What Are We Even Doing?

Sean Metcalf (@PyroTek3)
sean @ TrimarcSecurity.com
TrimarcSecurity.com

What Are We Even Doing?

Sean Metcalf (@PyroTek3)
sean @ TrimarcSecurity.com
TrimarcSecurity.com

About

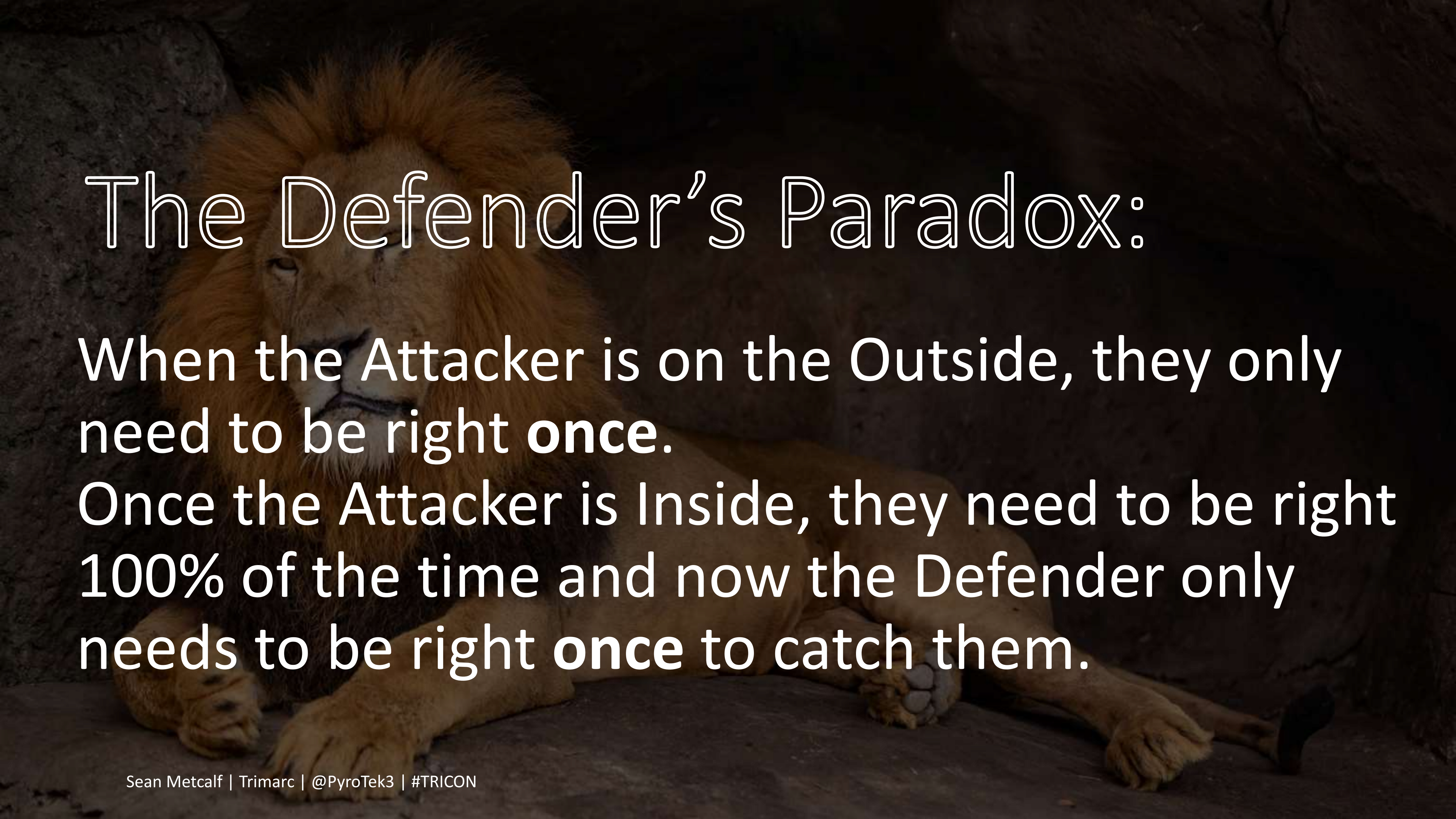
- Founder & CTO @ Trimarc (Trimarc.co), a professional services company that helps organizations better secure their Active Directory & Azure AD/Entra ID.
- Microsoft Certified Master (MCM) Directory Services
- Enterprise Security Weekly Co-Host (SecurityWeekly.com)
- Former Microsoft MVP
- Speaker: Black Hat, Blue Hat, Blue Team Con, BSides Charm, BSides DC, BSides PR, DEFCON, DerbyCon, TEC, Troopers
- Security Consultant / Researcher
- AD Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

Agenda

- Defensive Fallacies
- Why Are We Here
- AD Attack Timeline
- Challenges
- Red Team, Blue Team, Purple Team
- Community
- Conclusion

Defenders have to be Right 100% of the Time
while
Attackers only have to be Right Once

FALSE



The Defender’s Paradox:

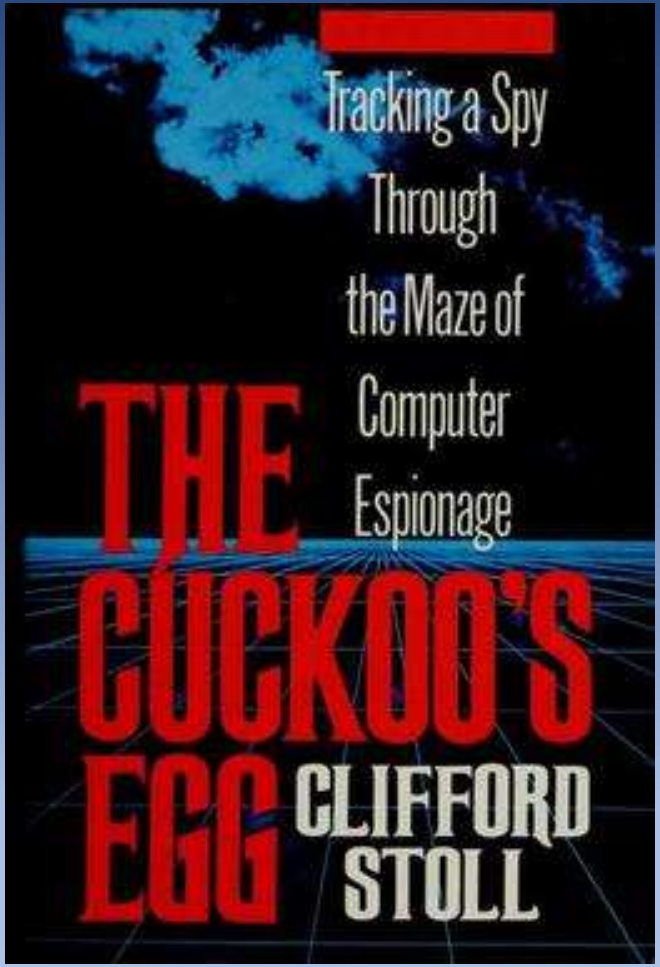
When the Attacker is on the Outside, they only need to be right **once**.
Once the Attacker is Inside, they need to be right 100% of the time and now the Defender only needs to be right **once** to catch them.

Attackers can do an *infinite* number of things.

However, they have a *finite* number of pathways.

Configure detection around these

Why Are We Here?



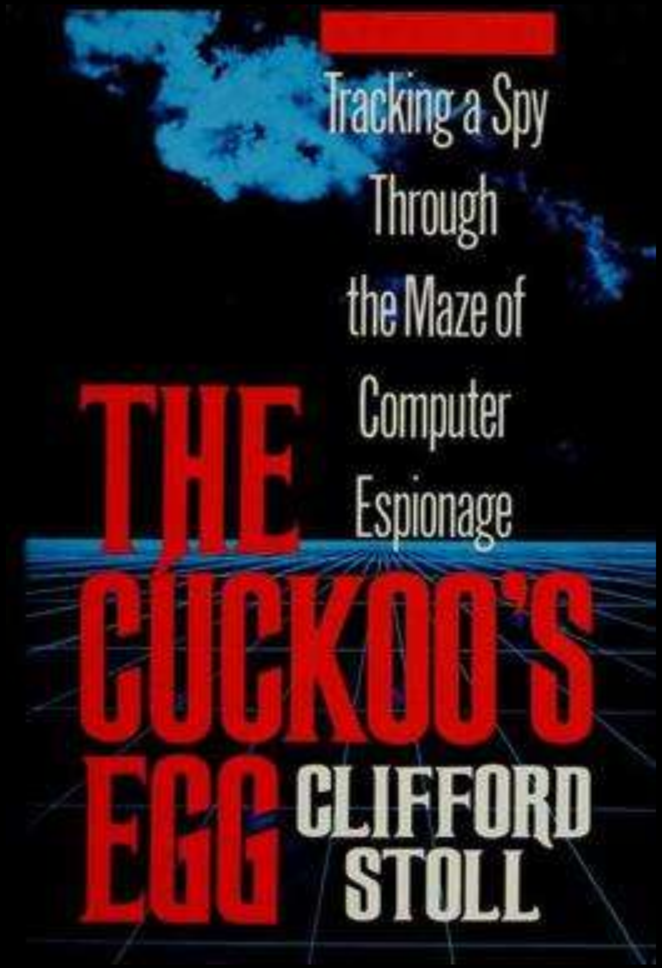
Let's Go Back In Time… to the 80s

https://berkeleylabnext90.lbl.gov/celebrate-the-past/photo-gallery/#1980s

It started with 9 seconds

Creating an SDI Department

From Russia, with Love


Tracking a Spy Through the Maze of Computer Espionage
THE CUCKOO'S EGG
CLIFFORD STOLL

Active Directory Attack Timelines: “Baby Steps”(2000 – 2009)

1997

April: Paul Ashton posted to NTBugtraq about “'Pass the Hash' with Modified SMB Client” leveraging the username and LanMan hash against NT.

2001

March: Sir Dystic of Cult of the Dead Cow (cDc) releases SMBRelay and SMBRelay2

2007

NBNSpoof tool created by Robert Wesley McGrew (LLMNR/NBT-NS)

2008

July: Hernan Ochoa publishes the "Pass-the-Hash Toolkit“ (later called WCE)

Active Directory Attack Timelines: “The Wonder Years” (2010 – 2014)

2010

March: Windows Credentials Editor (WCE) & RootedCon presentation by Hernan Ochoa

2011

May: First version of Mimikatz tool released by Benjamin Delpy

2012

Exploiting Windows 2008 Group Policy Preferences by Emilien Giraul

May: Chris Campbell’s post on GPP Passwords

October: Responder v1 tool released by Laurent Gaffie

2013

October: Invoke-Mimikatz PowerShell module released by Joe Bialek

2014

August: “Abusing Microsoft Kerberos sorry you guys don’t get it” Black Hat presentation by Benjamin Delpy & Skip Duckwell

- Golden Tickets
- Overpass-the-hash
- Pass-the-ticket

September: PAC Validation, The 20 Minute Rule and Exceptions (BHUSA 2014 part deux) blog post about Silver Tickets by Skip Duckwell

September: Kerberoast released by Tim Medin at DerbyCon

December: PowerView tool released by Will Schroeder

Active Directory Attack Timeline Summary (with Mitre ATT&CK): “The Wonder Years” (2010 – 2014)

Tools

Windows Credential Editor (WCE) (ID: S0005)

Mimikatz (ID: S0002)

Responder (ID: S0174)

PowerView

Privilege Escalation

Group Policy Preferences password (ID: T1552.006)

Pass the Ticket (ID: T1550.003)

Overpass-the-Hash

Kerberoast (ID: T1558.003)

Persistence

Golden Tickets (ID: T1558.001)

Silver Tickets (ID: T1558.002)

Active Directory Attack Timelines:
“The Golden Years” (2015 – 2019)

2015

DSInternals tool released by Michael Grafnetter

Kekeo tool released by Benjamin Delpy

PowerSploit toolset released by Matt Graeber

May: Impacket tool released by Alberto Solino (asolino)

May: Method to Detect Golden Tickets

August: PowerShell Empire released by Will @Hrmj0y & Justin Warner

August: DCSync update to Mimikatz by Vincent Le Toux & Benjamin Delpy

August: Black Hat 2015 presentation by Sean Metcalf: Unconstrained Delegation & Golden Tickets more powerful & Active Directory Persistence using AdminSDHolder

September: CrackMapExec v1.0.0 tool released by Marcello aka byt3bl33d3r

September: DerbyCon 2015 presentation by Sean Metcalf: Attacking DSRM

December: Attacking Group Managed Service Accounts (GMSAs) by Michael Grafnetter

2016

August: Bloodhound tool released at DEFCON 23 originally written by Will Schroeder, Rohan Vazarkar, & Andy Robbins

2017

May: DNSAdmin to Domain Admin by Shay Ber

May: Death Star python script released by byt3bl33d3r

May: Ntlmrelayx tool released by Fox-IT

August: ACE up the Sleeve Black Hat 2017 presentation by Andy Robbins and Will Schroeder

September: Sharphound tool release

2018

February: Bloodhound.py tool released by Dirk-jan Molema (Python based Bloodhound ingester)

July: GhostPack released as a collection of C# ports of popular PowerShell tools and collects these tools together

August: DCShadow attack by Vincent Le Toux & Benjamin Delpy

September: Rubeus tool released by Will Schroeder (port of Kekeo and added to GhostPack)

October: “Printer Bug” AD priv esc talk at DerbyCon by Will Schroeder, Lee Christensen, & Matt Nelson

Ldapdomaindump tool released by Dirk-jan Molema

2019

January: PrivExchange tool released by Dirk-jan Molema

January: Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory article “Wagging the Dog” by Elad Shamir

Active Directory Attack Timeline Summary (with Mitre ATT&CK): “The Golden Years” (2015 – 2019)

Tools

DSInternals

Kekeo

PowerSploit (ID: S0194)

Impacket (ID: S0357)

PowerShell Empire (ID: S0363)

DCSync added to Mimikatz (ID: T1003.006)

CrackMapExec (ID: S0488)

Bloodhound (ID: S0521)

DeathStar.py

NTLMRelayX

SharpHound

GhostPack

Rubeus (ID: S1071)

Privilege Escalation

DNSAdmin to Domain Admin

AD Permissions

“Printer Bug”

Resource-Based Constrained Delegation

Persistence

AD Permissions

DCShadow (ID: T1207)

Active Directory Attack Timelines: “The Third Age” (2020 – 2023)

2020

- December: Adalanche tool released by Lars Karlslund

2021

- April: RemotePotato0 tool released by antonioCoco & article by Antonio Cocomazzi and Andrea Pierini
- July: PetitPotam tool released
- August: Certified Pre-Owned (ADCS Attacks) Black Hat talk by Will Schroeder & Lee Christensen whitepaper download
- August: Certify ADCS tool released by Will Schroeder & Lee Christensen (in GhostPack)
- October: Kerberos Relay Attack by James Forshaw
- October: Certipy tool released by Oliver Lyak (ly4k) - Python port of the Certify tool
- November: “Is This My Domain Controller” Black Hat talk by Sagi Sheinfeld (@sagish1233), Eyal Karni (@eyal_karni), & Yaron Zinar (@YaronZi)

2022

- April: KrbRelayUp tool released by Dec0ne

2023

- October: CrackMapExec continues as NetExec (nxc)!

Active Directory Attack Timeline Summary (with Mitre ATT&CK): “The Third Age” (2020 – 2023)

Tools

RemotePotato0

PetitPotam

Certify

Certipy

KrbRelayUp

CrackMapExec continues as NetExec (nxc)

Privilege Escalation

Certified Pre-Owned (ADCS Attacks)

Kerberos Relay Attack

Persistence

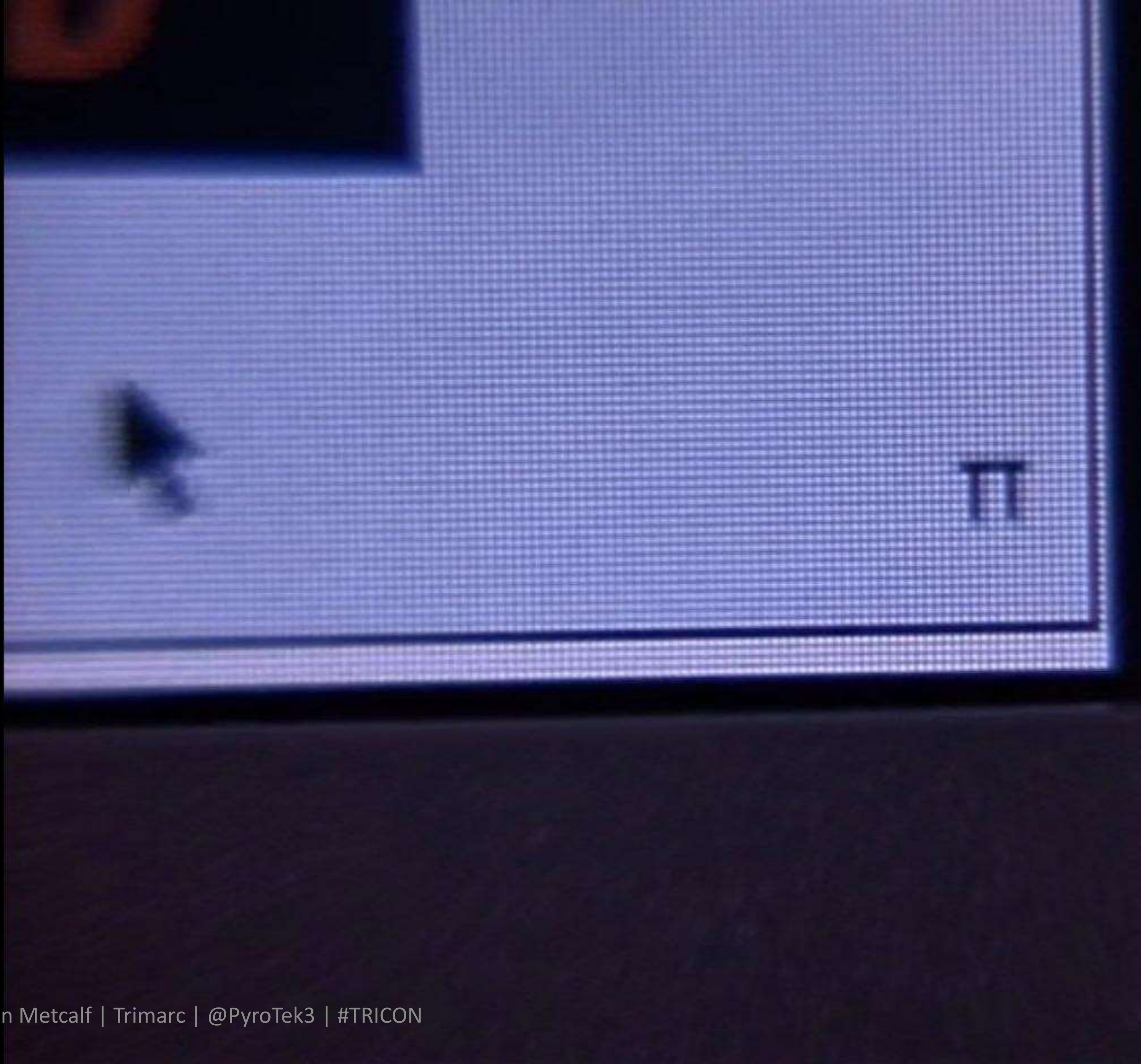
Certified Pre-Owned (ADCS Attacks)

Challenges

Challenge: Over-Confidence

Challenge: Assumptions

Challenge: Backdoors (ex. Solar Winds)

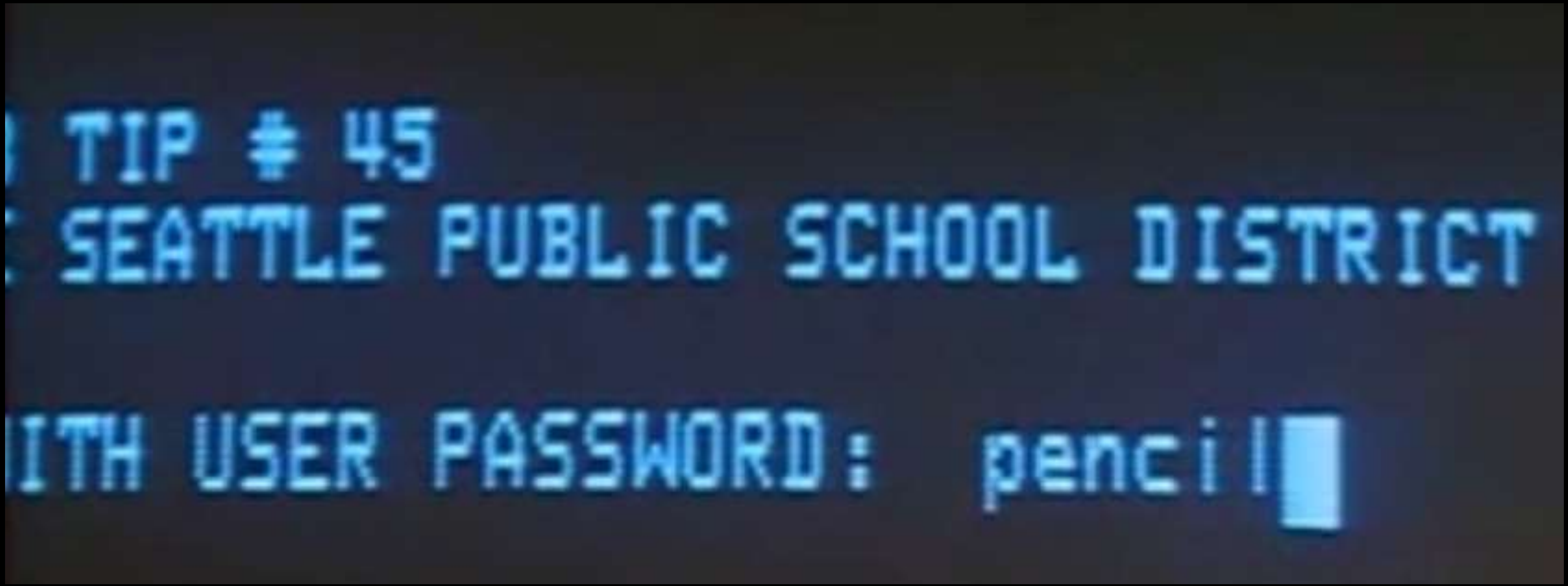


Challenge: Technical Debt

Challenge: Bad Passwords

1 2 3 4 5

Challenge: Bad Passwords



```
 TIP # 45
 SEATTLE PUBLIC SCHOOL DISTRICT

ITH USER PASSWORD:  pencil
```

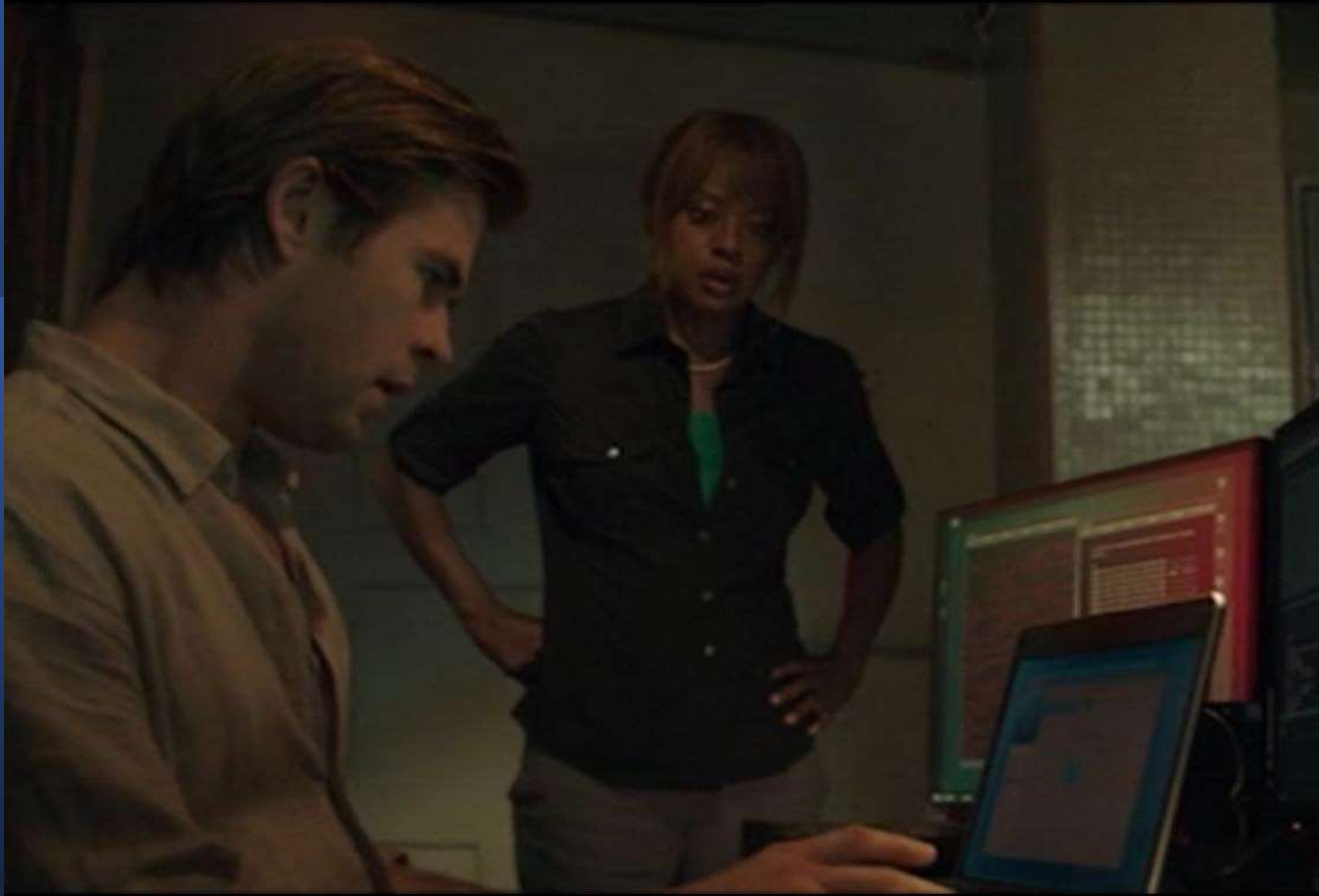
Nation-State, APTs, & Bears, Oh My!

Challenge: Insider Threat

Challenge: Social Engineering

Challenge: Social Engineering

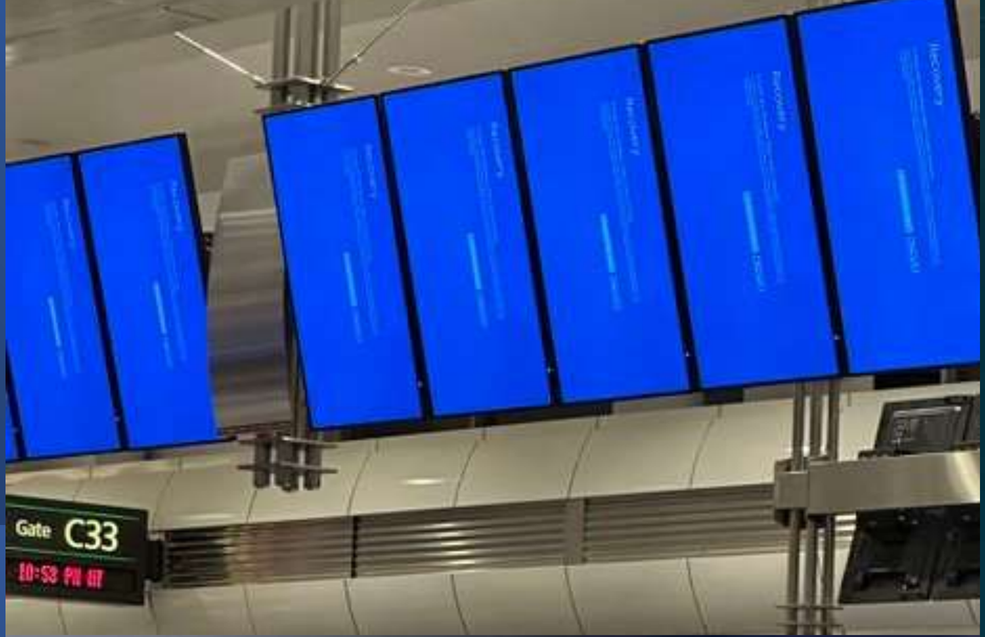
Challenge: Phishing

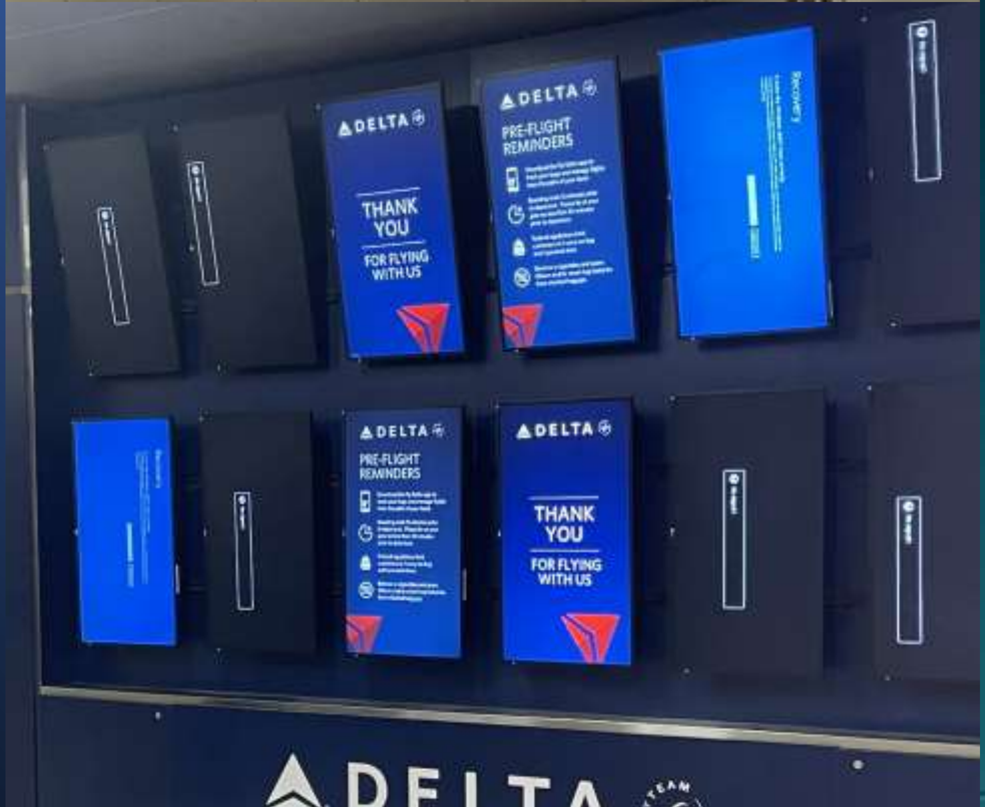


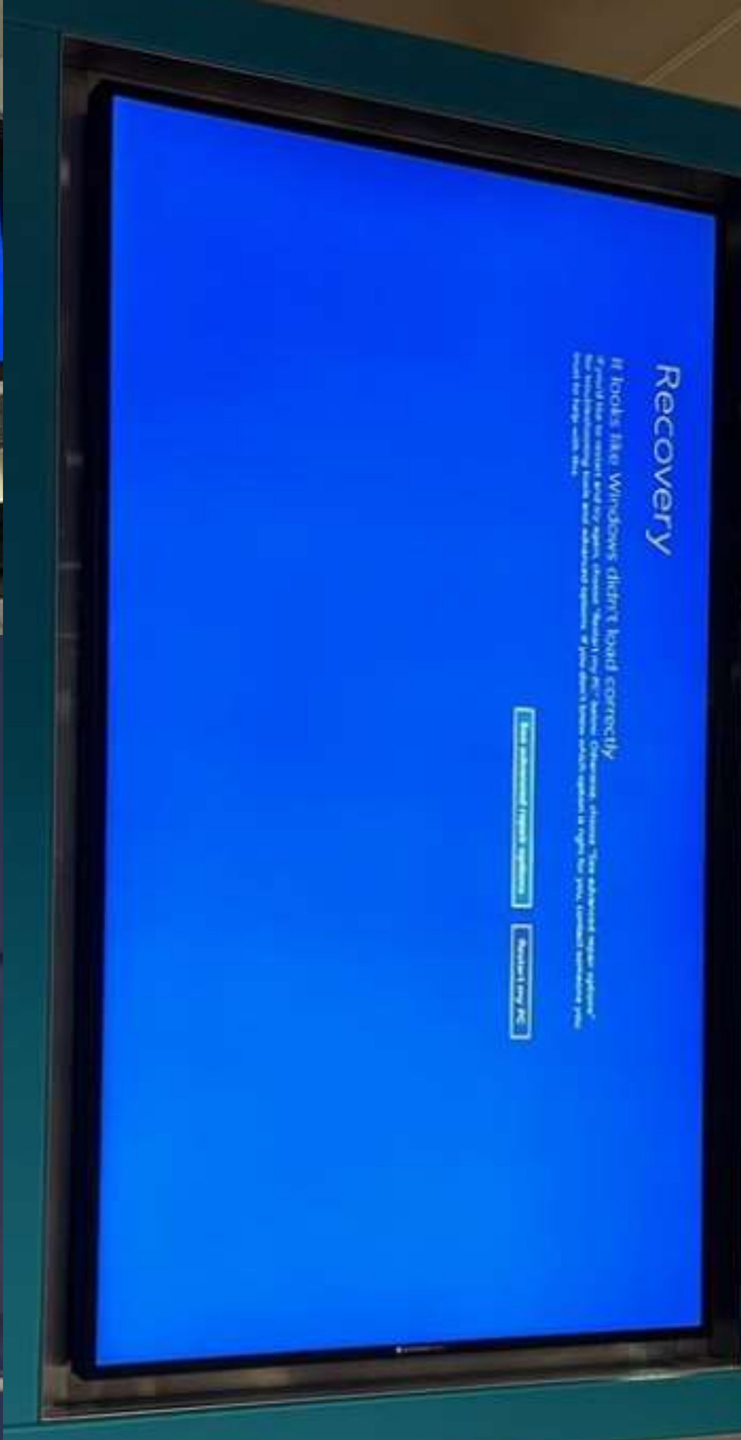
Challenge: Ransomware

Challenge: Ransomware

Challenge: Vendor Oops

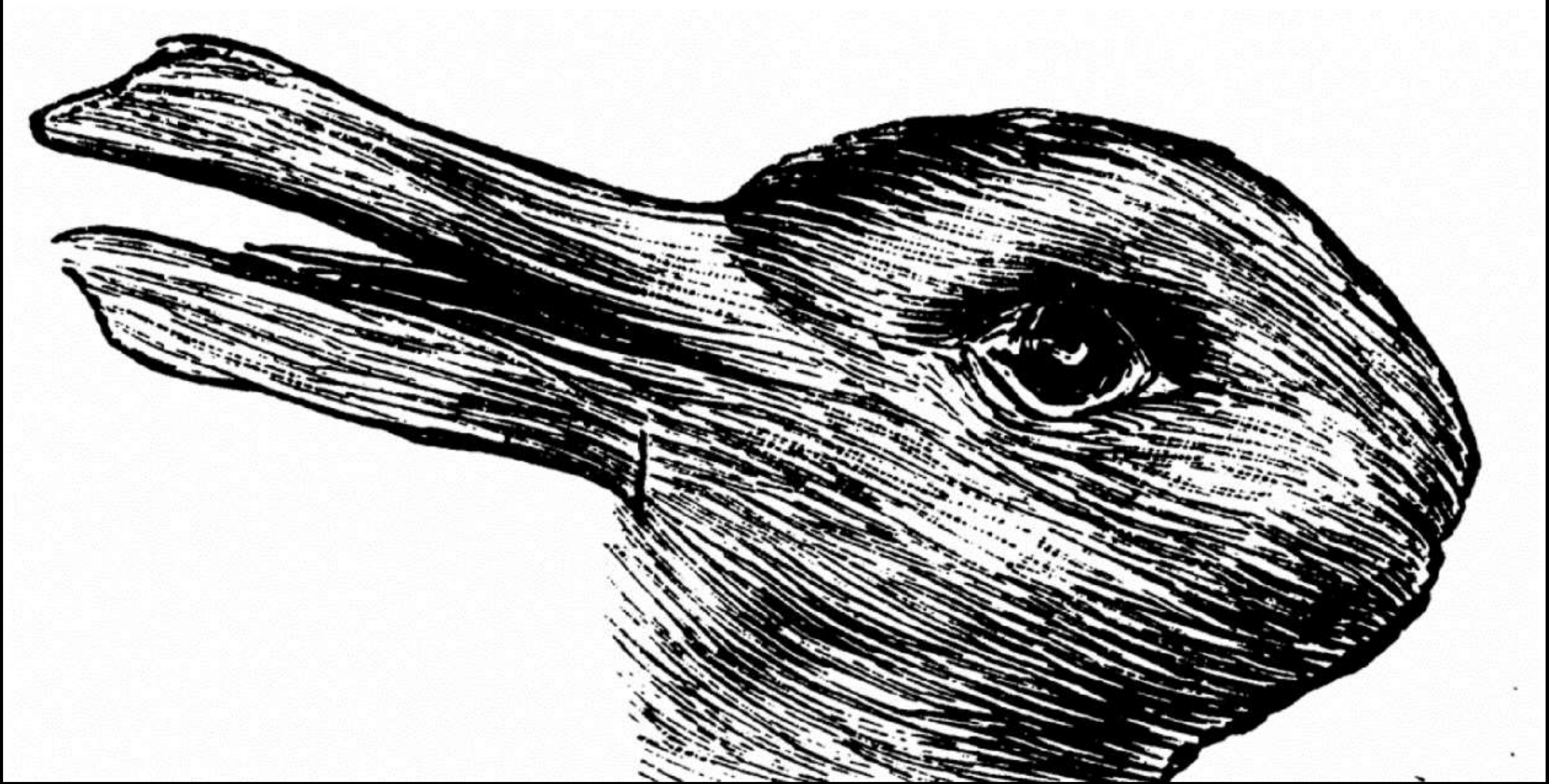


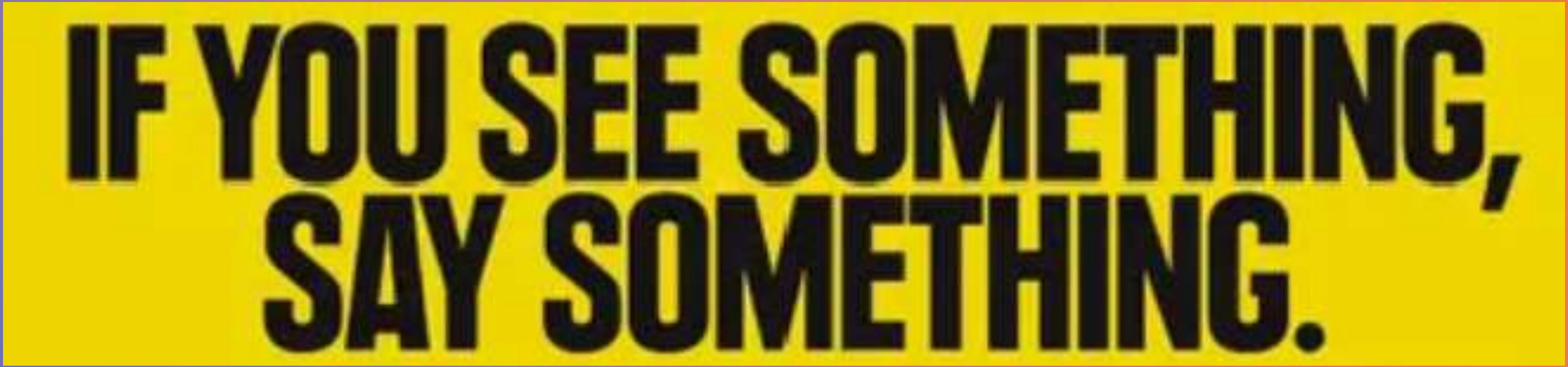




Red Team, Blue Team, Purple Team, What Team Am I On?

We Are ALL Part of The Blue Team





IF YOU SEE SOMETHING, SAY SOMETHING.

Impostor Syndrome

Who am I…?

YET

What was theoretical years ago is often practical today or tomorrow

Attackers keep identifying novel techniques that are often new takes on old issues.

“Nobody has the ability to make things perfect, but we are given chances to make it better”

A 40% security solution today is better than the 100% solution that won’t happen for years

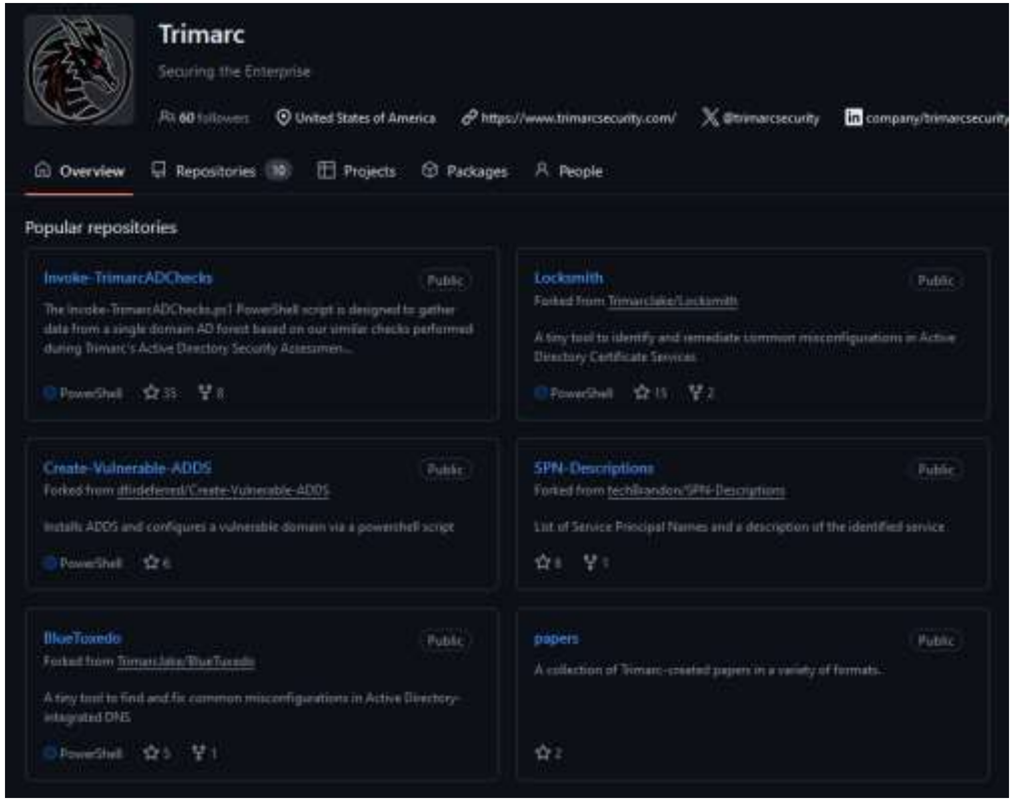
-Voltaire

Don’t let the Perfect be the Enemy of the Good

“A year from now, you’ll be a year older. What are you going to do?”

- Ramit Sethi

Community



Trimarc

Securing the Enterprise

60 followers · United States of America · https://www.trimarcsecurity.com/ · @trimarcsecurity · company/trimarcsecurity

Overview · Repositories 10 · Projects · Packages · People

Popular repositories

Invoke-TrimarcADChecks Public
The Invoke-TrimarcADChecks.ps1 PowerShell script is designed to gather data from a single domain AD forest based on our similar checks performed during Trimarc's Active Directory Security Assessmen...
PowerShell ☆ 35 Forks 8

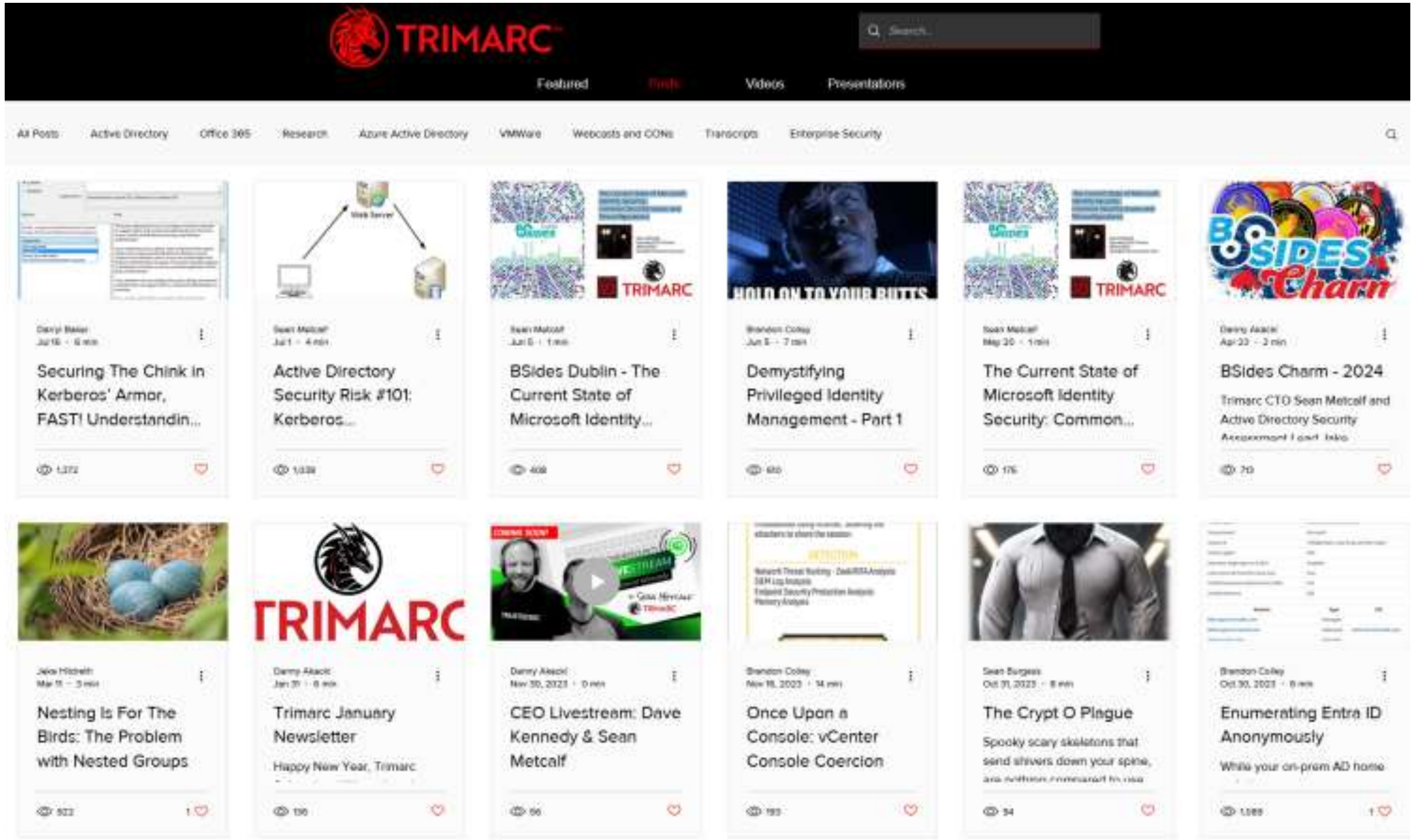
Locksmith Public
Forked from TrimarcJake/Locksmith
A tiny tool to identify and remediate common misconfigurations in Active Directory Certificate Services.
PowerShell ☆ 15 Forks 2

Create-Vulnerable-ADDS Public
Forked from dfirdeferred/Create-Vulnerable-ADDS
Installs ADDS and configures a vulnerable domain via a powershell script
PowerShell ☆ 6

SPN-Descriptions Public
Forked from techBrandon/SPN-Descriptions
List of Service Principal Names and a description of the identified service.
☆ 8 Forks 1

BlueTuxedo Public
Forked from TrimarcJake/BlueTuxedo
A tiny tool to find and fix common misconfigurations in Active Directory-integrated DNS.
PowerShell ☆ 5 Forks 1

papers Public
A collection of Trimarc-created papers in a variety of formats.
☆ 2



TRIMARC

Search...

Featured · Posts · Videos · Presentations

All Posts · Active Directory · Office 365 · Research · Azure Active Directory · VMWare · Webcasts and CONs · Transcripts · Enterprise Security

Darryl Baker · Jul 16 · 6 min
Securing The Chink in Kerberos' Armor, FAST! Understandin...
1,372

Sean Metcalf · Jul 1 · 4 min
Active Directory Security Risk #101: Kerberos...
1,038

Sean Metcalf · Jun 5 · 1 min
BSides Dublin - The Current State of Microsoft Identity...
408

Brandon Colley · Jun 5 · 7 min
Demystifying Privileged Identity Management - Part 1
610

Sean Metcalf · May 20 · 1 min
The Current State of Microsoft Identity Security: Common...
176

Danny Akacki · Apr 23 · 2 min
BSides Charm - 2024
Trimarc CTO Sean Metcalf and Active Directory Security Assessment Lead Jake...
70

Jake Hildreth · Mar 11 · 3 min
Nesting Is For The Birds: The Problem with Nested Groups
922 · 1

Danny Akacki · Jan 31 · 6 min
Trimarc January Newsletter
Happy New Year, Trimarc...
136

Danny Akacki · Nov 30, 2023 · 0 min
CEO Livestream: Dave Kennedy & Sean Metcalf
66

Brandon Colley · Nov 16, 2023 · 14 min
Once Upon a Console: vCenter Console Coercion
193

Sean Burgess · Oct 31, 2023 · 8 min
The Crypt O Plague
Spooky scary skeletons that send shivers down your spine, are nothing compared to use...
94

Brandon Colley · Oct 30, 2023 · 6 min
Enumerating Entra ID Anonymously
While your on-prem AD home...
1,089 · 1

linktr.ee/Trimarc

Slides, Video & Security Articles: Hub.TrimarcSecurity.com

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

TRIMARC