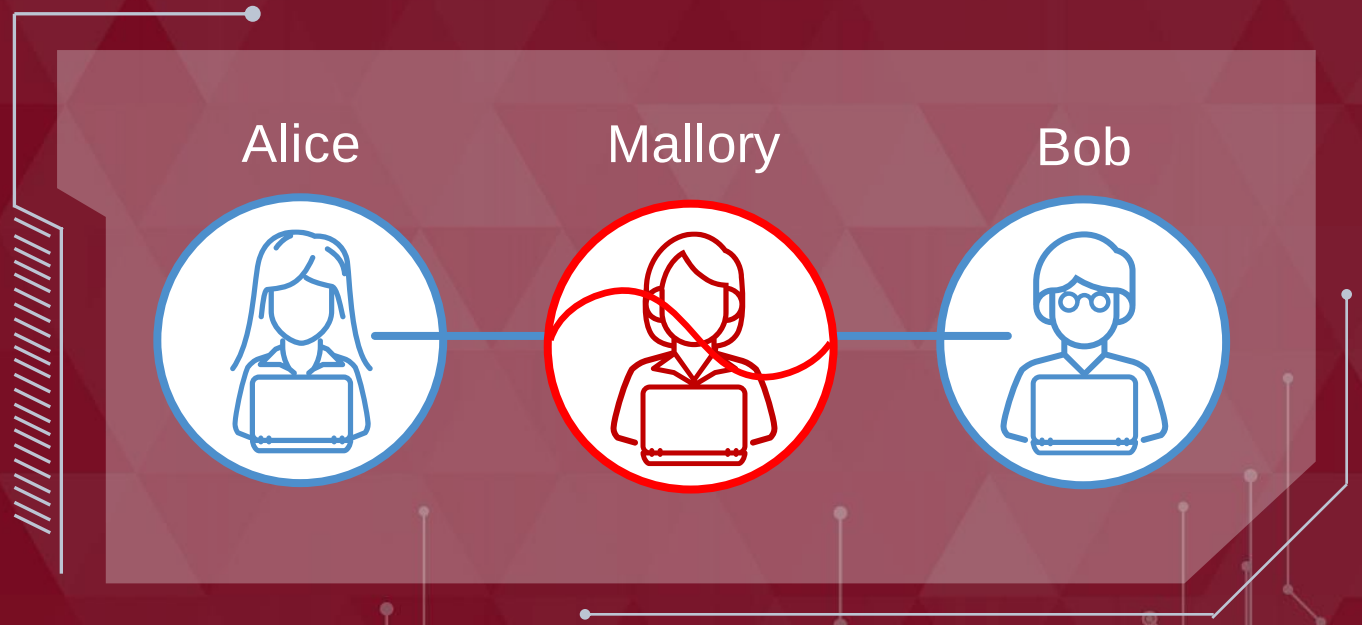
Option 1
Unsigned Powershell

MAN-IN-THE-MIDDLE

Attacker relays and potentially alters the communications between two parties

Types:

- **Physical Interception**
  - **Key-loggers**
  - **Network Taps**
  - **WIFI-Pineapple**



MAN-IN-THE-MIDDLE

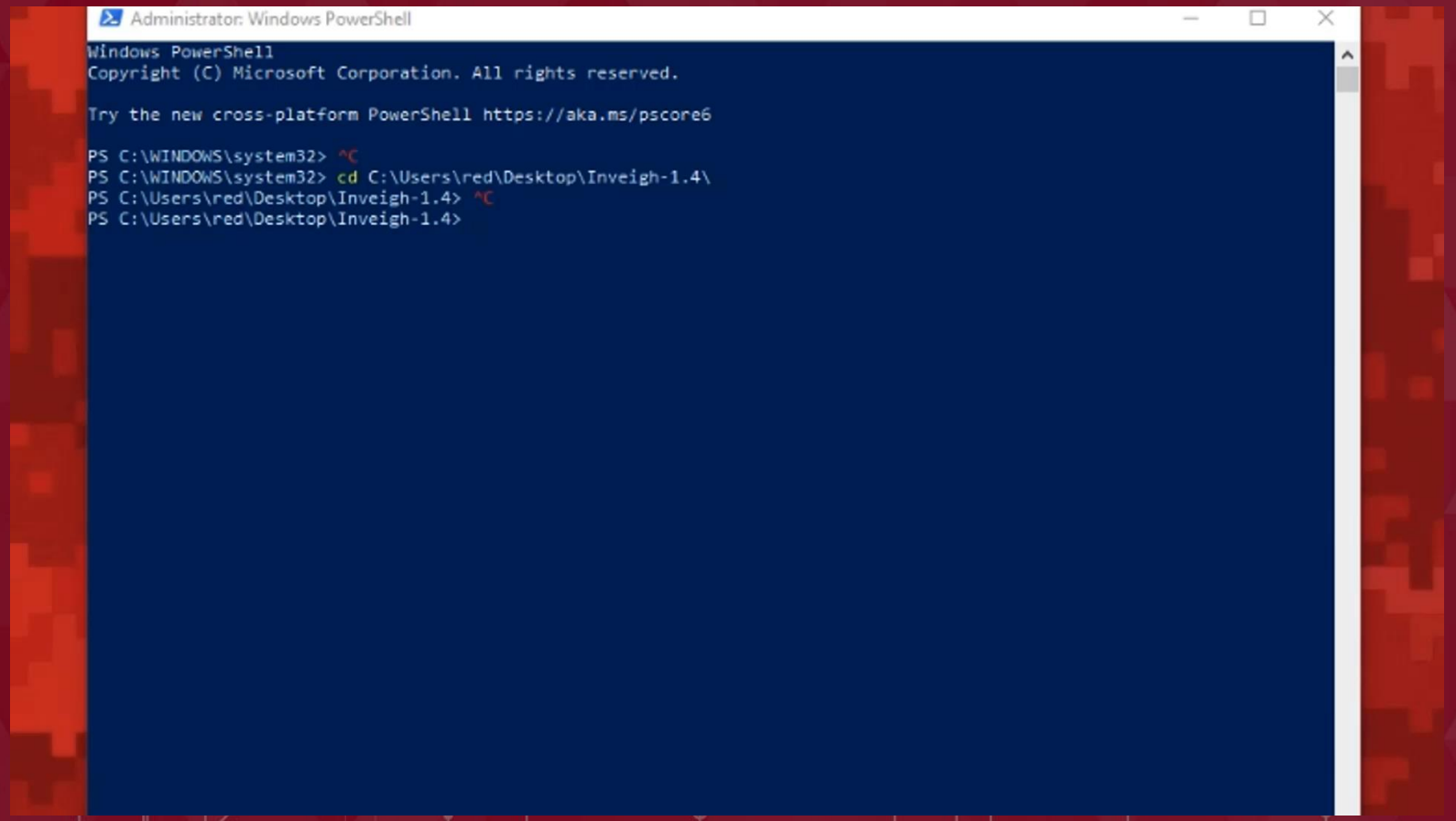
Attacker relays and potentially alters the communications between two parties

Types:

- Software
  - Responder & Inveigh
  - PyRDP

CYBERARK

INVEIGH TO DA BACKDOOR


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> ^C
PS C:\WINDOWS\system32> cd C:\Users\red\Desktop\Inveigh-1.4\
PS C:\Users\red\Desktop\Inveigh-1.4> ^C
PS C:\Users\red\Desktop\Inveigh-1.4>

CYBERARK

Mitigation 1
Admin Application Block

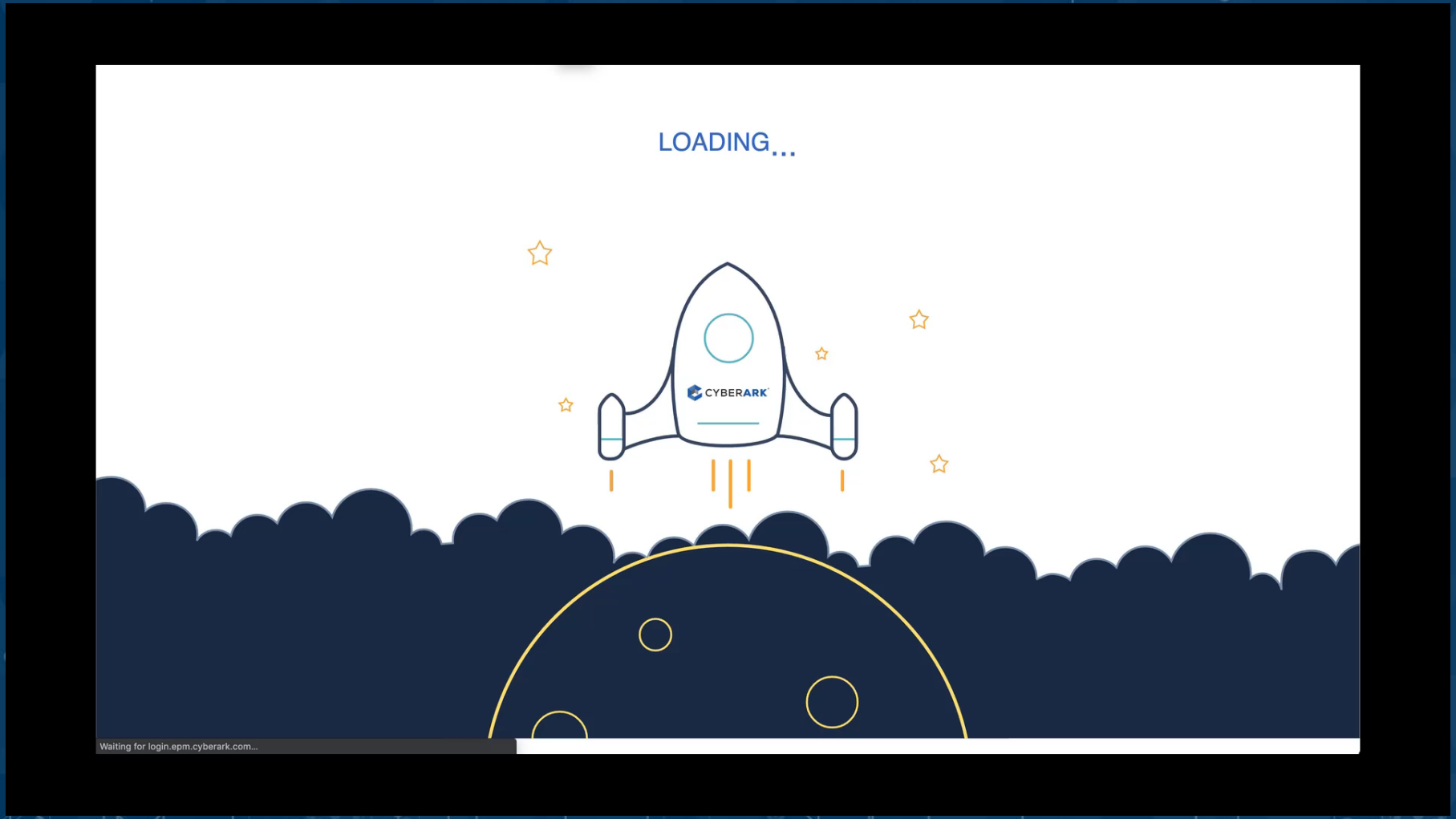
O.MG CABLE TO CRED HARVESTING

(PRIV THREAT DETECTION)

CYBERARK

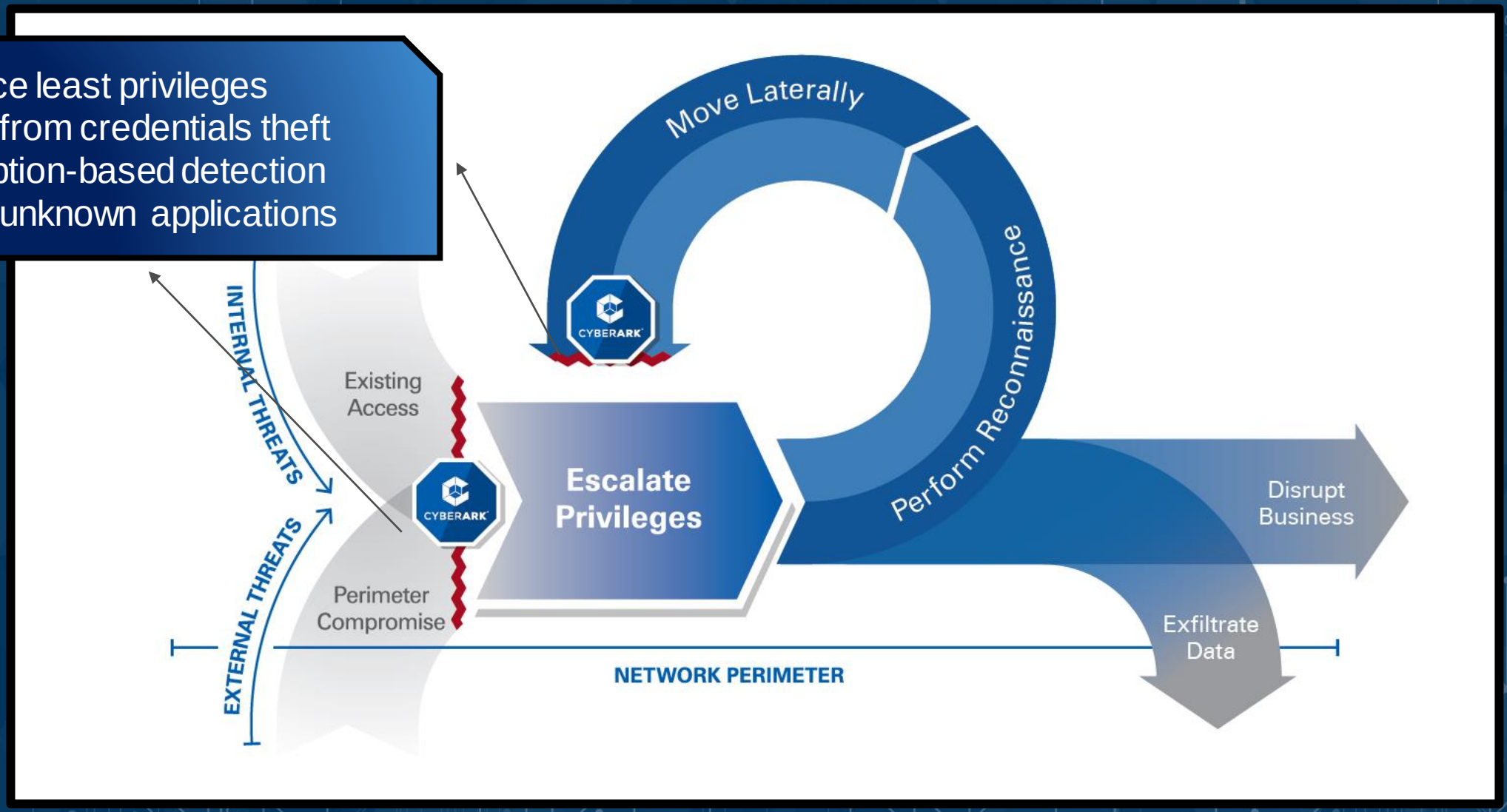
ATTACK

MITIGATION



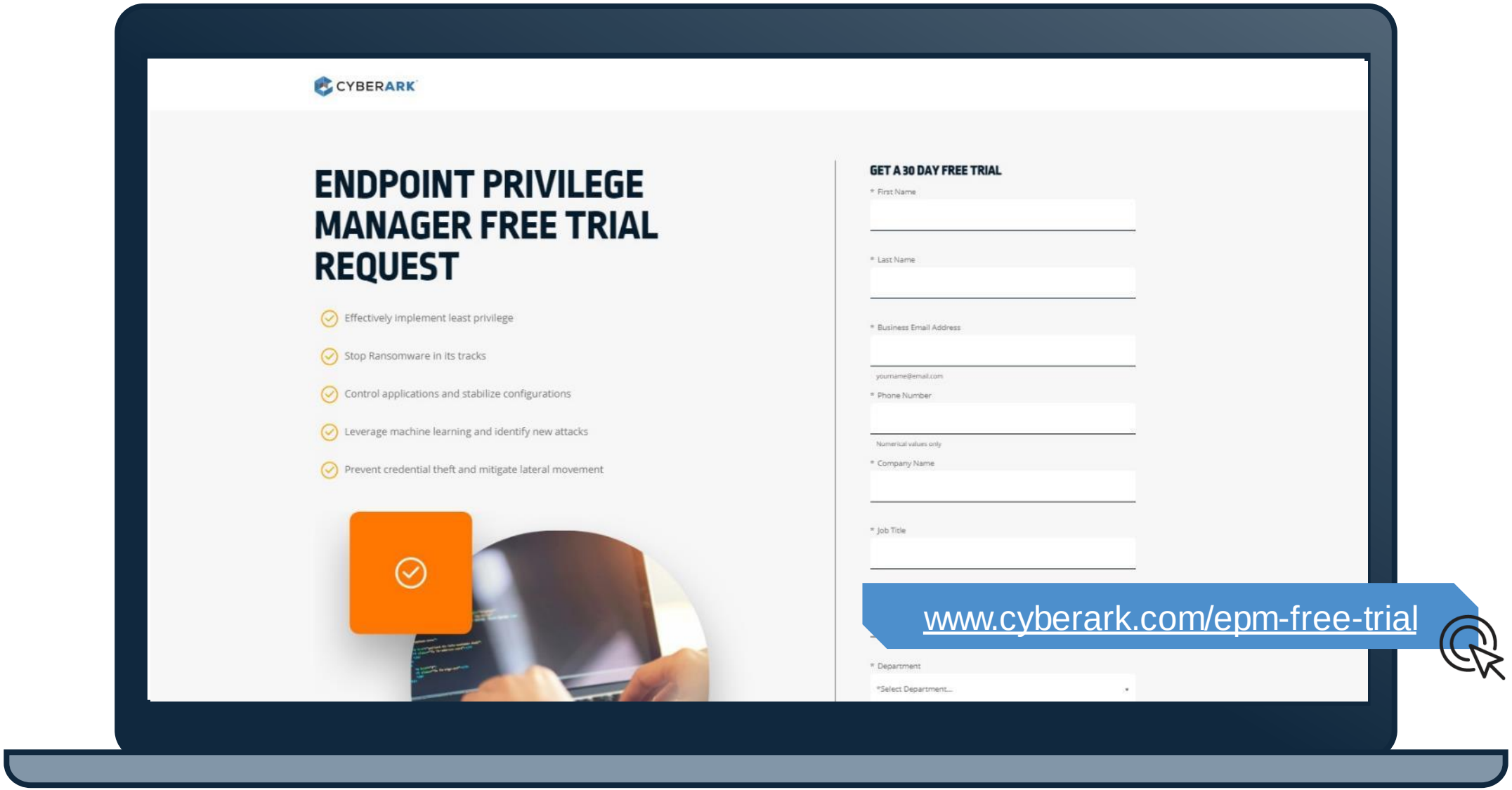
BREAK THE ATTACK CHAIN

- ✓ Enforce least privileges
- ✓ Block from credentials theft
- ✓ Deception-based detection
- ✓ Block unknown applications




CYBERARK
ATTACK & DEFEND
SERIES
QUESTIONS?

READY TO START? ENDPOINT PRIVILEGE MANAGER FREE TRIAL



UP NEXT

ENDPOINT PROTECTION TOOLING WEBINAR

July 1, 2021

UP NEXT

EXCLUSIVE: EPM HANDS-ON WORKSHOP

Americas & EMEA: July 20th

APJ: July 27th

THANK YOU