splunk> .conf2017

Splunking The Endpoint III:

Hands-On with Boss of the SOC data!

(plus some other stuff)

James Brodsky | Sr. SE Manager / BOTS Scenario Owner

28 September 2017 | Washington, DC

whoami

- Sr. Sales Engineering Manager, Boulder CO of some of the hardest working SEs in Splunk
- Supports Major Accounts for Splunk in the West
- Splunk Security Architects Crazy Uncle
- Splunking the Endpoint! .conf2015, .conf2016
- BOTS 1.0, 2.0 BOTN 1.0
- CSC 20 Whitepaper, FFIEC Whitepaper (co-author), Tripwire apps, blogs, Sysmon contributions, etc, etc....

splunk> .conf2017


%
5
^
6
&
7
*
8
(
9
)
0
_
-
R
T
Y
.conf2017
I
O
P
F
G
splunk>
BOSS
of the SOC 2017
.conf2017
C
V
B
N
It’s a hands-on session.
Eventually. But first slides.
Lots of slides.

Even if you're Shatner you still need to have brought a functional, modern computing device.

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

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

roll d20 to determine your server!

left side of room="a"

right side of room="b"

splunk> .conf2017

SPLUNKING THINGS

roll d20 to determine your server!

left side of room="a"

right side of room="b"

prepend with "0" if single digit

alice/epsecurity

= https://conf17-bots-endpoint-14a.splunkoxygen.com

or

= https://conf17-bots-endpoint-14b.splunkoxygen.com

Depending on what side of the room you are on.

splunk> .conf2017

.conf2017 - Splunking the Endpoint III - Hands-On with BOTS (and other) data!

Welcome to the 3rd edition of our .conf Endpoint breakout sessions, and the 2nd edition that includes a hands-on component. This year (2017) we'll showcase malware and ransomware investigation, data from non-Windows endpoints, and a brief tour through some of Ransomware's greatest hits of 2017. And, we'll mostly leverage data from Boss of the SOC (BOTS) v2.0 to do so.

This hands-on material was developed with awareness and consideration of the sessions that have come before it in 2015 and 2016, as well as a close collaboration with the BOTS team. Rather than publish all of the instructions and related resources for this session in an app, as was done in 2016, we have chosen to provide several bits of written collateral to help guide you through the BOTS (and some other ransomware) data.

https://splunk.box.com/v/conf2017-endpoint-ho-detailed

How to Use This App

Simply download one or more of the companion .PDFs linked below - whichever suits your learning style - and use the "Search" link above or here to run the searches and follow along with the session. Also download the encrypted JPG file from the last link. Once you get to the third major part of the session, visit the "WannaCry/EternalRocks/NotPetya" app here.

Companion Material Downloads

- Detailed Companion Document with Screenshots and Short Explanations
- Abbreviated Companion Document with Just Searches
- Full Companion Document in Whitepaper Format

- Encrypted Image File for Ransomware Step 3

Select additional content to view using the checkbox

splunk> .conf2017

What we'll cover

Agenda

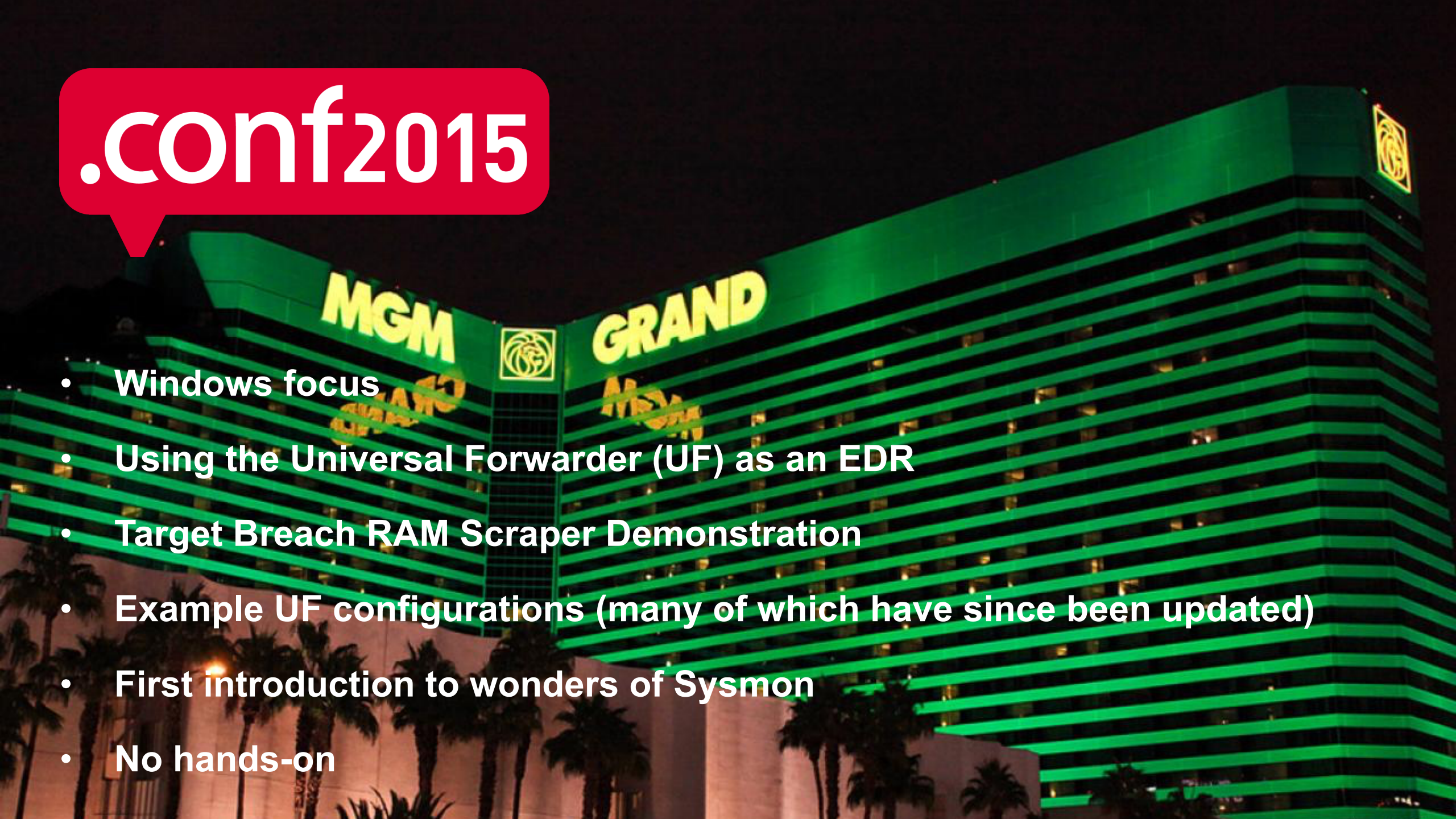
90 whirlwind minutes…

- Where have we been?
- What's new over the past year or so?
  - **Hands-on adventure #1**
- Endpoints aren't limited to Windows
  - **Hands-on odyssey #2**
- The part where we all have a group cry
  - **Hands-on journey #3**
- Q&A

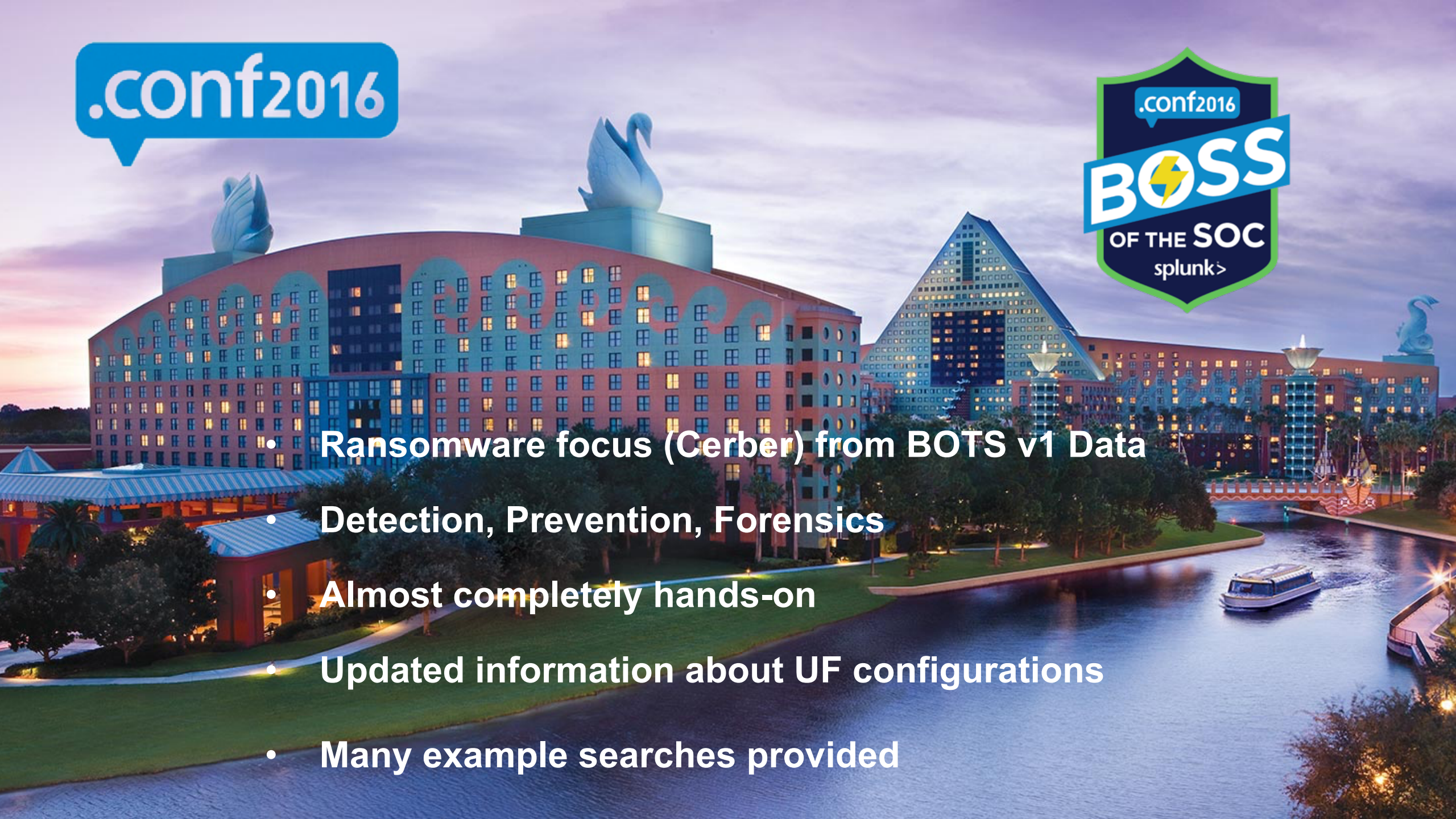
We're still talking about this…

…because frankly there's something new to talk about every year.

splunk> .conf2017



- Windows focus
- Using the Universal Forwarder (UF) as an EDR
- Target Breach RAM Scraper Demonstration
- Example UF configurations (many of which have since been updated)
- First introduction to wonders of Sysmon
- No hands-on


.conf2016
.conf2016
BOSS
OF THE SOC
splunk>
• Ransomware focus (Cerber) from BOTS v1 Data
• Detection, Prevention, Forensics
• Almost completely hands-on
• Updated information about UF configurations
• Many example searches provided

730 days later…still relevant.

The UF: More Than You Think!

Process/Apps/FIM

Vulnerabilities

Firewall

Registry

Wire Data

Forensics

Logs

Sysmon

*Including powershell!


splunk>
splunk>
Our new communications director has some updates to communicate about endpoint topics and Splunk.
And then he has to leave.

Update: Sysmon Love Fest

splunk> .conf2017

Microsoft Sysmon: It keeps getting better.

Splunk

- Splunk enables collection and rich queries of Sysmon data
- Configuring Splunk for Sysmon:
  https://github.com/splunk/TA-microsoft-sysmon
  - Install Splunk universal forwarder on Sysmon systems
  - Install Splunk Sysmon TA on search heads
  - Set Sysmon configuration to exclude Splunk binaries

```
<Image condition="contains">splunk</Image>
<Image condition="contains">streamfwd</Image>
...
```

Microsoft

RSAConference2017

Current Version: 6.10

splunk> .conf2017

What's new in Sysmon (past 2 years)?

- **Event Code 11: File Creation**
  - Poor mans FIM
  - Log when a file is created or over-written – monitor creation of things in autorun locations or with usually-suspicious extensions (.bat, .vbs, .ps1, .docm, .xlsm)

- **Event Codes 12, 13, 14: Registry key creation and modification**
  - More flexible/performant than registry monitoring built into UF
  - More persistent delivery than UF due to event log mechanism

- **Event Code 15: Alternate Data Stream Creation**
  - Tracks if/when files are created with ADS that have suspicious content (.bat, .vbs, .ps1, .cmd, etc…)
  - Browser Drops (Mark Of The Web)

- **Event Code 10: Process Access**
  - One process accessing the memory of other processes
  - Probably too noisy to use

And on 9/11/17, moar Sysmon…

- **Event Codes 17 and 18: Pipe Events**
  - Sometimes malware uses named pipes for interprocess communication

- **Event Codes 19, 20, and 21: WMI Stuff**
  - WMI event filter, event consumer, and event consumer to filter activity

For a good example of recent malware using BOTH of these techniques, research "Nyetya" derivative of Petya/NotPetya/Goldeneye.

http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

Sysmon TA has been updated in two places – we will see in 3.5 minutes…

How awesome are you, Taylor Swift?

- You are a wonderful person that knows how useful Sysmon is*.
- If you aren't using SwiftOnSecurity's Sysmon config, you should. Google "taytay swift sysmon" and you'll find it.
- And if you'd like some Splunky tweaks to it...those are on the next page.

**Not yet inclusive of latest 3 WMI Sysmon event codes.*

splunk> .conf2017

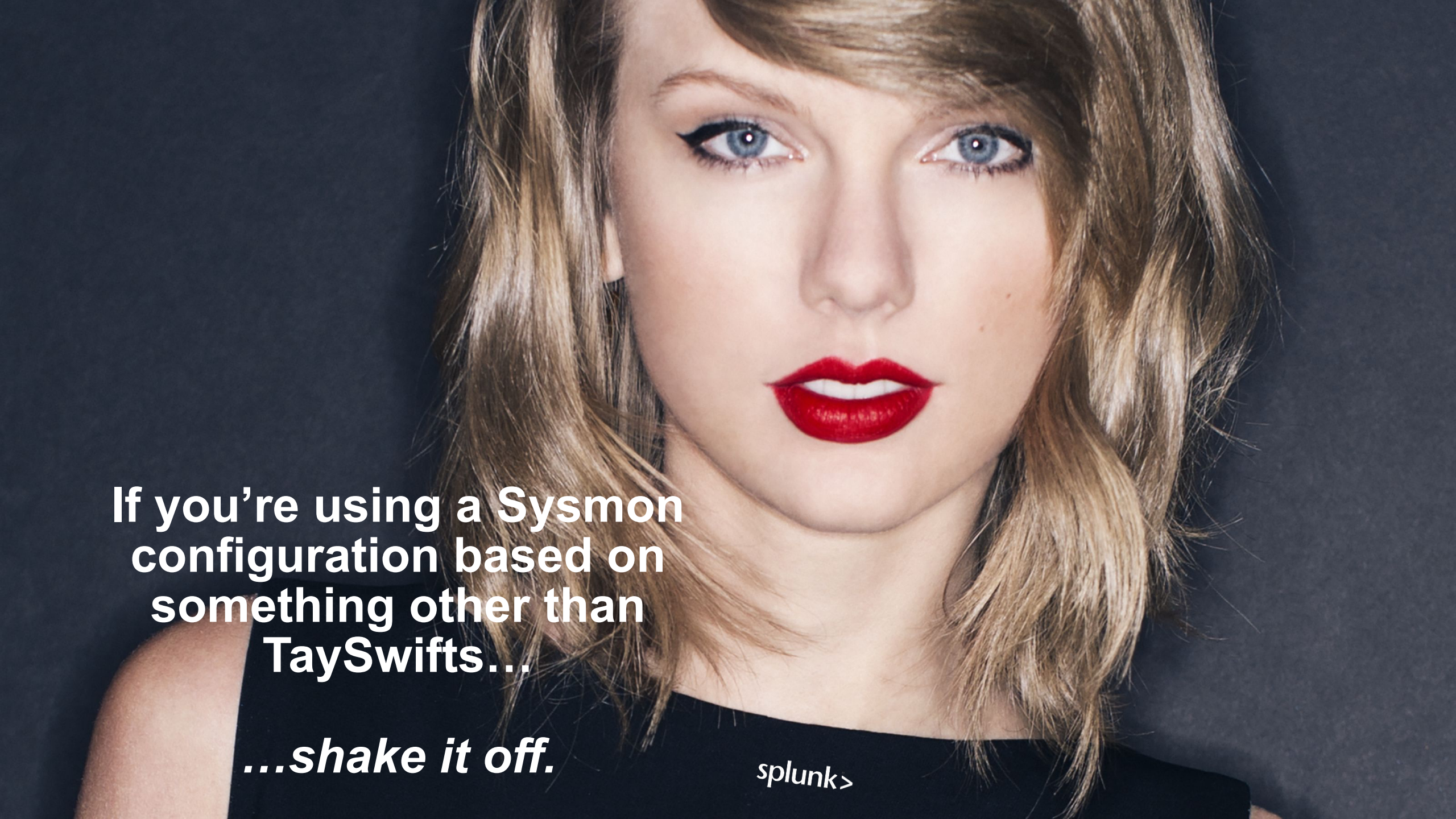
Exclusions for EventCode 1

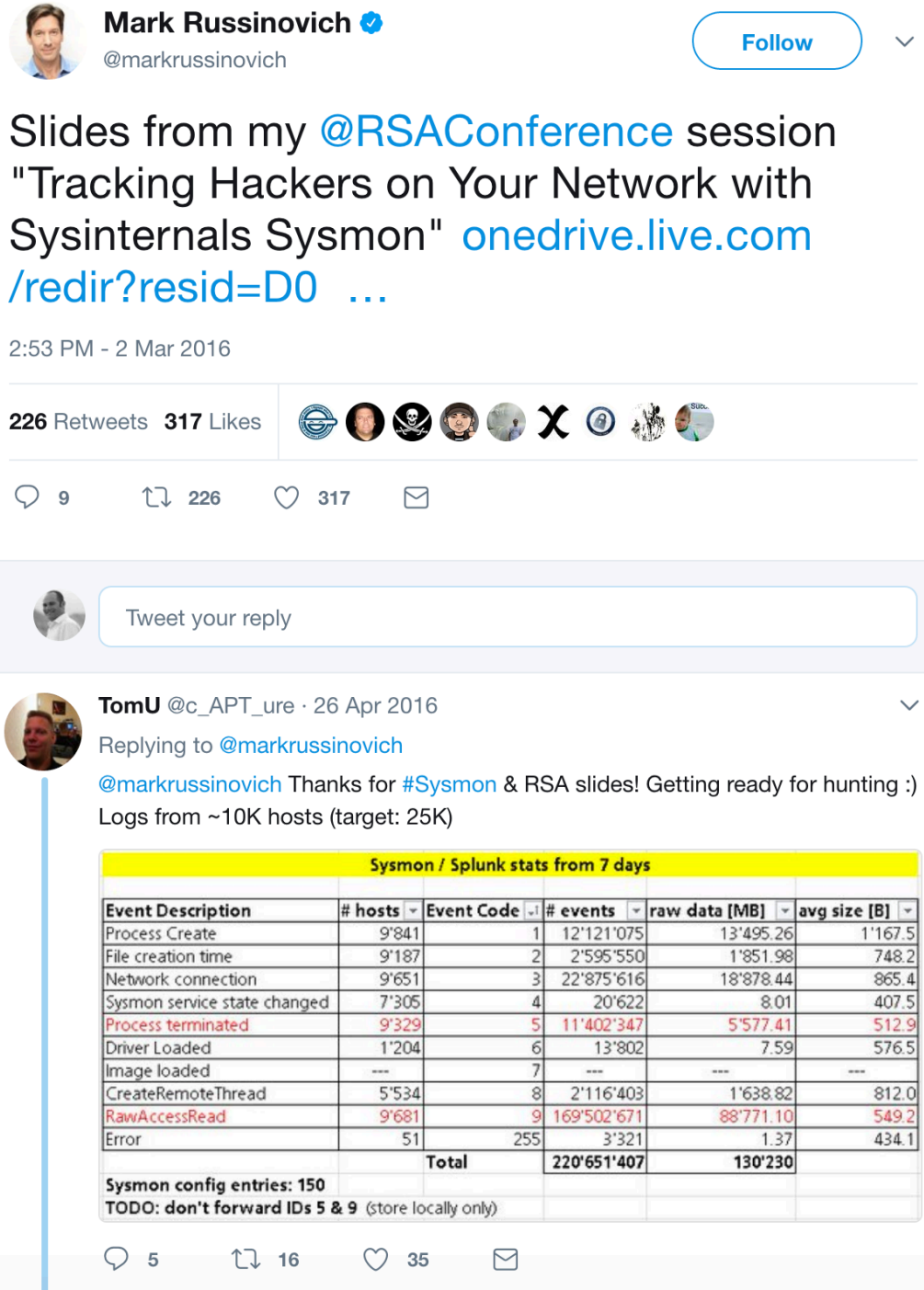
```
<!--SECTION: Splunk UF-->
<CommandLine condition="contains">splunk</CommandLine>
<CommandLine condition="contains">streamfwd</CommandLine>
<CommandLine condition="contains">splunkd</CommandLine>
<CommandLine condition="contains">splunkD</CommandLine>
<CommandLine condition="contains">splunk</CommandLine>
<CommandLine condition="contains">splunk-optimize</CommandLine>
<CommandLine condition="contains">splunk-MonitorNoHandle</CommandLine>
<CommandLine condition="contains">splunk-admon</CommandLine>
<CommandLine condition="contains">splunk-netmon</CommandLine>
<CommandLine condition="contains">splunk-regmon</CommandLine>
<CommandLine condition="contains">splunk-winprintmon</CommandLine>
<CommandLine condition="contains">btool</CommandLine>
<CommandLine condition="contains">SplunkUniversalForwarder</CommandLine>
```

Exclusions for EventCode 2

```
<FileCreateTime onmatch="exclude">
    <Image condition="image">OneDrive.exe</Image> <!--OneDrive constantly changes file times-->
    <Image condition="contains">setup</Image> <!--Ignore setups-->
    <Image condition="contains">splunk</Image>
    <Image condition="contains">streamfwd</Image>
    <Image condition="contains">splunkd</Image>
    <Image condition="contains">splunkD</Image>
    <Image condition="contains">splunk</Image>
    <Image condition="contains">splunk-optimize</Image>
    <Image condition="contains">splunk-MonitorNoHandle</Image>
    <Image condition="contains">splunk-admon</Image>
    <Image condition="contains">splunk-netmon</Image>
    <Image condition="contains">splunk-regmon</Image>
    <Image condition="contains">splunk-winprintmon</Image>
    <Image condition="contains">btool</Image>
</FileCreateTime>
```

Linked in the companion document


If you’re using a Sysmon configuration based on something other than TaySwifts…
…shake it off.
splunk>



Mark Russinovich
@markrussinovich

Follow

Slides from my @RSAConference session "Tracking Hackers on Your Network with Sysinternals Sysmon" onedrive.live.com/redir?resid=D0 …

2:53 PM - 2 Mar 2016

226 Retweets 317 Likes

9 226 317

Tweet your reply

TomU @c_APT_ure · 26 Apr 2016

Replying to @markrussinovich

@markrussinovich Thanks for #Sysmon & RSA slides! Getting ready for hunting :)
Logs from ~10K hosts (target: 25K)

Sysmon / Splunk stats from 7 days					
Event Description	# hosts	Event Code	# events	raw data [MB]	avg size [B]
Process Create	9'841	1	12'121'075	13'495.26	1'167.5
File creation time	9'187	2	2'595'550	1'851.98	748.2
Network connection	9'651	3	22'875'616	18'878.44	865.4
Sysmon service state changed	7'305	4	20'622	8.01	407.5
Process terminated	9'329	5	11'402'347	5'577.41	512.9
Driver Loaded	1'204	6	13'802	7.59	576.5
Image loaded	---	7	---	---	---
CreateRemoteThread	5'534	8	2'116'403	1'638.82	812.0
RawAccessRead	9'681	9	169'502'671	88'771.10	549.2
Error	51	255	3'321	1.37	434.1
		Total	220'651'407	130'230	
Sysmon config entries: 150					
TODO: don't forward IDs 5 & 9 (store locally only)					

5 16 35

10,000 hosts, 7 days, ~130GB.

~19GB a day.

Or, about 2MB per endpoint, per day.

(Your Mileage May Vary.)

splunk> .conf2017

Yesterday, This Happened.

You should check out this talk from 9/27. Seriously.

Effectively Enhancing our SOC with Sysmon, PowerShell Logging and Machine Learning to Detect and Respond to Today's Threats

Wednesday, September 27, 2017 | 2:15 PM-3:00 PM ADVANCED

Kent Farries, Sr. Systems Analyst, Security Intelligence & Analytics, TransAlta Corporation

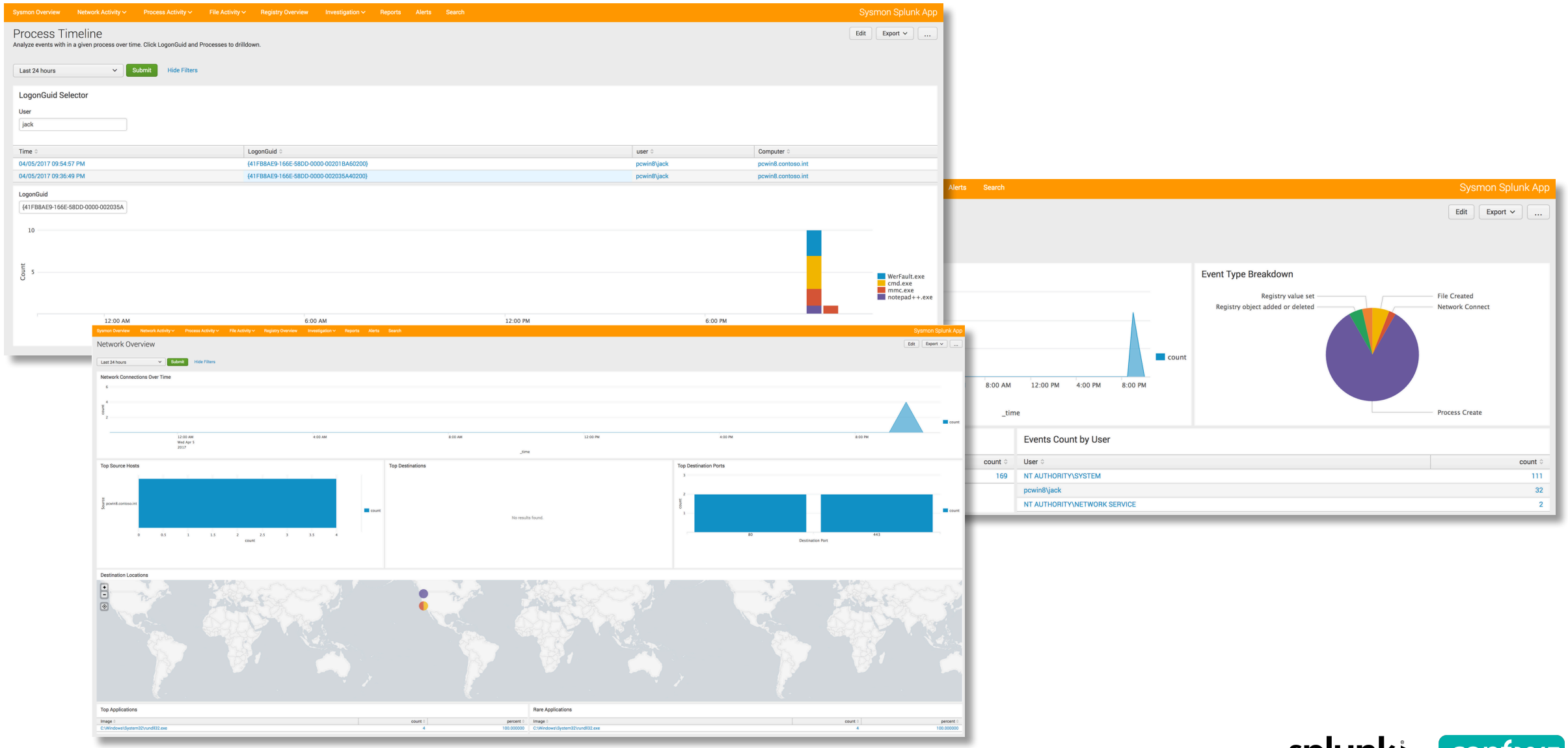
Ikenna Nwafor, Sr Systems Analyst, Security Design, TransAlta

With today's threats, TransAlta needed to improve its managed SOC with the goal of becoming a "pretty good SOC" in 2017. We had to look at how we are doing things today, what we should stop doing or automate and what we should be doing tomorrow. We decided that we needed to get better at hunting with limited resources, so we chose to leverage Sysmon, PowerShell logging and machine learning. This session will showcase how we used Splunk to efficiently collect and analyze the logs from thousands of endpoints to understand our security posture. We will also provide some insight from our lessons learned around deployment, tuning and capacity planning.

~1700 endpoints, ~10MB Per, Sysmon and Windows Events!

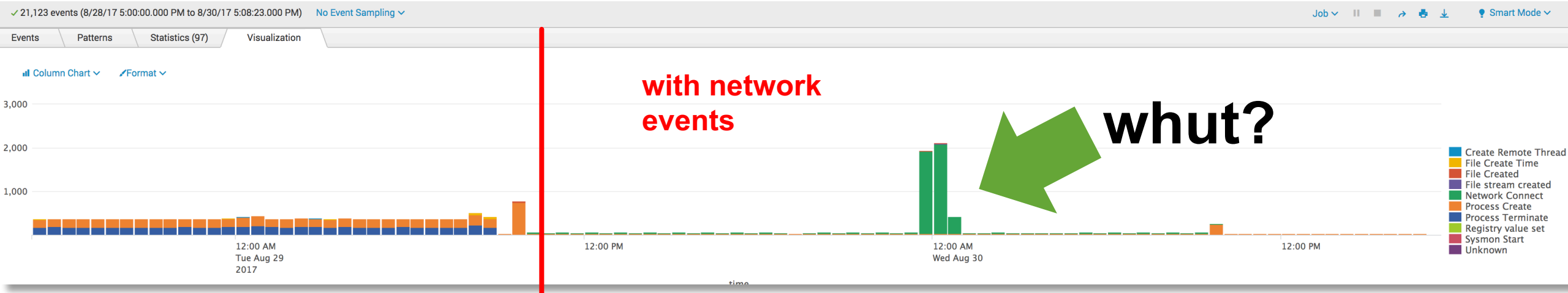
splunk> .conf2017

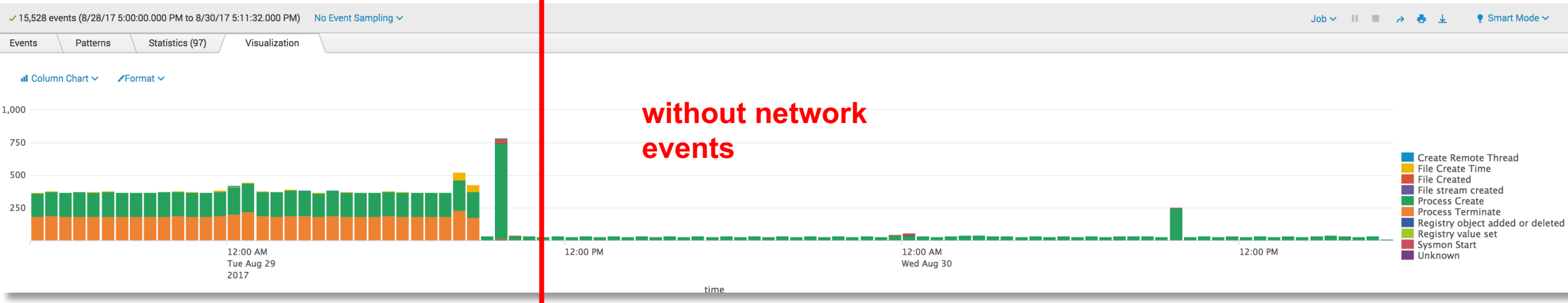
A cool community Sysmon app by HAGGIS!



splunk> .conf2017

Tayswift Config in Action

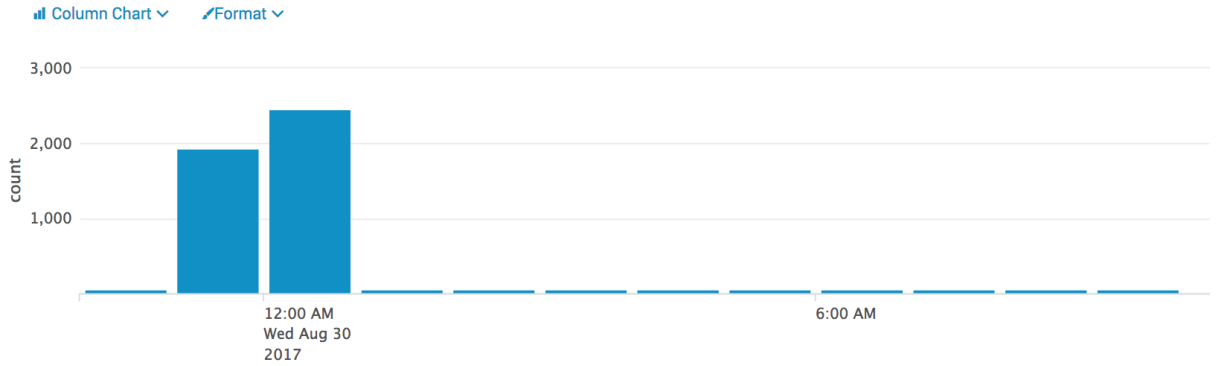


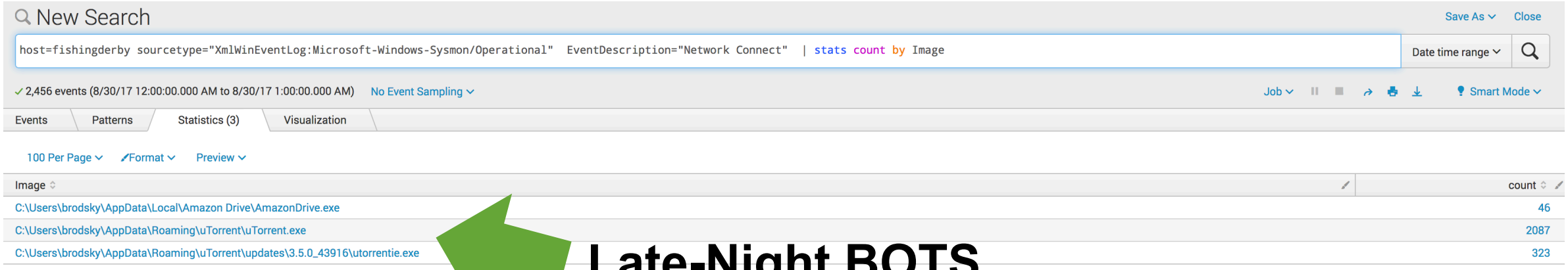


splunk> .conf2017

```
<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED-->
    <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv6, SourceIp, SourceHostname, SourcePort, SourcePortN
    <NetworkConnect onmatch="include">
    <!--COMMENT:    Takes a very conservative approach to network logging, limit to extremely high-signal events.-->
    <!--TECHNICAL:  For the DestinationHostname, Sysmon uses the GetNameInfo API, which may not always have the information or may be a CDN. Usi
    <!--TECHNICAL:  These exe's do not initiate their connections, and cannot be included: BITSADMIN-->
        <!--Suspicious sources-->
        <Image condition="begin with">C:\Users</Image> <!--Tools downloaded by users can use other processes for networking, but this is a v
        <Image condition="begin with">C:\ProgramData</Image> <!--Normally, network communications should be sourced from "Program Files" not
        <Image condition="begin with">C:\Windows\Temp</Image> <!--Suspicious anything would communicate from the system-level temp directory
```

Clever network filtering ***(the config is chock full of stuff like this)***

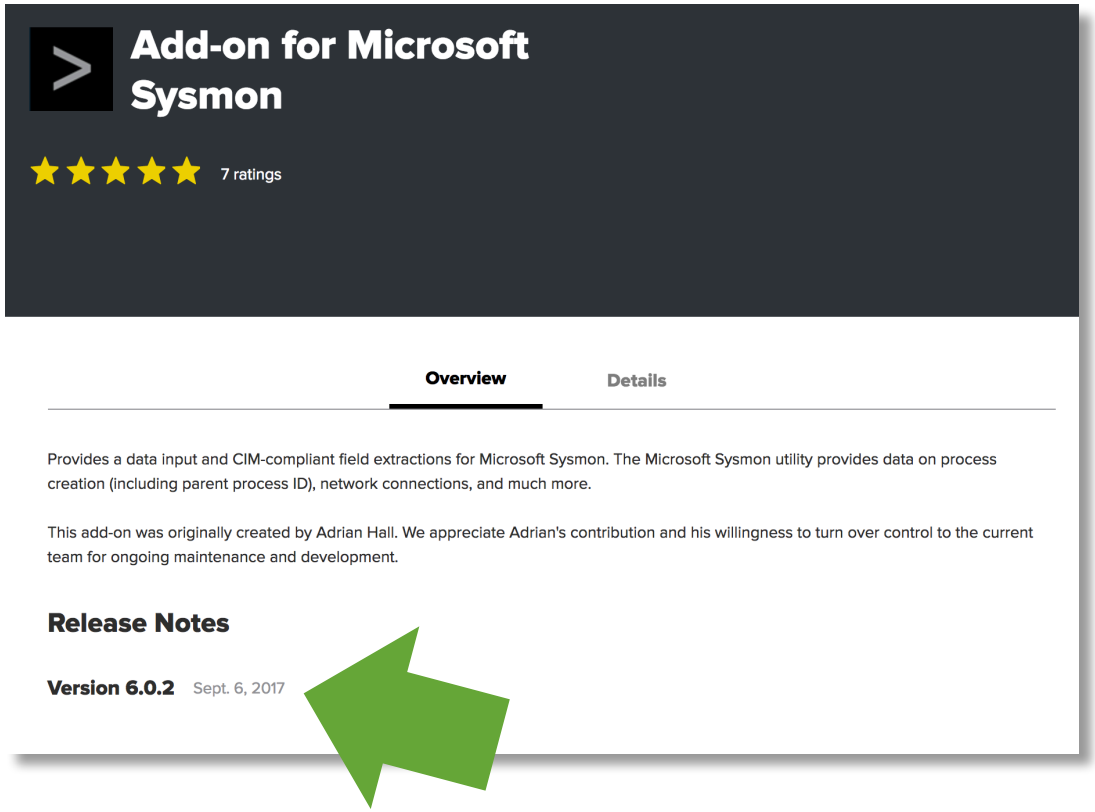




Late-Night BOTS scenario testing!

splunk> .conf2017

Recently Updated Splunkbase Sysmon TA. Why?



Additional Field Extractions

```
...  @@ -1,6 +1,6 @@
1    [XmlWinEventLog:Microsoft-Windows-Sysmon/Operational]
2    #SEDCMD-pwd_rule1 = s/ -pw ([^\s\<])+/ -pw ***MASK***/g
3  -REPORT-sysmon = sysmon-eventid,sysmon-version,sysmon-level,sysmon-task,sysmon-opcode,sysmon-keywords,sysmon-created,sysmon-record,sysmon-correlation,sysmon-channel,sysmon-computer,sysmon-sid,sysmon-data,sysmon-md5,sysmon-sha1,sysmon-sha256,sysmon-imphash
4    EVAL-src_ip = SourceIp
5    EVAL-src_host = SourceHostname
6    EVAL-src = if(isnotnull(SourceHostname),SourceHostname,SourceIp)
     @@ -21,6 +21,9 @@ EVAL-process_id = ProcessId
21   EVAL-user = User
22   EVAL-vendor_product = "Microsoft Sysmon"
23   EVAL-process = case(EventCode=="1" OR EventCode=="2" OR EventCode=="3" OR EventCode=="5" OR EventCode=="7" OR EventCode=="9" OR EventCode=="11" OR EventCode=="12" OR EventCode=="13" OR EventCode=="14" OR EventCode=="15" OR EventCode=="17" OR EventCode=="18", replace(Image,"(.*\\\)(?=.*(\.\w*)$|(\w+)$)",""),EventCode=="6","System",EventCode=="8" OR EventCode=="10",replace(SourceImage,"(.*\\\)(?=.*(\.\w*)$|(\w+)$)",""),1==1,"")
24   LOOKUP-eventcode = eventcode EventCode OUTPUTNEW EventDescription EventDescription AS signature
25   FIELDALIAS-signature_id = EventCode AS signature_id
26

1    [XmlWinEventLog:Microsoft-Windows-Sysmon/Operational]
2    #SEDCMD-pwd_rule1 = s/ -pw ([^\s\<])+/ -pw ***MASK***/g
3  +REPORT-sysmon = sysmon-eventid,sysmon-version,sysmon-level,sysmon-task,sysmon-opcode,sysmon-keywords,sysmon-created,sysmon-record,sysmon-correlation,sysmon-channel,sysmon-computer,sysmon-sid,sysmon-data,sysmon-md5,sysmon-sha1,sysmon-sha256,sysmon-imphash,sysmon-hashes
4    EVAL-src_ip = SourceIp
5    EVAL-src_host = SourceHostname
6    EVAL-src = if(isnotnull(SourceHostname),SourceHostname,SourceIp)
21   EVAL-user = User
22   EVAL-vendor_product = "Microsoft Sysmon"
23   EVAL-process = case(EventCode=="1" OR EventCode=="2" OR EventCode=="3" OR EventCode=="5" OR EventCode=="7" OR EventCode=="9" OR EventCode=="11" OR EventCode=="12" OR EventCode=="13" OR EventCode=="14" OR EventCode=="15" OR EventCode=="17" OR EventCode=="18", replace(Image,"(.*\\\)(?=.*(\.\w*)$|(\w+)$)",""),EventCode=="6","System",EventCode=="8" OR EventCode=="10",replace(SourceImage,"(.*\\\)(?=.*(\.\w*)$|(\w+)$)",""),1==1,"")
24   +EVAL-cmdline = CommandLine
25   +EVAL-parent_process_id = ParentProcessId
26   +EVAL-parent_process = ParentProcess
27   LOOKUP-eventcode = eventcode EventCode OUTPUTNE[illegible]n EventDescription AS signature
28   FIELDALIAS-signature_id = EventCode AS signature_[illegible]
29
```

better extractions for hashes, commandline data

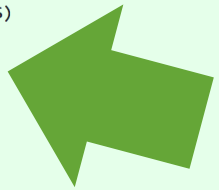
splunk> .conf2017

Better support for Change Analysis DM

8 default/transforms.conf — View

```
@@ -72,6 +72,14 @@ REGEX = (?<hashes>[A-Fa-f0-9]{32,})
 MV_ADD = true
 REPEAT_MATCH=true

+[sysmon-filename]
+SOURCE_KEY = TargetFilename
+REGEX = (?<file_name>[^\\\\]+$)
+
+[sysmon-registry]
+SOURCE_KEY = TargetObject
+REGEX = (?<object>[^\\\\]+$)
+
 [eventcode]
 default_match = Unknown
 filename = eventcode.csv
```



Filesystem_Changes	`file_name`	string	The name of the file that is the object of the event (without location information related to local file or directory structure).

			`dvc_host`, `dvc_ip`, or `dvc_name`.
All_Changes	`object`	string	Name of the affected object on the resource (such as a router interface, user account, or server volume).
All_Changes	`object_attrs`	string	The attributes that were updated on the updated

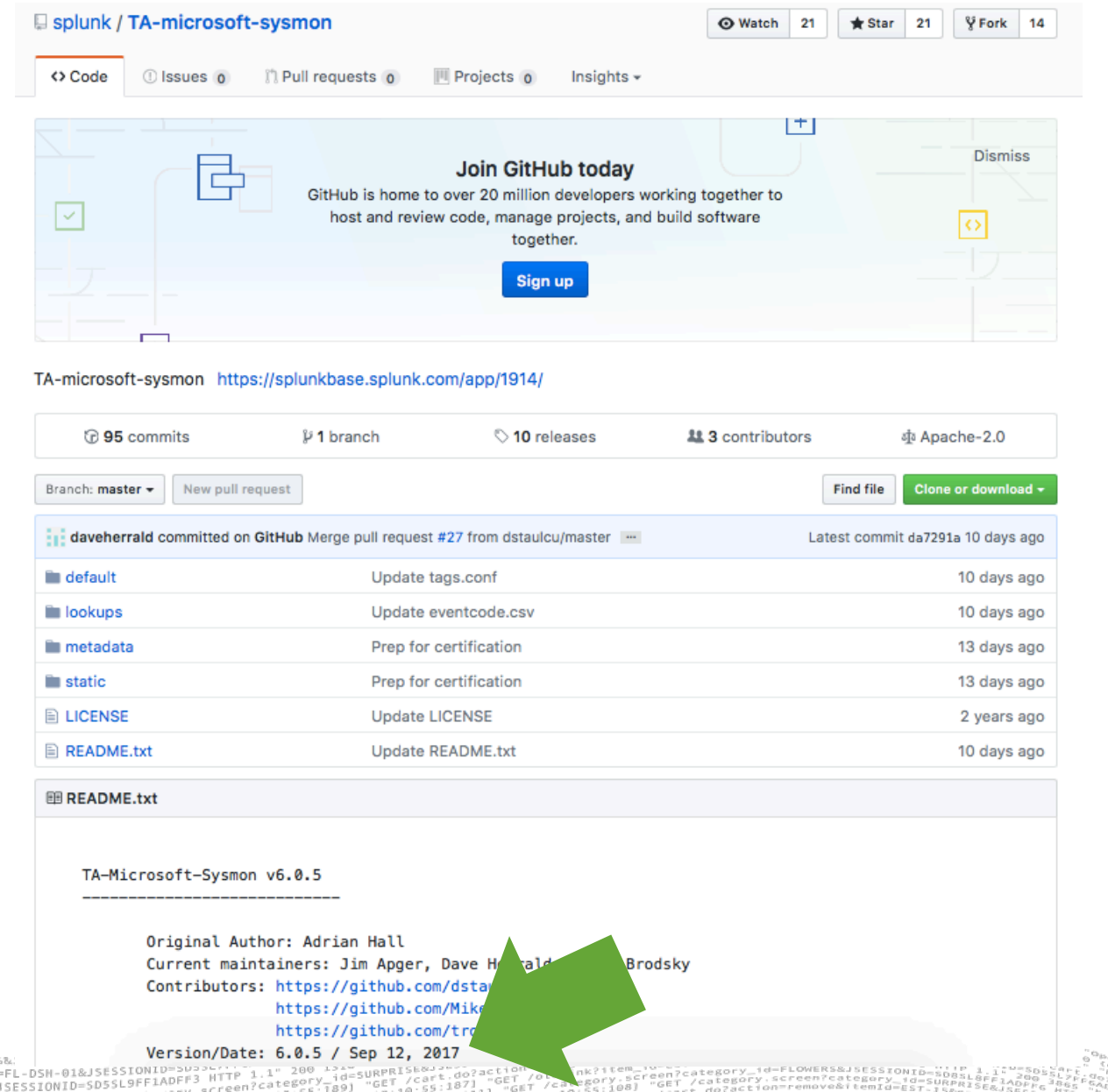
splunk> .conf2017

It’s still not perfect.

We need a real, standard Common Information Model for endpoint process data.

There is progress being made. Thank you, Security Research team.

Recently Updated Github Version of Sysmon TA



splunk> .conf2017

Update: Many Other New Things

In looking into compromised systems, often what is needed by incident responders and investigators is not enabled or configured when it comes to logging. To help get system logs properly Enabled and Configured, below are some cheat sheets to help you do logging well and so the needed data we all need is there when we look.

Cheat Sheets to help you in configuring your systems:

- **The Windows Logging Cheat Sheet** Updated Oct 2016
- **The Windows Splunk Logging Cheat Sheet** Updated Mar 2017
- **The Windows File Auditing Logging Cheat Sheet** Updated Oct 2016
- **The Windows Registry Auditing Logging Cheat Sheet** Updated Oct 2016
- **The Windows PowerShell Logging Cheat Sheet** Updated July 2016
- The Windows Sysmon Logging Cheat Sheet Coming soon

Michael Gough's Excellent Windows logging content.

All updated.

splunk> .conf2017

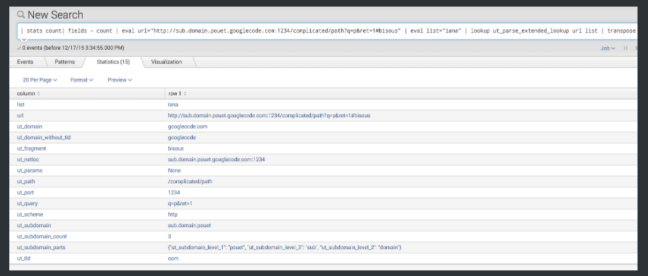
splunkbase

Search App by keyword, technology...

My Account | Support & Services

URL Toolbox

6 ratings



Overview | Details

UTBox is a set of building blocks for Splunk specially created for URL manipulation.

UTBox has been created to be modular, easy to use and easy to deploy in any Splunk environments. It only needs to be deployed on Splunk Search Heads and the bundles will automatically be sent to your Splunk Indexers.

One of the core feature of UTBox is to correctly parse URLs and complicated TLDs (Top Level Domain) using the Mozilla Suffix List. Other functions like shannon entropy, counting, suites, meaning ratio, bayesian analysis, etc, are also available.

UTBox has firstly be created for security analysts but may fit other needs as it's a set of building blocks. Enterprise Security users will need to modify the import statement to use UTBox.

You should also take a look at URLParser for efficient URL parsing: https://splunkbase.splunk.com/app/3396/

Release Notes

Version 1.6 April 18, 2016

Community Supported App

755 Installs

3,061 Downloads

LOGIN TO DOWNLOAD

VERSION
1.6

BUILT BY
Cedric Le Roux

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance, Utilities
App Type: App

COMPATIBILITY
Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, 6.0, 5.0
Platform: Platform Independent

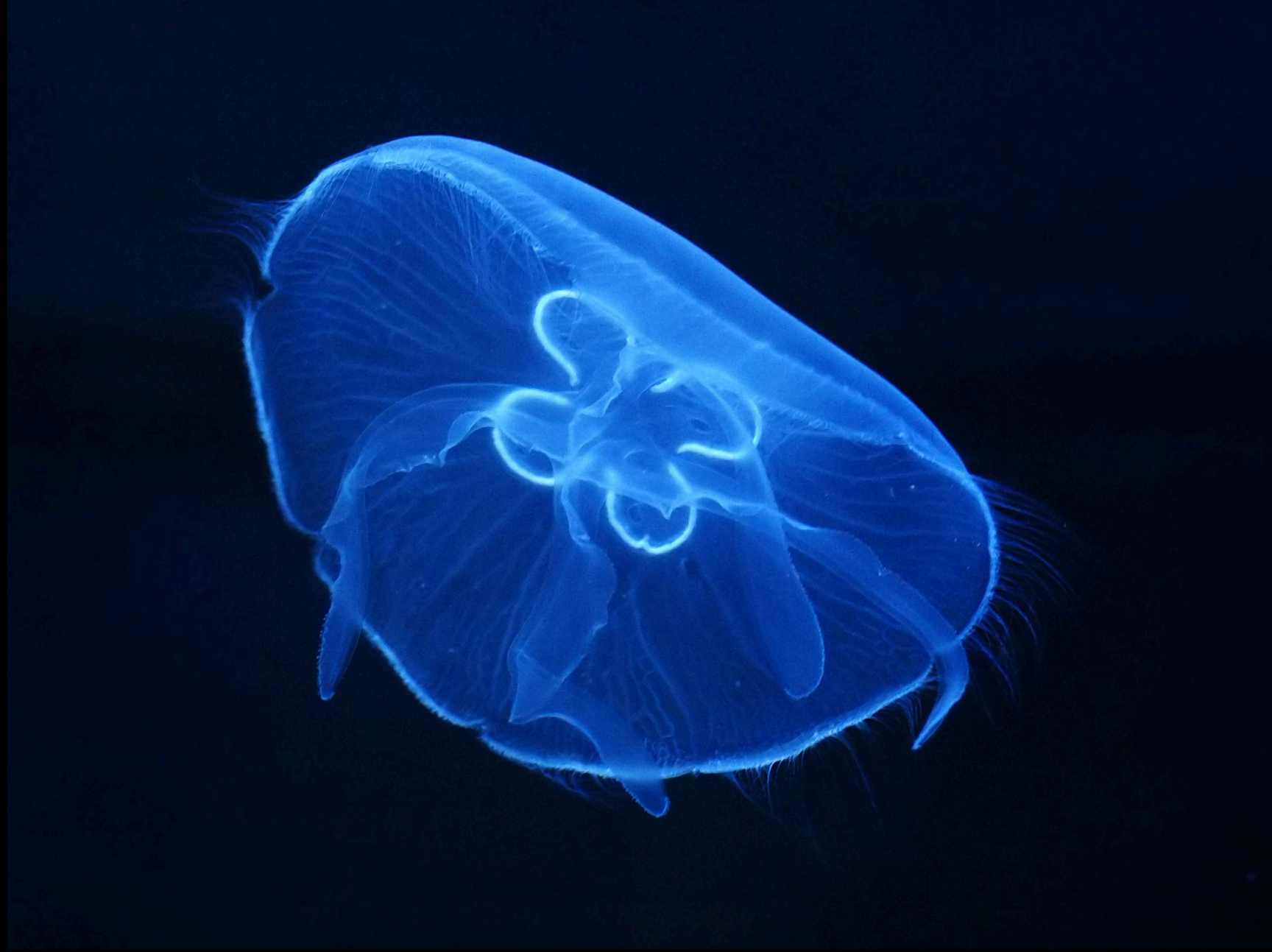
Our old friend, URL Toolbox…

Great for URL manipulation and string analysis!

splunk> .conf2017

…has a new friend, “JellyFisher.”

Also written by Cedric Le Roux



splunk> .conf2017

splunkbase™ Search App by keyword, technology... My Account Support & Services

JellyFisher

★★★★★ 1 rating

Overview Details

JellyFisher is a Splunk custom search command that leverage the excellent jellyfish python's library to do approximate and phonetic strings matching.

String comparison algorithms:
- Levenshtein Distance
- Damerau-Levenshtein Distance
- Jaro Distance
- Jaro-Winkler Distance
- Match Rating Approach Comparison
- Hamming Distance

Phonetic encoding algortihms:
- American Soundex
- Metaphone
- NYSIIS (New York State Identification and Intelligence System)
- Match Rating Codex

Example:
- The Levenshtein distance between "kitten" and "sitting" is 3.
- The soundex representation of both "Robert" and "Rupert" is "R163"

Release Notes

Version 0.1.0 June 21, 2017

15 Installs 32 Downloads

LOGIN TO DOWNLOAD

VERSION 0.1.0

BUILT BY Cedric Le Roux

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance, Utilities
App Type: App

COMPATIBILITY
Products: Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4
Platform: Platform Independent

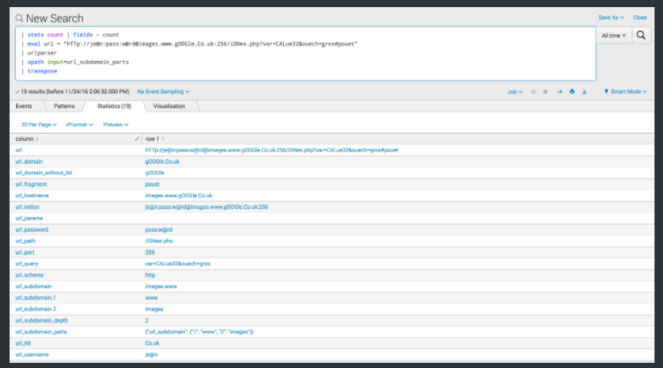
LICENSING
End User License Agreement for Third-Party Content

Leverages Python “jellyfish” Library for approximate and phonetic string matches

splunk> .conf2017

URLParser

★★★★★ 1 rating



Overview | **Details**

URLParser

URLParser is a custom search command designed to parse URLs. Because it relies on the new chuncked protocol, URLParser is compatible starting with Splunk 6.4.0 and above.

```
... | urlparser [field=fieldname] [listname="*|iana|mozilla|..."] [mode=[simple|extended]]
```

URLParser is a community supported app and compared to UTBox, URLParser is faster, extract more fields and is easier to use.

Extracted fields

URLParser will extract the following fields form the submitted URLs:

- url_domain
- url_domain_without_tld
- url_fragment
- url_hostname
- url_netloc
- url_params
- url_password
- url_path
- url_port

81 Installs

310 Downloads

LOGIN TO DOWNLOAD

VERSION
1.0.0

BUILT BY
Cedric Le Roux

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance, Utilities
App Type: App

COMPATIBILITY
Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4
Platform: Platform Independent

URLParser:

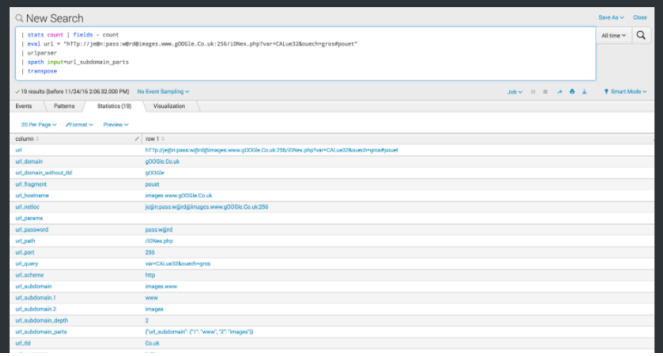
URL/domain manipulation portions of URL Toolbox in "turbo mode"

No stats analysis.

splunk> .conf2017

URLParser

★★★★★ 1 rating



URLParser:

URL/domain

3x-4x faster…

```
search url!=- url=* | head 200000 | urlparser listname="mozilla|iana"

This search has completed and has returned 5,123 results by scanning 204,129 events in 26.91 seconds
```

As a reference point for comparaison, here are the results with UTBox:

```
search url!=- url=* | head 200000 | eval list="*" | lookup ut_parse_extended_lookup url list

This search has completed and has returned 5,123 results by scanning 204,129 events in 83.123 seconds
```

Extracted fields

URLParser will extract the following fields form the submitted URLs:

- url_domain
- url_domain_without_tld
- url_fragment
- url_hostname
- url_netloc
- url_params
- url_password
- url_path
- url_port

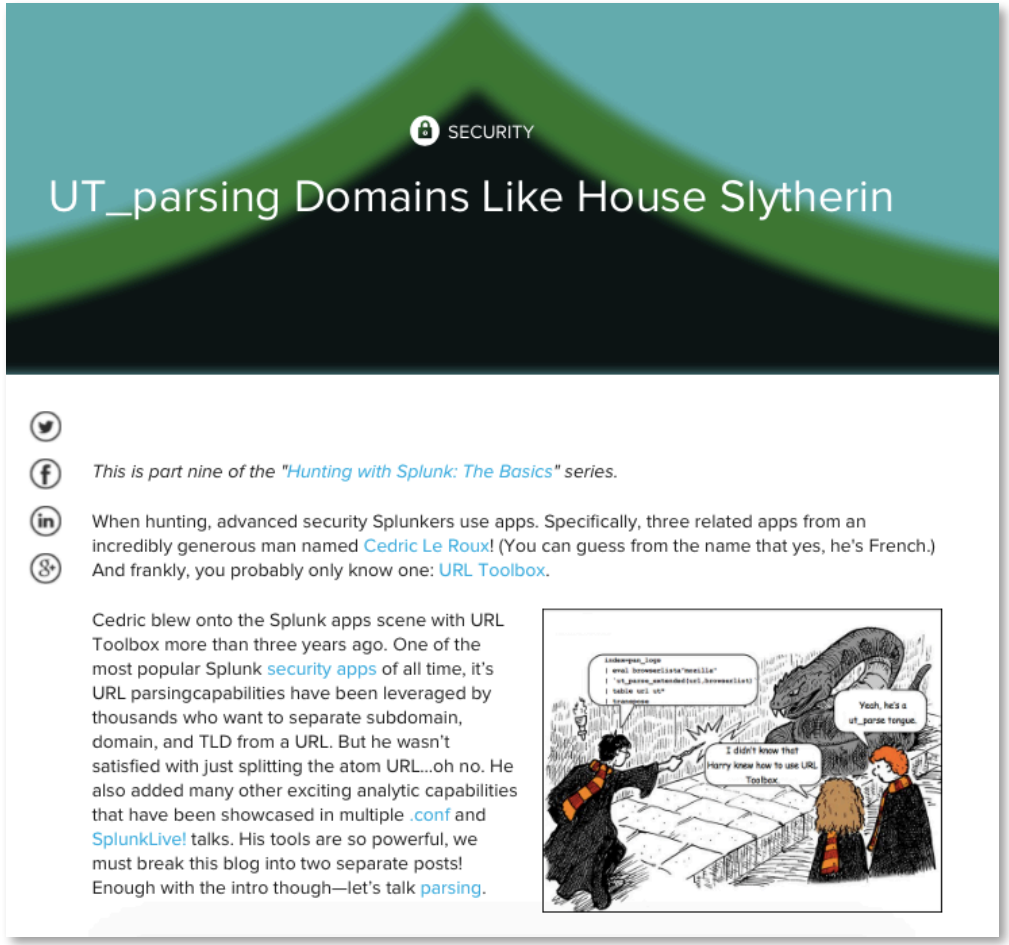
BUILT BY
Cedric Le Roux

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance, Utilities
App Type: App

COMPATIBILITY
Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 6.6, 6.5, 6.4
Platform: Platform Independent

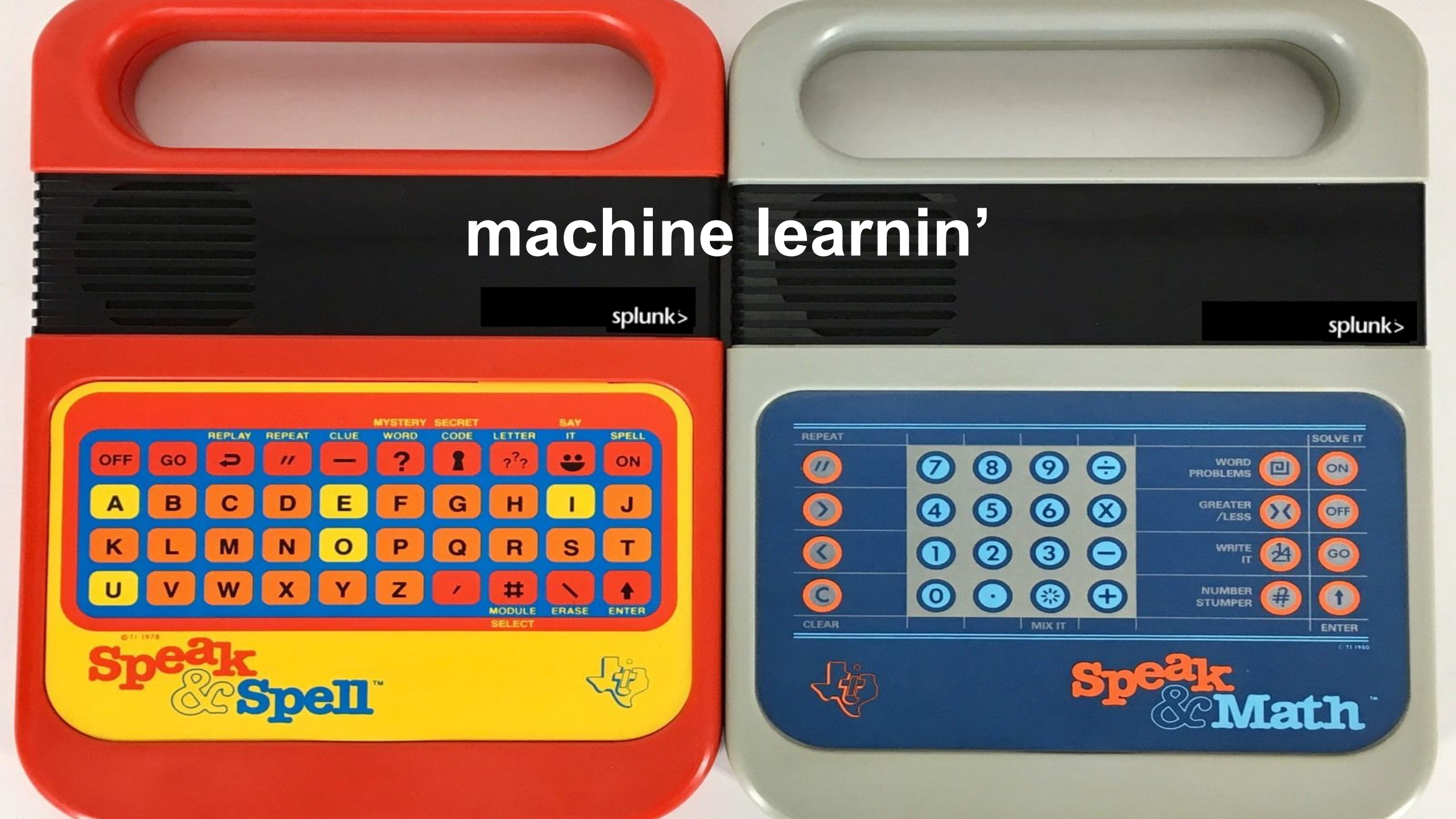
splunk> .conf2017

David Veuve is My SPL Patronus



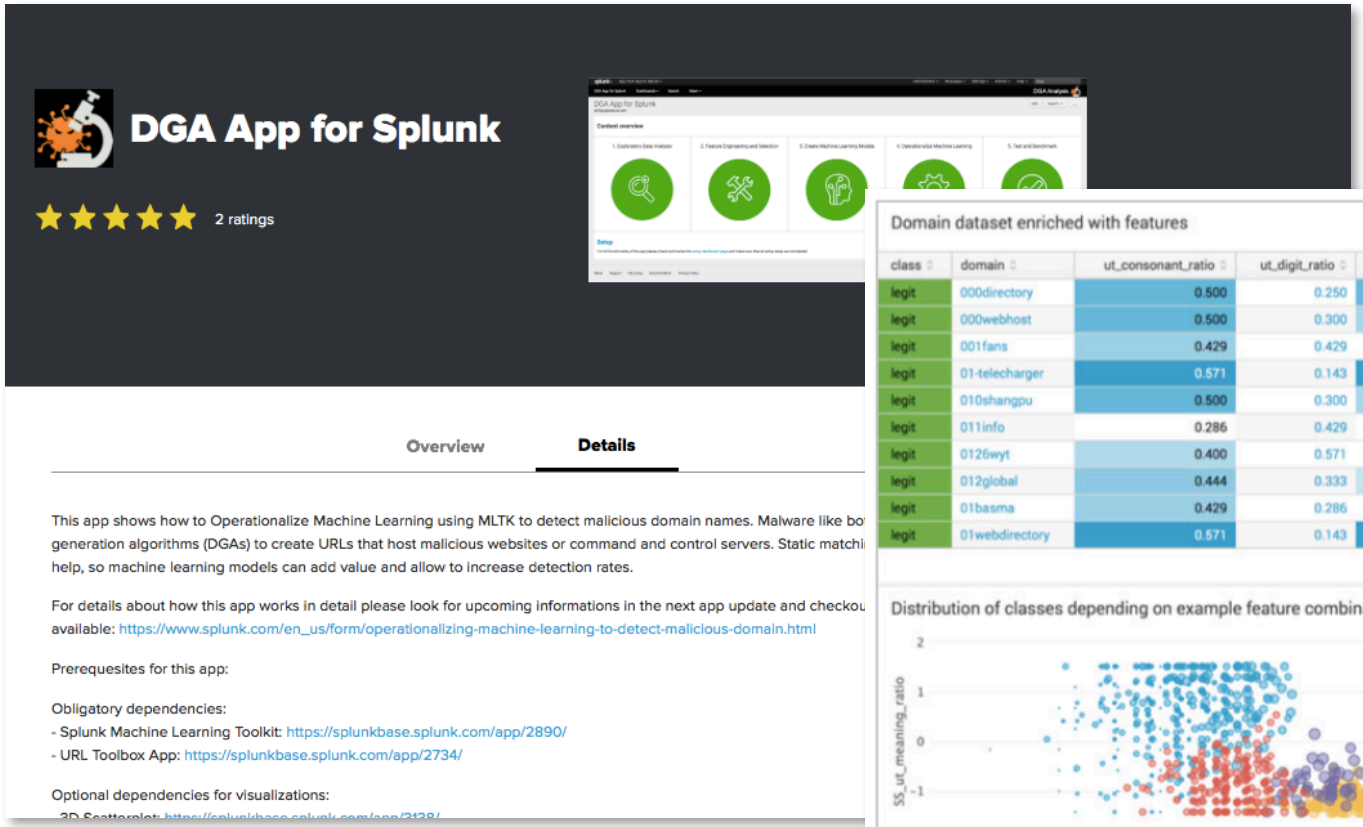
…and he will be yours too after you review his stuff.

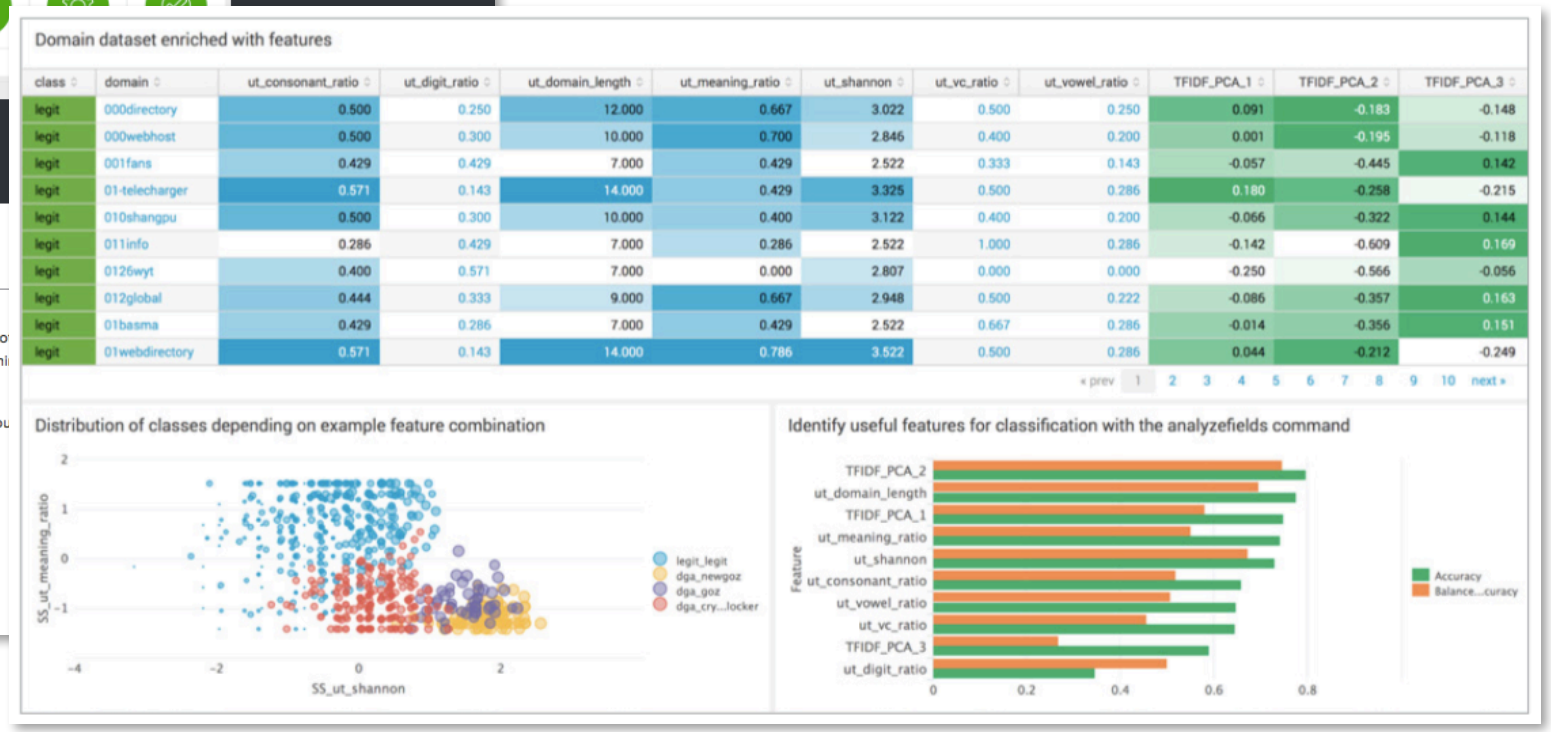
splunk> .conf2017


machine learnin’
splunk>
splunk>
MYSTERY SECRET SAY
REPLAY REPEAT CLUE WORD CODE LETTER IT SPELL
OFF GO ON
A B C D E F G H I J
K L M N O P Q R S T
U V W X Y Z
MODULE ERASE ENTER
SELECT
Speak & Spell™
REPEAT
SOLVE IT
WORD PROBLEMS
GREATER /LESS
WRITE IT
NUMBER STUMPER
ON
OFF
GO
CLEAR
MIX IT
ENTER
Speak & Math™

Practical Endpoint ML Example #1

DGA Analysis using MLTK – released this week!





splunk> .conf2017

“Collect all my DNS (or Netflow) data? Nope. Splunk is too expensive.”

splunk> .conf2017

Not anymore.

New Pricing for DNS or Netflow data is 33% of what you will pay for a normal Enterprise Term license.

- **500GB minimum**
- **Term, not permanent**
- **License tied to those two sourcetypes**
- **Call your Splunk account team**

splunk> .conf2017

Practical Endpoint ML Example #2

Windows Process Name Analysis in MLTK – from Tuesday!

Everyone Can Build a Security App!

Tuesday, September 26, 2017 | 12:05 PM-12:50 PM
Tuesday, September 26, 2017 | 1:10 PM-1:55 PM GOOD FOR ALL SKILL LEVELS

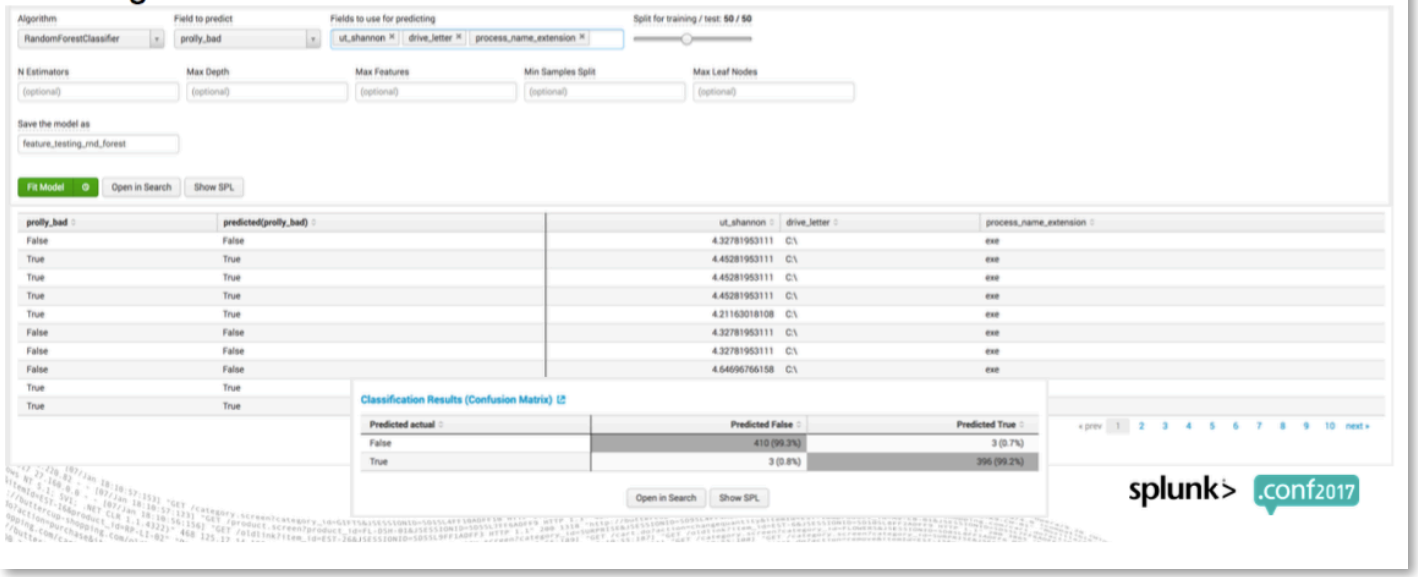
Young Cho, Technical Marketing Manager, Security, Splunk
Jae Lee, Product Marketing Director, Splunk
Anthony Tellez, Lead, Business Analytics & IoT, Splunk

Attend this guided, hands-on session to learn security best practices related to building a Splunk App – specifically, key aspects of operationalizing security searches, visualizations and workflow. We'll cover a range of topics, including: - Overall methodology: when and how building an app can help with security challenges and how to design an app to extract key insights from common data sources. - Foundational concepts: TA application, data validation, CIM, summarization, data enrichment, analysis techniques, visualizations, rules definition and more. - More advanced: including modeling, applying data science techniques, forming hypotheses and process considerations. You'll learn first-hand by iteratively developing an app that you can then take home and continue to use as a learning or testing tool. Alternatively, you can customize and/or deploy or even rebuild it using your security or compliance framework of choice. The app includes the security-rich dataset used in last year's (.conf2016's) Boss of the SOC competition. You can get great, useful info and techniques from this session regardless of your skill level with Splunk or whether your current primary use case is security, IT operations or something else. Laptops are required to participate.

Improve Searches

Use the Machine Learning Toolkit, External Apps

- An option for improving the searches is utilizing the machine learning toolkit to engineer features to detect similar behavior.



https://splunk.box.com/v/Buildingasecurityapp

splunk> .conf2017

Exercise 1: Sysmon in BOTS - APT and Ransomware Scenarios

SPLUNKER THINGS

roll d20 to determine your server!

left side of room="a"

right side of room="b"

prepend with "0" if single digit

alice/epsecurity

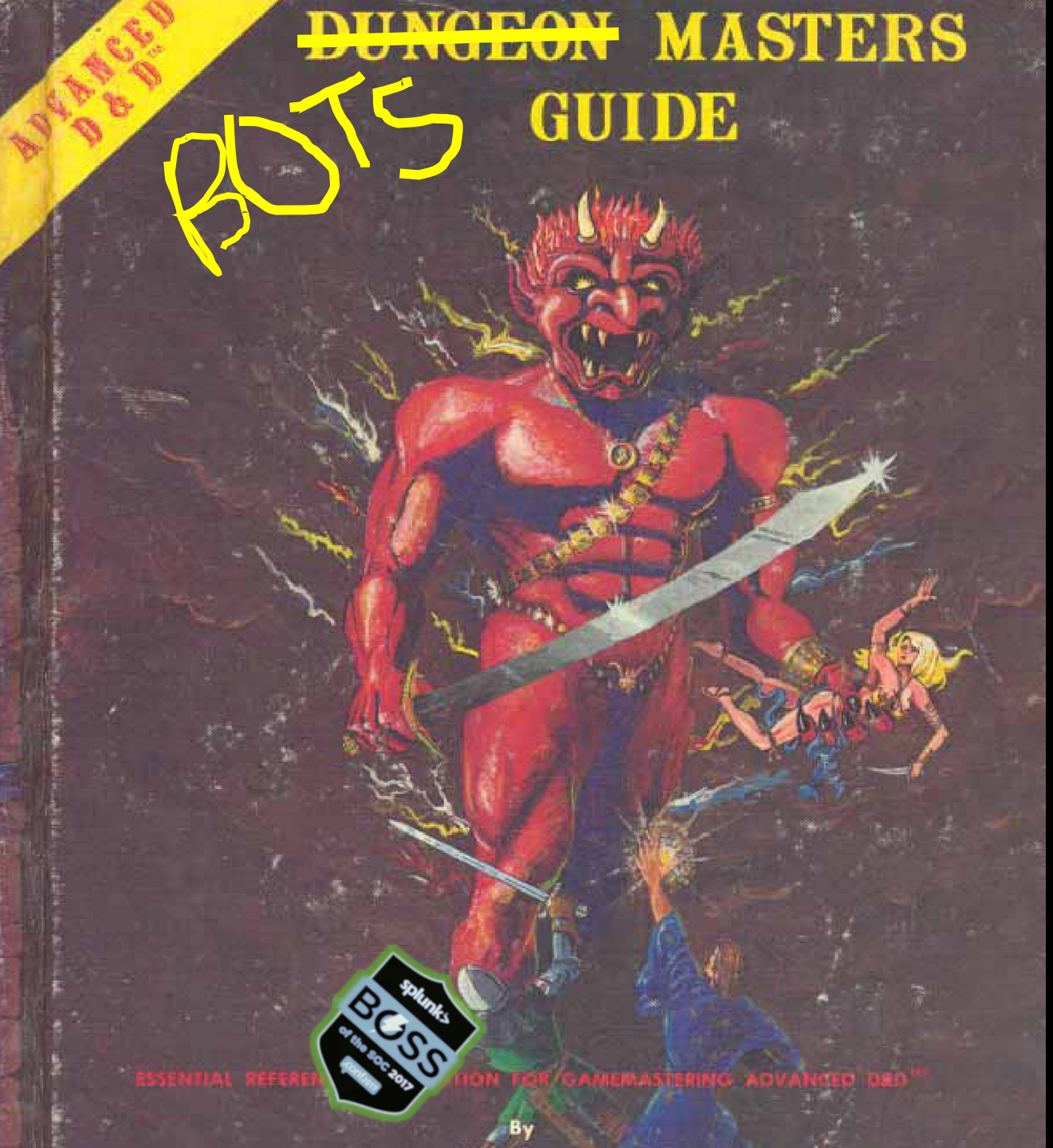
= https://conf17-bots-endpoint-14a.splunkoxygen.com

or

= https://conf17-bots-endpoint-14b.splunkoxygen.com

Depending on what side of the room you are on.

splunk> .conf2017



Get ready to ~~cheat~~ learn.

splunk> BOSS of the SOC 2017 .conf2017

splunk> .conf2017

Did you play?

Let's recap the first scenario…

Theme: How to go from finding an unusual process executing on an endpoint to full-blown exfiltration of corporate secrets via DNS in 12 easy searches.

splunk> .conf2017

About this dataset...

splunk> .conf2017

How to go from finding an unusual process executing on an endpoint to full-blown exfiltration of corporate secrets via DNS in 12 easy searches.

Please log into your Splunk systems.

splunk> .conf2017

Something like this

```
index=bots-apt sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1| eval allcommand=CommandLine+":"+ParentCommandLine | eval set="@base64@" | `ut_countset(_raw,set)` | spath input=ut_countset | rename ut_countset.sum AS base64charcount| dedup allcommand | eval totallen=len(_raw)| eval commandlen=len(allcommand)| eval ratio = base64charcount/totallen| stats values(allcommand) by ratio,totallen,base64charcount,commandlen| where ratio>.90| sort -ratio
```

Additional .conf2017 Content Worth Looking At!

Review these talks when you are able

Security Ninjutsu Part Four: Attackers Be Gone in 45 Minutes of Epic SPL

Wednesday, September 27, 2017 | 2:15 PM-3:00 PM GOOD FOR ALL SKILL LEVELS

David Veuve, Principal Security Strategist, Splunk Inc.

My favorite part of any spy movie is the gadgets. You see a spy in normal attire, without knowing that the jacket is bulletproof and the watch shoots amnesia darts. That spy i...

More

Quickly Advance Your Security Posture With Splunk Security Essentials

Tuesday, September 26, 2017 | 1:10 PM-1:55 PM GOOD FOR ALL SKILL LEVELS

David Veuve, Principal Security Strategist, Splunk Inc.

Whether you're looking to reduce breaches, set up monitoring to anticipate attacks, or build more predictive capabilities, you will learn to apply the power of Splunk's search...

More

Searching FAST: How to Start Using tstats and Other Acceleration Techniques

Wednesday, September 27, 2017 | 12:05 PM-12:50 PM INTERMEDIATE

David Veuve, Principal Security Strategist, Splunk Inc.

You know the use cases, you understand stats. You might strut through the halls of .conf events as an advanced SPLer. But you've heard a whisper on the wind, a next-level appr...

More

Hunting the Known Unknowns: Finding Evil With SSL Traffic

Tuesday, September 26, 2017 | 12:05 PM-12:50 PM ADVANCED

Steve Brant, Senior Security Strategist, Splunk Inc.
Ryan Kovar, Staff Security Strategist, Splunk Inc.

This year's "Hunting" session will describe how to find malicious adversaries using SSL. The talk will cover new ways to log SSL/TLS certificates and how to find malware in yo...

More

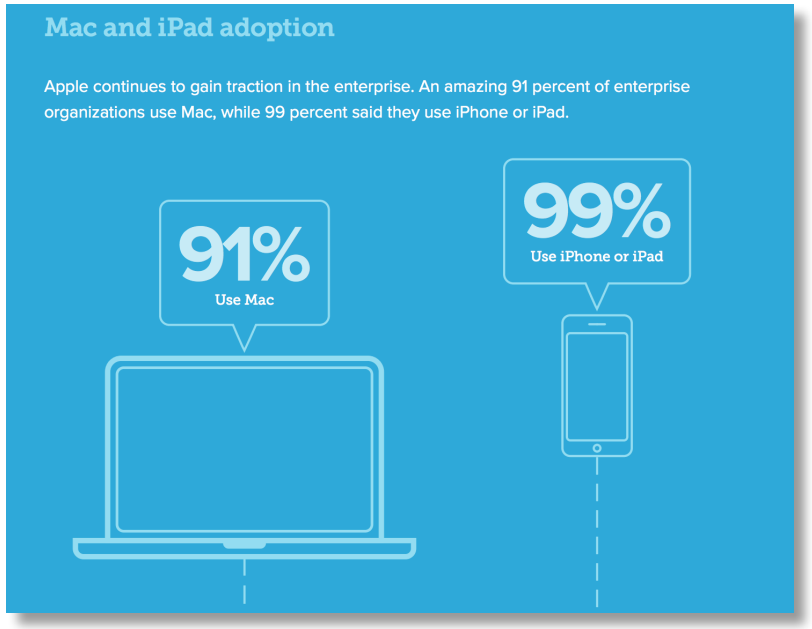
splunk> .conf2017

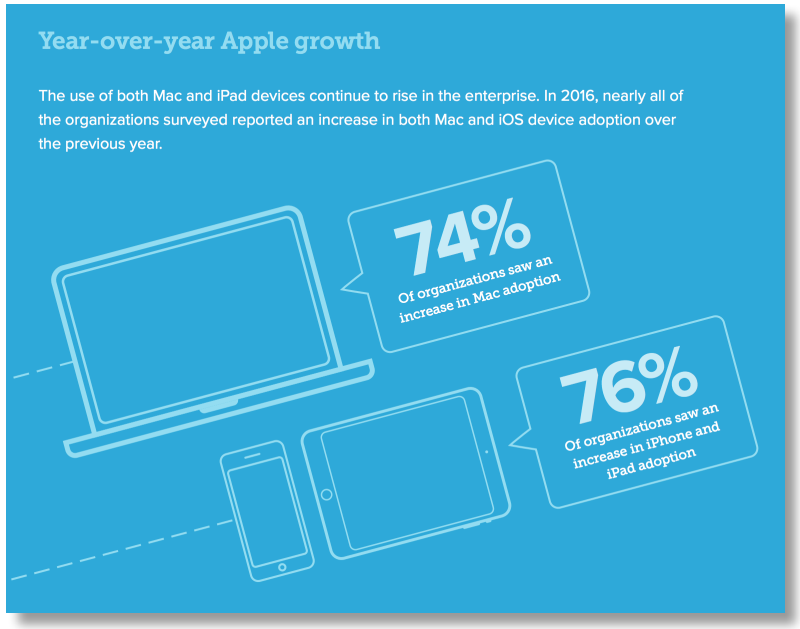
Not Everyone Runs Windows

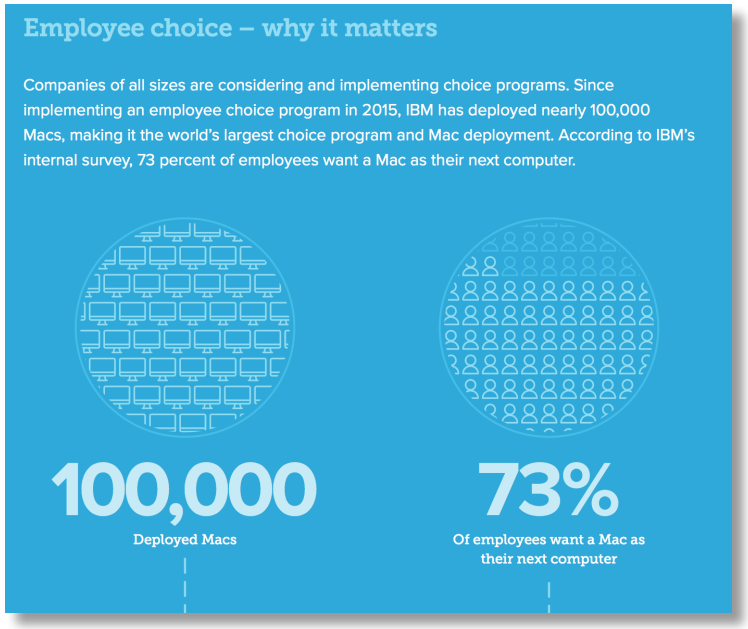
splunk> .conf2017


Browsing Yelp reviews of all avocado toast food trucks within 500 yards.
NOT worried about malware, amirite?

You most likely have some Macs.

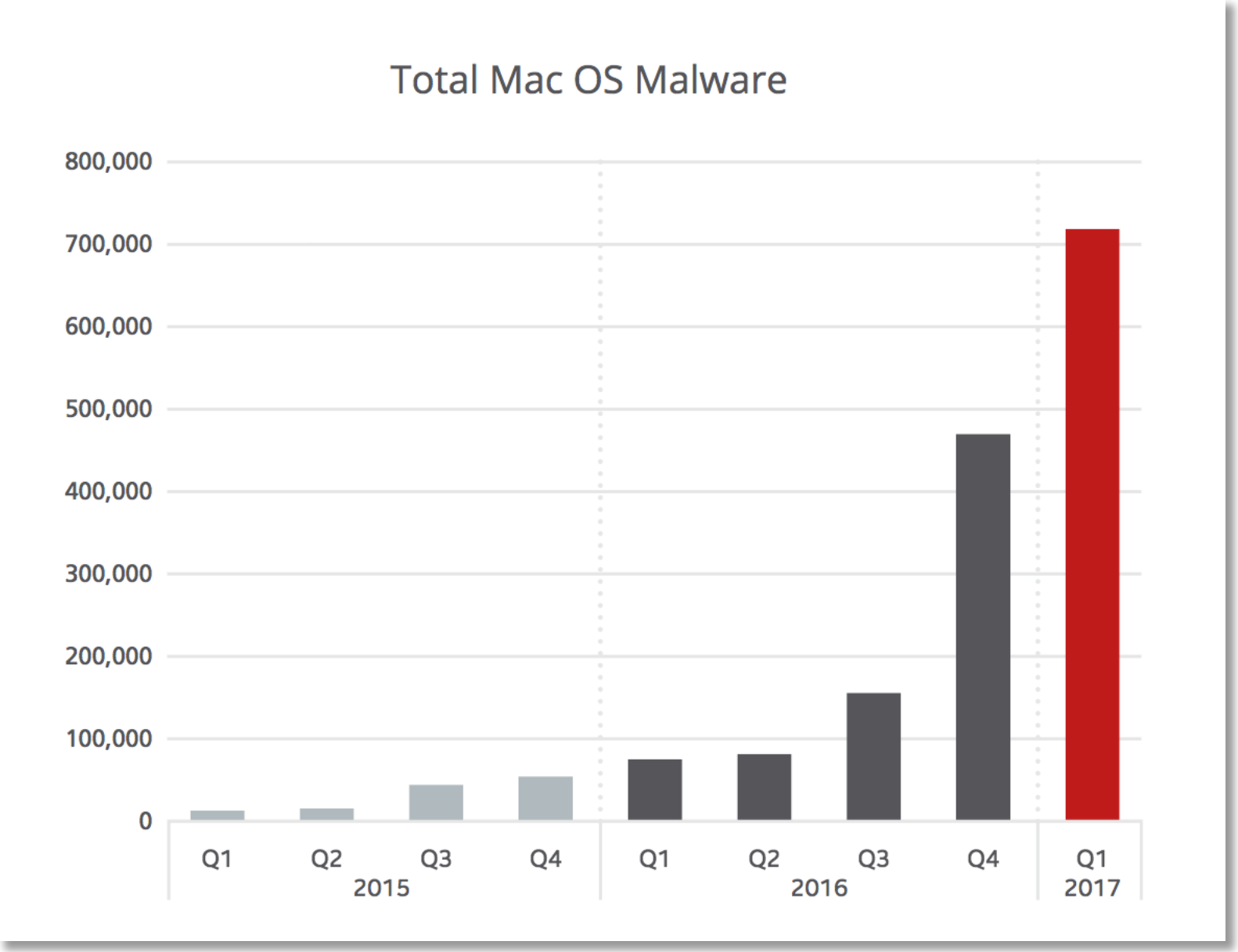






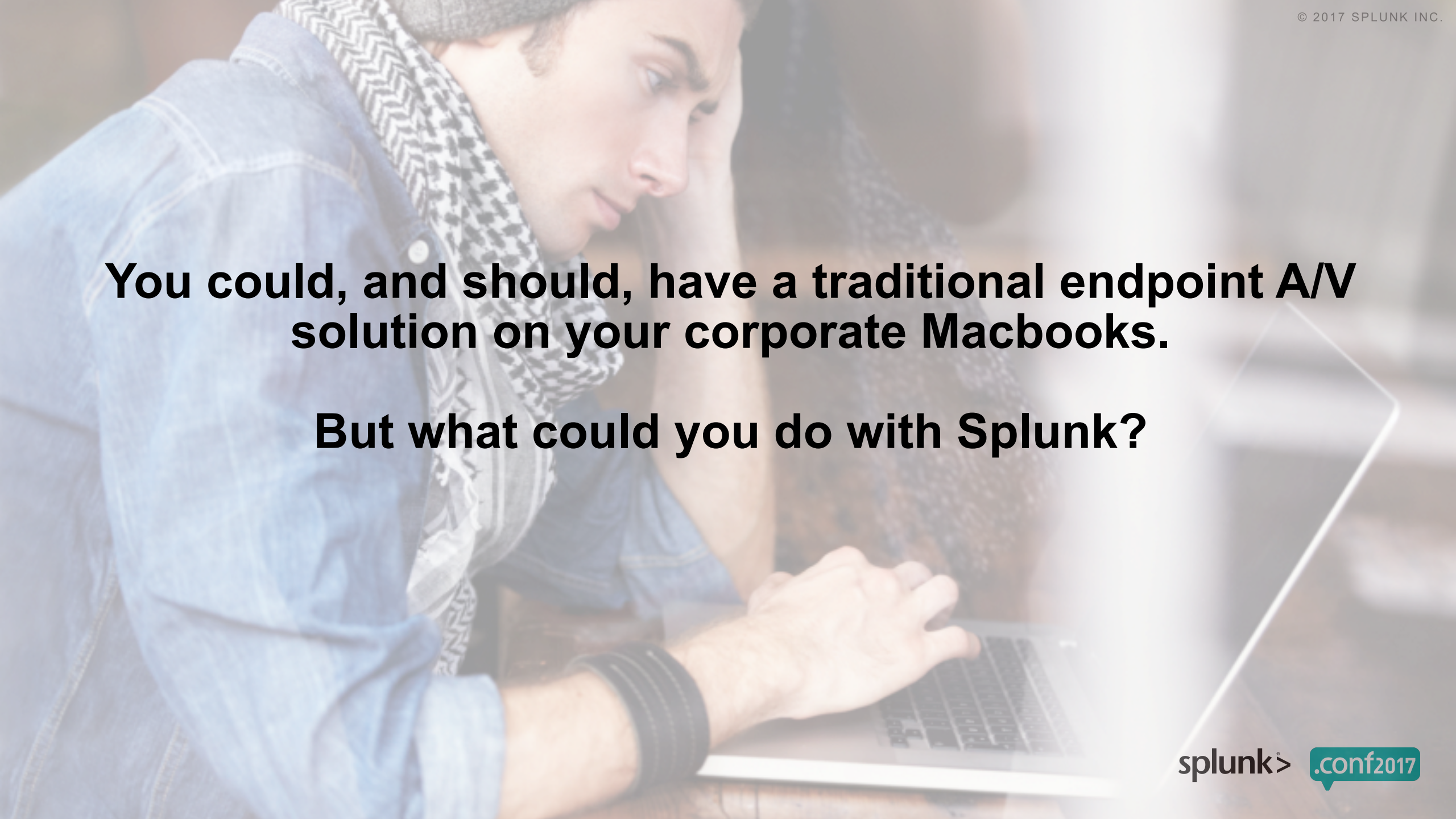
(2016 JAMF "Managing Apple Devices in the Enterprise")

splunk> .conf2017



(2017 McAfee)

splunk> .conf2017



You could, and should, have a traditional endpoint A/V solution on your corporate Macbooks.

But what could you do with Splunk?

Here's what we said about Windows…

The UF: More Than You Think!

Process/Apps/FIM

Vulnerabilities

Firewall

Registry

Wire Data

Forensics

Logs

Sysmon

The UF: More Than You Think!

Process/Apps/FIM

Vulnerabilities

Firewall

Registry

Wire Data

UF + nix TA + Stream + osquery!

Forensics

Logs

Sysmon

osquery

Home Docs FAQ Community Downloads

Performant Endpoint Visibility

osquery allows you to easily ask questions about your Linux, Windows, and macOS infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company.

Read the deployment guide

or start contributing!

Star 9,811 Fork 1,142

```
osquery> SELECT uid, name FROM listening_ports l, processes p WHERE l.pid=p.pid;
```

osquery gives you the ability to query and log things like running processes, logged in users, password changes, USB devices, firewall exceptions, listening ports, and more. You can perform ad-hoc queries or schedule them, optionally enable file integrity monitoring and process accounting too. More details can be found here

Enterprise Ready

CentOS, Ubuntu LTS, Windows, and macOS, and almost every Linux OS released since 2011 are supported with no dependencies. osquery powers some of the most demanding companies, including Facebook.

Differential Changes

Know when critical objects are added, modified or deleted from a system. Use a combination of event streams and polling with set differentials.

Feature Velocity

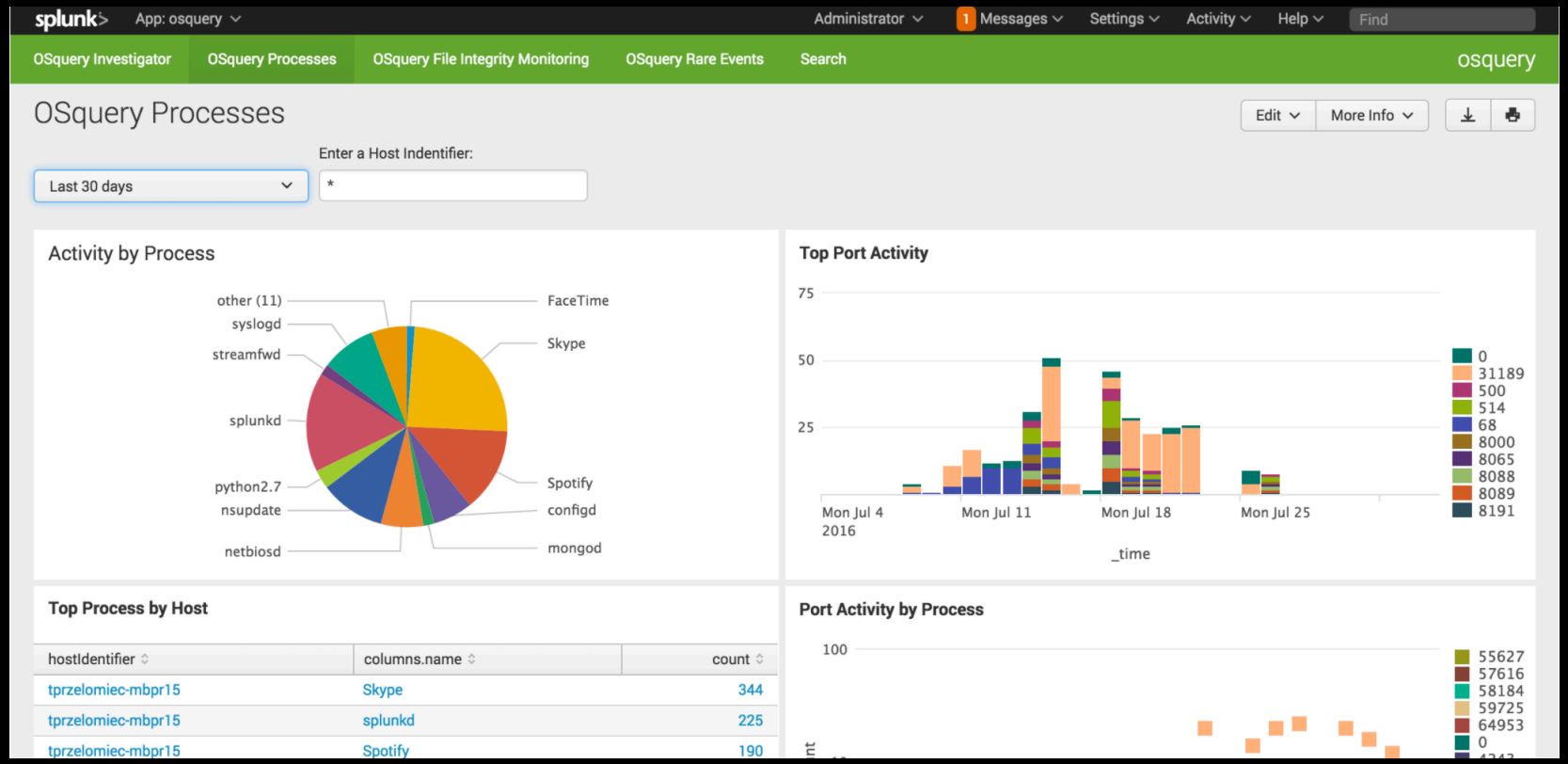
You control the roadmap. Developed in the open, by the community, for the community on Github.

Query your endpoints via SQL syntax for gobs of OS/IR/forensic info.

Linux, macOS, Windows, etc…

Open source.

splunk> .conf2017



Community App written by Thomas Przelomiec (Splunk)

Ad-Hoc or Scheduled.

JSON output gathered by UF.

Highly scalable (started by Facebook)

FIM!

Community-Contributed Query Packs and Guidance

Introduction to osquery for Threat Detection & DFIR

Jen Andre on May 9, 2016

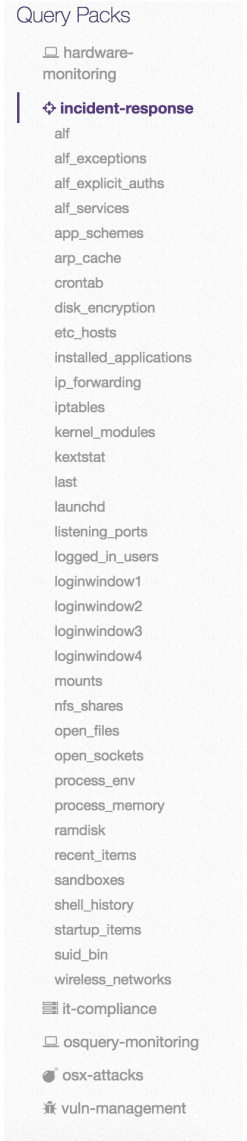
0

What is osquery?

osquery is an open source tool created by Facebook for querying various information about the state of your machines. This includes information like:

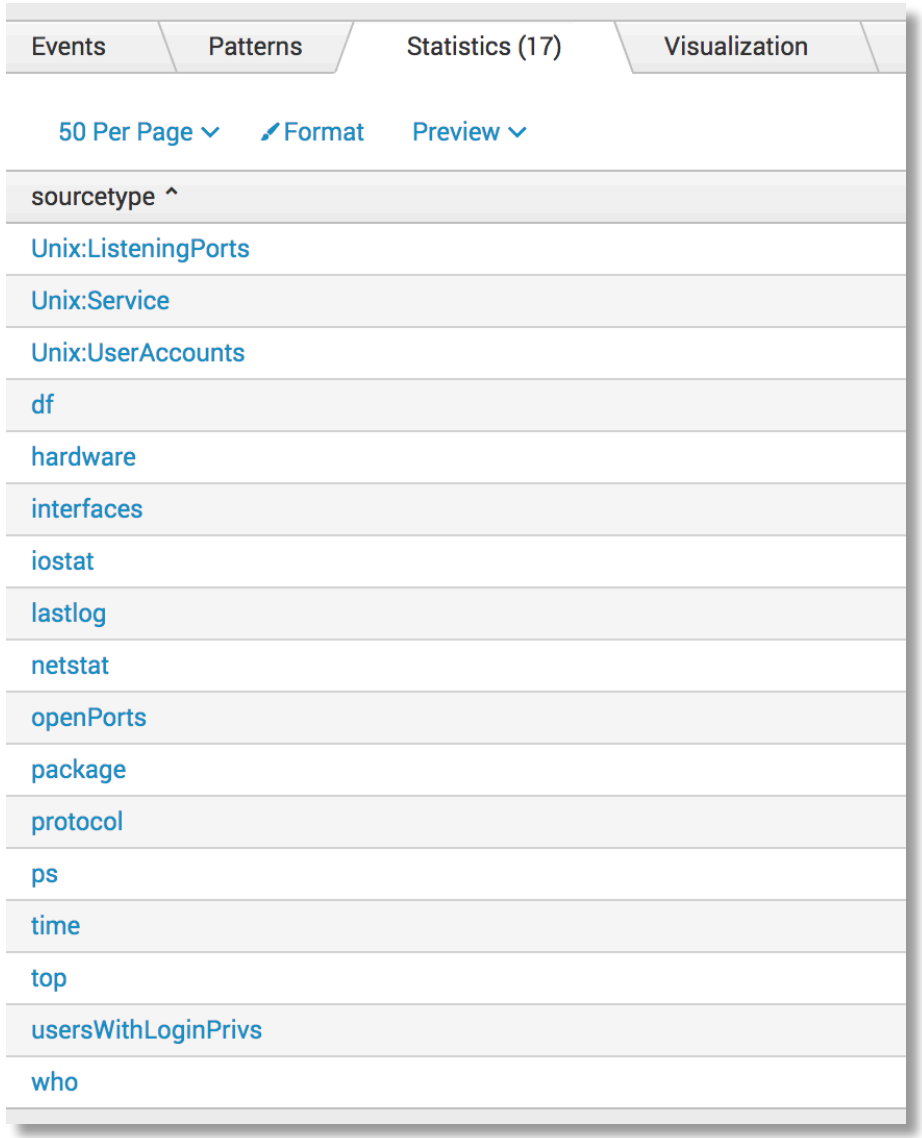
- Running processes
- Kernel modules loaded
- Active user accounts
- Active network connections

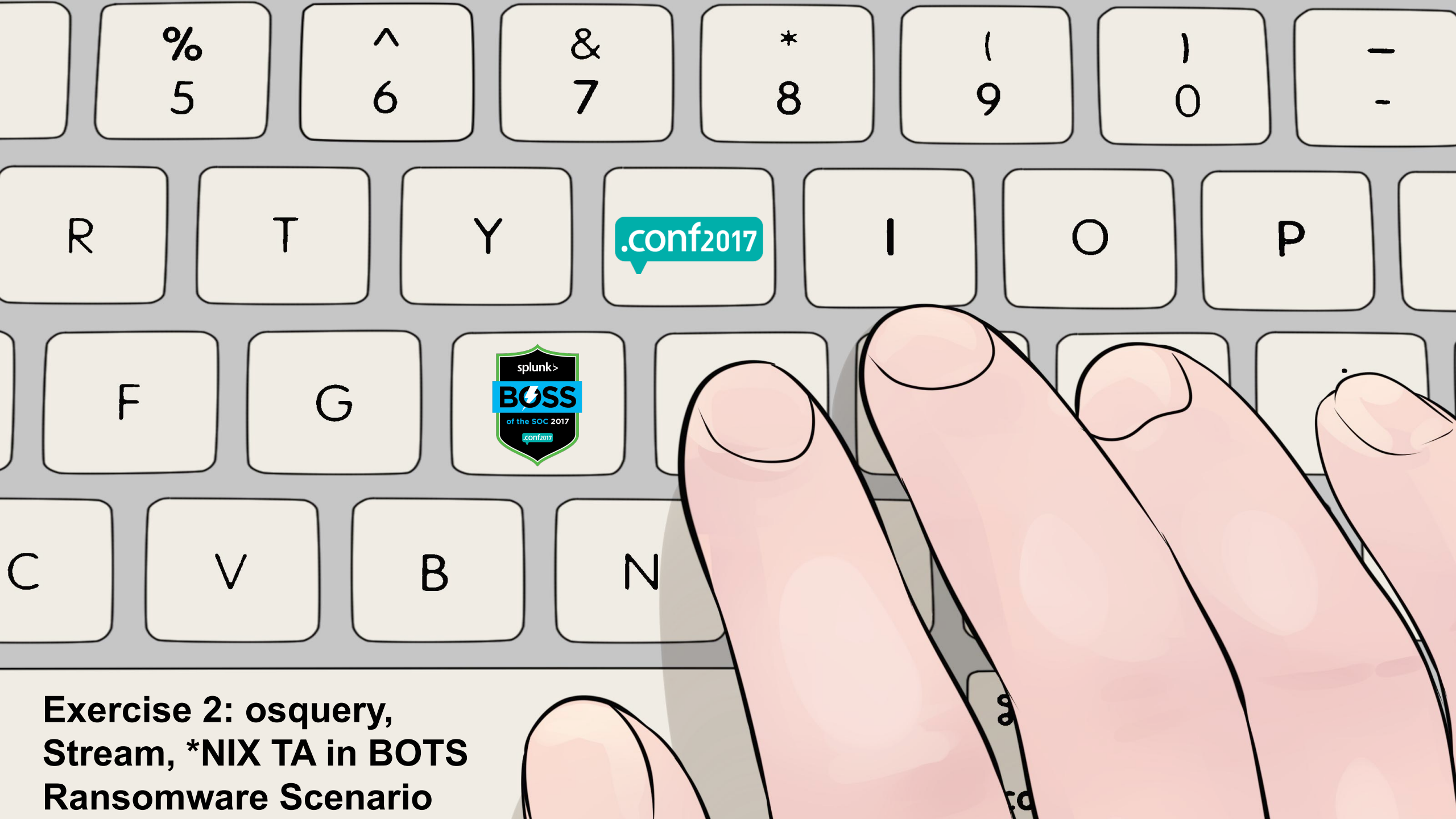
And much more!



splunk> .conf2017

Don’t forget about the *NIX TA



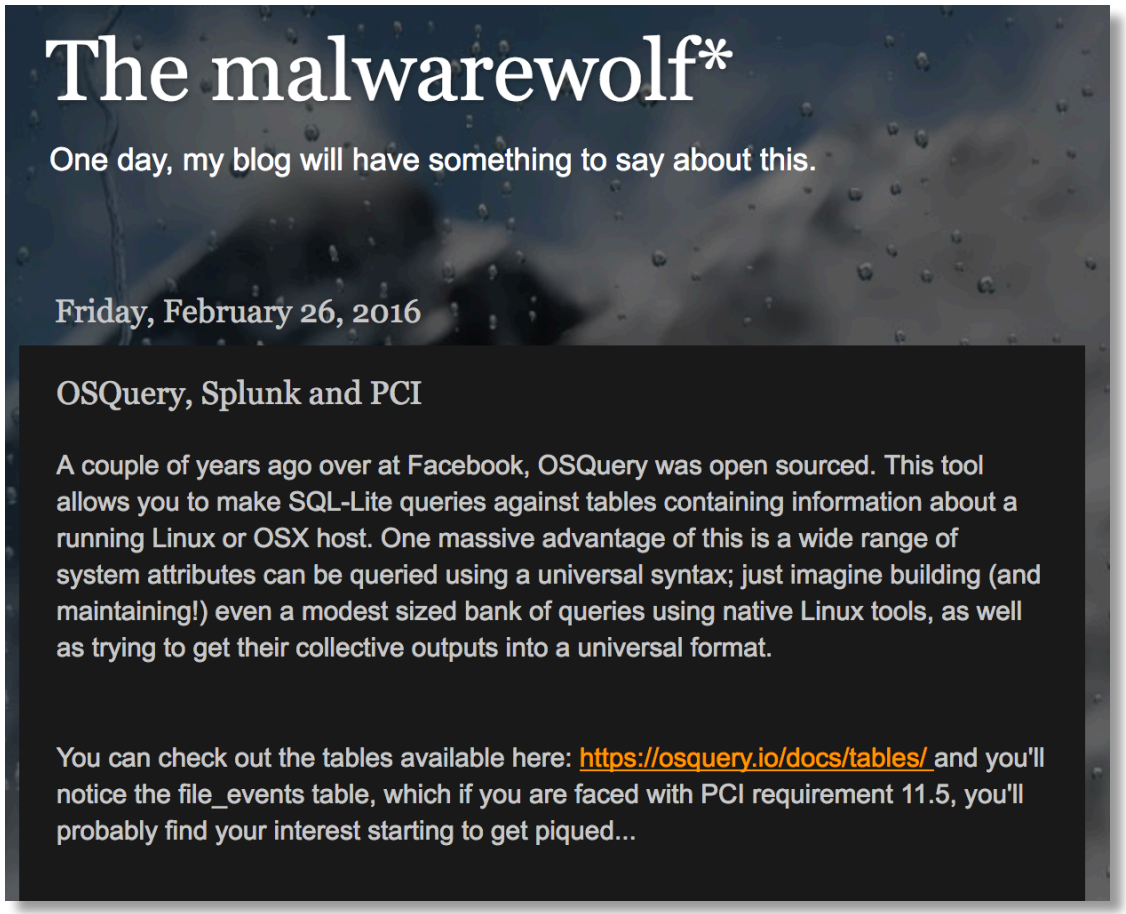


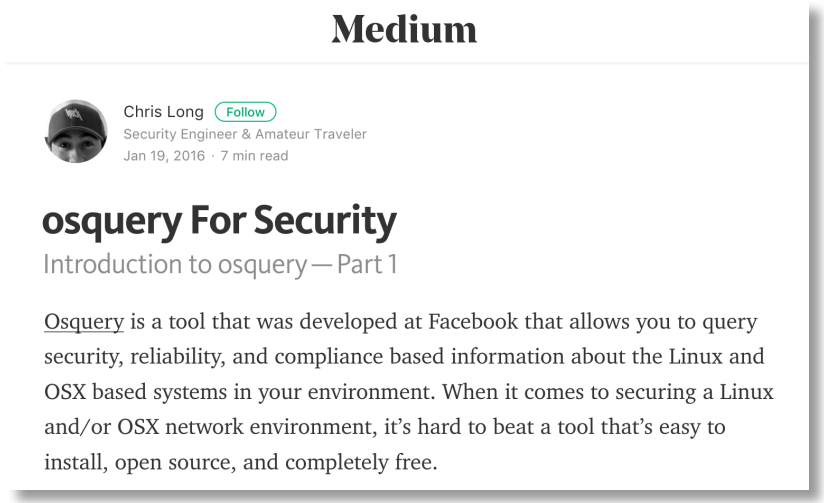
Exercise 2: osquery, Stream, *NIX TA in BOTS Ransomware Scenario

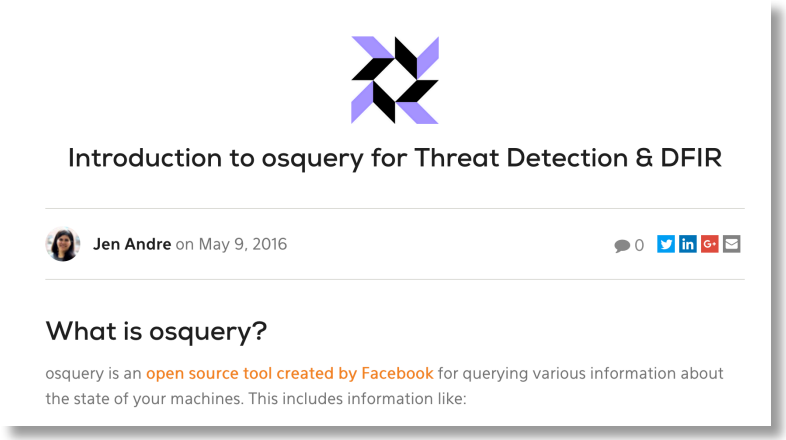
Theme: Let's save the day by using osquery to find ransomware that royally messed up some critical marketing files, and then decrypt them!

Upon further review…

Learn more about osquery



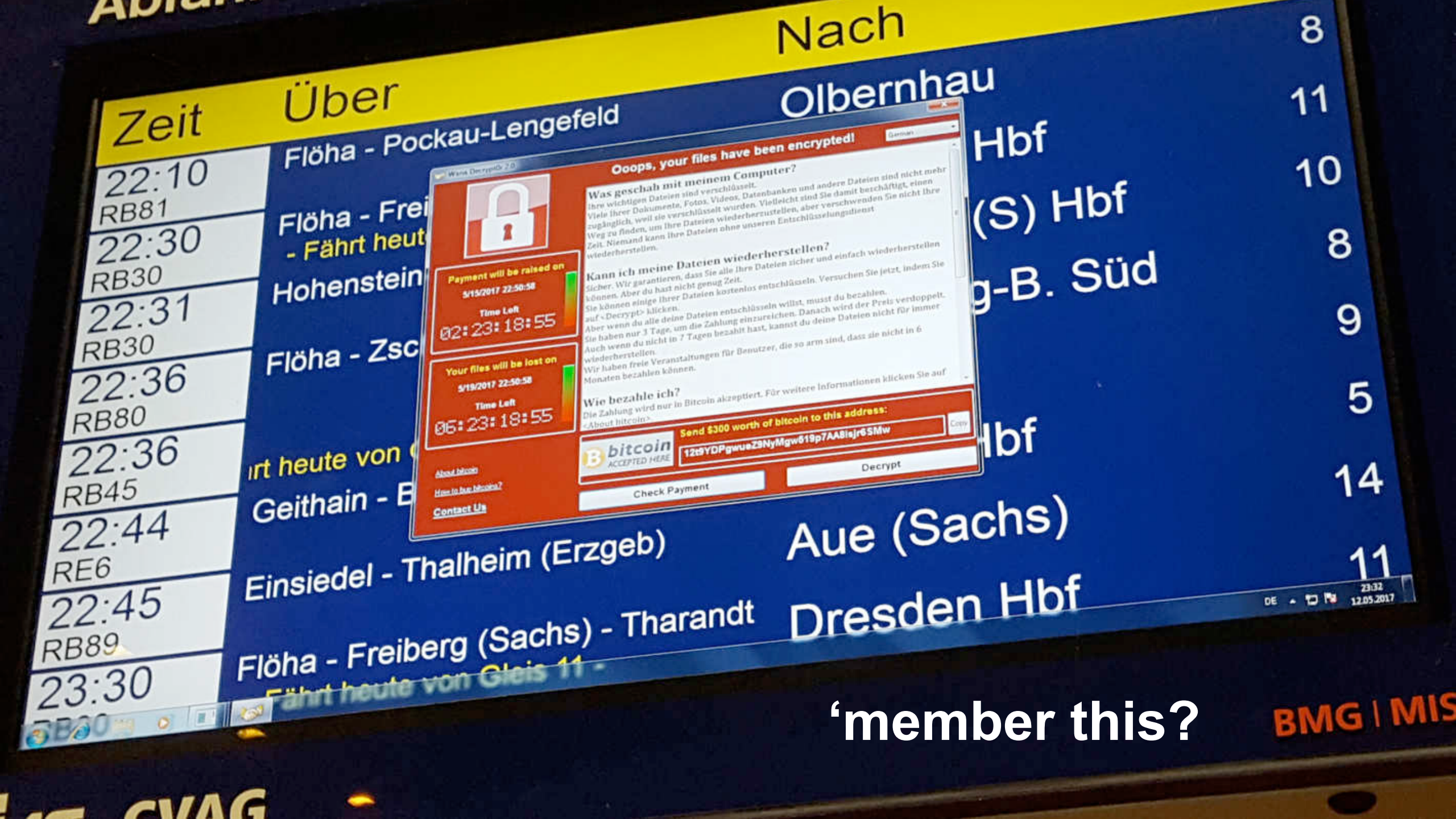


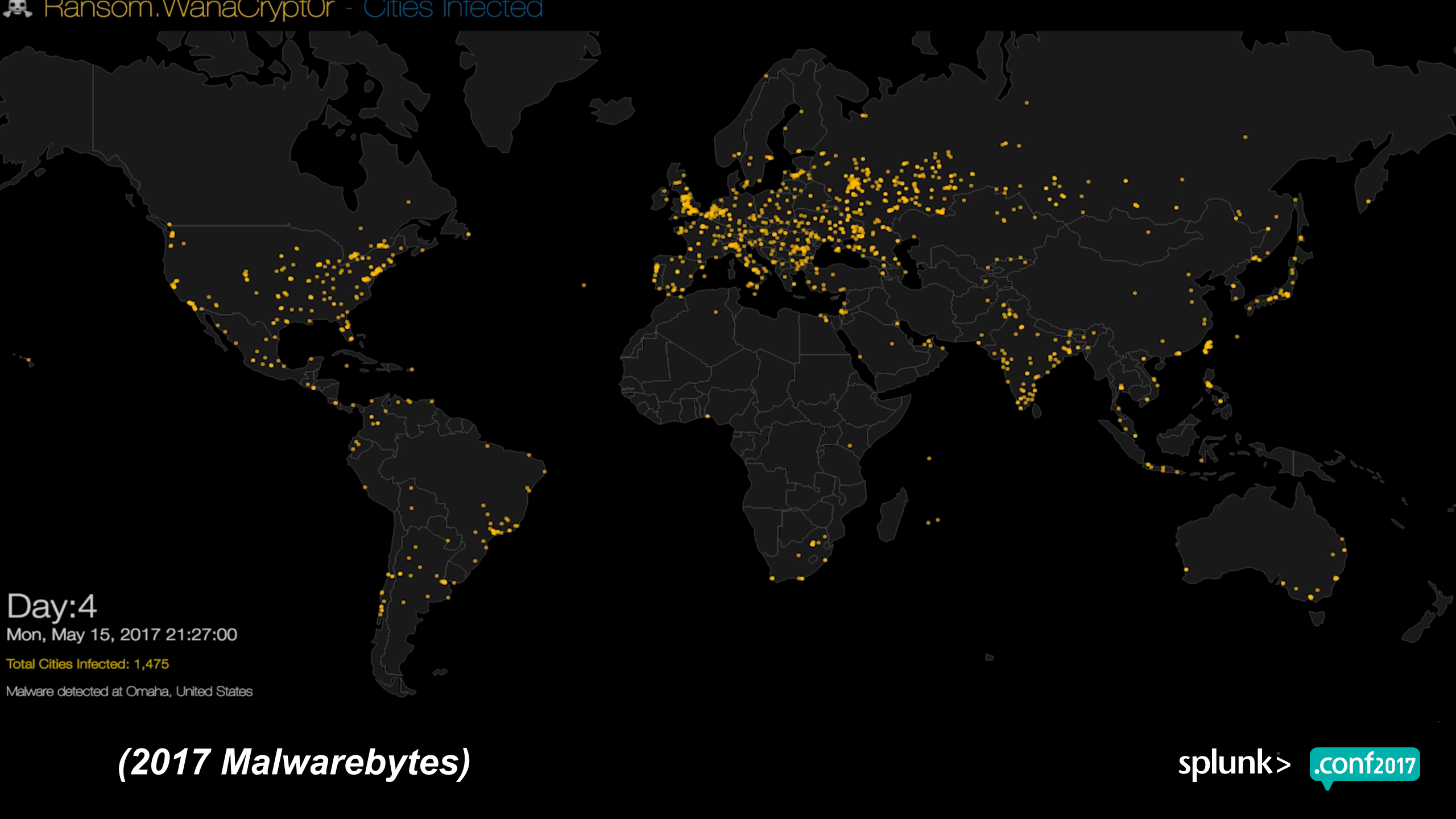


splunk> .conf2017

You may have heard. Ransomware is still a thing.

splunk> .conf2017


Zeit
Über
Nach
22:10 RB81 Flöha - Pockau-Lengefeld Olbernhau 8
22:30 RB30 Flöha - Frei - Fährt heut Hohenstein Hbf 11
22:31 RB30 Flöha - Zsc (S) Hbf 10
22:36 RB80 g-B. Süd 8
22:36 RB45 Geithain - B 9
22:44 RE6 Einsiedel - Thalheim (Erzgeb) Hbf 5
22:45 RB89 Flöha - Freiberg (Sachs) - Tharandt Aue (Sachs) 14
23:30 Dresden Hbf 11
Ooops, your files have been encrypted!
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
Payment will be raised on
5/15/2017 22:50:58
Time Left
02:23:18:55
Your files will be lost on
5/19/2017 22:50:58
Time Left
06:23:18:55
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
‘member this?
BMG | MIS



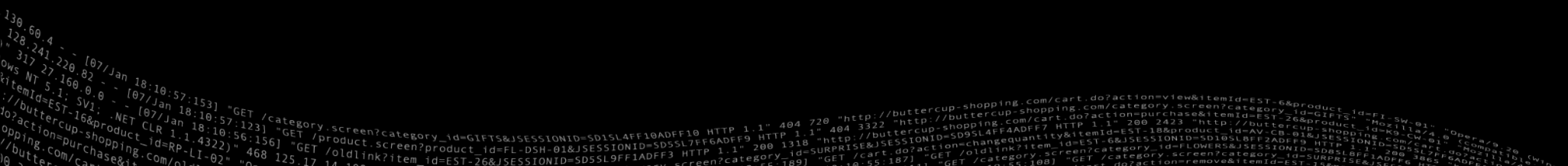
(2017 Malwarebytes)

Friday, May 12th, 2017

Behavioral Approach to Malware Detection

Splunk searches to find ransomware, early!

- Most malware/ransomware **behaves in predictable ways.**
- Assuming you instrument your environment appropriately (with the UF, or other) **you should be searching for certain things.**
- Searches that **we've been talking about for the past two years would have helped** with:
  - WannaCry
  - NotPetya
  - EternalRocks
  - …and whatever comes down the pike next.



splunk> .conf2017

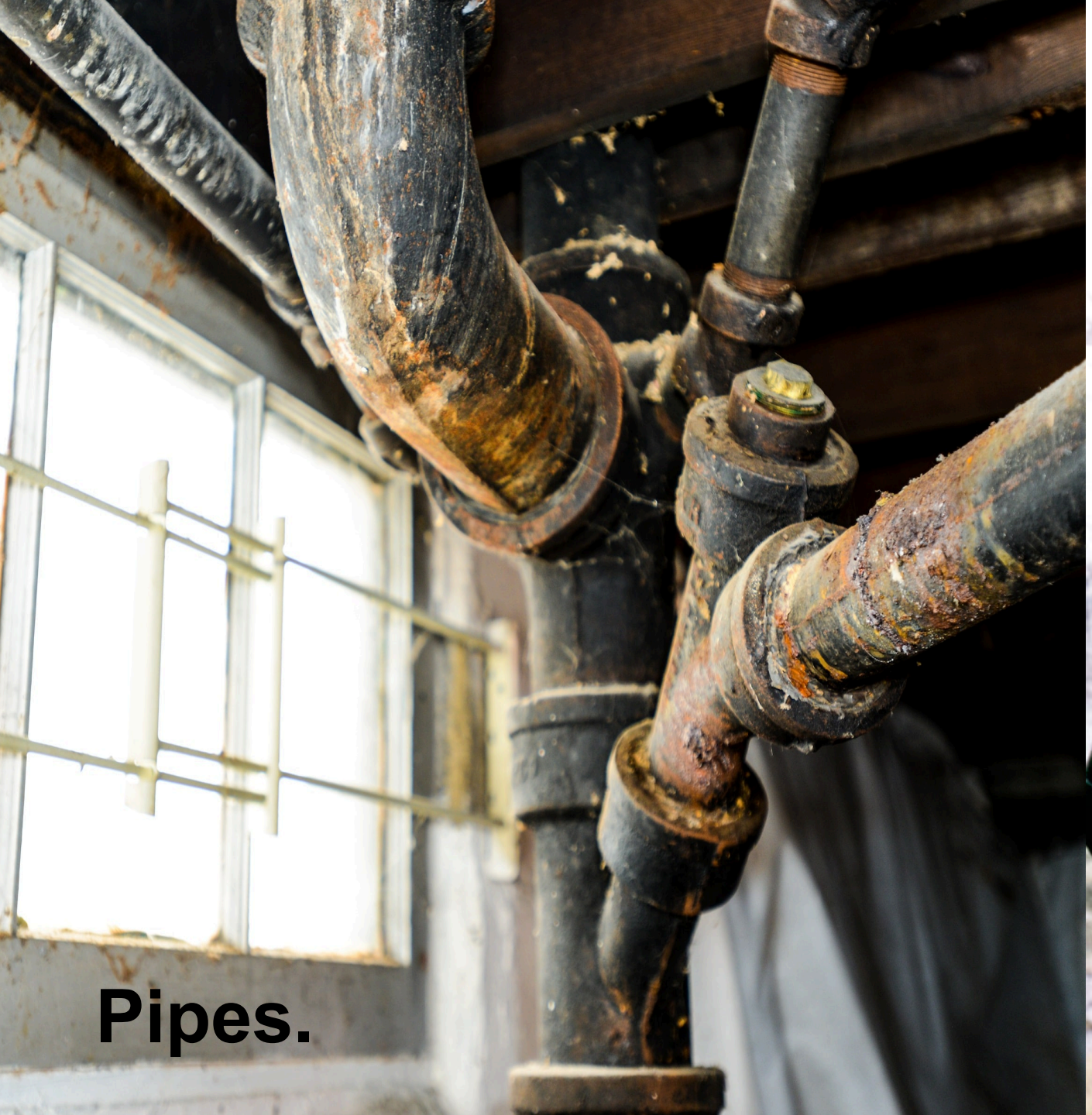
non sequitur


This is a pike.

Yes, also a pike.

splunk> .conf2017

Indeed, a pike.


Pipes.


splunk>
BOSS
of the SOC 2017

Believe it or not, the original term is “pike.”

Canadian Oxford Dictionary, 2nd Edition:

> **come down the pike** *N Amer*. appear on the scene; come to notice. [Abbreviation of TURNPIKE]

The American Heritage College Dictionary, 4th Edition:

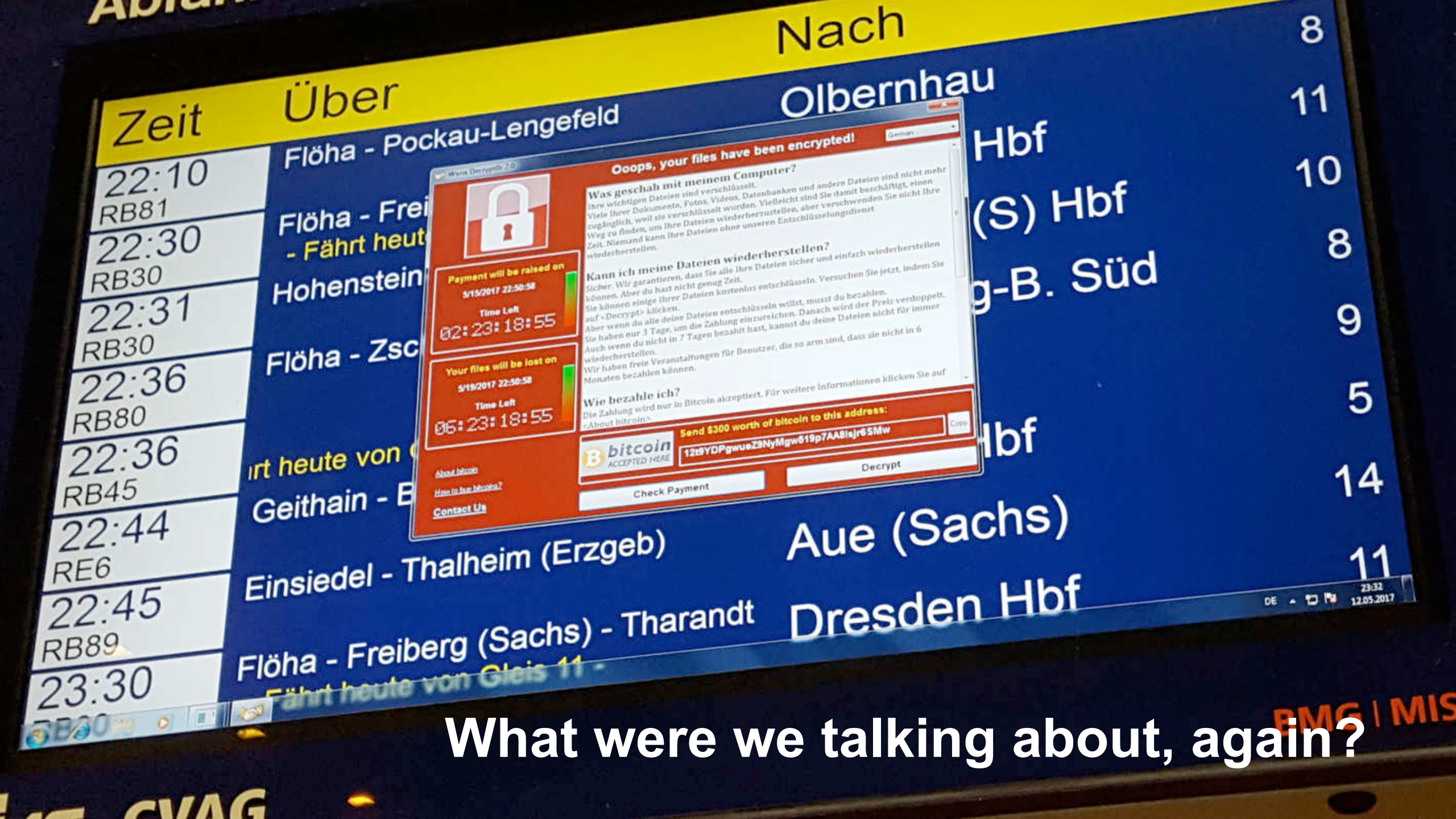
> ***Idiom: come down the pike*** *Slang* To become prominent. [Short for TURNPIKE.]

The American Heritage Dictionary of the English Language, 5th Edition:

> ***Idiom: come down the pike*** *Slang* To come into prominence: *"a policy . . . allowing for little flexibility if an important new singer comes down the pike"* (Christian Science Monitor). [Short for TURNPIKE.]

…and now you can say you learned something at .conf. Tell your manager!

splunk> .conf2017



What were we talking about, again?

#alternativepricing

Don't Pay Ransomware

Splunk Insights for Ransomware provides smaller organizations with an additional layer of security to help combat ransomware. By enabling a broader analytics-driven approach to security, Splunk Insights for Ransomware enables understaffed IT and security shops to gain end-to-end visibility into potential ransomware activity across the IT environment.

Assess security posture, investigate and verify efficiently, and remediate quickly and appropriately – from critical infrastructure to deprecated operating systems, Splunk Insights for Ransomware helps you get better at staying on top of security hygiene to combat persistent and emerging ransomware threats, so you can maintain business continuity in the face of mutations -- even global, fast-propagating attacks like WannaCry.

- **Central visibility and analysis of ransomware: Use relevant data – endpoint, network, etc. – to identify and assess potential ransomware activity**
- **Faster, streamlined investigation of ransomware activity: Pivot easily between technologies to find evidence of ransomware threats, across security and IT**

Get Started

White Paper
Detecting Unknown Malware and Ransomware

Try Now
Analyze Endpoint Activity

Video
Ransomware Vulnerability Assessment

Contact Us

splunk> .conf2017

User-based Pricing (up to 1000 users) (not stackable)

Let's revisit Ransomware's Greatest Hits.

splunk> .conf2017

Exercise 3: WannaCry, EternalRocks, and NotPetya

Theme: Yes, Ms. Chief of Information Security. This expensive solution called Splunk that we bought can help us detect and defend against WannaCry/NotPetya/TheFlavorOfTheWeek.

Ransomware, Schmansomware

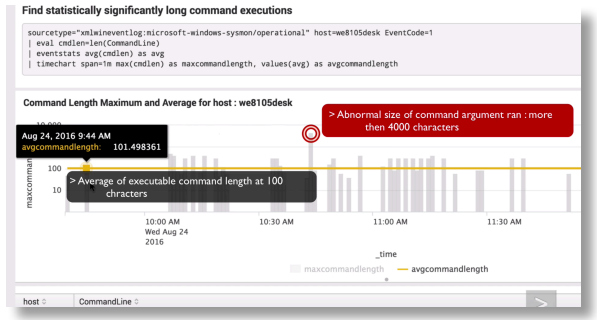
Early detection, prevention…

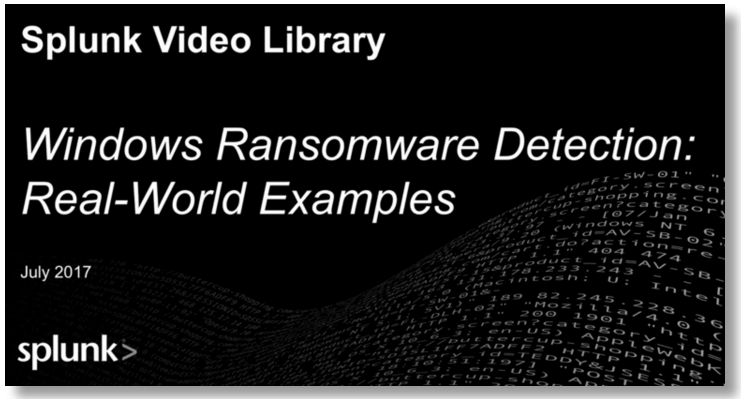
Analyze Endpoint Activity

Find malware infections before damage is caused to business operations

- ✔ Validate the method and source of infection by analyzing endpoint behavior
- ✔ Scope the broader impact of the malware or ransomware infection
- ✔ Understand how to prevent similar infections in the future

Try This Use Case | Watch the Video Demo





Ransomware Wrangling with Splunk

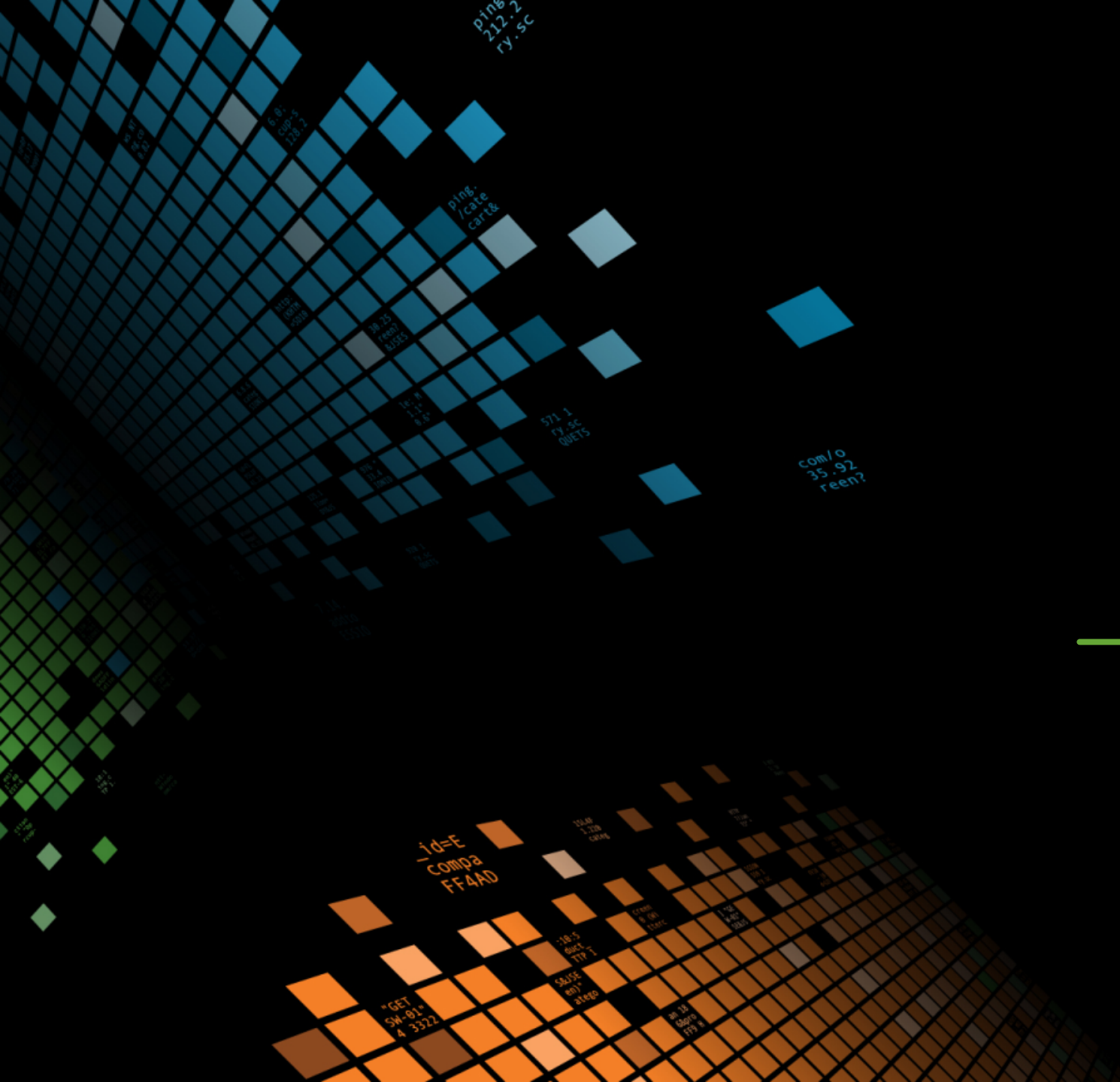
Tuesday, September 27, 2016 | 11:35 AM-12:20 PM

INTERMEDIATE | **Products:** Other, Splunk Enterprise Security, Splunk Enterprise | **Role:** Security Analyst | **Track:** Security / Compliance / Fraud | **Session Focus:** Threat Detection | **Other Topics:** applyingThreatIntelligenceContext, Best Practices, ransomware

Speakers
Kenneth Westin, Security Market Specialist, Splunk

Recording

splunk> .conf2017



Q&A

Thank You

Don't forget to rate this session in the .conf2017 mobile app

…or there won't be a Splunking the Endpoint IV!

splunk> .conf2017