



CYBERARK

Targeted Attacks and the Privileged Pivot

Barak Feldman
National Director, CyberArk

Robert Jett
PNW Account Manager, CyberArk



Cyber Attacks: A Daily Event, Overwhelming Coverage

South Korea Blames North Korea for Cyber Attack

By Adario Strange | April 10, 2013 10:15am EST | 1 Comment



Last month's mysterious cyber attack that cut off banks and television stations in South Korea was executed by North Korea's intelligence agency, according to official investigators based in Seoul.

The findings were revealed in the *Korea Herald* today as South Korea's Ministry of Science, Information and Communications Technology (information communications technology) and the Future Planning connected the attacks to North Korea's Reconnaissance General Bureau.

On March 20, the computer systems of local Korean television stations KBS, YTN, and MBC were

theguardian

News | US | World | Sports | Comment | Culture | Business | More

News > World news > The NSA files

Edward Snowden NSA files: secret surveillance and our revelations so far

Leaked National Security Agency documents have led to several hundred Guardian stories on electronic privacy and the state

FAST FEED

CHINESE HACKERS TARGET NEW YORK TIMES IN FOUR-MONTH CYBERATTACK

THE CYBERATTACKS DATE BACK TO WHEN THE NEWSPAPER PUBLISHED AN EXPOSE DETAILING THE WEALTH ACCUMULATED BY THE PREVIOUS CHINESE PREMIER, WEN JIABAO.

BY: ADDY DUGDALE



Topic: Security



Follow via: RSS, Email

Swiss spy agency warns CIA, MI6 over 'massive' secret data theft

Summary: Switzerland's national security agency warns that a huge amount of secret, counter-terrorist data may have been leaked by no other than a disgruntled 'administrator-level' employee.



By Zack Whittaker for Zero Day | December 4, 2012 -- 13:58 GMT (05:58 PST)

Follow @zackwhittaker

Secret counter-terrorism information shared by foreign governments, which may not be limited to the U.K. and U.S. administrations, is thought to have been stolen by a senior IT employee of Switzerland's state intelligence service.

First reported by the *Reuters* news agency, the U.S.' Central Intelligence Agency (CIA) and the U.K.'s Secret Intelligence Agency (MI6), have been warned that data they shared may no longer be just in

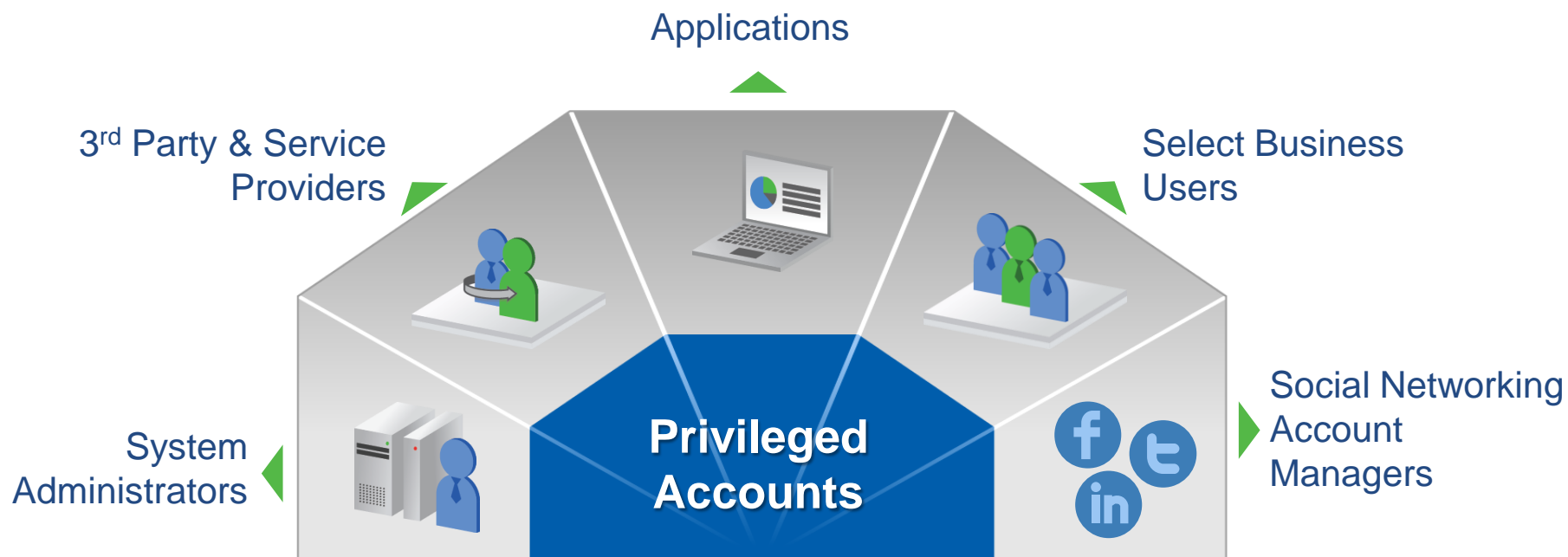


CYBERARK

**Regardless of where they
started, they all became
insiders!**

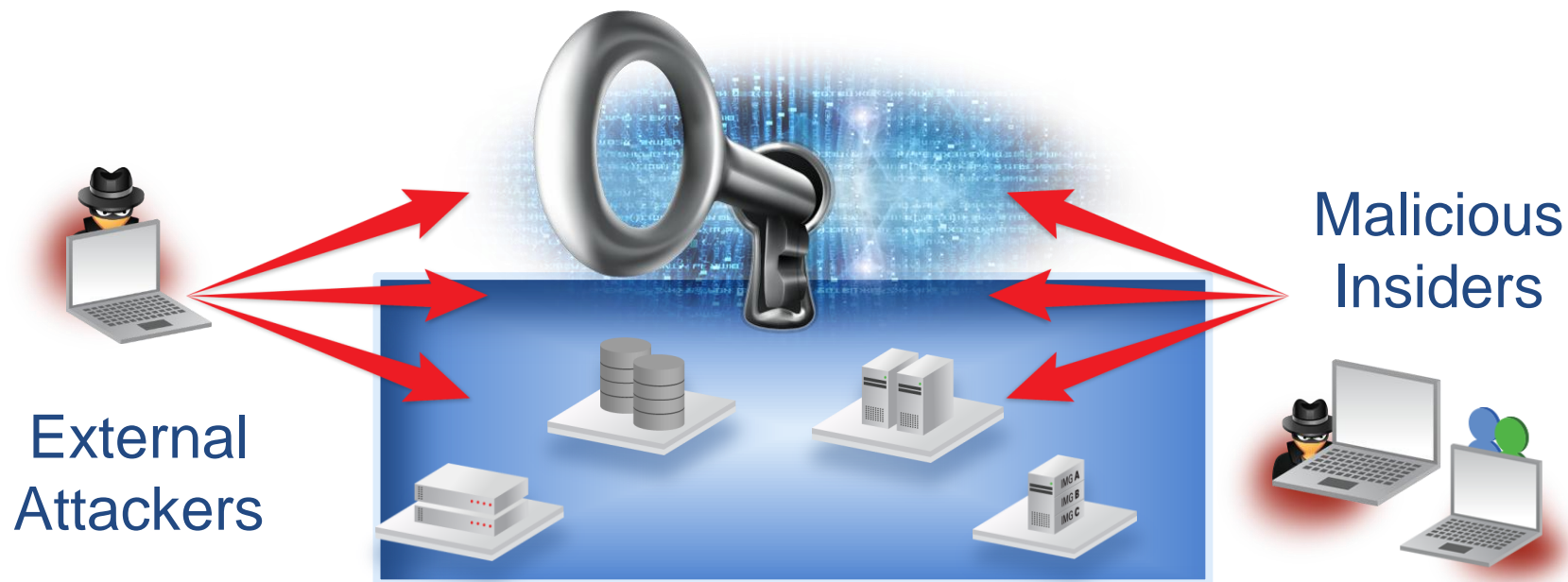


Privileged Accounts Create a Huge Attack Surface



- Privileged accounts exist in every connected device, database, application, industrial controller and more!
- Typically a ~3X ratio of privileged accounts to employees

The One Thing Attackers Need to Succeed!



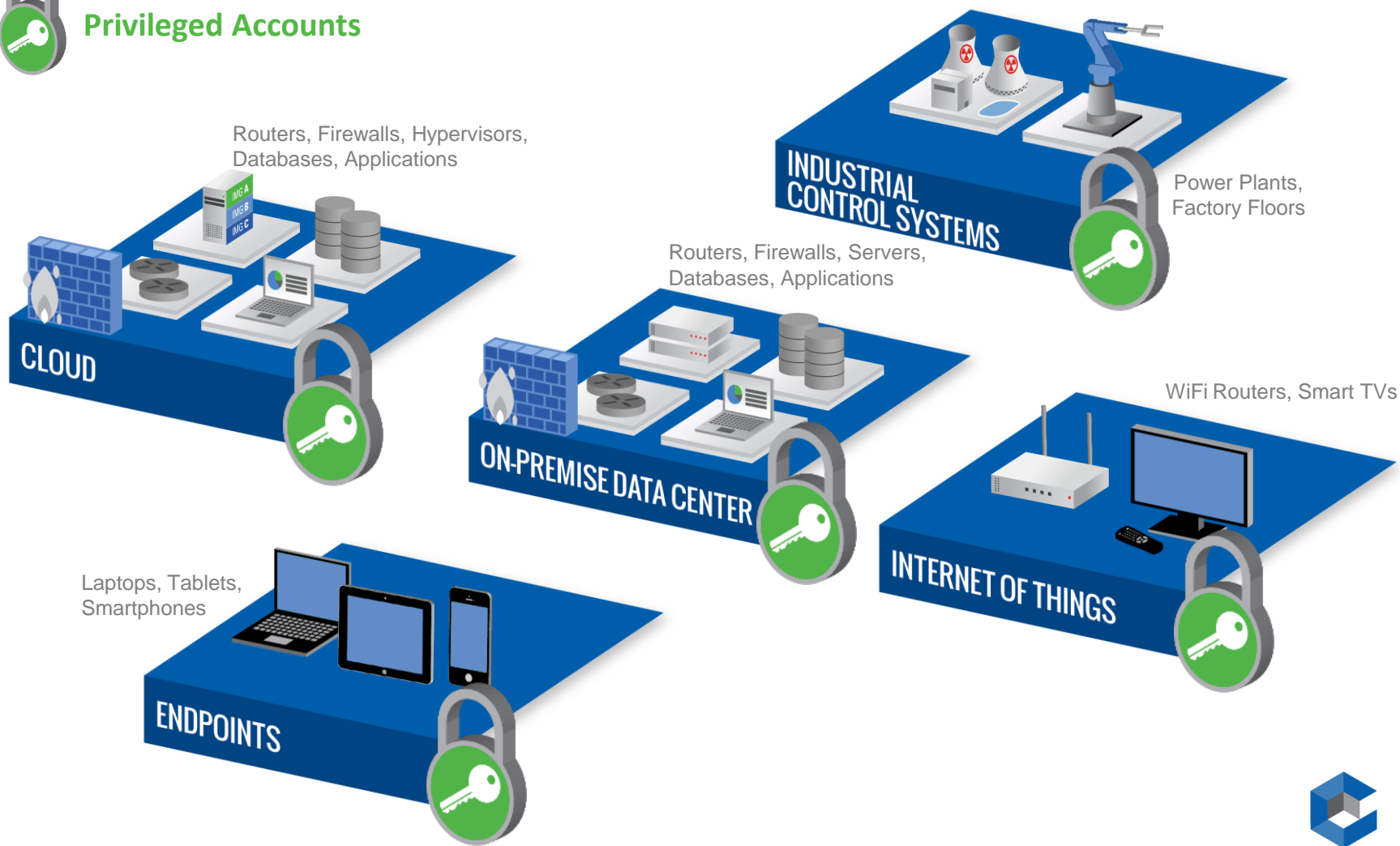
Privileged Accounts – “Keys to the IT Kingdom”



Privileged Credentials are Everywhere



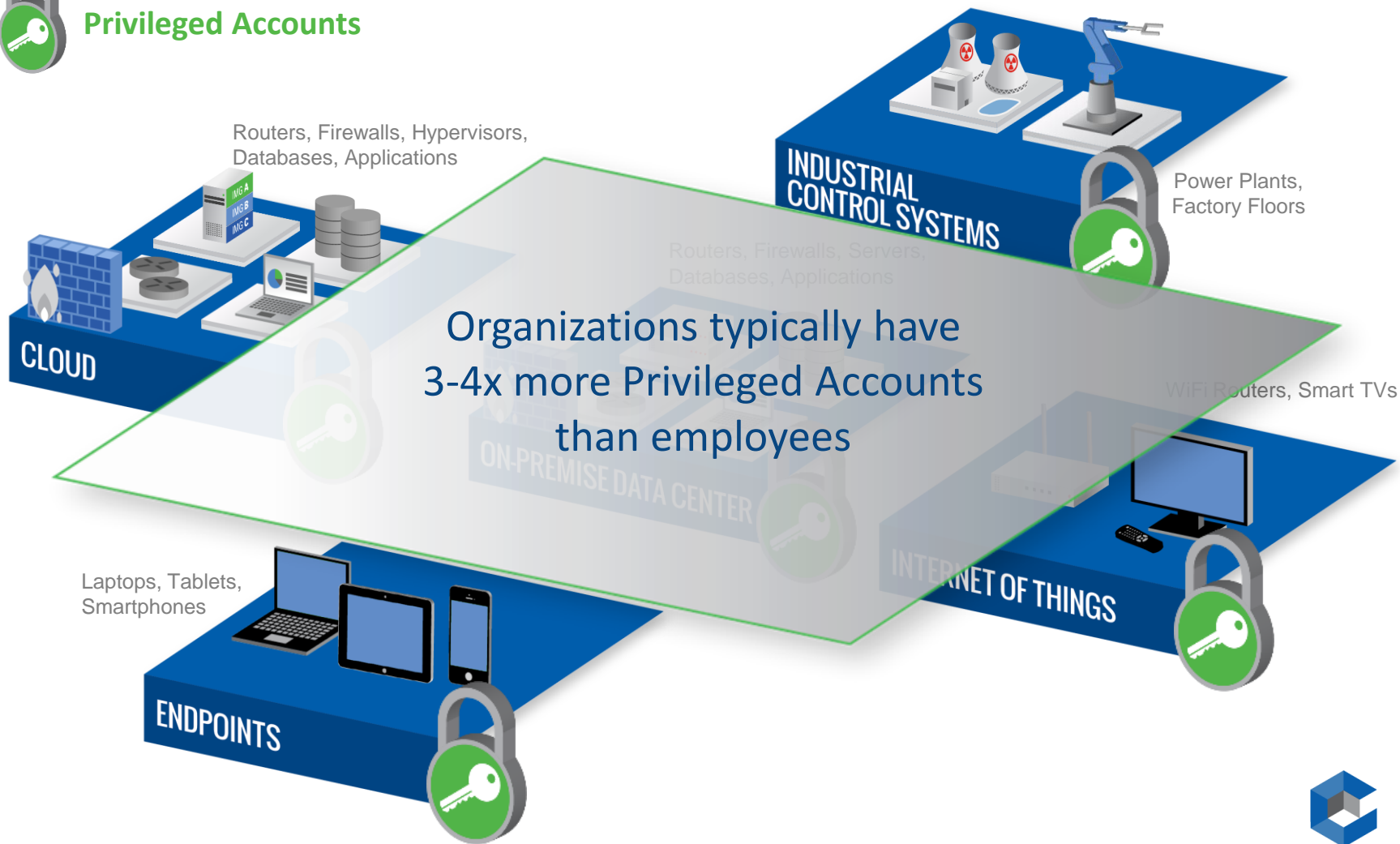
Privileged Accounts



Privileged Credentials are Everywhere



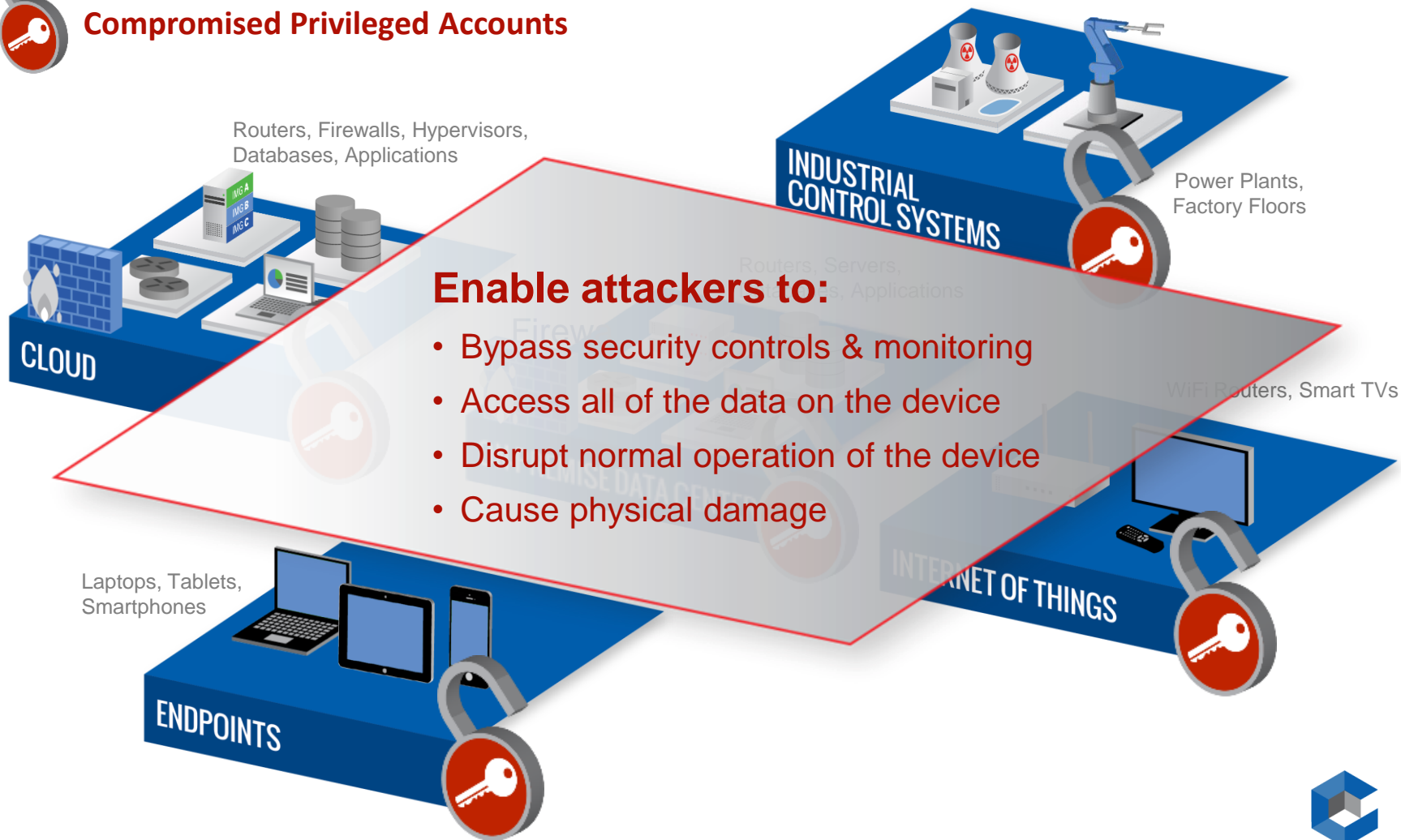
Privileged Accounts



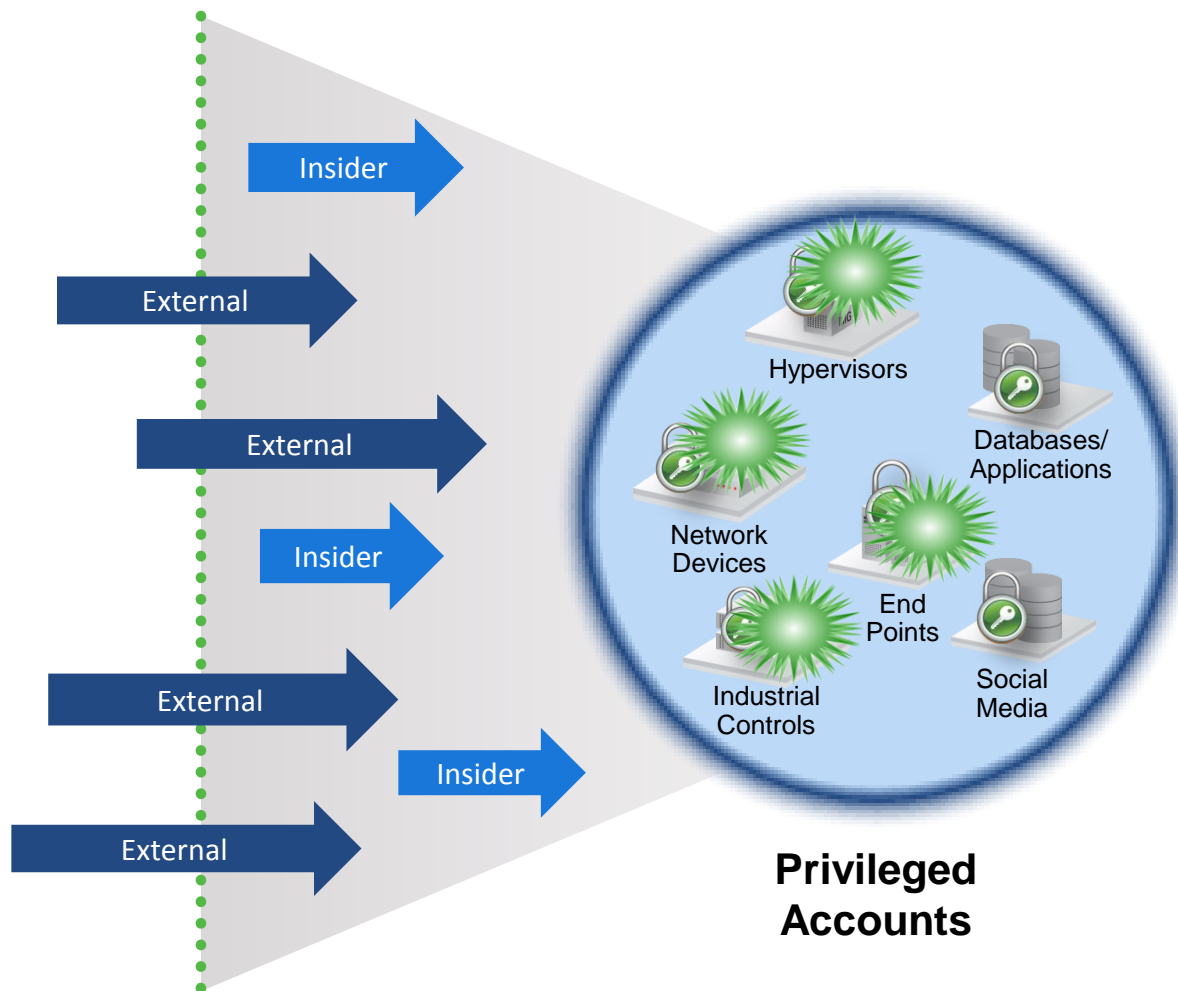
Hijacked Credentials Put the Attacker in Control



Compromised Privileged Accounts



Proactive Protection, Detection & Response



Proactive protection

- Only authorized users
- Individual accountability
- Limit scope of privilege

Targeted detection

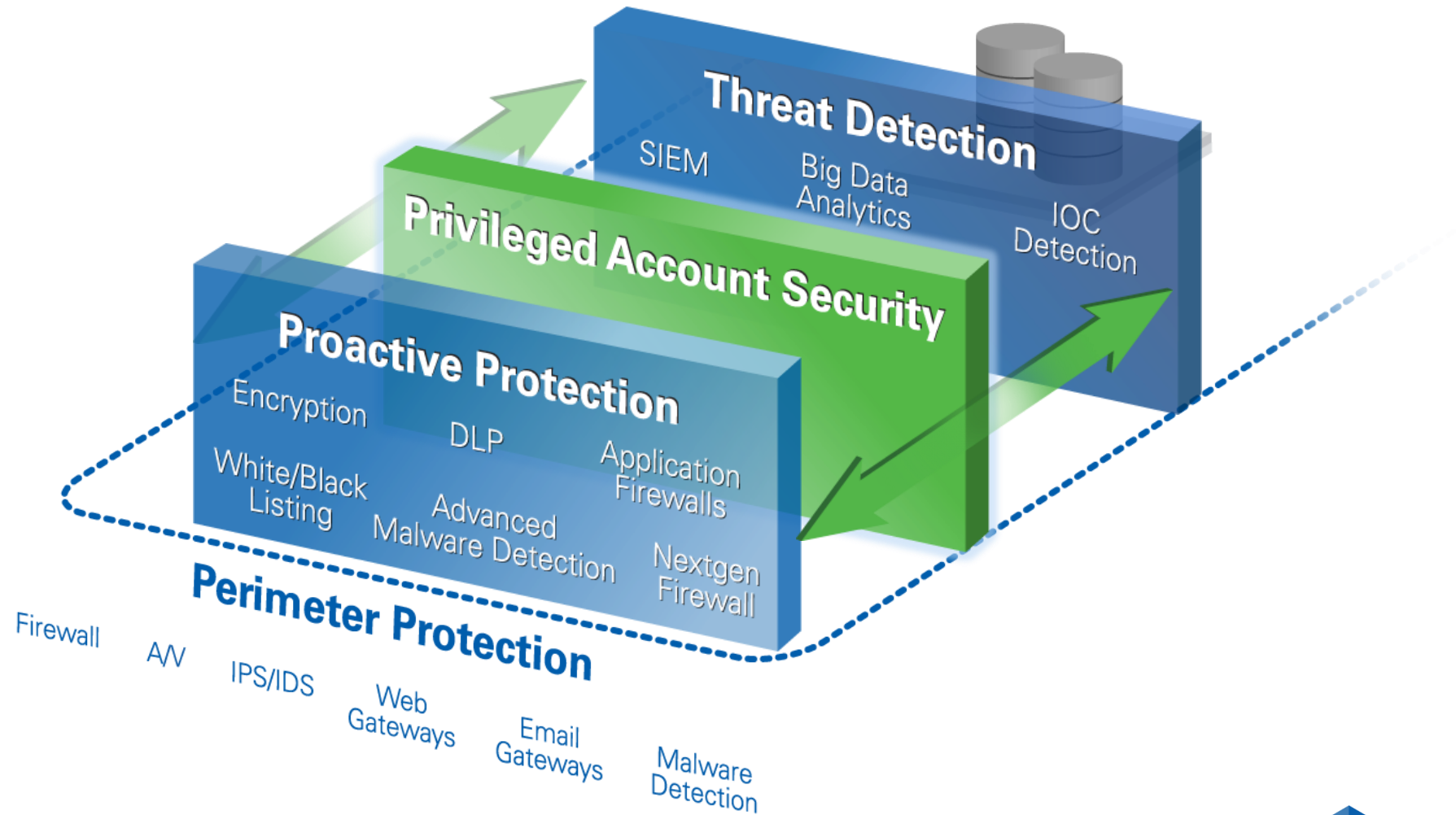
- Continuous monitoring
- Malicious behavior
- High risk behavior
- Alerting

Real-time response

- Session termination
- Full forensics record of activity



Privileged Account Security – Now a Critical Security Layer



Solving The Privileged Account Security Problem

Threats

- Advanced Threat
- Insider Threats
- Securing the Hybrid Cloud
- Securing Application Credentials
- Securing Shared Admin Accounts
- Sharing Sensitive Information

Audit & Compliance

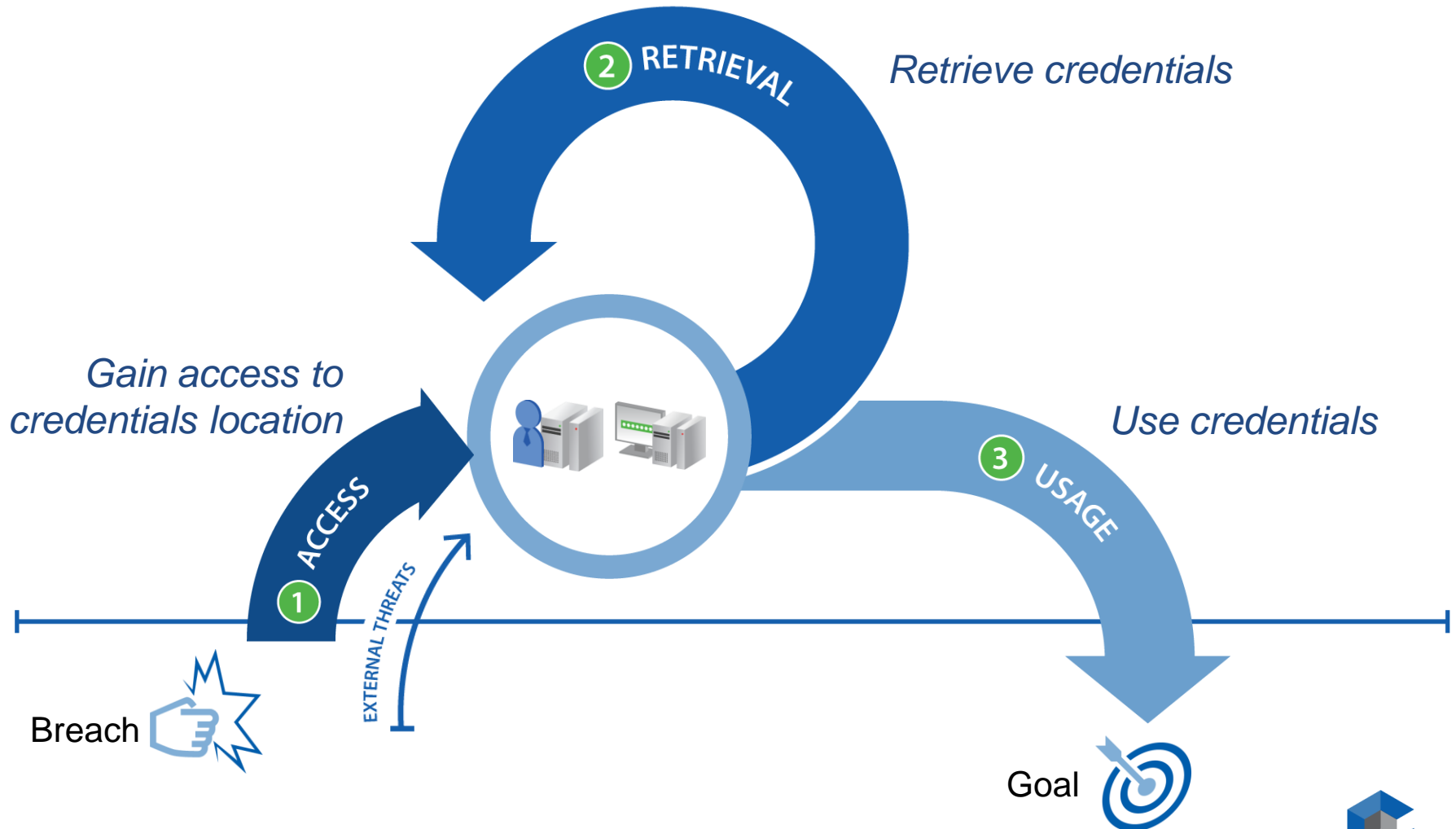
- Control & Accountability for Privileged Users
- Monitor & Record Privileged Activity
- Compliance Reporting
- Remote User Access Control
- Auditing Secure File Transfer

Industrial Controls/SCADA

- Securing and Monitoring Shared Admin Accounts for ICS Systems
- Controlling and Monitoring Remote Vendors
- Smart Grid Security



The Privilege Escalation Cycle



Primary Recommendations

Restrict Lateral Movement

- Assign a UNIQUE password on every endpoint for built-ins
- Establish Credential Boundaries on Domain; One-Time Passwords

Isolate High Value Assets

- Ensure users can not access sensitive assets directly from their endpoint
- Do not allow users or their machines to know a password (keyloggers, malware, etc.)

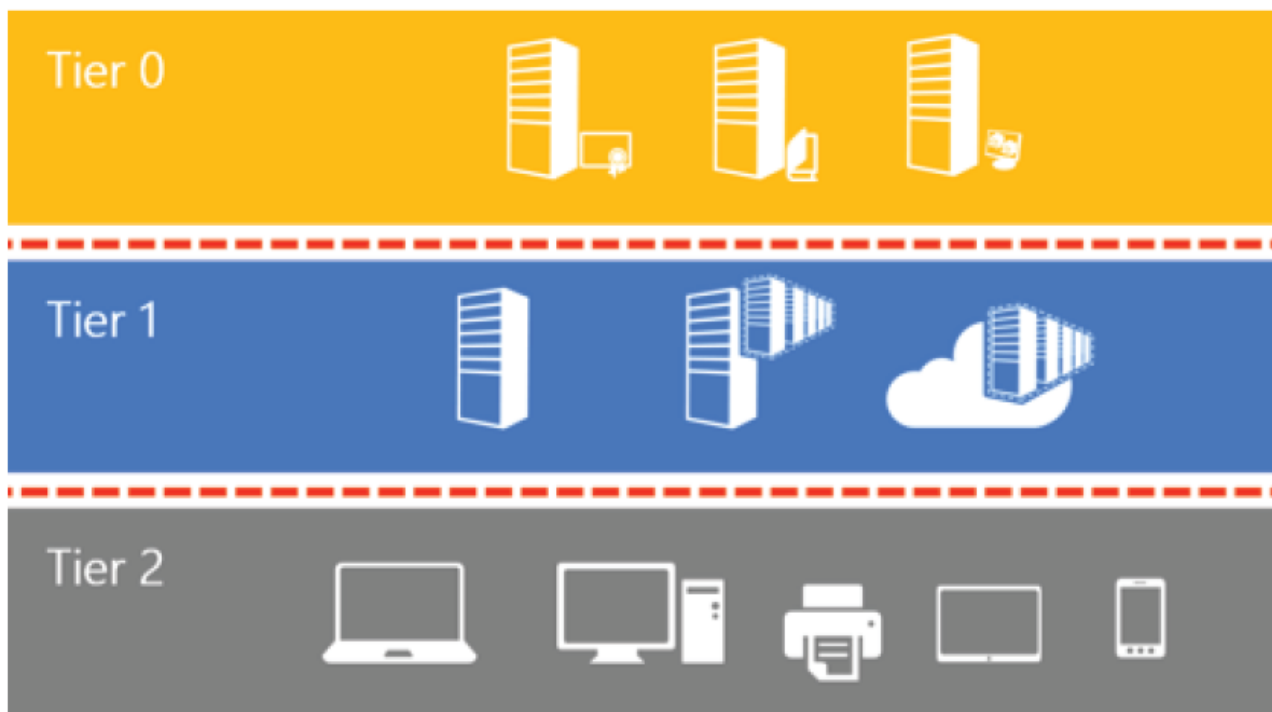
Monitor Behavior

- Look for changes in behavior for common privileged accounts and sensitive assets, especially indicators of credential theft
- Enable reactive countermeasures



Credential Boundaries

**See MSFT Whitepaper: Mitigating Pass the Hash Attacks and Other Credential Theft Version 2*



Tier 0 – Forest admins: Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers

Tier 1 – Server admins: Direct or indirect administrative control over a single or multiple servers

Tier 2 – Workstation Admins: Direct or indirect administrative control over a single or multiple devices

Strategic Best Practices Summary

Session Recording & Desktop Isolation

- Isolate High value assets and create a new layer of security using proxy server.
- Leverage Universal connectors and native access to enforce PIV cards and role based accounts.
- Record all privileged activity without the use of an agent

Password Management

- Change passwords to built-in accounts to a unique value per end point
- Frequently change passwords to minimize the risk of credential (hash) theft

Privileged Analytics and Anomalies

- Watch for anomalous behavior of privileged accounts and bypass of controls to limit and stop events in progress.

Least Privilege Access and App Controls

- Reduce a large number of privileged users from desktops and servers by using a least privileged escalation model in Windows desktops/Servers and Unix/Linux.



What to do now – Getting Started

Identify

- Run free assessment tools to find out where privileged accounts exist and how they are being used/misused

Change

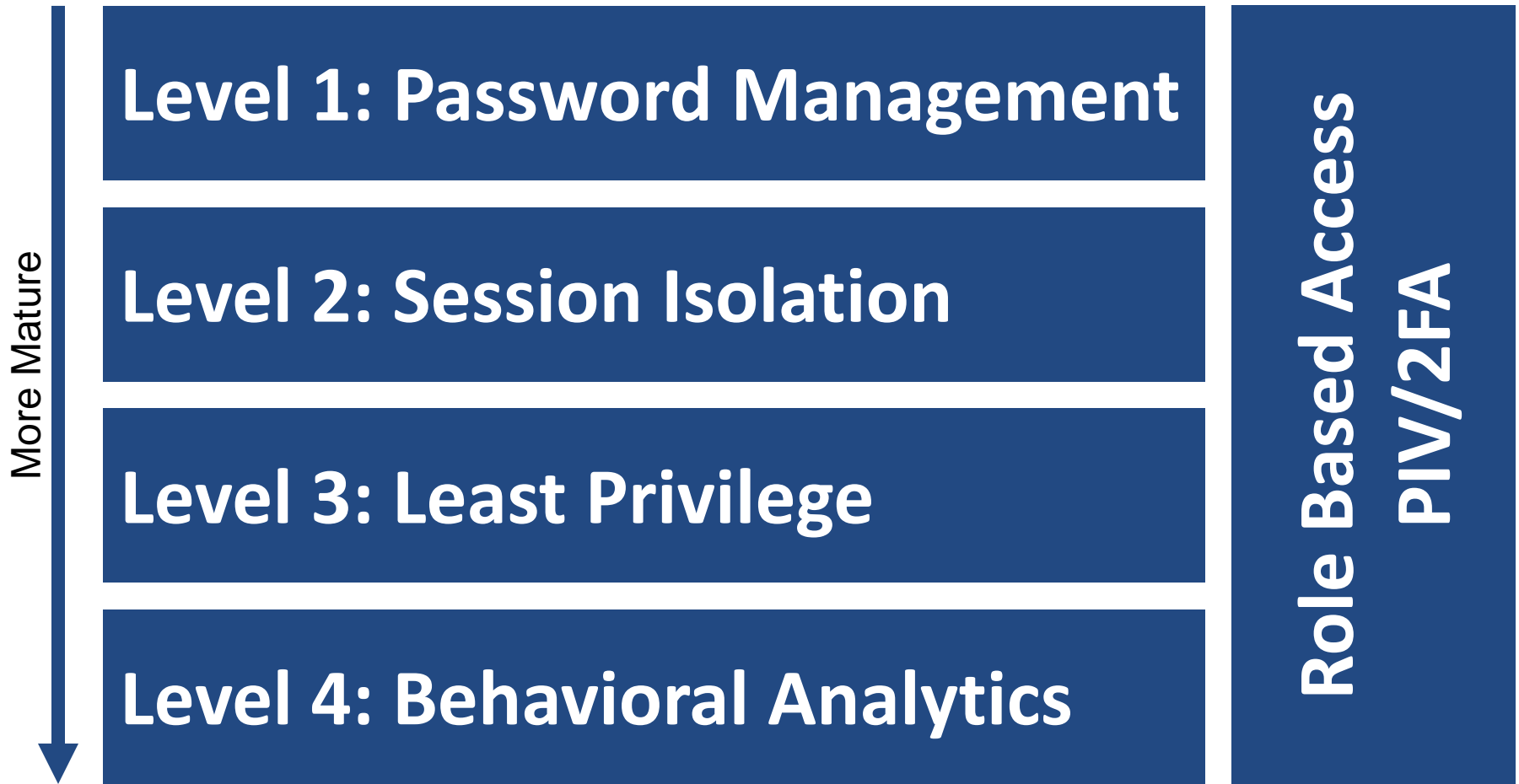
- Identify top 3-5 data center technologies and high Value assets and Isolate and change the built-in backdoor ids on each to a unique random password

Isolate

- Identify what systems/information an 'attacker' would target and assign priority
- Prevent end users from accessing these devices directly moving forward and do not disclose passwords



CyberArk Maturity Model – Levels of Control



Primary Recommendations

Reduce Attack Surface

Establish Role based access and Least Privilege Models

Randomize Built-in Backdoor Admin Passwords

Isolate Passwords of Critical Assets

Lateral Movement

Monitor Privileged Behavior

Credential Theft

Enterprise Password Vault (EPV) and Viewfinity (OPM)

Privileged Session Manager (PSM)

Privileged Threat Analytics (PTA)

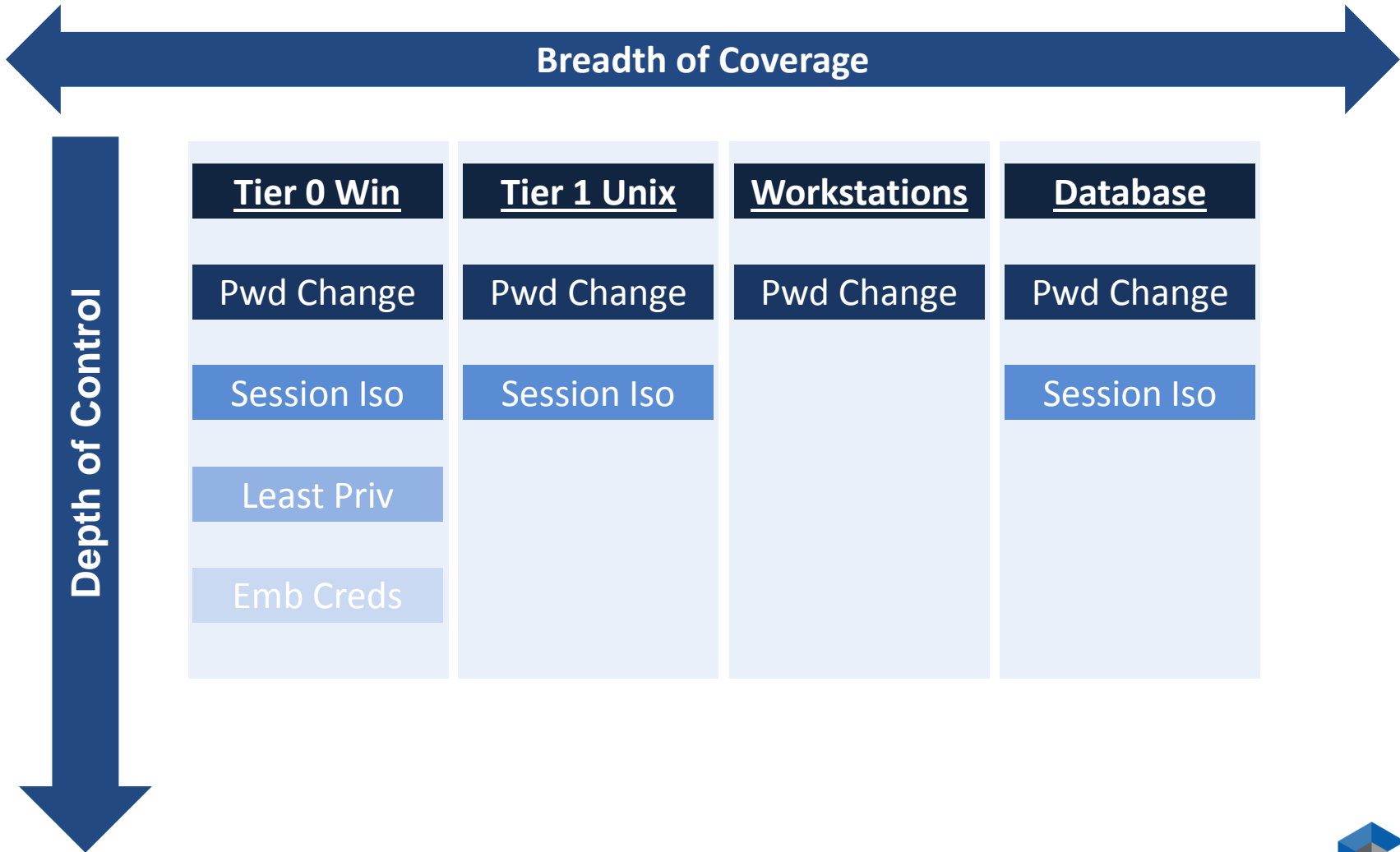




CYBERARK

Extra Slides

How to Measure Success – Wide & Deep



As defenses evolve, attackers adapt and innovate. In 2014 we observed new and emerging techniques at each stage of the attack lifecycle. These are a few highlights.

Hiding Webshells

Attackers continued to use novel techniques to deploy and hide web-based malware. Mandiant saw several stealthy techniques, including the following:

- Shells planted on servers that used SSL encryption to evade network monitoring
- Single-line “eval” shells embedded in legitimate web pages
- Server configuration files that were modified to load malicious DLLs

Hijacking the VPN

Mandiant witnessed more cases in which attackers successfully gained access to victims’ VPNs than in any prior year.

Leveraging WMI and PowerShell
Attackers increasing WMI and PowerShell powerful built-in components of Windows, to maintain access, gather data, and move laterally.

Malicious Security Packages

Attackers took advantage of Windows security package extensibility to load backdoors and password loggers.

Maintain Presence

Move Laterally



Plaintext Passwords

Attackers used recompiled variants of the Mimikatz utility to steal plaintext passwords from memory while evading anti-virus detection.

Kerberos Attacks

After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.

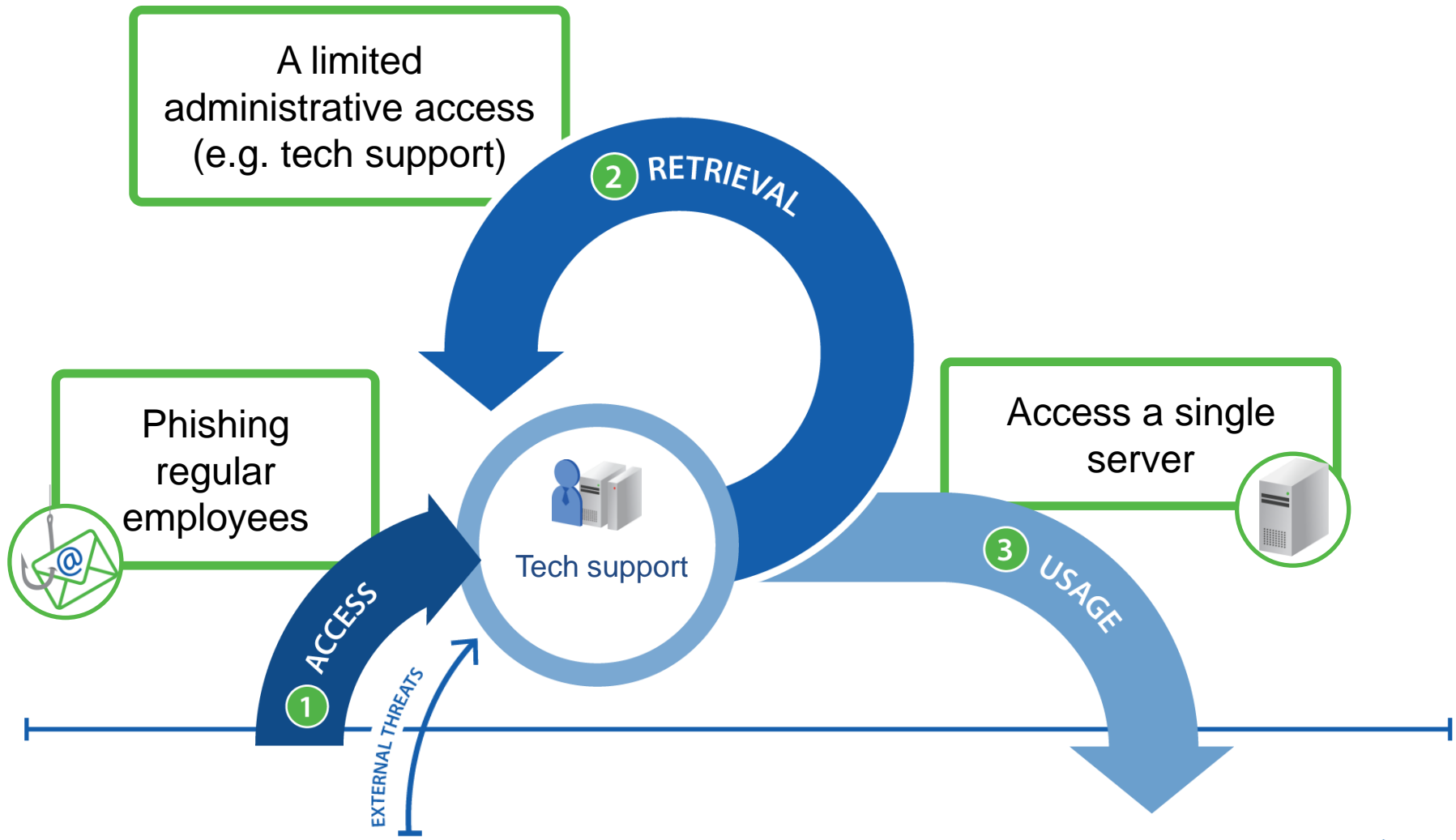




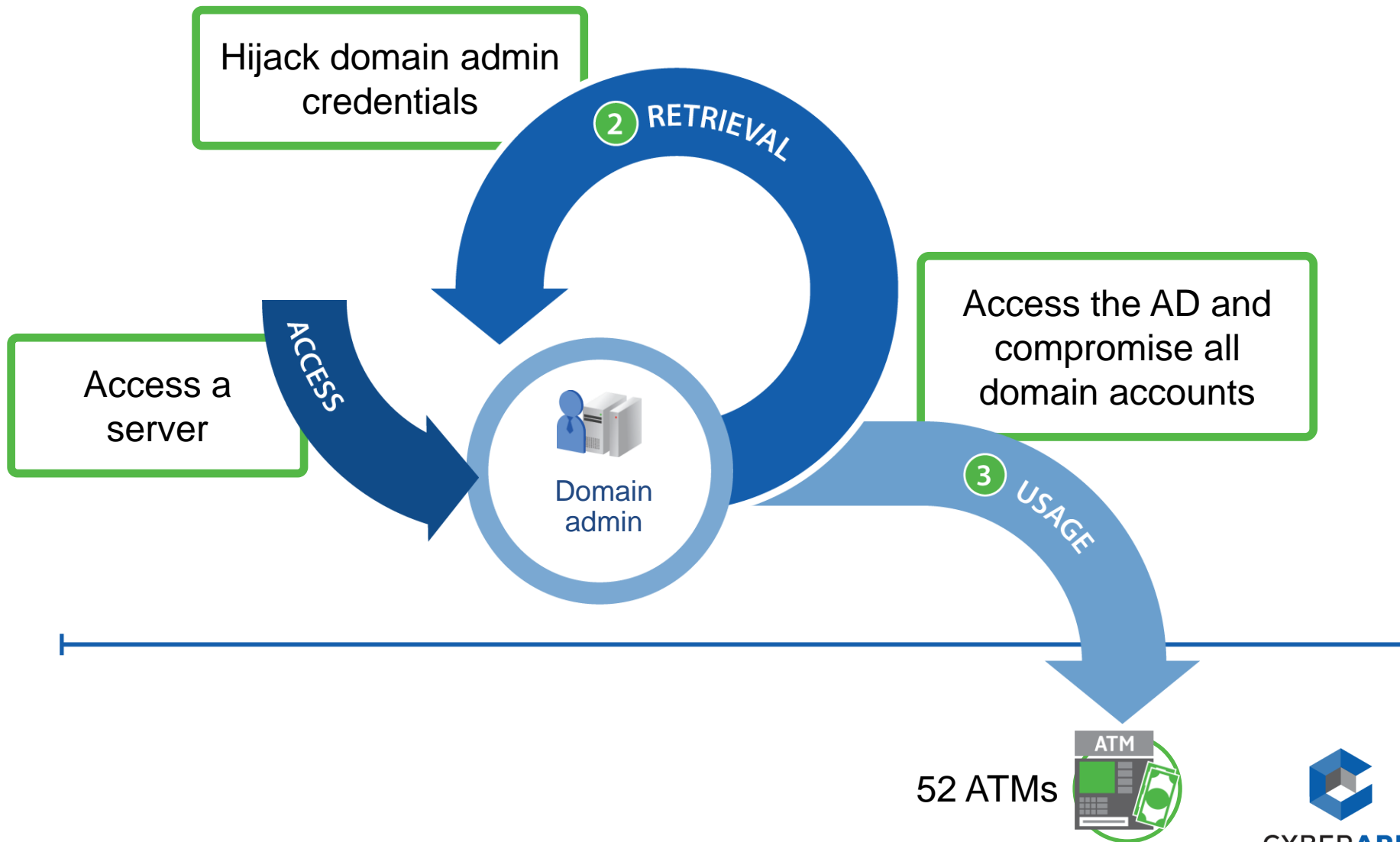
CYBERARK

The Anunak/Carbanak Attacks

The Anunak/Carbanak Attacks



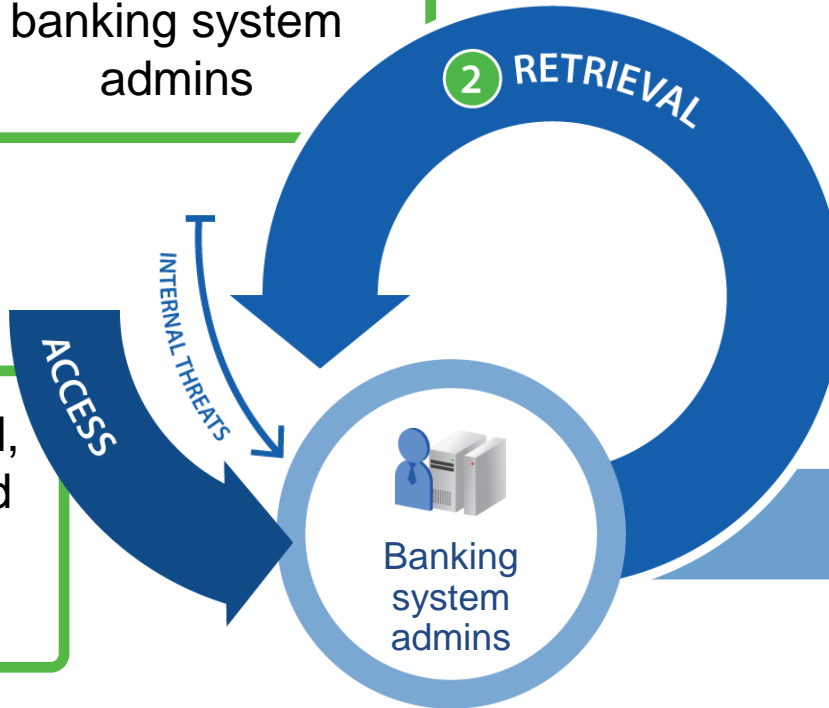
The Anunak/Carbanak Attacks



The Anunak/Carbanak Attacks

Hijack credentials of banking system admins

Access email, workflow and banking servers



- Install software to monitor activity (photo, video, etc.)
- Enable remote access to servers

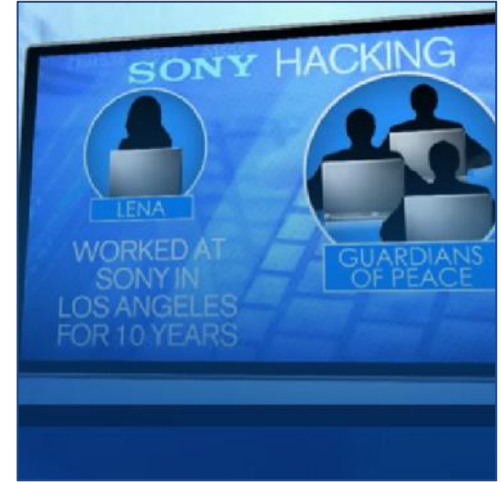
Transactions:

- Bank accounts
- E-currency
- Mobile prepaids



CYBERARK

Who are the attackers?



Does attribution help mitigation?



CYBERARK

CyberArk Contacts:

Rob Jett

Robert.jett@cyberark.com

(510) 717-9910

Barak Feldman

Barak.Feldman@cyberark.com