



**CYBERARK®**

## **WHERE TO START?**

**30 DAY SPRINT - BUILDING A FRAMEWORK TO SUCCESS**

Elliot Wood – Senior Technical Advisor

June 2018

# SESSION OBJECTIVES

## WHY ARE WE HERE TODAY?

- Overview of common tactics in advanced attacks
- Explain the privilege pathway
- Recommend four controls to reduce risk
- Outline a methodology for rapidly implementation

## CIO Journal.

### Malware Targets Vulnerable Admin Accounts

Many a CIO has warned employees about malicious e-mail that potentially gives hackers an entry into corporate networks. Increasingly, sophisticated cyber attacks are using so-called privileged accounts.

## SECURITYWEEK

### Privileged Accounts Play Key Role in Advanced Cyber Attacks

Malware and data breaches are increasing the return on investment for attackers. Privileged accounts are part of multi-stage operations where they breach networks, gather information, and exfiltrate data.



### Privileged Account Details Are Often Sensitive and Can Be a New Entry Point for Attackers

Privileged user accounts can be a way for attackers to infiltrate a network.



### Privileged Accounts at Root of Most Data Breaches

If enterprises ever were given wake-up call, it should be this: stealing and exploiting privileged accounts is the most common cause of data breaches.

### Dark Reading

### Watch the Watchers: Trusted Employees Can Do Damage

### Privileged Account: The Master Keys Hackers Know Best

One big reason cyberintruders can easily roam far and wide, once they crack inside a company network, is that many organizations pay scant heed to privileged accounts.



## Grasping the Problem with Privileged Accounts

Many in the security industry tend to focus on authentication strength a

## The New York Times

### Attack Gains Access to U.S. Systems

By DAVID E. SANGER, NICOLE PERLOTH and MICHAEL D. SHEAR JUNE 30, 2015



England + Add to myFT

### England's NHS hit by large scale cyber attack

6 HOURS AGO by: Financial Times

England's National Health Service has been hit by a large scale cyber attack, with hospitals across the country reporting IT systems are down.



### Privilege Comes with Peril in World of Cybersecurity

Security experts have been warning enterprises for some time that the greatest security threats come from within: their own employees. And that message has apparently

## Uber Hack Shows Vulnerability of Software Code-Sharing Services

By Jeremy Kahn

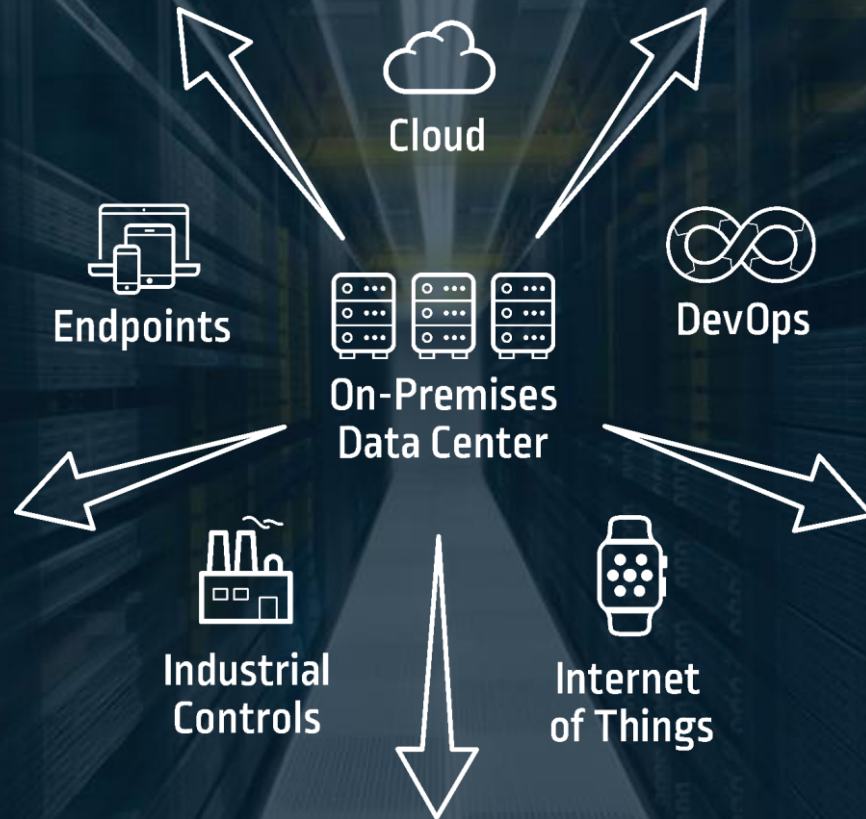
Cyber-Safe

Every single Yahoo account was hacked - 3 billion in all

by Selena Larson @selenalarsen October 4, 2017 8:30 AM

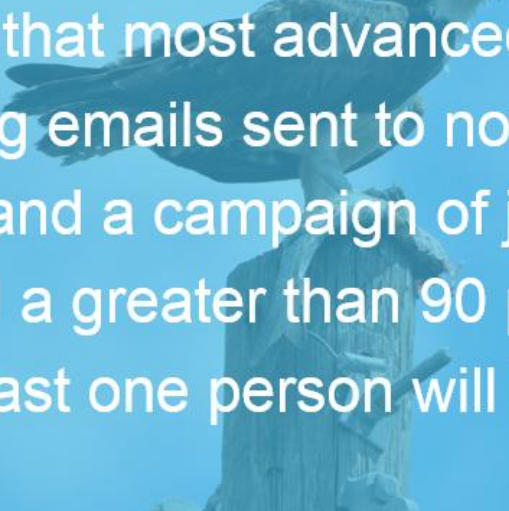
## "WannaCry" ransomware attack losses could reach \$4 billion

# THE ATTACK SURFACE CONTINUES TO GROW



## CYBER ATTACKS TYPICALLY START WITH PHISHING

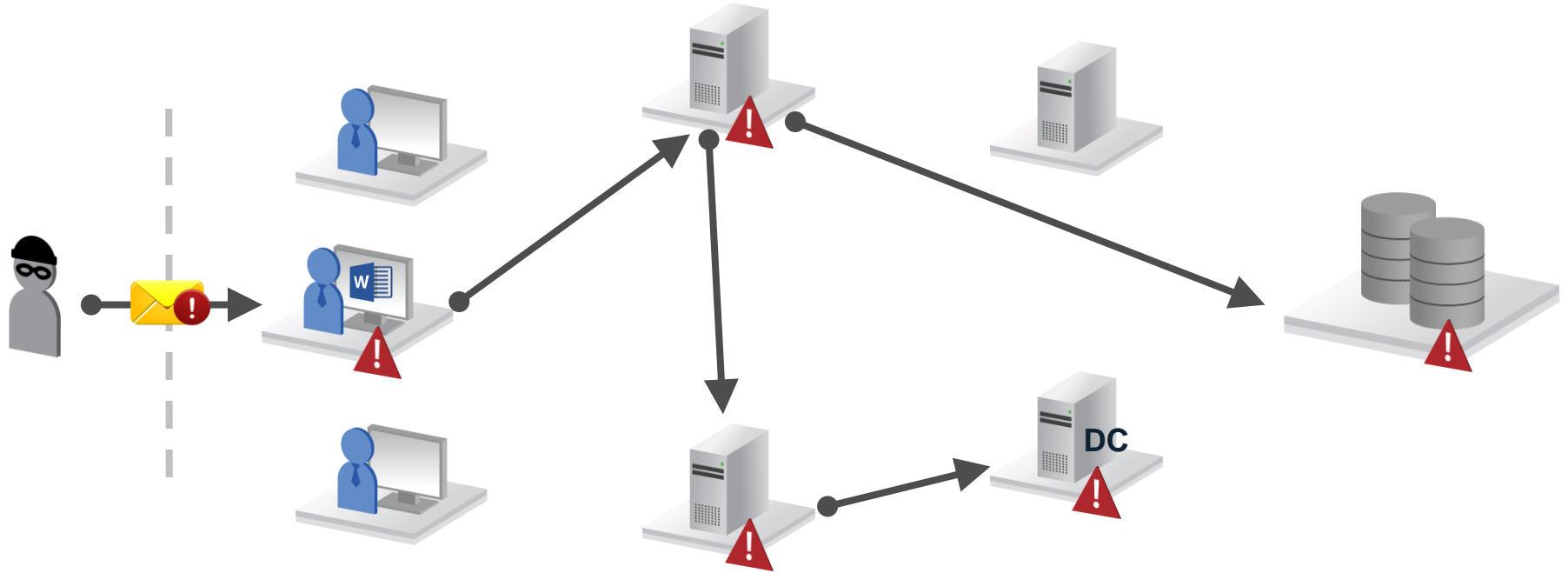
---



“Evidence shows that most advanced attacks start with phishing emails sent to non-privileged business users, and a campaign of just 10 emails will typically yield a greater than 90 percent chance that at least one person will become the criminal’s prey.”

Verizon 2015 Data Breach Investigations Report

# SAMPLE ATTACK SCENARIO



# THE PRIVILEGE SPRINT

---

- Rapid reduction of privileged account risk, focused on Active Directory
- “Act as if you’ve been breached”

Four core objectives:

- 1 Reduce the attack surface**
- 2 Isolate privileged access**
- 3 Require two-factor authentication for privileged access**
- 4 Detect attacks on privilege**

# 1 REDUCE THE ATTACK SURFACE

---

- Eliminate unnecessary accounts and entitlements
- Implement a password of the day approach for personal privileged accounts
- Vault and automatically change the passwords for remaining privileged accounts
- Don't over use privilege
  - Domain Administrators should only log on to Domain Controllers



## 2 ISOLATE PRIVILEGED ACCESS

---

- Establish a barrier between the untrusted workstation and sensitive assets
- Most approaches utilize a hardened “jump server”
- Greatly reduces risk of credential theft
- Increases visibility and accountability for privileged activities

### 3 REQUIRE 2FA FOR PRIVILEGED ACCESS

---

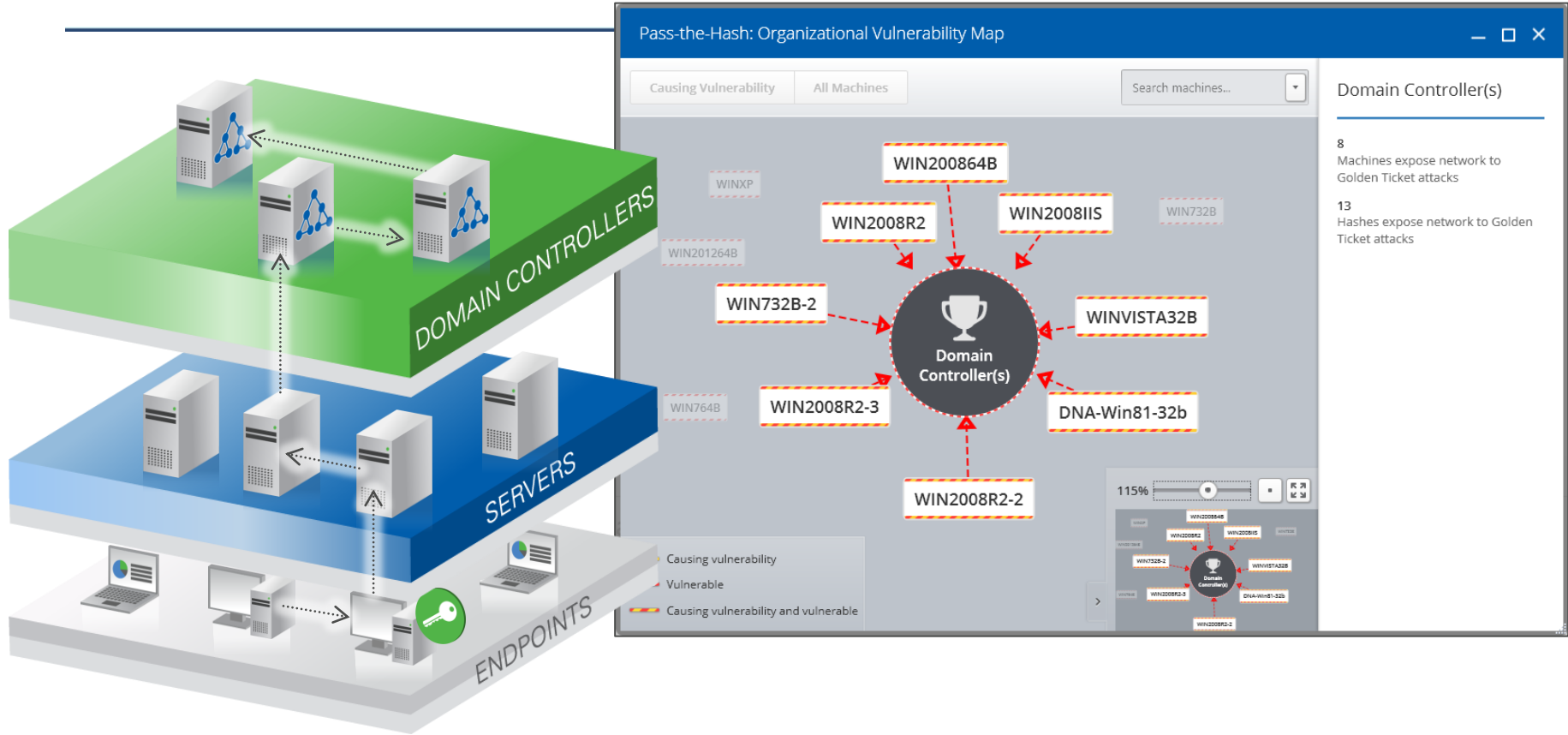
- Strong authentication for privilege is mandatory
- Challenging to manage native integrations
- Enforcing two-factor at the “jump server” standardizes deployment

## 4 DETECT ATTACKS ON PRIVILEGE

---

- Solutions can detect pass-the-hash and golden tickets in real-time
- Behavioral profiling and anomaly detection
- Improves odds of detection at all phases of an attack

# IDENTIFYING KEY RISKS – DOMAIN COMPROMISE



# IDENTIFYING KEY RISKS – LATERAL MOVEMENT

## CREDENTIAL THEFT VULNERABILITY

## VULNERABILITY STATUS

### PASS-THE-HASH: ACTIVE THREATS

97 Privileged account hashes found on

### PASS-THE-HASH: INACTIVE THREATS

277 Privileged account hashes previously found on all Privileged accounts (Last 90 days)

### PASS-THE-HASH:

#### MITIGATED WITH PRIVILEGED ACCOUNT SECURITY

Privileged Accounts Security can frequently detect and prevent the use of one-time passwords on all Privileged accounts.

Before: 97 Privileged account hashes found on all Privileged accounts  
After: 12 Privileged account hashes found on all Privileged accounts

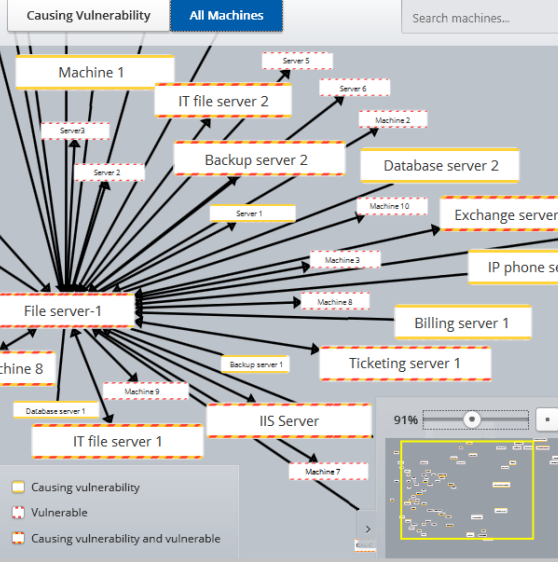
### PASS-THE-HASH: ORGANIZATION

See a map of all vulnerable machines and vulnerabilities found in your organization.

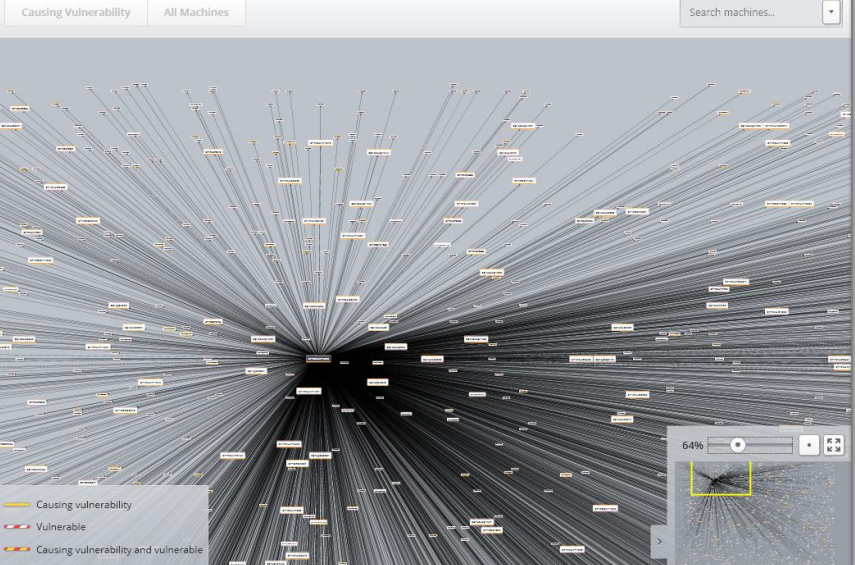
OPEN PTH MAP

### PASS-THE-HASH: VULNERABLE MACHINES

#### Pass-the-Hash: Organizational Vulnerability Map



#### Pass-the-Hash: Organizational Vulnerability Map



# CYBERARK PRIVILEGED ACCESS SECURITY HYGIENE PROGRAM



# SESSION KEY TAKEAWAYS

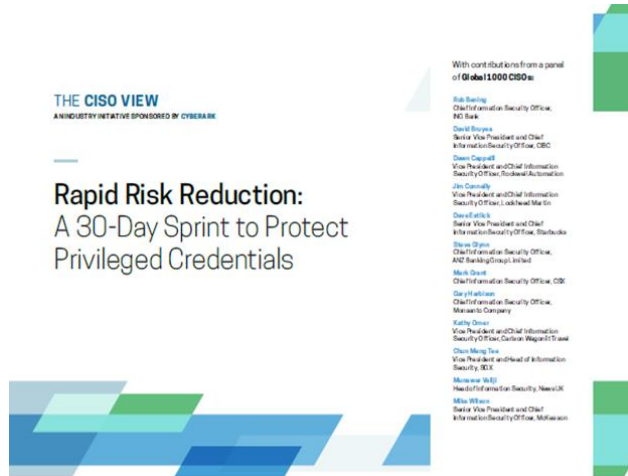
## WHAT HAVE WE LEARNED

- In the past 24 months, many successful attacks have used hijacked privileged credentials
- Protecting privileged credentials must be a top organizational priority
- Significant risk reduction does not take long
- It's possible to adopt a proven framework for an intensive 30-day sprint to implement a set of key controls around privileged credentials

# SESSION NEXT STEPS

## WHERE TO START

- Run DNA to discovery privilege accounts across your organisation.
- Review your privilege account security hygiene plan
- Download a copy of the “The CISO View Report” - <https://www.cyberark.com/cisoview/>
- Focus on rapid risk reduction!







**CYBERARK<sup>®</sup>**

**THANK YOU**