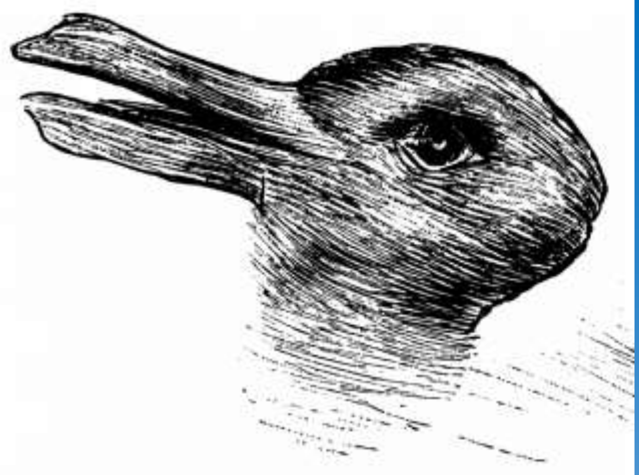
Into the Blue

A Journey Beyond Space & Time

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

Turn on Original Sound
Speaker View
Priscilla Bardio...
Shari Clare, 360@...
Simon Booth, 9...
Jules Park, 90@7
Alex Kim, 90@5
D...ay, 90@8
Yatin Moham...
...Park, 90@6
Steven Crosby,...
Winston Twu, 90@...
Katie Williams...
Dan Roman, 9...
Art Gilbreath, 9...
Waylon Betz, 9...
...Sadler 90@1
Shawn Lan, 90@-1
Andy de Artola, 9...
Raphael Villa, ...
Joanna Jiang, ...
Bernie Santo...
Brett Litle, 90@...
1/2
Brian Spragg...
Andy Kim, 90...
Equine Ling, 90...
Evan Eyerly, ...
Alex Guerrero, 1...
Brook Bayuh, 90...
Eric Platt, 90@-1...
1/2
David King, 9...
Chris Gleave...
Heather Goold, ...
James Desmon...
George Guti...
Jay Mohammed...
Austin Stumpe, ...
Jeffrey Faulkner...
James Woolridg...
Janelle Spar...
Dustin DeMayo,...
John Mensie, 0...
Katherine Sm...
Katrina Tsai, 0@0...

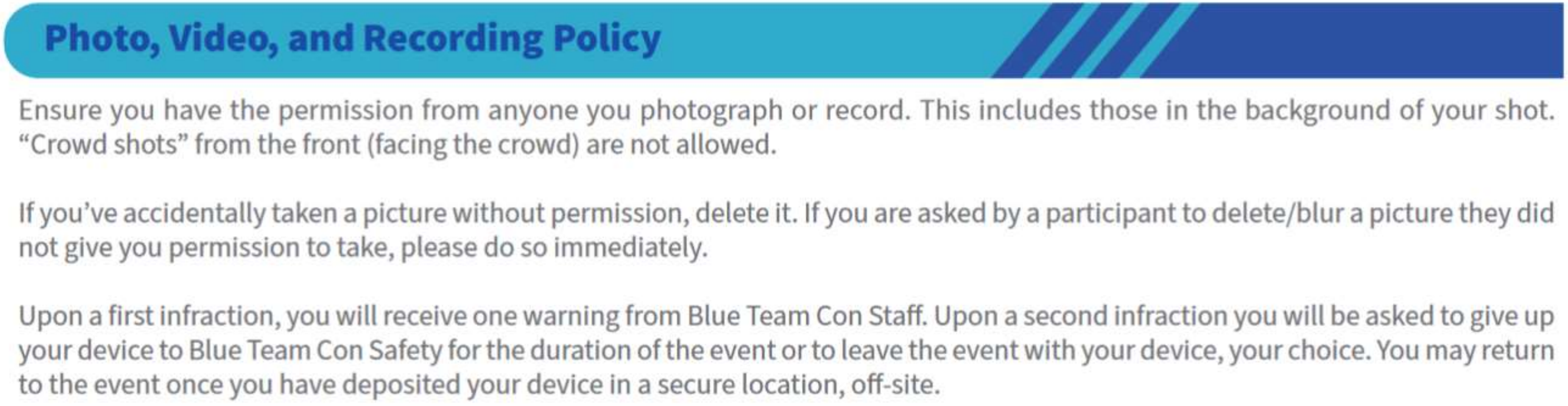


Into the Blue

A Journey Beyond Space & Time

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

BlueTeamCon Policy



Photo, Video, and Recording Policy

Ensure you have the permission from anyone you photograph or record. This includes those in the background of your shot. "Crowd shots" from the front (facing the crowd) are not allowed.

If you've accidentally taken a picture without permission, delete it. If you are asked by a participant to delete/blur a picture they did not give you permission to take, please do so immediately.

Upon a first infraction, you will receive one warning from Blue Team Con Staff. Upon a second infraction you will be asked to give up your device to Blue Team Con Safety for the duration of the event or to leave the event with your device, your choice. You may return to the event once you have deposited your device in a secure location, off-site.

Sean says:
You can take photos of me during my keynote
(afterwards, please ask first)

Sean Metcalf | Trimarc | @PyroTek3 | #BlueTeamCon

Agenda

Who am I?

Why this Talk?

Why Are We Here?

InfoSec Challenges

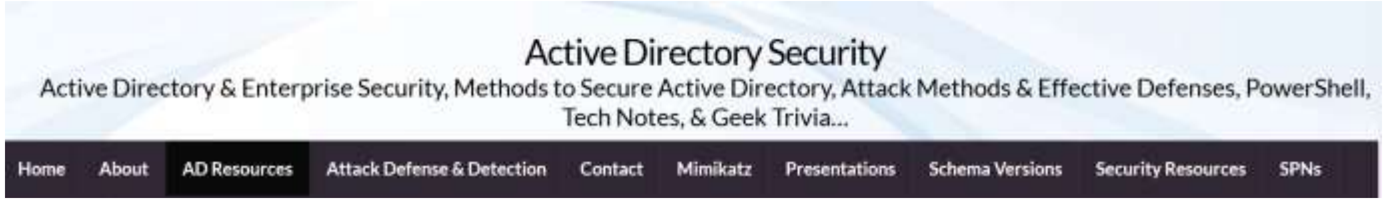
Blue vs Red vs Purple

Conclusion

Who Am I?

MVP Microsoft® Most Valuable Professional

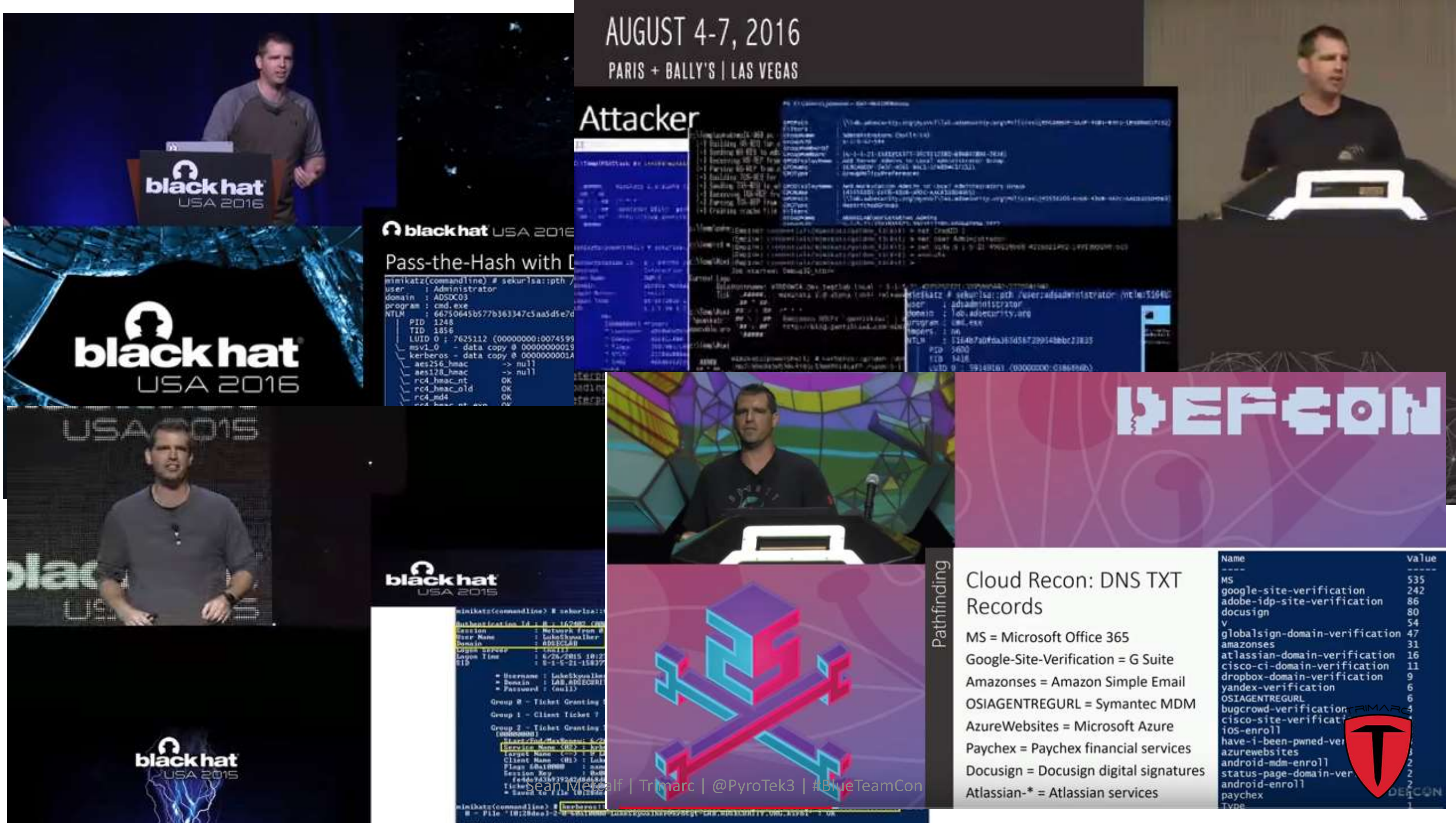
Microsoft® CERTIFIED Master



Active Directory Security

Active Directory & Enterprise Security, Methods to Secure Active Directory, Attack Methods & Effective Defenses, PowerShell, Tech Notes, & Geek Trivia...

TRIMARC



Pass-the-Hash with D

```
mimikatz(commandline) # sekurlsa::pth /
user    : Administrator
domain  : ADSDC03
program : cmd.exe
NTLM    : 66750645b577b363347c5aa5d5e7d
  |  PID  1248
  |  TID  1856
  |  LUID 0 ; 7625112 (00000000:00745999
  \_ msv1_0   - data copy @ 000000000019
  \_ kerberos - data copy @ 00000000001A
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
```

Attacker

```
mimikatz # sekurlsa::pth /user:adsadministrator /ntlm:5164b
user    : adsadministrator
domain  : lab.adsecurity.org
program : cmd.exe
impers. : no
NTLM    : 5164b7abfda365d5673995 4bbbc23835
  |  PID  5600
  |  TID  5416
```

Pathfinding

Cloud Recon: DNS TXT Records

MS = Microsoft Office 365

Google-Site-Verification = G Suite

Amazonses = Amazon Simple Email

OSIAGENTREGURL = Symantec MDM

AzureWebsites = Microsoft Azure

Paychex = Paychex financial services

Docusign = Docusign digital signatures

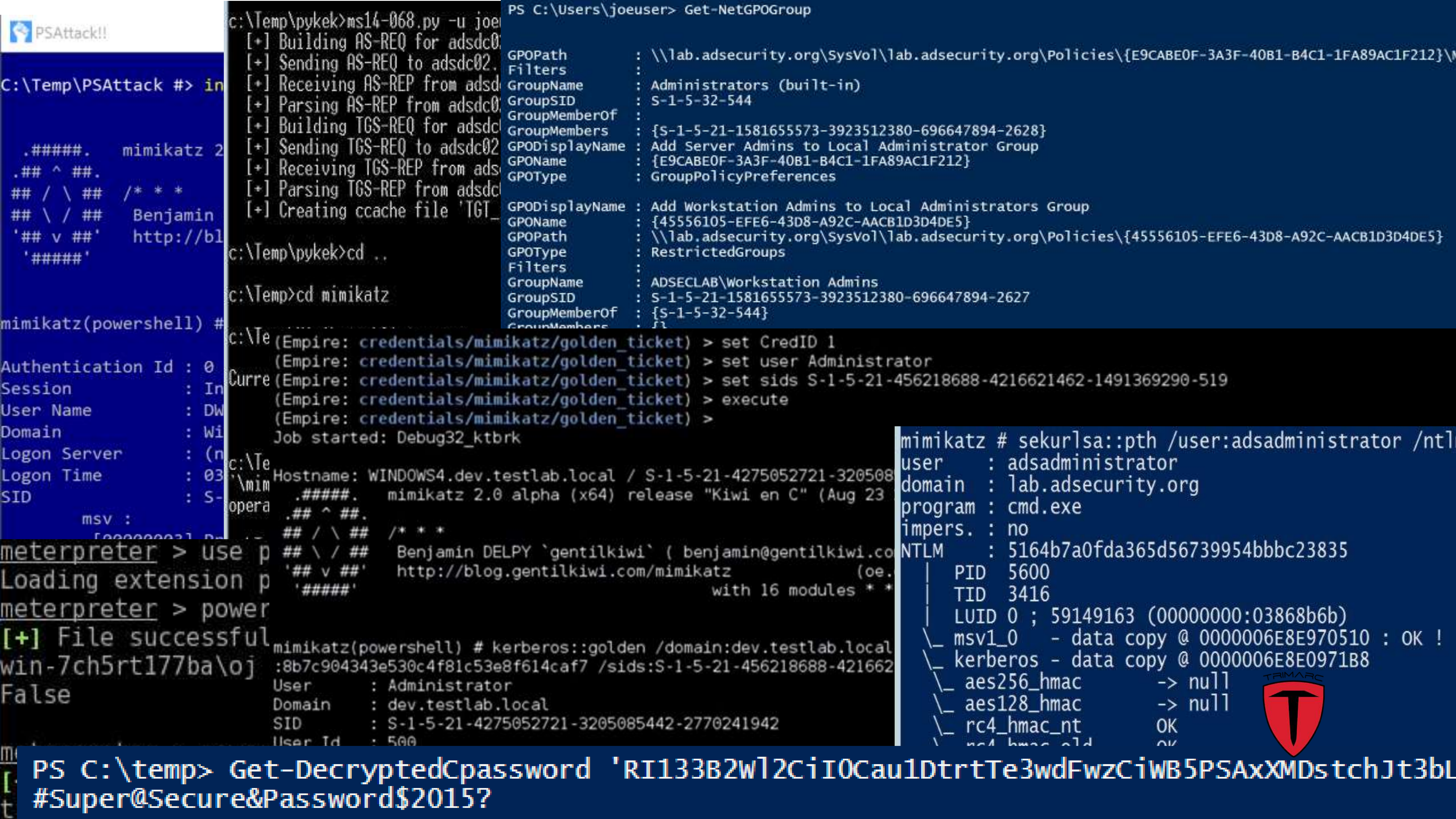
Atlassian-* = Atlassian services

```
Name                                Value
----                                -----
MS                                  535
google-site-verification            242
adobe-idp-site-verification         86
docusign                            80
v                                   54
globalsign-domain-verification      47
amazonses                           31
atlassian-domain-verification       16
cisco-ci-domain-verification        11
dropbox-domain-verification         9
yandex-verification                 6
OSIAGENTREGURL                      6
bugcrowd-verification               4
cisco-site-verificati               4
iOS-enroll
have-i-been-pwned-ver               3
azurewebsites                       3
android-mdm-enroll                  2
status-page-domain-ver              2
android-enroll                      2
paychex                             1
Type                                1
```

I've Done Some Stuff

- 2015: Published original method to detect Golden Tickets.
- 2015: Made Golden Tickets more effective by adding Enterprise Admins to SIDHistory in the ticket (extrasids).
- 2015: Described what rights were necessary to DCSync, including initial detection guidance.
- 2015: Described "SPN Scanning" – identifying services on a network without port scanning.
- 2015: Identified how to use Silver Tickets to compromise AD (via DCs) for persistence.
- 2015: Described how to pass-the-hash using the DC's DSRM password.
- 2016: Published methods to better detect PowerShell attack activity.
- 2017: Described how to modify AdminSDHolder permissions for persistence.
- 2017: Published first effective detection of Kerberoasting with no false positives (still effective).
- 2017: Published Password Spray (AD) detection when attackers use Kerberos.
- 2017: Discussed how to forge federation tokens (aka "GoldenSAML") & compromise AD through Azure AD Connect (on-prem).
- 2018: Described how most Read-Only Domain Controller deployments are vulnerable & how to improve.
- 2018: Discussed how to bypass most enterprise password vault security.
- 2019: Presented on Microsoft Cloud (Azure AD & Microsoft Office 365) attack & defense at BlackHat & DEFCON Cloud Security Village
- 2020: Published info on how to compromise Azure instances (VMs) from Microsoft Office 365.
- 2021: 1 of 3 people thanked during CISA Director's BlackHat keynote for SolarWinds help.
- "Stealth" contributor to Bloodhound.
- Published lots of AD attack & defense techniques (conference talks & blog posts).

Why This Talk?



```
PSAttack!!

C:\Temp\PSAttack #> in

  .#####.   mimikatz 2
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin
 '## v ##'   http://bl
  '#####'

mimikatz(powershell) #

Authentication Id : 0
Session           : In
User Name         : DW
Domain            : Wi
Logon Server      : (n
Logon Time        : 03
SID               : S-
        msv :
```

```
c:\Temp\pykek>ms14-068.py -u joe
  [+] Building AS-REQ for adsdc0
  [+] Sending AS-REQ to adsdc02.
  [+] Receiving AS-REP from adsd
  [+] Parsing AS-REP from adsdc0
  [+] Building TGS-REQ for adsdc
  [+] Sending TGS-REQ to adsdc02
  [+] Receiving TGS-REP from ads
  [+] Parsing TGS-REP from adsdc
  [+] Creating ccache file 'TGT_

c:\Temp\pykek>cd ..

c:\Temp>cd mimikatz

c:\Te
Curre

c:\Te
'\mim
opera
```

```
PS C:\Users\joeuser> Get-NetGPOGroup

GPOPath         : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}\
Filters         :
GroupName       : Administrators (built-in)
GroupSID        : S-1-5-32-544
GroupMemberOf   :
GroupMembers    : {S-1-5-21-1581655573-3923512380-696647894-2628}
GPODisplayName  : Add Server Admins to Local Administrator Group
GPOName         : {E9CABE0F-3A3F-40B1-B4C1-1FA89AC1F212}
GPOType         : GroupPolicyPreferences

GPODisplayName  : Add Workstation Admins to Local Administrators Group
GPOName         : {45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOPath         : \\lab.adsecurity.org\SysVol\lab.adsecurity.org\Policies\{45556105-EFE6-43D8-A92C-AACB1D3D4DE5}
GPOType         : RestrictedGroups
Filters         :
GroupName       : ADSECLAB\Workstation Admins
GroupSID        : S-1-5-21-1581655573-3923512380-696647894-2627
GroupMemberOf   : {S-1-5-32-544}
GroupMembers    : {}
```

```
(Empire: credentials/mimikatz/golden_ticket) > set CredID 1
(Empire: credentials/mimikatz/golden_ticket) > set user Administrator
(Empire: credentials/mimikatz/golden_ticket) > set sids S-1-5-21-456218688-4216621462-1491369290-519
(Empire: credentials/mimikatz/golden_ticket) > execute
(Empire: credentials/mimikatz/golden_ticket) >
Job started: Debug32_ktbrk
```

```
mimikatz # sekurlsa::pth /user:adsadministrator /ntl
user    : adsadministrator
domain  : lab.adsecurity.org
program : cmd.exe
impers. : no
NTLM    : 5164b7a0fda365d56739954bbbc23835
  |  PID  5600
  |  TID  3416
  |  LUID 0 ; 59149163 (00000000:03868b6b)
  \_ msv1_0   - data copy @ 0000006E8E970510 : OK !
  \_ kerberos - data copy @ 0000006E8E0971B8
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
```

```
meterpreter > use p
Loading extension p
meterpreter > power
[+] File successful
win-7ch5rt177ba\oj
False
```

```
Hostname: WINDOWS4.dev.testlab.local / S-1-5-21-4275052721-320508
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 23
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.co
 '## v ##'   http://blog.gentilkiwi.com/mimikatz              (oe.
  '#####'                                     with 16 modules * *

mimikatz(powershell) # kerberos::golden /domain:dev.testlab.local
:8b7c904343e530c4f81c53e8f614caf7 /sids:S-1-5-21-456218688-421662
User      : Administrator
Domain    : dev.testlab.local
SID       : S-1-5-21-4275052721-3205085442-2770241942
User Id   : 500
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiIOCau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL
#Super@Secure&Password$2015?
```

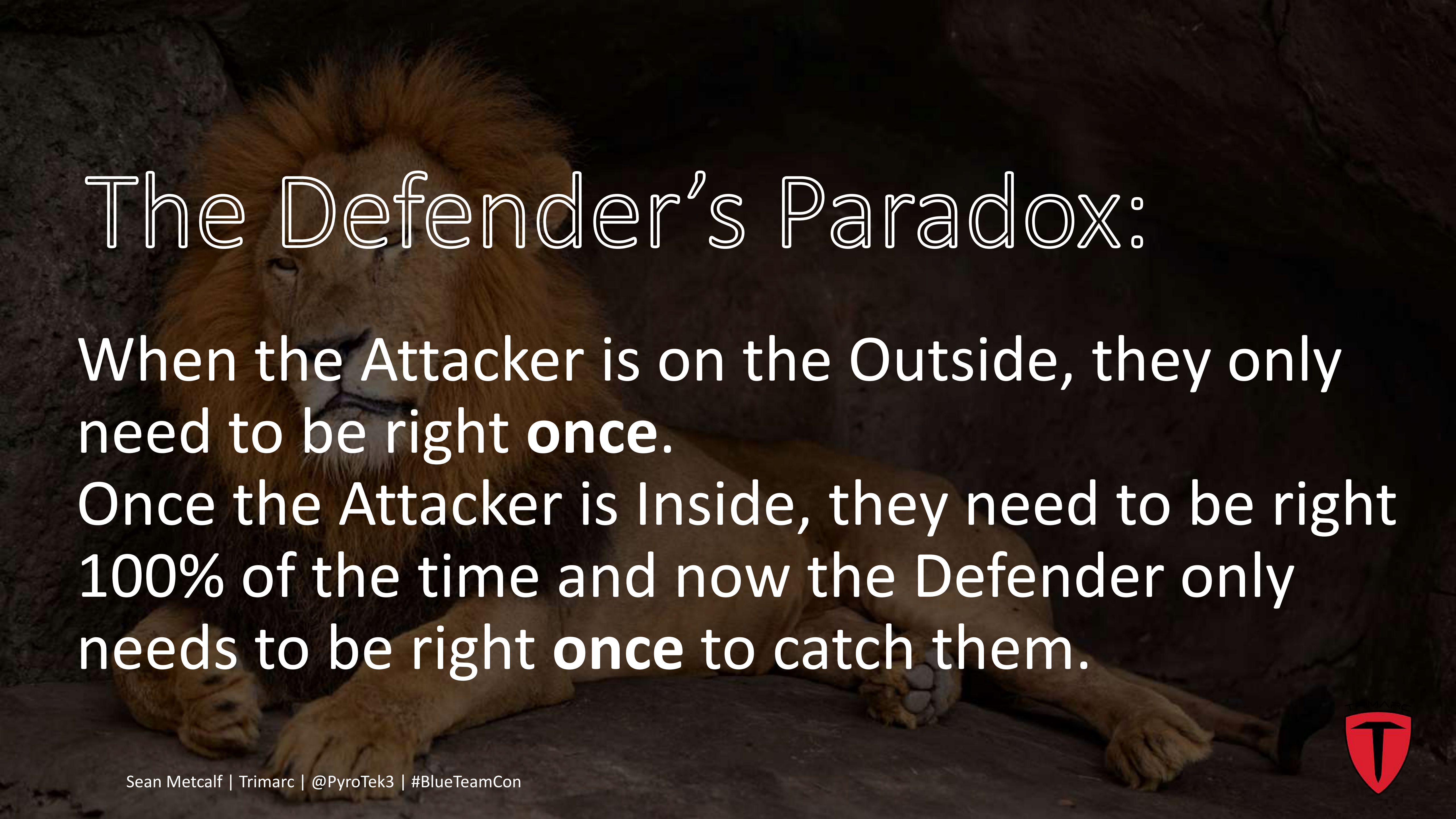
Table Mountain National Park
Warning
Please look under your vehicle for penguins
South African
NATIONAL PARKS

Jim Lawrence
kootenayreflections.com

Sean Metcalf | Trimarc | @PyroTek3 | #BlueTeamCon

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

FALSE



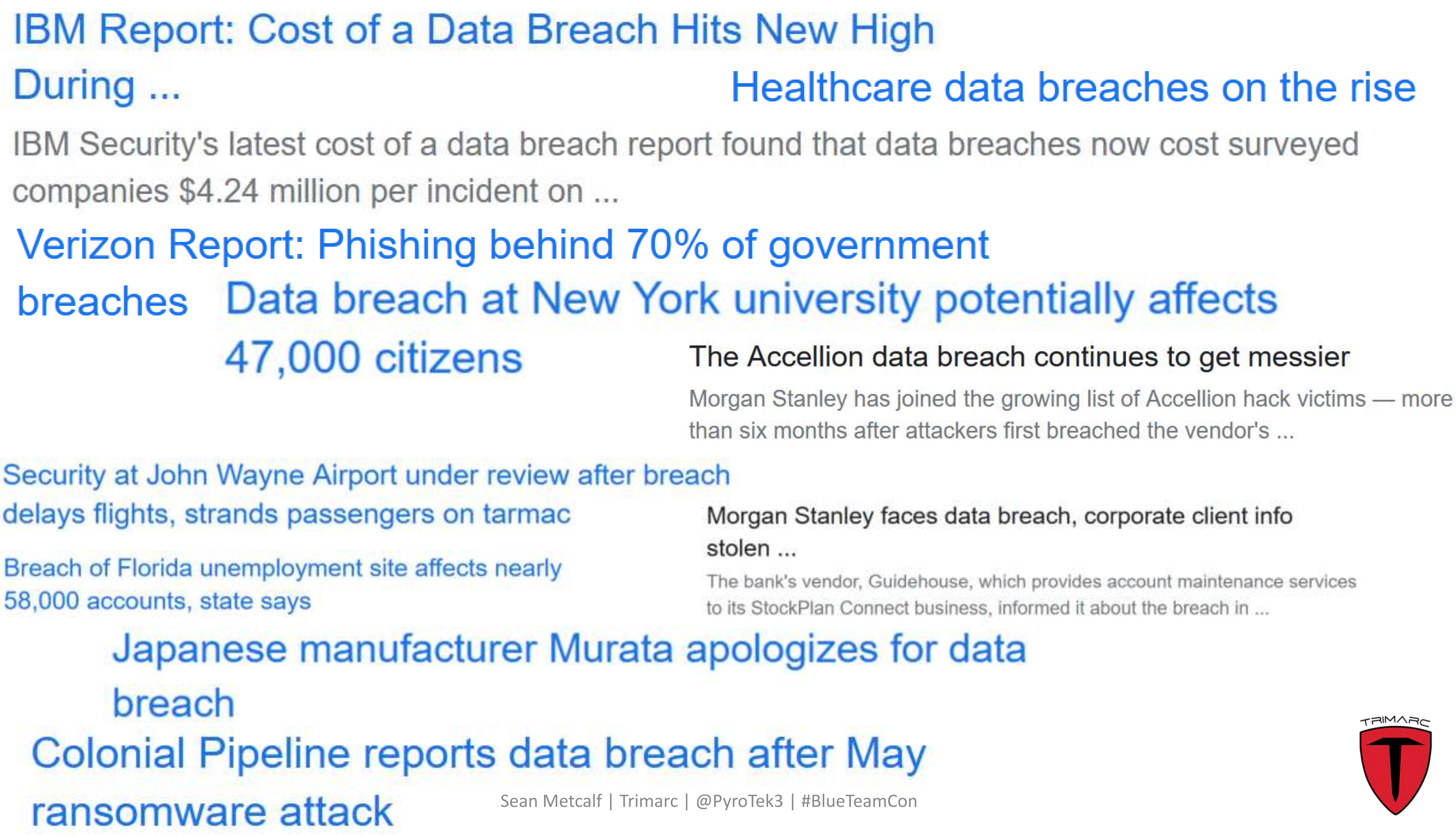
The Defender’s Paradox:

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



IBM Report: Cost of a Data Breach Hits New High During ...

IBM Security's latest cost of a data breach report found that data breaches now cost surveyed companies $4.24 million per incident on ...

Healthcare data breaches on the rise

Verizon Report: Phishing behind 70% of government breaches

Data breach at New York university potentially affects 47,000 citizens

The Accellion data breach continues to get messier

Morgan Stanley has joined the growing list of Accellion hack victims — more than six months after attackers first breached the vendor's ...

Security at John Wayne Airport under review after breach delays flights, strands passengers on tarmac

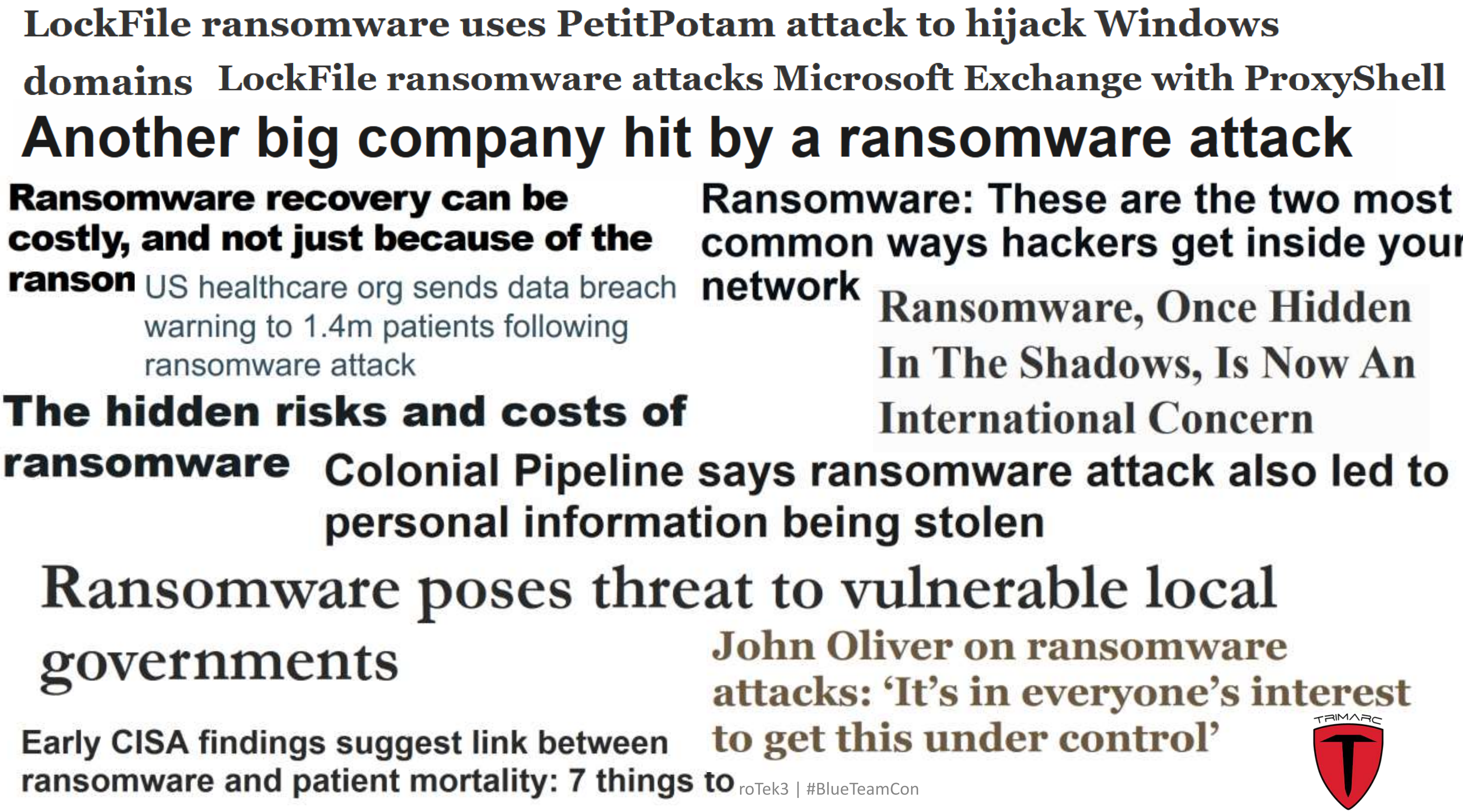
Breach of Florida unemployment site affects nearly 58,000 accounts, state says

Morgan Stanley faces data breach, corporate client info stolen ...

The bank's vendor, Guidehouse, which provides account maintenance services to its StockPlan Connect business, informed it about the breach in ...

Japanese manufacturer Murata apologizes for data breach

Colonial Pipeline reports data breach after May ransomware attack



LockFile ransomware uses PetitPotam attack to hijack Windows domains

LockFile ransomware attacks Microsoft Exchange with ProxyShell

Another big company hit by a ransomware attack

Ransomware recovery can be costly, and not just because of the ranson

US healthcare org sends data breach warning to 1.4m patients following ransomware attack

Ransomware: These are the two most common ways hackers get inside you network

Ransomware, Once Hidden In The Shadows, Is Now An International Concern

The hidden risks and costs of ransomware

Colonial Pipeline says ransomware attack also led to personal information being stolen

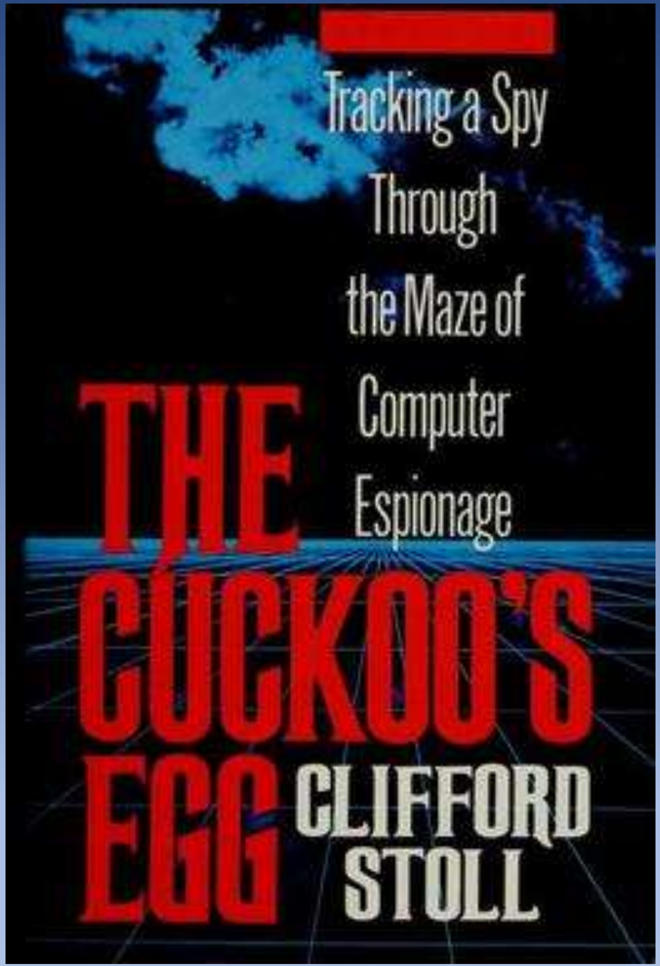
Ransomware poses threat to vulnerable local governments

John Oliver on ransomware attacks: 'It's in everyone's interest to get this under control'

Early CISA findings suggest link between ransomware and patient mortality: 7 things to

TRIMARC

Why Are We Here?



Let’s Go Back In Time… to the 80s

https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)

Let’s Go Back In Time… to the 80s

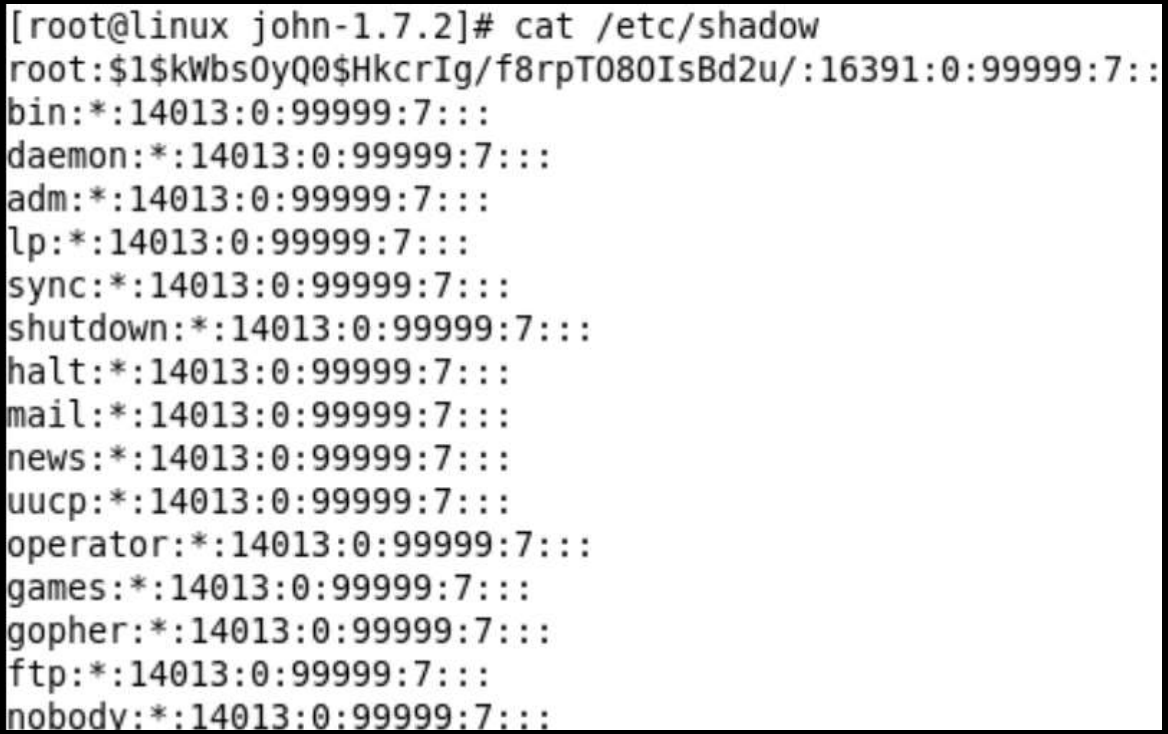
https://berkeleylabnext90.lbl.gov/celebrate-the-past/photo-gallery/#1980s

It started with 9 seconds

The Computer Terminal & Modem Days

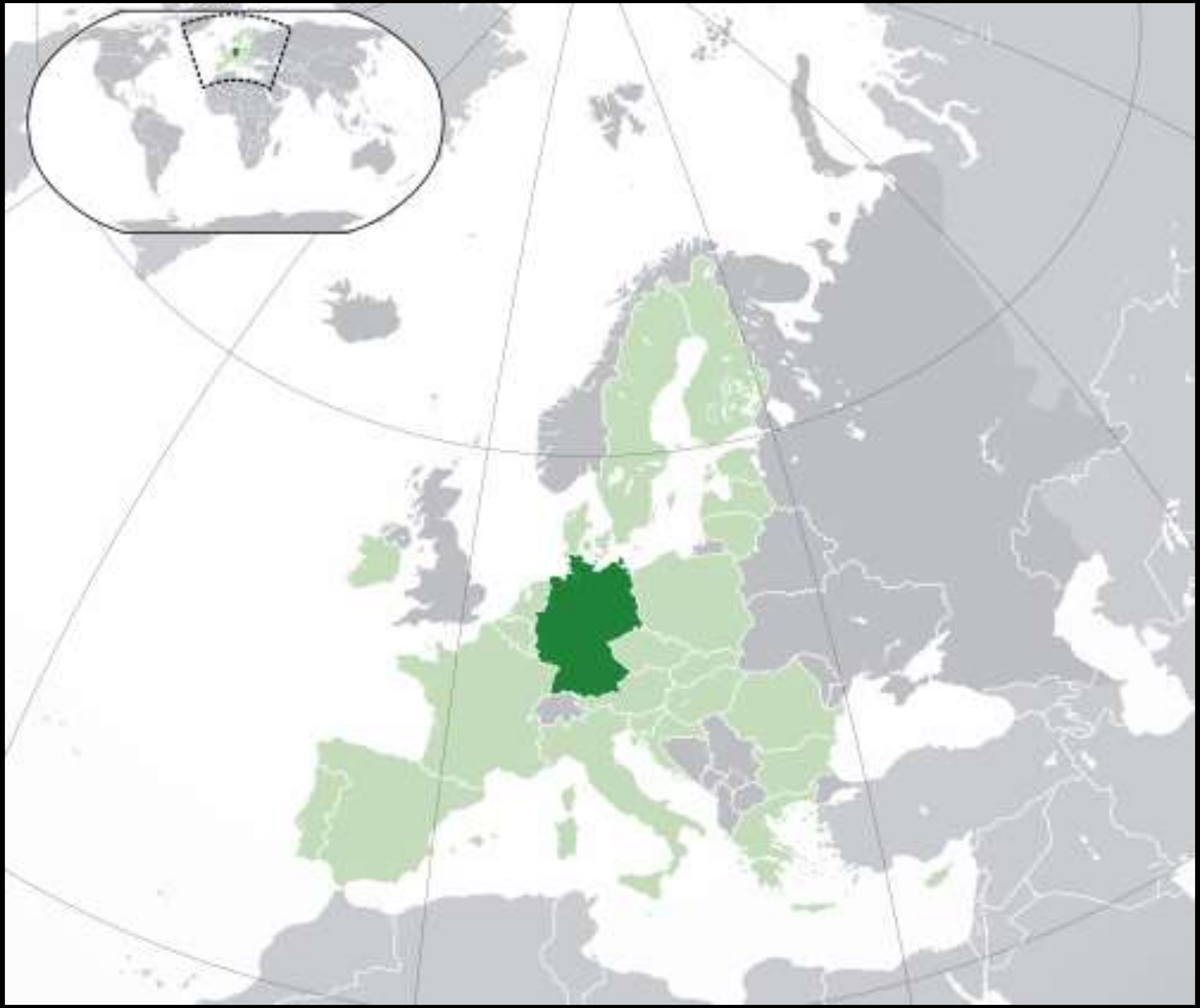
https://en.wikipedia.org/wiki/Teleprinter

Attacker Access & Persistence



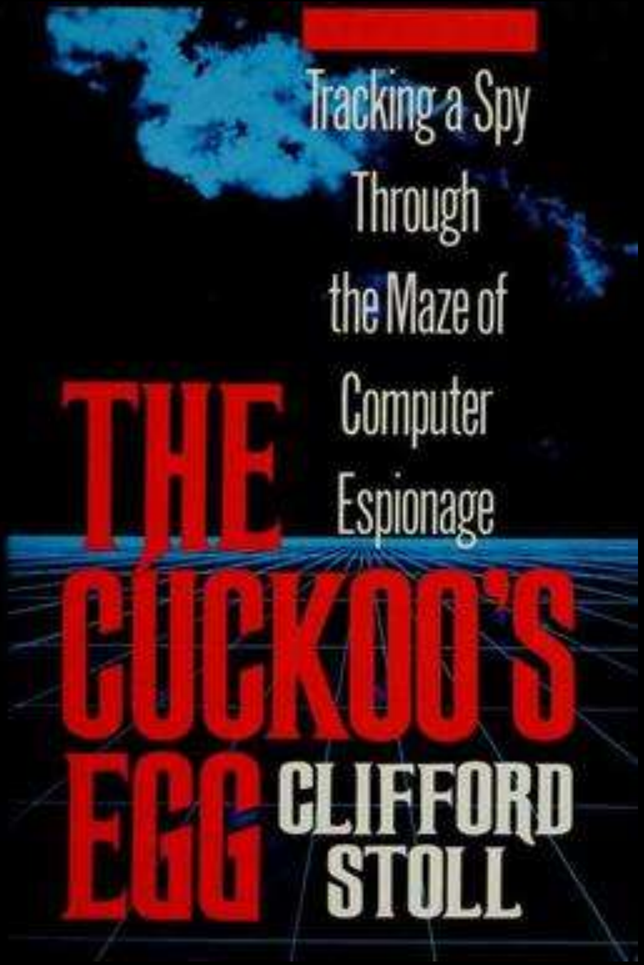
```
[root@linux john-1.7.2]# cat /etc/shadow
root:$1$kWbsOyQ0$HkcrIg/f8rpTO8OIsBd2u/:16391:0:99999:7::
bin:*:14013:0:99999:7:::
daemon:*:14013:0:99999:7:::
adm:*:14013:0:99999:7:::
lp:*:14013:0:99999:7:::
sync:*:14013:0:99999:7:::
shutdown:*:14013:0:99999:7:::
halt:*:14013:0:99999:7:::
mail:*:14013:0:99999:7:::
news:*:14013:0:99999:7:::
uucp:*:14013:0:99999:7:::
operator:*:14013:0:99999:7:::
games:*:14013:0:99999:7:::
gopher:*:14013:0:99999:7:::
ftp:*:14013:0:99999:7:::
nobody:*:14013:0:99999:7:::
```

Germany



Creating an SDI Department

From Russia, with Love


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

The Red Team

*"In military wargaming, the **opposing force** (or OPFOR) **in a simulated conflict** may be referred to as a **red cell**, this is an interchangeable term for **red team**.*

The key theme is that the adversary (red team) leverages tactics, techniques, and equipment as appropriate to emulate the desired actor.

*The red team challenges operational planning by **playing the role of a mindful adversary**.*

In United States wargaming simulations, the U.S. force is always the blue team, and the opposing force is always the red team."

https://en.wikipedia.org/wiki/Red_team

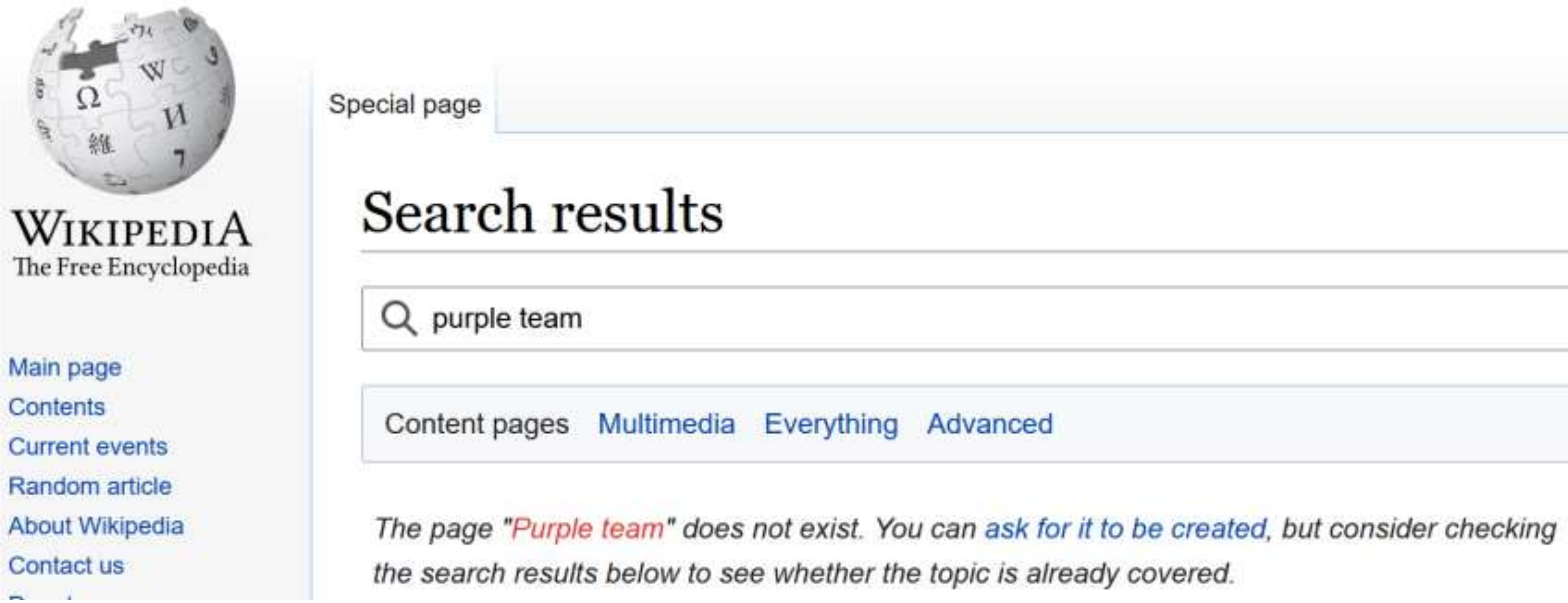
The Blue Team

"A blue team is a group of individuals who ***perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure,*** *and to* ***make certain all security measures will continue to be effective after implementation****."*

"As part of the United States computer security defense initiative, red teams were developed to exploit other malicious entities that would do them harm. As a result, ***blue teams were developed to design defensive measures against*** *such* ***red team activities****."*

https://en.wikipedia.org/wiki/Blue_team_(computer_security)

The Purple Team



Search results

purple team

The page "Purple team" does not exist. You can ask for it to be created, but consider checking the search results below to see whether the topic is already covered.

Red vs Blue

Photo by Ed Speir IV.
All Rights Reserved. Used with Permission.

Red vs Blue

Red vs Blue

Doing the same things for decades

Where Do I Belong in InfoSec?

Photo Credit: Sean Metcalf

Sean Metcalf | Trimarc | @PyroTek3 | #BlueTeamCon

What is a Hacker?

“an enthusiastic and skillful computer programmer or user”

Sean Metcalf | Trimarc | @PyroTek3 | #BlueTeamCon

Effective Defense Requires Understanding Offensive Techniques and Strategy

Now Hiring Entry Level Position in InfoSec, You Just Need…

2 PHDs (Doctor of Cybersecurity required)

15 years of Artificial Intelligence (AI)

25 years of Machine Learning (ML)

25 years of AWS experience

10 years of Kubernetes experience

3 Master degrees (infosec, cybersecurity, and computer security)

Buzzwords in the resume to get past initial gatekeeper system

From Operations to Security

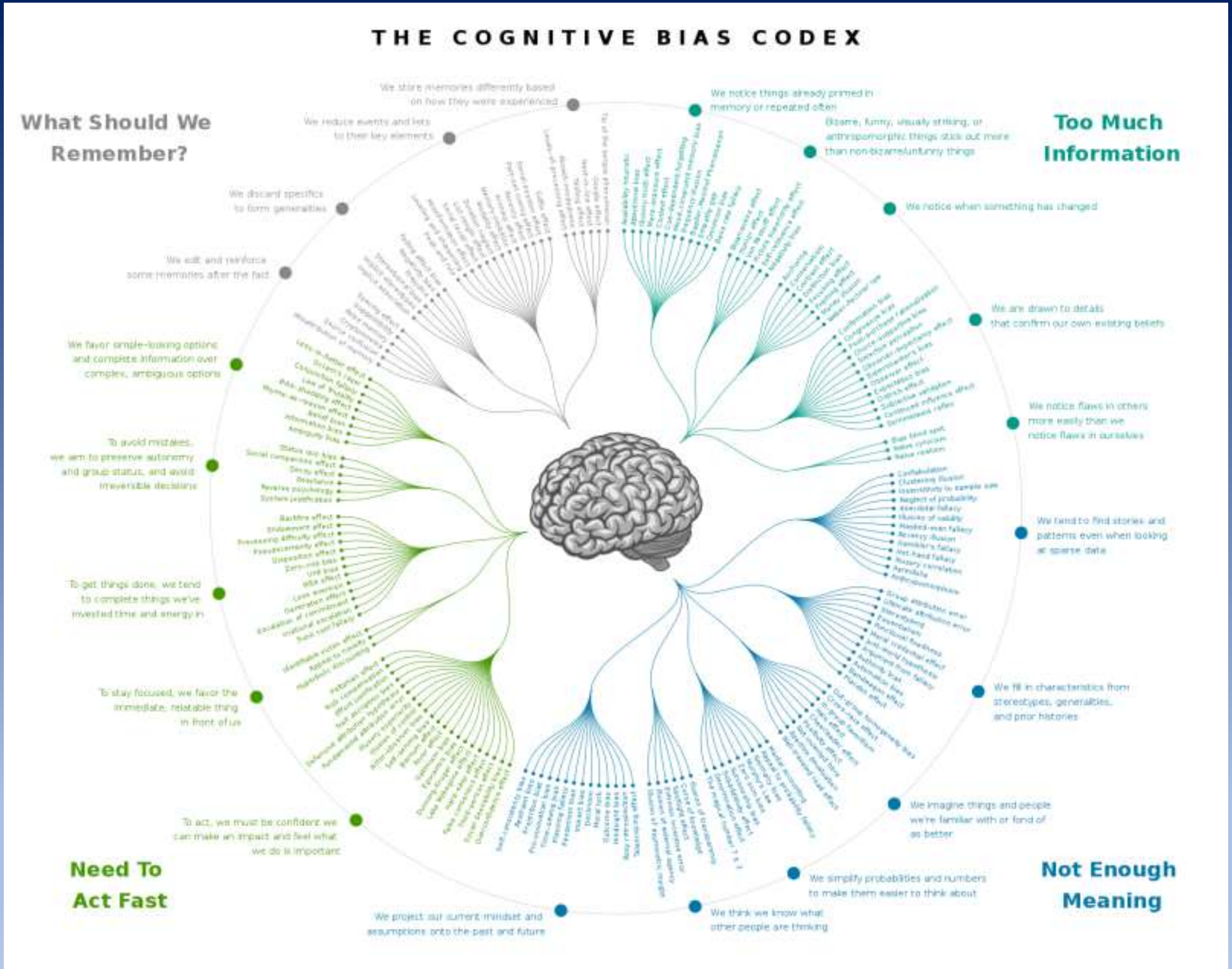
Certifications can help

If you have worked in operations in the past 5 to 10 years (+), you have likely done security work. Put that on your resume.

If you want to do security work, you can!

Companies Often Overlook Good Candidates

Job Hunting?
Take the time to improve your resume, it makes a huge difference!


THE COGNITIVE BIAS CODEX
What Should We Remember?
Too Much Information
Need To Act Fast
Not Enough Meaning
We store memories differently based on how they were experienced
We reduce events and lists to their key elements
We discard specifics to form generalities
We edit and reinforce some memories after the fact
We notice things already primed in memory or repeated often
Bizarre, funny, visually striking, or anthropomorphic things stick out more than non-bizarre/unfunny things
We notice when something has changed
We are drawn to details that confirm our own existing beliefs
We notice flaws in others more easily than we notice flaws in ourselves
We tend to find stories and patterns even when looking at sparse data
We fill in characteristics from stereotypes, generalities, and prior histories
We imagine things and people we're familiar with or fond of as better
We simplify probabilities and numbers to make them easier to think about
We think we know what other people are thinking
We project our current mindset and assumptions onto the past and future
To act, we must be confident we can make an impact and feel what we do is important
To stay focused, we favor the immediate, relatable thing in front of us
To get things done, we tend to complete things we've invested time and energy in
To avoid mistakes, we aim to preserve autonomy and group status, and avoid irreversible decisions
We favor simple-looking options and complete information over complex, ambiguous options

https://www.leeholmes.com/list-of-infosec-cognitive-biases/

InfoSec in Movies

Challenge: Over-Confidence

Mitigation: Over-confidence

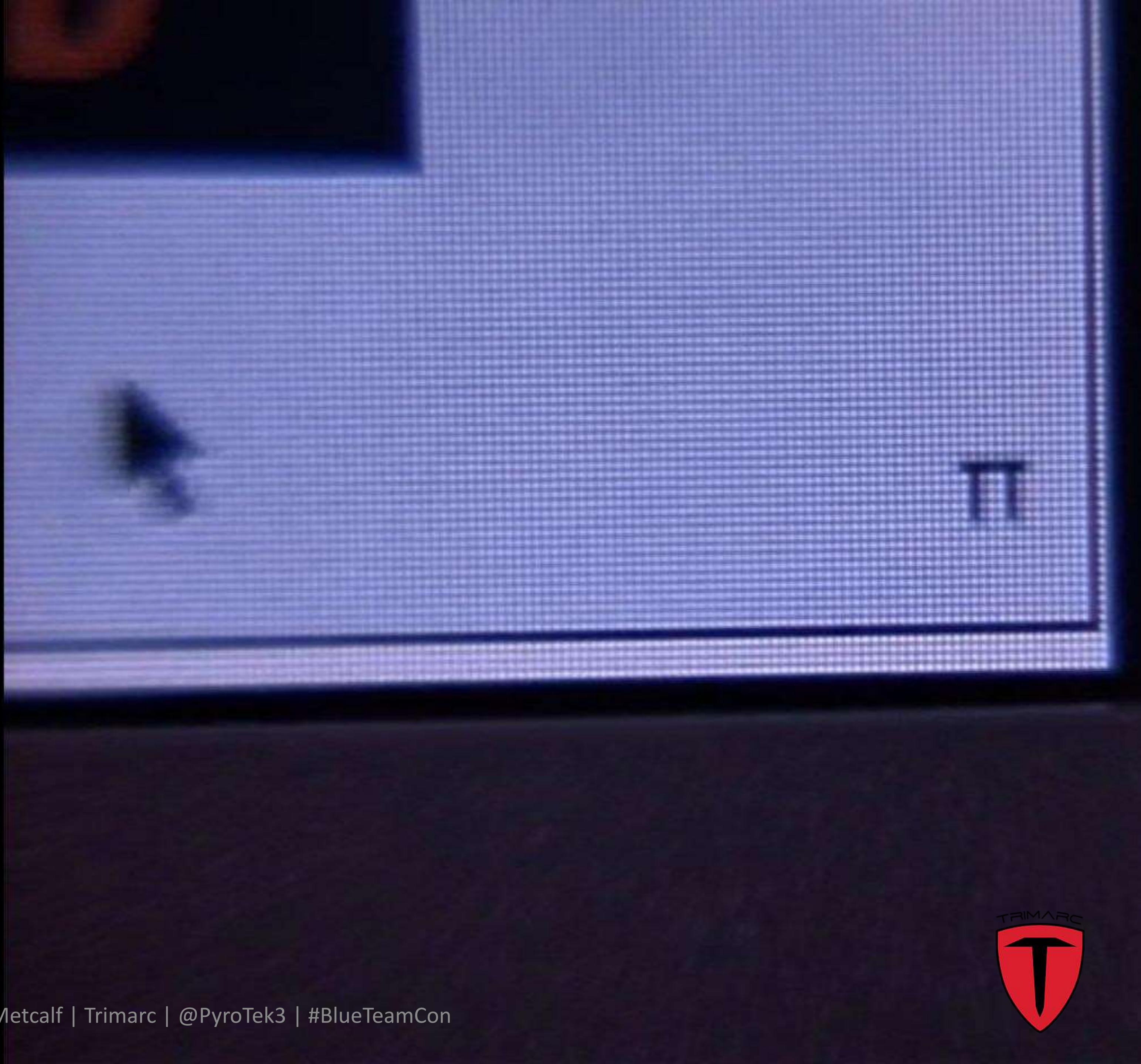
Assess	Realistically assess threats
Determine	Determine appropriate mitigation
Recognize	Recognize that perfect storms happen & prepare

Challenge: Assumptions

Mitigation: Assumptions

1. Challenge assumptions
2. Play devil's advocate (What if …?)
3. Yes, but what if you're wrong? (attackers take advantage of this)
4. Defense in depth is best

Challenge: Backdoors (ex. Solar Winds)



Solar Winds Rights

Domain Admin rights on AD (WMI access on DCs)

SYSADMIN on SQL

Read-only on Vmware
(was it only configured for read-only?)

Contributor or Reader on Azure

Instance rights on AWS

Config management on network devices (routers)

Global Admin on Azure AD / Office 365

Mitigation: Backdoors

- Difficult to detect supply chain attacks
- Perform appropriate threat modeling
- Identify weak spots
- **Limit vendor service account access**
- There is no silver bullet

Challenge: Technical Debt

Mitigation: Technical Debt

1

Identify all systems & applications that are out of support

2

Work to decommission & replace old systems (where possible)

3

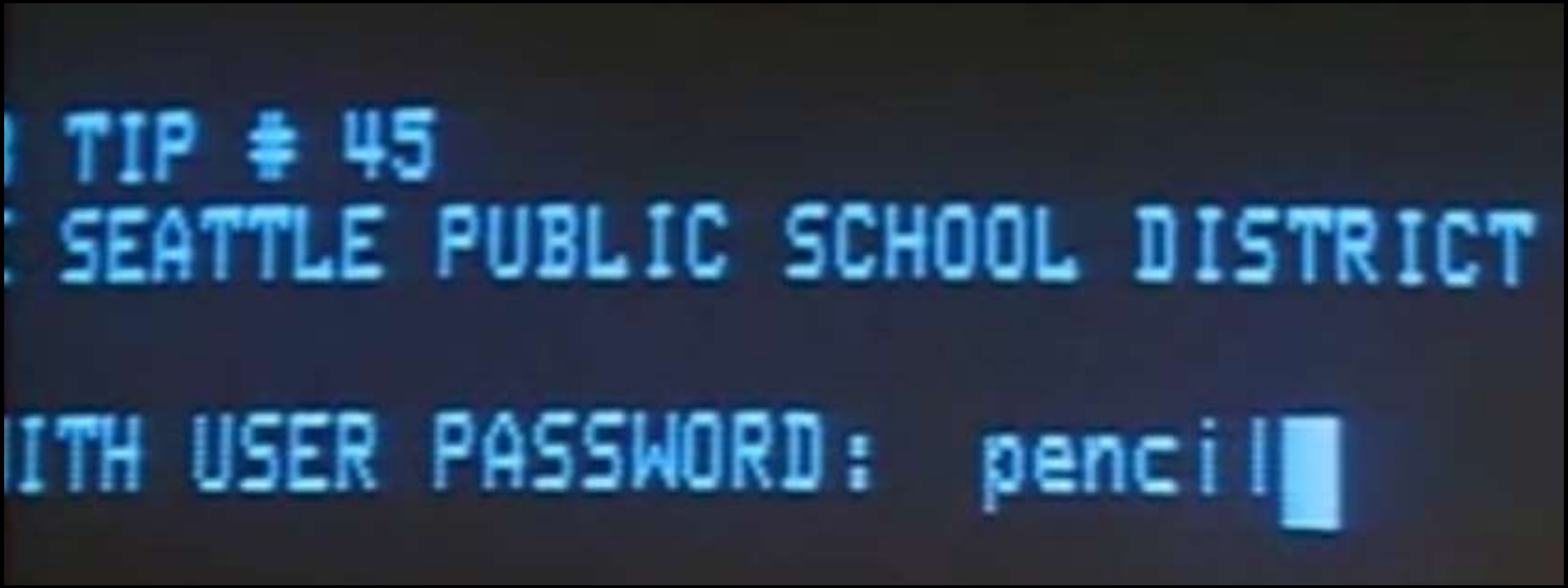
Identify methods to appropriately isolate old systems on the network

Challenge: Bad Passwords

1 2 3 4 5

Challenge: Bad Passwords

Challenge: Bad Passwords



```
 TIP # 45
 SEATTLE PUBLIC SCHOOL DISTRICT

ITH USER PASSWORD:  pencil
```

Mitigation: Bad Passwords

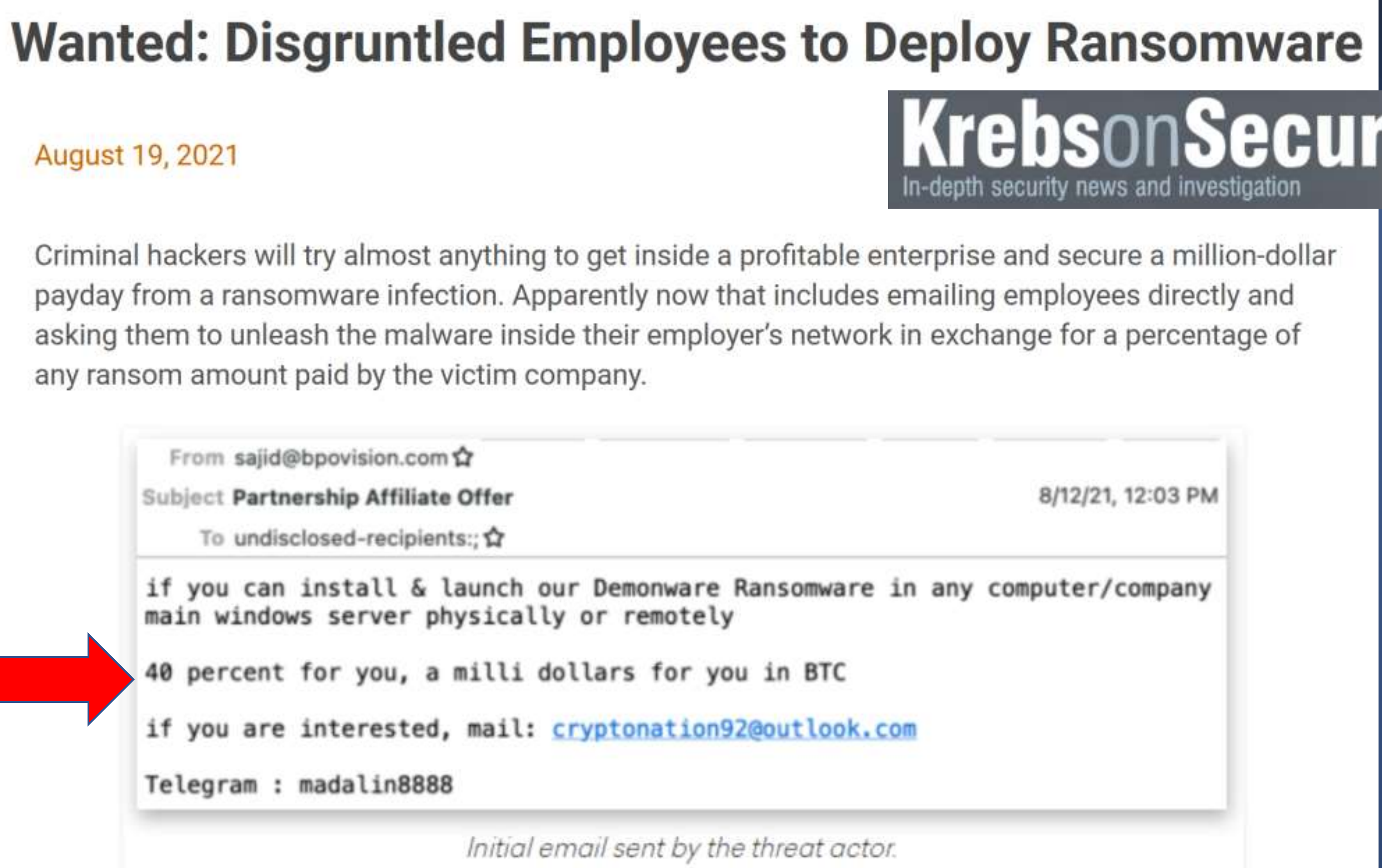
- Password filtering systems (Azure AD Password Protection)
- Longer passwords that change less frequently (14 character, changes every 1-2 years)
- NIST Special Publication 800-63B

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

Mitigations: Nation State, APTs, etc

- You are not likely being targeted by a nation-state
- But if you are, these still work!
- Focus on foundational security:
  - **Patching** (focus on critical & high priority vulns)
  - **System Inventory** (especially for sensitive systems)
  - **Principal of Least Privilege** (not everyone gets admin rights)
  - Appropriate **Event Auditing** (especially on DCs & sensitive systems)
  - **Logging & Alerting** – ensure you have visibility into what’s happening on workstations
  - **Isolating Privileged Credentials** (ensure that admin credentials are difficult to find & steal)
  - Leverage **Host-based Firewalls** to control traffic (pre-work for Zero Trust)

Challenge: Insider Threat



Wanted: Disgruntled Employees to Deploy Ransomware

KrebsonSecurity
In-depth security news and investigation

August 19, 2021

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.

From sajid@bpovision.com ☆
Subject Partnership Affiliate Offer 8/12/21, 12:03 PM
To undisclosed-recipients:; ☆

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```

Initial email sent by the threat actor.

https://krebsonsecurity.com/2021/08/wanted-disgruntled-employees-to-deploy-ransomware/

Mitigation: Insider Threat

- Code review & auditing
- 2-person approval of code push to production
- Audit log of activity & review for unusual activity (especially after hours)
- Process to report unusual behavior to security
- Special Logon (Windows Event)

Challenge: Social Engineering

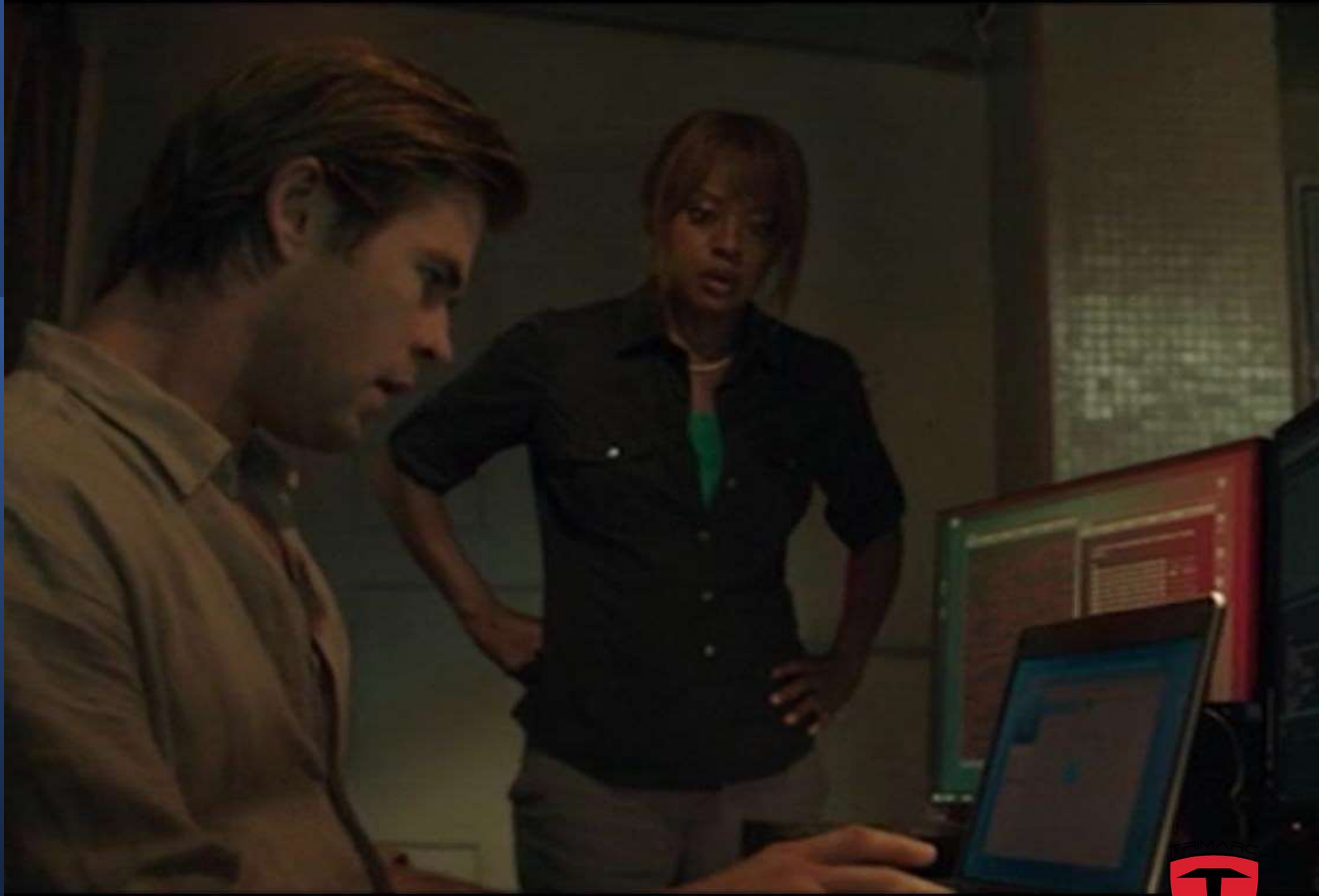
Challenge: Social Engineering

Mitigation: Social Engineering

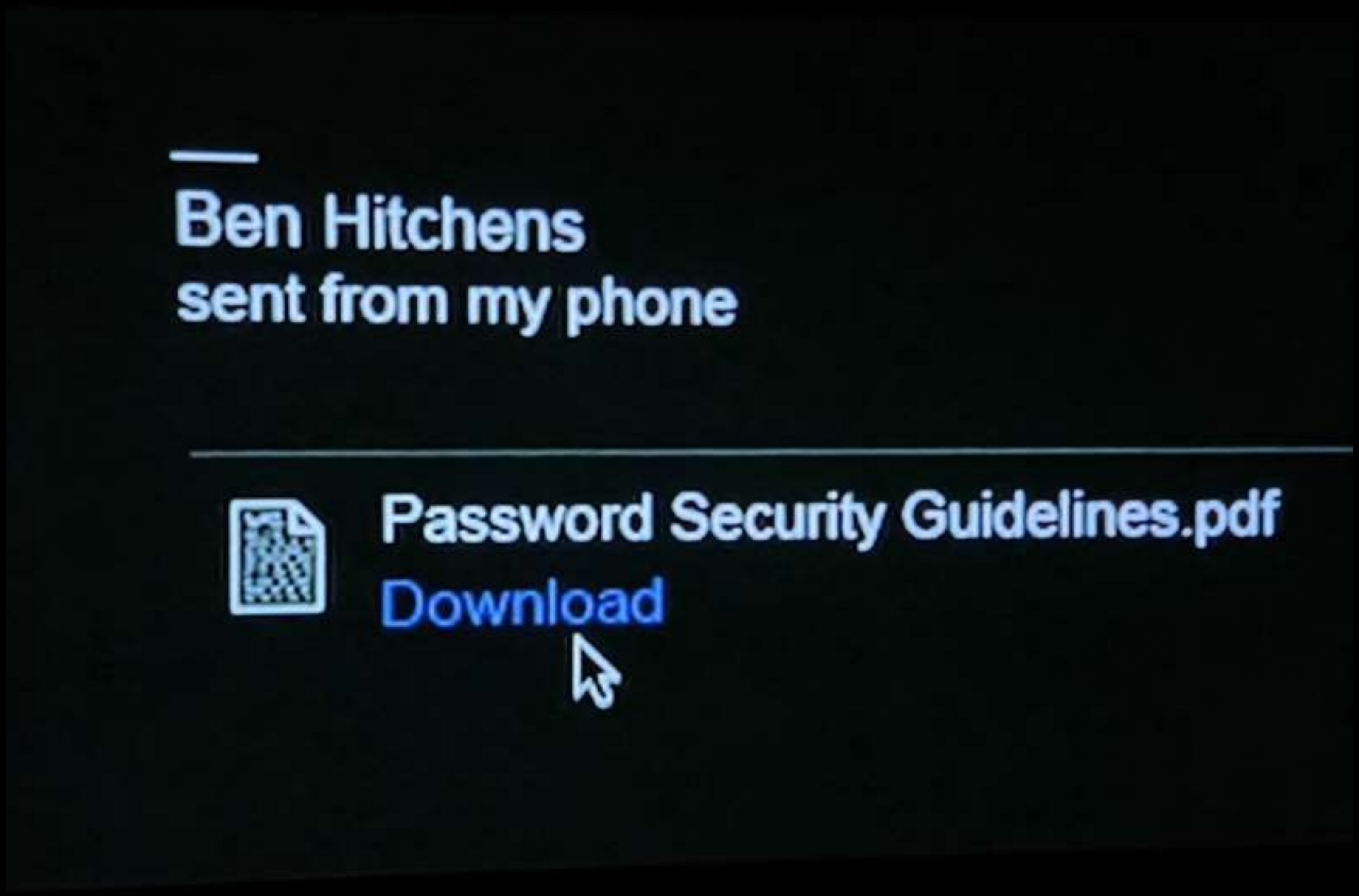
Train employees to report unusual activities.

Ensure everyone badges in and visitors require badges

Challenge: Phishing



Challenge: Phishing



Ben Hitchens
sent from my phone

Password Security Guidelines.pdf
Download

Mitigation: Phishing

Don’t blame users for clicking links – IT has trained users to click links!

Implement email security sandboxing capability.

Restrict email attachment & web downloads are appropriately filtered and scanned.

Limit access to external links in email (URL validation)

If phishing simulation is used, ensure that any “failures” result in additional phish training.

Ensure that users have an easy method to report suspected phishing email.

Challenge: Ransomware

Challenge: Ransomware

Challenge: Ransomware

Sean Metcalf | Trimarc | @PyroTek3 | #BlueTeamCon

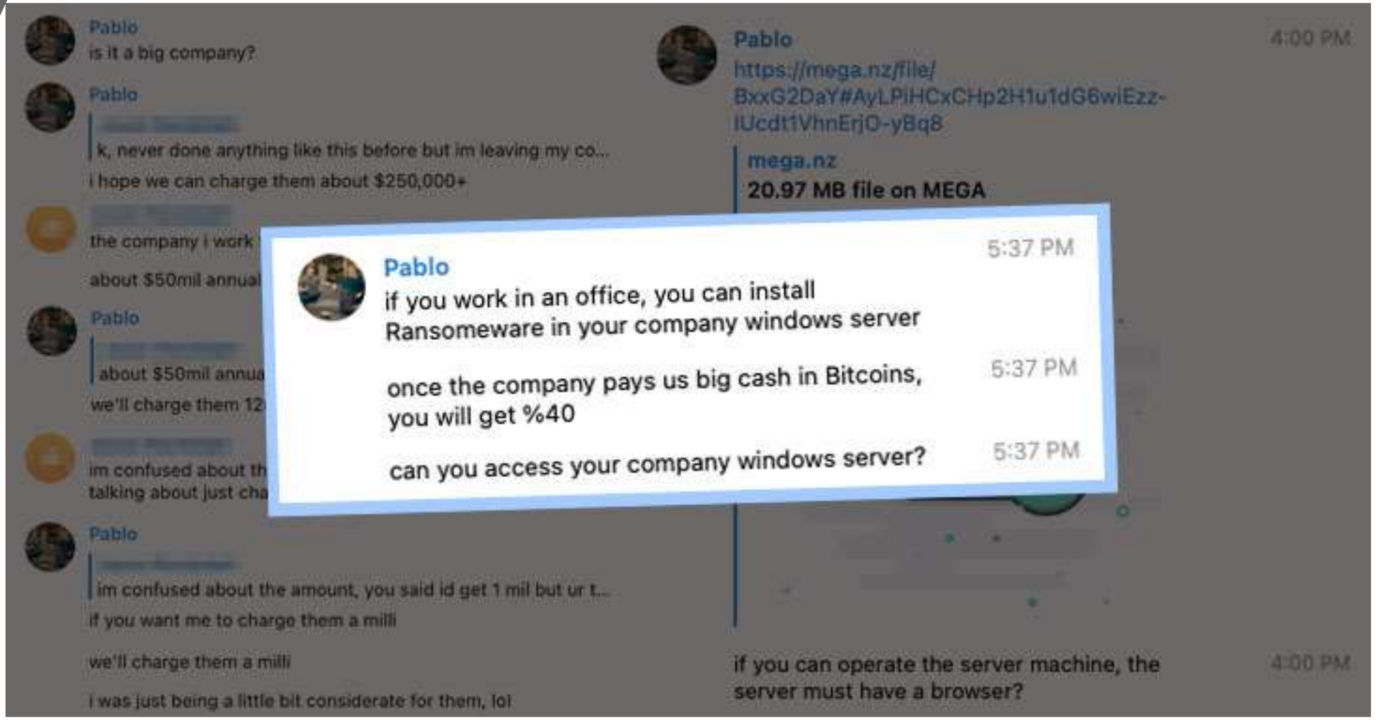
How Does Ransomware Typically Get In?

Phishing

Microsoft Remote Desktop Protocol (RDP) from Internet

Campaign emails company insiders and initially offers 1 million in Bitcoin if they install DemonWare on an organization's network.

Cybercrime Group Asking Insiders for Help in Planting Ransomware



Pablo
is it a big company?

Pablo
[redacted]
k, never done anything like this before but im leaving my co...
i hope we can charge them about $250,000+

[redacted]
the company i work

about $50mil annual

Pablo
[redacted]
about $50mil annua
we'll charge them 12

[redacted]
im confused about th
talking about just cha

Pablo
[redacted]
im confused about the amount, you said id get 1 mil but ur t...
if you want me to charge them a milli

we'll charge them a milli

i was just being a little bit considerate for them, lol

Pablo 5:37 PM
if you work in an office, you can install Ransomeware in your company windows server

once the company pays us big cash in Bitcoins, you will get %40 5:37 PM

can you access your company windows server? 5:37 PM

Pablo 4:00 PM
https://mega.nz/file/BxxG2DaY#AyLPiHCxCHp2H1u1dG6wiEzz-lUcdt1VhnErjO-yBq8
mega.nz
20.97 MB file on MEGA

if you can operate the server machine, the server must have a browser? 4:00 PM

https://thehackernews.com/2021/08/cybercrime-group-asking-insiders-for.html

Mitigation: Ransomware

- Ensure there are unique local Administrator passwords (Microsoft LAPS)
- Don’t let users have local admin rights (temporary access through agent)
- Prevent local accounts from authenticating over the network (GPO)
- Block SMB traffic between workstations (host-based firewall)
- Ensure AD Admins use admin workstations
- Improve Insider Threat Mitigation
- Perform regular backups (& store off-line when possible)

But What About…

Zero Trust?

0 chance

Microsoft Admin Tiering Model

Let’s get Tier 0 figured out first!

Network Segmentation

This is the long game…

Red Team

Are you ready?

More Security Boxes

easy

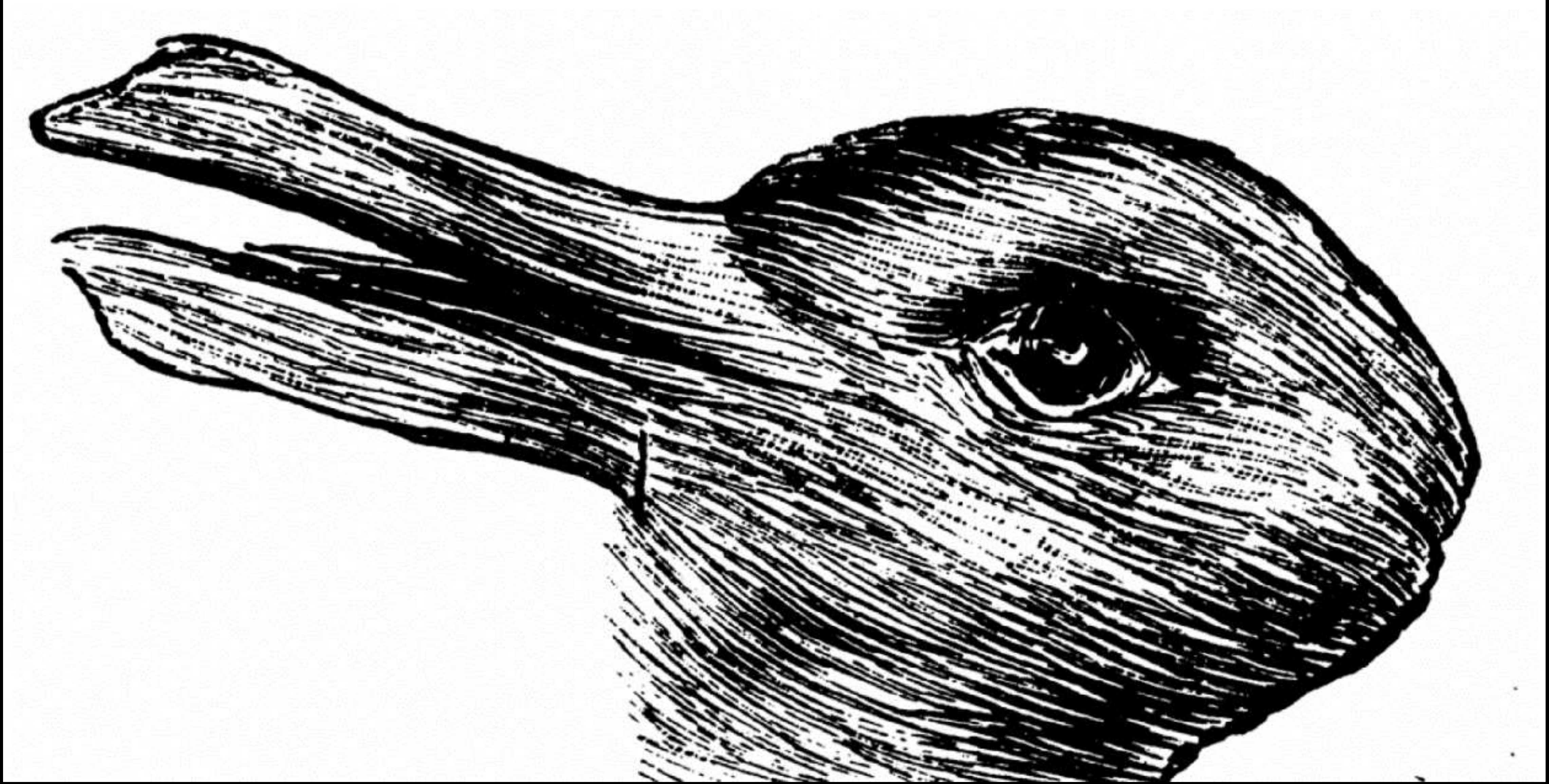
Basics aren’t always easy

Patching, asset inventory, logging & alerting, …
These are iterative, not one-offs

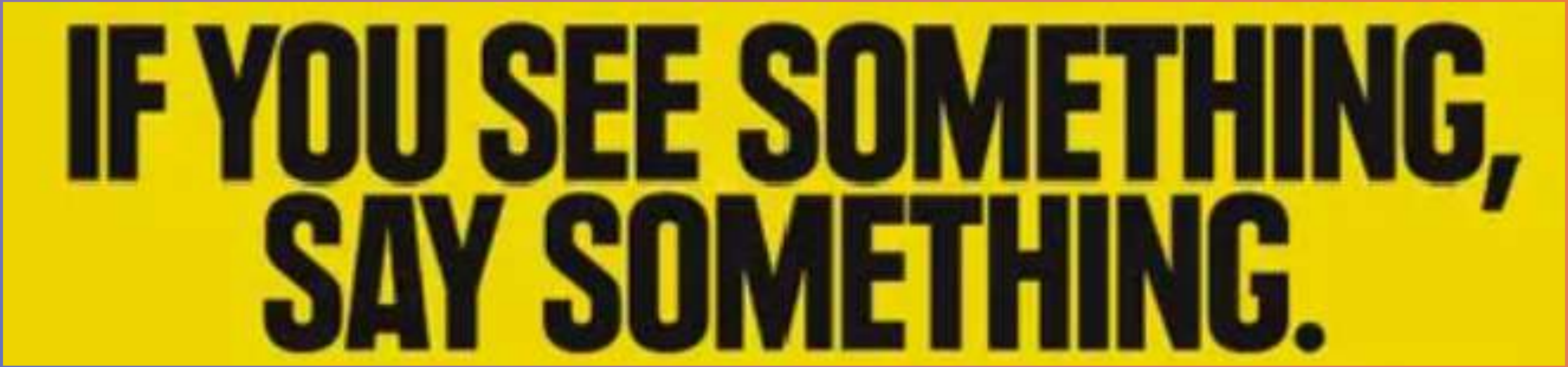
Everything Starts with Executive Buy-In

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

We Are ALL Part of The Blue Team



Likely Attacker?

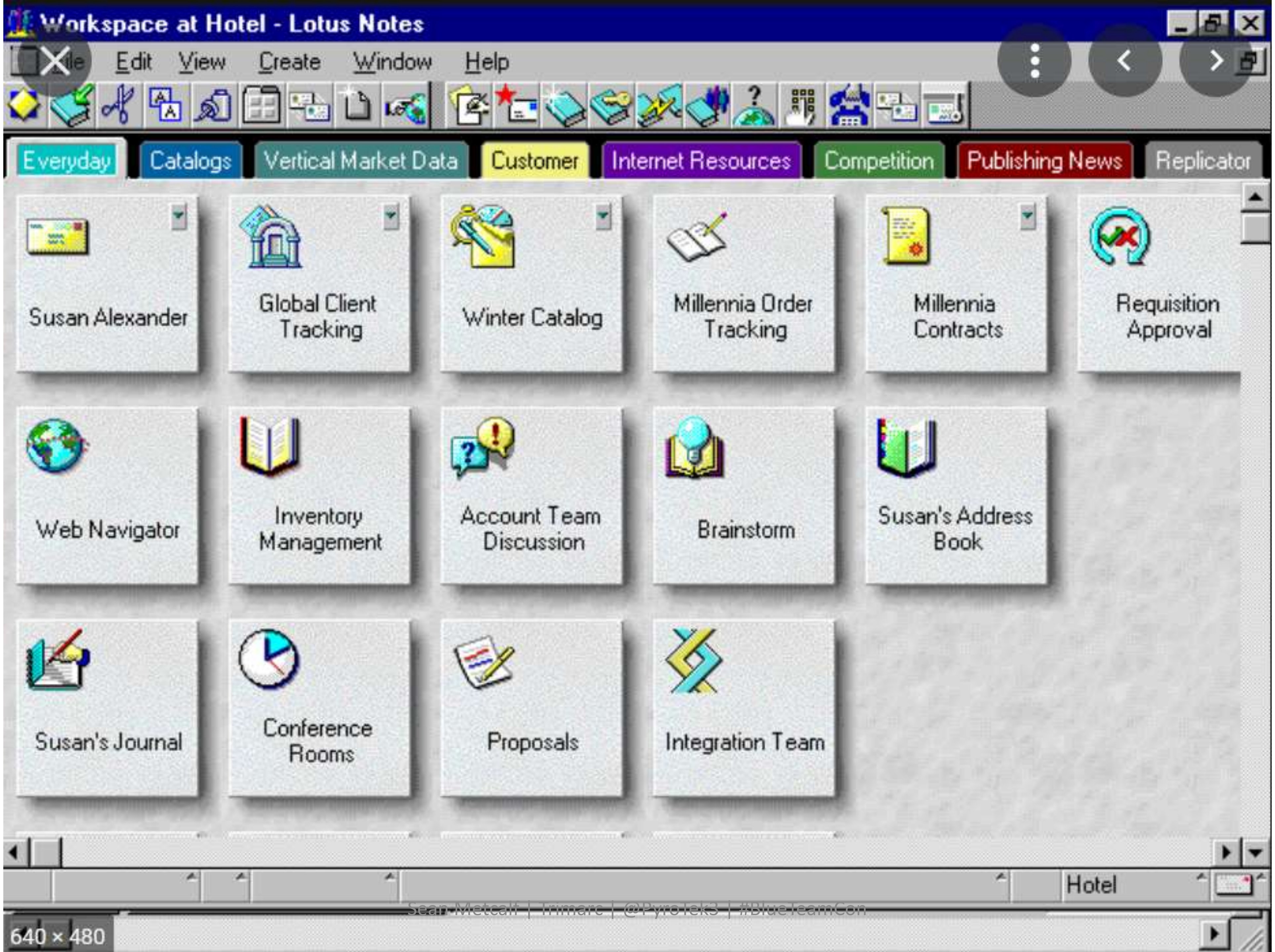


IF YOU SEE SOMETHING,
SAY SOMETHING.

Impostor Syndrome

Who am I…?

All the Adversary Needs is Access



Workspace at Hotel - Lotus Notes
File
Edit
View
Create
Window
Help
Everyday
Catalogs
Vertical Market Data
Customer
Internet Resources
Competition
Publishing News
Replicator
Susan Alexander
Global Client Tracking
Winter Catalog
Millennia Order Tracking
Millennia Contracts
Requisition Approval
Web Navigator
Inventory Management
Account Team Discussion
Brainstorm
Susan's Address Book
Susan's Journal
Conference Rooms
Proposals
Integration Team
Hotel
640 × 480

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 >5 years

-Voltaire

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

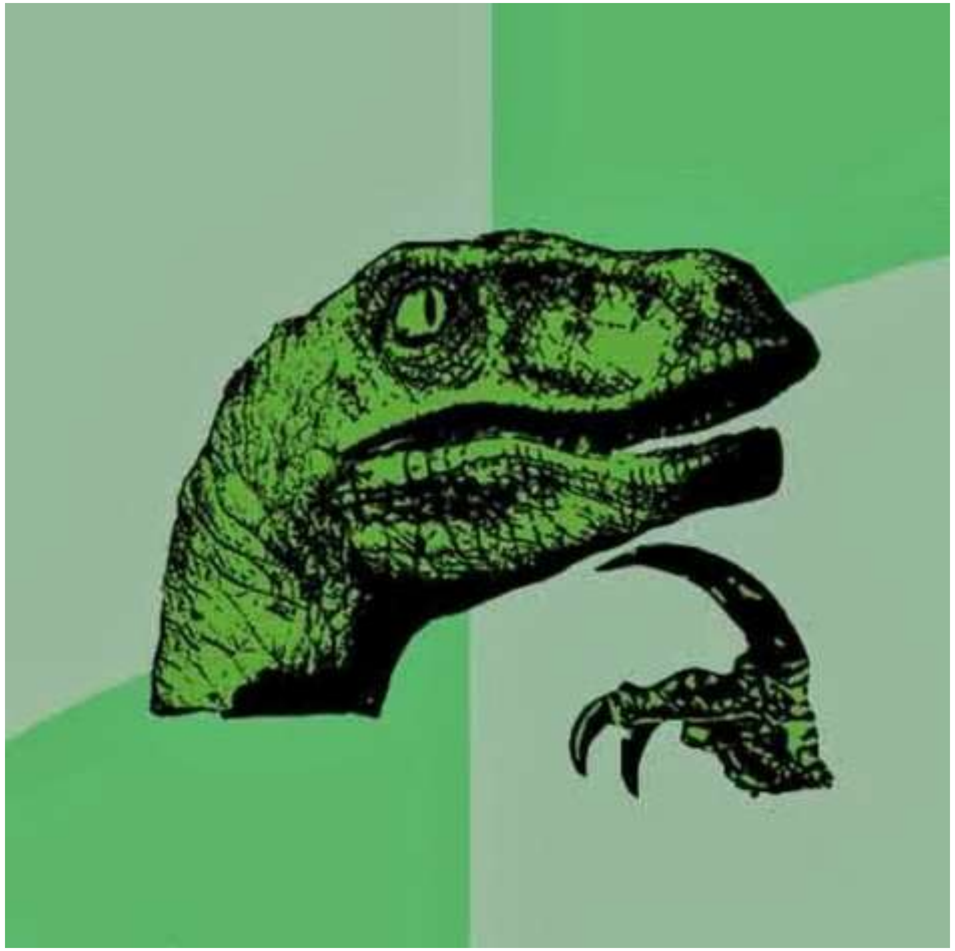
Twitter Blue Team (150+)

https://twitter.com/i/lists/1430231620968226820?s=20

@_dirkjan
@_wald0
@0gtweet
@4n6lady
@aboutsecurity
@alexchantavy
@andregironda
@anton_chuvakin
@Antonlovesdnb
@ateixei
@austinjmurphy
@bad_packets
@bl4ckh0l3z
@BlackMatter23
@BleepinComputer
@blubbfiction
@blueteamblog
@brakesec
@campuscodi
@CCrowMontance
@Centurion
@cglyer
@chrissanders88
@CISAJen
@cnoanalysis

- @Cyb3rMonk
- @cyb3rops
- @Cyb3rPandaH
- @Cyb3rWard0g
- @DanielGallagher
- @darktracer_int
- @DavidJBianco
- @DebugPrivilege
- @DefensiveDepth
- @dez_
- @DfirDiva
- @DFIRmadness
- @DidierStevens
- @divinetechygirl
- @domchell
- @dougburks
- @DrAzureAD
- @dreadphones
- @duff22b
- @el_d33
- @eric_capuano
- @eric_conrad
- @EricRZimmerman
- @ErikVaBu
- @executemalware
- @fabian_bader
- @FrankMcG
- @FrodeHommedal
- @FuzzySec
- @gentilkiwi
- @GossiTheDog
- @grifter801
- @h2jazi
- @hackerxbella
- @hacks4pancakes
- @harmj0y
- @harshbothra_
- @hasherezade
- @HeirhabarovT
- @Hexacorn
- @iagox86
- @iHeartMalware
- @ImposeCost
- @InfoSec_Pom
- @InfoSystir
- @ionstorm
- @ItsReallyNick
- @James_inthe_box
- @JAMESWT_MHT
- @jaredcatkinson
- @JBizzle703
- @jeffmcjunkin
- @jessysaurusrex
- @jfslowik
- @jhencinski
- @JohnLaTwC
- @jonasLyk
- @jorgeorchilles
- @jsecurity101
- @KimZetter
- @kyleehmke
- @kylerankin
- @Lee_Holmes
- @likethecoins
- @LitMoose
- @lorenzofb
- @M_haggis
- @malware_traffic
- @MalwareJake
- @malwrhunterteam
- @markaorlando
- @markmorow
- @mattblaze
- @mattifestation
- @mattnotmax
- @MITREattack
- @MSAdministrator
- @muteki_rtw
- @mvelazco
- @n0x08
- @nas_bench
- @NathanMcNulty
- @neu5ron
- @NicoleBeckwith
- @nullcookies
- @obilodeau
- @olafhartong
- @OrOneEqualsOne
- @PhilippeDeRyck
- @piffey
- @pmelson
- @pyrotek3
- @rickastley
- @rimpq
- @rj_chap
- @rodtrent
- @rootsecdev
- @rrcyrus
- @SadProcessor
- @samilamppu
- @SantasaloJoosua
- @sbousseaden
- @ScoubiMtl
- @sec_soup
- @SecHubb
- @securelyfitz
- @SecurityMapper
- @securityonion
- @shortxstack
- @sS55752750
- @SteveBellovin
- @SteveD3
- @stevesyfuhs
- @strandjs
- @stvemillertime
- @subTee
- @svch0st
- @SwiftOnSecurity
- @t_gidwani
- @TactiKoolSec
- @taviso
- @TheDFIRReport
- @TheHackersNews
- @therealwlambert
- @thijslecomte
- @Thomas_Live
- @threathuntergrl
- @tiraniddo
- @uuallan
- @VK_Intel
- @yugoslavskiy

Conclusion



- We need you to help make things better.
- In InfoSec, things change weekly (sometimes daily!)
- Focus on what positive impact you can make
- Ignore what you *could* be doing and do what you think you *should*

Slides: Hub.TrimarcSecurity.com

https://twitter.com/i/lists/1430231620968226820?s=20

Sean Metcalf (@PyroTek3)
sean @ Trimarc Security . com
www.ADSecurity.org
TrimarcSecurity.com