SPLUNKING THE ENDPOINT V:

Enough Already! (SEC2007)

brodsky@splunk.com
Director Global Security Strategists | Security Kittens

October, 2019

V1.0

splunk> .conf19

whoami – @james_brodsky

- Director, Global Security Strategists (Louisville, CO)
- Lead a team of Splunk security strategists across the US, UK, Australia
- Have been involved with security here since my start
- .conf Splunking the Endpoint! for FIVE years
- BOTS 1.0, 2.0, 3.0, 4.0. BOTN 1.0, 2.0.
- CSC 20 Whitepaper, FFIEC Whitepaper (co-author), other compliance, Tripwire apps, blogs, Sysmon contributions, etc, etc....

It's a hands-on session.
Eventually. But first slides.
Lots of pink slides.

Nope. Still can't get Splunk to run on an Apple *IIe.* You need to be using a functional, modern computing device.

And it needs to be **on the Internet**.

And it needs a **relatively modern browser**.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

It is fun to assign folks to servers randomly…

.conf2017 .conf18 .conf19

Our BOTS adversary this year *"Violent Memmes"* is loosely based on APT 28/29 and Turla.

splunk> .conf19

=

My thought process.

=

=

=

=

=

splunk> .conf19

(not me.)

=

=

=

+

=

.conf19

splunk> .conf19

ebay

Hi James, your order is being shipped!

Check order status | Go to site

Your order will ship to:

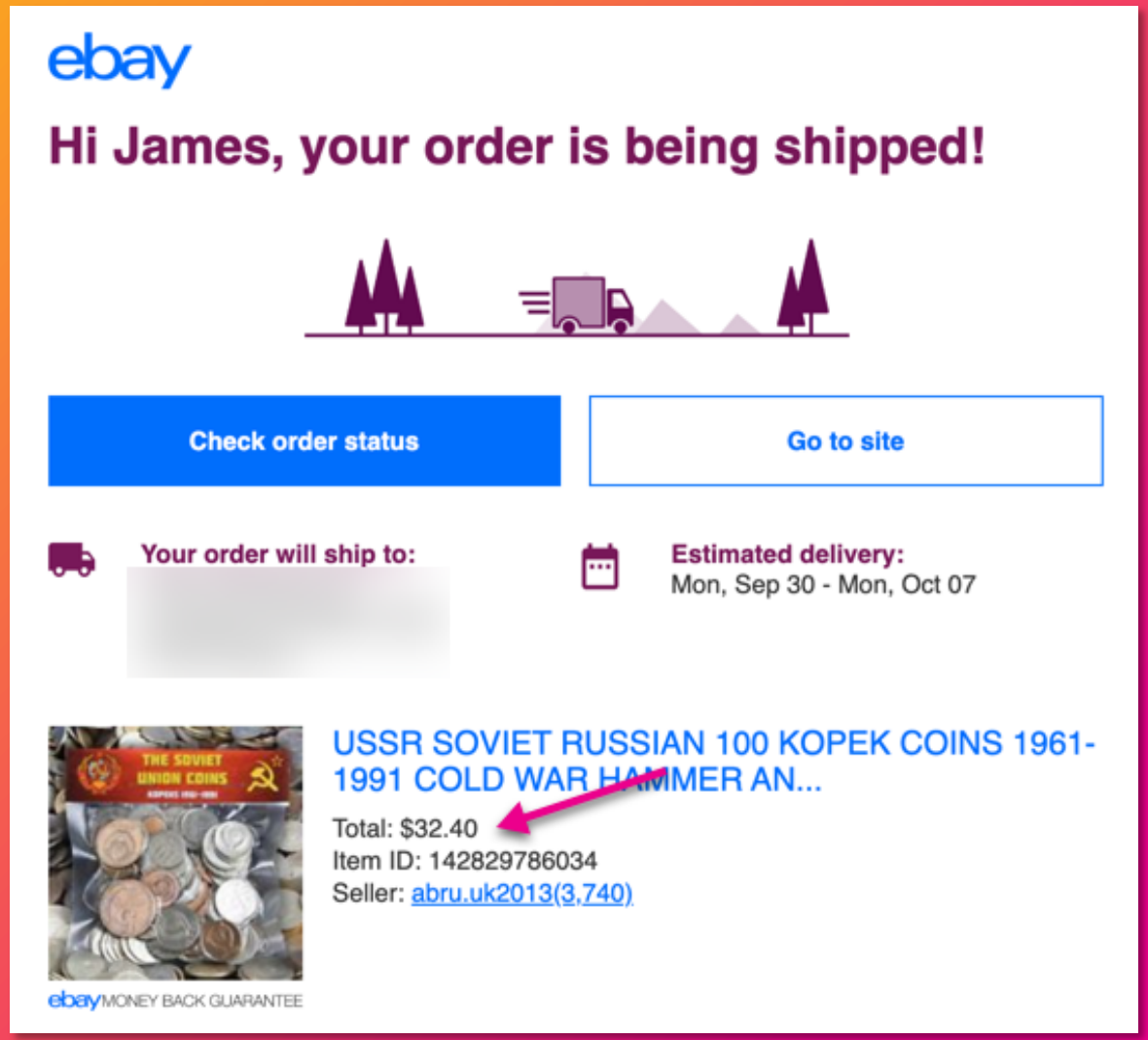
Estimated delivery:
Mon, Sep 30 - Mon, Oct 07

USSR SOVIET RUSSIAN 100 KOPEK COINS 1961-1991 COLD WAR HAMMER AN...

Total: $32.40
Item ID: 142829786034
Seller: abru.uk2013(3,740)

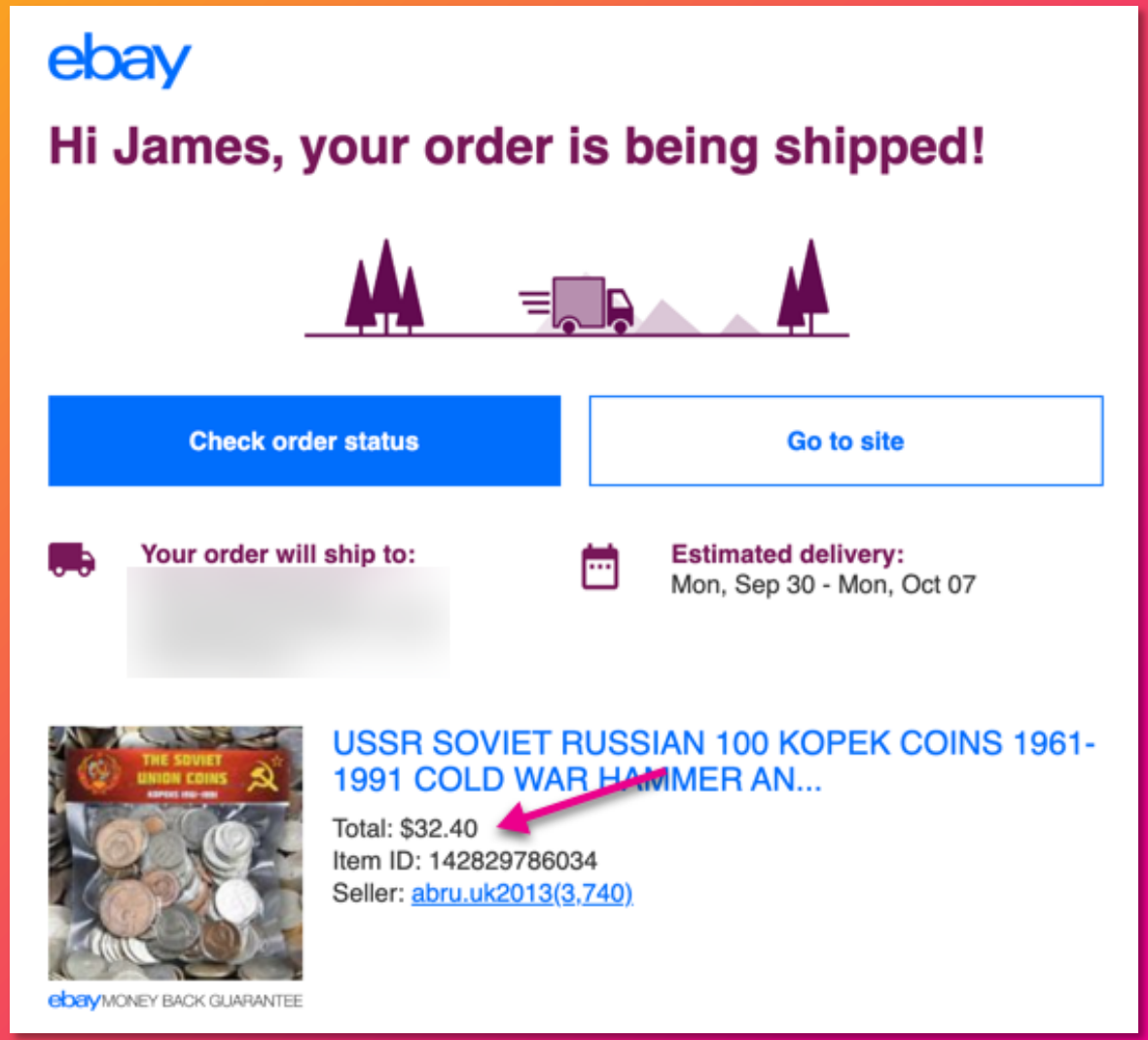
ebay MONEY BACK GUARANTEE

1 Ruble = 100 kopeks



1 Ruble = 100 kopeks

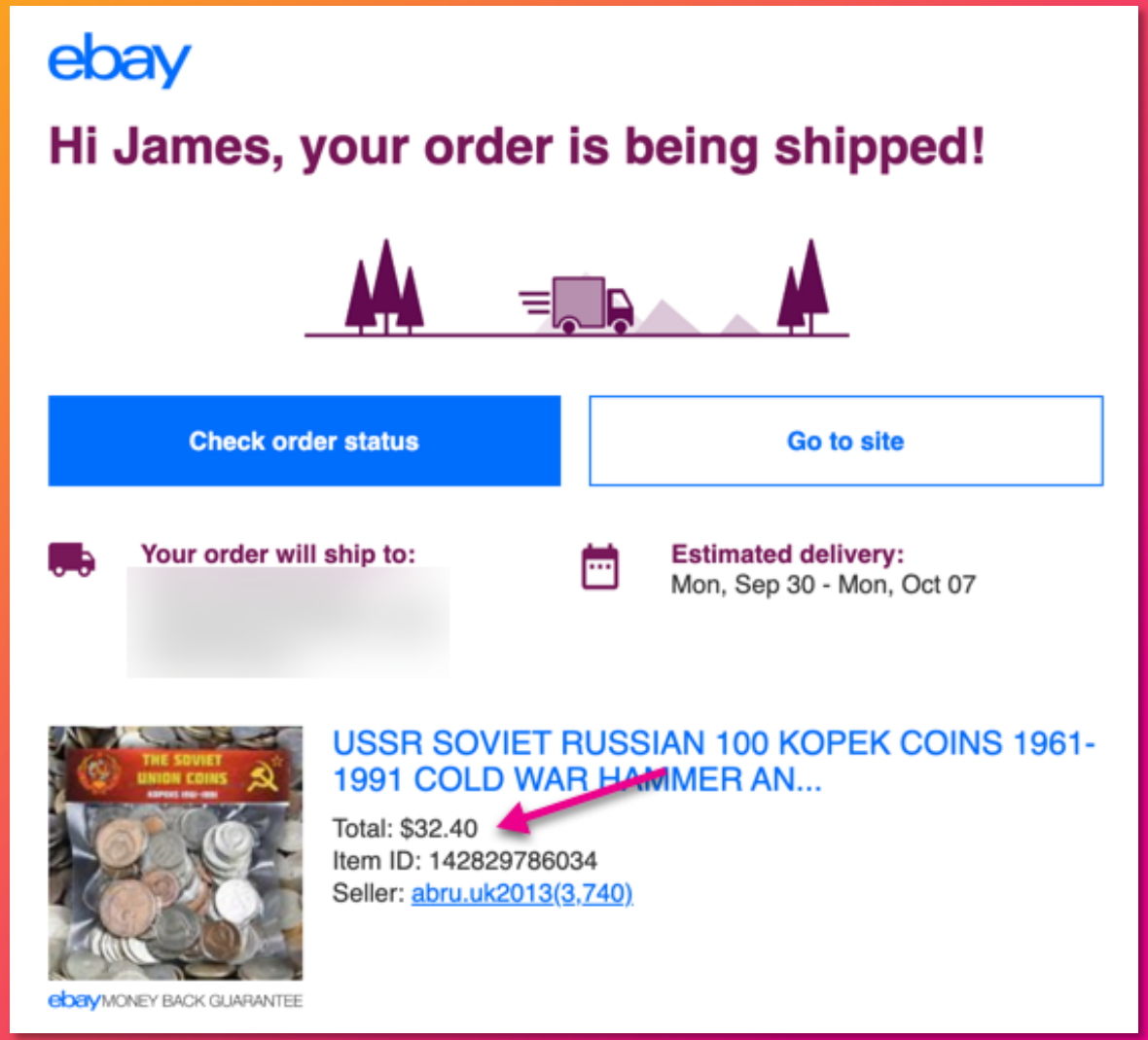
$32.40/300 = 11 cents per kopek coin from eBay, September 2019



1 Ruble = 100 kopeks

$32.40/300 = 11 cents per kopek coin from eBay, September 2019

Historical value of former Soviet ruble in 1992 = $1.80 USD (or 18 cents/kopek)

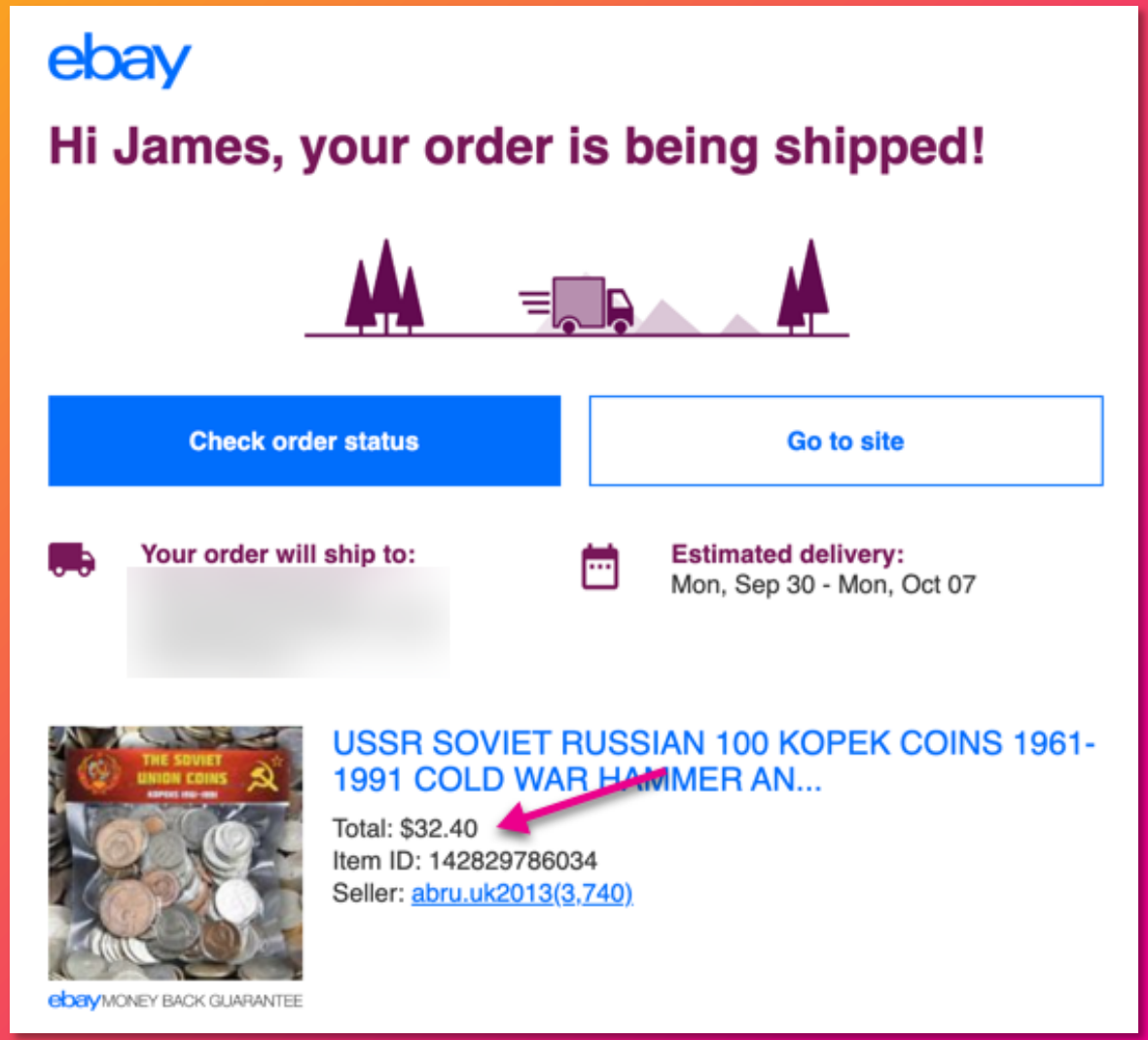


1 Ruble = 100 kopeks

$32.40/300 = 11 cents per kopek coin from eBay, September 2019

Historical value of former Soviet ruble in 1992 = $1.80 USD (or 18 cents/kopek)

Cumulative Rate of Inflation from 1992-2019=82.9%, or 33 cents!



1 Ruble = 100 kopeks

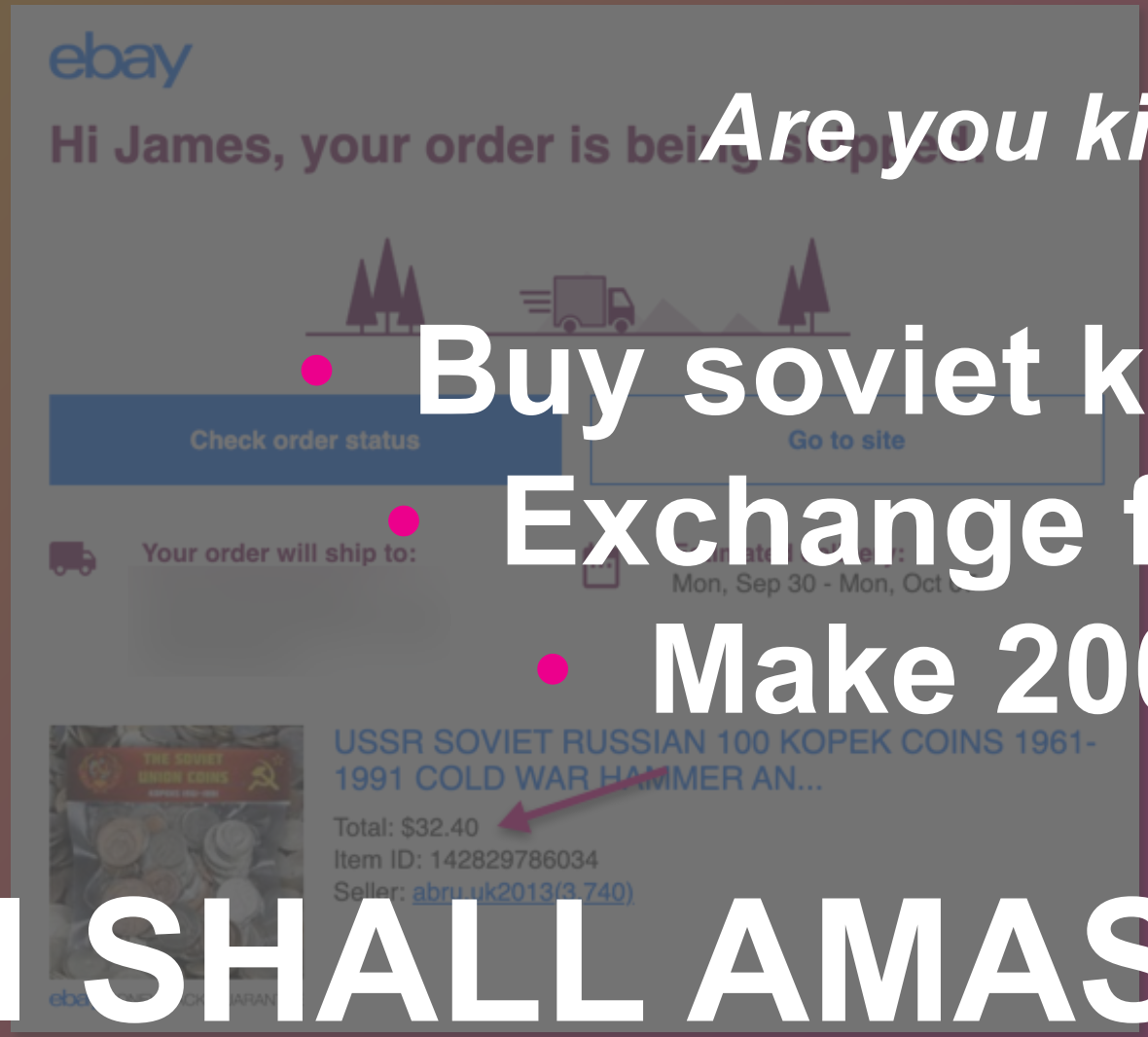
$32.40/300 = 11 cents per kopek coin from eBay, September 2019

Historical value of former Soviet ruble in 1992 = $1.80 USD (or 18 cents/kopek)

Cumulative Rate of Inflation from 1992-2019=82.9%, or 33 cents!

300 kopeks should be worth $99!

…and I paid $32.40.



Are you kidding me?

- **Buy soviet kopeks on eBay**
- **Exchange for US dollars**
- **Make 200% profit…**

I SHALL AMASS A FORTUNE

1 Ruble=100 kopeks

$32.40/300 = 11 cents per kopek coin from eBay, September 2019

Historical value of former Soviet ruble in 1992: $1.30 USD (or 18 cents/kopek)

Cumulative Rate of Inflation from 1992-2019=82.9%, or 33 cents!

300 kopeks should be worth $99

I could retire early!

From: jbrodsky@splunk.com (James Brodsky)
To: [redacted]
Cc:
Bcc:
Subject: HIGH PRIORITY: BRODSKY RESIGNATION!

Dear [redacted]

For the past six and a half years I have enjoyed my time helping to bring value to security customers at Splunk. However, when perusing eBay over the weekend, I found a significant loophole involving the former Soviet kopek, and suddenly realized that I could very easily triple my money by purchasing massive quantities of the old coins and converting them into US Dollars.

Therefore, my last day with the company will be 10/18/2019. I'll see what I can do in order to prepare someone to take over the Endpoint talk at .conf, and also someone else to write terrible questions involving arcane search commands in BOTS that everyone gets angry about.

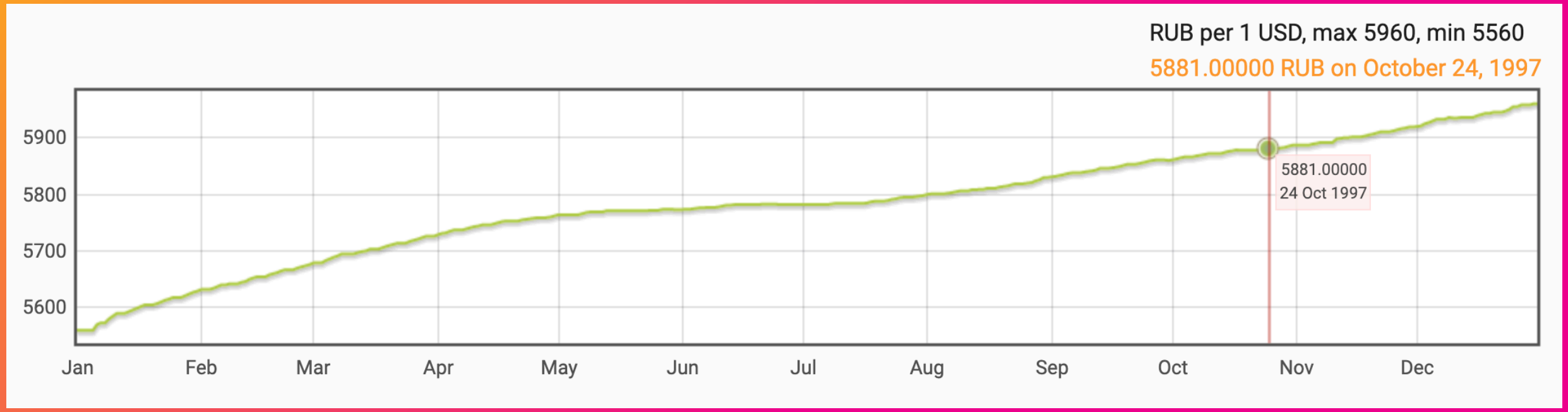
Thanks for your support, and you can reach me in the future at kopek_kurrency@aol.com.

-jb

I sent a resignation letter!

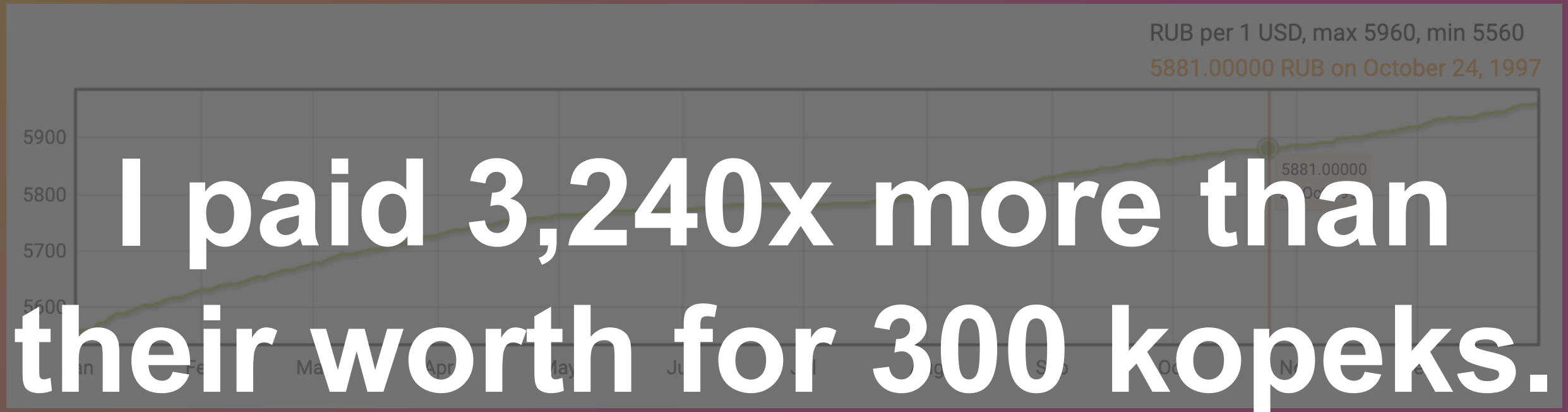

kopek one
I bought a jet!

…then I looked to see what happened to the ruble after 1992.



600 kopeks equals 1 cent.
300 kopeks that I bought = ½ a cent.
+ inflation 1997-2019: about ¾ a cent.

….but then….



I paid 3,240x more than their worth for 300 kopeks.

☹

600 kopeks equals 1 cent.
300 kopeks = ½ a cent.
+ inflation 1997-2019: about ¾ a cent.

Lear Jets R' Us

09/07/2019 09:37 PM

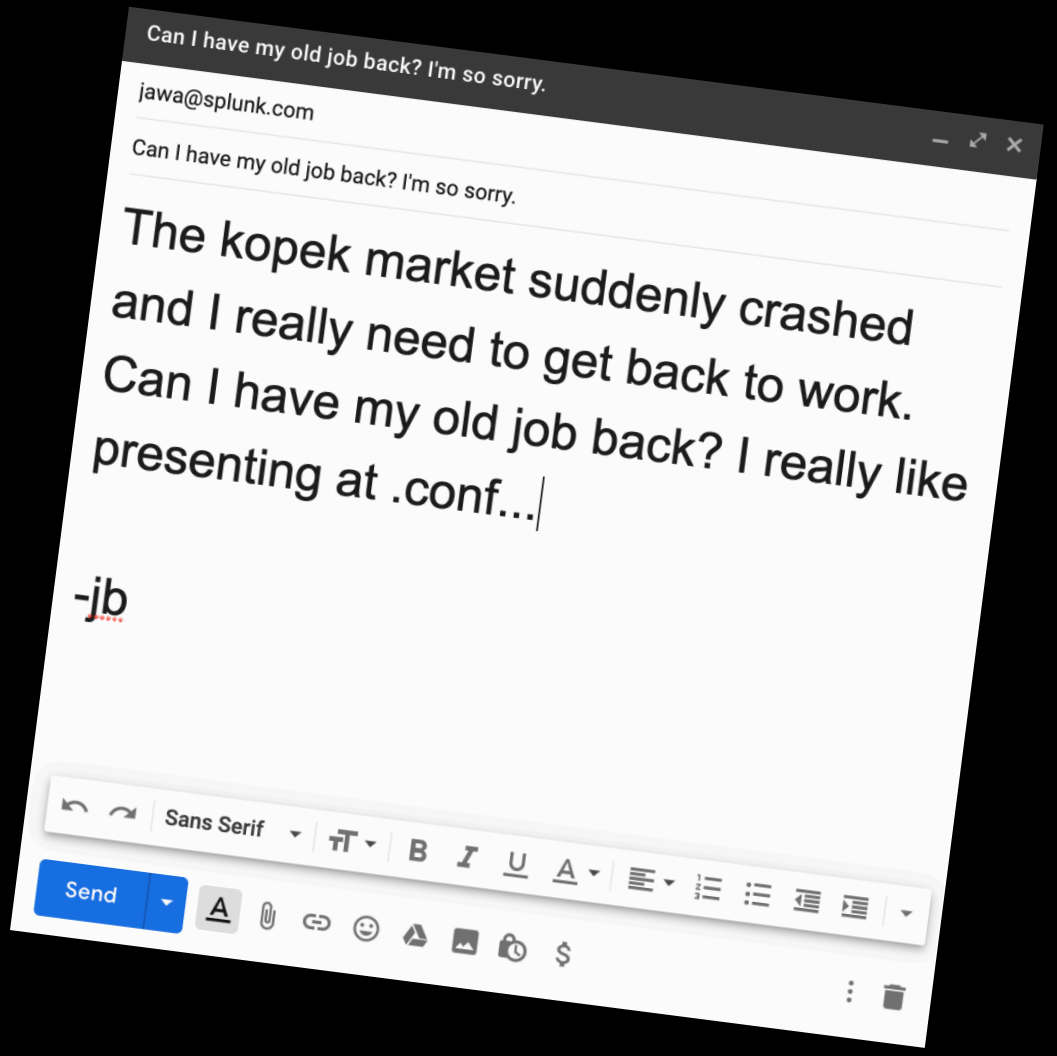
ITEM	TOTAL
1986 Lear 55	750,000.00
Total:	750,000.00

MER 18122803
CARD ISSUER
VISA SALE
Jimmy R Points
AUTHORIZATION CODE - 290807

ACCOUNT
**********3305
Exp: 09/23
SEQ 1884219

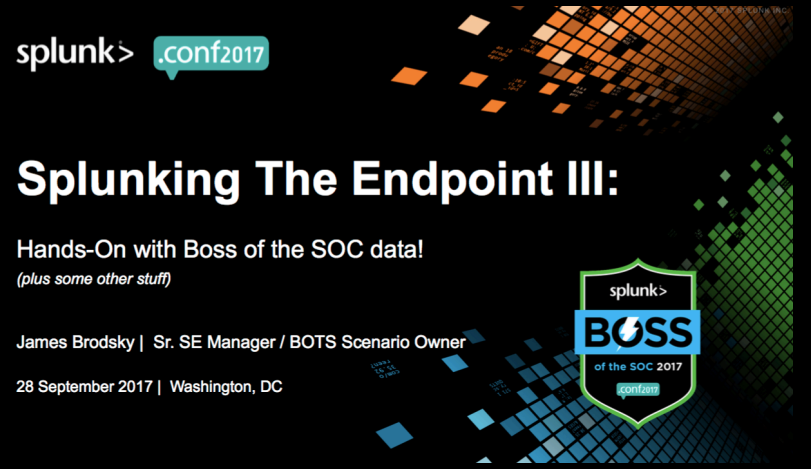
RETURN RECEIPT

I returned the jet.



I groveled for my old job.

And here I am, presenting the FIFTH endpoint talk in as many years!



therefore...

splunk> .conf19

We will NOT cover...

- What a Universal Forwarder is
- RAM Scraping POS Malware
- Ransomware
- Mac endpoints
- Why sysmon and osquery are awesome
- Stranger Things
- Endpoint forensics
- Why everything is pink
- The difference between “pike” and “pipe”
- John Denver
- Machine Learning/AI
- Giuten free fortune cookies
- Powershell Empire
- Subverting Sysmon
- Avocado Toast
- Voltaire

All of these topics and more, in the .conf archives…

search “brodsky.”

But we will cover...

- What the latest endpoint surveys tell us & what Splunk has seen recently
- Alternatives to the UF, and Best Practices for commercial solutions
- What NOT to do when you collect with the UF
- New Stuff in Sysmon, Windows TA, etc…
- Endpoint Diet! Clever Event Reduction techniques
- An new way to guide which WinEvents to collect

But we will cover...

- What the latest endpoint surveys tell us & what Splunk has seen recently
- Alternatives to the UF, and Best Practices for commercial solutions
- New stuff in Sysmon, Windows 10, etc.
- Endpoint Diet! Clever Event Reduction techniques
- An new way to guide which WinEvents to collect

…and lots of hands-on fun with BOTS data in-between!


ENDPOINTS!
LAPTOPS
NEXT-GEN++++++
TOO MUCH %$*&# DATA
DID MY REGISTRY CHANGE?
BREACHES BREACHES BREACHES

What's an endpoint?

(courtesy McAfee)

In 2016, we said…the endpoint was important!

Closest to humans

Underprotected

Versatile

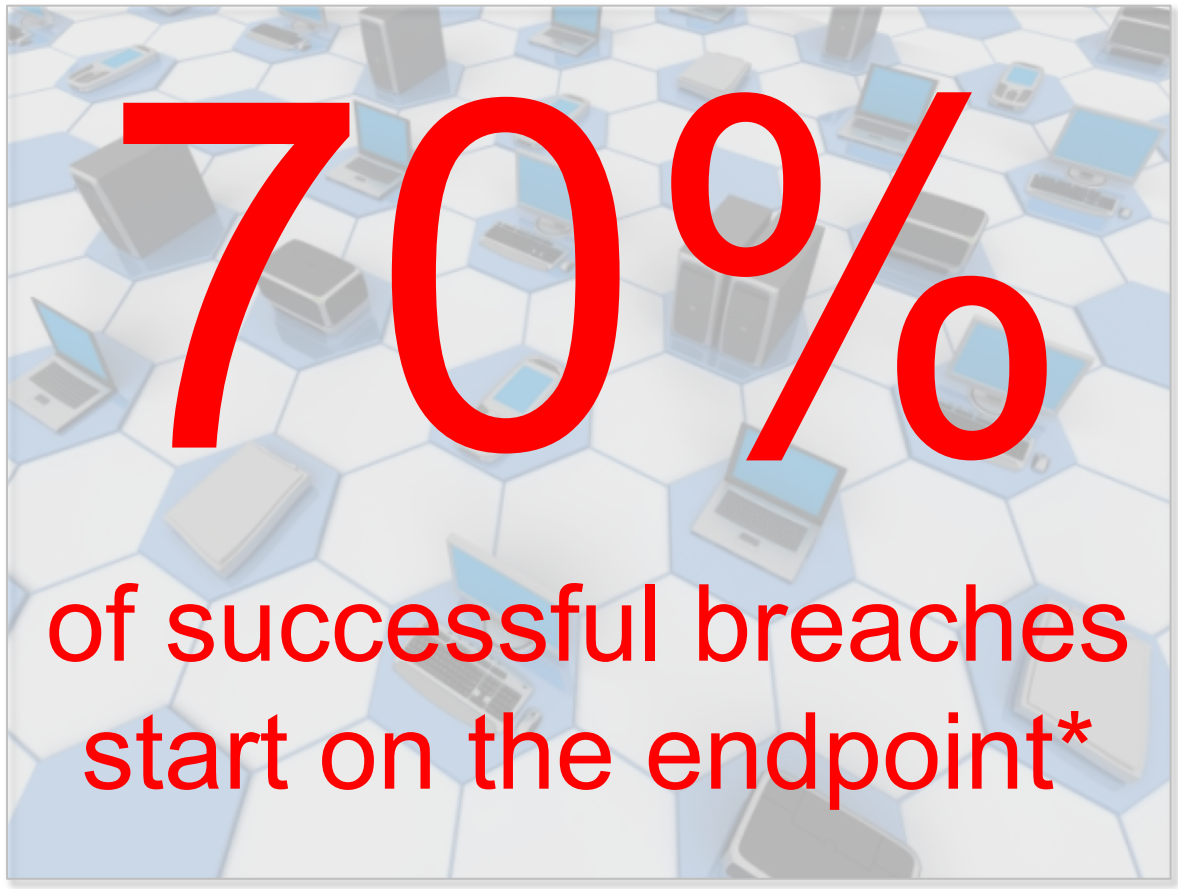
Data-rich

In 2016, we said…the endpoint was important!

The weak link

Closest to humans

Underprotected

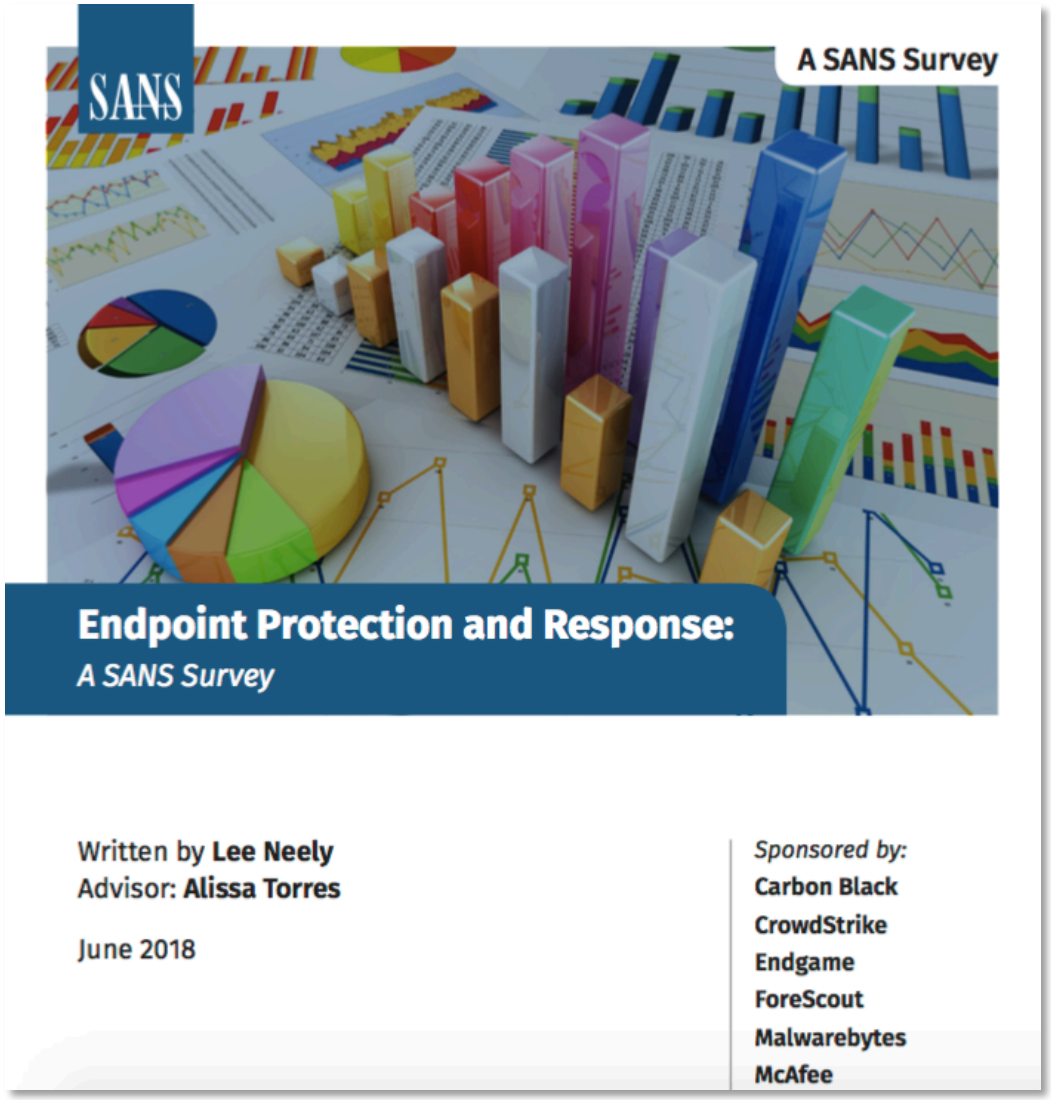


Versatile

Data-rich

*IDC study 2016

And in 2018, that went up to….

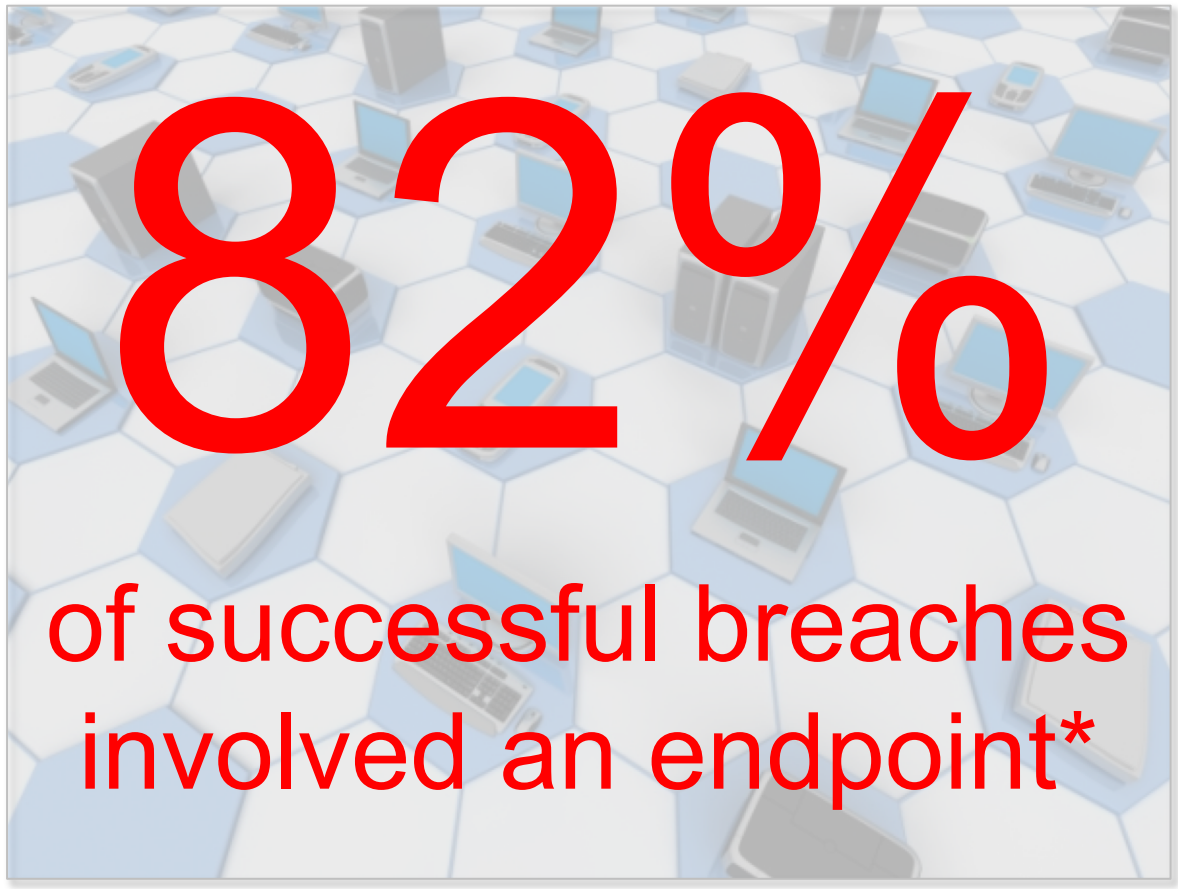


2018: The Endpoint Is STILL Important!

And STILL the weak link

Closest to humans

Underprotected



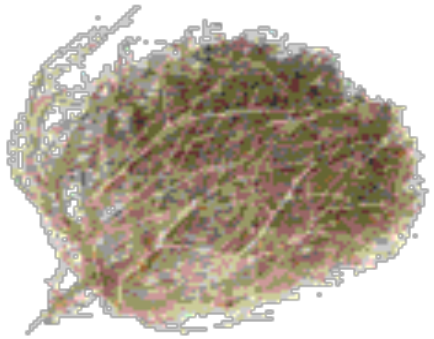
Versatile

Data-rich

*SANS 2018 Endpoint Security Survey

OK, 2019?

OK, 2019?



splunk> .conf19

OK, 2019?

(j/k…the survey hasn't been completed yet….)

SANS 2018: Stats about Endpoint Threats

- 42% of IT professionals said they had suffered a breach on their endpoints.
- 20% said they did not know if they had been breached.
- 82% of those that knew of a breach said it had involved a desktop.
- 69% cited corporate laptops as the target.
- 42% cited employee-owned laptops.
- Only 47% of antivirus capabilities detected threats.
- 26% were detected by endpoint detection and response (EDR) capabilities.
- For those exploited endpoints, the top threat vectors were found to be web “drive-bys” (63%), social engineering and phishing attacks (53%), and ransomware (50%).
- Of the IT professionals that had acquired next-gen endpoint security solutions, 37% haven’t implemented their full capabilities.
- 49% of those next-gen security solutions possess fileless malware detection features, but 38% of IT professionals haven’t implemented them.

SANS 2018: Stats about Endpoint Threats

- 42% of IT professionals said they had suffered a breach on their endpoints.
- 20% said they did not know if they had been breached.
- 82% of those that knew of a breach said it had involved a desktop.
- 69% cited corporate laptops as the target.
- 42% cited employee-owned laptops.
- Only 47% of antivirus capabilities detected threats.
- 26% were detected by endpoint detection and response (EDR) capabilities.
- For those exploited endpoints, the top threat vectors were found to be web "drive-bys" (63%), social engineering and phishing attacks (53%), and ransomware (50%).

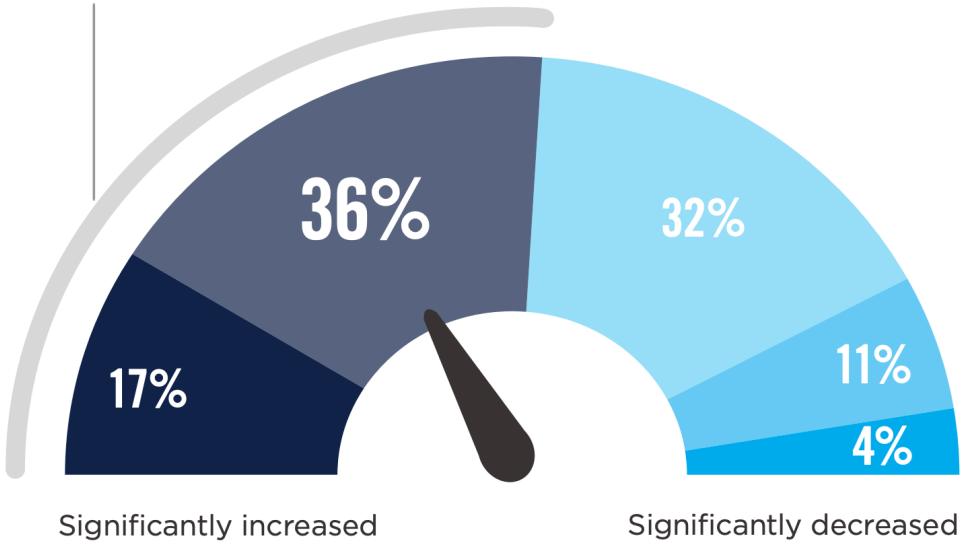
50% had a purchased a "next-gen" endpoint security solution, and…

- Of the IT professionals that had acquired next-gen endpoint security solutions, 37% haven't implemented their full capabilities.
- 49% of those next-gen security solutions possess fileless malware detection features, but 38% of IT professionals haven't implemented them.

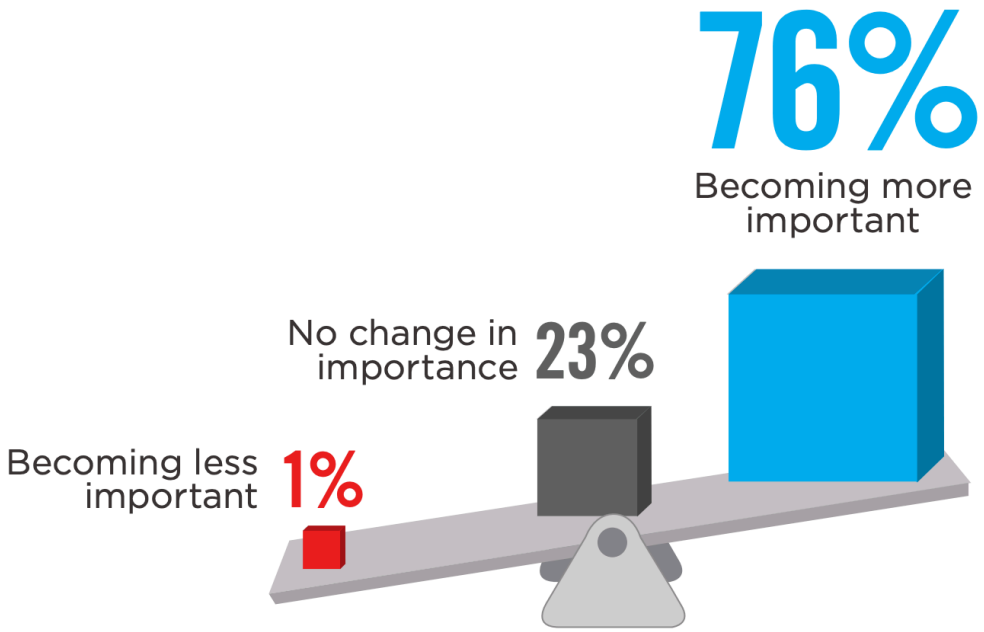
AlienVault-Sponsored 2019 Survey

How has endpoint security risk to your organization changed in the last 12 months?

53% See an increase or significant increase in endpoint security risk



How is the importance of endpoint security changing as part of your organization's overall IT security strategy?



Splunk Security Specialists:
~5x increase in endpoint assistance requests in 2019

splunk> .conf19

AlienVault-Sponsored 2019 Survey

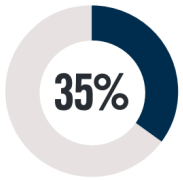
What was the most significant impact of endpoint attack(s) against your organization?

52%
Loss of end user productivity

40%
Loss of IT productivity

37%
System downtime

Reputation and brand damage



Theft of information assets

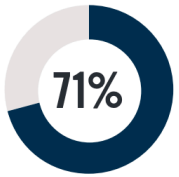
Business/revenue impact

What level of visibility are you looking for from an endpoint security solution?

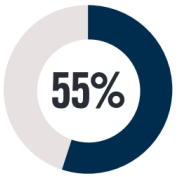
93%
Network connections

81%
File modifications

74%
Registry changes



Process information



Memory content and structures

User informatiom

Splunk Security Specialists: This matches up with the requests that we service!

Action	Asset	Count
Hacking - Use of stolen creds	Server - Mail	340
Social - Phishing	Server - Mail	270
Social - Phishing	User Dev - Desktop	251
Malware - Backdoor	User Dev - Desktop	229
Malware - C2	User Dev - Desktop	210
Hacking - Use of backdoor or C2	User Dev - Desktop	208
Malware - Spyware/Keylogger	User Dev - Desktop	103
Malware - Adminware	User Dev - Desktop	91
Misuse - Privilege abuse	Server - Database	90
Malware - Capture app data	Server - Web application	83

Table 1
Top action and asset variety combinations within breaches, (n= 2,013)

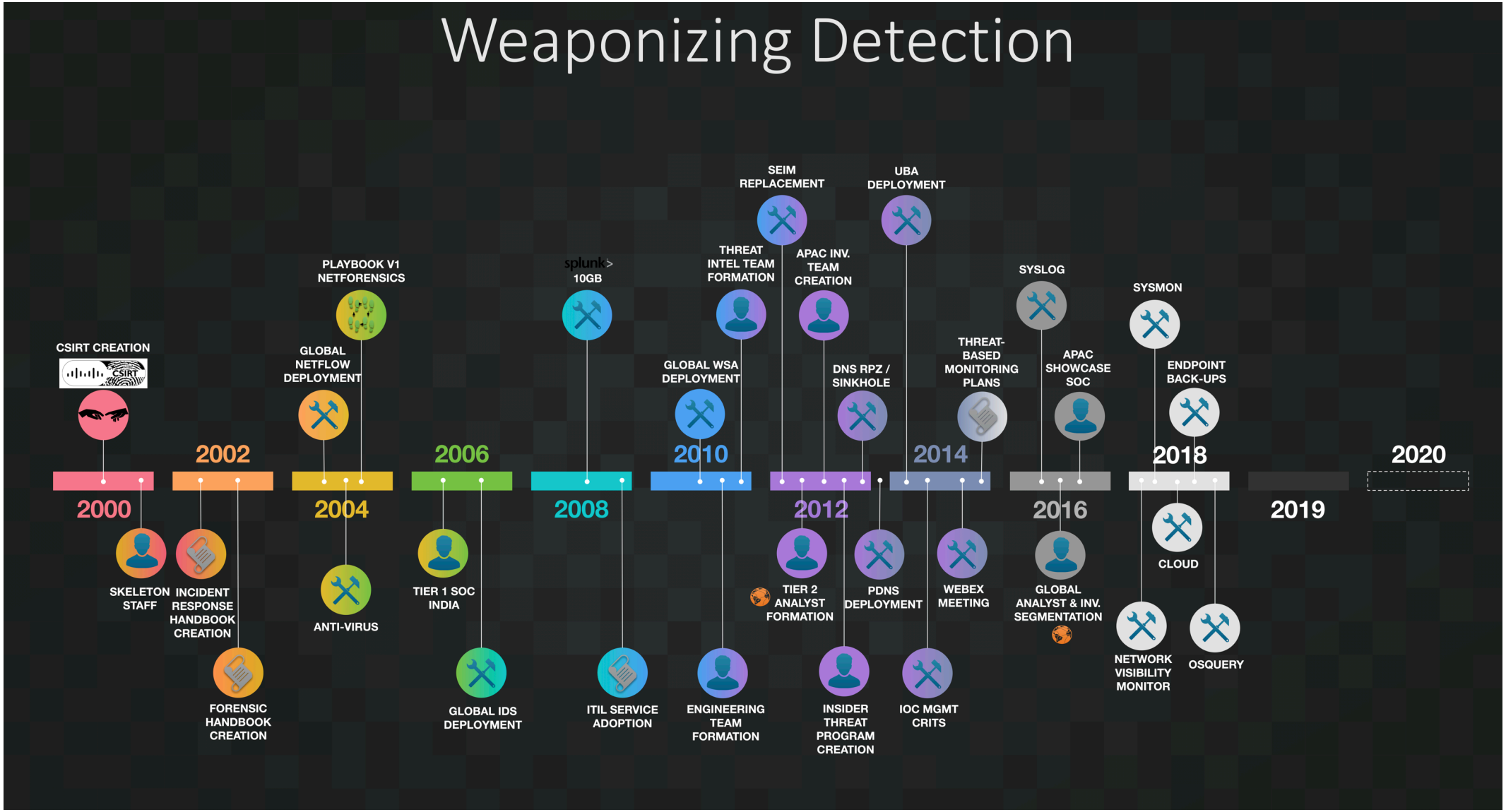
2019 Verizon DBIR

what about…

- Windows Event Logs: 46% (#1 source by volume)
  - UNIX TA: 16%
  - Windows Perfmon: 6%
  - Windows Registry: 6%
  - McAfee EPO: 6%
  - Symantec Endpoint: 4%
  - Non-Microsoft DNS: 4%
  - Carbon Black: 2%
  - Crowdstrike: 2%
  - Microsoft Sysmon: 1%

(Q1 2019 internal data)

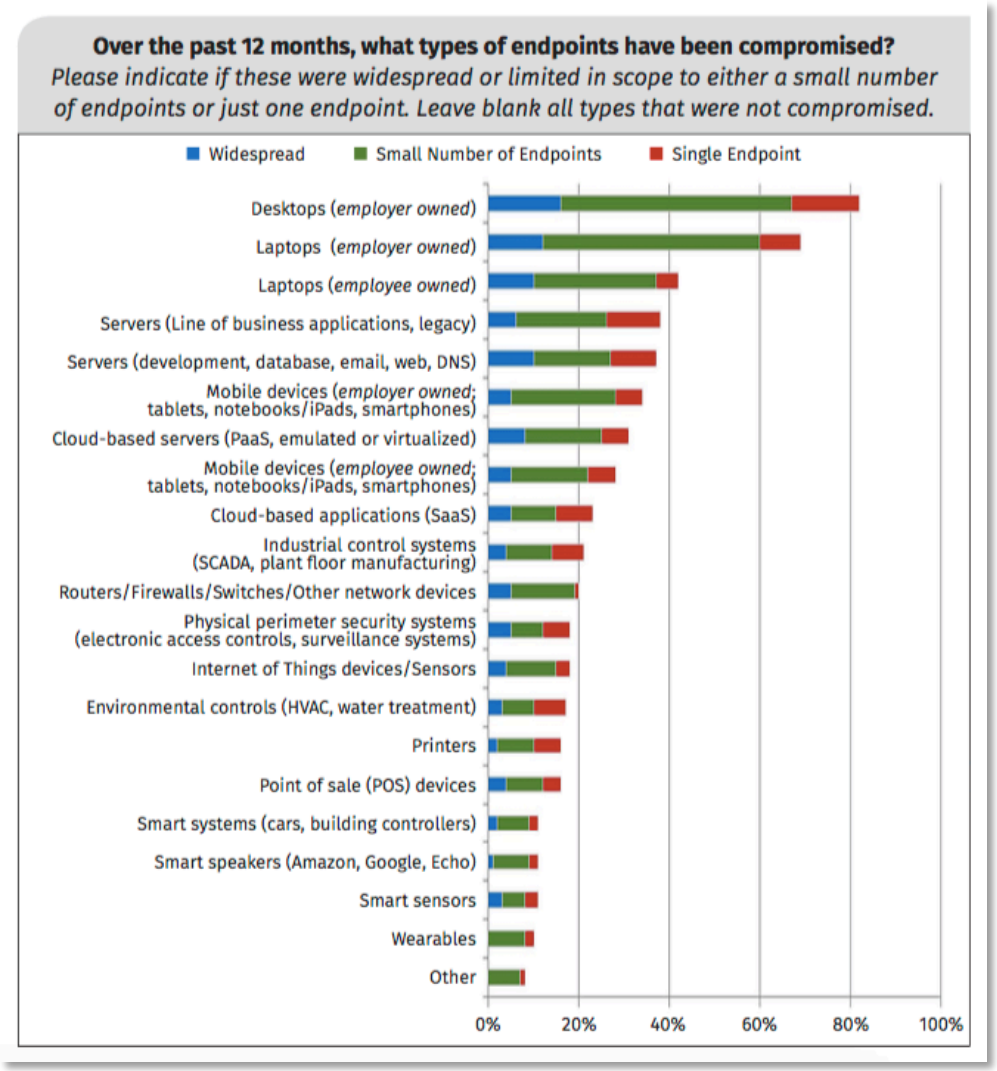
Cisco CSIRT…



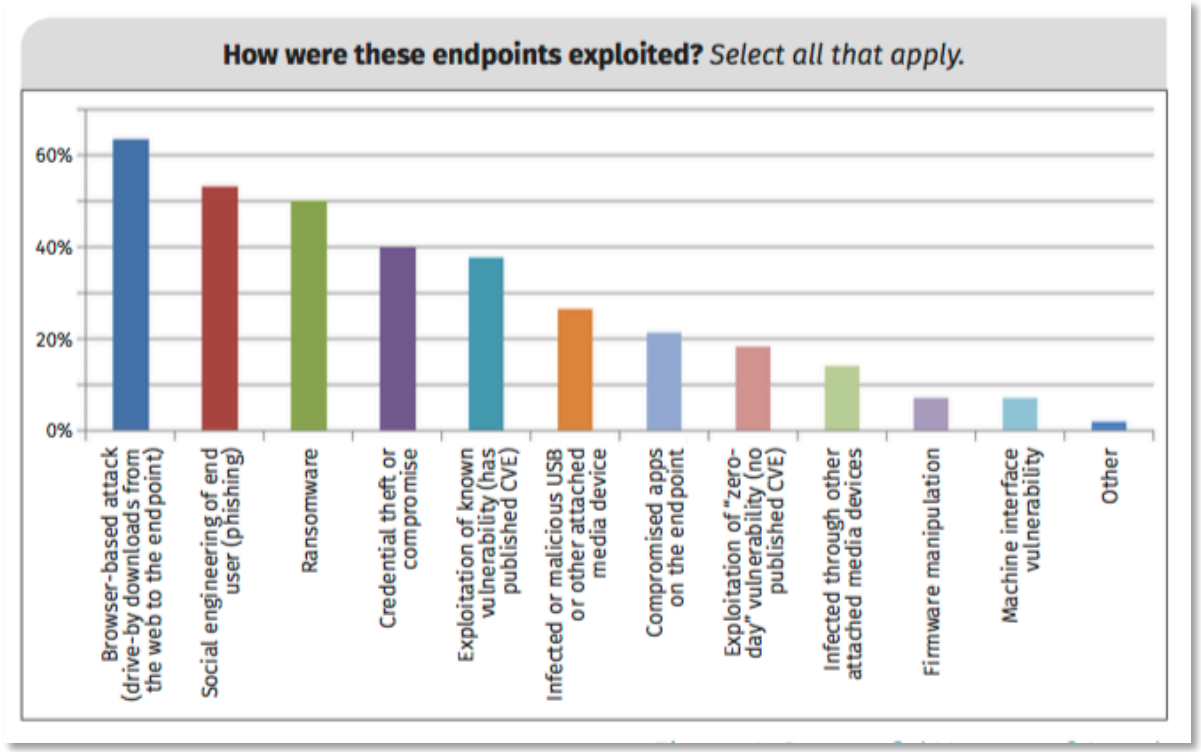
(Valites/Bollinger, 2019)

splunk> .conf19

SANS 2018: Which endpoints and how?

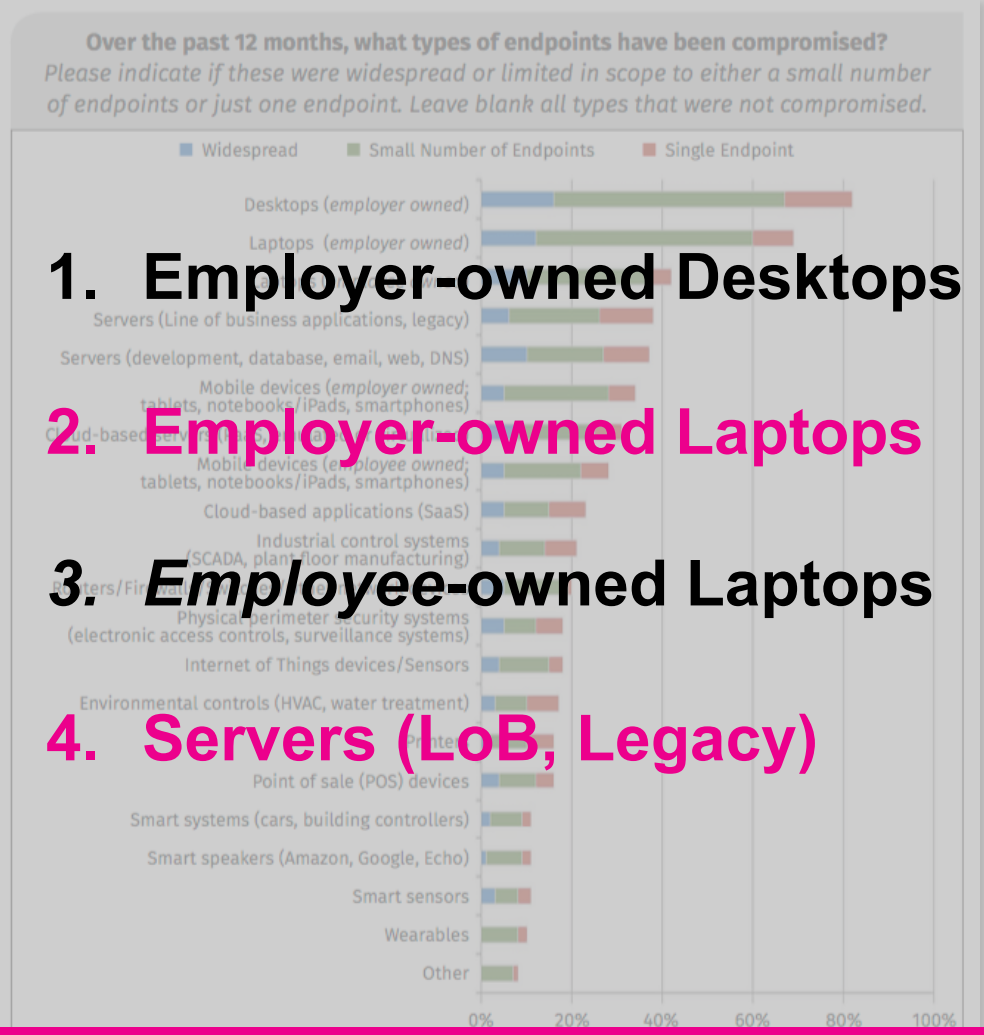


Neely, 2018



Neely, 2018

SANS 2018: Which endpoints and how?



1. Employer-owned Desktops
2. Employer-owned Laptops
3. *Employee*-owned Laptops
4. Servers (LoB, Legacy)

1. Web Click/Drive By
2. Social/Phishing
3. Ransomware
4. Cred Theft
5. Known Vuln
6. Malicious USB

Neely, 2018

Let's get hands-on!

Neely, 2018

https://[redacted]

USER: [redacted]

LOGIN INSTRUCTIONS:

Obtain kopek.

Obtain scratch card.

Use kopek to remove the special grey latex ink circle.

Insert number into URL.

Keep kopek for good luck!

splunk>enterprise App: .conf19 Endpoint Hands-On ▾ Alice Bluebird ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Introduction Search .conf19 Endpoint Hands-On

Introduction

Edit Export ▾ ...

Splunking the Endpoint V: 2019 Hands-On!

This app showcases tracking the Violent Femmes APT group as they move through the kill chain to eventually exfiltrate data from Frothly, the small homebrewing supply company at the center of (and willing victim within) Splunk's Boss of the SOC (BOTS) v2, v3 and v4 blue-team Capture-The-Flag-esque security competitions. Also included is some material surrounding Frothly's penetration test, and around their acquisition of the Thirsty Berner brewery. A summary of the data available for exploration can be viewed below.

Rather than publish all of the instructions and related resources for this session in an app, we have chosen to provide written collateral to help guide you through the data.

How to Use This App

Simply access the companion Google document in the top level of the folder below and use the "Search" link above or here to run the searches and follow along with the session.

Companion Material Downloads

- Supporting Materials on Google Drive

Select additional content to view using [illegible] boxes below:

☐ Data Summary ☐ Supporting Apps

Next Step

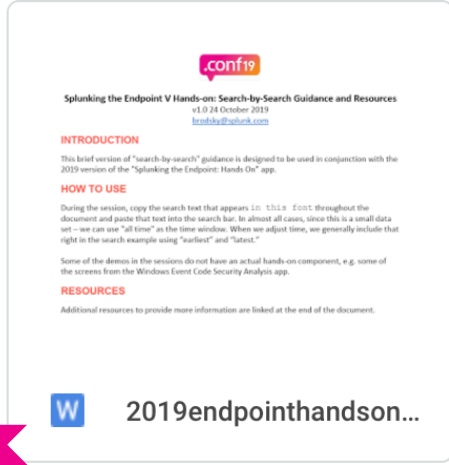
Next: Search!

Shared with me > .conf19 Splunking the Endpoint

Files

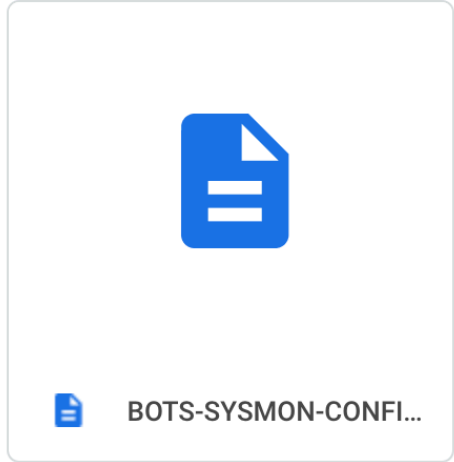
Name

2019endpointhandson...



2019endpointhandson...

BOTS-FOR-UF-inputs.c...



BOTS-SYSMON-CONFI...

splunk_wineventcode_...

This one.

(We will copy and paste from it!)

Premium

FROTHLY

Quality


Premium
FROTHLY
Quality

Thirsty Berner Brewery


FROTHY
Premium
Quality


VIOLENT
MEMES

1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions

CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

2 TECHNICAL AXIS

- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Schtasks.exe for beacon and persistence
- PSExec for lateral movment
- Yandex browser

VICTIMS

Western innovative Brewers and Home Brewing companies

VIOLENT MEMES

THREATCONNECT

Thanks ThreatConnect!


splunk>
Hands On! Sysmon and
Windows Event Logs….

What was the initial access mechanism into Thirsty Berner for Violent Memmes?

Sourcetypes: Microsoft Sysmon and Powershell logging

MITRE ATT&CK: Initial Access
T1192 Spearphishing Link
T1086 Powershell

SYSMON LOGGING AND POWERSHELL SCRIPT BLOCK LOGGING

Several actions occurred when a malicious file that originated with the phishing email was executed. One action resulted in the downloading of a script from a web site. What is the name of the script?

(29 correct!)

(Hands On Redacted)


”This is amazing. I will go back and collect ALL of my Powershell logs!”

A Cautionary Tale

How to get data in…

And avoid trouble doing so!

A guy walks into a Splunk meeting…


splunk>


splunk>


°F
F
1/2
splunk>


UNION OF SOVIET
SOCIALIST REPUBLICS

This innocent looking inputs.conf….

SPL Services / Seckit_IDM / SecKit_TA_idm_windows

inputs.conf

Source | master | 4bb45a7 | Full commit

seckit_ta_idm_windows / src / SecKit_TA_idm_windows_inputs / default / **inputs.conf**

```
1  [script://$SPLUNK_HOME\etc\apps\SecKit_TA_idm_windows\bin\runpowershell.cmd get-AllInterfaceConfig.ps1]
2  interval=3600
3  disabled=false
4  index=oswinscripts
5
```

SPL Services / Seckit_IDM / SecKit_TA_idm_windows

get-AllInterfaceConfig.ps1

Source | master | 4bb45a7 | Full commit

seckit_ta_idm_windows / src / ... / powershell / **get-AllInterfaceConfig.ps1**

```
#
# Determine the health and statistics of this Microsoft DNS Server
#
$Output = New-Object System.Collections.ArrayList
$Date = Get-Date -format 'yyyy-MM-ddTHH:mm:sszzz'
write-host -NoNewline ""$Date

# Name of Server
$ServerName = $env:ComputerName
write-host -NoNewline ""Server=`"$ServerName`""

Get-NetConnectionProfile -NetworkCategory DomainAuthenticated | ForEach-Object {
    $dict = [ORDERED]@{}
    $dict.Add('Domain',$_.Name)
    $dict.Add('InterfaceAlias',$_.InterfaceAlias)
    $dict.Add('InterfaceIndex',$_.InterfaceIndex)
    $dict.Add('NetworkCategory',$_.NetworkCategory)
    $dict.Add('IPv4Connectivity',$_.IPv4Connectivity)
    $dict.Add('IPv6Connectivity',$_.IPv6Connectivity)

    $adapter = Get-NetAdapter -InterfaceIndex $_.InterfaceIndex
    $dict.Add('InterfaceDescription',$adapter.InterfaceDescription)
    $dict.Add('Status',$adapter.Status)
    $dict.Add('MacAddress',($adapter.MacAddress -replace "-",":").ToLower())
    $dict.Add('LinkSpeed',$adapter.LinkSpeed)


    Get-NetIPConfiguration -InterfaceIndex $_.InterfaceIndex | ForEach-Object {
        Get-NetIPAddress -InterfaceIndex $_.InterfaceIndex -AddressFamily IPv4 | ForEach-Object {
          $dict.Add('IPv4Address',$_.IPAddress)
          $dict.Add('IPv4PrefixLength',$_.PrefixLength)
          $dict.Add('IPv4PrefixOrigin',$_.PrefixOrigin)
          $dict.Add('IPv4SuffixOrigin',$_.SuffixOrigin)
          $dict.Add('IPv4AddressState',$_.AddressState)
          $dict.Add('IPv4PreferredLifetime',$_.PreferredLifetime)
          $dict.Add('IPv4SkipAsSource',$_.SkipAsSource)
          $dict.Add('IPv4PolicyStore',$_.PolicyStore)

        }
        Get-DnsClientServerAddress -InterfaceIndex $_.InterfaceIndex -AddressFamily IPv4  | ForEach-Object {
                    $dict.Add('IPv4DNS',$_.ServerAddresses)
        }
        Get-NetIPAddress -InterfaceIndex $_.InterfaceIndex -AddressFamily IPv6 | ForEach-Object {
          $dict.Add('IPv6Address',$_.IPAddress)
          $dict.Add('IPv6PrefixLength',$_.PrefixLength)
          $dict.Add('IPv6PrefixOrigin',$_.PrefixOrigin)
          $dict.Add('IPv6SuffixOrigin',$_.SuffixOrigin)
          $dict.Add('IPv6AddressState',$_.AddressState)
          $dict.Add('IPv6ValidLifetime',$_.ValidLifetime)
          $dict.Add('IPv6PreferredLifetime',$_.PreferredLifetime)
```

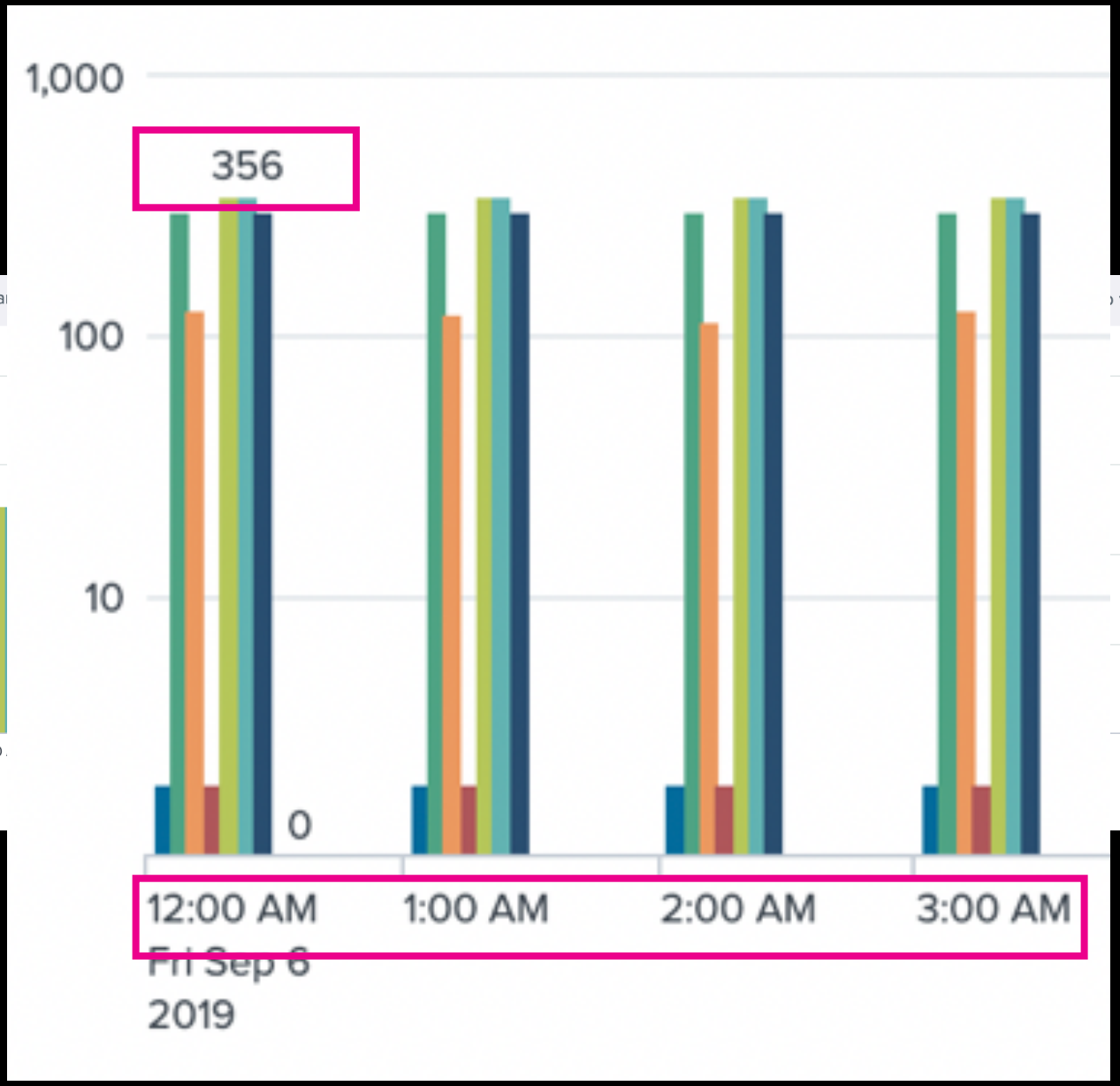
+ more below…

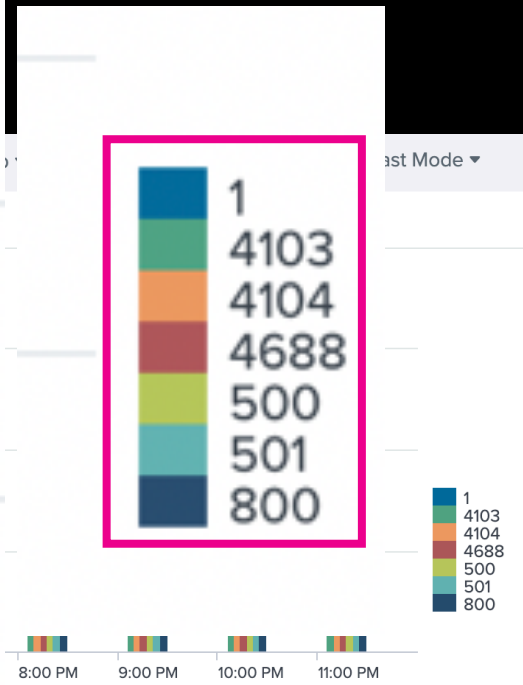
Many for-each statements for iteration = many, many, many log entries in Powershell logs due to use of Microsoft APIs

How many logs?

Teh badness.

~2000 per run.





splunk> .conf19

Seckit IDM Event Size in MB

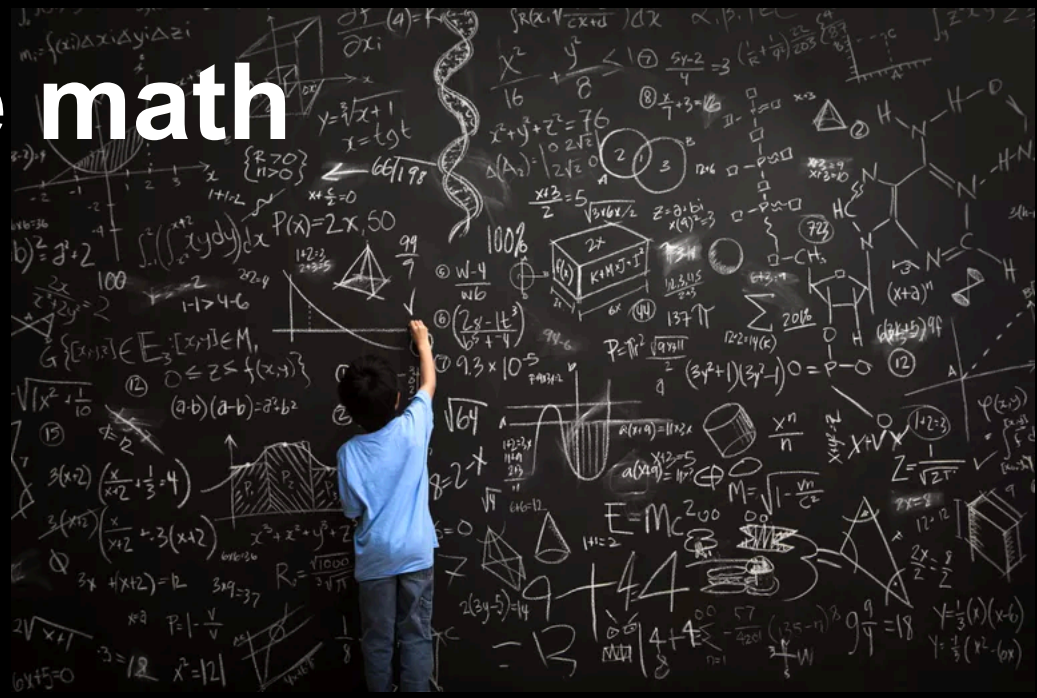
_time	1	4103	4104	4688	500	501	800
2019-09-06 00:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 01:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 02:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 03:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 04:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 05:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 06:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 07:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 08:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 09:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 10:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 11:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 12:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 13:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 14:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 15:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 16:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 17:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 18:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 19:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 20:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 21:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 22:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 23:00		0.43	1.23	0.00	0.33	0.34	0.39
	0.01	10.35	29.54	0.05	8.04	8.14	9.39

Seckit IDM Event Size in MB

_time	1	4103	4104	4688	500	501	800
2019-09-06 00:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 01:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 02:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 03:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 04:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 05:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 06:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 07:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 08:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 09:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 10:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 11:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 12:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 13:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 14:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 15:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 16:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 17:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 18:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 19:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 20:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 21:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 22:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 23:00		0.43	1.23	0.00	0.33	0.34	0.39
	0.01	10.35	29.54	0.05	8.04	8.14	9.39

~56 MB Per day per host from ONE POWERSHELL SCRIPT.

let's do the math



56/24 = 2.3MB per hour
2.3MB * 10 hours daily = 23MB per endpoint
23 * 16,000 = 368GB a day

…except ~1/3rd were servers, so…

23 * 11,000 = 253GB and 56 * 5,000 = 280GB

533GB a day.

Seckit IDM Event Size in MB

_time	1	4103	4104	4688	500	501	800
2019-09-06 00:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 01:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 02:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 03:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 04:00	0.00	0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 05:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 06:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 07:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 08:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 09:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 10:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 11:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 12:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 13:00			.23	0.00	0.33	0.34	0.39
2019-09-06 14:00			.23	0.00	0.33	0.34	0.39
2019-09-06 15:00			23	0.00	0.33	0.34	0.39
2019-09-06 16:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 17:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 18:00			1.23	0.00	0.33	0.34	0.39
2019-09-06 19:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 20:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 21:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 22:00		0.43	1.23	0.00	0.33	0.34	0.39
2019-09-06 23:00		0.43	1.23	0.00	0.33	0.34	0.39
	0.01	10.35	29.54	0.05	8.04	8.14	9.39

OMG.

time.

What are they? Should we collect?

Event Log: Windows PowerShell							
Event ID	**v2**	**v3**	**v4**	**v5**	**Correlate**	**Auditing**	**Notes**
400	X	X	X	X	403	Always logged, regardless of logging settings	This even can be used to identify (and terminate) outdated versions of PowerShell running.
403	X	X	X	X	400	Always logged, regardless of logging settings	
500	X	X	X	X	501	Requires **$LogCommandLifeCycleEvent = $true** in profile.ps1	This event is largely useless since it can be bypassed with the -nop command line switch
501	X	X	X	X	500	Requires **$LogCommandLifeCycleEvent = $true** in profile.ps1	This event is largely useless since it can be bypassed with the -nop command line switch
600	X	X	X	X	500	Always logged, regardless of logging settings	
800		X	X	X	500	ModuleLogging	This event is inconsistently logged with PowerShell V3

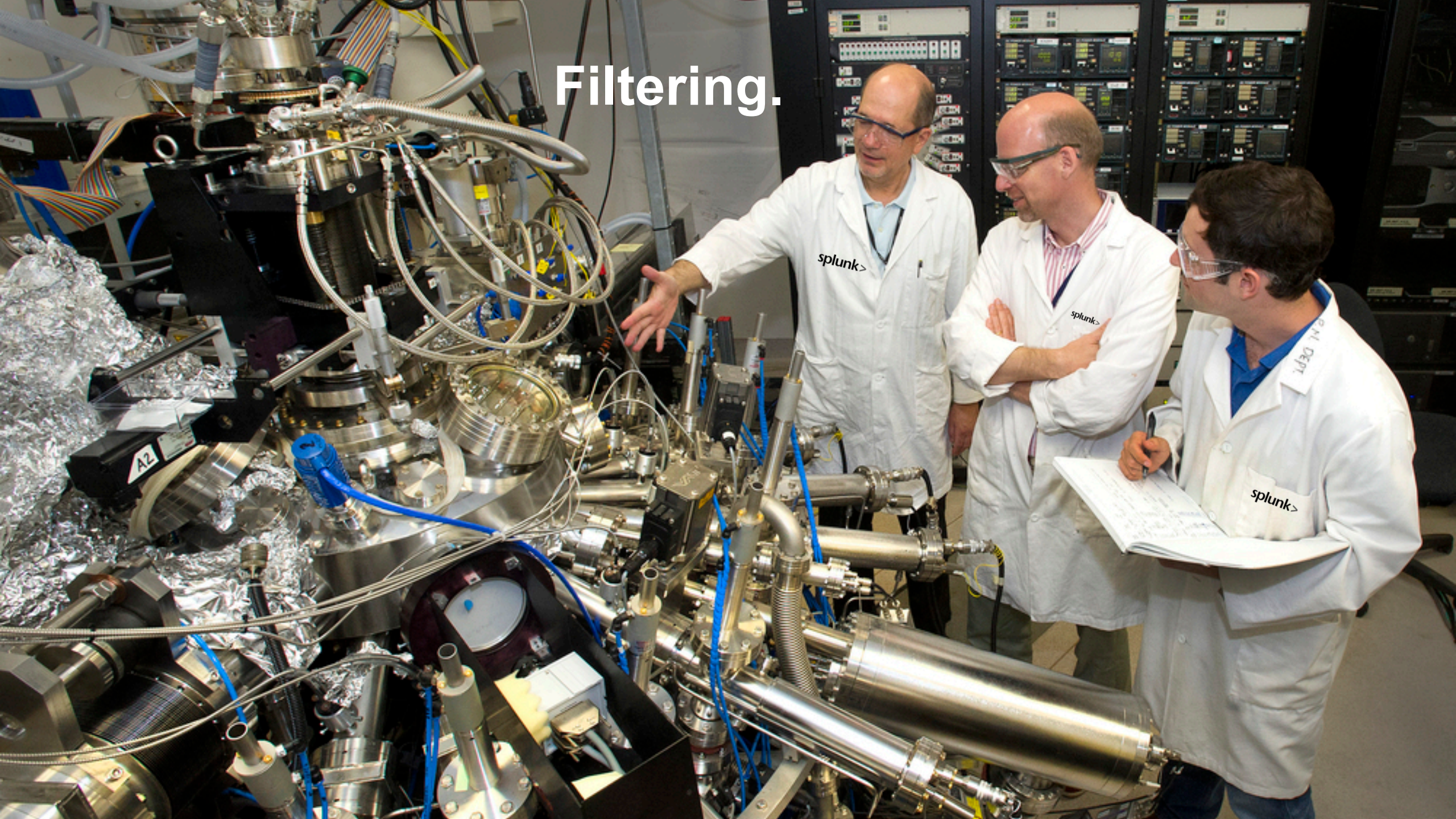
Event Log: Microsoft-Windows-PowerShell/Operational							
Event ID	**v2**	**v3**	**v4**	**v5**	**Correlate**	**Auditing**	**Notes**
4100				X			Logged when PowerShell encounters an error
4103			X	X		ModuleLogging	May be logged along with 500 & 501
4104				X		ScriptBlockLogging	
40961		X	X	X		Always logged, regardless of logging settings	
40962		X	X	X		Always logged, regardless of logging settings	

What's interesting to note is that newer versions of PowerShell will often log to both event logs simultaneously.

4104 = Almost always yes
4103 = Sometimes…
800 = same as 4103!
50x = "largely useless" – basically logs starts and stops
4100 = Sure, minor volume

https://www.eventsentry.com/blog/2018/01/powershell-p0wrh11-securing-powershell.html

Filtering.



Three places to get example blacklists…

1. Version 6.0 of the Windows TA (Splunkbase)

2. Automine's (David Shpritz)'s Github and related presentation:
https://www.aplura.com/assets/pdf/SplunkWindowsEventLogs.pdf
https://gist.github.com/automine/a3915d5238e2967c8d44b0ebcfb66147

3. What we used for BOTS
https

Here's where we ended up for SecKit IDM…

[WinEventLog://Microsoft-Windows-Powershell/Operational]
index = main
disabled = false
renderXml = 0
blacklist = EventCode="4104" Message="(?:Path:).+(?:\\splunk-powershell-common.ps1)"
blacklist1 = EventCode="4104" Message="(?:Path:).+(?:\\splunk-powershell.ps1)"
blacklist2 = EventCode="4104" Message="(?:Path:).+(?:\\generate_windows_update_logs.ps1)"
blacklist3 = EventCode="4103" Message="(?:Host Application =).(?:.*\\splunk-powershell.ps1\s.*)"
blacklist4 = EventCode="(4104|4103)" Message="(?:Path:).+(?:**get-AllInterfaceConfig.ps1**)"
blacklist5 = EventCode="4103" Message="(?:Host Application =).(?:.***get-AllInterfaceConfig.ps1**)"

[WinEventLog://Windows PowerShell]
index = main
disabled = false
renderXml = 0
blacklist = EventCode="(800|500|501)" Message="(?:HostApplication=).(?:.***get-AllInterfaceConfig.ps1**)"

EventCode

3 Values, 100% of events

Selected: Yes | No

Reports

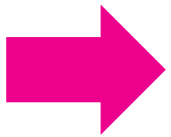
Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

Avg: 2733.7389704716293 **Min:** 800 **Max:** 4104 **Std Dev:** 1627.403367599553

Values	Count	%
4103	13,072	41.46%
800	13,072	41.46%
4104	5,385	17.08%



EventCode

2 Values, 100% of events

Selected: Yes | No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

Avg: 4103.997974888619 **Min:** 4103 **Max:** 4104 **Std Dev:** 0.04496476106941514

Values	Count	%
4104	2,464	99.797%
4103	5	0.202%

But … FAIL. It is still 1.2MB per run!

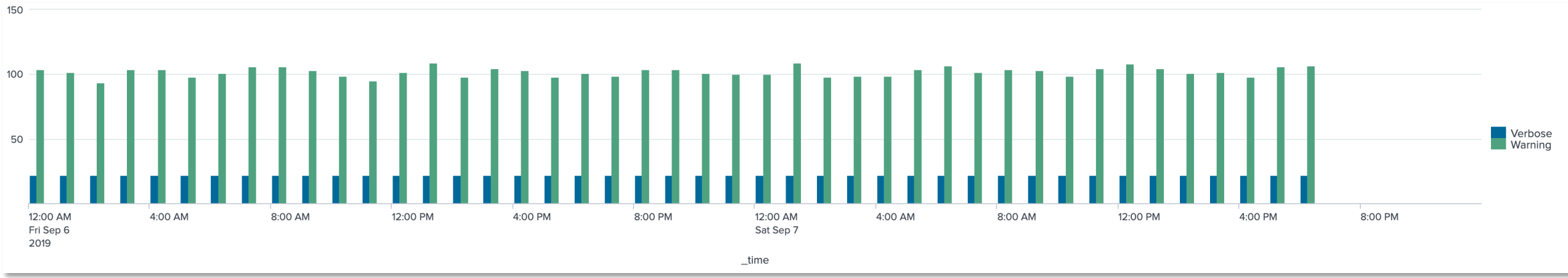
_time	bytes	MB
2019-10-17 04:00	1359250	1.2962818145751953
2019-10-17 05:00	1291778	1.2319355010986328
2019-10-17 06:00	1291778	1.2319355010986328
2019-10-17 07:00	1289974	1.230215072631836
2019-10-17 08:00	1290876	1.2310752868652344
2019-10-17 09:00	1292229	1.232365608215332
2019-10-17 10:00	1292229	1.232365608215332
2019-10-17 11:00	1289523	1.2297849655151367
2019-10-17 12:00	1290876	1.2310752868652344
2019-10-17 13:00	1291778	1.2319355010986328
2019-10-17 14:00	1291327	1.2315053939819336
2019-10-17 15:00	1291778	1.2319355010986328
2019-10-17 16:00	1292229	1.232365608215332
2019-10-17 17:00	1291327	1.2315053939819336
2019-10-17 18:00	1291327	1.2315053939819336
2019-10-17 19:00	1294033	1.234086036682129
2019-10-17 20:00	1290425	1.2306451797485352
2019-10-17 21:00	1292229	1.232365608215332

Because you can’t filter the 4104…

>	10/17/19
	11:31:20.000 PM
		10/17/2019 04:31:20 PM
		LogName=Microsoft-Windows-PowerShell/Operational
		SourceName=Microsoft-Windows-PowerShell
		EventCode=4104
		EventType=3
		Type=Warning
		ComputerName=ABUNGSTEIN-L.froth.ly
		User=NOT_TRANSLATED
		Sid=S-1-5-18
		SidType=0
		TaskCategory=Execute a Remote Command
		OpCode=On create calls
		RecordNumber=281689
		Keywords=None
		Message=Creating Scriptblock text (5 of 5):
		
		lse
		
		if ($PSBoundParameters.ContainsKey('Name')) {
		
		[object]$__cmdletization_value = ${Name}
		
		$__cmdletization_methodParameter = [Microsoft.PowerShell.Cmdletization.MethodParameter]@{Name = 'Name'; Par
		$__cmdletization_value; IsValuePresent = $true}
		
		} else {

But 4104 events “automatically” warn for suspicious modules? Maybe only collect those?

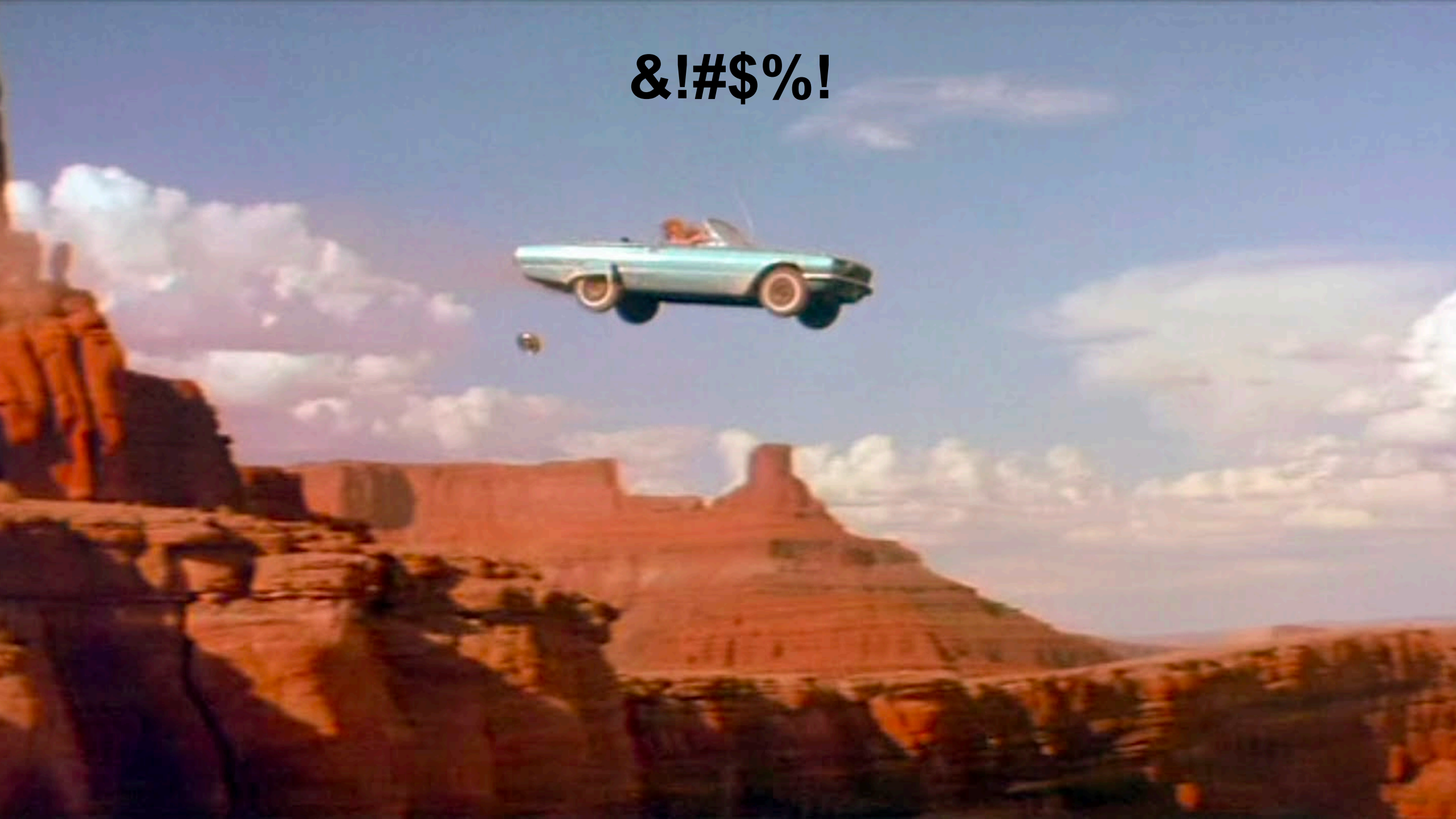
Nope.



```
// Calling Add-Type
case 3012981990: return "Add-Type";
case 3359423881: return "DllImport";

// Doing dynamic assembly building / method indirection
case 2713126922: return "DefineDynamicAssembly";
case 2407049616: return "DefineDynamicModule";
case 3276870517: return "DefineType";
case 419507039: return "DefineConstructor";
case 1370182198: return "CreateType";
case 1973546644: return "DefineLiteral";
case 3276413244: return "DefineEnum";
case 2785322015: return "DefineField";
case 837002512: return "ILGenerator";
case 3117011: return "Emit";
case 883134535: return "UnverifiableCodeAttribute";
case 2920989166: return "DefinePInvokeMethod";
case 1996222179: return "GetTypes";
case 3935635674: return "GetAssemblies";
case 955534258: return "Methods";
case 3368914227: return "Properties";

// Suspicious methods / properties on "Type"
case 398423780: return "GetConstructor";
case 376120273: return "GetConstructors";
case 1998297200: return "GetDefaultMembers";
case 1982269700: return "GetEvent";
case 1320818671: return "GetEvents";
case 1982805860: return "GetField";
case 1337439631: return "GetFields";
case 2784018083: return "GetInterface";
case 2864332761: return "GetInterfaceMap";
case 405214768: return "GetInterfaces";
case 1534378352: return "GetMember";
case 321088771: return "GetMembers";
case 1534592951: return "GetMethod";
case 327741340: return "GetMethods";
case 1116240007: return "GetNestedType";
case 243701964: return "GetNestedTypes";
case 1077700873: return "GetProperties";
case 1020114731: return "GetProperty";
case 257791250: return "InvokeMember";
case 3217683173: return "MakeArrayType";
case 821968872: return "MakeByRefType";
case 3538448099: return "MakeGenericType";
case 3207725129: return "MakePointerType";
case 1617553224: return "DeclaringMethod";
case 3152745313: return "DeclaringType";
case 4144122198: return "ReflectedType";
case 3455789538: return "TypeHandle";
case 637454598: return "UnderlyingSystemType";

// Doing things with System.Runtime.InteropServices
case 1855303451: return "InteropServices";
case 839491486: return "Marshal";
case 1928879414: return "AllocHGlobal";
case 3180922282: return "PtrToStructure";
case 1718292736: return "StructureToPtr";
case 3390778911: return "FreeHGlobal";

// General Obfuscation
case 1606191041: return "MemoryStream";
case 2147536747: return "DeflateStream";
case 1820815050: return "FromBase64String";
case 3656724093: return "EncodedCommand";
case 2920836328: return "Bypass";
case 3473847323: return "ToBase64String";
case 4192166699: return "ExpandString";
case 2462813217: return "GetPowerShell";

// Suspicious Win32 API calls
case 2123968741: return "OpenProcess";
case 3630248714: return "VirtualAlloc";
case 3303847927: return "VirtualFree";
case 512407217: return "WriteProcessMemory";
case 2357873553: return "CreateUserThread";
case 756544032: return "CloseHandle";
case 3400025495: return "GetDelegateForFunctionPointer";
case 314128220: return "kernel32";
case 2469462534: return "CreateThread";
case 3217199031: return "memcpy";
case 2283745557: return "LoadLibrary";
case 3317813738: return "GetModuleHandle";
case 2491894472: return "GetProcAddress";
case 1757922660: return "VirtualProtect";
case 2693938383: return "FreeLibrary";
case 2873914970: return "ReadProcessMemory";
case 2889068903: return "WriteByte";
case 3667925519: return "WriteInt32";
case 2742077861: return "OpenThreadToken";
case 2826980154: return "PtrToString";
case 3735047487: return "ZeroFreeGlobalAllocUnicode";
case 788615220: return "OpenProcessToken";
case 1264589033: return "GetTokenInformation";
case 2165372045: return "SetThreadToken";
case 197357349: return "ImpersonateLoggedOnUser";
case 2446460563: return "GetLogonSessionData";
case 2534763616: return "CreateProcessWithToken";
case 3512478977: return "DuplicateTokenEx";
case 3126049082: return "OpenWindowStation";
case 3990594194: return "OpenDesktop";
case 3195806696: return "MiniDumpWriteDump";
case 3990234693: return "AddSecurityPackage";
case 611728017: return "EnumerateSecurityPackages";
case 4283779521: return "GetProcessHandle";
case 845600244: return "DangerousGetHandle";
```

Almost 200 modules are “Warning” worthy.

https://github.com/PowerShell/PowerShell/blob/master/src/System.Management.Automation/engine/runtime/CompiledScriptBlock.cs



&!#$%!

LESSONS LEARNED!

- The SecKit IDM Interface Config powershell script is fundamentally incompatible with recommended powershell logging. The 4104 from it are unfilterable at the UF/HF level. Reduce interval?
- Many other useful powershell logs may be difficult to filter: YMMV.
- Make sure you aren’t collecting duplicate info (4103 and 800!)
- Make sure you know what you’re collecting, at what interval, and why! Maybe an alternative to powershell for gathering?


splunk>
Can we filter better?
YES. But first…

“Thanks for the advice. But what event codes SHOULD we collect?”


splunk>
16
7
12
1116
3
4624
13
11
3
800
4663
4103
4104
5156
4647
1102
22
4660
4704
1102
7045
1
4625
4688
4100
That’s a good question!

We typically answer with…

Microsoft

SANS

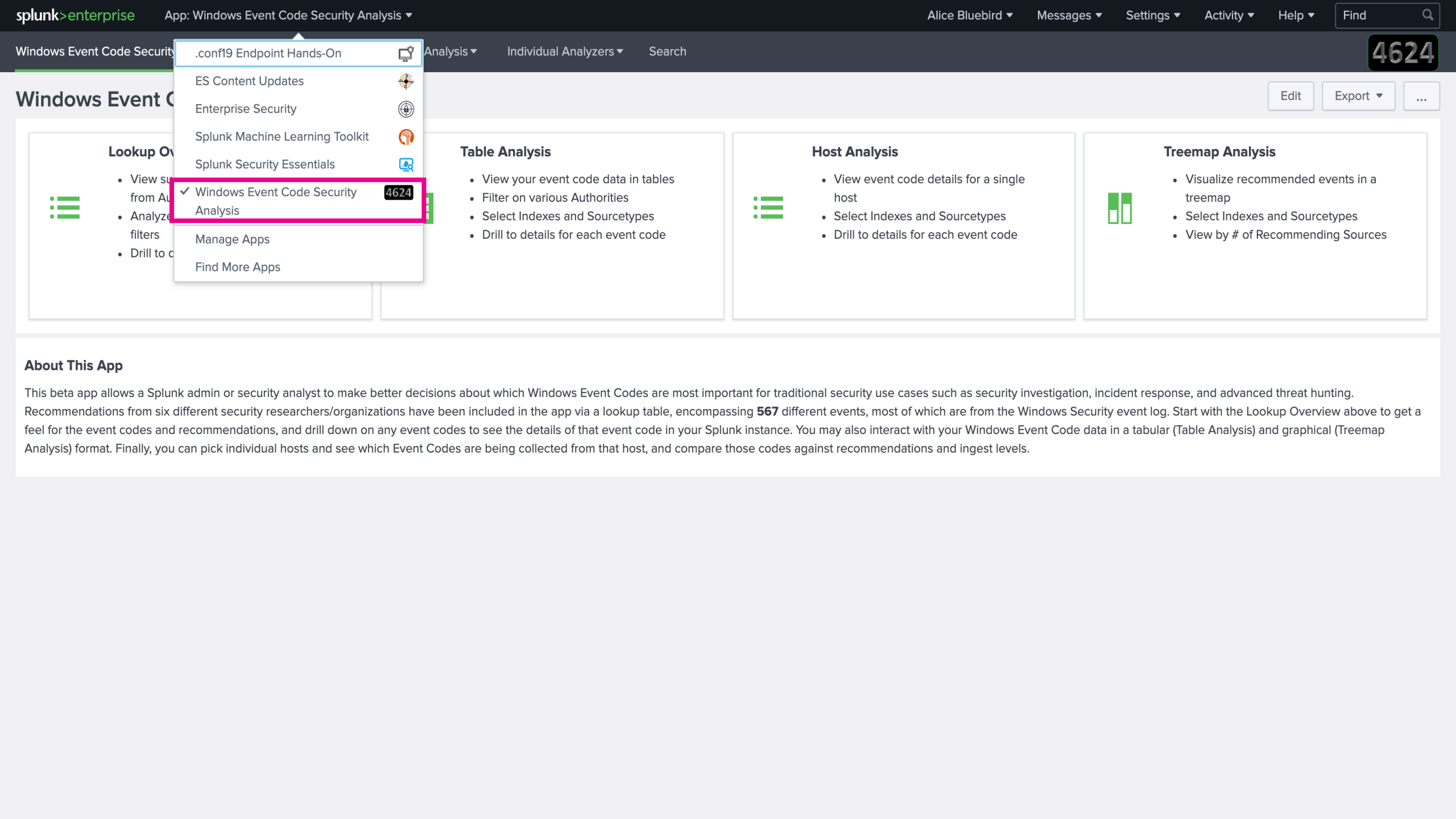
We typically answer with…

Microsoft

What if we had an app for that?

SANS


splunk>
Hands On! Windows
Event Code Guidance!


splunk>enterprise
App: Windows Event Code Security Analysis
Alice Bluebird
Messages
Settings
Activity
Help
Find
Windows Event Code Security
Analysis
Individual Analyzers
Search
4624
.conf19 Endpoint Hands-On
ES Content Updates
Enterprise Security
Splunk Machine Learning Toolkit
Splunk Security Essentials
Windows Event Code Security Analysis
4624
Manage Apps
Find More Apps
Windows Event C
Edit
Export
...
Lookup Ov
View su
from Au
Analyze
filters
Drill to d
Table Analysis
View your event code data in tables
Filter on various Authorities
Select Indexes and Sourcetypes
Drill to details for each event code
Host Analysis
View event code details for a single host
Select Indexes and Sourcetypes
Drill to details for each event code
Treemap Analysis
Visualize recommended events in a treemap
Select Indexes and Sourcetypes
View by # of Recommending Sources
About This App
This beta app allows a Splunk admin or security analyst to make better decisions about which Windows Event Codes are most important for traditional security use cases such as security investigation, incident response, and advanced threat hunting. Recommendations from six different security researchers/organizations have been included in the app via a lookup table, encompassing 567 different events, most of which are from the Windows Security event log. Start with the Lookup Overview above to get a feel for the event codes and recommendations, and drill down on any event codes to see the details of that event code in your Splunk instance. You may also interact with your Windows Event Code data in a tabular (Table Analysis) and graphical (Treemap Analysis) format. Finally, you can pick individual hosts and see which Event Codes are being collected from that host, and compare those codes against recommendations and ingest levels.

Windows Event Code Security Analysis

Edit | Export ▾ | ...

Lookup Overview

- View summarized recommendations from Authorities
- Analyze all details in the lookup via filters
- Drill to details in your data

Table Analysis

- View your event code data in tables
- Filter on various Authorities
- Select Indexes and Sourcetypes
- Drill to details for each event code

Host Analysis

- View event code details for a single host
- Select Indexes and Sourcetypes
- Drill to details for each event code

Treemap Analysis

- Visualize recommended events in a treemap
- Select Indexes and Sourcetypes
- View by # of Recommending Sources

Click.

About This App

This beta app allows a Splunk admin or security analyst to make better decisions about which Windows Event Codes are most important for traditional security use cases such as security investigation, incident response, and advanced threat hunting. Recommendations from six different security researchers/organizations have been included in the app via a lookup table, encompassing **567** different events, most of which are from the Windows Security event log. Start with the Lookup Overview above to get a feel for the event codes and recommendations, and drill down on any event codes to see the details of that event code in your Splunk instance. You may also interact with your Windows Event Code data in a tabular (Table Analysis) and graphical (Treemap Analysis) format. Finally, you can pick individual hosts and see which Event Codes are being collected from that host, and compare those codes against recommendations and ingest levels.

Lookup Overview

Export ▾ ...

Select one or more Authorities using the filter

Authority

Michael Gough × NSA ×

Hide Filters

Select “Michael Gough and NSA.”

Current Filter: 2 Authorities

ec_guidance_gough=1 OR ec_guidance_nsa=1

Number of Event Codes Total in Lookup

567

EVENT CODES IN LOOKUP

Number of Event Codes Selected (2 selected)

220

EVENT CODES SELECTED

Top 10 Event Log Sources (2 selected)

Event Log	count	percent
Security	92	41.818182
Microsoft-Windows-Windows Defender/Operational	20	9.090909
System	17	7.727273
Microsoft-Windows-WLAN-AutoConfig/Operational	13	5.909091
Application	11	5.000000
Microsoft-Windows-Powershell/Operational	7	3.181818
System or Sysmon	6	2.727273
Microsoft-Windows-Application-Experience/Program-Inventory	6	2.727273
Microsoft-Windows-TaskScheduler/Operational	5	2.272727
Microsoft-Windows-CodeIntegrity/Operational	5	2.272727

This table displays, for the current selected authorities, what event codes are recommended from those authorities and what event sources they come from.

Codes Ranked by Weight (2 selected)

EventCode	Event Log	EventDescription	Total
4624	Security	An account was successfully logged on.	6
4625	Security	An account failed to log on.	6
4657	Security	A registry value was modified.	5
4719	Security	System audit policy was changed.	5
5140	Security	A network share object was accessed.	5
4634	Security	An account was logged off.	4
4648	Security	A logon was attempted using explicit credentials.	4
4688	Security	A new process has been created.	4
4720	Security	A user account was created.	4
4722	Security	A user account was enabled.	4

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

This table displays, for the current selected authorities, what event codes are recommended from those authorities and how many sources (in total) suggest that event code should be collected.

Lookup Overview

Export ▾ ...

Select one or more Authorities using the filter

Authority

Michael Gough × NSA ×

Hide Filters

Current Filter: 2 Authorities

ec_guidance_gough=1 OR ec_guidance_nsa=1

Number of Event Codes Total in Lookup

567

EVENT CODES IN LOOKUP

Number of Event Codes Selected (2 selected)

220

EVENT CODES SELECTED

Top 10 Event Log Sources (2 selected)

Event Log	count	percent
Security	92	41.818182
Microsoft-Windows-Windows Defender/Operational	20	9.090909
System	17	7.727273
Microsoft-Windows-WLAN-AutoConfig/Operational	13	5.909091
Application	11	5.000000
Microsoft-Windows-Powershell/Operational	7	3.181818
System or Sysmon	6	2.727273
Microsoft-Windows-Application-Experience/Program-Inventory	6	2.727273
Microsoft-Windows-TaskScheduler/Operational	5	2.272727
Microsoft-Windows-CodeIntegrity/Operational	5	2.272727

This table displays, for the current selected authorities, what event codes are recommended from those authorities and what event sources they come from.

Codes Ranked by Weight (2 selected)

EventCode	Event Log	EventDescription	Total
4624	Security	An account was successfully logged on.	6
4625	Security	An account failed to log on.	6
4657	Security	A registry value was modified.	5
4719	Security	System audit policy was changed.	5
5140	Security	A network share object was accessed.	5
4634	Security	An account was logged off.	4
4648	Security	A logon was attempted using explicit credentials.	4
4688	Security	A new process has been created.	4
4720	Security	A user account was created.	4
4722	Security	A user account was enabled.	4

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

This table displays, for the current selected authorities, what event codes are recommended from those authorities and how many sources (in total) suggest that event code should be collected.

Lookup Overview

Export ▾ ...

Select one or more Authorities using the filter

Authority

Michael Gough × NSA ×

Hide Filters

Current Filter: 2 Authorities

ec_guidance_gough=1 OR ec_guidance_nsa=1

Number of Event Codes Total in Lookup

567

EVENT CODES IN LOOKUP

Number of Event Codes Selected (2 selected)

220

EVENT CODES SELECTED

Top 10 Event Log Sources (2 selected)

Event Log	count	
Security	92	
Microsoft-Windows-Windows Defender/Operational	20	
System	17	
Microsoft-Windows-WLAN-AutoConfig/Operational	13	
Application		
Microsoft-Windows-Powershell/Operational	7	
System or Sysmon	6	
Microsoft-Windows-Application-Experience/Program-Inventory	6	
Microsoft-Windows-TaskScheduler/Operational	5	2.272
Microsoft-Windows-CodeIntegrity/Operational	5	2.272727

This table displays, for the current selected authorities, what event codes are recommended from those authorities and what event sources they come from.

SCROLL DOWN

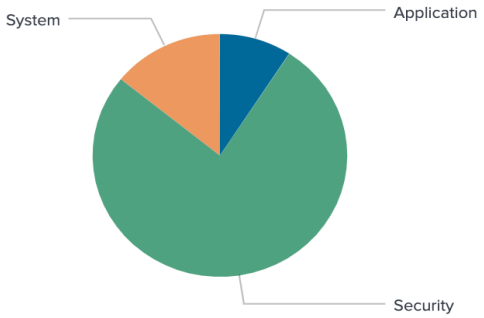
nked by Weight (2 selected)

ode	Event Log	EventDescription	Total
4624	Security	An account was successfully logged on.	6
4625	Security	An account failed to log on.	6
4657	Security	A registry value was modified.	5
4719	Security	System audit policy was changed.	5
	urity	A network share object was accessed.	5
	Security	An account was logged off.	4
648	Security	A logon was attempted using explicit credentials.	4
4688	Security	A new process has been created.	4
4720	Security	A user account was created.	4
4722	Security	A user account was enabled.	4

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

This table displays, for the current selected authorities, what event codes are recommended from those authorities and how many sources (in total) suggest that event code should be collected.

Security/System/Application Breakdown (2 selected)



Count of Codes by Authority (2 selected)

Category	Total EventCodes	URL
NSA	194	https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events
Microsoft AD	91	https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
Andrea Fortuna	88	https://www.andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/
Michael Gough	49	https://www.malwarearchaeology.com/cheat-sheets
Mike Lombardi	15	https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1511904841.pdf
SANS Forensics Guidance	15	https://isc.sans.edu/forums/diary/Windows+Events+log+for+IRForensics+Part+1/21493/

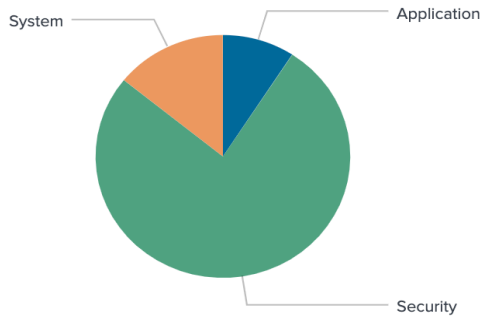
This table displays, for the current selected authorities, what overlap exists with other authorities. In otherwords "for my currently selected authorities, what other authorities recommend how many of the same event codes?

Michael Gough ATT&CK Mapping (2 selected)

https://www.malwarearchaeology.com/s/Windows-ATTCK_Logging-Cheat-Sheet_ver_Sept_2018.pdf

EventCode	Event Description	Event Log	Andrea Fortuna	Michael Gough	Microsoft	Mike Lombardi	NSA	OTHER	SANS Forensics Guidance	Total
4624	An account was successfully logged on.	Security	1	1	1	1	1	0	1	6
4657	A registry value was modified.	Security	1	1	1	1	1	0	0	5
5140	A network share object was accessed.	Security	1	1	1	1	1	0	0	5
4688	A new process has been created.	Security	0	1	1	1	1	0	0	4
5145	A network share object was checked to see whether the client can be granted desired access.	Security	1	1	1	0	1	0	0	4
5156	The Windows Filtering Platform has allowed a connection.	Security	1	1	1	1	0	0	0	4
7045	New Windows Service	System	0	1	0	1	1	0	1	4
4104	Script Block Logging	Microsoft-Windows-Powershell/Operational	0	1	0	1	1	0	0	3
4663	An attempt was made to access an object.	Security	1	1	1	0	0	0	0	3
4103	Module Logging	Microsoft-Windows-Powershell/Operational	0	1	0	0	1	0	0	2

Security/System/Application Breakdown (2 selected)



Count of Codes by Authority (2 selected)

Category	Total EventCodes	URL
NSA	194	https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events
Microsoft AD	91	https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
Andrea Fortuna	88	https://www.andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/
Michael ough	49	https://www.malwarearchaeology.com/cheat-sheets
	15	https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1511904841.pdf
	15	https://isc.sans.edu/forums/diary/Windows+Events+log+for+IRForensics+Part+1/21493/

SCROLL UP

plays, for the current selected authorities, what overlap exists with other authorities. In otherwords "for my currently orities, what other authorities recommend how many of the same event codes?

Michael Gough ATT&CK Mapping (2 selected)

https://www.malwarearchaeology.com/s/Windows-ATTCK_Logging-Cheat-Sheet_ver_Sept_2018.pdf

EventCode	Event Description	Event Log	Andrea Fortuna	Michael Gough	Microsoft	Mike Lombardi	NSA	OTHER	SANS Forensics Guidance	Total
4624	An account was successfully logged on.	Security	1	1	1	1	1	0	1	6
4657	A registry value was modified.	Security	1	1	1	1	1	0	0	5
5140	A network share object was accessed.	Security	1	1	1	1	1	0	0	5
4688	A new process has been created.	Security	0	1	1	1	1	0	0	4
5145	A network share object was checked to see whether the client can be granted desired access.	Security	1	1	1	0	1	0	0	4
5156	The Windows Filtering Platform has allowed a connection.	Security	1	1	1	1	0	0	0	4
7045	New Windows Service	System	0	1	0	1	1	0	1	4
4104	Script Block Logging	Microsoft-Windows-Powershell/Operational	0	1	0	1	1	0	0	3
4663	An attempt was made to access an object.	Security	1	1	1	0	0	0	0	3
4103	Module Logging	Microsoft-Windows-Powershell/Operational	0	1	0	0	1	0	0	2

Lookup Overview

Export ▾ ...

Select one or more Authorities using the filter

Authority

Michael Gough × NSA ×

Hide Filters

Current Filter: 2 Authorities

ec_guidance_gough=1 OR ec_guidance_nsa=1

Number of Event Codes Total in Lookup

567

EVENT CODES IN LOOKUP

Number of Event Codes Selected (2 selected)

220

EVENT CODES SELECTED

Top 10 Event Log Sources (2 selected)

Event Log	count	percent
Security	92	41.818182
Microsoft-Windows-Windows Defender/Operational	20	9.090909
System	17	7.727273
Microsoft-Windows-WLAN-AutoConfig/Operational	13	5.909091
Application	11	5.000000
Microsoft-Windows-Powershell/Operational	7	3.181818
System or Sysmon	6	2.727273
Microsoft-Windows-Application-Experience/Program-Inventory	6	2.727273
Microsoft-Windows-TaskScheduler/Operational	5	2.272727
Microsoft-Windows-CodeIntegrity/Operational	5	2.272727

This table displays, for the current selected authorities, what event codes are recommended from those authorities and what event sources they come from.

Codes Ranked by Weight (2 selected)

EventCode	Event Log	EventDescription	Total
4624	Security	An account was successfully logged on.	6
4625	Security	An account failed to log on.	6
4657	Security	A registry value was modified.	5
4719	Security	System audit policy was changed.	5
5140	Security	A network share object was accessed.	5
4634	Security	An account was logged off.	4
4648	Security	A logon was attempted using explicit credentials.	4
4688	Security	A new process has been created.	4
4720	Security	A user account was created.	4
4722	Security	A user account was enabled.	4

Click on 4688.

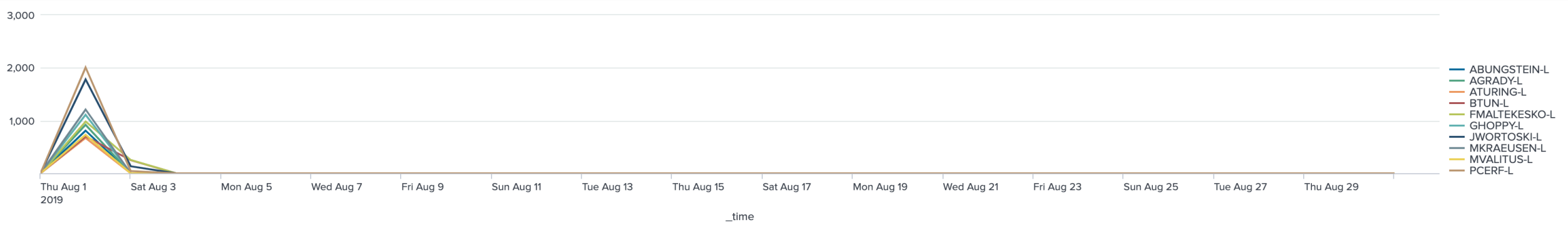
« Prev 1 2 3 4 5 6 7 8 9 10 Next »

This table displays, for the current selected authorities, what event codes are recommended from those authorities and how many sources (in total) suggest that event code should be collected.

Individual Event Code Analysis

Export ...

Aug 2019 | Sources: ALL | Indexes: ALL | Event Code: 4688 | Sourcetype: wineventlog / xmlwineventlog | Submit | Hide Filters



10	YES	22	2	YES	NO
HOSTS WITH THIS EVENT CODE	TAGGED SOMEWHERE IN CIM?	MB SEEN FROM THIS EVENT IN TIME SELECTED	AVG MB SEEN PER HOST IN TIME SELECTED	MITRE ATT&CK FRAMEWORK?	POSSIBLE DUPLICATE?

Event Code	Event Log	Event Description	Number of Recommendations	sourcetype	Number of Hosts	Number of Events	source	indexes
4688	Security	A new process has been created.	4	WinEventLog	10	11600	WinEventLog:Security	main

<1m ago

Authority	Recommends?
Andrea Fortuna	NO
Michael Gough	YES
Microsoft	YES
Mike Lombardi	YES
NSA	YES
SANS Forensics Guidance	NO

<1m ago

Individual Event

Export ▾ ...

Recommended Events Table
Other Events Table

Aug 2019 | ALL × | ALL × | Event Code: 4688 | Sourcetype: (•) wineventlog ( ) xmlwineventlog | Submit | Hide Filters

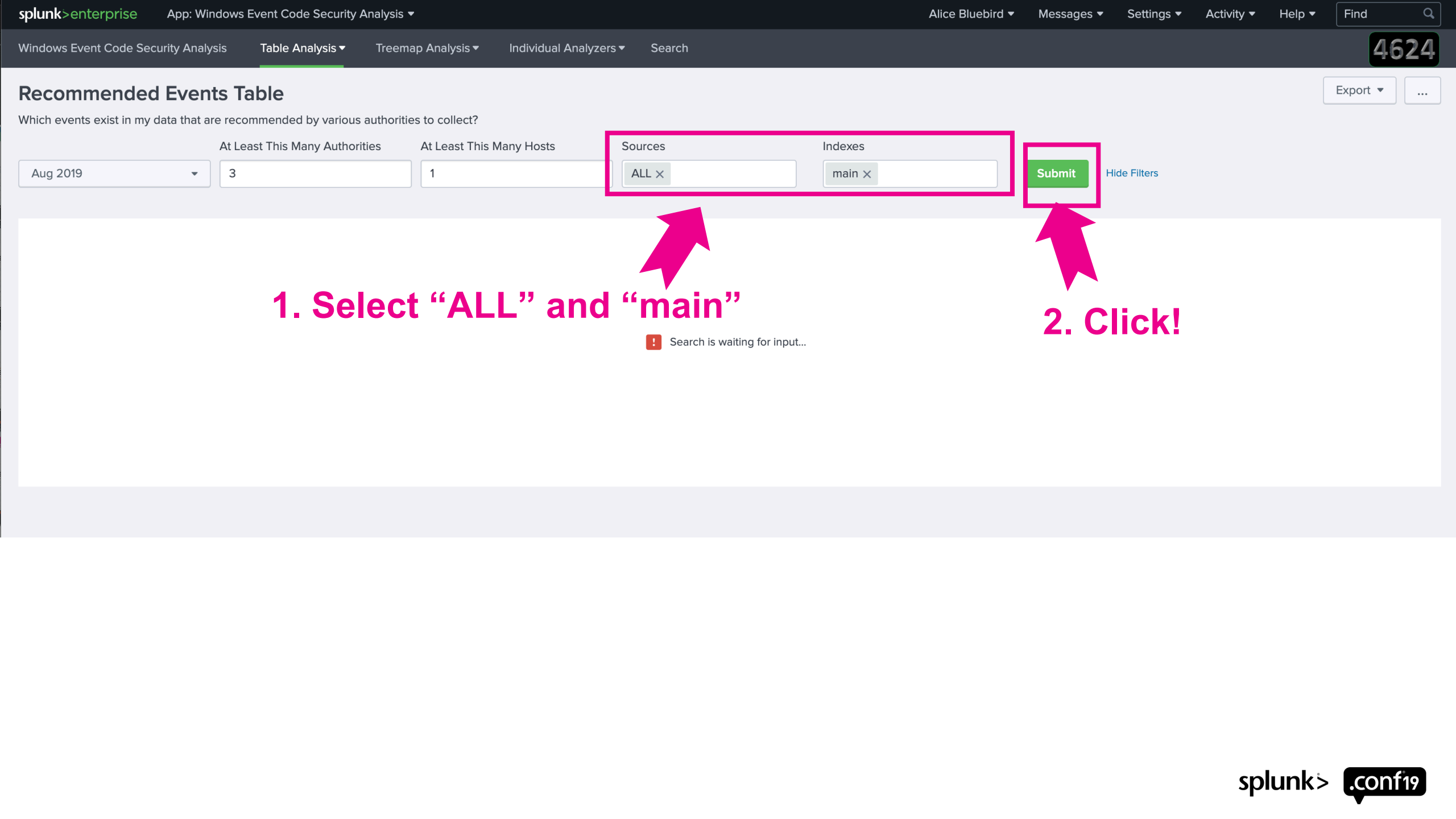
Click and select "Recommended Events Table"

10	YES	22	2	YES	NO
HOSTS WITH THIS EVENT CODE	TAGGED SOMEWHERE IN CIM?	MB SEEN FROM THIS EVENT IN TIME SELECTED	AVG MB SEEN PER HOST IN TIME SELECTED	MITRE ATT&CK FRAMEWORK?	POSSIBLE DUPLICATE?

Event Code	Event Log	Event Description	Number of Recommendations	sourcetype	Number of Hosts	Number of Events	source	indexes
4688	Security	A new process has been created.	4	WinEventLog	10	11600	WinEventLog:Security	main

24m ago

Authority	Recommends?
Andrea Fortuna	NO
Michael Gough	YES
Microsoft	YES
Mike Lombardi	YES
NSA	YES
SANS Forensics Guidance	NO



Recommended Events Table

Export ▾ ...

Which events exist in my data that are recommended by various authorities to collect?

Aug 2019	At Least This Many Authorities: 3	At Least This Many Hosts: 1	Sources: ALL ×	Indexes: main ×	Submit	Hide Filters

Which events are we collecting that we "should" be, and from how many hosts?

EventCode	ATT&CK	Category	Event Log	EventDescription	Level	NumHosts	Source	Subcategory	duplicate_possible	observed_volume	NumRecommenders
4624	1	Logon/Logoff	Security	An account was successfully logged on.	Information	23	WinEventLog:Security	Logon	0	In Development	7
4634	0	Logon/Logoff	Security	An account was logged off.	Information	17	WinEventLog:Security	Logoff	0	In Development	5
4648	0	Logon/Logoff	Security	A logon was attempted using explicit credentials.	Information	14	WinEventLog:Security	Logon	0	In Development	5
4672	0	Privilege Use	Security	Special privileges assigned to new logon.	Information	12	WinEventLog:Security	Sensitive Privilege Use / Non Sensitive Privilege Use	0	In Development	4
4688	1	Detailed Tracking	Security	A new process has been created.	Information	10	WinEventLog:Security	Process Creation	0	In Development	5
4647	0	Logon/Logoff	Security	User initiated logoff	Information	7	WinEventLog:Security	Logoff	0	In Development	4
4625	0	Logon/Logoff	Security	An account failed to log on.	Information	6	WinEventLog:Application WinEventLog:Security	Logon	1	In Development	7
4719	0	Policy Change	Security	System audit policy was changed.	Information	6	WinEventLog:Security	Audit Policy Change	0	In Development	6
4778	0	Logon/Logoff	Security	A session was reconnected to a Window Station.	Information	6	WinEventLog:Security	Other Logon/Logoff Events	0	In Development	5
4779	0	Logon/Logoff	Security	A session was disconnected from a Window Station.	Information	6	WinEventLog:Security	Other Logon/Logoff Events	0	In Development	5
7045	1	System	System	New Windows Service	Information	5	WinEventLog:System	Service	0	In Development	4
4720	0	Account Management	Security	A user account was created.	Information	4	WinEventLog:Security	User Account Management	0	In Development	5
4722	0	Account	Security	A user account was enabled.	Information	4	WinEventLog:Security	User Account	0	In Development	5

Other Events Table

Export ▾ ...

Which events exist in my data that are NOT recommended by any authorities?

At Least This Many Hosts: 1 | Sources: ALL × | Indexes: main × | Aug 2019 | Submit | Hide Filters

EventCode	ATT&CK	Category	Event Log	EventDescription	Level	NumHosts	Source	Subcategory	duplicate_possible	observed_volume	NumRecommenders
40961	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	19	WinEventLog:Microsoft-Windows-PowerShell/Operational WinEventLog:Microsoft-Windows-Powershell/Operational WinEventLog:System	Not in Lookup	Not in Lookup	Not in Lookup	0
40962	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	19	WinEventLog:Microsoft-Windows-PowerShell/Operational WinEventLog:Microsoft-Windows-Powershell/Operational	Not in Lookup	Not in Lookup	Not in Lookup	0
53504	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	19	WinEventLog:Microsoft-Windows-PowerShell/Operational WinEventLog:Microsoft-Windows-Powershell/Operational	Not in Lookup	Not in Lookup	Not in Lookup	0
0	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	14	WinEventLog:Application	Not in Lookup	Not in Lookup	Not in Lookup	0
15	0	Sysmon	Sysmon	File Create Stream Hash	Information	12	WinEventLog:Application WinEventLog:System	Sysmon	1	In Development	0
16384	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	11	WinEventLog:Application	Not in Lookup	Not in Lookup	Not in Lookup	0
916	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	11	WinEventLog:Application	Not in Lookup	Not in Lookup	Not in Lookup	0
10016	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	10	WinEventLog:System	Not in Lookup	Not in Lookup	Not in Lookup	0
1003	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	10	WinEventLog:Application	Not in Lookup	Not in Lookup	Not in Lookup	0
16394	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	Not in Lookup	10	WinEventLog:Application	Not in Lookup	Not in Lookup	Not in Lookup	0
8198	Not in	Not in	Not in	Not in Lookup	Not in	10	WinEventLog:Application	Not in	Not in Lookup	Not in Lookup	0

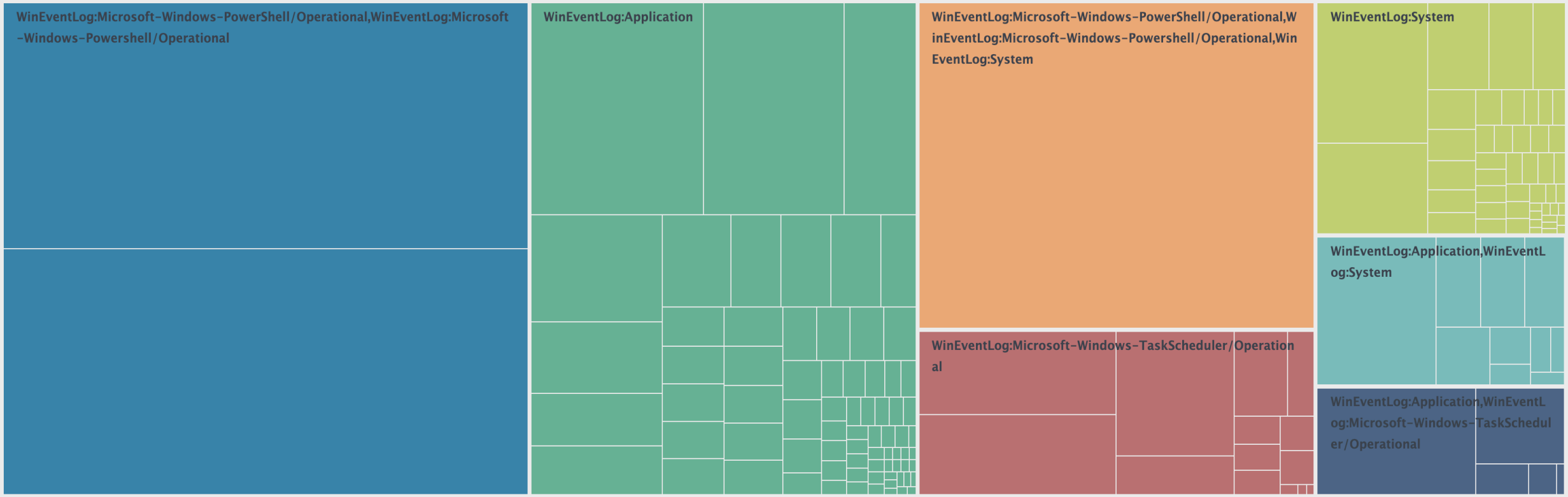
Which events are we collecting that we MAYBE should NOT (for security use cases), and from how many hosts?

Other Events Treemap

Export ▾ ...

Which events are not recommended for security, but we are collecting them anyway?

Aug 2019 ▾	At Least This Many Hosts: 1	Sources: ALL ×	Indexes: main ×	Submit	Hide Filters



Same question, answered graphically…

Individual Event Code Analysis
Individual Host Analysis

Recommended Events Table

Which events exist in my data that are recommended by various authorities co

Export ▾ ...

At Least This Many Authorities: 3
At Least This Many Hosts: 1
Sources: ALL ×
Indexes: main ×
Aug 2019
Submit
Hide Filters

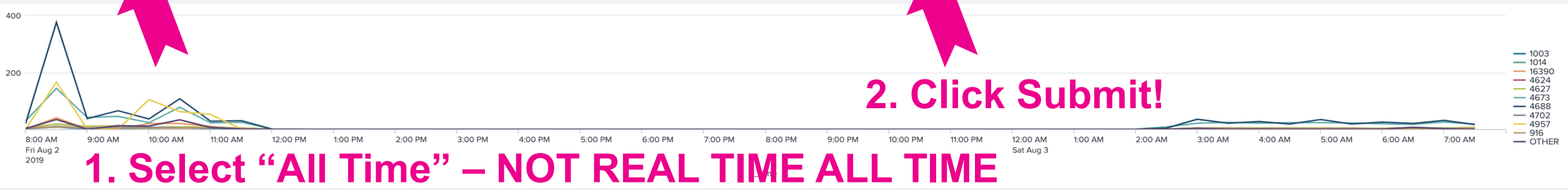
Select “Individual Host Analysis”

EventCode	ATT&CK	Category	Event Log	EventDescription	Level	NumHosts	Source	Subcategory	duplicate_possible	observed_volume	NumRecommenders
4624	1	Logon/Logoff	Security	An account was successfully logged on.	Information	23	WinEventLog:Security	Logon	0	In Development	7
4634	0	Logon/Logoff	Security	An account was logged off.	Information	17	WinEventLog:Security	Logoff	0	In Development	5
4648	0	Logon/Logoff	Security	A logon was attempted using explicit credentials.	Information	14	WinEventLog:Security	Logon	0	In Development	5
4672	0	Privilege Use	Security	Special privileges assigned to new logon.	Information	12	WinEventLog:Security	Sensitive Privilege Use / Non Sensitive Privilege Use	0	In Development	4
4688	1	Detailed Tracking	Security	A new process has been created.	Information	10	WinEventLog:Security	Process Creation	0	In Development	5
4647	0	Logon/Logoff	Security	User initiated logoff	Information	7	WinEventLog:Security	Logoff	0	In Development	4
4625	0	Logon/Logoff	Security	An account failed to log on.	Information	6	WinEventLog:Application WinEventLog:Security	Logon	1	In Development	7
4719	0	Policy Change	Security	System audit policy was changed.	Information	6	WinEventLog:Security	Audit Policy Change	0	In Development	6
4778	0	Logon/Logoff	Security	A session was reconnected to a Window Station.	Information	6	WinEventLog:Security	Other Logon/Logoff Events	0	In Development	5
4779	0	Logon/Logoff	Security	A session was disconnected from a Window Station.	Information	6	WinEventLog:Security	Other Logon/Logoff Events	0	In Development	5
7045	1	System	System	New Windows Service	Information	5	WinEventLog:System	Service	0	In Development	4
4720	0	Account Management	Security	A user account was created.	Information	4	WinEventLog:Security	User Account Management	0	In Development	5
4722	0	Account	Security	A user account was enabled.	Information	4	WinEventLog:Security	User Account	0	In Development	5

Individual Host Analysis

Edit | Export ▾ | ...

All time | Sources: ALL × | Indexes: ALL × | Host: BTUN-L | Sourcetype: (•) wineventlog ( ) xmlwineventlog | Submit | Hide Filters



1. Select "All Time" – NOT REAL TIME ALL TIME

2. Click Submit!

EventCode	count	sourcetype	EventDescription	MB	Recommended?
4688	948	WinEventLog	A new process has been created.	1.78	YES
4673	627	WinEventLog	A privileged service was called.	0.37	YES
4624	114	WinEventLog	An account was successfully logged on.	0.26	YES
4957	384	WinEventLog	Windows Firewall did not apply the following rule:	0.20	YES
4627	114	WinEventLog	Group membership information.	0.15	YES
4702	44	WinEventLog	A scheduled task was updated.	0.13	YES
1003	26	WinEventLog		0.11	NO
16390	90	WinEventLog		0.03	NO
916	65	WinEventLog		0.02	NO
1014	51	WinEventLog		0.02	NO

« Prev 1 2 3 4 Next »

37
DIFFERENT EVENT CODES SEEN IN TIME SELECTED

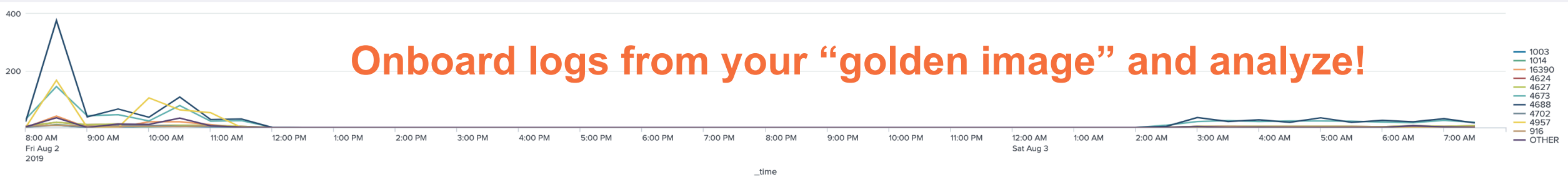
3
MB SEEN FROM THIS HOST IN TIME SELECTED

sourcetype	Number of Events	source	indexes
WinEventLog	2556	WinEventLog:Application WinEventLog:Security WinEventLog:System	main
WinEventLog:Microsoft-Windows-Powershell/Operational	18	WinEventLog:Microsoft-Windows-Powershell/Operational	main

Individual Host Analysis

Edit | Export ▾ | ...

All time | Sources: ALL × | Indexes: ALL × | Host: BTUN-L | Sourcetype: (•) wineventlog ( ) xmlwineventlog | Submit | Hide Filters



Onboard logs from your "golden image" and analyze!

EventCode	count	sourcetype	EventDescription	MB	Recommended?
4688	948	WinEventLog	A new process has been created.	1.78	YES
4673	627	WinEventLog	A privileged service was called.	0.37	YES
4624	114	WinEventLog	An account was successfully logged on.	0.26	YES
4957	384	WinEventLog	Windows Firewall did not apply the following rule:	0.20	YES
4627	114	WinEventLog	Group membership information.	0.15	YES
4702	44	WinEventLog	A scheduled task was updated.	0.13	YES
1003	26	WinEventLog		0.11	NO
16390	90	WinEventLog		0.03	NO
916	65	WinEventLog		0.02	NO
1014	51	WinEventLog		0.02	NO

« Prev 1 2 3 4 Next »

37

DIFFERENT EVENT CODES SEEN IN TIME SELECTED

3

MB SEEN FROM THIS HOST IN TIME SELECTED

sourcetype	Number of Events	source	indexes
WinEventLog	2556	WinEventLog:Application WinEventLog:Security WinEventLog:System	main
WinEventLog:Microsoft-Windows-Powershell/Operational	18	WinEventLog:Microsoft-Windows-Powershell/Operational	main

Where do I get it?

1. From the link provided in the Endpoint App:

https://splk.it/conf19-splunk-endpoint

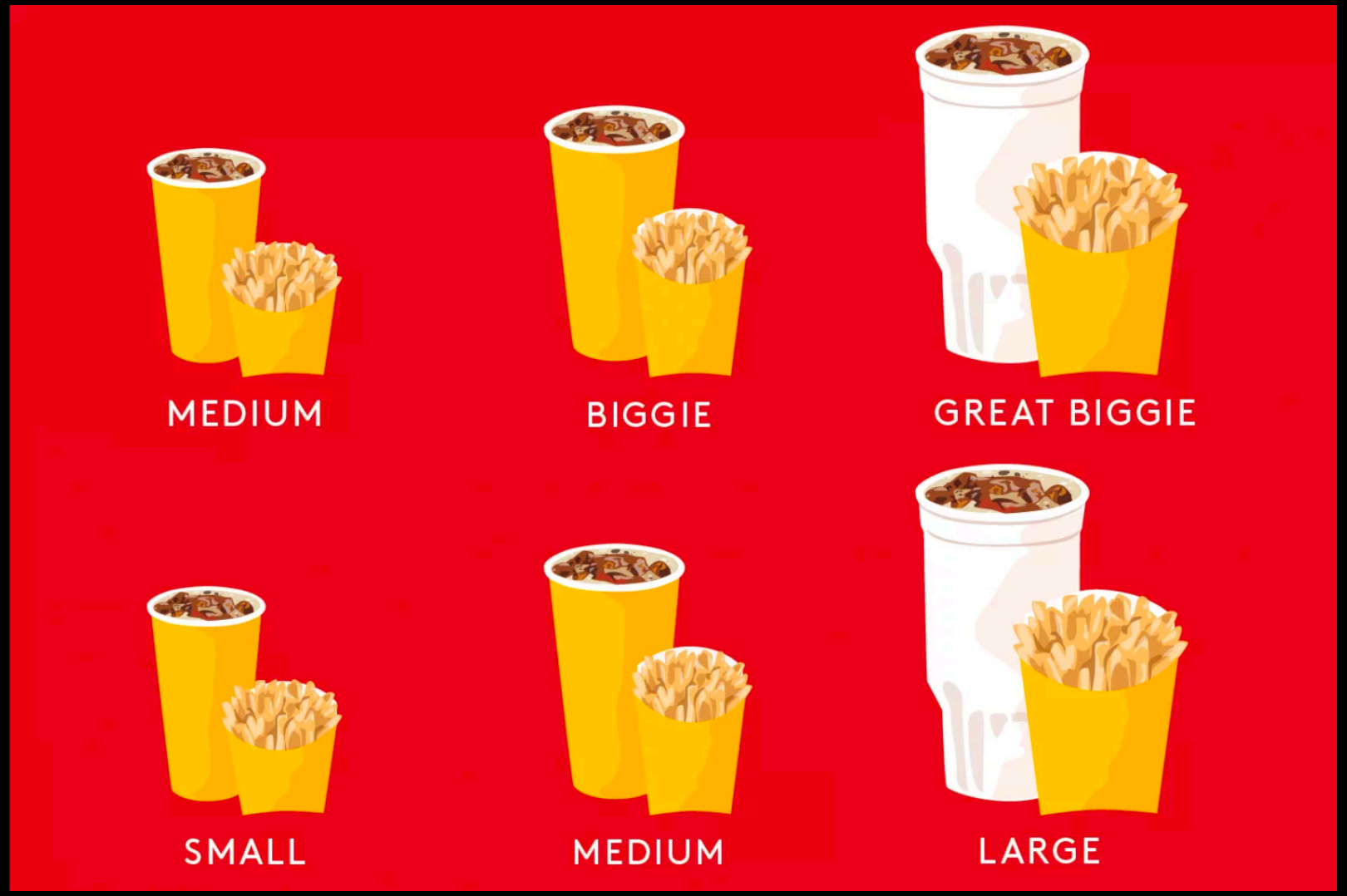
2. Github:

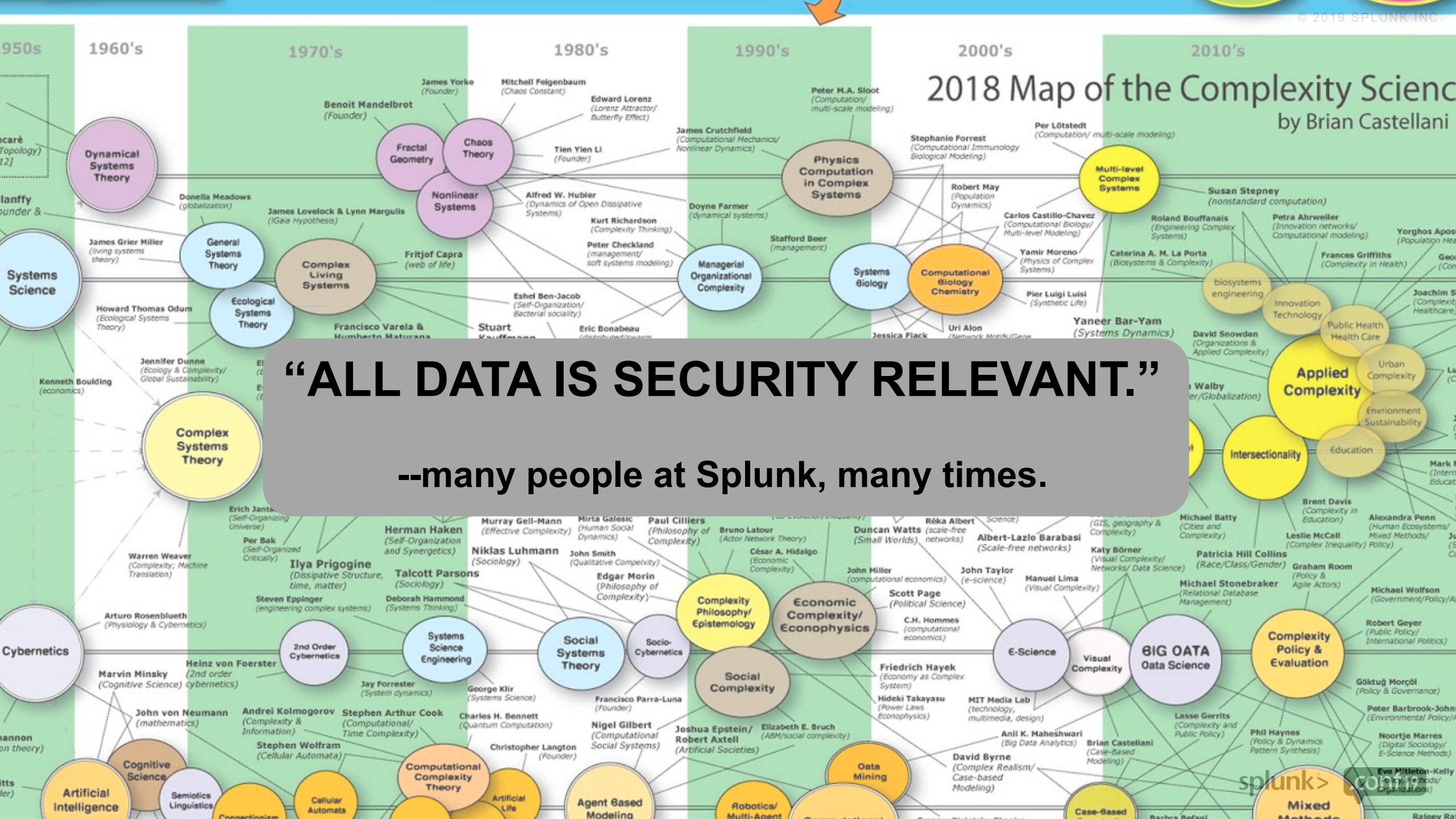
https://github.com/stressboi/splunk_wineventcode_secanalysis

COMING! jp-CERT analysis as a 7th source!


Even with the best intentions…
Splunk eats too much.

What's normal?

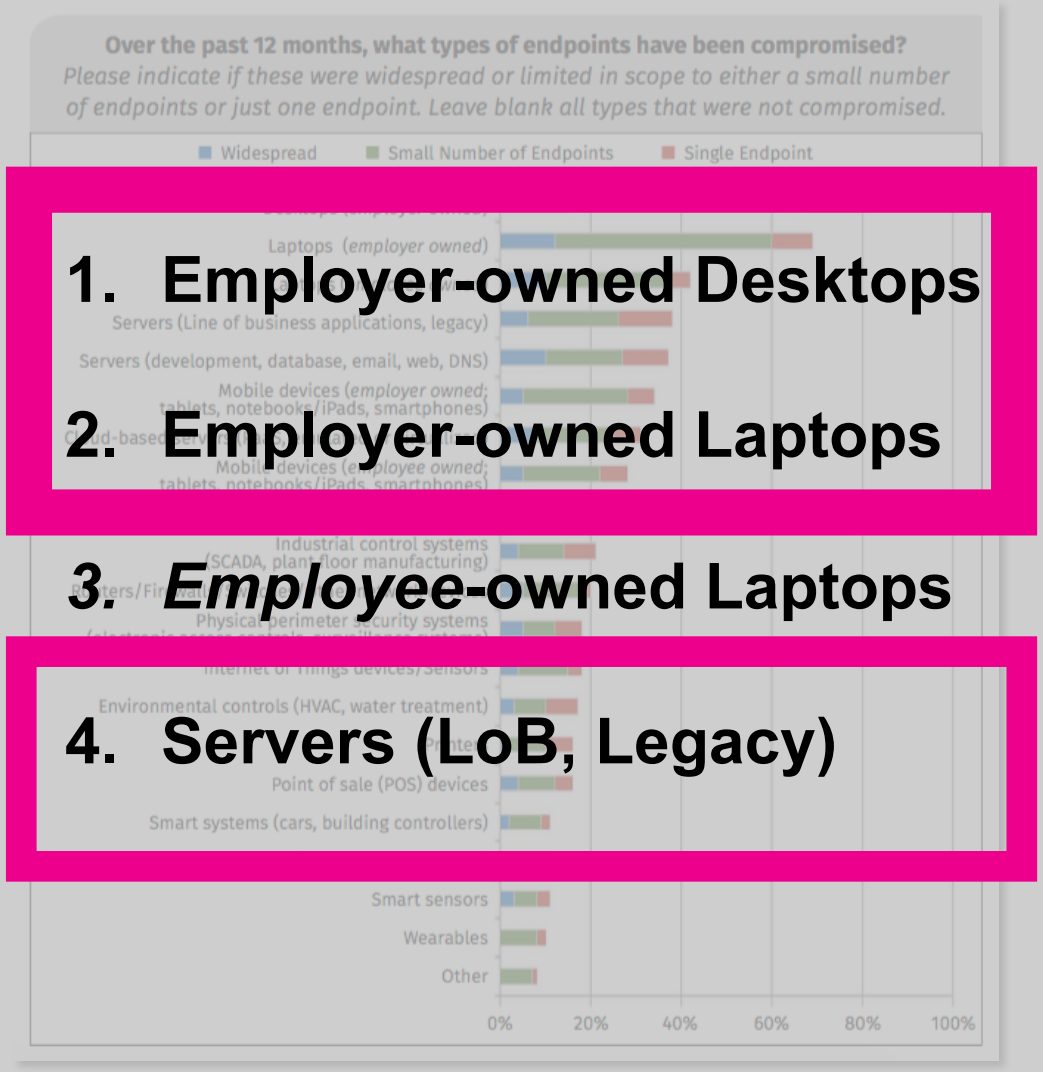




"ALL DATA IS SECURITY RELEVANT."

--many people at Splunk, many times.

What kind of endpoints and how?



1. Employer-owned Desktops
2. Employer-owned Laptops
3. *Employee*-owned Laptops
4. Servers (LoB, Legacy)

Neely, 2018

If these are the most likely endpoints to be compromised, shouldn't we be collecting logs from them?

Neely, 2018

What to collect from user endpoints?

Using the Universal Forwarder on Windows

- Basic
  - Windows Event logs
    - Security
      - Set up command process auditing (4688)
    - System
    - Application
  - WindowsUpdateLog (on supported systems)
- Intermediate
  - Sysmon (with TaySwift or Olaf config + Splunk Tweaks)
    - Captures registry instead of Splunk regmon
  - Powershell
    - Module Logging
    - Script Block Logging
  - Scripted Inputs
- Advanced/Specific
  - Splunk Stream
  - Perfmon
  - Powershell Transcription Logs
  - Applocker
  - Windows Firewall
  - WinPrintMon
  - Native USB Auditing

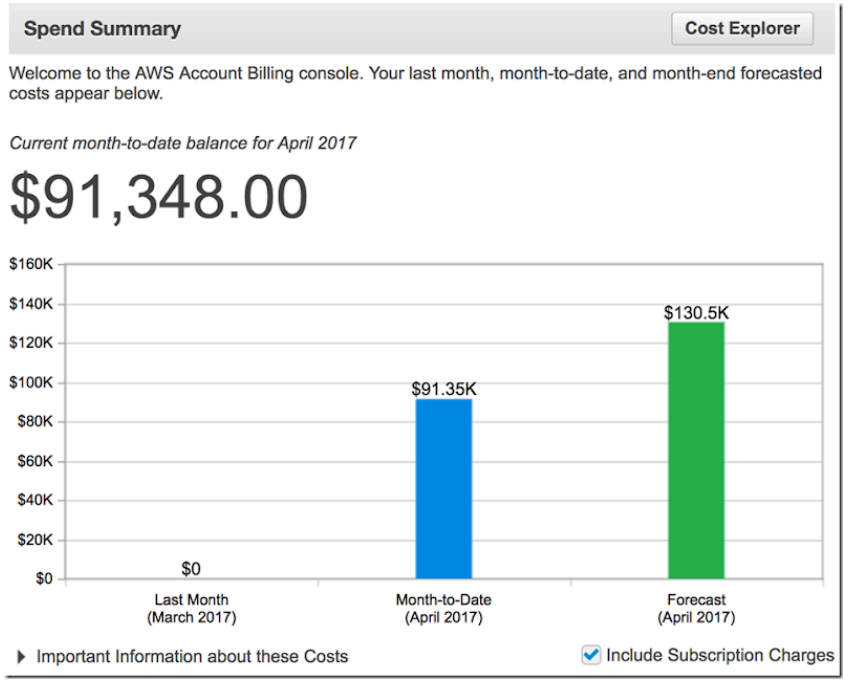
What to collect from user endpoints?

Using the Universal Forwarder on Windows

- Basic
  - Windows Event logs
    - Security
      - Set up command process auditing (4688)
    - System
    - Application
  - WindowsUpdateLog (on supported systems)
- Intermediate
  - Sysmon (with TaySwift or Olaf config + Splunk Tweaks)
    - Captures registry instead of Splunk regmon
  - Powershell
    - Module Logging
    - Script Block Logging
  - Scripted Inputs
- Advanced/Specific
  - Splunk Stream
  - Perfmon
  - Powershell Transcription Logs
  - Applocker
  - Windows Firewall
  - WinPrintMon
  - Native USB Auditing

And what happens if you collect absolutely everything with no filtering?

Storage and compute doesn't grow on trees.



splunk> .conf19

Endpoint Logging (Justin Henderson, SANS 555 Course Author)

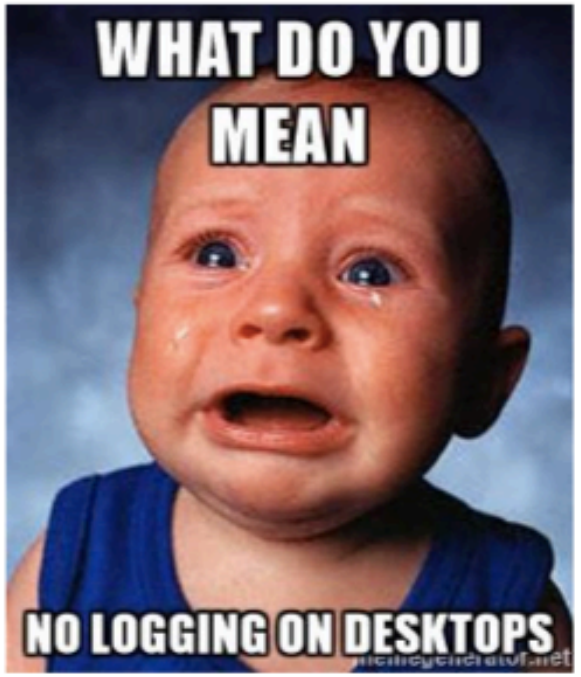
Today, client-side attacks are more common

- Means the attack occurs at the desktop
- Which means you need desktop logs...

Yet, cost of desktop logs is considered too high

- If strategy is collect everything, that is true
- If strategy is to stay nimble and tactical, it is more expensive not to log...

Advanced agent filtering is helpful or file server tricks



What did we collect this year for BOTS?

- Latest UF (7.3.x) on every endpoint
- Latest Windows TA with all standard scripted inputs enabled except none of the “Mon” inputs (regmon, netmon, printmon, etc)
- Windows Security, System, Application Events using Michael Gough’s audit config and some blacklisting on Security events
- Microsoft Sysmon v10 with Olaf Hartong’s latest config + some more Splunk filtering tweaks
- Windows Powershell/Operational log (4103 and 4104 events)
- CB Response with watchlists and five standard threat feeds, as well as netconn and process events
- Splunk Stream collecting DNS, HTTP, TCP, UDP, DHCP and a few other protocols

To gauge ingest levels we look at Windows Events, Sysmon, Scripted TA output, and Powershell.

What ingest did we see?

_time	ABUNGSTEIN-L	AGRADY-L	BSTOLL-L	BTUN-L	FMALTEKESKO-L	GHOPPY-L	JWORTOSKI-L	MVALITUS-L	PCERF-L
2019-08-02 00:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 01:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 02:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 03:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000
2019-08-02 04:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 05:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 06:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 07:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000
2019-08-02 08:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 09:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 10:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 11:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000
2019-08-02 12:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 13:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 14:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 15:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000
2019-08-02 16:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 17:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 18:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 19:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000
2019-08-02 20:00	0.24869728088378906000	0.59389591217041020000	0.09420394897460938000	10.49557971954345700000	0.64506053924560550000	0.65571689605712890000	10.26805210113525400000	0.91140842437744140000	2.11278629302978500000
2019-08-02 21:00	0.69047355651855470000	0.47948837280273440000	0.01041793823242187500	0.33814239501953125000	0.99037742614746090000	5.84523391723632800000	0.69832420349121090000	0.23190784454345703000	1.98094558715820310000
2019-08-02 22:00	0.06999111175537110000	0.38000011444091797000	0.01308059692382812500	0.24058151245117188000	0.07157993316650390000	1.57241821289062500000	0.46176910400390625000	0.21506023406982422000	1.97122001647949220000
2019-08-02 23:00	0.15992832183837890000	0.34910583496093750000	0.00257492065429687500	0.12786197662353516000	0.11996841430664062000	0.24280929565429688000	0.37053871154785156000	0.23142528533935547000	2.06956958770751950000

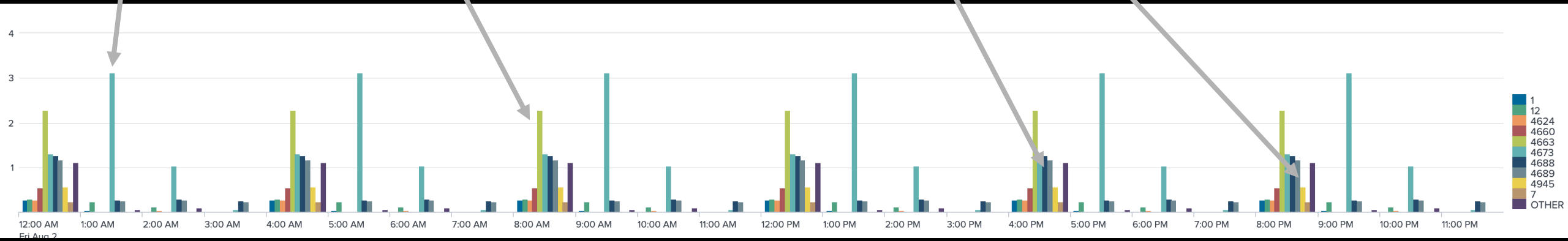
Upwards of 50MB per endpoint? Uhoh.

4688=Critical, but can also use Sysmon 1

4673=Not recommended to collect

4689=Not recommended to collect

4663=Granular object auditing



In general, we had lots of extra stuff.

If we remove those four codes…

_time	ABUNGSTEIN-L	AGRADY-L	BSTOLL-L	BTUN-L	FMALTEKESKO-L	GHOPPY-L	JWORTOSKI-L	MVALITUS-L	PCERF-L
2019-08-02 00:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 01:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 02:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 03:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382
2019-08-02 04:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 05:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 06:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 07:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382
2019-08-02 08:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 09:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 10:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 11:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382
2019-08-02 12:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 13:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 14:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 15:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382
2019-08-02 16:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 17:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 18:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 19:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382
2019-08-02 20:00	0.064	0.248	2.728	2.525	0.219	0.423	1.451	0.302	0.526
2019-08-02 21:00	0.215	0.203	0.334	0.107	0.333	1.129	0.157	0.099	0.299
2019-08-02 22:00	0.008	0.181	0.285	0.051	0.011	0.273	0.085	0.077	0.296
2019-08-02 23:00	0.028	0.179	0.057	0.038	0.015	0.060	0.062	0.085	0.382

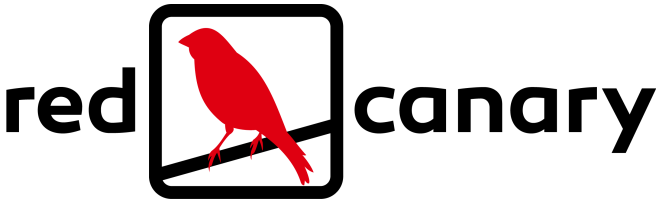
Best case, ~6MB a day, worst, ~12MB!

BOTS Lessons Learned

1. If you can at all use Sysmon, do so. Much more granular and flexible filtering for process events, file creates. 4688 is better than nothing.

2. Be ruthless about what event codes you collect. Collect the ones that meet your use case and are “recommended.”

3. renderXML=true may save you some space, we used Classic because of some issues we found with blacklisting



Carbon Black.

- Large, Fortune 500 company based in the US
- 70,000 Windows endpoints running **Carbon Black Response**
- **cb-event-forwarder** to get raw sensor data in Splunk
- COLLECT: Process info, network connection info, alerts, watchlists
- NOT COLLECT: File modifications, registry modifications, and module loads: diminishing returns from both splunk license and storage perspective…

(and if you need to, you can always hunt this stuff in the native tool.)

600GB a day (about 8.5MB per endpoint, per day!)

Security, Compliance and Fraud | All Skill Levels

SEC1952 - Finding Evil Is Never An Accident: How to Hunt in BOTS

SCHEDULE **Tuesday, October 22 | 04:15 PM - 05:00 PM** | L4-4501 MARCELLO (VENETIAN)

SPEAKERS

Michael Haag, **Director of Advanced Threat Detection, Red Canary**

To secure the modern endpoint, you need sufficient data, the right visibility and analysis, and the technology necesary to stop an intrusion. We will leverage BOTSv4 data in this session to help you test and validate Splunk use cases related to...

Industries: Not industry specific
Products: Splunk Enterprise, Splunk Cloud

What our BOTS machines collected from CB

Event Collection

Disabling event collection will impact visibility, but may improve sensor and server performance.

Process Events

- [x] Process Information
  Collect metadata including starts, stops, pid.
- [x] Process user context
  Collect username associated with events.
- [x] File modifications
  Record modifications of binary files, eg. dll/exe.
  - [x] Non-binary file writes
    Record filemod events for non-binary files.
- [x] Binary module loads
  Collect load events for .dll, .sys, .exe, .so, .dylib.
- [x] Network connections
  Collect in/outgoing network events.

Windows Events

- [x] Cross process events
  Collect events across process boundaries.
- [x] Registry modifications
  Collect write and delete events in the registry.
- [ ] EMET events
  Collect EMET mitigation and protection events.

Binary / Module / Storefile Events

- [x] Binaries
  Collect binary modules.
- [x] Binary info
  Collect metadata that describes binaries.

What our BOTS machines looked like from CB

_time	ABUNGSTEIN-L	AGRADY-L	BSTOLL-L	BTUN-L	FMALTEKESKO-L	GHOPPY-L	JWORTOSKI-L	MVALITUS-L	PCERF-L
2019-08-02 00:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 01:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 02:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 03:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 04:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 05:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 06:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 07:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 08:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 09:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 10:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 11:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 12:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 13:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 14:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 15:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 16:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 17:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 18:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 19:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 20:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 21:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 22:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 23:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919

What our BOTS machines looked like from CB

These look like 7-8 MB a day…

What the heck is that?

_time	ABUNGSTEIN-L	AGRADY-L	BSTOLL-L	BTUN-L	FMALTEKESKO-L	GHOPPY-L	JWORTOSKI-L	MVALITUS-L	PCERF-L
2019-08-02 00:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 01:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 02:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 03:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 04:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 05:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 06:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 07:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 08:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 09:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 10:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 11:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 12:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 13:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 14:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 15:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 16:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 17:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 18:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 19:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919
2019-08-02 20:00	0.542	0.948	2.885	2.894	1.317	1.758	4.967	0.739	0.866
2019-08-02 21:00	0.587	0.659	0.616	0.824	0.243	1.352	4.502	0.460	0.849
2019-08-02 22:00	0.366	0.611	0.663	0.492		1.290	3.766	0.494	0.836
2019-08-02 23:00	0.470	0.501	0.642	0.415		0.512	2.971	0.502	0.919

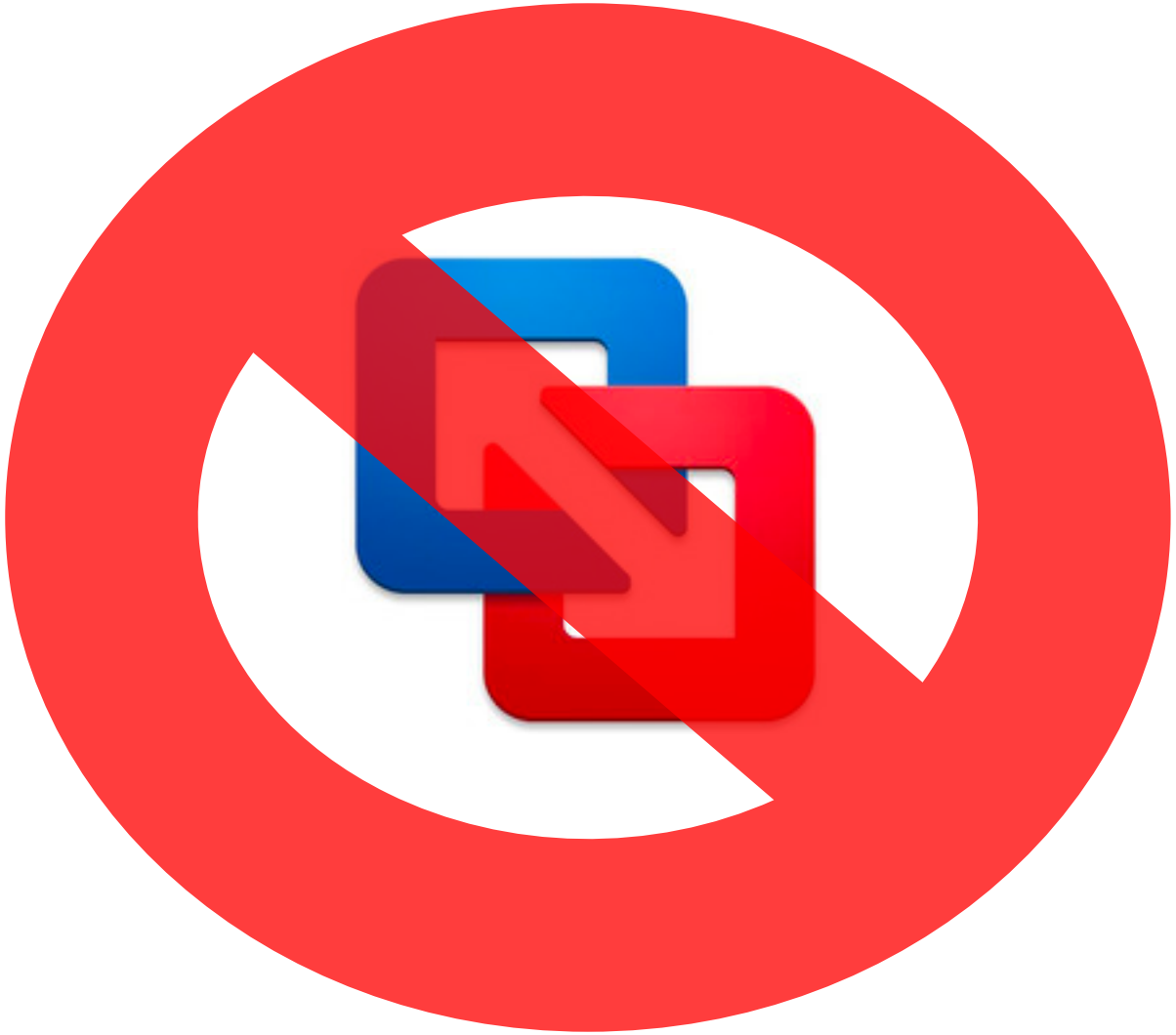
JWORTOSKI had a broken IPv6 config?

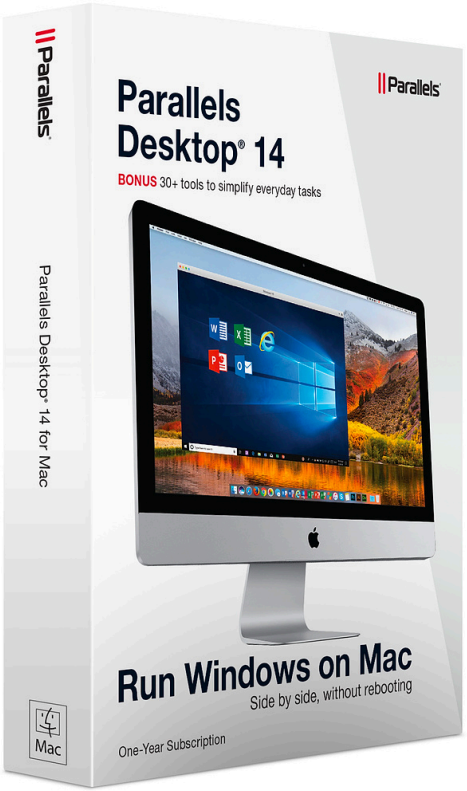
8/2/19
11:59:49.000 PM

{ [-]
  cb_server: cbserver
  computer_name: JWORTOSKI-L
  direction: outbound
  domain:
  event_type: netconn
  link_process: https://34.220.185.163/#analyze/00000003-0000-086c-01d5-4727be08fe6c/0
  link_sensor: https://34.220.185.163/#/host/3
  local_ip: fe80::d903:176e:3226:9023
  local_port: 56999
  md5: 0861726716C9610CE5F6BCF3F4858DA1
  pid: 2156
  process_guid: 00000003-0000-086c-01d5-4727be08fe6c
  process_path: c:\windows\system32\svchost.exe
  protocol: 17
  proxy: false
  remote_ip: fe80::21c:42ff:fe00:18
  remote_port: 53
  sensor_id: 3
  sha256: 29F04D5F4B8D798038CB9647178A8B9C68E16DC50DA850937F6E993FC7967B75
  timestamp: 1564790389
  type: ingress.event.netconn
}

Show as raw text

JWORTOSKI was different.





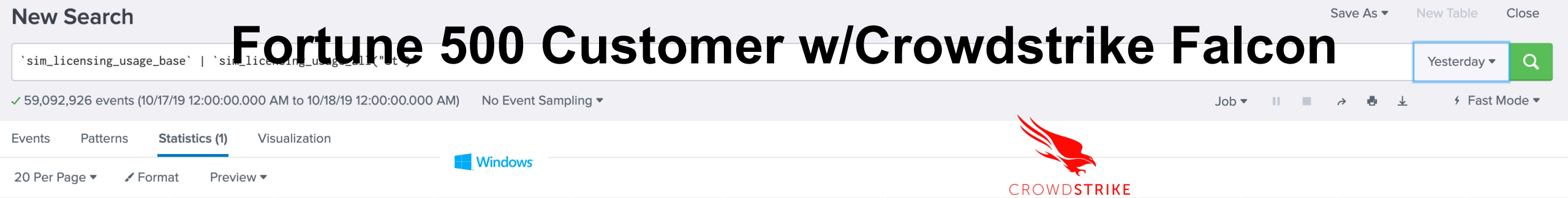
Other Endpoints…

computer_name	MULTICAST	LINKLOCAL
ABUNGSTEIN-L	234	420
AGRADY-L	264	270
BSTOLL-L	528	516
BTUN-L	432	18
FMALTEKESKO-L	84	0
GHOPPY-L	294	0
JWORTOSKI-L	2310	58278
MVALITUS-L	174	258
PCERF-L	204	0

- Evidently CB's "netconn" collects IPv6 by default
- Could filter this in a number of places – cb forwarder config or UF on forwarder box with indexed extractions, or indexers
- Review your data and look for anomalies like this to filter out!

BOTS 5: ONLY IPv6! You heard it here first.

Fortune 500 Customer w/Crowdstrike Falcon



_time	BlazeM	Perfmon:Process	WinEventLog	akamai:cm:json	channel-services	cisco:asa	cs_replicator	netstat	opsec	ucd_server	OTHER
2019-10-17	146.950	192.046	633.507	362.761	350.767	367.543	868.057	127.839	142.524	462.597	1027.639

633GB from ~4,500 Production Windows Servers (~140MB a day per Server)

868GB from ~18,000 Endpoints (mostly Windows) (~48MB a day per Endpoint)

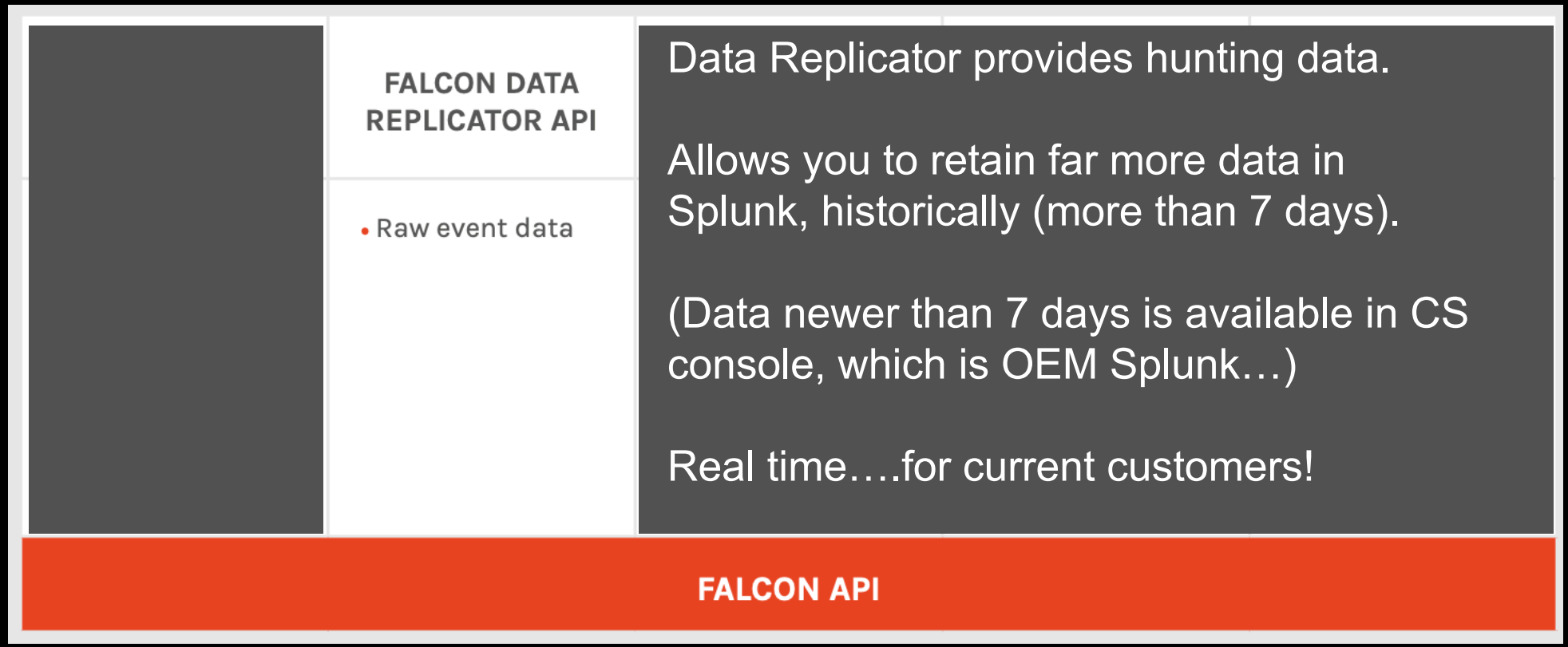
NO FILTERING.

splunk> .conf19

- **Three ways to get data into your own Splunk instance:**
  - Falcon SIEM Connector (detections and audit events)
  - Falcon Streaming API (detections and audit events)
  - Falcon Replicator (granular sensor data) usually via SQS

FALCON STREAMING API	FALCON DATA REPLICATOR API	FALCON QUERY API	FALCON INTEL API	FALCON THREAT GRAPH API
• Detections • Audit events	• Raw event data	• Search for IOCs, devices and detections • Manage detections and custom IOC watch list	• Actors • Indicators • News • Tailored intel	• Detections • IOC search • Process metadata
FALCON API				

- **Three ways to get data into your own Splunk instance:**
  - Falcon SIEM Connector (detections and audit events)
  - Falcon Streaming API (detections and audit events)
  - Falcon Replicator (granular sensor data) usually via SQS



New Search

Save As ▾ New Table Close

```
sourcetype=cs_replicator index="crowdstrike_raw"| top limit=20 event_simpleName
```

Last 30 minutes ▾

✓ 5,997,907 events (10/18/19 9:22:00.000 PM to 10/18/19 9:52:23.000 PM) No Event Sampling ▾

Job ▾ Smart Mode ▾

Events Patterns **Statistics (20)** Visualization

20 Per Page ▾ Format Preview ▾

Data from Crowdstrike's Falcon Replicator…

Process (over 80%), DNS, File, etc.

event_simpleName	count	percent
ProcessRollup2	4347072	72.485135
EndOfProcess	696210	11.608935
ProcessRollup2Stats	217471	3.626214
ChannelVersionRequired	146640	2.445145
SetWinEventHookEtw	78958	1.316583
DnsRequest	67367	1.123309
SensorHeartbeat	66752	1.113054
ImageHash	48792	0.813581
NetworkConnectIP4	38867	0.648087
NewScriptWritten	30864	0.514641
DirectoryCreate	26272	0.438072
PeFileWritten	21576	0.359768
TerminateProcess	18268	0.304609
UserLogon	17957	0.299424
UserLogonFailed2	17754	0.296039
ExecutableDeleted	17209	0.286951
NewExecutableWritten	16759	0.279447
UserLogoff	16593	0.276680
ConfigStateUpdate	9702	0.161776
CurrentSystemTags	7975	0.132979

New Search

Save As | New Table | Close

```
sourcetype=cs_replicator index="crowdstrike_raw"| top limit=2
```

Last 30 minutes

✓ 5,997,907 events (10/18/19 9:22:00.000 PM to 10/18/19 9:52:23.000 P

Job | Smart Mode

Events | Patterns | **Statistics (20)** | Visualization

20 Per Page | Format | Preview

Data
Repl

Proc
Auth

event_simpleName	percent
ProcessRollup2	72.485135
EndOfProcess	11.608935
ProcessRollup2Stats	3.626214
ChannelVersionRequired	2.445145
SetWinEventHookEtw	1.316583
DnsRequest	1.123309
SensorHeartbeat	1.113054
ImageHash	0.813581
NetworkConnectIP4	0.648087
NewScriptWritten	0.514641
DirectoryCreate	0.438072
PeFileWritten	0.359768
TerminateProcess	0.304609
UserLogon	0.299424
UserLogonFailed2	0.296039
ExecutableDeleted	0.286951
NewExecutableWritten	0.279447
UserLogoff	0.276680
ConfigStateUpdate	0.161776
CurrentSystemTags	0.132979

Powershell Encoded

✓ Powershell Encoded ("system" user excluded)

Scheduled Task Registered

Suspicious Registry Changes

Executables Running from Recycle Bin

Reconnaissance Tools

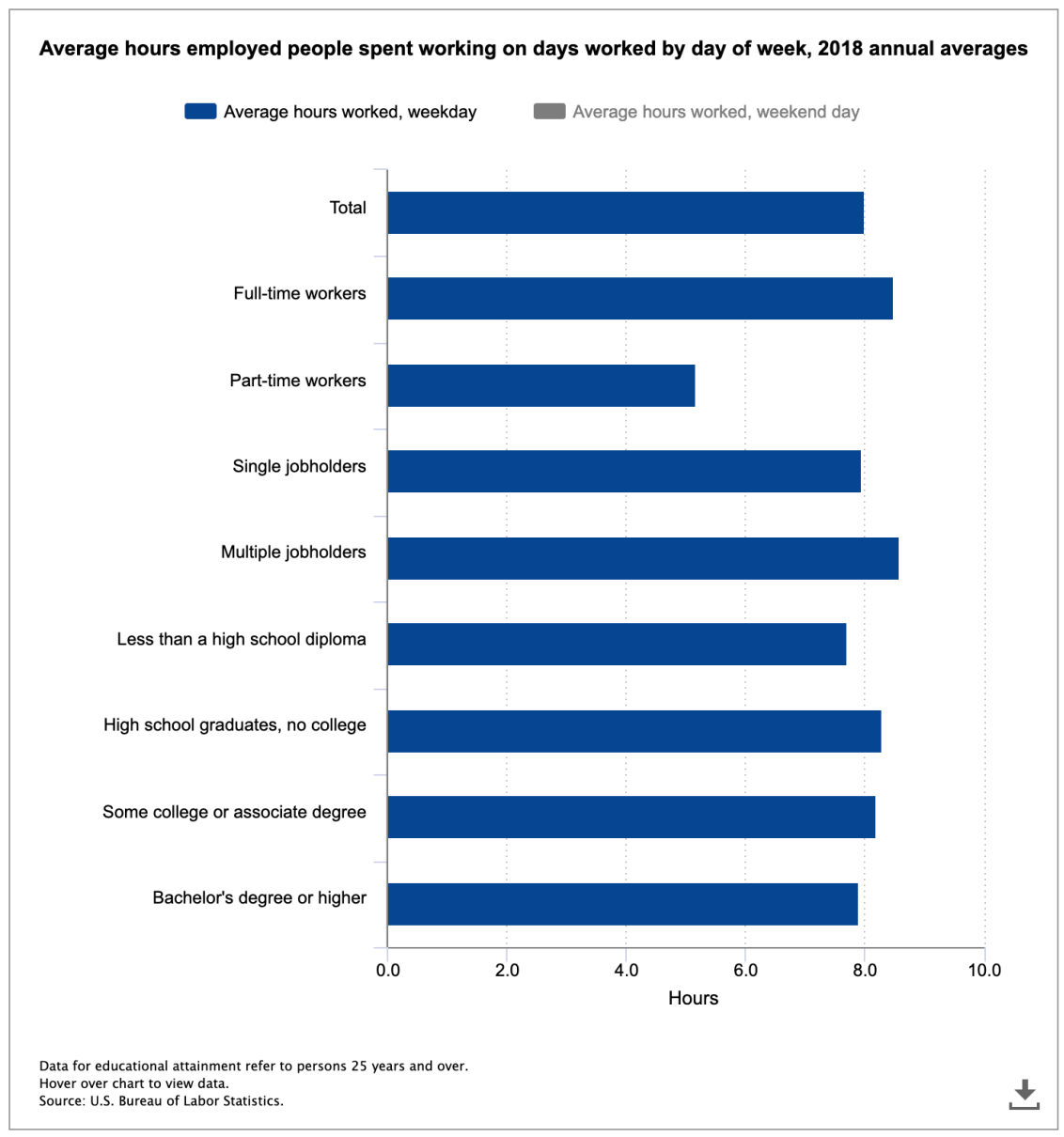
Hunting Suspicious Processes

Hunting Phishing Attacks & Malicious Attachments

Files Written to Removable Media

Rare DNS

Remote Access Tool Usage



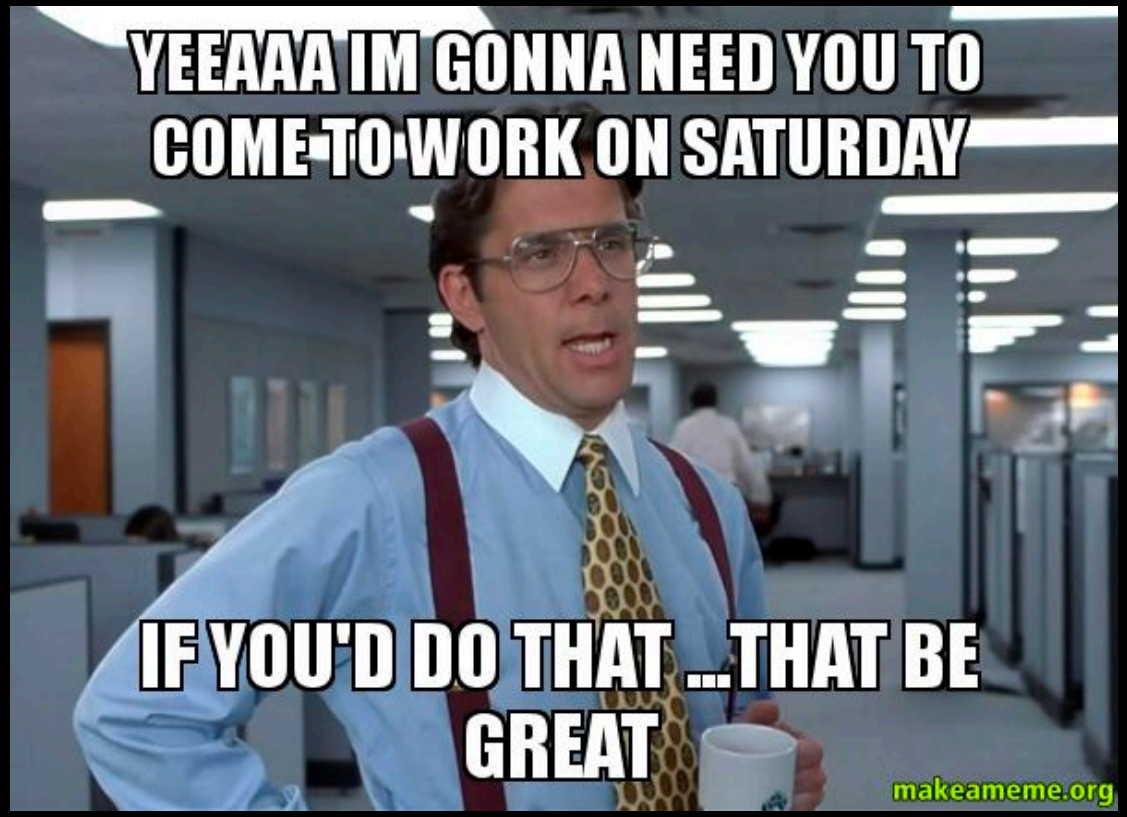
What would endpoint collection nirvana look like?

Well, how many hours a day do your employees work?

Except for … millennials?

~1MB per hour a “nirvana” goal.

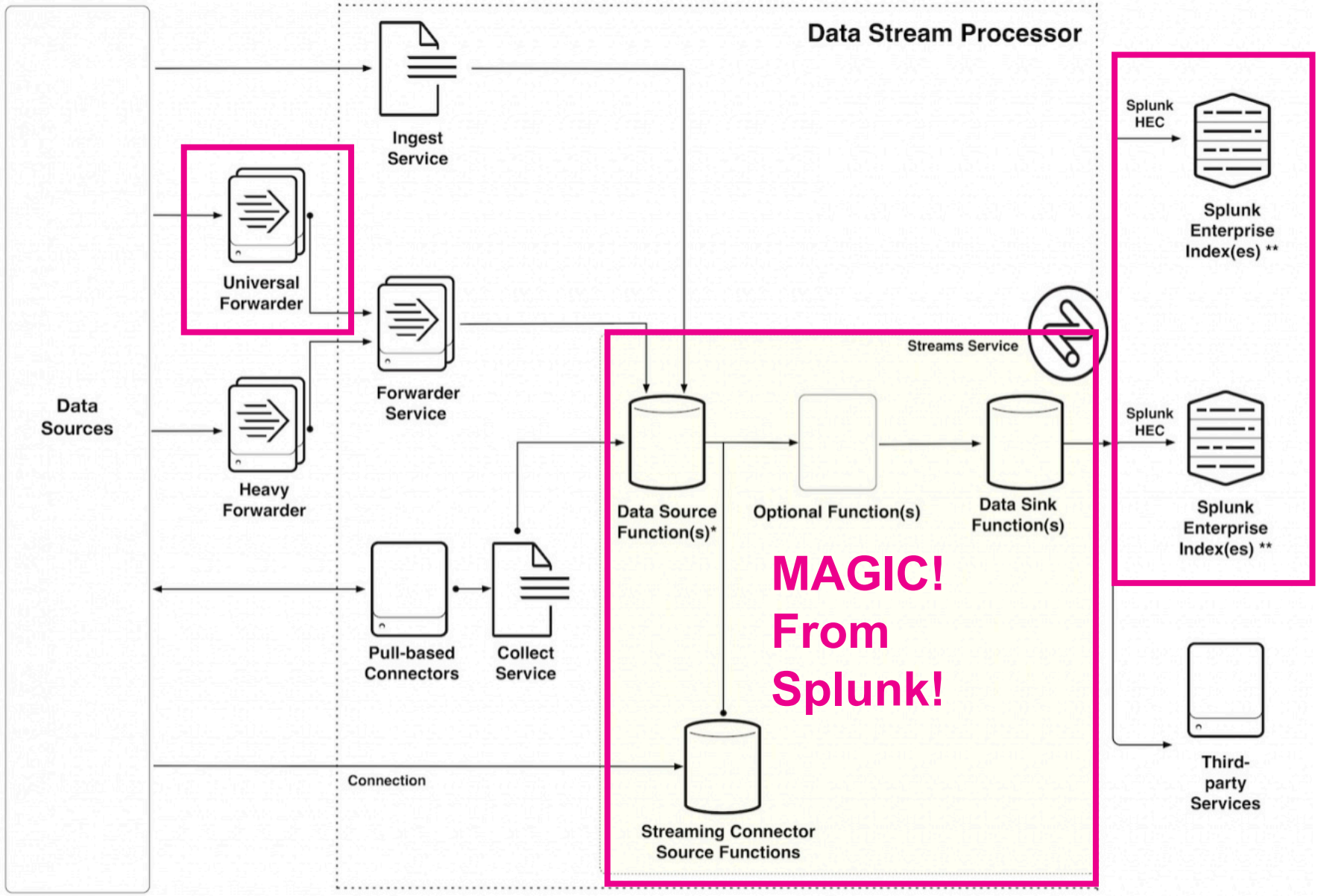
But realistically, max 2MB per work-hour.

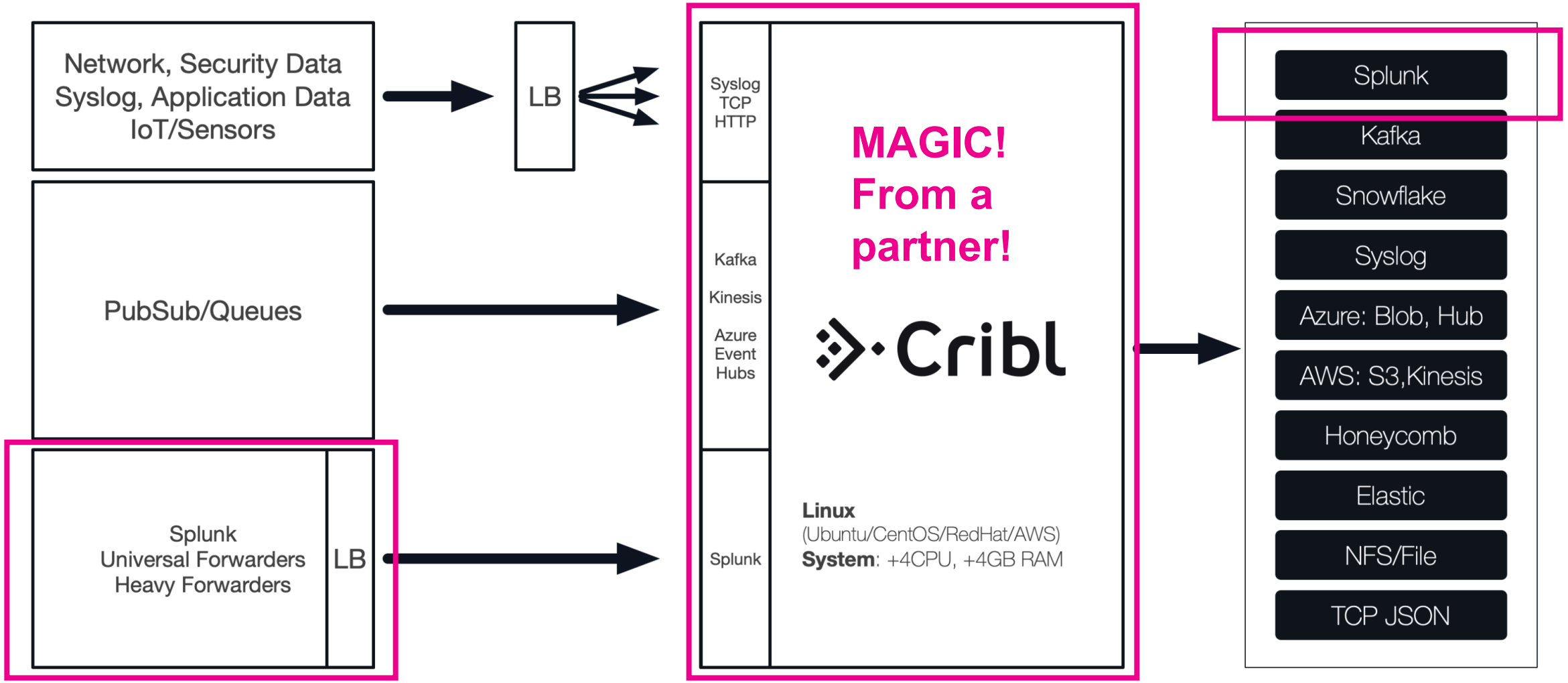


“Sure, but know that it’s gonna increase our Splunk ingest/storage/compute cost.”

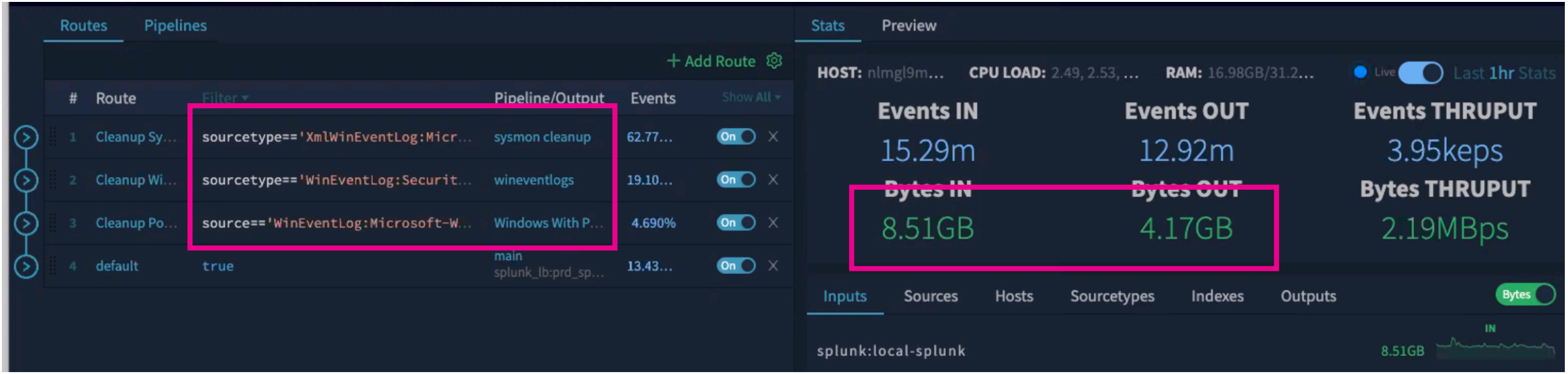
What can we do besides audit config and filter?

Pre-Index, or “Stream” Processing!





What magic?



(x10)

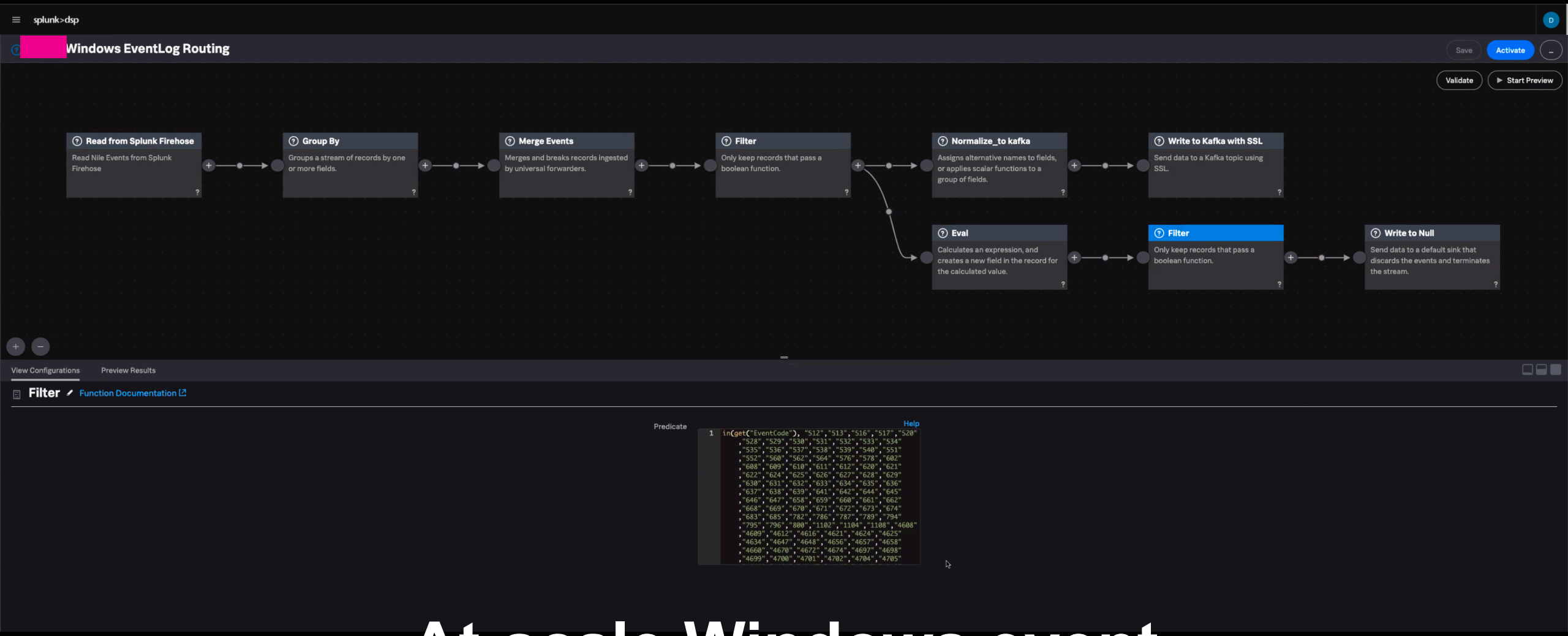
“Reduce by Half.”

splunk> .conf19

“But I can just continue to play with audit configs at the source, and white/blacklists…”

Key Takeaway: Stream Processing **centralizes** and **eases** the config and puts YOU in complete control of your events, and where they end up.

Let forwarders forward and indexers index and search.



At-scale Windows event filtering and routing in DSP!

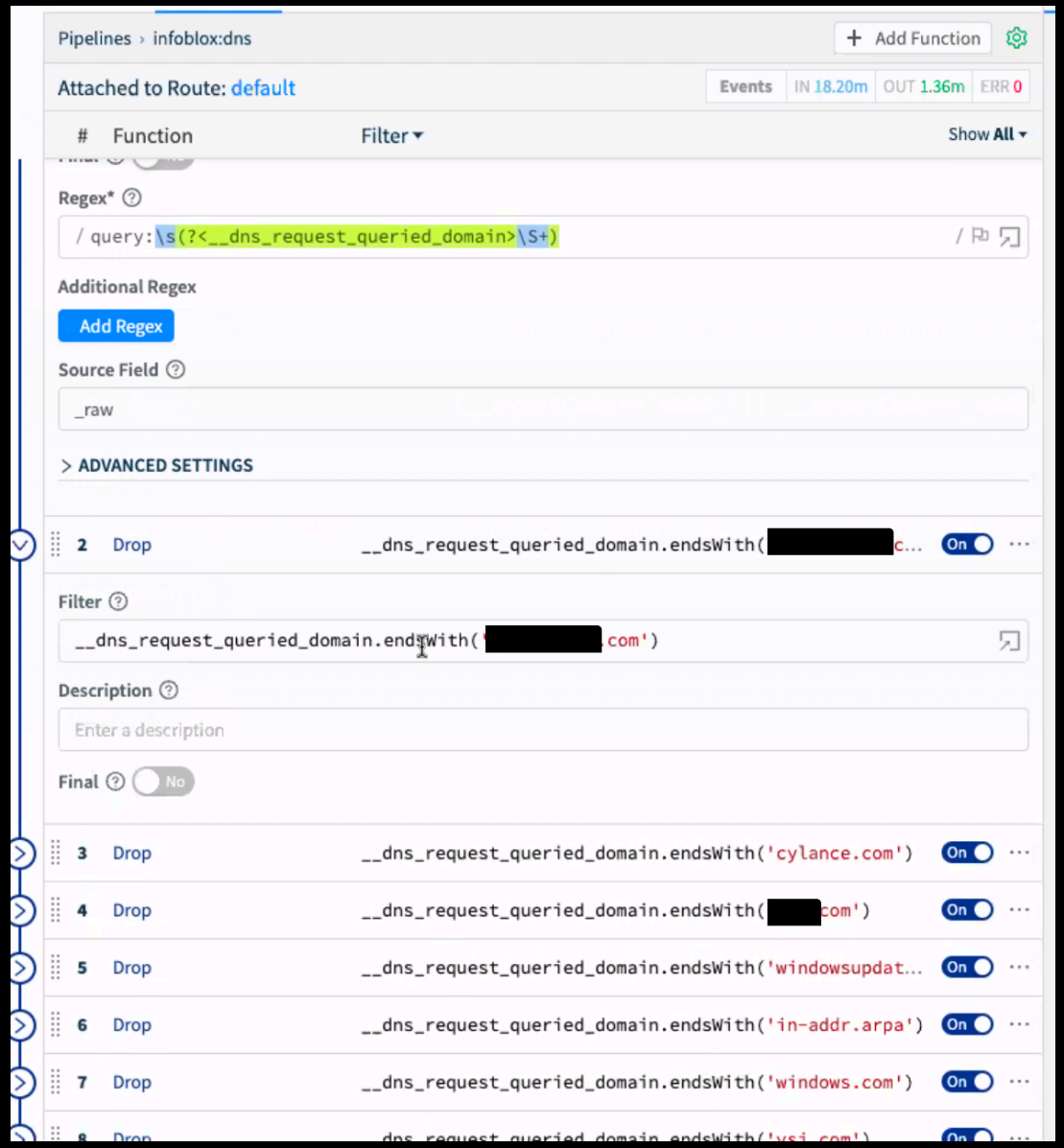
splunk> .conf19

```
{
        "filter": "true",
        "id": "serde",
        "description": "Filter out unwanted kv pairs",
        "conf": {
          "mode": "reserialize",
          "type": "json",
          "srcField": "_raw",
          "remove": [
            "cid",
            "name",
            "TokenType",
            "IntegrityLevel",
            "ImageSubsystem",
            "Entitlements",
            "EffectiveTransmissionClass",
            "ConfigStateHash"
          ],
          "fieldFilterExpr": ""
        }
      },
```

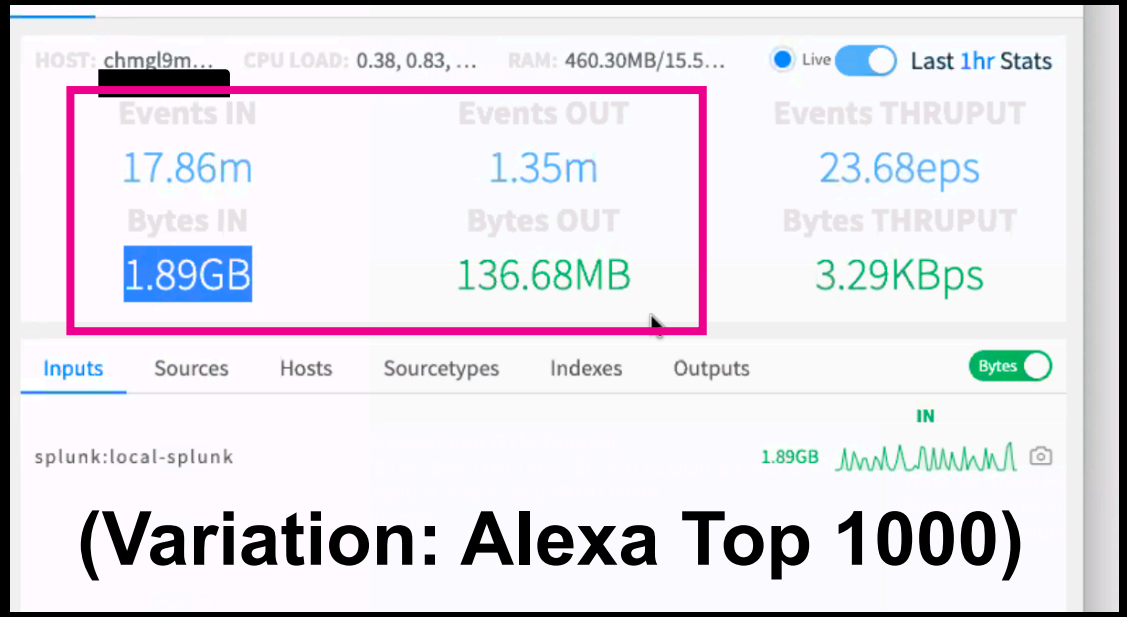
Cribl filtering of unwanted Crowdstrike k/v pairs!

7TB became 3TB.

(They also dropped certain classes of events…)



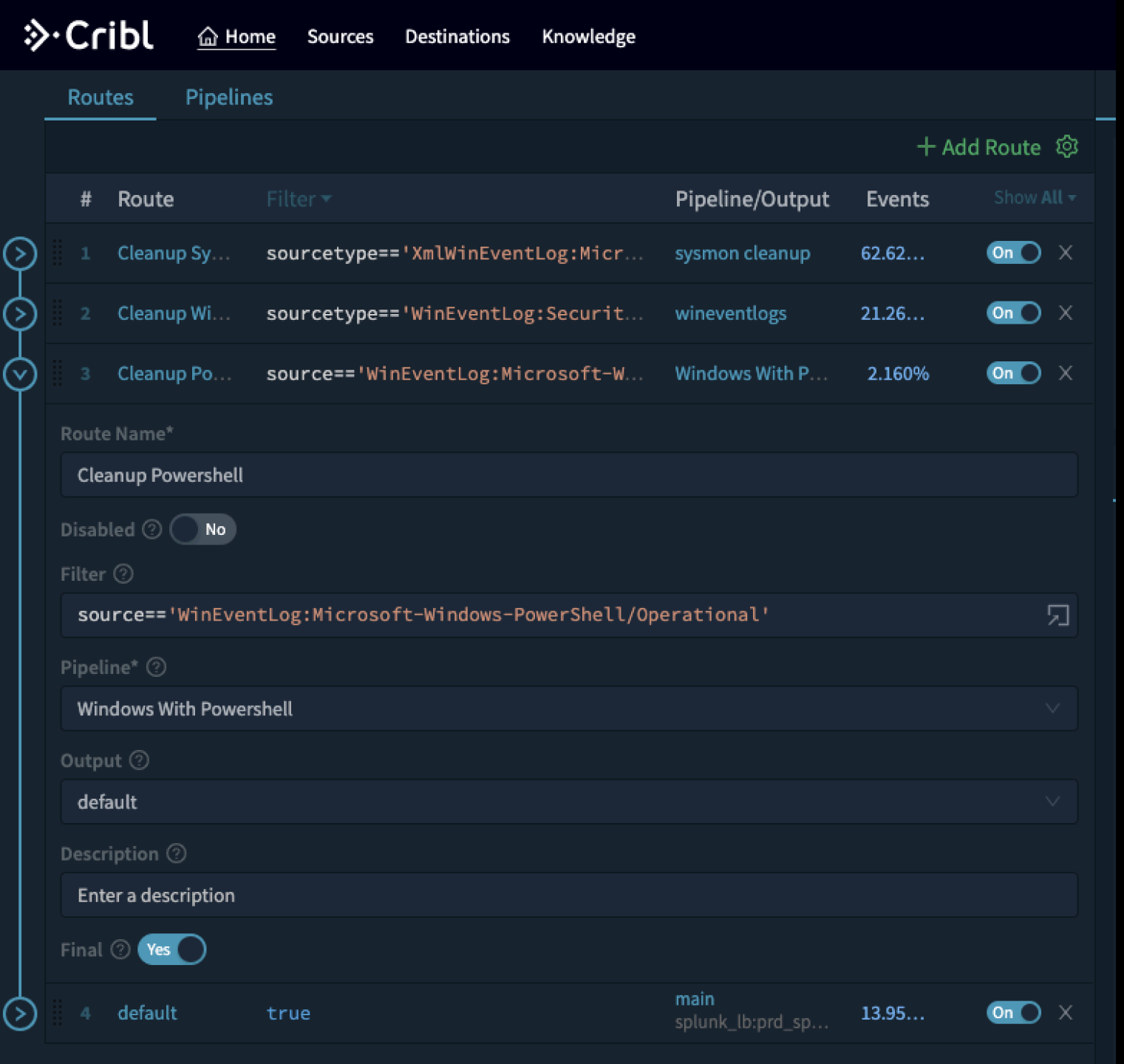
Filtering of Common DNS Destinations!



(Variation: Alexa Top 1000)

https://blog.cribl.io/2019/01/28/using-cribl-to-analyze-dns-logs-in-real-time-part-2/

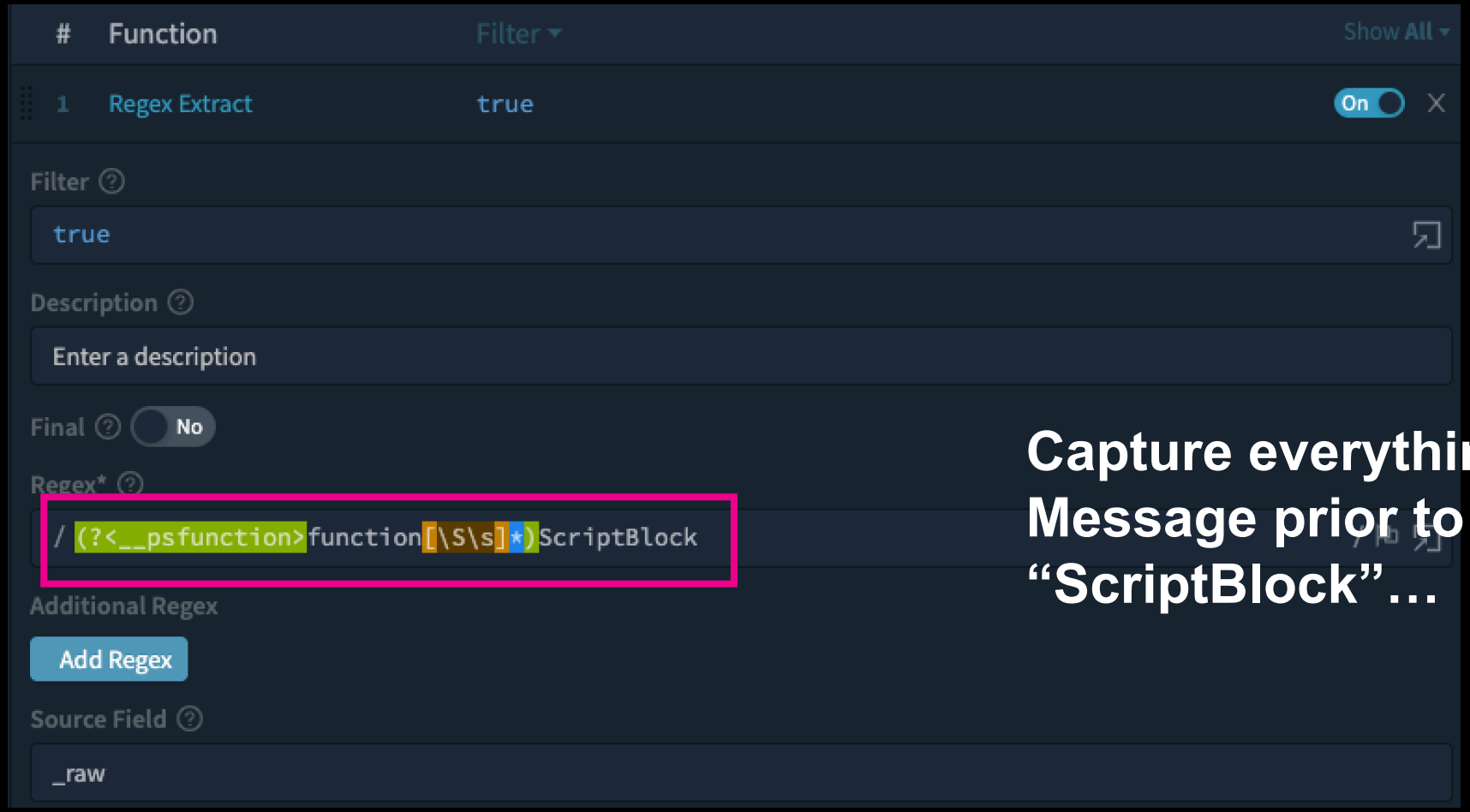
splunk> .conf19



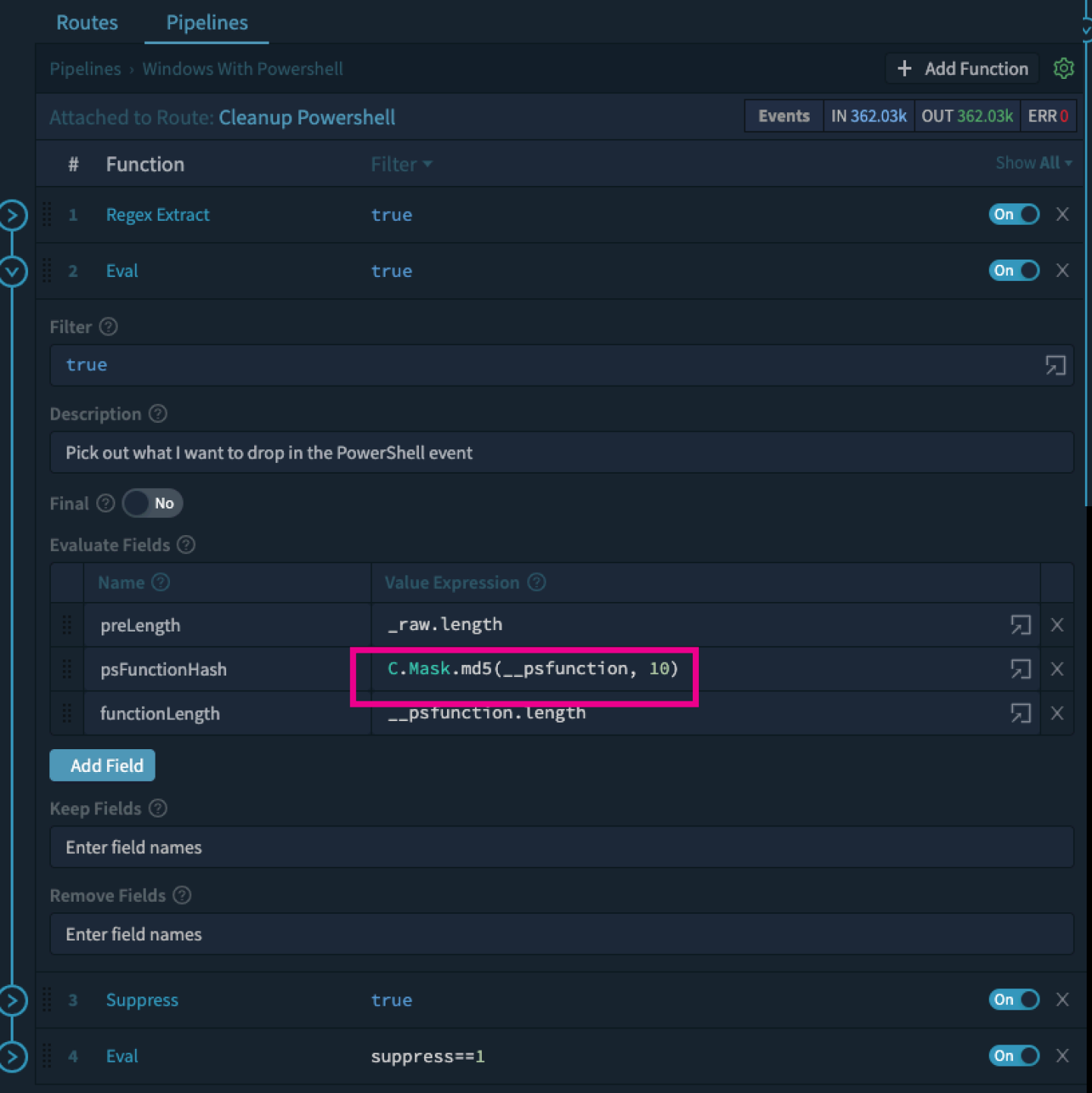
Remember our pesky 4104 filtering issue?

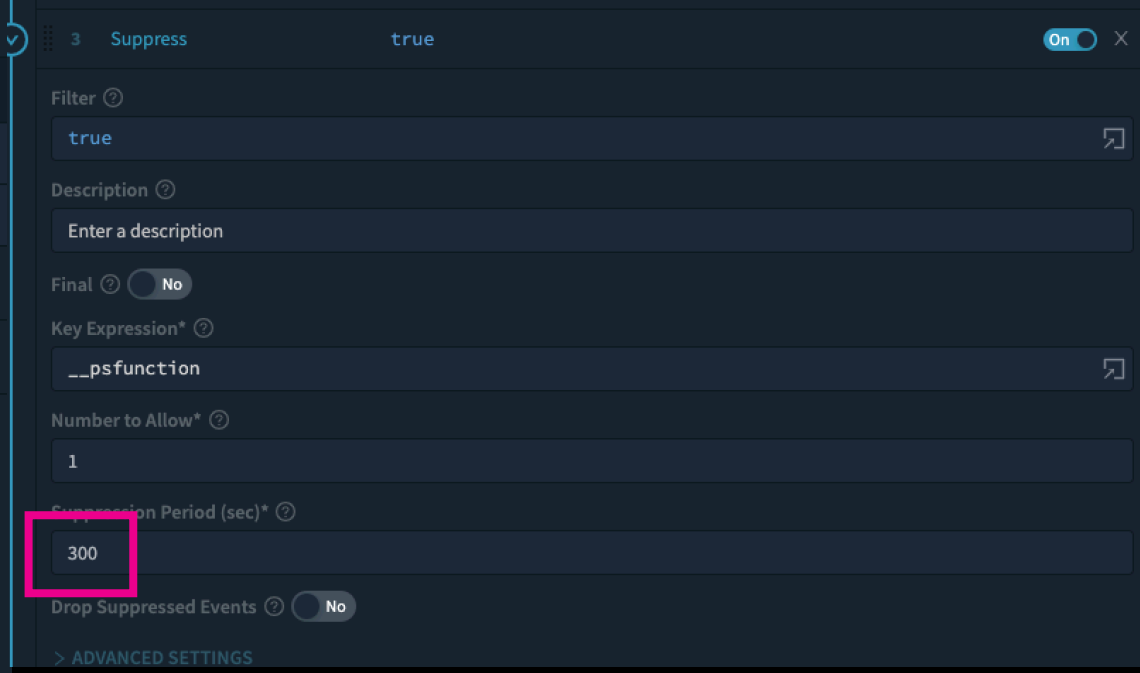
MD5 Hashing of Powershell Script Block Logging Content!

splunk> .conf19



Capture everything in the Message prior to "ScriptBlock"…





…and if it's the same hash, suppress it unless 10m (configurable) has elapsed.

DSP too?

Splunk® Data Stream Processor

Data Stream Processor Function Reference

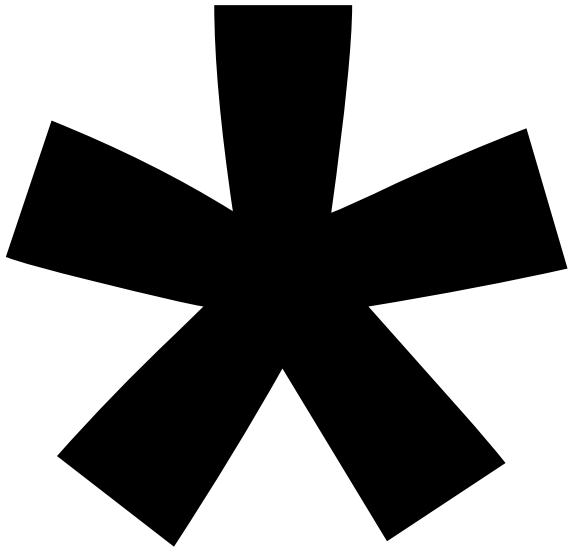
Download manual as PDF

Cryptographic scalar functions	`md5`	Computes and returns the MD5 hash of a byte value X.
	`sha1`	Computes and returns the secure hash of a byte value X based on the FIPS compliant SHA-1 hash function.
	`sha256`	Computes and returns the secure hash of a byte value X based on the FIPS compliant SHA-256 hash function.
	`sha512`	Computes and returns the secure hash of a byte value X based on the FIPS compliant SHA-512 hash function.

DSP has a very rich library of functions…including hashing.

Does it scale?

DSP: 5 nodes
27TB a day.




A
UNIVERSAL
PICTURE
splunk>
FORWARDER

The Universal Forwarder: Pros and Cons

- No per-node license
- Fully supported by Splunk
- Lots of success and community help
- Efficient and secure transfer of data
- Efficient distribution of data (if architected properly)
- Less complexity
- Lots of capability besides “just logs”

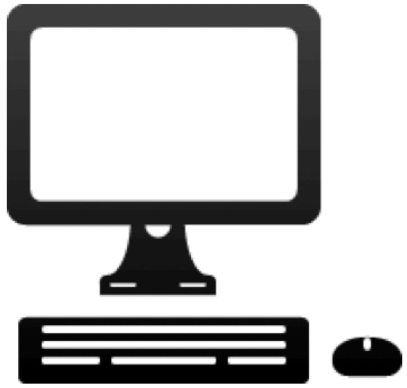
Slides from .confs of yore…

The UF: It's More Than You Think

Process/Apps/FIM

Registry

Scripts



Perfmon

Wire Data

Sysmon

Logs

*Including PowerShell!

The Universal Forwarder: Pros and Cons

- No per-node license
- Fully supported by Splunk
- Lots of success and community help
- Efficient and secure transfer of data
- Efficient distribution of data (if architected properly)
- Less complexity
- Lots of capability besides “just logs”

- It’s an agent.


People HATE agents.

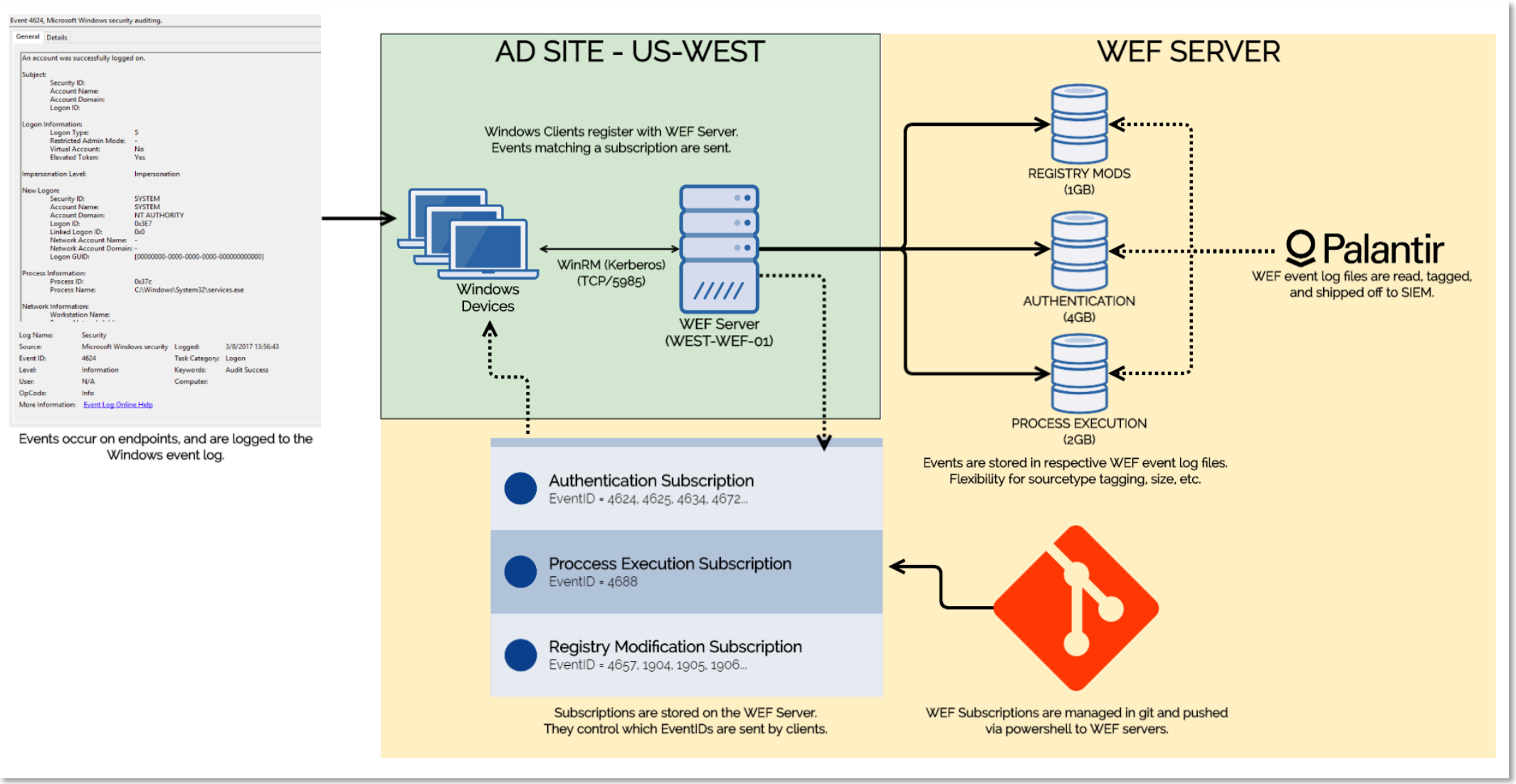
The Universal Forwarder: Pros and Cons

- No per-node license
- Fully supported by Splunk
- Lots of success and community help
- Efficient and secure transfer of data
- Efficient distribution of data (if architected properly)
- Less complexity
- Lots of capability besides “just logs”

- It’s an agent
- You have to install and maintain it
- It doesn’t run on all OS’s you may have
- It only sends to Splunk*
- Improperly configured it can impact performance
- It can be used for good…or evil…

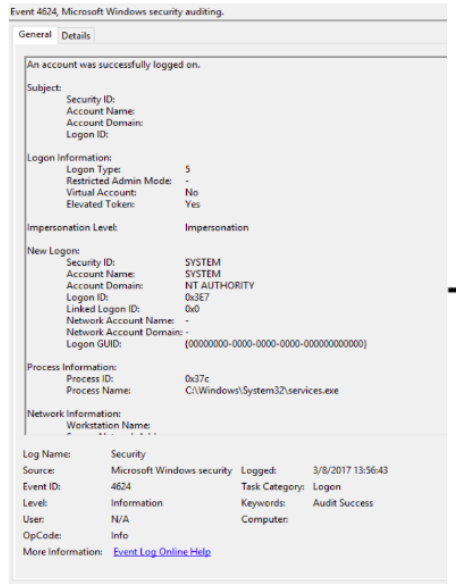

NO
UNIVERSAL
PICTURE
FORWARDER

You could use Windows Event Forwarding!

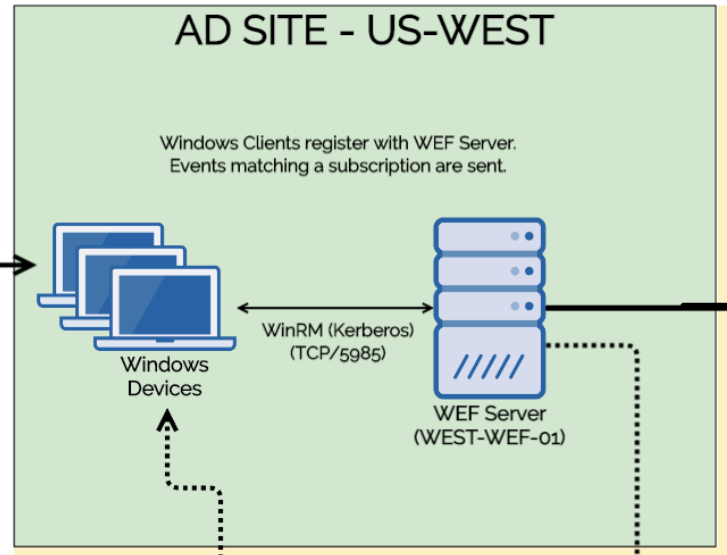


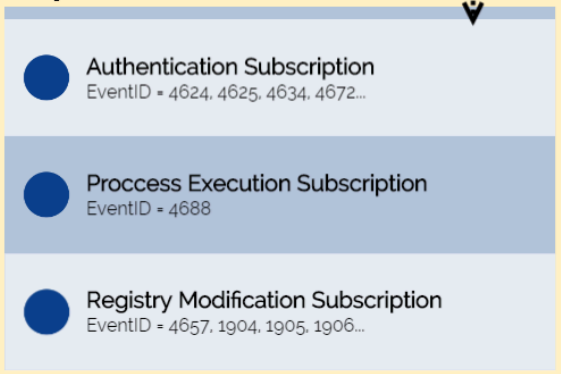
splunk> .conf19

You could use Windows Event Forwarding!

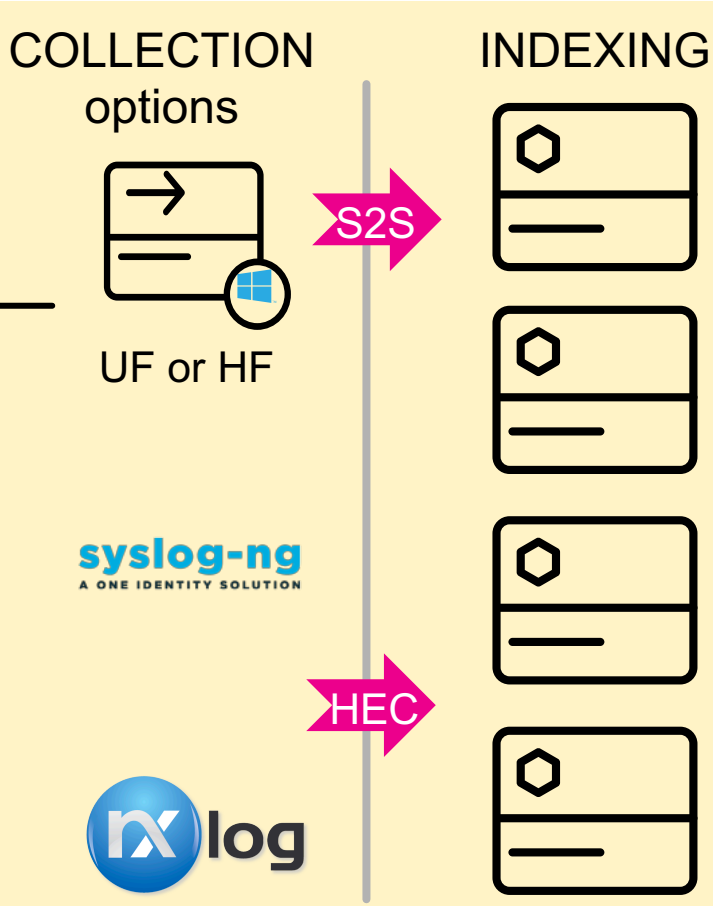


Events occur on endpoints, and are logged to the Windows event log.





Subscriptions are stored on the WEF Server.
They control which EventIDs are sent by clients.



Maybe winlogbeat or Azure Event Hub, too…

WEF Pros and Cons

- No agent!
- No additional license cost
- Supported by Microsoft
- Can support most modern versions of Windows
- Might be the “only” option due to agentless
- Easy to configure on the endpoint via GPO
- No need to filter UF “junk” from 4688/Powershell/Sysmon
- Now supported by the Windows TA so…”officially supported” by Splunk (XML needed)

- You shift processing to a much smaller number of nodes! Latency abounds.
- You have to create and maintain a complex collection infrastructure.
- Higher network utilization due to XML:SOAP wrappers
- DCOM and RPC=++ attack surface
- Difficult to collect off campus
- No failover, no load balancing, might lose events.
- Data sources limited to “events that can log to .evtx format” so no IIS, DHCP, Windows Update, scripted collection…
- If you don’t use UF/HF then custom props/transforms
- Must use XML render
- Troubleshooting notoriously hard!

Hardening Windows Remote Management (WinRM)

```
Tactic: Lateral dispersion between systems via Windows Remote Management (WinRM)
and PowerShell remoting
```

Manual operators may leverage Windows Remote Management (WinRM) to propagate ransomware throughout an environment. WinRM is enabled by default on all Windows Server operating systems (since Windows Server 2012 and above), but disabled on all client operating systems (Windows 7 and Windows 10) and older server platforms (Windows Server 2008 R2).

PowerShell Remoting (PS Remoting) is a native Windows remote command execution feature that's built on top of the WinRM protocol.

If WinRM has ever been enabled on a client (non-server) operating system, then the following configurations will exist on an endpoint, and will not be remediated solely through the PowerShell command noted in Figure 20.

- WinRM listener configured
- Windows Firewall exception configured

These items will need to be disabled manually through the commands in Figure 23 and Figure 24.

Figure 20.

PowerShell Command to disable WinRM / PowerShell Remoting on an endpoint.

PowerShell:

```
Disable-PSRemoting -Force
```

Note: Disabling PowerShell Remoting does not prevent local users from creating PowerShell sessions on the local computer - or for sessions destined for remote computers.

After running the command, the message recorded in Figure 21 will be displayed.

Figure 21. Warning message after disabling PSRemoting.

```
PS C:\WINDOWS\system32> Disable-PSRemoting -Force
WARNING: Disabling the session configurations does not undo all the changes made by
Enable-PSSessionConfiguration cmdlet. You might have to manually undo the changes b
    1. Stop and disable the WinRM service.
    2. Delete the listener that accepts requests on any IP address.
    3. Disable the firewall exceptions for WS-Management communications.
    4. Restore the value of the LocalAccountTokenFilterPolicy to 0, which restricts remote access to members of the
Administrators group on the computer.
```

WEF relies on WinRM.

WinRM should be hardened (prevent lateral move).

```
winrm set winrm/config/client '@{TrustedHosts="JumpBox1,JumpBox2"}'
```

splunk> .conf19

```
[WinEventLog://ForwardedEvents]
blacklist1 = EventCode="566" Message="Object Type:\s+(?!groupPolicyContainer)"
blacklist2 = 4656,4658,4660-4663,4665-4667,4673,4690,4793,4907,4932,4933,4985
blacklist3 = 5061,5058,5145,5152,5154,5156-5158
blacklist4 = 26401,36886
blacklist5 = EventCode="4688" Message="(?:New Process
Name:).+(?:SplunkUniversalForwarder\\bin\\splunk.exe)|.+(?:SplunkUniversalForwarder\\bin\\splunkd.exe)|.+(?:SplunkUniversalForwar
der\\bin\\btool.exe)|.+(?:Splunk\\bin\\splunk.exe)|.+(?:Splunk\\bin\\splunkd.exe)|.+(?:Splunk\\bin\\btool.exe)|.+(?:Agent\\MonitoringHost.e
xe)"
blacklist6 = 2002,4614,4664,4675,4700-
4702,4717,4779,4905,4931,4933,4944,4945,4957,5012,5024,5056,5058,5059,5061,5379,5440,5442,5444,5447,5448,5450,5478,5632,5633,588
9,5890,6278,6419,6421,6422,7001,7036,7043
blacklist7 = EventCode="4674"
Message=".*[\S\s]*Account\sName:\s:.+specadmin.+Process\sName:.+\\Windows\\SysWOW64\\wbem\\WmiPrvSE.exe|.+\\Windows\\Syst
em32\\wbem\\WmiPrvSE.exe"
current_only = 0
disabled = 0
evt_dc_name =
evt_dns_name =
evt_resolve_ad_obj = 0
host = WinEventLogForwardHost
renderXML=false
interval = 60
sourcetype = WinEventLog:ForwardedEvents
start_from = oldest
suppress_sourcename=true
suppress_keywords=true
suppress_type=true
suppress_task=true
suppress_opcode=true
suppress_text=true
```

Prevents event latency, but actually isn't ideal, and isn't CIM compliant…

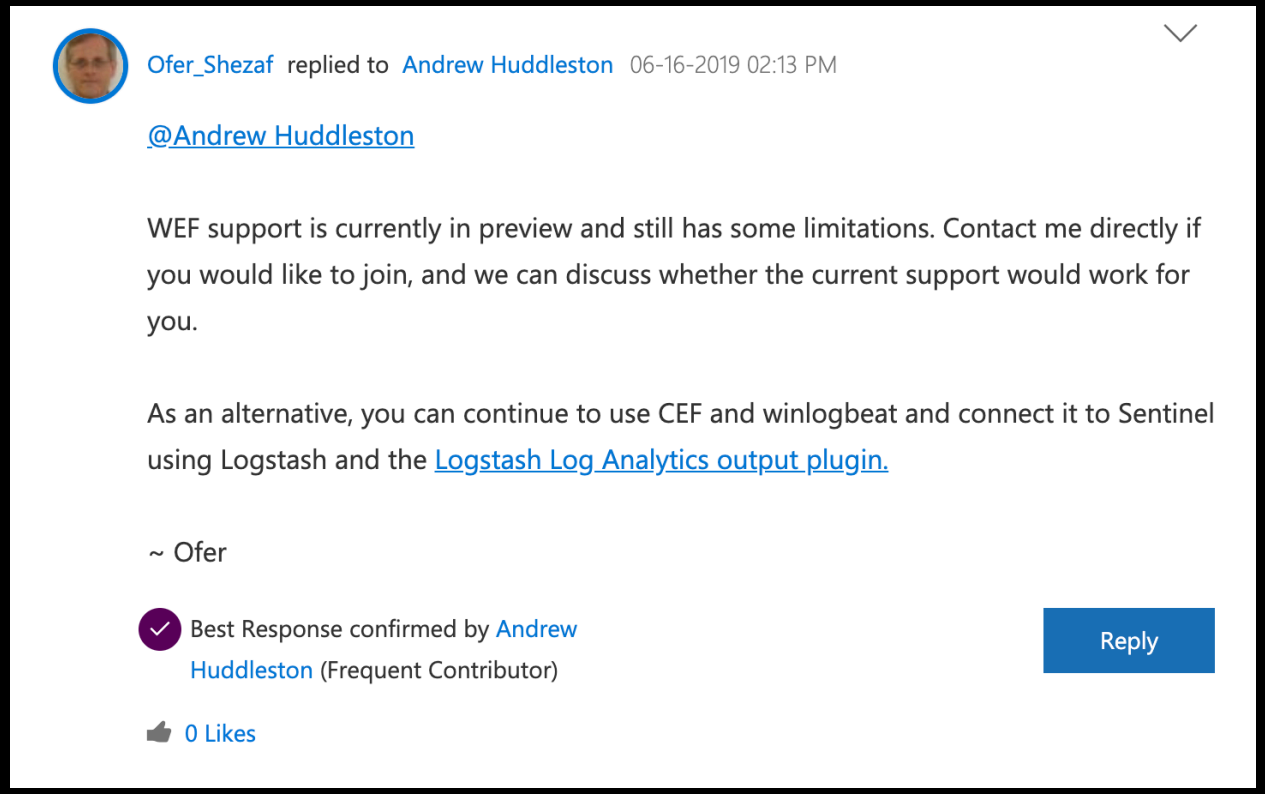

We don’t have a lot of examples of successful WEF/WEC deployment at scale. ☹

what about…

You could use cloud storage*!

Microsoft WEF → WEC → Azure Event Hub → splunk>

- Windows Logs



Ofer_Shezaf replied to Andrew Huddleston 06-16-2019 02:13 PM

@Andrew Huddleston

WEF support is currently in preview and still has some limitations. Contact me directly if you would like to join, and we can discuss whether the current support would work for you.

As an alternative, you can continue to use CEF and winlogbeat and connect it to Sentinel using Logstash and the Logstash Log Analytics output plugin.

~ Ofer

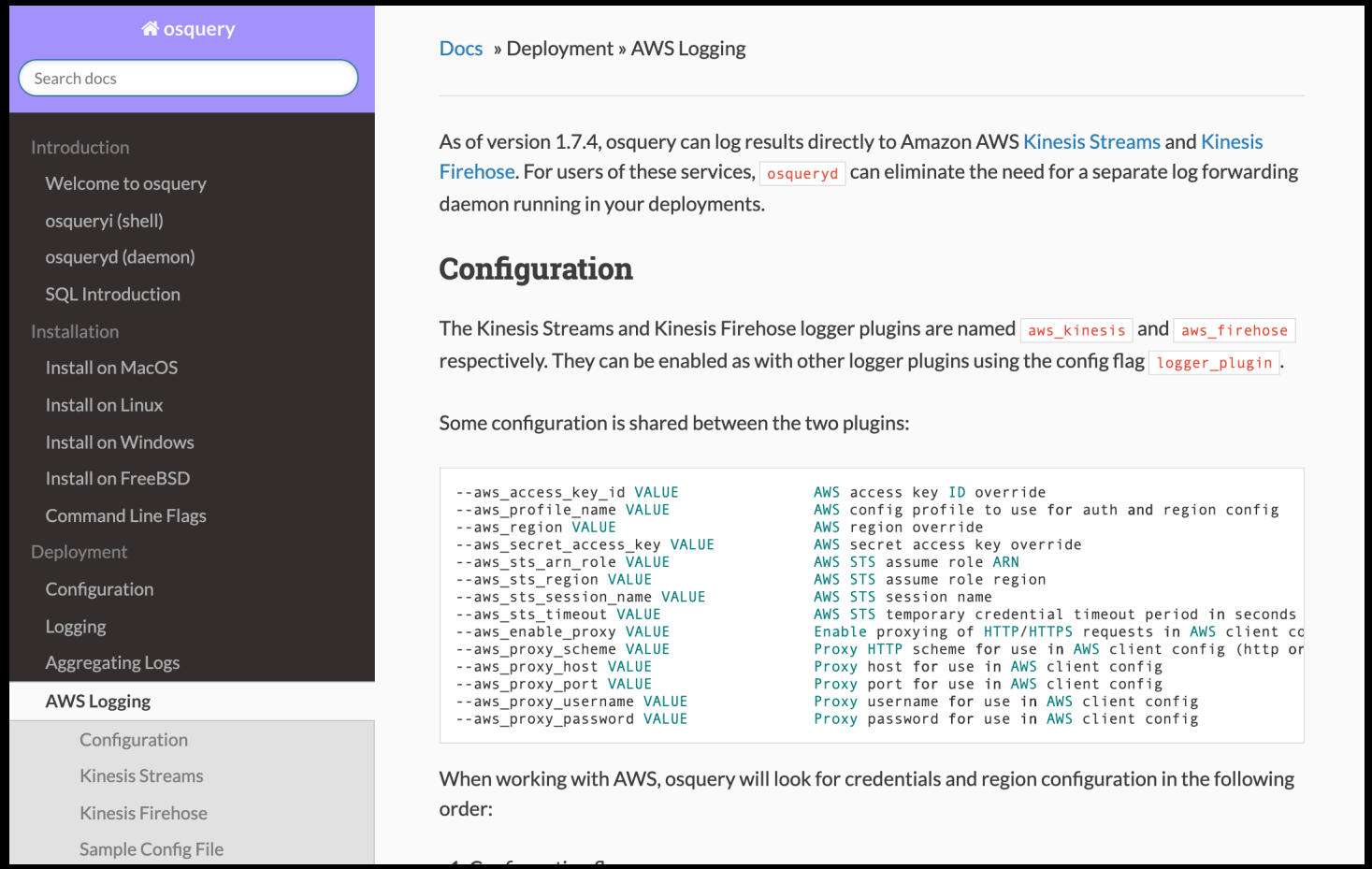
Best Response confirmed by Andrew Huddleston (Frequent Contributor)

Reply

0 Likes

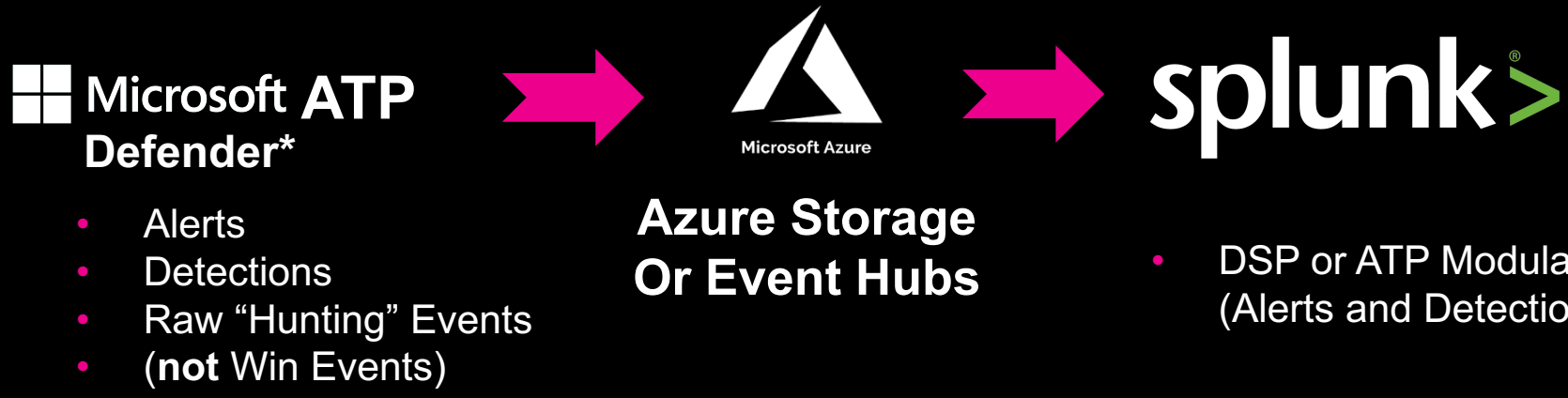
You could use cloud functionality*!

osquery → aws Kinesis Streams or Firehose* (S3) → splunk>



- Splunk Add On for Amazon Kinesis Firehose
- Splunk Input for Kinesis Streams
- SQS-based S3 input

You could pay for and use Microsoft Defender ATP!



- Alerts
- Detections
- Raw “Hunting” Events
- (**not** Win Events)

- DSP or ATP Modular Input (Alerts and Detections)

- ATP capability built into Windows 10, later server versions. Installable on 7,8,2016, 2012
- Needs E5 license for desktops and Azure Security Center licenses for servers
- MacOS (but signature based)
- No CIM mapping


splunk>
Hands On! Encoded
Powershell Logs!

How did Violent Memmes avoid C2 detection during execution?

Sourcetypes: Microsoft Sysmon and/or WinEventLog:Security

MITRE ATT&CK: Execution
T1086: Powershell
T1043: Commonly Used Port
T1132: Data Encoding
T1172: Domain Fronting

WINDOWS AND SYSMON EVENTS

The adversary used domain fronting to obfuscate the origin of their command and control (C2) traffic. Clues exist that provide insights into the HTTP host header used to mask the true origin of the traffic. What is the host header that is used by the adversary?

(7 correct!)

(Hands On Redacted)

What's New?

What's new with Sysmon?

- DNS Logging with EventCode 22
- Our TA for Sysmon is Endpoint CIM compliant
- The Github version supports Sysmon 10.x
- Researchers publishing new rulesets for granular detections:
  - UAC Bypass
  - Chinese/Vietnamese/Iranian keyboard layout connecting to server

Updated Olaf/TaySwift Sysmon to Eliminate this:

ParentCommandLine

12 Values, 100% of events

Reports

Top values Top values by time

Events with this field

Top 10 Values	Count
C:\Windows\system32\cmd.exe /c wmic os get LocalDateTime /value 2>nul	2,270
C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_installed_apps.bat""	1,595
C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listening_ports.bat""	203
C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_timesync_configuration.bat""	203
C:\Windows\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_timesync_status.bat""	203
C:\WINDOWS\system32\cmd.exe /c wmic os get LocalDateTime /value 2>nul	66
C:\WINDOWS\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listening_ports.bat""	22
C:\WINDOWS\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_timesync_configuration.bat""	22
C:\WINDOWS\system32\cmd.exe /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_timesync_status.bat""	22
cmd /c ""C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listening_ports.bat""	22

https:/

New “SEDCMD” Cleanups in Win TA 6.0!

[source::XmlWinEventLog:Security]
…
Explanation for SEDCMD Extractions
windows_security_event_formater: This will replace all values like "Account Name:-" to "Account Name:"
windows_security_event_formater_null_sid_id: This will replace all values like "Security ID:NULL SID" to "Security ID:" and all values like "Logon ID:0x0" to "Logon ID:"
cleansrcip: This will replace all values like "Source Network Address: ::1" or "Source Network Address:127.0.0.1" to "Source Network Address:"
cleansrcport: This will replace all values like "Source Port:0" to "Source Port:"
remove_ffff: This will replace all values like "Client Address: ::ffff:10.x.x.x" to "Client Address:10.x.x.x" which Addresses most of the Ipv6 log event issues
clean_info_text_from_winsecurity_events_certificate_information: This will delete all the infomation text at the end of event starting from "Certificate information is..." before indexing
clean_info_text_from_winsecurity_events_token_elevation_type: This will delete all the infomation text at the end of event starting from "Token Elevation Type indicates..." before indexing
clean_info_text_from_winsecurity_events_this_event: This will delete all the infomation text at the end of event starting from "This event is generated..." before indexing
cleanxmlsrcport: This will replace all values like <Data Name='IpPort'>0<\/Data> to <Data Name='IpPort'><\/Data> in XmlWinEventLog:Security
cleanxmlsrcip: This will replace all values like <Data Name='IpAddress'>::1<\/Data> or <Data Name='IpAddress'>127.0.0.1<\/Data> to <Data Name='IpAddress'><\/Data> in XmlWinEventLog:Security

SEDCMD Extractions
#SEDCMD-windows_security_event_formater = s/(?m)(^\s+[^:]+\:)\s+-?$/\1/g
#SEDCMD-windows_security_event_formater_null_sid_id = s/(?m)(:)(\s+NULL SID)$/\1/g s/(?m)(ID:)(\s+0x0)$/\1/g
#SEDCMD-cleansrcip = s/(Source Network Address: (\:\:1|127\.0\.0\.1))/Source Network Address:/
#SEDCMD-cleansrcport = s/(Source Port:\s*0)/Source Port:/
#SEDCMD-remove_ffff = s/::ffff://g
#SEDCMD-clean_info_text_from_winsecurity_events_certificate_information = s/Certificate information is only[\S\s\r\n]+$//g
#SEDCMD-clean_info_text_from_winsecurity_events_token_elevation_type = s/Token Elevation Type indicates[\S\s\r\n]+$//g
#SEDCMD-clean_info_text_from_winsecurity_events_this_event = s/This event is generated[\S\s\r\n]+$//g

For XmlWinEventLog:Security
#SEDCMD-cleanxmlsrcport = s/<Data Name='IpPort'>0<\/Data>/<Data Name='IpPort'><\/Data>/
#SEDCMD-cleanxmlsrcip = s/<Data Name='IpAddress'>(\:\:1|127\.0\.0\.1)<\/Data>/<Data Name='IpAddress'><\/Data>/

Non-destructive truncate of Message block

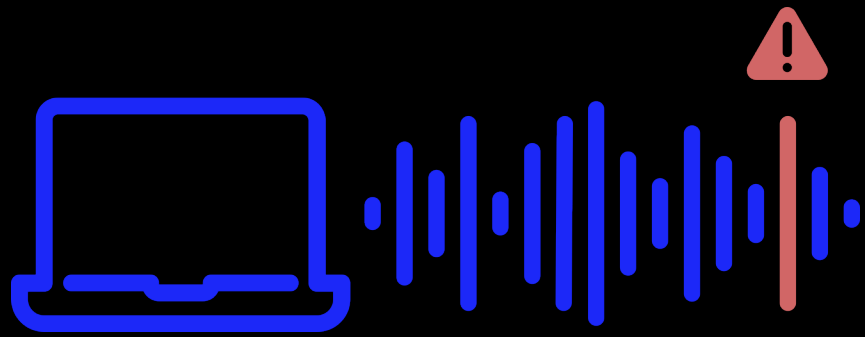
cmdReporter macOS Agent!

cmdReporter is an endpoint detection and response tool for macOS.

Using native built-in resources, it collects the
data IT security teams need to hunt threats on macOS computers in real time.

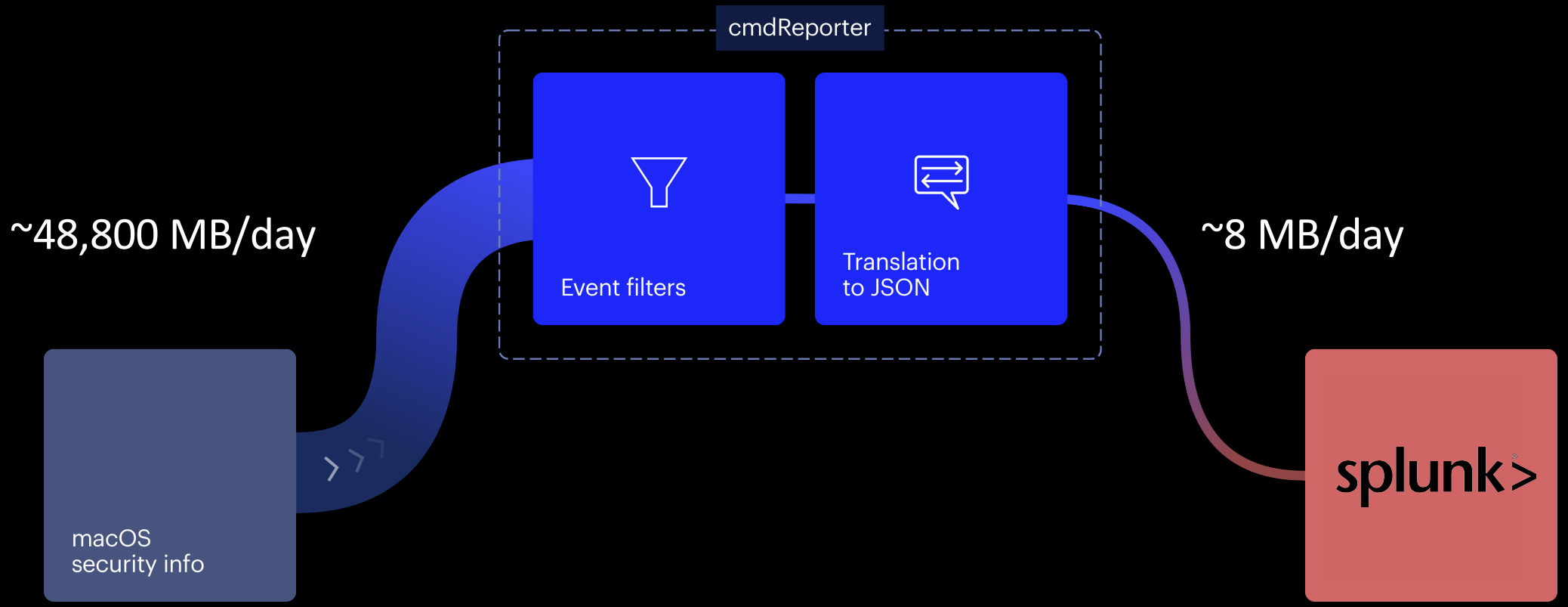
8MB daily on average, 14MB if highly granular network connections enabled
(If a process changes prefs, elevates privs, or makes network connections info is sent)

25,000 mac endpoints so far…



Thanks Dan Griggs!

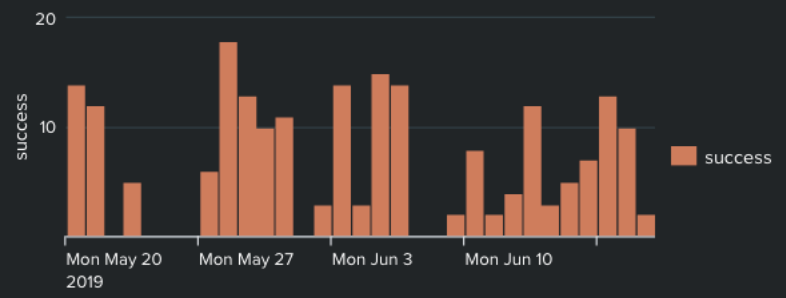
What cmdReporter does



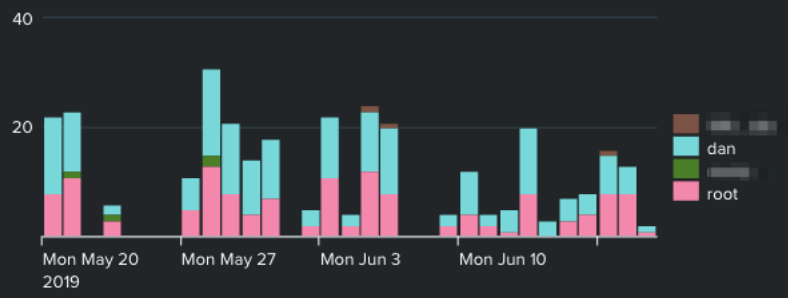
macOS 10.15b1 security data in Splunk cross-platform dashboard

Authentications and Changes

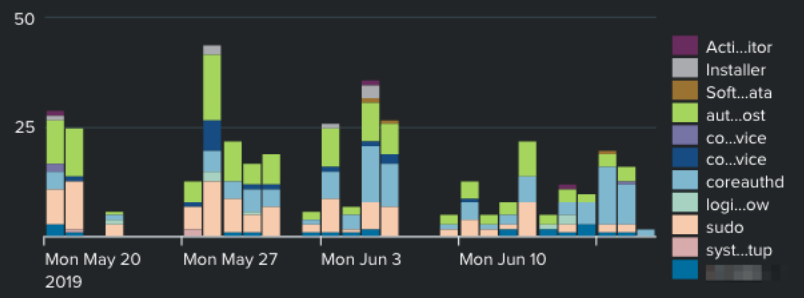
Authentications by Action



Authentications by User



Authentications by App



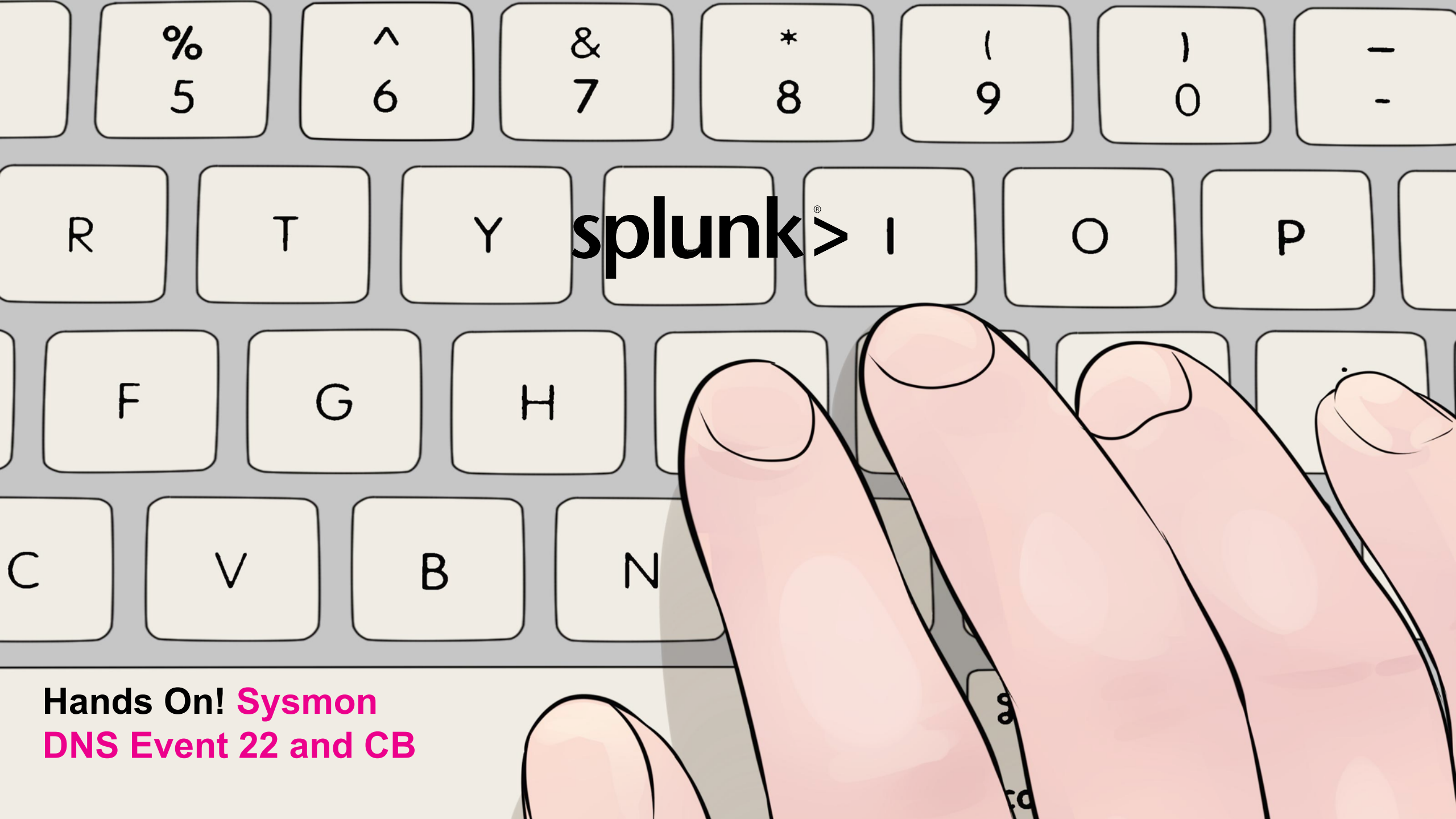
Asset Authentications

_time	src	dest	action	app	count	user	src_user
2019-06-11 23:44:32	Dan_macbook_pro		success	sudo	370	root	dan
2019-05-20 21:28:16	[redacted]		success	Activity Monitor Installer com.apple.preference.security.remoteservice com.apple.preferences.sharing.remoteservice com.apple.preferences.users.remoteservice coreauthd	252	dan	dan
2019-06-18 22:33:46	Dan_macbook_pro	Dan_macbook_pro	success	sudo	186	root	dan
2019-05-23 23:00:34	[redacted]		success	sudo	160	root	dan
2019-06-12 14:54:12	Dan_macbook_pro		success	Apple Configurator 2 Autoupdate Finder GitHub Desktop Installer com.apple.preferences.configurationprofiles.remoteservice coreauthd lldb-rpc-server storedownloadd	153	dan	dan

« prev 1 2 3 4 next »

cmd Reporter

(infosec app)


splunk>
Hands On! Sysmon
DNS Event 22 and CB

What evidence can we find surrounding previous infiltration from Violent Memmes?

Sourcetypes: Microsoft Sysmon (or any other source that provides DNS query info), Carbon Black Response

MITRE ATT&CK: Establish and Maintain Infrastructure, Execution
T1333 Dynamic DNS (pre ATT&CK)
T1085 Rundll32

SYSMON DNS LOGGING AND CARBON BLACK PROCESS EXECUTION

There is evidence in the logs that the Violent Memmes have been on the Frothly network before. If you follow that evidence, what is the Base64 string of the fully qualified domain name (FQDN) the adversary communicates with?

(ZERO correct! 80 wrong attempts.)

(Hands On Redacted)

Take-aways!

- Endpoints remain one of the most important security data sources.
- There are many rich and varied endpoint sources both free and commercial you can ingest, and they are critical for advanced detection.
- Not everything is critical to collect and we now have tools to help you decide what is best for you!

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION