Gestire gli accessi ed incrementare la sicurezza degli Endpoint

2017.10.26 – Milano

TIG Cybertech Practical Workshop

Massimo Carlotti – CyberArk Sales Engineer

CYBERARK

AGENDA

- Why are we still discussing about these topics?
- How can we protect ourselves from known and unknown threats like this?
- Live Demo

Recycled Question!
Why are we still discussing about these topics?

? What is **STILL** the most common attack vector for threat actors today?

> Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication

James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

The Human Being

Built for trust

Helpful

Busy

Ambitious

Connected

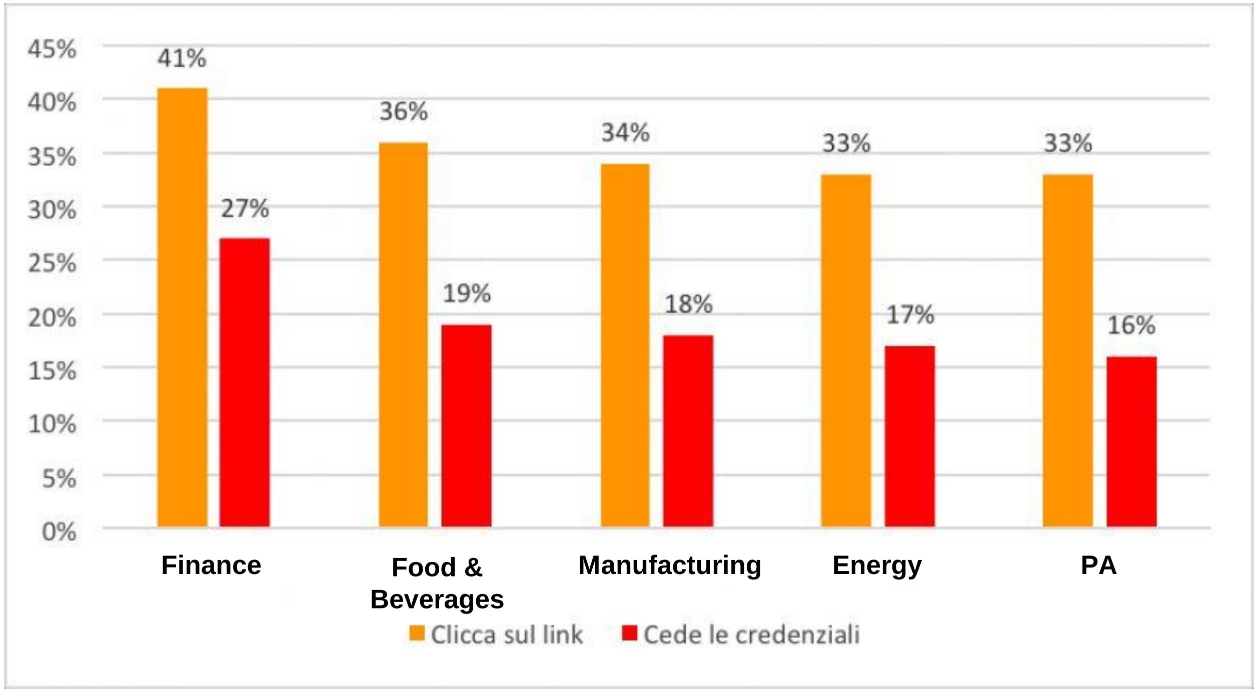
A DEFENSE CONSTANT

VULNERABLE

Test SDVA di CEFRIEL
(Social Driven Vulnerability Assessment)

- "I dati dimostrano che la crescita esponenziale di attacchi informatici non può prescindere dall'**elemento umano**. Da test di phishing che Cefriel ha effettuato su più di 20 imprese per 40mila persone coinvolte in tutta Europa risulta che oltre il **60% clicca su link ingannevoli** presenti nella mail mentre il **40% arriva a cedere le proprie credenziali** senza verificare la veridicità del mittente. Sorprende ancora di più il fatto che la grande maggioranza di questi fenomeni accade nei primi **20 minuti dal ricevimento** della mail stessa."

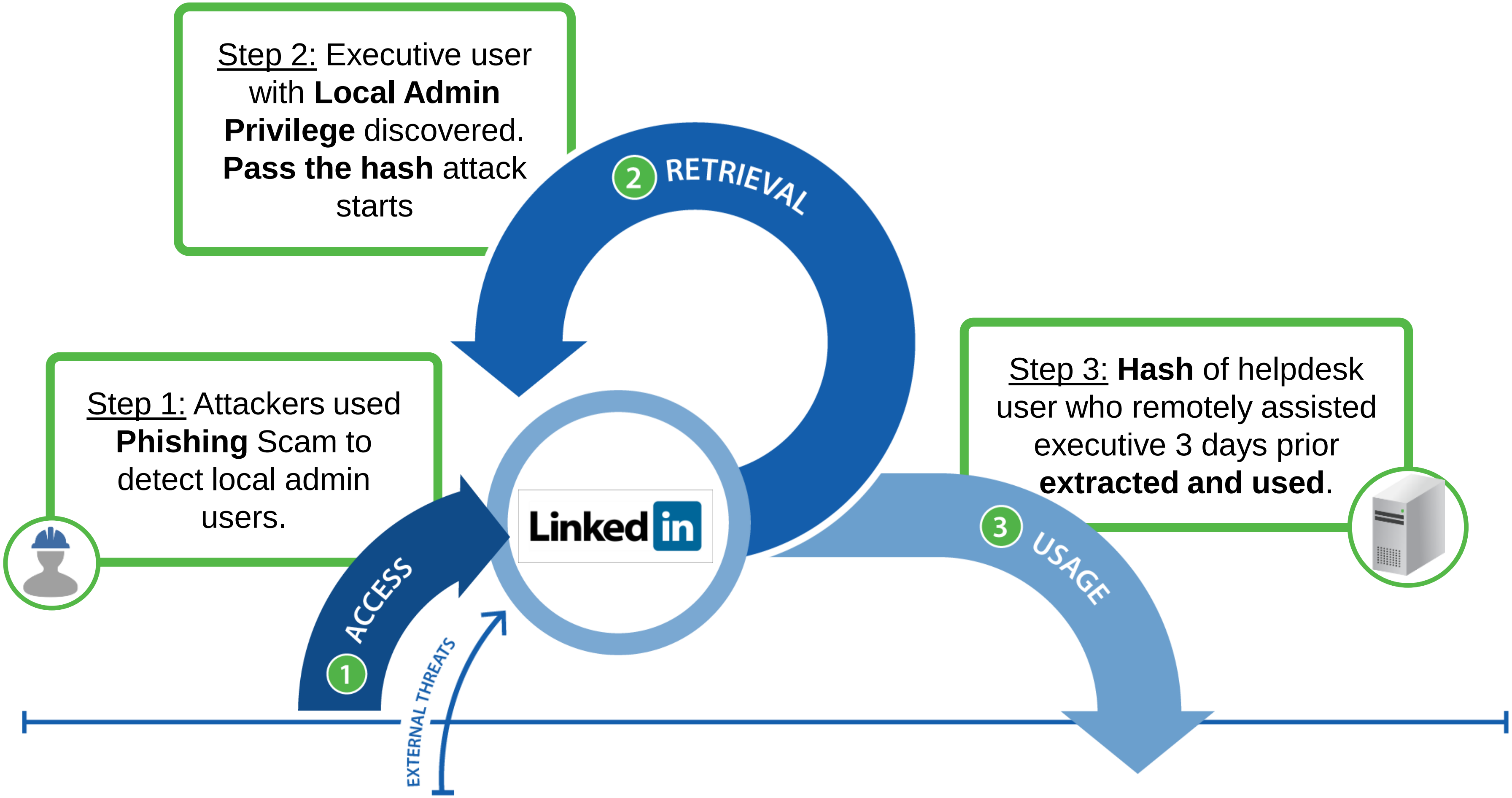
- "Oltre a un ingente piano di investimenti in cyber-security è necessario un progetto di formazione per cambiare l'approccio culturale."



Fonte: CEFRIEL - Ottobre 2017

Attack Pattern 1:
System Compromise & Data Exfiltration

How did the attack start?



Step 1: Attackers used **Phishing** Scam to detect local admin users.

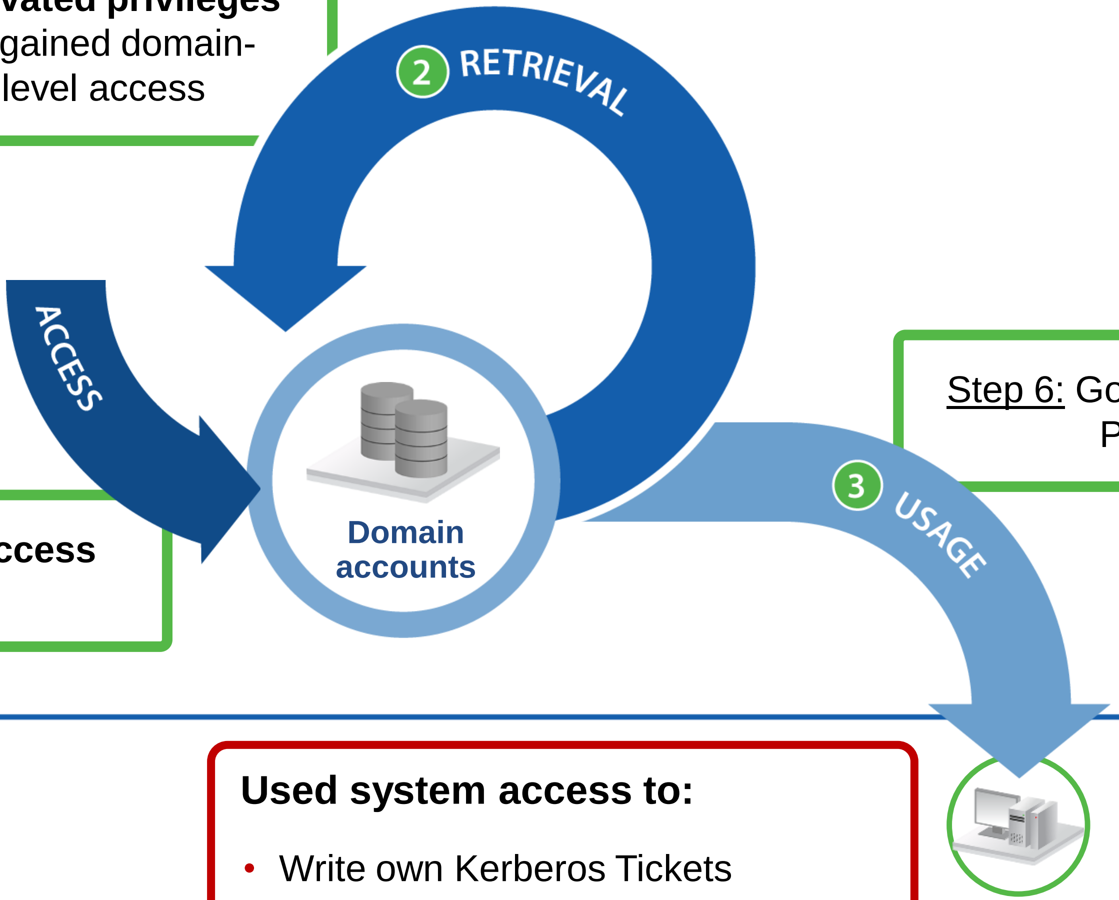
Step 2: Executive user with **Local Admin Privilege** discovered. **Pass the hash** attack starts

Step 3: **Hash** of helpdesk user who remotely assisted executive 3 days prior **extracted and used**.

What happened?

Step 5: **Elevated privileges** until they gained domain-admin level access

Step 4: **Server Access** gained



Step 6: Golden Ticket **Attack** Performed

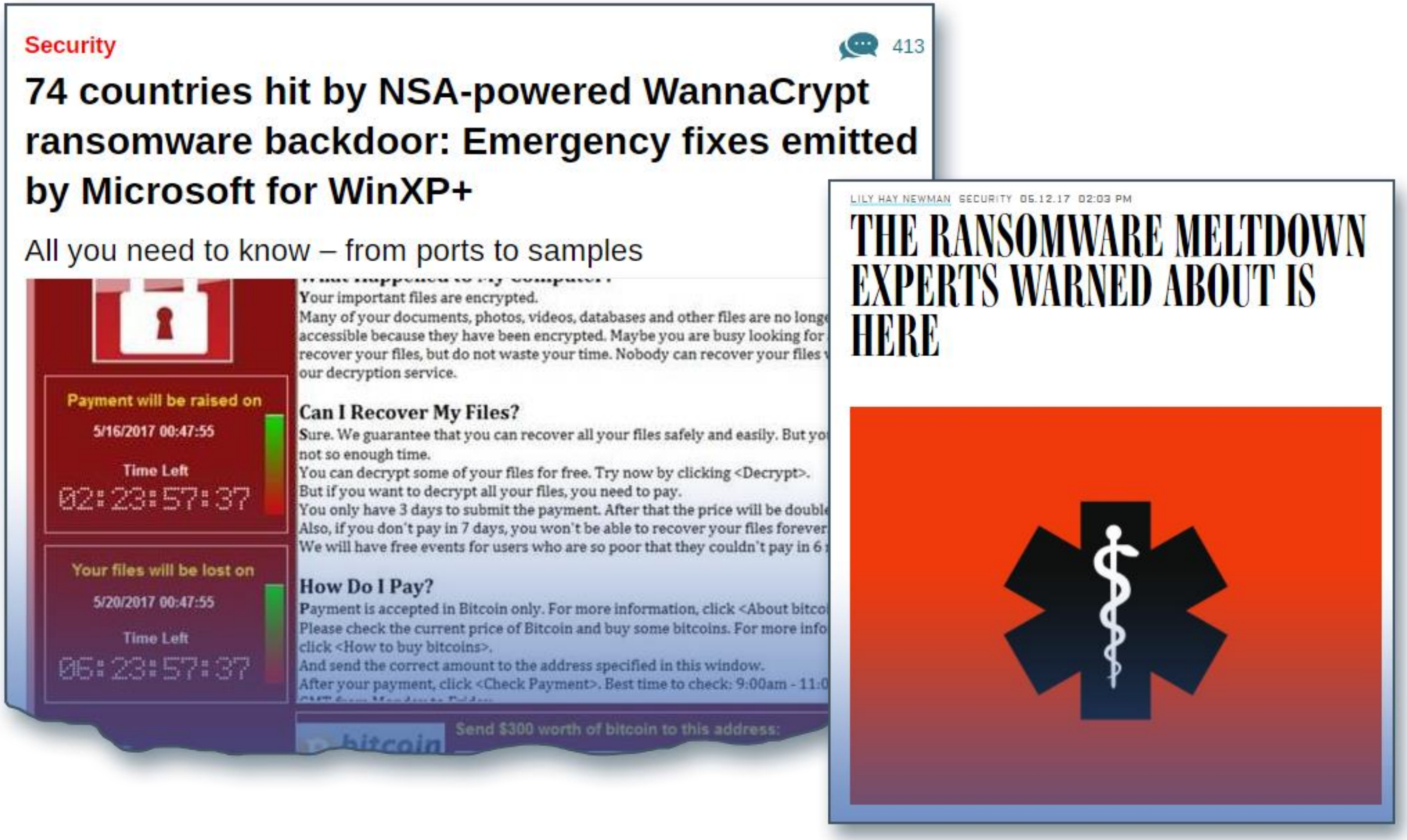
Used system access to:

- Write own Kerberos Tickets
- Compromise Business
- Exfiltrate Data

CYBERARK

Attack Pattern 2: Ransomware

Another Month, Another Wake Up Call



Security

413

74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+

All you need to know – from ports to samples

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longe
accessible because they have been encrypted. Maybe you are busy looking for
recover your files, but do not waste your time. Nobody can recover your files
our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But yo
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be double
Also, if you don't pay in 7 days, you won't be able to recover your files forever
We will have free events for users who are so poor that they couldn't pay in 6

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitco
Please check the current price of Bitcoin and buy some bitcoins. For more info
click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:0
GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

LILY HAY NEWMAN SECURITY 05.12.17 02:03 PM

THE RANSOMWARE MELTDOWN EXPERTS WARNED ABOUT IS HERE

Modern Ransomware Flow
=> Landing

1 **Phishing email**

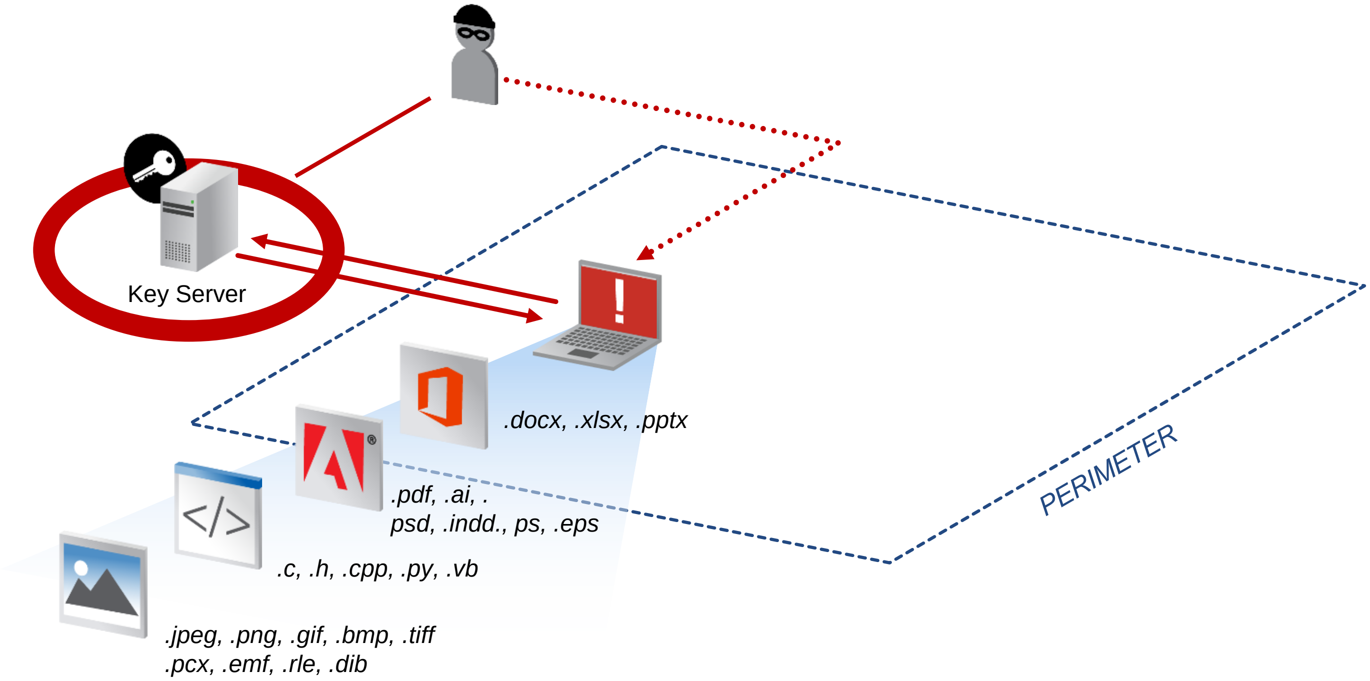
Targeting employees; employees open attachment

2 **Retrieve encryption key**

Ransomware reaches out to key server for unique key

3 **Build file inventory**

Machine is scanned for files; inventory is built



CYBERARK®

Modern Ransomware Flow
=> Lateral Movement and Execution

4 **Attempt to propagate**

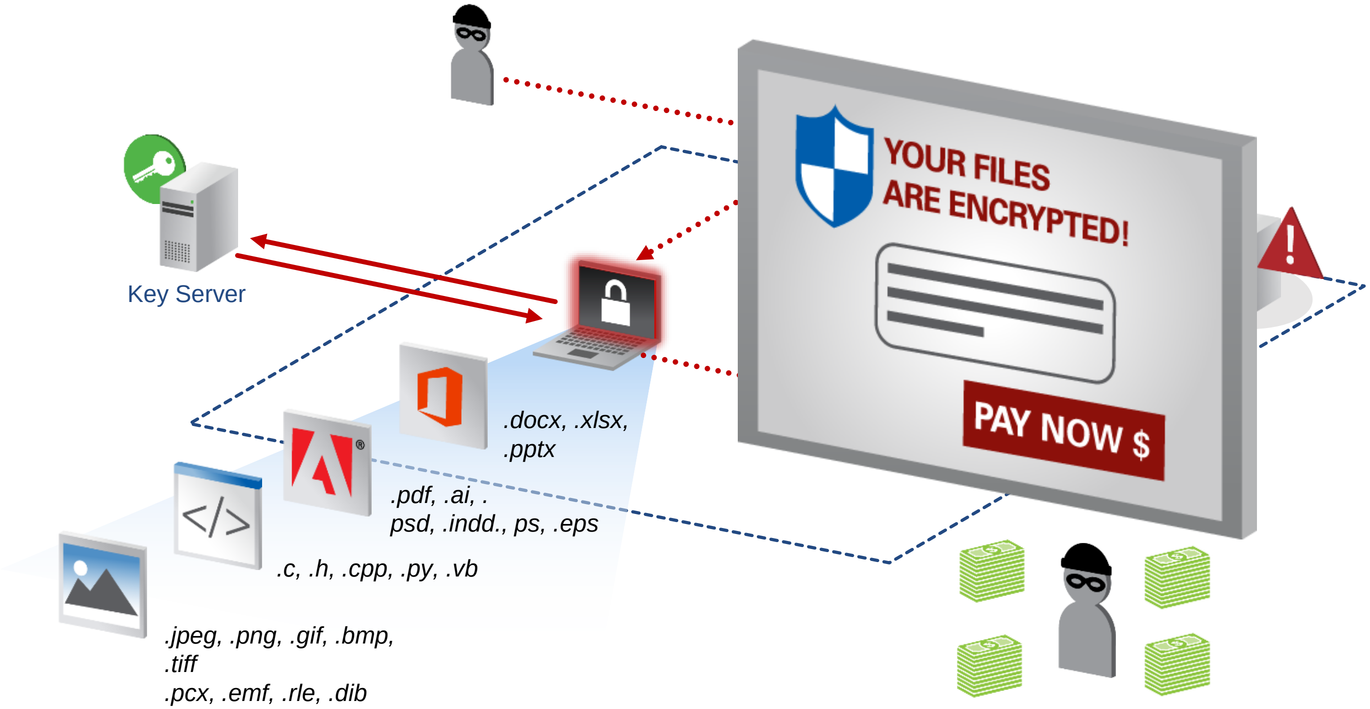
Scan for connected machines; capture credentials if able

5 **Spread through network**

Jump or log in to connected machines; drop ransomware

6 **Encrypt, notify, repeat**

Encrypt inventoried files; notify user of ransom requirement


Key Server
YOUR FILES ARE ENCRYPTED!
PAY NOW $
.docx, .xlsx, .pptx
.pdf, .ai, . psd, .indd., ps, .eps
.c, .h, .cpp, .py, .vb
.jpeg, .png, .gif, .bmp, .tiff
.pcx, .emf, .rle, .dib

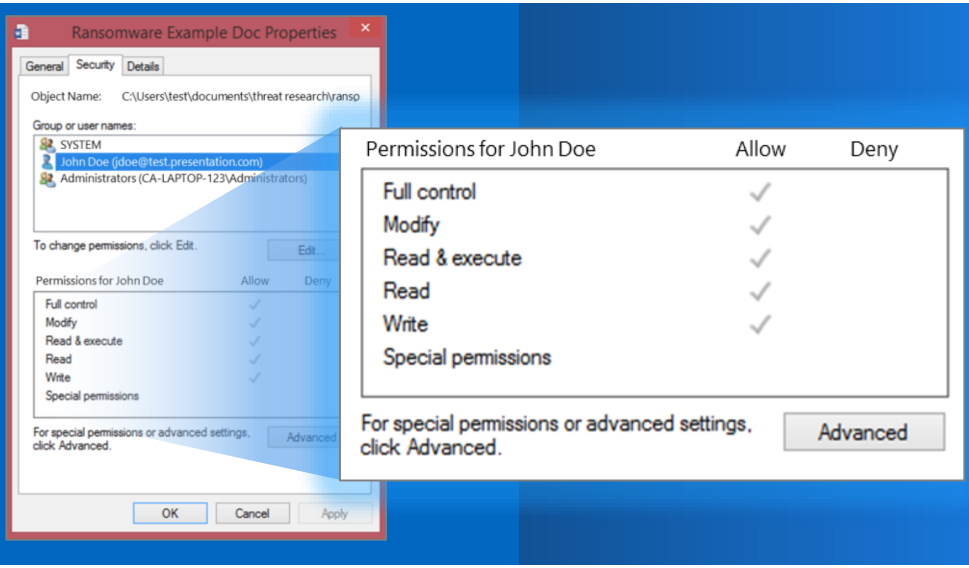
CYBERARK

Why Is Today’s Ransomware So Effective?

1 Polymorphic malware helps evades detection

2 Privileges needed to encrypt files are standard user privileges

3 Leverages escalated privilege to aid in propagation and attack



Object Name: C:\Users\test\documents\threat research\ranso

Group or user names:

SYSTEM
John Doe (jdoe@test.presentation.com)
Administrators (CA-LAPTOP-123\Administrators)

To change permissions, click Edit.

Permissions for John Doe	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

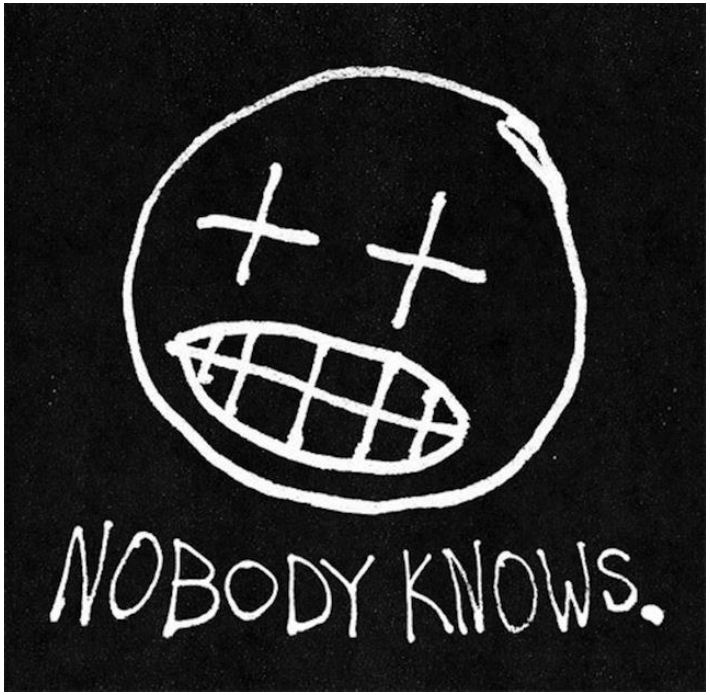
Permissions for John Doe	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

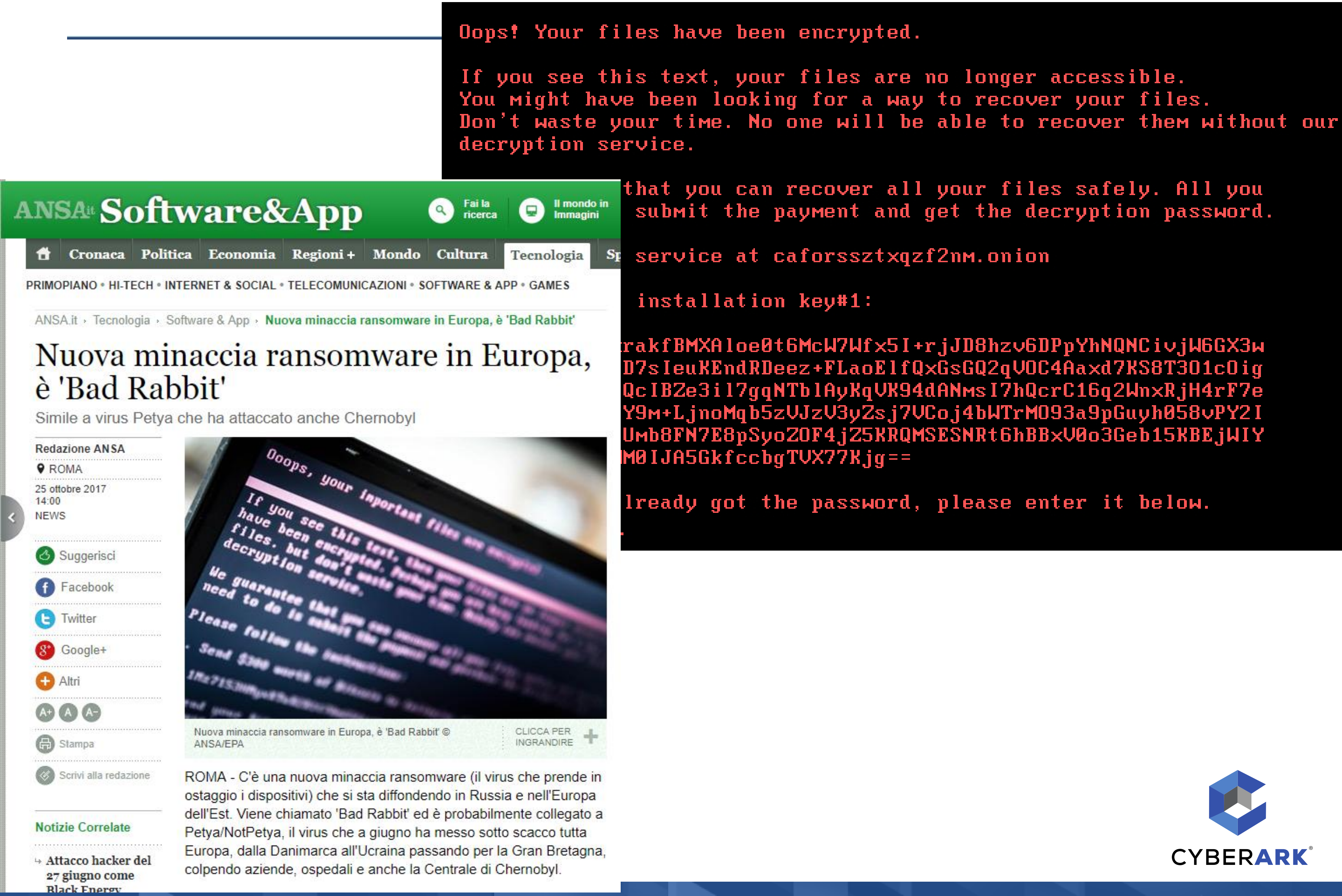
What’s Around The Corner?

- WannaCry uses 2 NSA-leaked hacking tools
- In May, EternalRocks was discovered, leveraging 7 NSA exploits
- Rise of CryptoWorms – More effective propagation
- Attack surface is becoming more varied
  - GeorgiaTech PLC Ransomware POC
- Programmatic credential theft increasing

What’s Around The Corner?



Latest news: BAD RABBIT



```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

that you can recover all your files safely. All you
 submit the payment and get the decryption password.

 service at caforssztxqzf2nm.onion

 installation key#1:

rakfBMXAloe0t6McW7Wfx5I+rjJD8hzv6DPpYhNQNCivjW6GX3w
D7sIeuKEndRDeez+FLaoElfQxGsGQ2qVOC4Aaxd7KS8T301cOig
QcIBZe3il7gqNTblAyKqVK94dANmsI7hQcrC16q2WnxRjH4rF7e
Y9m+LjnoMqb5zVJzV3y2sj7VCoj4bWTrM093a9pGuyh058vPY2I
Umb8FN7E8pSyoZOF4jZ5KRQMSESNRt6hBBxV0o3Geb15KBEjWIY
M0IJA5GkfccbgTVX77Kjg==

lready got the password, please enter it below.
```

ANSA.it Software&App
Fai la ricerca
Il mondo in Immagini
Cronaca
Politica
Economia
Regioni +
Mondo
Cultura
Tecnologia
Sp
PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP • GAMES
ANSA.it › Tecnologia › Software & App › Nuova minaccia ransomware in Europa, è 'Bad Rabbit'

Nuova minaccia ransomware in Europa, è 'Bad Rabbit'

Simile a virus Petya che ha attaccato anche Chernobyl

Redazione ANSA
ROMA
25 ottobre 2017
14:00
NEWS

Suggerisci
Facebook
Twitter
Google+
Altri
A+ A A-
Stampa
Scrivi alla redazione
Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
Send $300 worth of Bitcoin to following address:
CLICCA PER INGRANDIRE

Nuova minaccia ransomware in Europa, è 'Bad Rabbit' © ANSA/EPA

ROMA - C'è una nuova minaccia ransomware (il virus che prende in ostaggio i dispositivi) che si sta diffondendo in Russia e nell'Europa dell'Est. Viene chiamato 'Bad Rabbit' ed è probabilmente collegato a Petya/NotPetya, il virus che a giugno ha messo sotto scacco tutta Europa, dalla Danimarca all'Ucraina passando per la Gran Bretagna, colpendo aziende, ospedali e anche la Centrale di Chernobyl.

Notizie Correlate

- Attacco hacker del 27 giugno come Black Energy

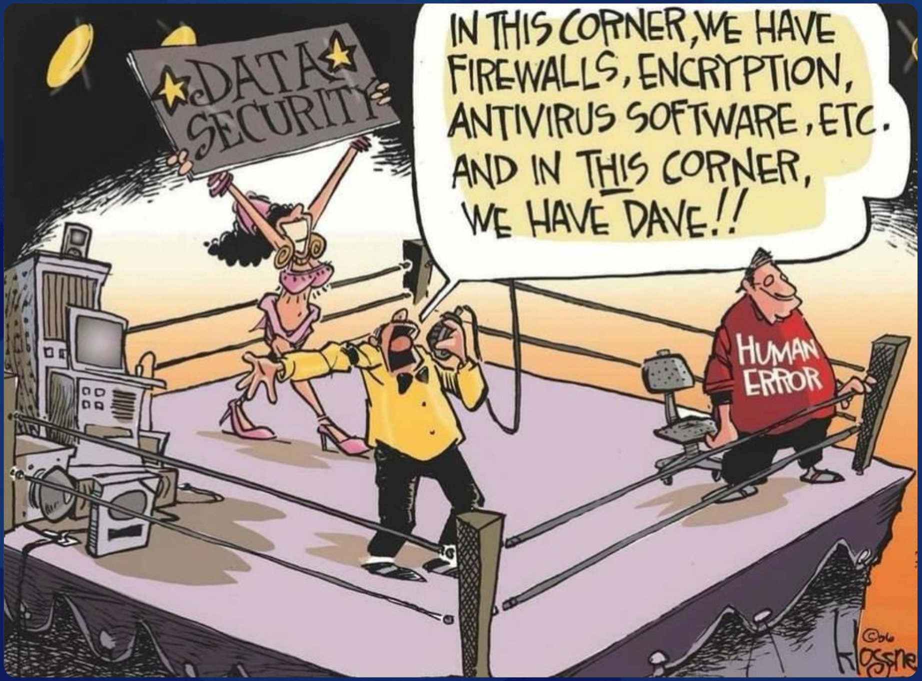
CYBERARK

How can we protect ourselves from known and unknown threats like this?

STEP 1:

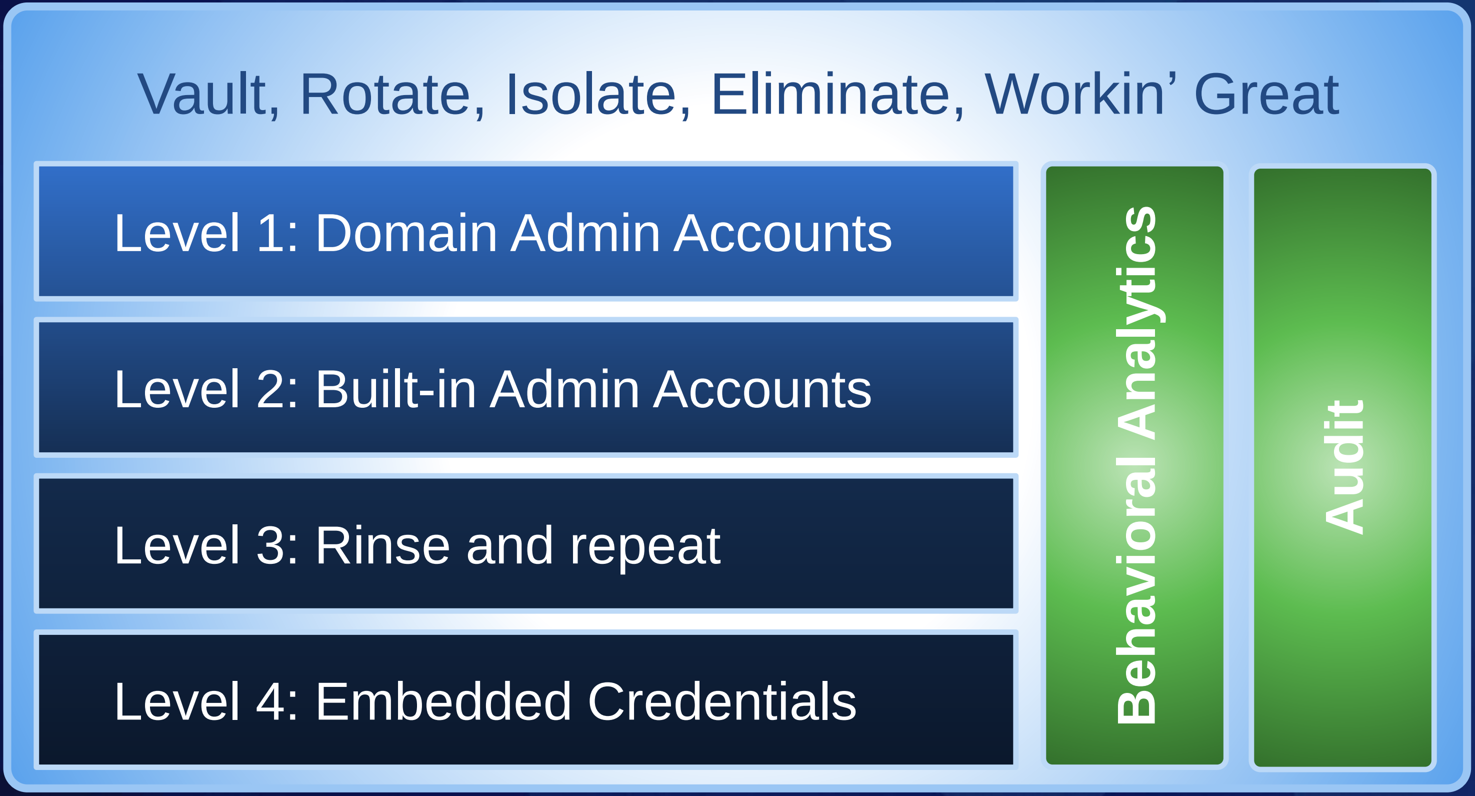
Use/audit what you have

- Update your AV
- Patch, patch and patch some more
- Don’t forget the perimeter
- Protect Data
- Audit your security controls
- Perform backups
- …
- Continue to educate users
- Don’t assume that “it could never happen” to you


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06 Klossne

STEP 2:

Don’t Neglect Controls at the IT Layer



Vault, Rotate, Isolate, Eliminate, Workin’ Great

Level 1: Domain Admin Accounts

Level 2: Built-in Admin Accounts

Level 3: Rinse and repeat

Level 4: Embedded Credentials

Behavioral Analytics

Audit

Qual è la situazione in azienda con riferimento alla gestione delle credenziali e agli audit delle sessioni degli utenti

Domanda 1. Avete definito, per i sistemi sensibili, procedure di gestione delle credenziali (complessità, rotazione, permessi di utilizzo, …) e audit completi delle sessioni degli utenti (testo, video, comandi,…)?

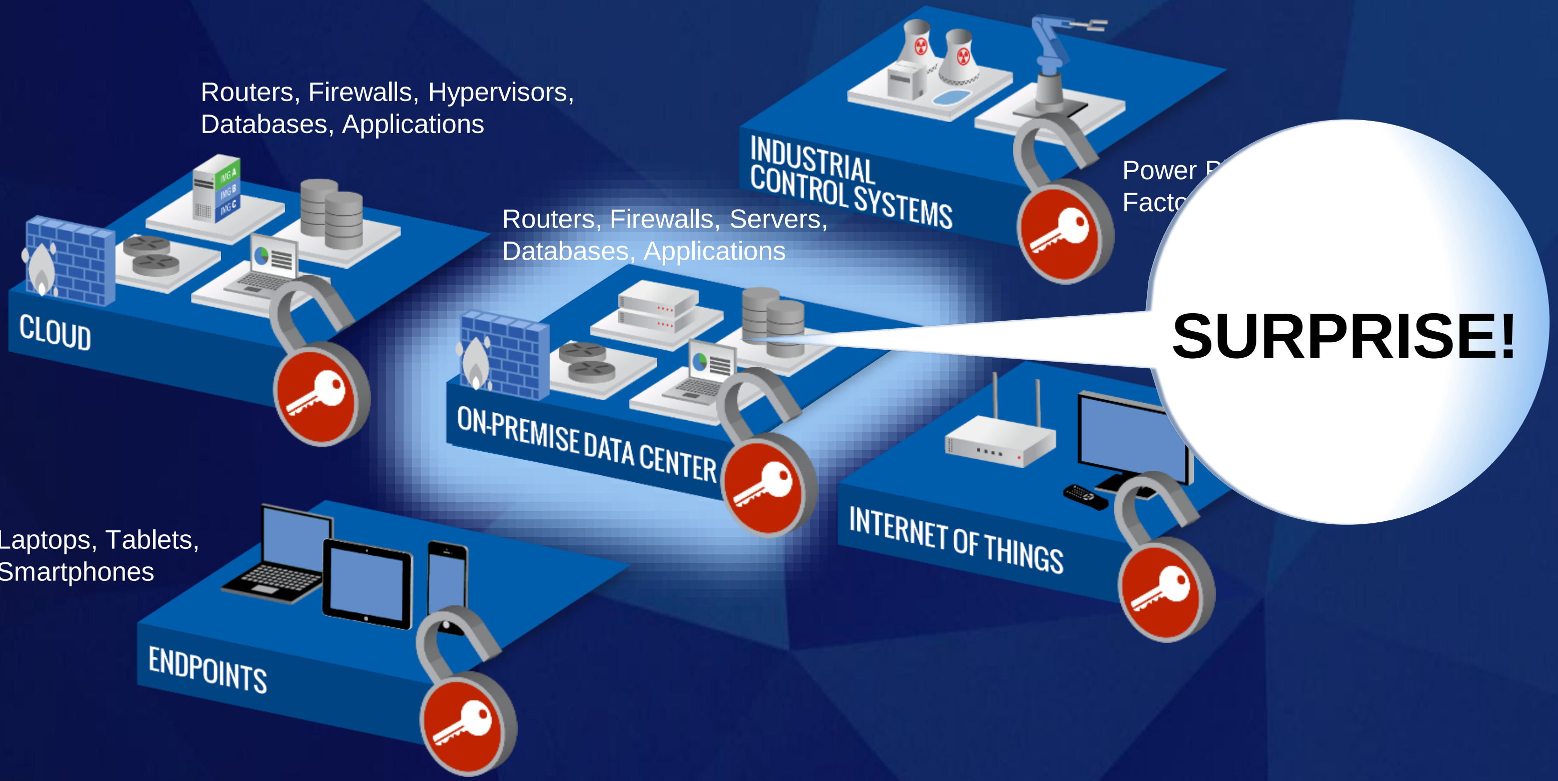
Entra su sli.do
Codice evento
#cpw002

The Innovation Group
Innovating business and organizations through ICT

CYBERARK®

STEP 3:

Remove local admin rights on every layer



Routers, Firewalls, Hypervisors,
Databases, Applications

Routers, Firewalls, Servers,
Databases, Applications

Power P
Facto

Laptops, Tablets,
Smartphones

SURPRISE!

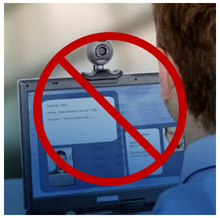
Privileged Access Management

Domanda 2. Avete già provveduto a fornire ai vostri utenti profili con "minori privilegi possibili"?

Entra su sli.do
Codice evento
#cpw002

Okay True, But Without Them, Users Can’t:

Install device drivers like printers, display, network, etc.



Update and install conference and communication tools like GoToMeeting, TeamViewer, Microsoft Lync

Run standard software updates including Adobe, JAVA, Apple, Citrix, etc.

Effectively use development tools such as Microsoft Visual Studio, eclipse, SQL Developer, TOAD, etc.

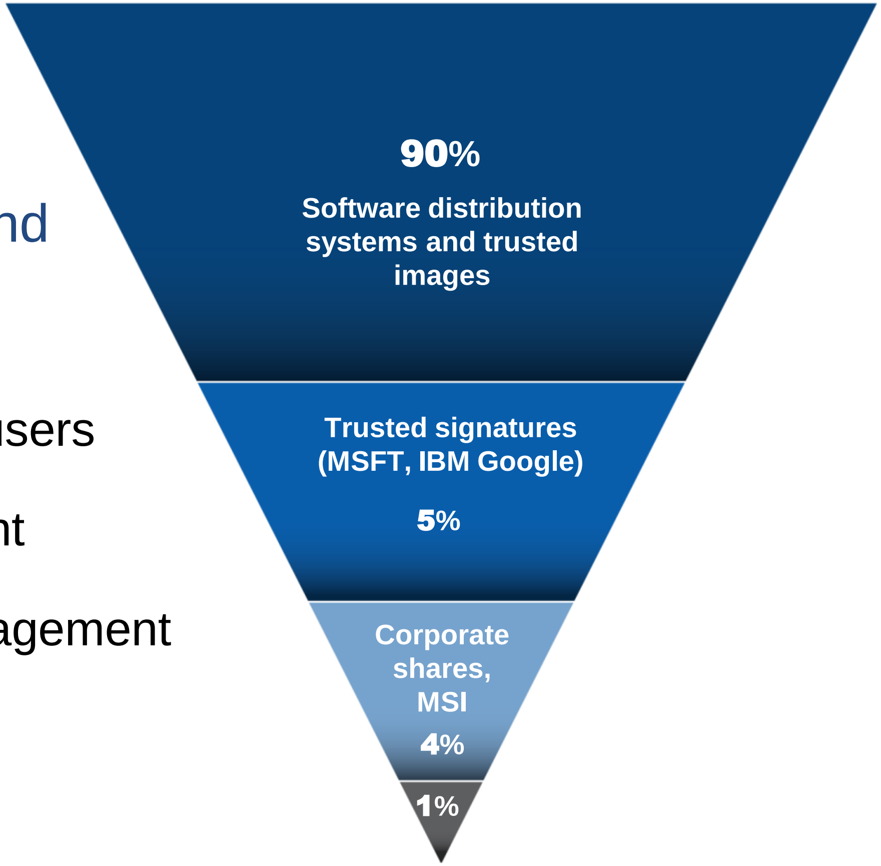
The dilemma – Security VS Operational impact

	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*

Building the concept of "trust"

Trusted Sources:
policies for **over 99%** of applications are created and enforced automatically.

- Non-disruptive to end users
- Streamlined deployment
- Efficient on-going management
- Accurate and reliable



90%

Software distribution systems and trusted images

Trusted signatures (MSFT, IBM Google)

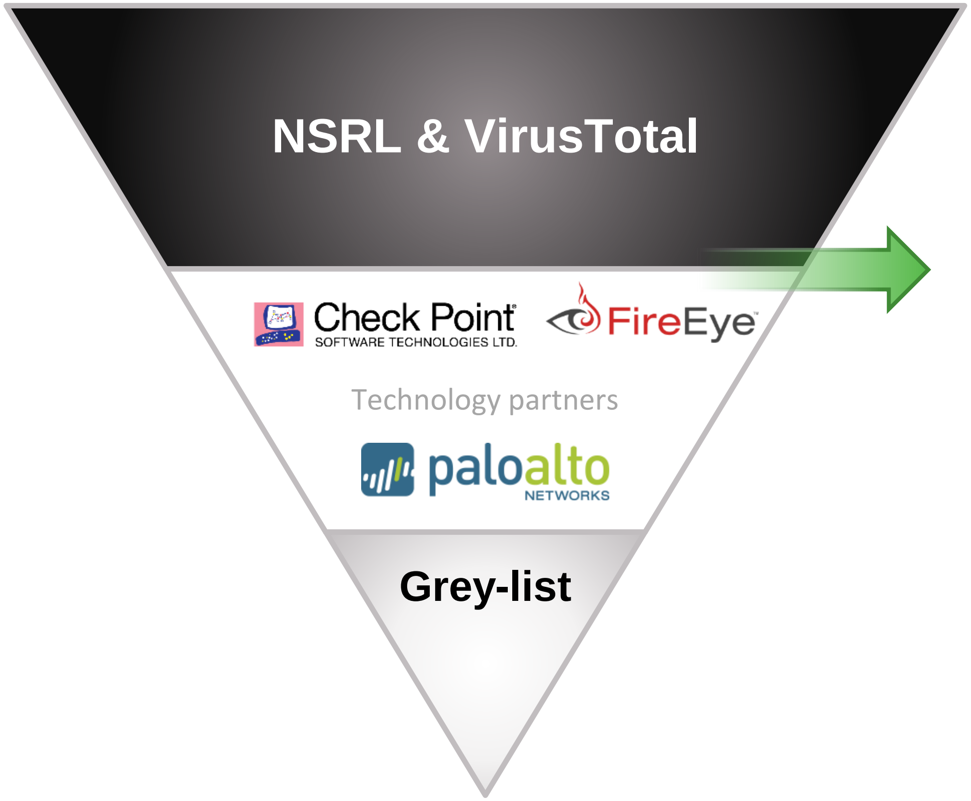
5%

Corporate shares, MSI

4%

1%

What happens to the 1%?



Forensics and Remediation

- Obtain reputation rating
- Block known bad; allow known good
- Identify original source and all known locations of malware
- Block malware propagation and cut access to C&C

…yet we still have a **Grey Area**

STEP 4:

Enforce Application Control

Prevent malicious applications from executing with whitelisting, blacklisting, and ***greylisting***

Windows System
Windows System

Reduce the attack surface

by centrally managing and enforcing application controls

- Block malicious applications from reaching critical servers or executing on workstations
- Detect and block credential theft

Continuously monitor

the installation and execution of applications which are not yet classified

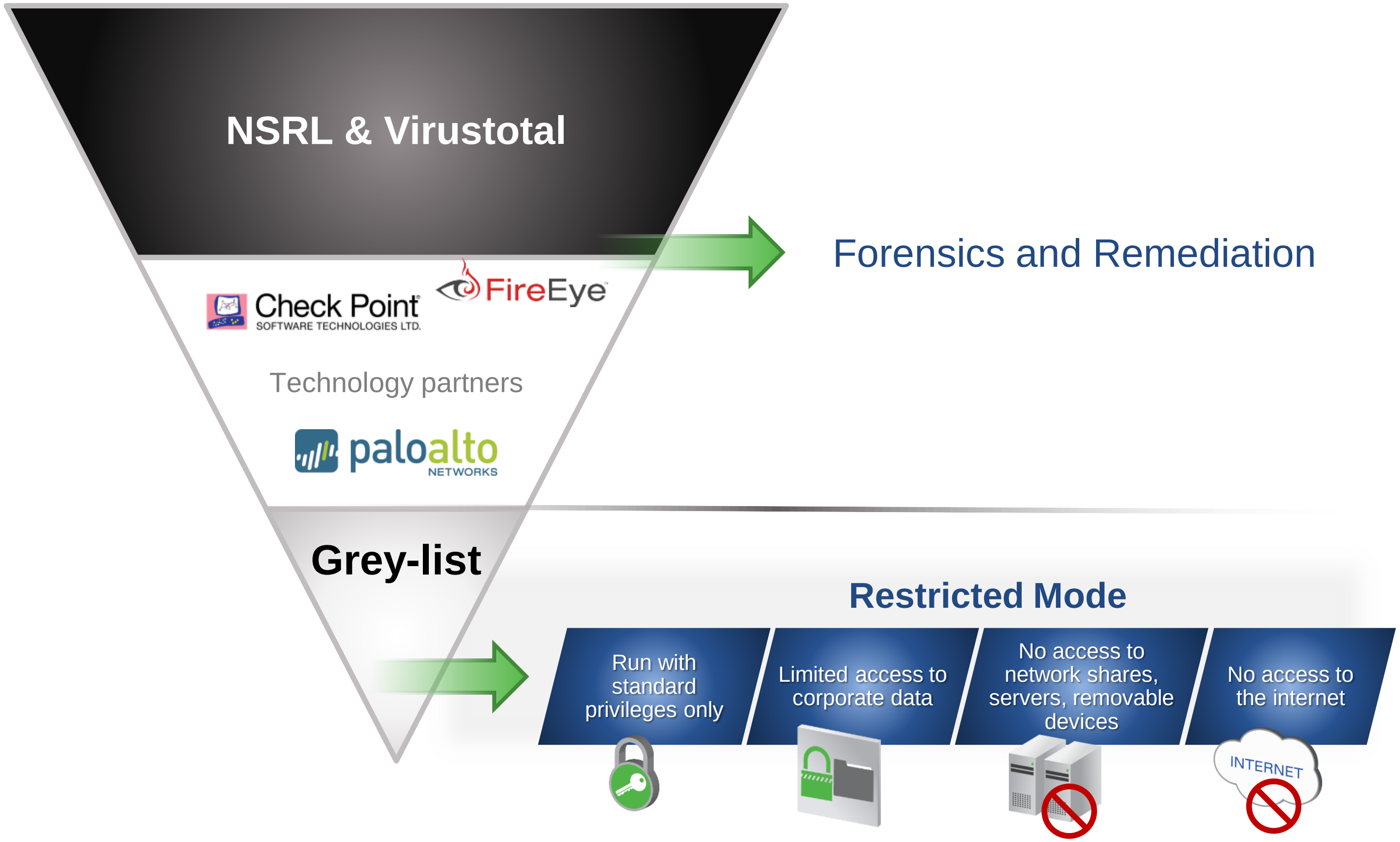
- Enable unknown applications to securely run in restricted mode

Application Control

Domanda 3. Avete già introdotto iniziative di "Application Control" per definire e gestire in modo chiaro quali software sono autorizzati in azienda?

Entra su sli.do
Codice evento
#cpw002

Then Handle Exceptions And Edge Cases



NSRL & Virustotal

Forensics and Remediation

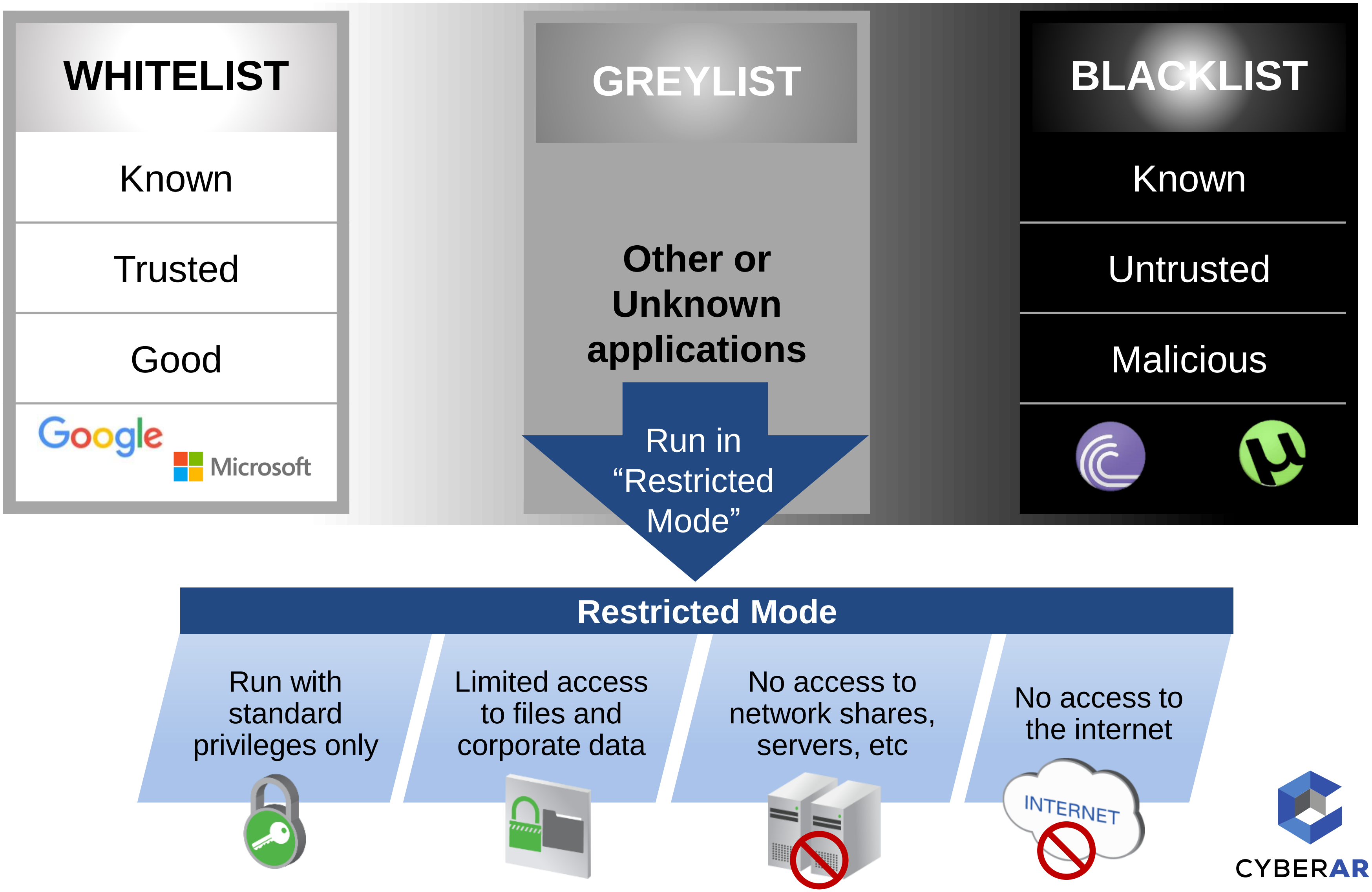
Technology partners

Grey-list

Restricted Mode

- Run with standard privileges only
- Limited access to corporate data
- No access to network shares, servers, removable devices
- No access to the internet

Protection using application control



WHITELIST

Known

Trusted

Good

GREYLIST

Other or Unknown applications

Run in “Restricted Mode”

BLACKLIST

Known

Untrusted

Malicious

Restricted Mode

Run with standard privileges only

Limited access to files and corporate data

No access to network shares, servers, etc

No access to the internet

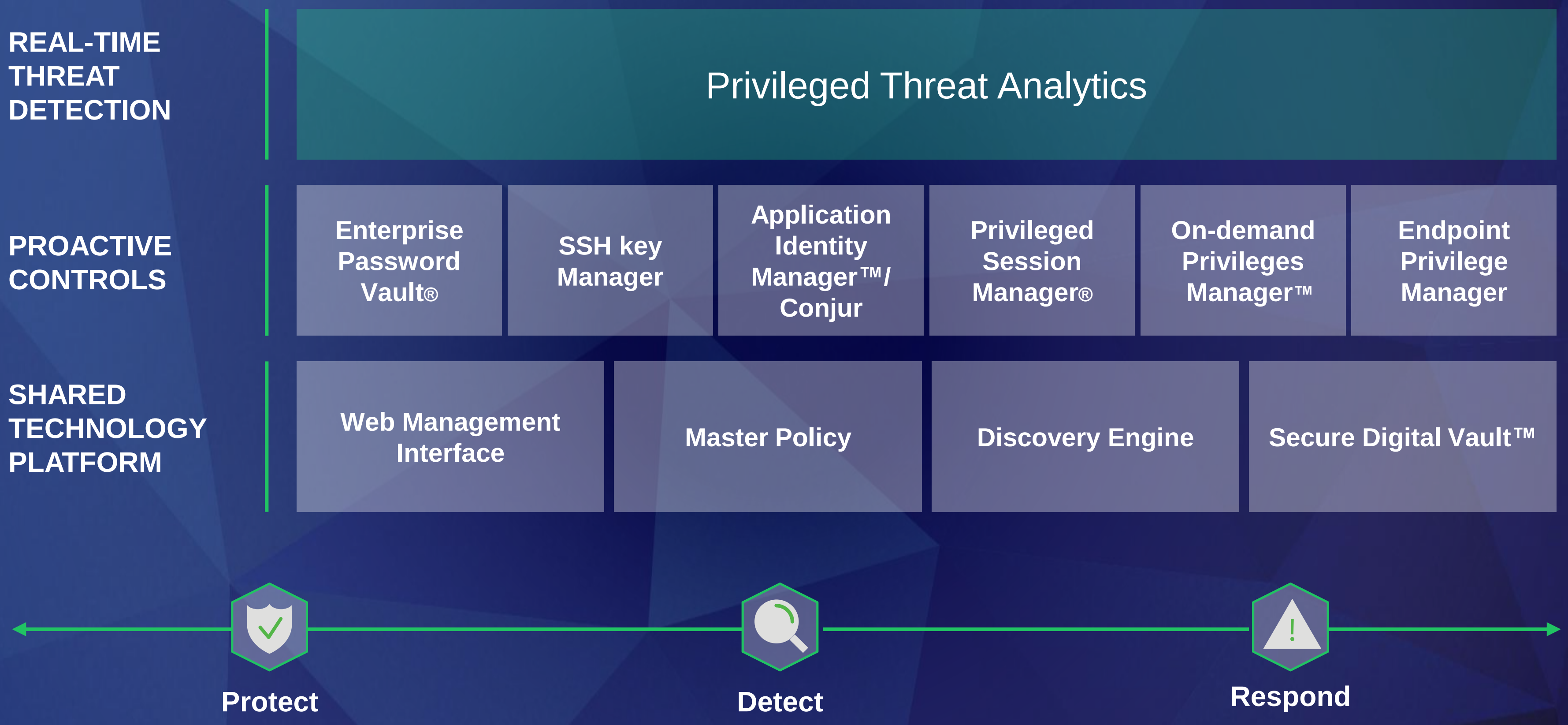
A Note on Credential Theft

Privileged and non-privileged credentials exist all over systems and facilitate lateral movement

Browser Credential Cache	**Flat Files**	**Remote Access Apps**
IT Applications	**Windows Hashes**	**Windows Elements**

Combine password rotation, least privilege, application greylisting, and proactive credential theft detection/blocking!

CyberArk addresses Steps 2 + 3 + 4



REAL-TIME THREAT DETECTION

Privileged Threat Analytics

PROACTIVE CONTROLS

Enterprise Password Vault®

SSH key Manager

Application Identity Manager™/ Conjur

Privileged Session Manager®

On-demand Privileges Manager™

Endpoint Privilege Manager

SHARED TECHNOLOGY PLATFORM

Web Management Interface

Master Policy

Discovery Engine

Secure Digital Vault™

Protect

Detect

Respond

CYBERARK

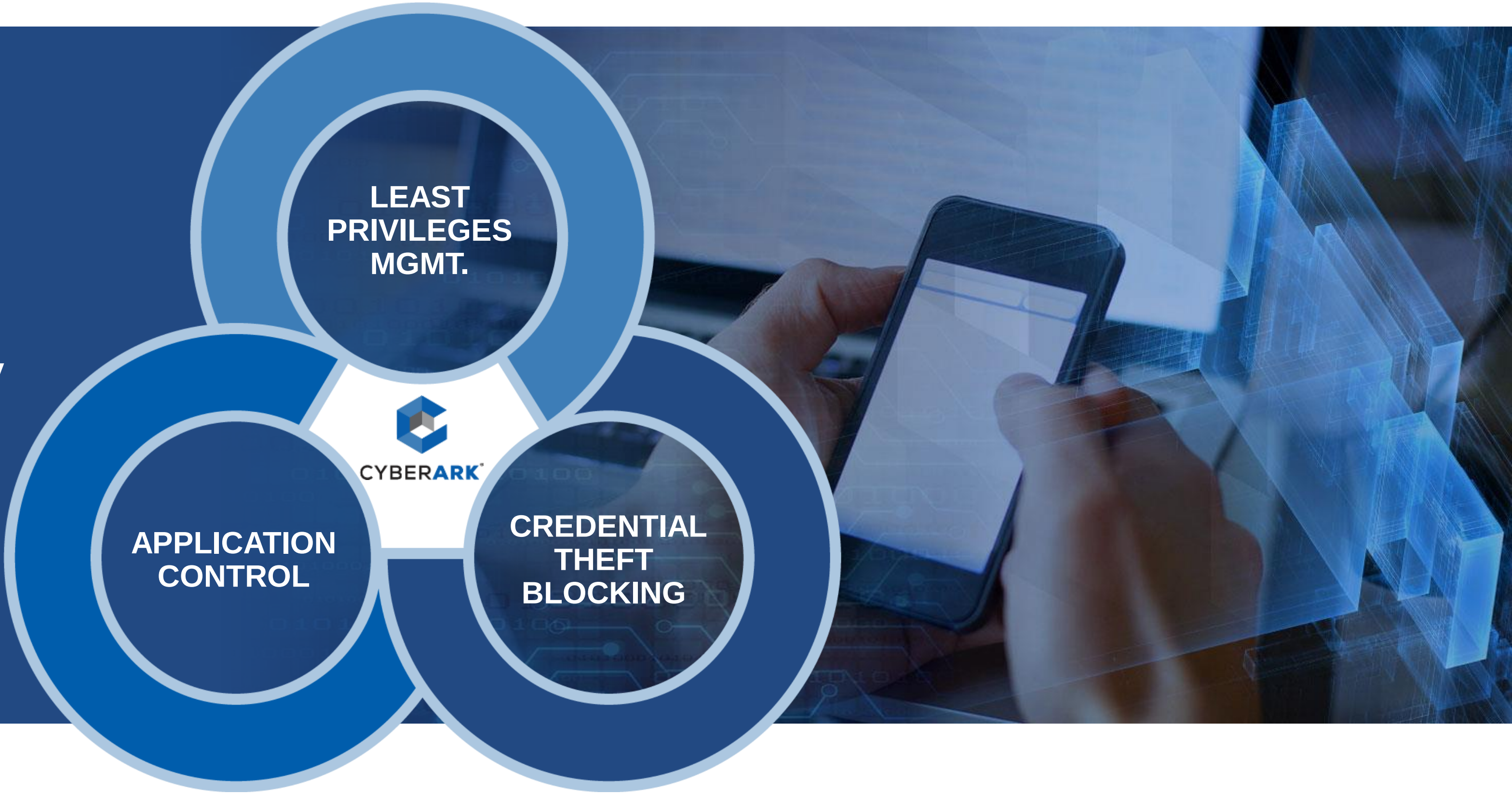
Time for a Demo!

CyberArk Endpoint Privilege Manager

Enables

Privilege Security

on the Endpoint



LEAST PRIVILEGES MGMT.

APPLICATION CONTROL

CREDENTIAL THEFT BLOCKING

CYBERARK

THANK YOU!