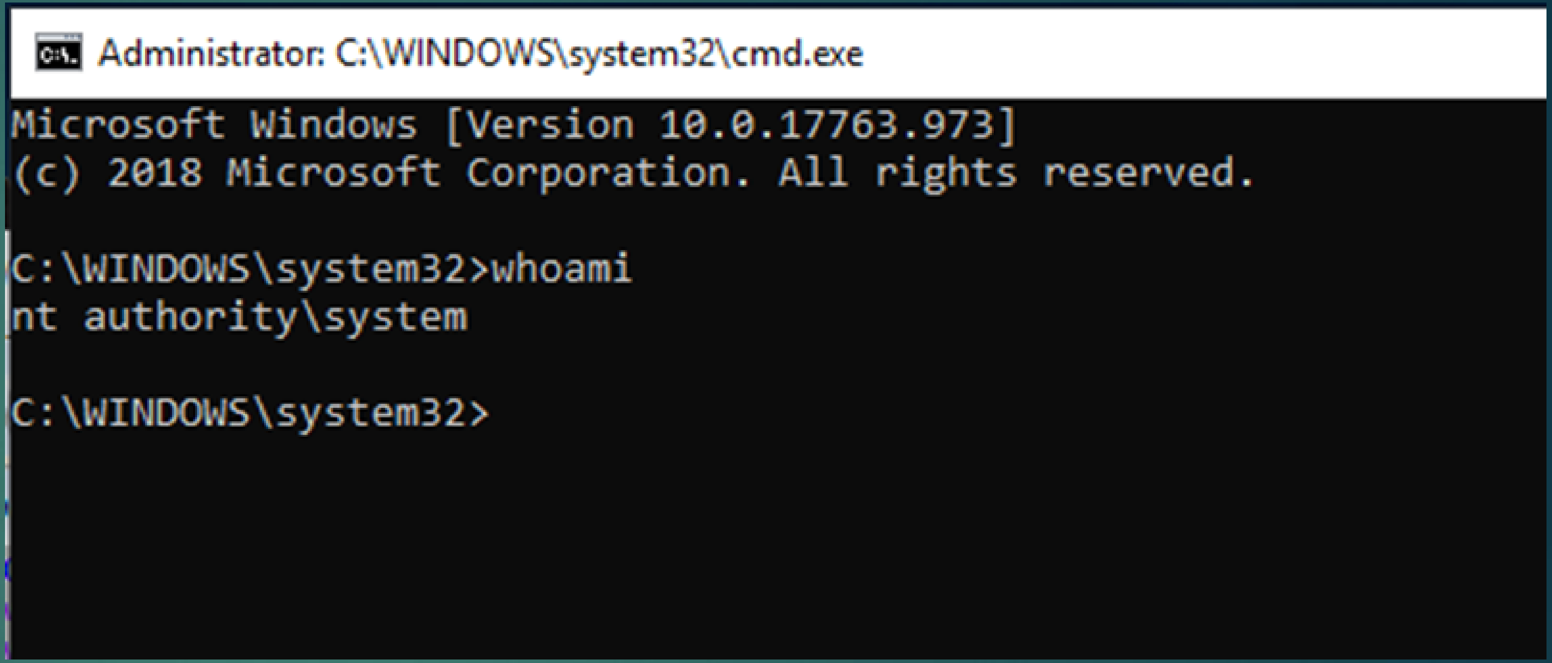
Keeping up with the Jones’s and other APT threats

CALGARY B-SIDES NOV 2020

Whoami

- 33 Years in IT
- 22 Years in Security
- Blue Team, GSWN
- ArcSight, Splunk
- Father, Hockey Coach, Security geek, Otaku, Logs, Sysmon, Blue Team
- @JockStrapp2

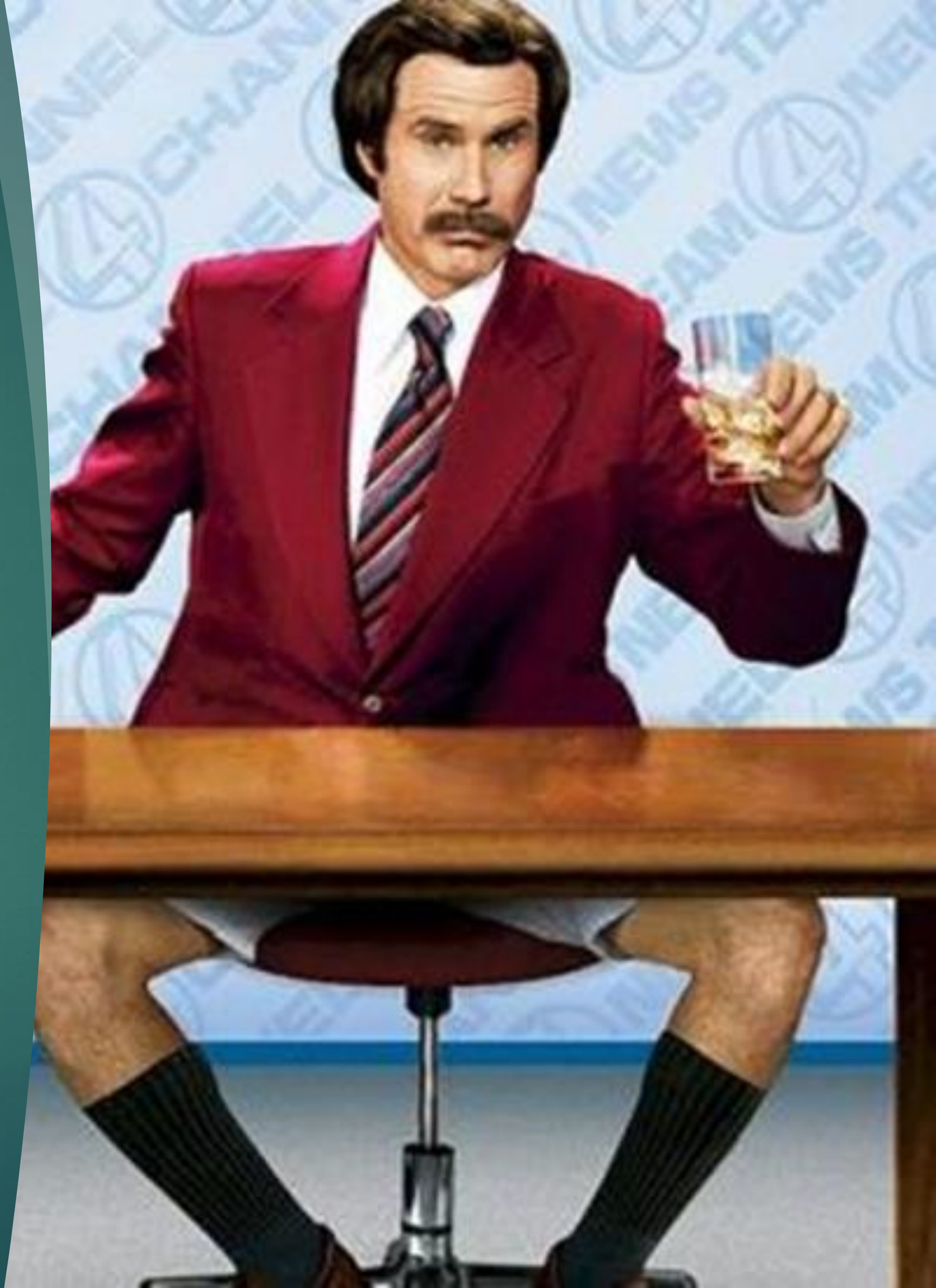


```
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system

C:\WINDOWS\system32>
```

`Sysmon` User="NT AUTHORITY\\SYSTEM" Image="C:\\Windows\\System32\\whoami.exe"

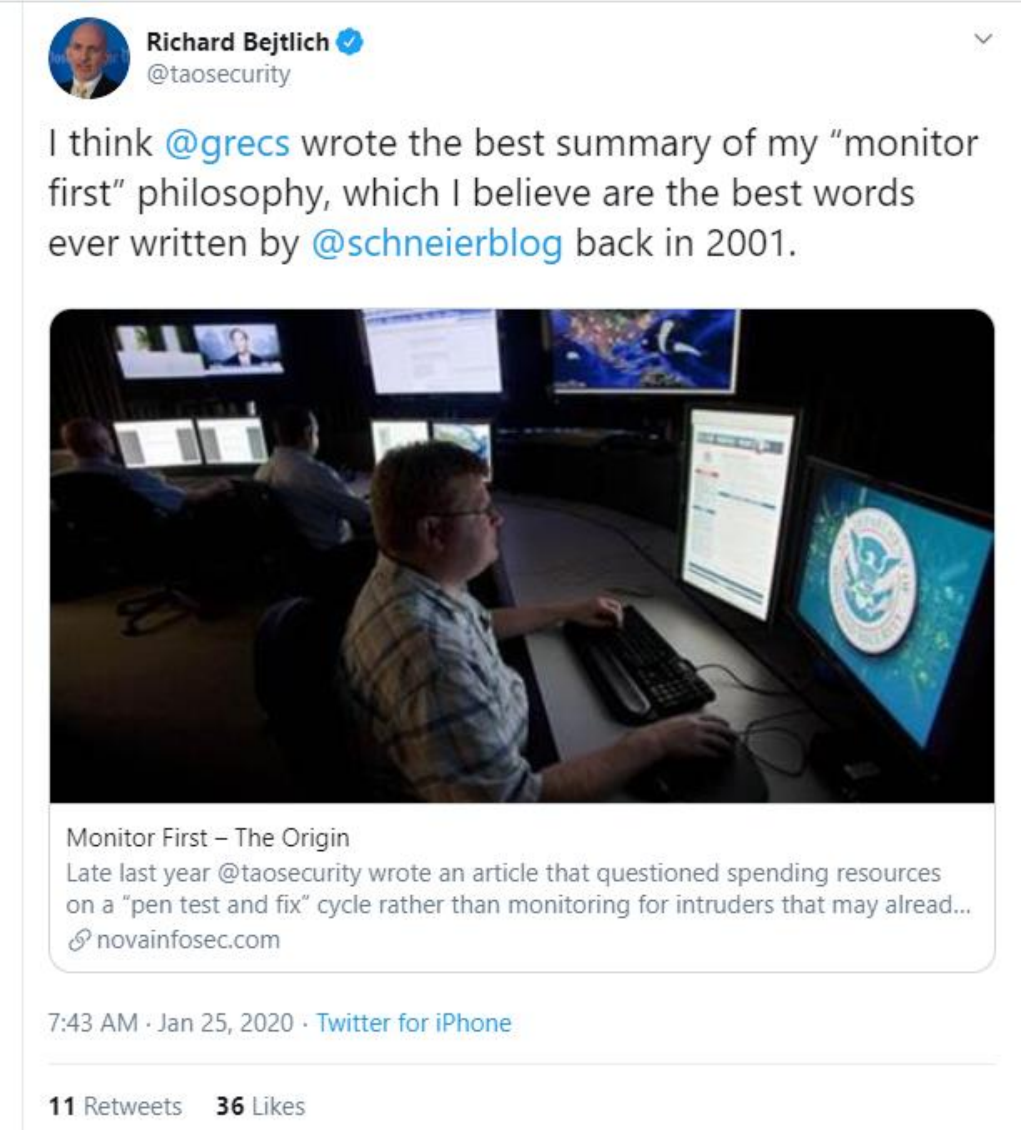
Agenda

- Monitor first Paradigm
- Responding to CVE's
- Patching
- How data moves in your environment
- Attribution and forensics matter
- Places you will go



Monitor First paradigm

- https://www.novainfosec.com/2015/06/25/monitor-first-the-origin/
- How does a CIO know what security products to install, and whether they are working
- It's something that a network administrator can do today to provide immediate value.
- Permits them to establish baseline metrics from which they can measure improvements
- Can establish real risk



Richard Bejtlich
@taosecurity

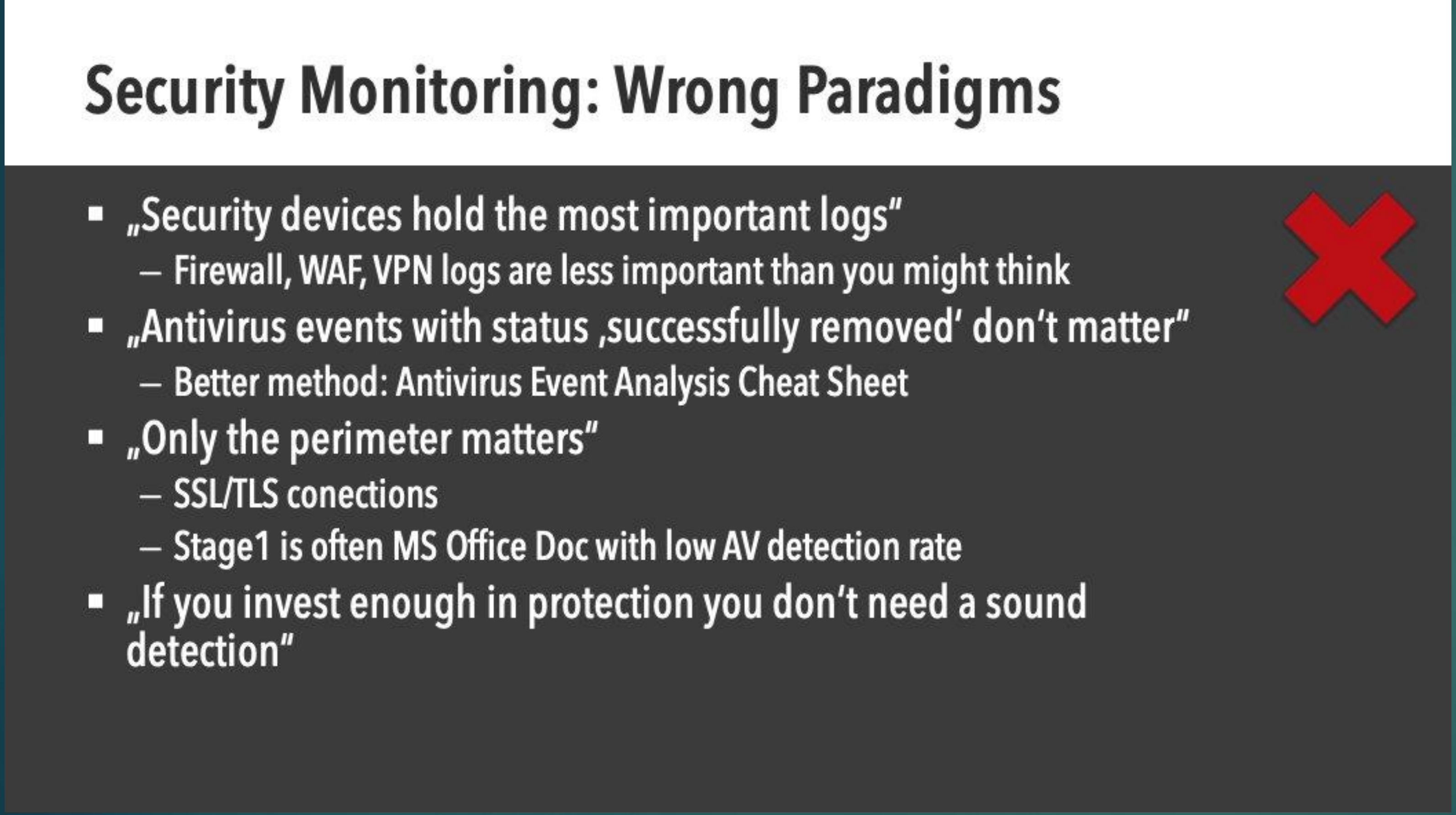
I think @grecs wrote the best summary of my "monitor first" philosophy, which I believe are the best words ever written by @schneierblog back in 2001.

Monitor First – The Origin
Late last year @taosecurity wrote an article that questioned spending resources on a "pen test and fix" cycle rather than monitoring for intruders that may alread...
novainfosec.com

7:43 AM · Jan 25, 2020 · Twitter for iPhone

11 Retweets 36 Likes

Security monitoring



Security Monitoring: Wrong Paradigms

- „Security devices hold the most important logs"
  - Firewall, WAF, VPN logs are less important than you might think
- „Antivirus events with status ‚successfully removed' don't matter"
  - Better method: Antivirus Event Analysis Cheat Sheet
- „Only the perimeter matters"
  - SSL/TLS conections
  - Stage1 is often MS Office Doc with low AV detection rate
- „If you invest enough in protection you don't need a sound detection"

Monitoring Best Values

- Whoami /system
- Logs cleared
- WDigest Changes
- Cmd, Powershell usage
- Applocker Application Whitelisting, DLL monitoring
- WDAC, ASR
- RDP HiJack
- Net Commands
- 5 Critical Process in 10 minutes
- Application Crashes
- East West traffic

"Perfect is the enemy of good"

-Voltaire

Monitoring Best Values

- Explicit Credential logon EventCode 4648
- LSASS process access/File Created
- Accounts created
- New Task/Service
- New Process and then connection outbound
- Macros run
- WMI consumers
- System crashes
- Windows Sethc utilman
- User logon multiple hosts

Monitoring Best Values

- Mitre Attack Matrix
- Kill Chain
- Autoruns
- Check every binary against Virus Total

Emergency Phone Not Installed
Please Do Not Have An Emergency At This Location

Tools

- Sysmon
- https://github.com/olafhartong/sysmon-modular
- Splunk free trial
- Splunk Security Essentials
- Threat Hunting App for Splunk (Olaf Hartong)
- Virus Total Integration
  - https://github.com/kinkster/bsides
- Autoruns (uses Plantir AutorunsToWinEventLog)
  - https://github.com/palantir/windows-event-forwarding
- https://github.com/clong/DetectionLab

You Retweeted

SwiftOnSecurity @SwiftOnSecurity · May 22

If you haven't played with Sysmon, literally takes minutes to grab it and load my rule-set, I guarantee you you'll see something cool.

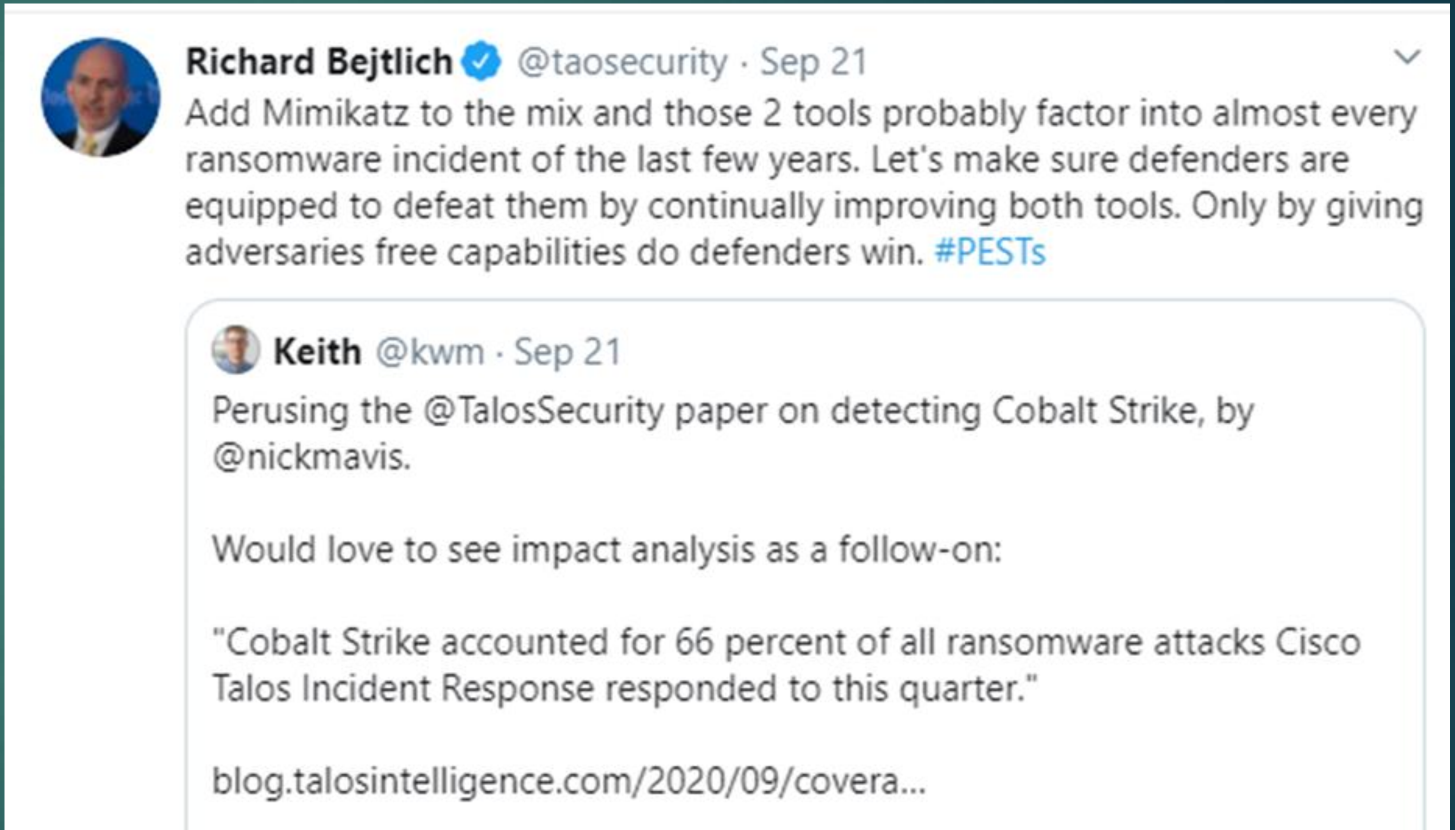
Kevin Beaumont @GossiTheDog

Fun with @SwiftOnSecurity's Sysmon configs on SMB Eternal* honeypot. It catches lsass.exe writing out files during EternalBlue exploit.

10 147 405

Monitoring Examples

- PowerShell to detect Cobalt Strike
- Mimikatz



Richard Bejtlich @taosecurity · Sep 21

Add Mimikatz to the mix and those 2 tools probably factor into almost every ransomware incident of the last few years. Let's make sure defenders are equipped to defeat them by continually improving both tools. Only by giving adversaries free capabilities do defenders win. #PESTs

> **Keith** @kwm · Sep 21
>
> Perusing the @TalosSecurity paper on detecting Cobalt Strike, by @nickmavis.
>
> Would love to see impact analysis as a follow-on:
>
> "Cobalt Strike accounted for 66 percent of all ransomware attacks Cisco Talos Incident Response responded to this quarter."
>
> blog.talosintelligence.com/2020/09/covera...

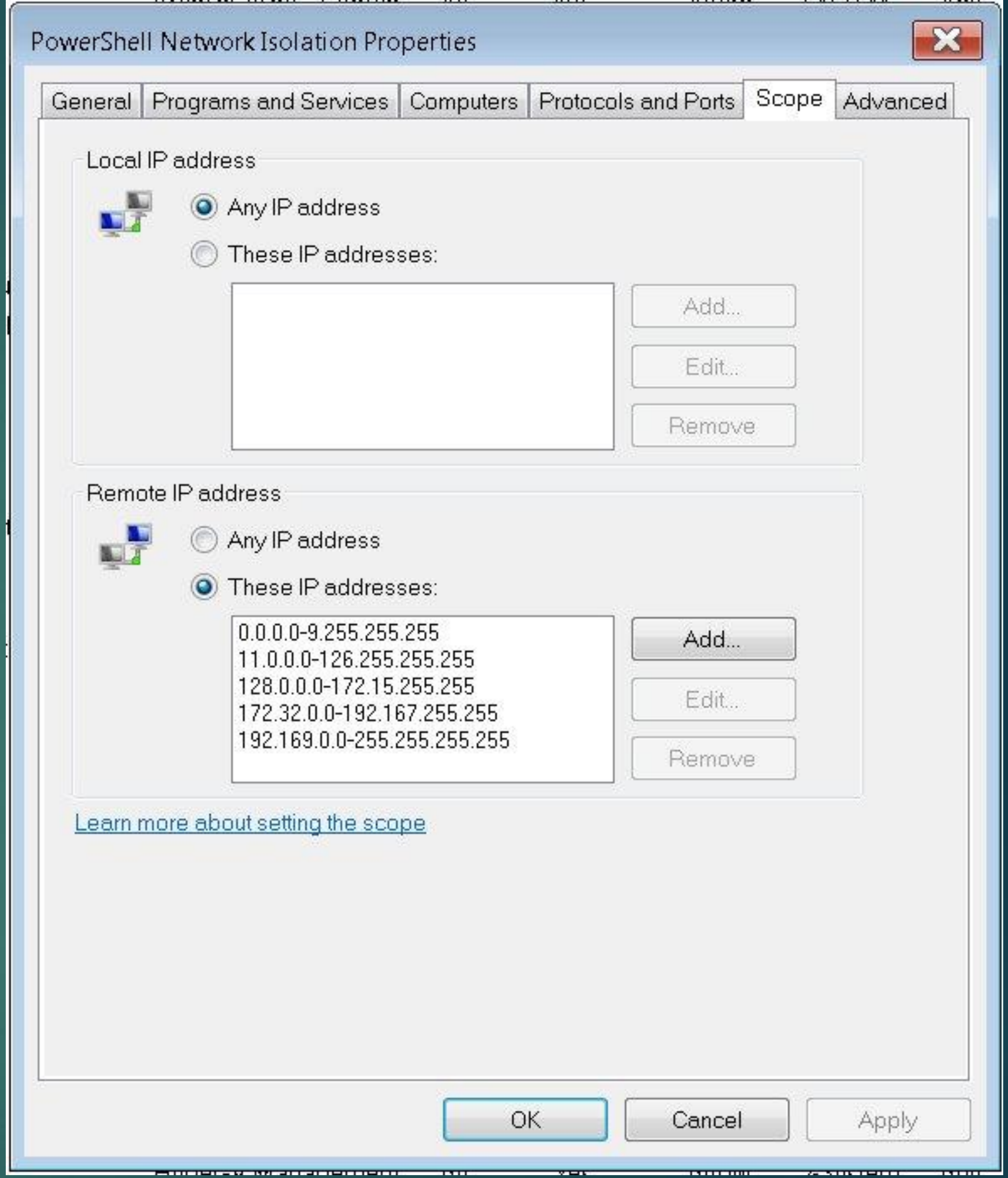
PowerShell

- Enable script logging
- Block outbound PowerShell with Windows Host Firewall
- Constrained language mode
- Monitor for
  - Abnormally long
  - Base 64
  - PowerShell outbound
  - PowerShell spawned cmd (55%) *
  - Suspicious Command Line

- source="WinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4103 OR EventCode=4104
- source="WinEventLog:Windows PowerShell" EventCode=400
- \`Sysmon\` AND Processes.process_name=powershell*.exe
- * increased-use-of-powershell-in-attacks-16-en (Symantec 2017)

PowerShell

- Block outbound PowerShell with Windows Host Firewall
- Most detailed Firewall rule will apply through GPO
- https://twitter.com/onfvp/status/1299007243074109440



PowerShell Network Isolation Properties

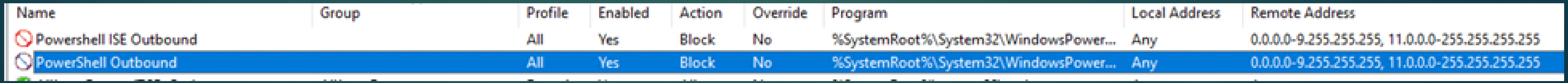
Local IP address

● Any IP address
○ These IP addresses:

Remote IP address

○ Any IP address
● These IP addresses:

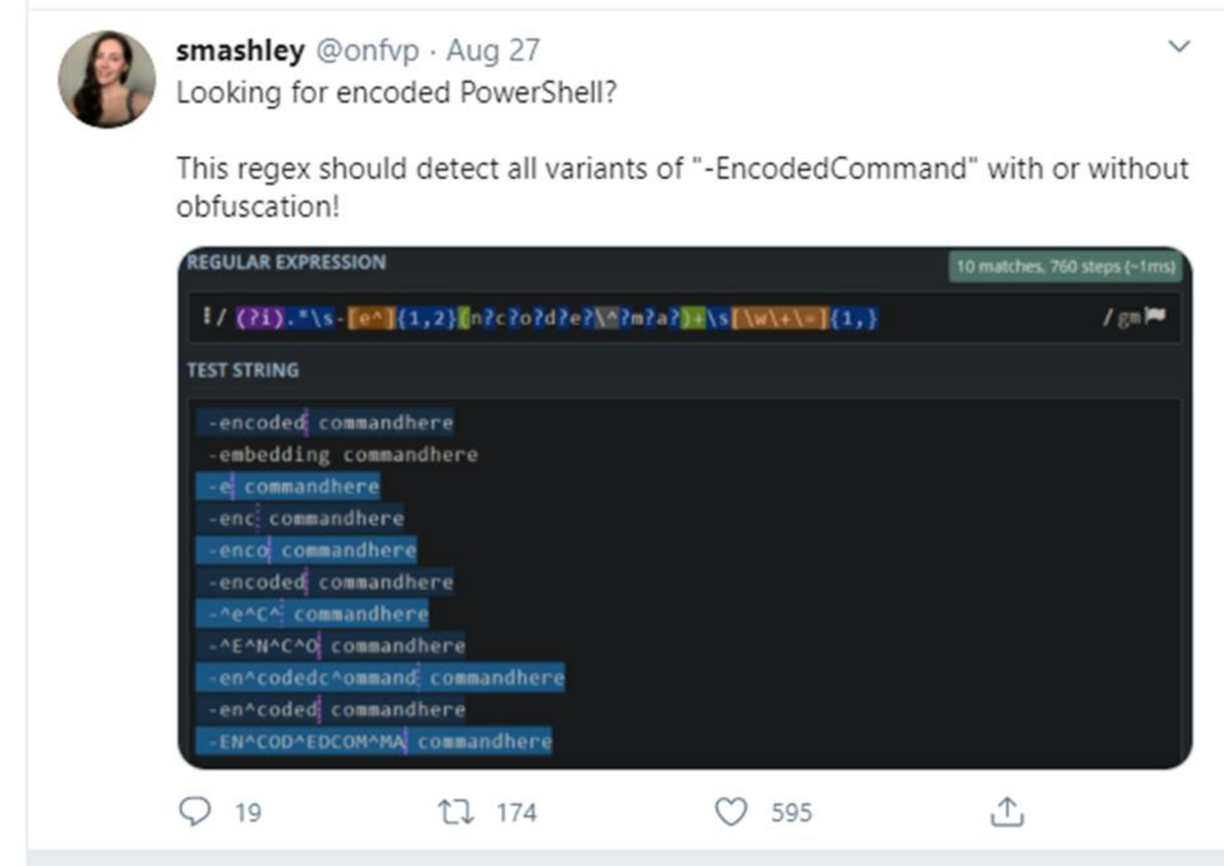
```
0.0.0.0-9.255.255.255
11.0.0.0-126.255.255.255
128.0.0.0-172.15.255.255
172.32.0.0-192.167.255.255
192.169.0.0-255.255.255.255
```



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address
Powershell ISE Outbound		All	Yes	Block	No	%SystemRoot%\System32\WindowsPower...	Any	0.0.0.0-9.255.255.255, 11.0.0.0-255.255.255.255
PowerShell Outbound		All	Yes	Block	No	%SystemRoot%\System32\WindowsPower...	Any	0.0.0.0-9.255.255.255, 11.0.0.0-255.255.255.255

PowerShell Cobalt Strike

- Message=*IO.MemoryStream*
- source="WinEventLog:System" EventCode=7045
- System.Management.Automation.ni.dll EventCode 7
- source="WinEventLog:Autoruns" powershell (Message=*-W*Hidden* OR Message=*-nologo* OR Message=*-nop* OR Message=*iex* OR Message=*Out-MiniDump* OR Message=*-enc* OR Message=*-EncodedCommand* OR Message=*downloadString* OR Message=*DownloadFile* OR Message=*DownloadData* OR Message=*ShellExecute* OR Message=*Invoke-Mimikatz* OR Message=*schtasks*create* OR Message=*Webclient* OR Message=*FromBase64String* OR Message=*IO.StreamReader* OR Message=*IO.MemoryStream* OR System.Reflection.AssemblyName OR Message=*IO.Compression.DeflateStream*)
- https://twitter.com/onfvp/status/1299007243074109440



smashley @onfvp · Aug 27

Looking for encoded PowerShell?

This regex should detect all variants of "-EncodedCommand" with or without obfuscation!

REGULAR EXPRESSION

10 matches, 760 steps (~1ms)

```
/ (?i).*\s-[e^]{1,2}(n?c?o?d?e?\^?m?a?)+\s[\w\+\=]{1,} / gm
```

TEST STRING

```
-encoded commandhere
-embedding commandhere
-e commandhere
-enc commandhere
-enco commandhere
-encoded commandhere
-^e^C^ commandhere
-^E^N^C^O commandhere
-en^codedc^ommand commandhere
-en^coded commandhere
-EN^COD^EDCOM^MA commandhere
```

Mimikatz

- Detection
  - Explicit Credential Logon
  - Debug-Assigned-Logon
  - Debug-User-Right
  - LSASS File created
  - LSASS process access
- Hardening
  - Remove from all workstations SeDebugPrivilege and SeCreateTokenPrivilege

Mimikatz Detect

- Explicit Credential Logon
- source="WinEventLog:Security" EventCode=4648 (Process_Name="*net.exe" OR Process_Name="*wmic.exe" OR Process_Name="*powershell.exe" OR Process_Name="*cmd.exe") src_user!=*$
- Debug User Right
- source="WinEventLog:Security" EventCode=4704 User_Right=SeDebugPrivilege
- Debug Assigned Logon
- index=wineventlog EventCode=4672 user!=SYSTEM user!=*$ SeDebugPrivilege
- LSASS File creation
- `sysmon` EventCode=11 Image="C:\\WINDOWS\\System32\\lsass.exe“
- https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES/tree/master/Credential%20Access

Prevention

Info Sec Advice

Hardening your endpoints

- Monitor for WDIGEST changes
- Remove from all workstations SeDebugPrivilege,SeCreateTokenPrivilege
- Windows Host Firewall, inbound restrictions
- PowerShell Outbound restrictions
- Disable WPAD, LLMNR, NetBios, SMB v1
- SAMiR10 on Servers and workstations
- Deny access to this computer from the network (Built-in\Administrators)

Monitoring Gaps/ Automation/and Validation

- https://github.com/olafhartong/sysmon-modular
- https://github.com/SwiftOnSecurity/sysmon-config
- https://blog.reconinfosec.com/automating-coverage-analysis-with-att-ck-navigator/
- https://github.com/timfrazier1/AdversarySimulation
- https://github.com/redcanaryco/invoke-atomicredteam/wiki
  - Invoke-atomicTest T1003 –ShowDetailsBrief
  - Invoke-atomicTest T1117 –TestNumbers 1,2
- https://github.com/NextronSystems/APTSimulator

Security Blogs

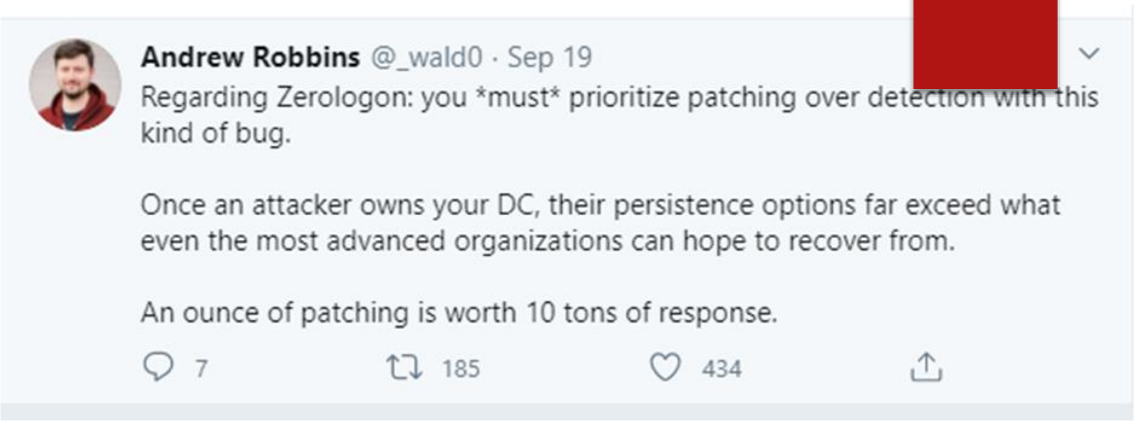
- FireEye M-trends 2020. Of the top five most common techniques, we observed three used for valid access (t1086, t1035, t1133), one used for both valid and illicit access (t1064), and only one around purely attacker-derived tooling (t1027). This trend is pervasive throughout the full list of observed techniques (Fig. 3). We observed only 40% of all MITRE ATT&CK techniques in use against FireEye clients.
- The art and science of detecting Cobalt Strike Talos
  - `New-Object IO.MemoryStream(,[Convert]:: FromBase64String
- The DFIR Report (Ryuk Speed Run, 2 Hours to Ransom)
  - Cobalt Strike, AdFind, Rubeus
- Warzone: Behind the enemy lines checkpoint
  - powershell Add-MpPreference -ExclusionPath C:\

CVE responses

- 02/11/2020, CVE-2020-0674 CVSS 7.5 Affects the scripting engine in Internet Explorer, specifically a JScript component. The problematic component is a library named jscript.dll, which provides compatibility with a deprecated version of the JScript scripting language. Microsoft-Windows-CodeIntegrity/Operational Event ID 3076
- 01/14/2020, CVE-2020-0601. CVSS Score 8.1. A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. Microsoft-Windows-Sysmon/Operational Event ID 7
- 07/14/2020, CVE-2020-1350. CVSS Score 10. A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. Application" ID=1
  - source="WinEventLog:Application" EventCode=1 | rex field=Message "(?m)(?<Alert_Info>.*)" | table _time host EventCode Additional_Information Alert_Info

Patching

- CVE-2020-1472, Aug 11 2020 Netlogon Elevation of Privilege Vulnerability
- Your patching person is the Key
- Your Configuration Administrator is also your best Friend
- source="WinEventLog:System" EventCode=5827 OR EventCode=5828"



Andrew Robbins @_wald0 · Sep 19

Regarding Zerologon: you *must* prioritize patching over detection with this kind of bug.

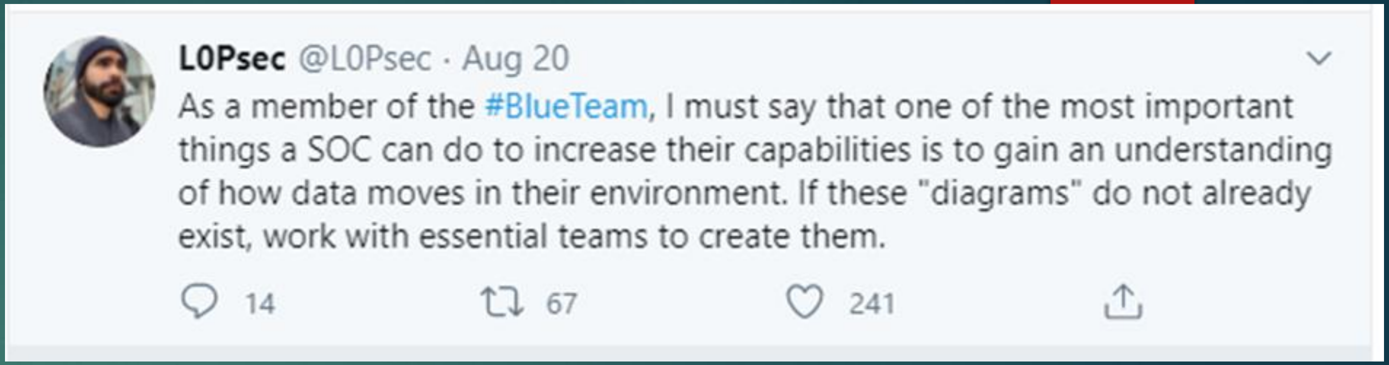
Once an attacker owns your DC, their persistence options far exceed what even the most advanced organizations can hope to recover from.

An ounce of patching is worth 10 tons of response.

7 185 434

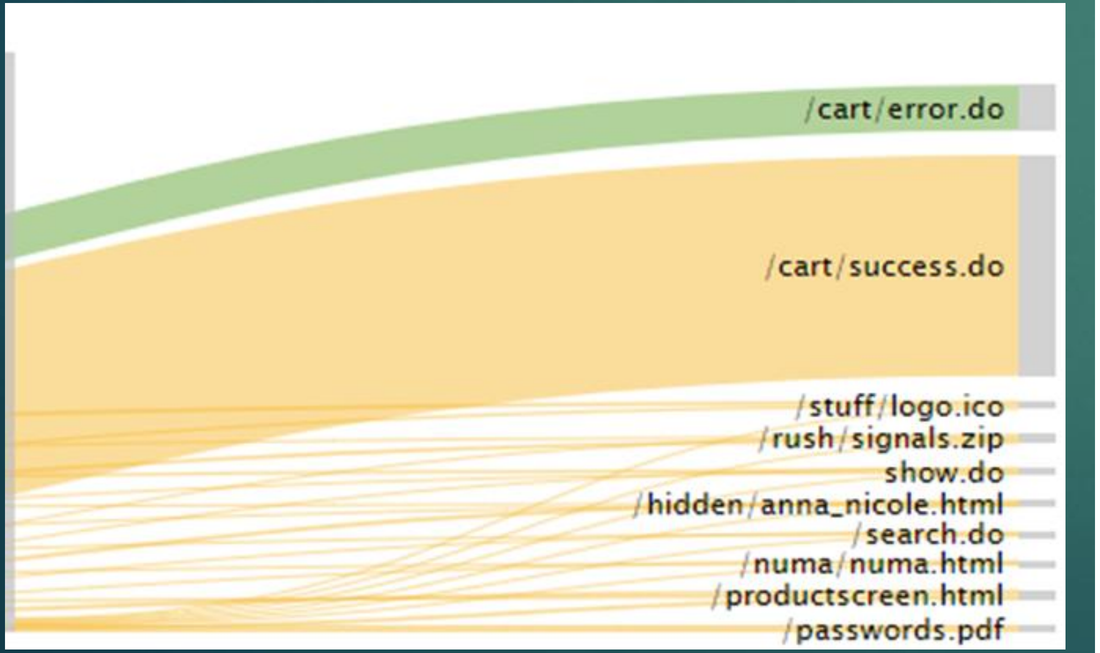
Data paths

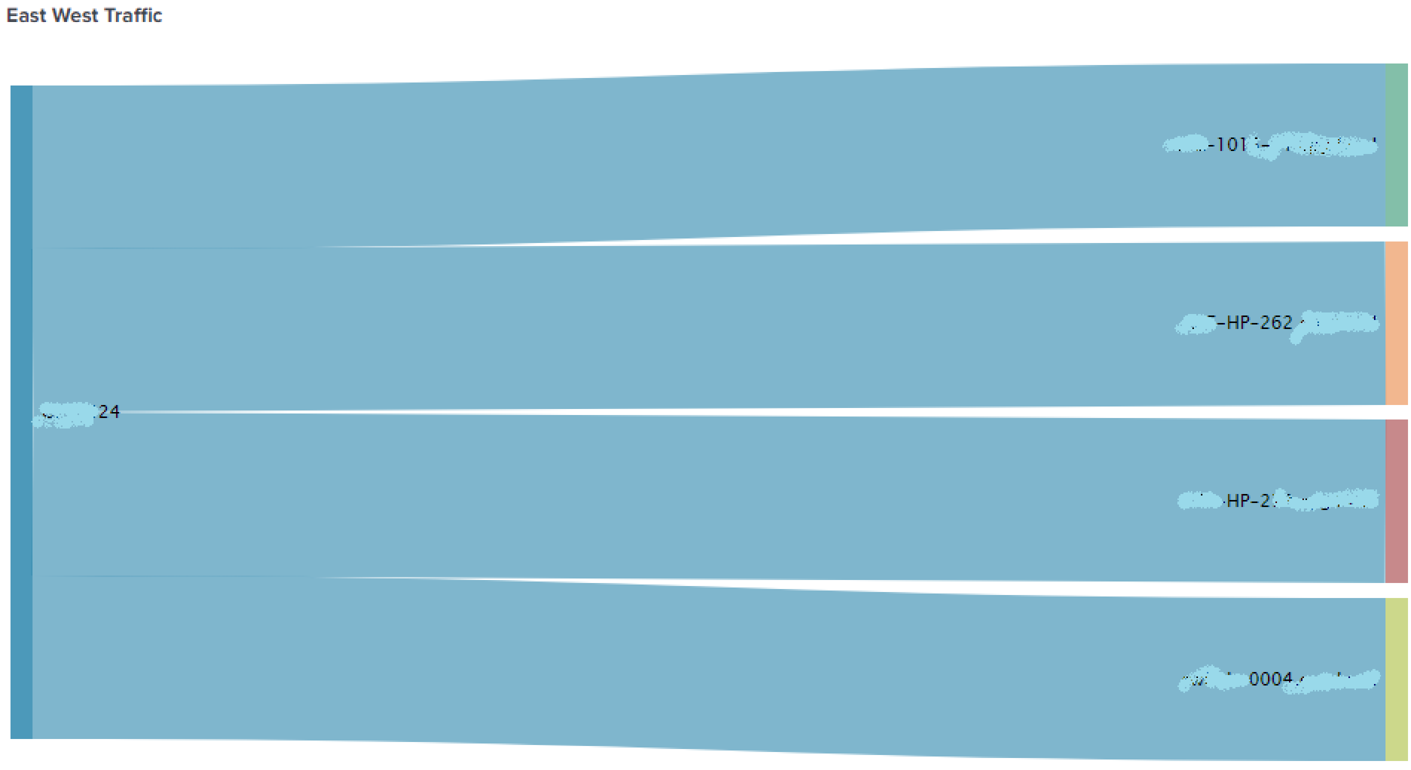
- Lateral movement/East West Traffic
- SSH, dB traffic, FTP, SMB
- Sankey Diagrams for Splunk



L0Psec @L0Psec · Aug 20

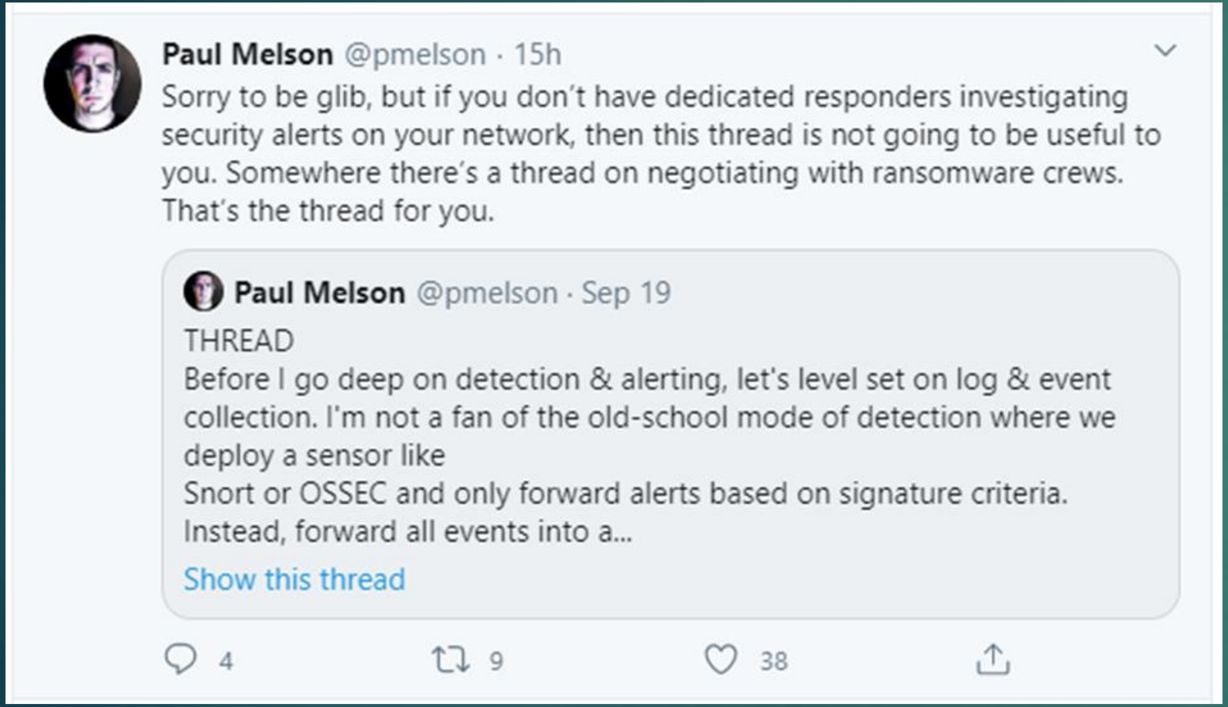
As a member of the #BlueTeam, I must say that one of the most important things a SOC can do to increase their capabilities is to gain an understanding of how data moves in their environment. If these "diagrams" do not already exist, work with essential teams to create them.





East West Traffic

Investigations matter /Attribution matters

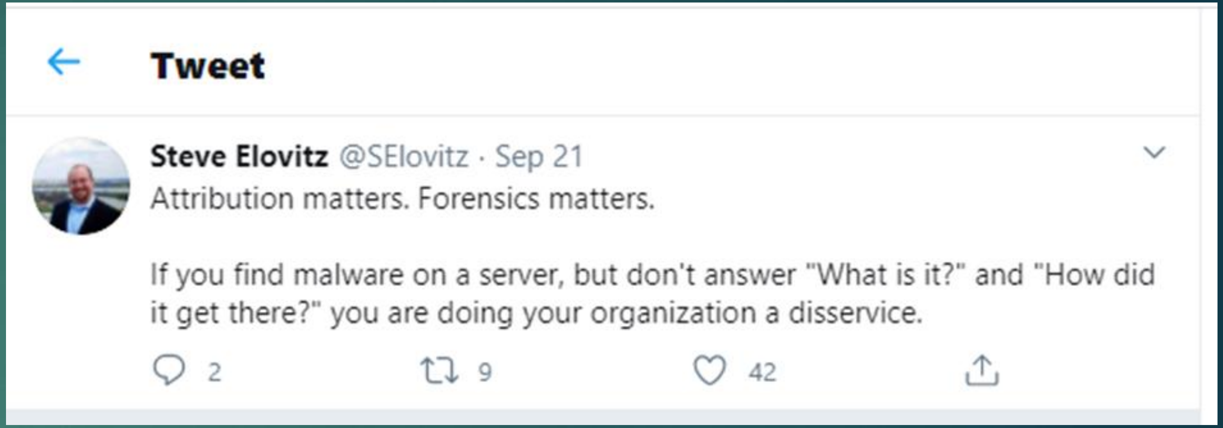


Paul Melson @pmelson · 15h

Sorry to be glib, but if you don't have dedicated responders investigating security alerts on your network, then this thread is not going to be useful to you. Somewhere there's a thread on negotiating with ransomware crews. That's the thread for you.

> **Paul Melson** @pmelson · Sep 19
>
> THREAD
> Before I go deep on detection & alerting, let's level set on log & event collection. I'm not a fan of the old-school mode of detection where we deploy a sensor like
> Snort or OSSEC and only forward alerts based on signature criteria. Instead, forward all events into a...
>
> Show this thread

4 9 38

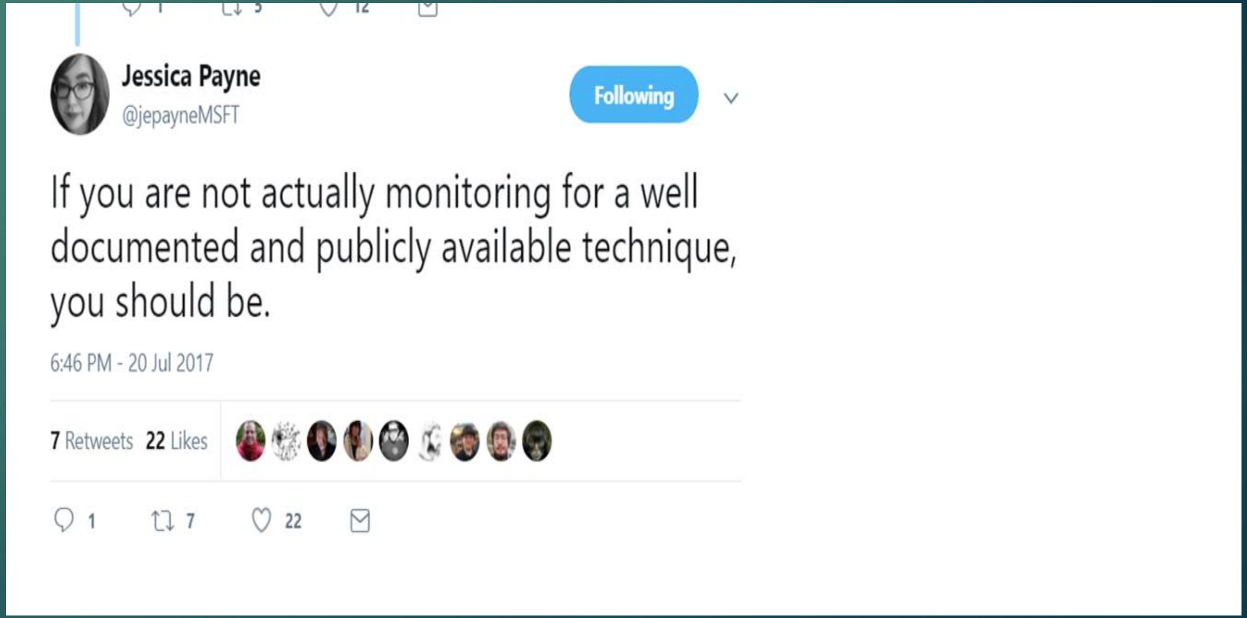


Steve Elovitz @SElovitz · Sep 21

Attribution matters. Forensics matters.

If you find malware on a server, but don't answer "What is it?" and "How did it get there?" you are doing your organization a disservice.

2 9 42



Jessica Payne
@jepayneMSFT

If you are not actually monitoring for a well documented and publicly available technique, you should be.

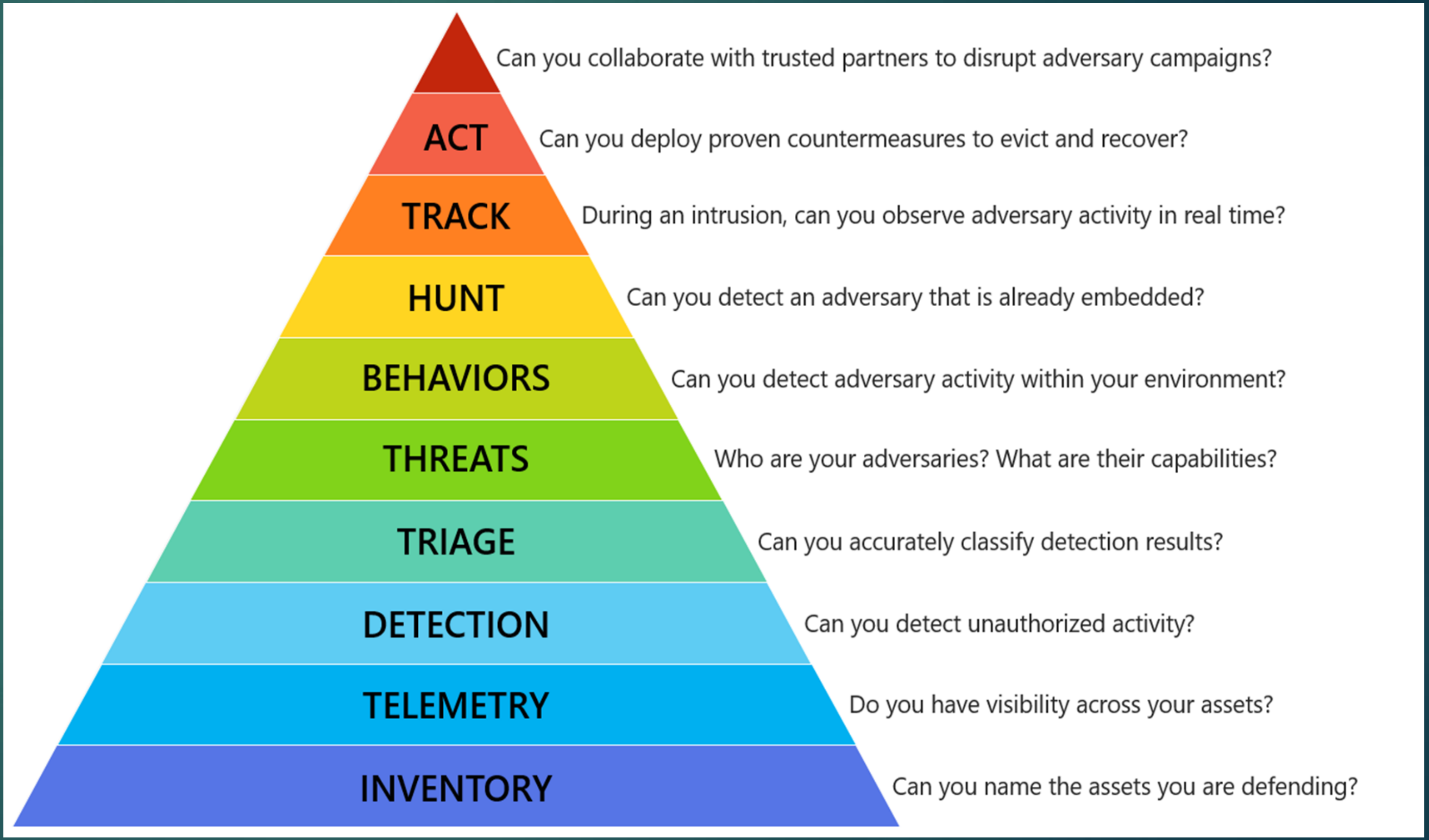
6:46 PM - 20 Jul 2017

7 Retweets 22 Likes

1 7 22

The Incident Response Hierarchy of Needs

- Your company may not require attribution
- Threat intelligence & sharing
- Reality is that you do require at a minimum investigations



Can you collaborate with trusted partners to disrupt adversary campaigns?

ACT — Can you deploy proven countermeasures to evict and recover?

TRACK — During an intrusion, can you observe adversary activity in real time?

HUNT — Can you detect an adversary that is already embedded?

BEHAVIORS — Can you detect adversary activity within your environment?

THREATS — Who are your adversaries? What are their capabilities?

TRIAGE — Can you accurately classify detection results?

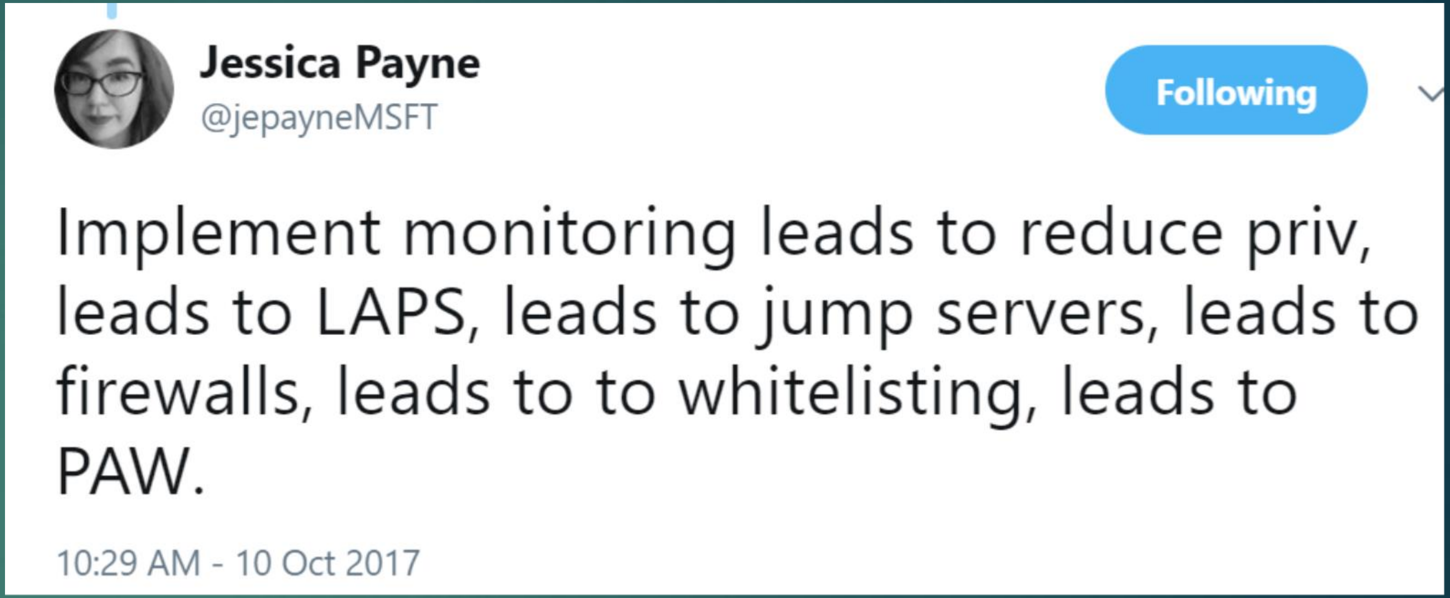
DETECTION — Can you detect unauthorized activity?

TELEMETRY — Do you have visibility across your assets?

INVENTORY — Can you name the assets you are defending?

Places you will go

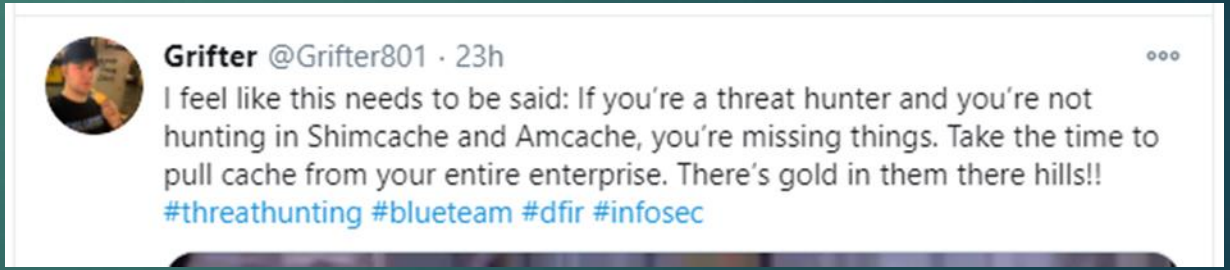
- Applocker
- Windows Defender Application Control
- Disable Java
- Macro inventory
- Data flows
- Answer questions about impact of CVE's immediately
- Categorize your investigations and review techniques that allowed malware to get in



Jessica Payne
@jepayneMSFT

Implement monitoring leads to reduce priv, leads to LAPS, leads to jump servers, leads to firewalls, leads to to whitelisting, leads to PAW.

10:29 AM - 10 Oct 2017

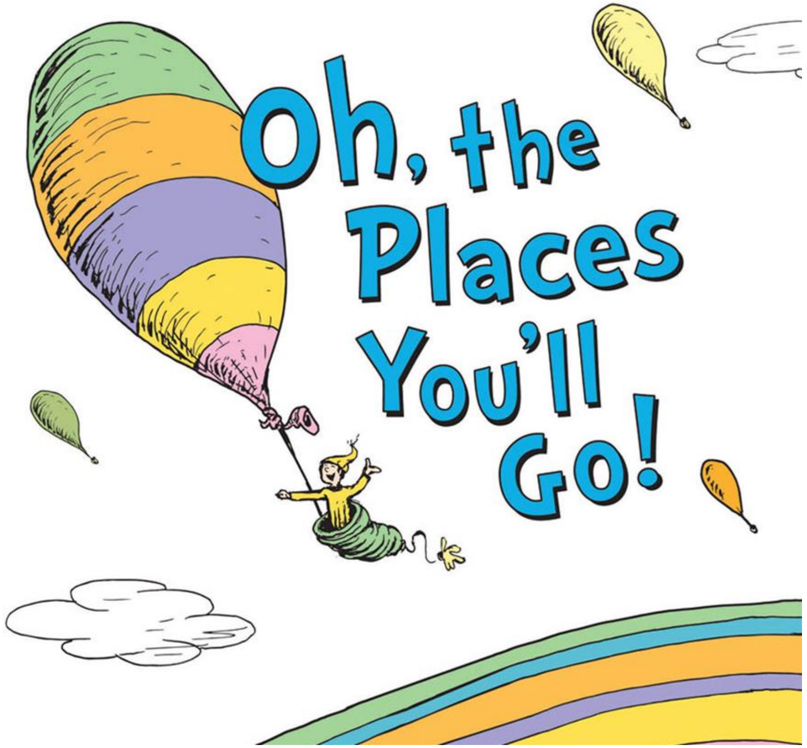


Grifter @Grifter801 · 23h

I feel like this needs to be said: If you're a threat hunter and you're not hunting in Shimcache and Amcache, you're missing things. Take the time to pull cache from your entire enterprise. There's gold in them there hills!! #threathunting #blueteam #dfir #infosec

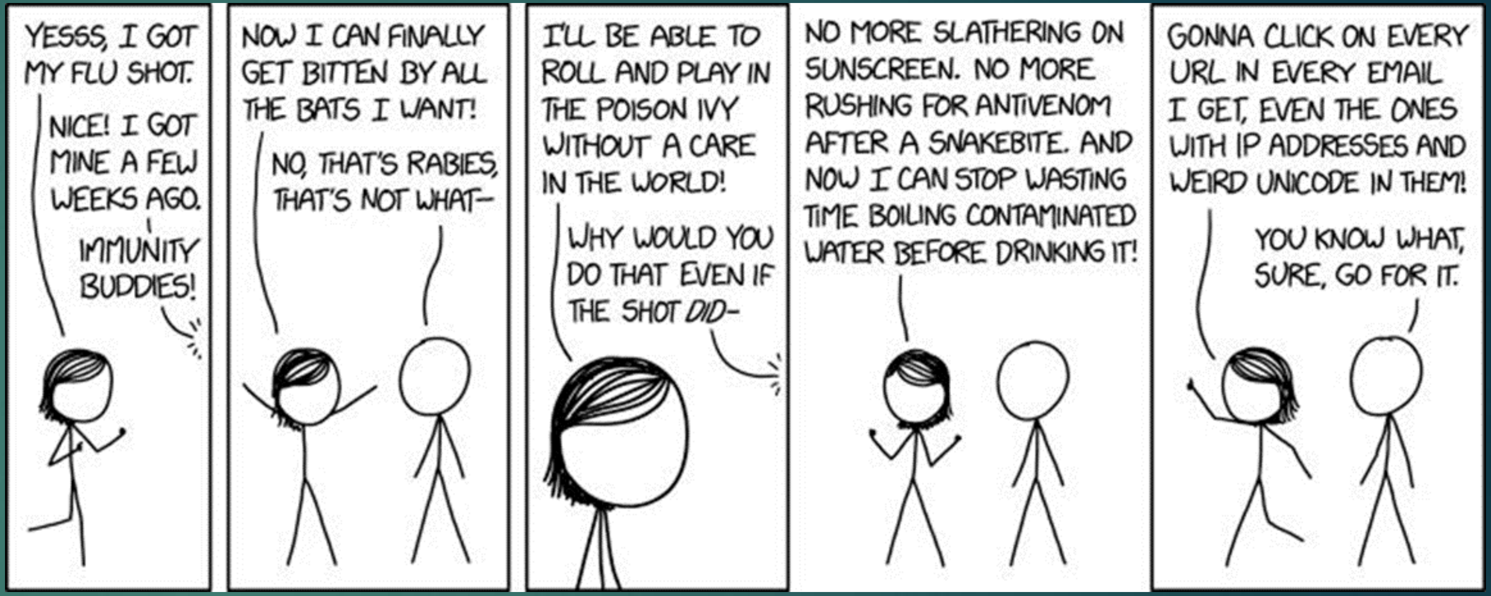
Places you will go

- Validate your logs with open-source tools
- Require & monitor Code signing
- Increase security in your suppliers
- Increase security in Vendor Maintenance
- Threat Intelligence
- Community sharing



Why

- Security deserves to see all the malware that your users are installing
- Let end users know that you can identify patient Zero
- You can see every hash that has run in your enterprise
- Get changes approved faster
- Fight back
- Show real numbers that support the risk
- Attackers morals have declined drastically in the last year
- KRBTGT password reset


YESSS, I GOT MY FLU SHOT.
NICE! I GOT MINE A FEW WEEKS AGO.
IMMUNITY BUDDIES!
NOW I CAN FINALLY GET BITTEN BY ALL THE BATS I WANT!
NO, THAT'S RABIES, THAT'S NOT WHAT–
I'LL BE ABLE TO ROLL AND PLAY IN THE POISON IVY WITHOUT A CARE IN THE WORLD!
WHY WOULD YOU DO THAT EVEN IF THE SHOT DID–
NO MORE SLATHERING ON SUNSCREEN. NO MORE RUSHING FOR ANTIVENOM AFTER A SNAKEBITE. AND NOW I CAN STOP WASTING TIME BOILING CONTAMINATED WATER BEFORE DRINKING IT!
GONNA CLICK ON EVERY URL IN EVERY EMAIL I GET, EVEN THE ONES WITH IP ADDRESSES AND WEIRD UNICODE IN THEM!
YOU KNOW WHAT, SURE, GO FOR IT.

Appendix

- cmd
- `Sysmon` (process_name=cmd.exe OR parent_process_name=cmd.exe)
- Explicit Credential Logon
- source="WinEventLog:Security" EventCode=4648 (Process_Name="*net.exe" OR Process_Name="*wmic.exe" OR Process_Name="*powershell.exe" OR Process_Name="*cmd.exe") src_user!=*$

Appendix

- Logs cleared
- source="WinEventLog:System" EventCode=104
- Macros (http://az4n6.blogspot.com/2016/02/more-on-trust-records-macros-and.html)
- Applocker
- source="WinEventLog:Microsoft-Windows-AppLocker/EXE and DLL" EventCode=8004
- ASR
- source="WinEventLog:Microsoft-Windows-Windows Defender/Operational“ EventCode=1121

Appendix

- Net
- `Sysmon` Image="C:\\Windows\\System32\\net.exe" OR Image="C:\\Windows\\System32\\net1.exe“
- 3 Critical processes in 10 minutes
- `Sysmon` process_name="msbuild.exe" OR process_name="psexec.exe" OR process_name="at.exe" OR process_name="schtasks.exe" OR process_name="vssadmin.exe" OR process_name="utilman.exe" OR process_name="wmic.exe" OR process_name="mshta.exe" OR process_name="whoami.exe" OR process_name="systeminfo.exe" OR process_name="csvde.exe" OR process_name="nbtstat.exe" OR process_name="cmdkey.exe" OR process_name="sc.exe")
- | bin span=10m _time | stats values(process_name), count by host _time user_name | where count>3

Appendix

- Cmd Line references for building out Alerts
- https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
- https://arno0x0x.wordpress.com/2017/11/20/windows-oneliners-to-download-remote-payload-and-execute-arbitrary-code/
- https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/