splunk> .conf2017

Essentials to creating your own Security Posture using Splunk Enterprise

Using Splunk to maximize the efficiency and effectiveness of the SOC / IR

Richard W. McKee, MS-ISA, CISSP | Principal Cyber Security Analyst
Nevada National Security Site

September 28, 2017 | Washington, DC

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.

splunk> .conf2017

“ It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.”

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tzu, *The Art of War*

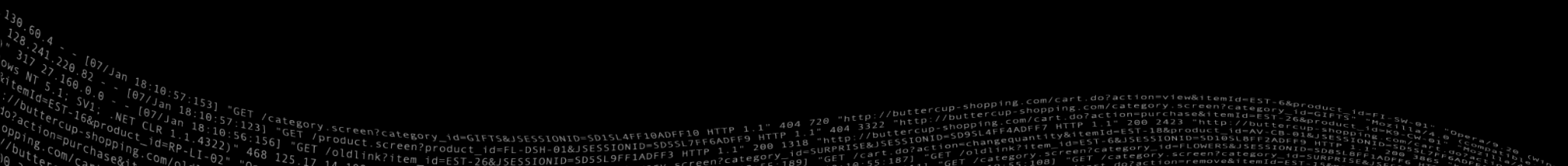
https://en.wikiquote.org/wiki/Sun_Tzu

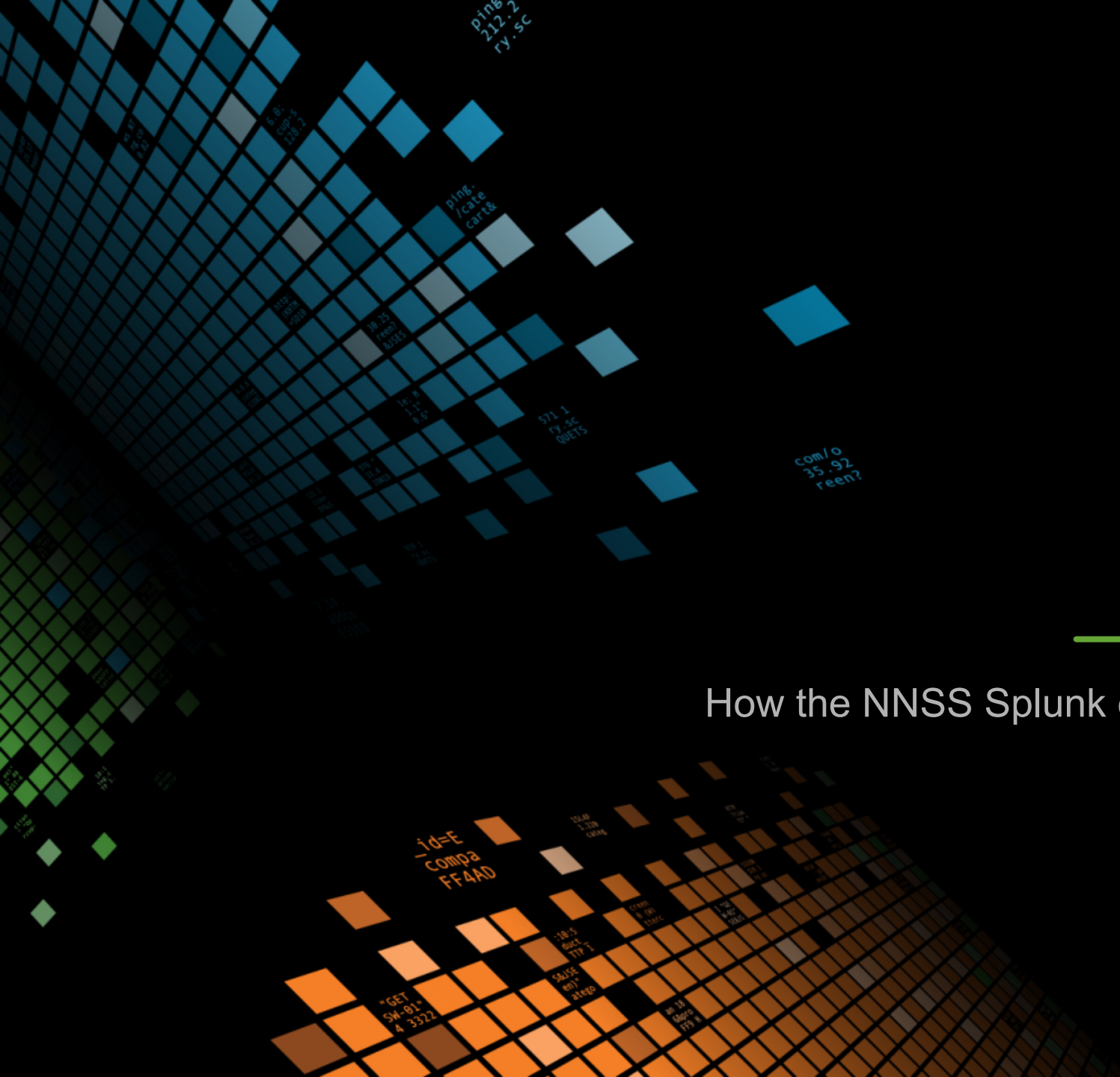
Richard W. McKee

Background – Experience and Education

- Principal Cyber Security Analyst – Nevada National Security Site

- 25 years in law enforcement
  - Last 11 years in computer forensics and cyber investigations (criminal and national security)
- Master of Science – Information Security and Assurance
- Bachelor of Business Administration – Management Information Systems
- Certifications – CISSP, Splunk Certified Power User, EnCE, GPEN, GCIH, GREM, GMON, GNFA, GISP

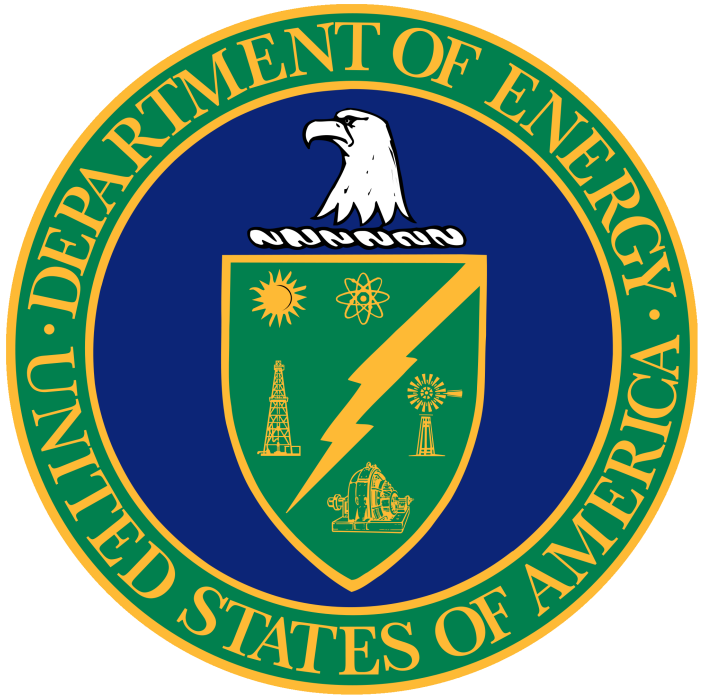




Background

How the NNSS Splunk experience relates to your enterprise

What is the NNSS?



NNSA
National Nuclear Security Administration

NEVADA NATIONAL
NNSS
SECURITY SITE

NEVADA NATIONAL
NNSS
SECURITY SITE


Nevada National Security Site, NV


Lawrence Livermore Operations,
Livermore, CA


Special Technologies
Laboratory
Santa Barbara, CA

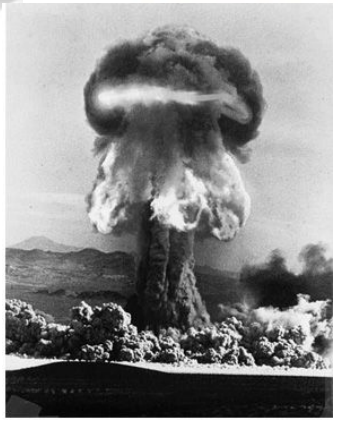

Remote Sensing Laboratory
Nellis AFB, NV


North Las Vegas Operations
North Las Vegas, NV


New Mexico Operations
Albuquerque, NM


New Mexico Operations
Los Alamos, NM


Remote Sensing Laboratory
Andrews AFB, MD



splunk> .conf2017

Prevention is Ideal…
But Detection is a Must

- Splunk is the primary SIEM for the NNSS
- All hosts and devices capable of sending logs to Splunk do so
- Cyber has made logging a policy requirement and all in-house developers or hired consultants must write software capable of logging and sending events to Splunk

Data Sources

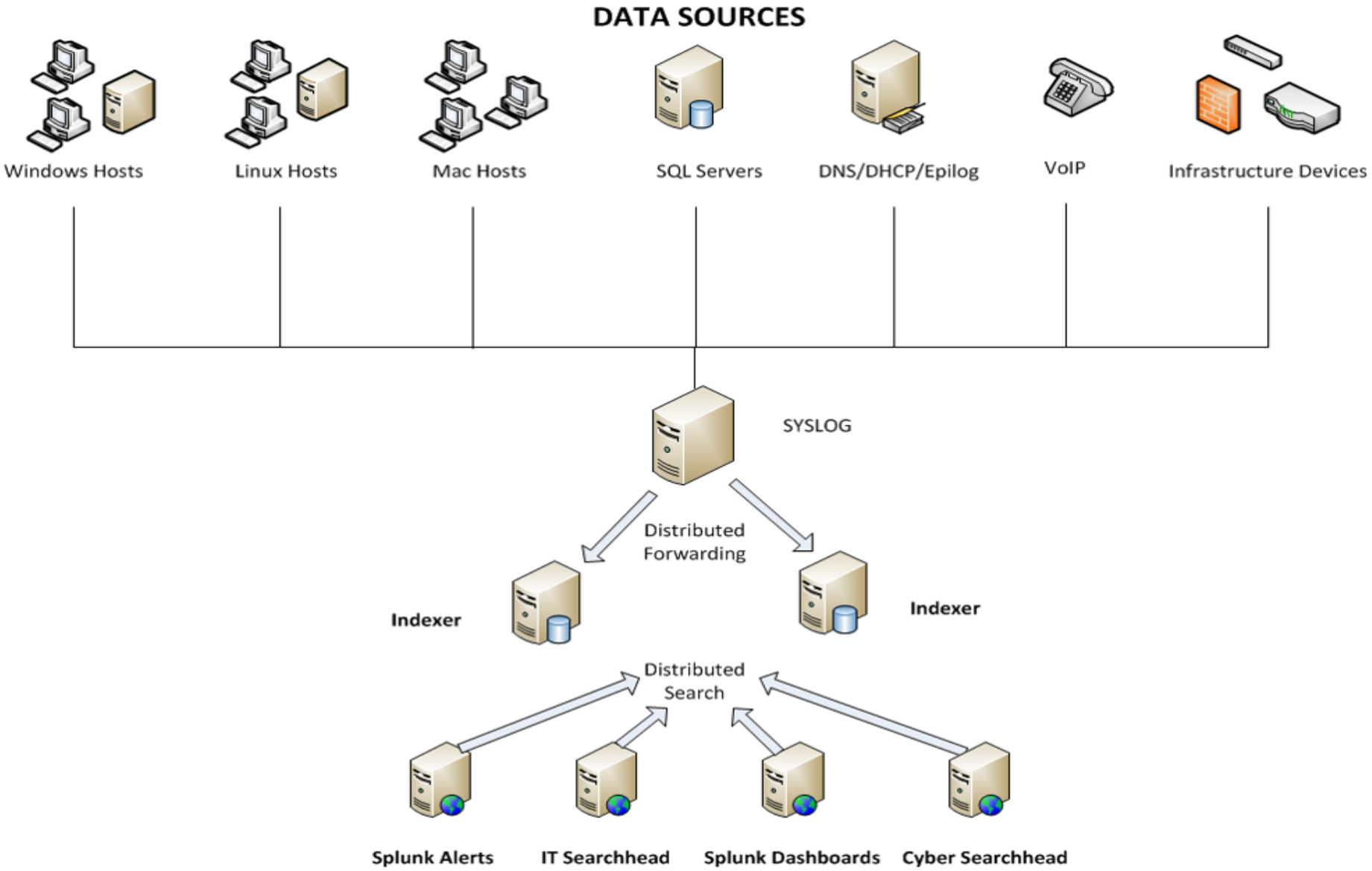
"…know yourself..."

- Windows Hosts
- Linux Hosts
- Mac Hosts
- Routers and Switches
- Firewalls
- Endpoint Protection
- Syslog
- Internal Splunk servers
- Databases

- VPN
- RSA
- Active Directory
- VoIP Phones and Servers
- Email Security Appliance
- Malware Sandbox
- FortiMail
- DLP
- Mobile Device Management

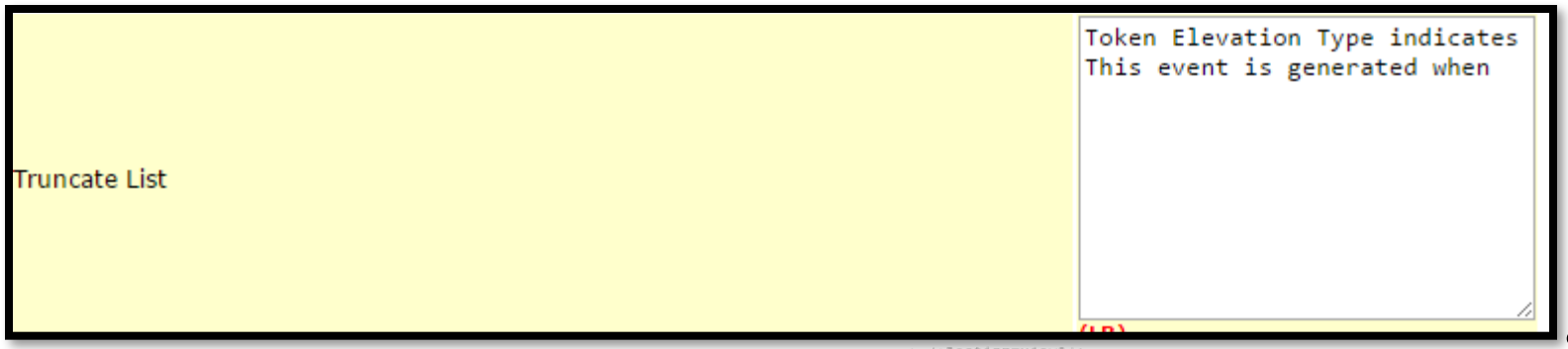
Configuration

- A physical syslog server is the primary feed for Splunk
- For security, only the syslog server can communicate directly with the Splunk indexers
- All forwarders and devices feed the syslog box directly*
- A 10Gbps tap is also feeding the syslog server
- If Splunk fails, logs are also temporarily stored on Syslog



Host Logs

- Enterprise Snare is used to grab logs from sources. NNSS brought the Snare developer in from Australia to custom create agents for Windows, Mac, Linux, SQL, and Epilog
- The Snare Agents are highly customizable and act as the first filter prior to Splunk, allowing the reduction of unnecessary data



Snare Configuration

Action Required	Criticality	Event ID Include/Exclude	Event ID Match	User Match	General Match	Source Match	Return	Event Src
Delete Modify	Information	Exclude		**Include:** *	**Include:** *	**Include:** *	Success Failure Error Information	Security
Delete Modify	Information	Include	Logon_Logoff	**Exclude:**	**Include:** *	**Include:** *	Success Failure	Security
Delete Modify	Information	Include	520,4616,1102,517,4697,601	**Include:** *	**Include:** *	**Include:** *	Success Failure Error Information Warning Critical	Security
Delete Modify	Information	Include	User_Right_Events	**Include:** *	**Exclude:**	**Include:** *	Success Failure Error Information Warning	Security
Delete Modify	Information	Include	Process_Events	**Include:** *	**Include:** *	**Include:** *	Success Failure Error Information Warning	Security

splunk> .conf2017

Snare Custom Config

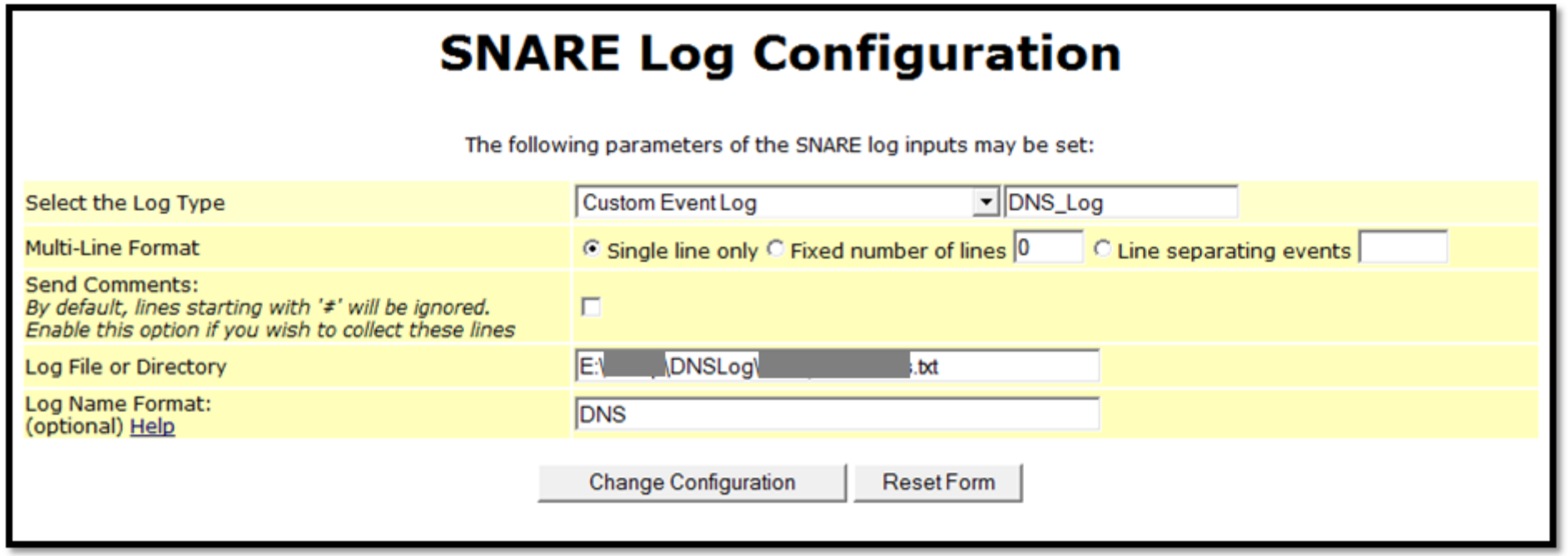
Identify the high level event	○ Logon or Logoff ○ Account Administration ○ Access a file or directory ○ Change the security policy ○ Start or stop a process ○ Restart, shutdown and system ○ Use of user rights ○ Filtering platform events ○ USB Event ◉ Any event(s)
Event ID Search Term *Optional, Comma separated: only used by the 'Any Event' setting above*	◉ Include ○ Exclude *
General Search Term *Wildcards accepted*	◉ Include ○ Exclude ☐ Regular Expression *
User Search Term *User Names, comma separated. Wildcards accepted*	◉ Include ○ Exclude *
Source Search Term *Source Names, comma separated. Wildcards accepted*	◉ Include ○ Exclude Microsoft-Windows-TaskScheduler
Identify the event types to be captured	☑ Success Audit ☑ Failure Audit ☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Verbose ☐ ActivityTracing
Identify the event logs (ignored if any objective other than 'Any event(s)' is selected):	☐ Security ☐ System ☐ Application ☐ Directory Service ☐ DNS Server ☐ DFS-Replication ☐ Legacy FRS ☑ Custom Event Log
Select the Alert Level	○ Critical ○ Priority ○ Warning ◉ Information ○ Clear

splunk> .conf2017

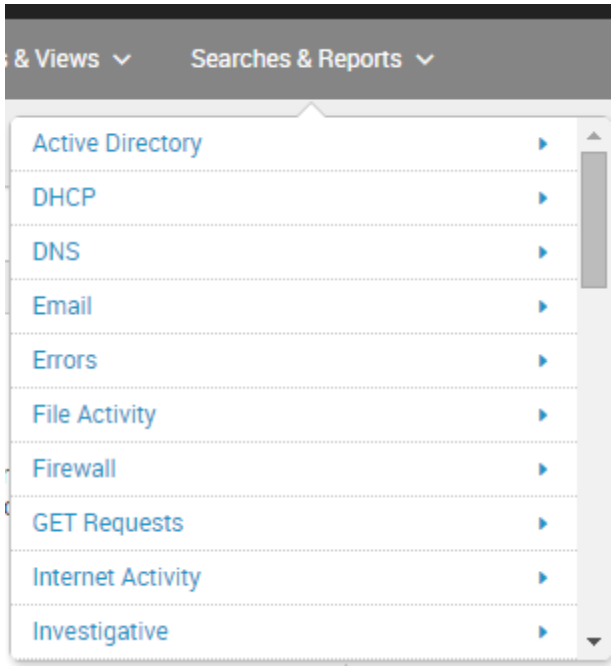
Epilog Agent

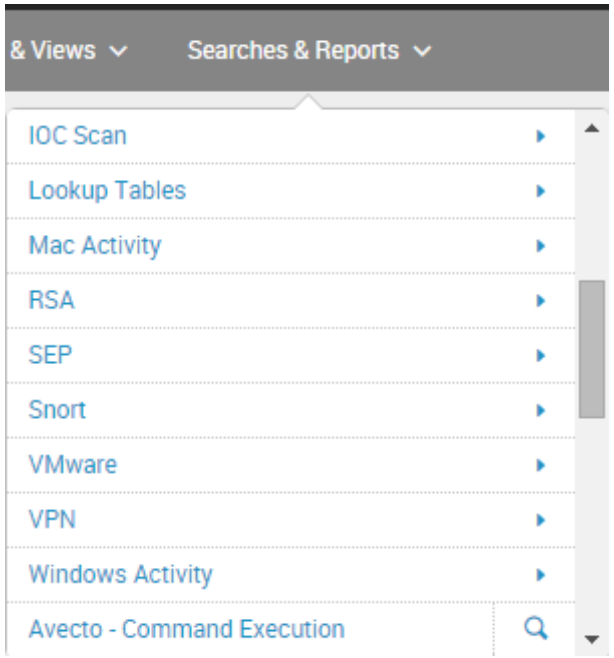
- Possible uses:
  - AV Logs from Linux hosts
  - DNS Logs from Domain Controllers
  - DHCP Logs from Domain Controllers
- Can be used to monitor any flat text files from any directory or UNC path

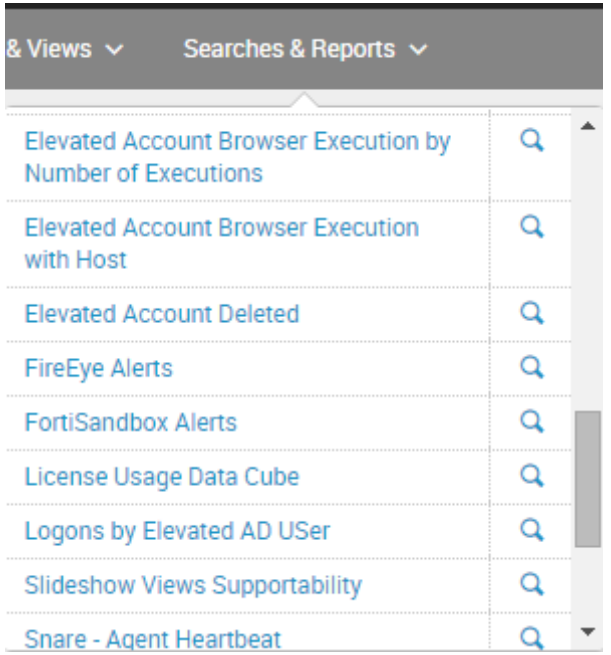
Epilog Agent



Splunk Searching & Reporting Highly Customized for IR



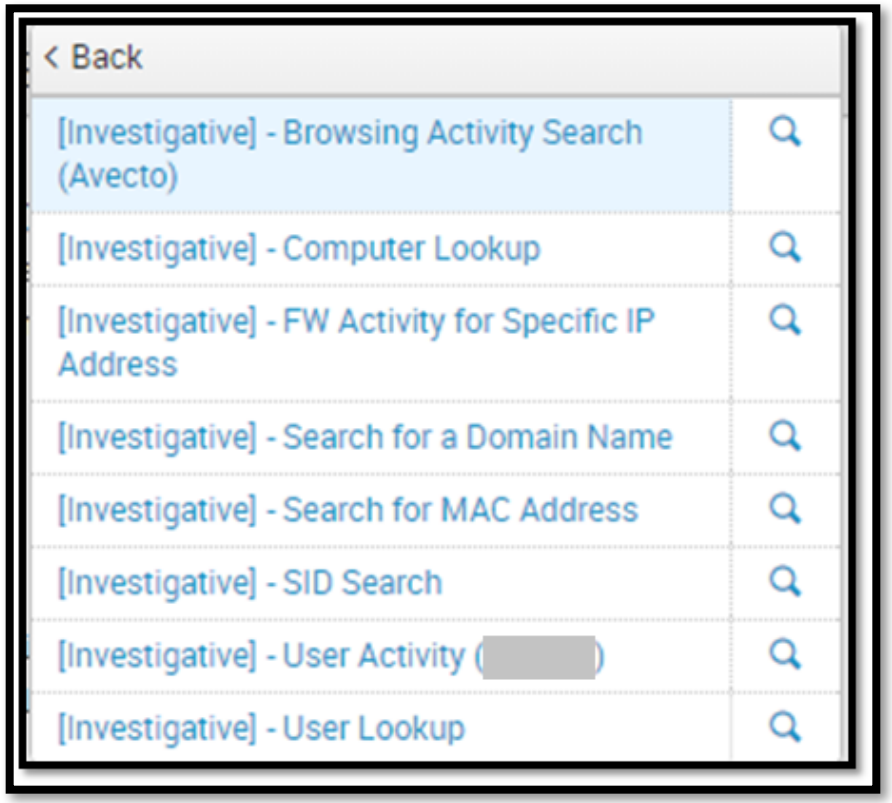




splunk> .conf2017

Quick Investigative Searches

- These searches are complete except for areas for the incident responder to put a username, IP, hostname, etc.



Search Examples - DNS

DATE/TIME (UTC) ^	REQUESTER CLIENT IP	DOMAIN
03-13-2016 04:53:59		clients4.google.com
03-13-2016 04:53:59		csc3-2010-crl.verisign.com
03-13-2016 04:53:59		prod.nexusrules.live.com.akadns.net
03-13-2016 04:53:59		ocsp.globalsign.com
03-13-2016 04:53:59		www.microsoft.com
03-13-2016 04:53:59		ent-shasta-rrs.symantec.com
03-13-2016 04:53:59		streamerapi.finance.yahoo.com
03-13-2016 04:53:59		csc3-2009-2-crl.verisign.com
03-13-2016 04:53:59		pki.energy.gov
03-13-2016 04:53:59		ent-shasta-rrs.symantec.com
03-13-2016 04:53:59		www.google.com
03-13-2016 04:53:59		chk.l2.nessus.org
03-13-2016 04:53:59		ent-shasta-rrs.symantec.com
03-13-2016 04:53:59		nexusrules.officeapps.live.com

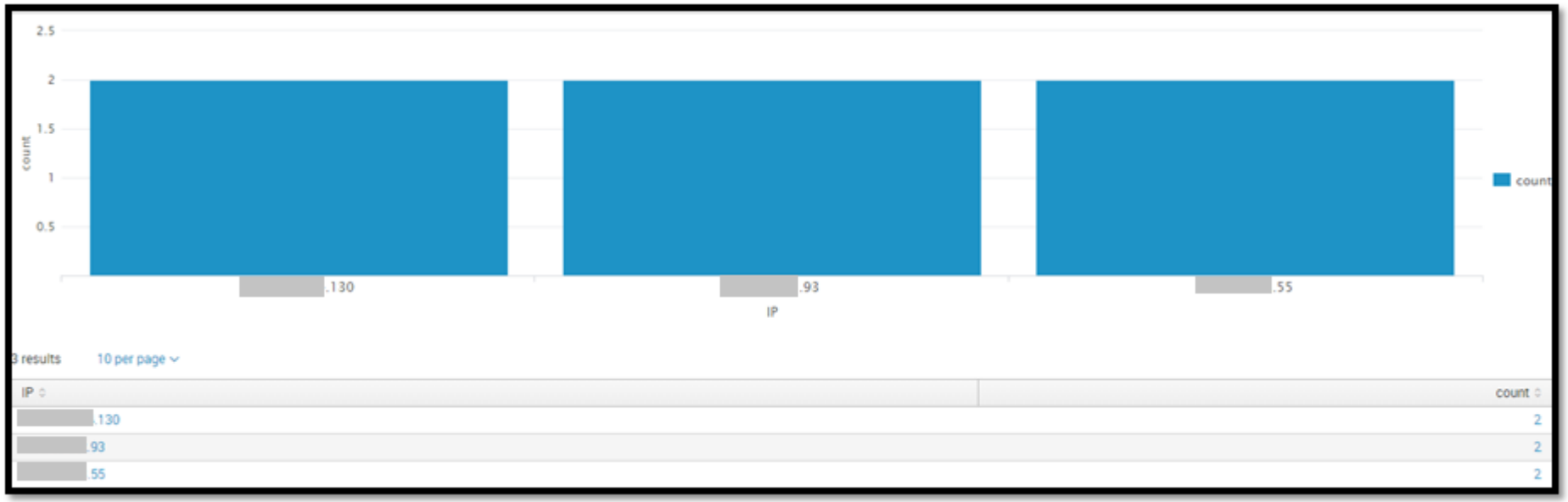
Search Examples – Files Written to USB

DATE/TIME FILE WRITTEN (LOCAL)	USER	HOSTNAME	DOMAIN	USB DEVICE ID	FILES WRITTEN
2016-03-12 20:53:35			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/~Archive3.pst.tmp
2016-03-12 20:53:35			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/Archive3.pst
2016-03-12 20:49:27			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/July 9 2013.pst
2016-03-12 20:49:27			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/~July 9 2013.pst.tmp
2016-03-12 20:49:20			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/~Archive3.pst.tmp
2016-03-12 20:49:20			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/Archive3.pst
2016-03-12 20:49:07			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/~Archive 4.pst.tmp
2016-03-12 20:49:07			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/Archive 4.pst
2016-03-12 20:38:26			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/~Archive3.pst.tmp
2016-03-12 20:38:26			NTSOPS	USBSTOR\Disk&Ven_Apricorn&Prod_Aegis_FIPS_DT&Rev_0217\AA0000022A1F&0	F:/Exchange/Archive3.pst

Serial number of the USB device is captured, allowing CIRT to do serial number lookups and correlation

splunk> .conf2017

Search Examples – Possible Compromised Hosts



Firewall logs are examined daily and hosts that meet two or three of the following are highlighted:

1 – Hosts with the most data flowing out

2 – Hosts with the highest number of connections

3 – Hosts with the longest duration of connections

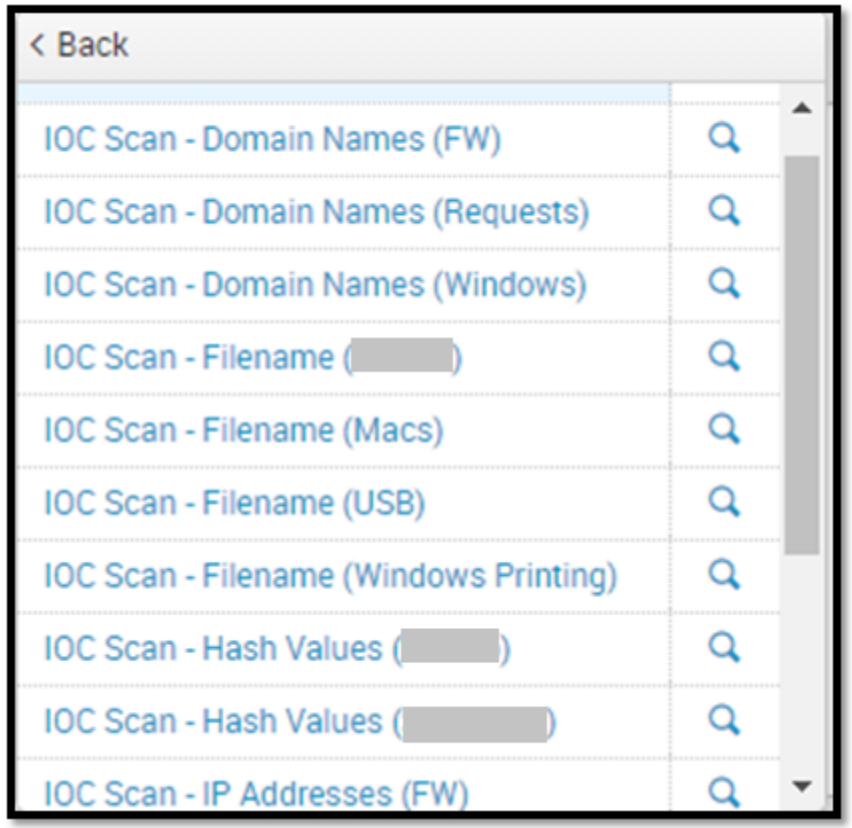
splunk> .conf2017

Search Examples – GET Requests

DATE/TIME (UTC)	SOURCE IP	DESTINATION IP	DESTINATION CITY	DESTINATION REGION	DESTINATION COUNTRY	GET REQUEST
03-13-2016 04:22:51		74.113.233.187	White Plains	NY	United States	anx.apnanalytics.com/tr.gif?anxa=TBNotifier&tbnguid=931F74FE-43F5 08&anxr=w6oxRvGb&ie_hpr=-5&osDetail=6.3.1.sp0.x64&wx_tboff=0&c
03-13-2016 04:22:51		199.36.100.106	New York	NY	United States	tbapi.search.ask.com/v6/apnu/update?tb=OVO2-SP&cbid=^BAO&v=33
03-13-2016 03:14:05		65.52.108.27	Redmond	WA	United States	g.bing.com/GWX/GWX? ts=1457838808370&SQM=4195fb5ad069431a99d94a37c22905c7&GV FA5D-42c9-9DF0-014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/
03-13-2016 03:14:05		65.52.108.27	Redmond	WA	United States	g.bing.com/GWX/GWX? ts=1457838807980&SQM=4195fb5ad069431a99d94a37c22905c7&GV 014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/1.1
03-13-2016 00:54:55		93.184.215.59	Washington	DC	United States	cdn.pokki.com/pokki/platforms/version56e3af4771eed.exe HTTP/1.1
03-13-2016 00:48:19		74.113.233.187	White Plains	NY	United States	anx.apnanalytics.com/tr.gif?anxa=TBNotifier&tbnguid=829444A8-CF4 27&anxr=A8PsHV4W&ie_hpr=0&osDetail=10.0.1.sp0.x64&cr_ds=0&an
03-13-2016 00:44:37		65.52.108.27	Redmond	WA	United States	g.bing.com/GWX/GWX? ts=1457829892004&SQM=4e694025c3564ead844a9b51f4cace12&GV FA5D-42c9-9DF0-014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/
03-13-2016 00:44:36		65.52.108.27	Redmond	WA	United States	g.bing.com/GWX/GWX? ts=1457829891598&SQM=4e694025c3564ead844a9b51f4cace12&GV 014BE8F893FD%7D%5CAppName,GWX.exe,2 HTTP/1.1

splunk> .conf2017

Search Examples – IOCs



Search Examples – RSA Activity

DATE/TIME (UTC)	USER	ACTION	RESULT
03-13-2016 07:18:02		success	AUTHN_METHOD_SUCCESS
03-13-2016 07:12:36		success	AUTHN_METHOD_SUCCESS
03-13-2016 07:12:18		failure	AUTHN_METHOD_FAILED
03-13-2016 07:12:18		failure	AUTHN_METHOD_FAILED
03-13-2016 06:51:01		success	AUTHN_METHOD_SUCCESS
03-13-2016 06:36:43		success	AUTHN_METHOD_SUCCESS

RSA Activity includes PIN resets, token failures, and emergency backup PIN access

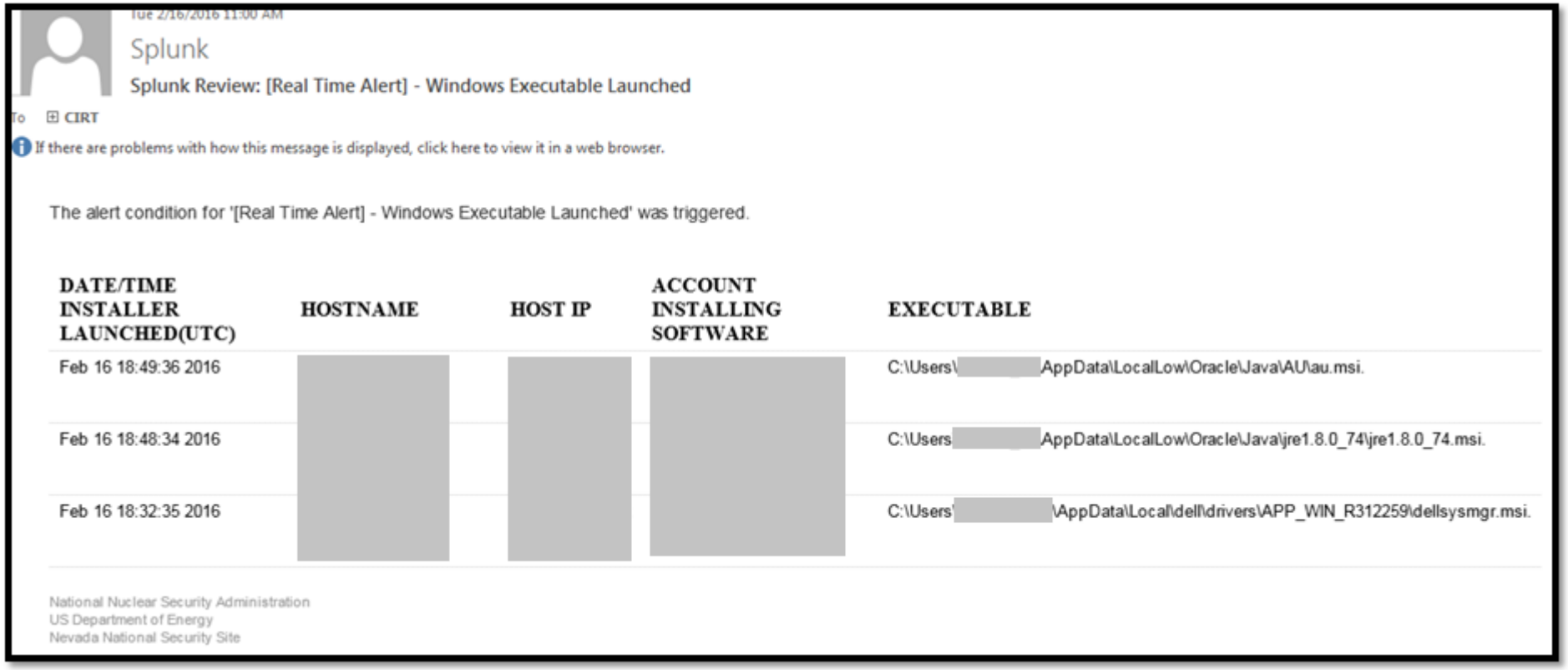
Search Examples – Process Execution

DATE/TIME (UTC)	HOSTNAME	DOMAIN	Avecto_description	SOFTWARE VERSION	PROCESS ID	PARENT PROCESS ID	HASH	COMMAND EXECUTED
Mar 13 07:53:22 2016			Task Scheduler Engine	6.1.7600.16385	4252	332	2D5A9FFAE8898BA67963290FC4E1DDF99DED5E2E	taskeng.exe {68819784-53C7-4 941922548-1860439328-29390
Mar 13 07:53:22 2016			Adobe Reader and Acrobat Manager	1.824.16.6751	7848	4252	7224E3586E6576C071A6141F3073A831734B08D4	"C:\Program Files (x86)\Comm
Mar 13 07:53:20 2016			Windows host process (Rundll32)	6.1.7600.16385	5464	5500	963B55ACC8C566876364716D5AAFA353995812A8	rundll32 C:\WINDOWS\system32\spool\ /pjob=29993 /pname"\\nts-ps2
Mar 13 07:53:19 2016			COM Surrogate	6.1.7600.16385	7128	848	E977B87698C3E595D55827665E22FBF788DD3F9F	C:\WINDOWS\system32\DllHos FF9B966D75B0}

This search identifies software, versions, PID, PPID, Hash values of executable, path, etc. This is used with a lookup table to identify new software and find malware based on path and hash

splunk> .conf2017

Splunk Alert Example



Tue 2/16/2016 11:00 AM

Splunk

Splunk Review: [Real Time Alert] - Windows Executable Launched

To ⊞ CIRT

If there are problems with how this message is displayed, click here to view it in a web browser.

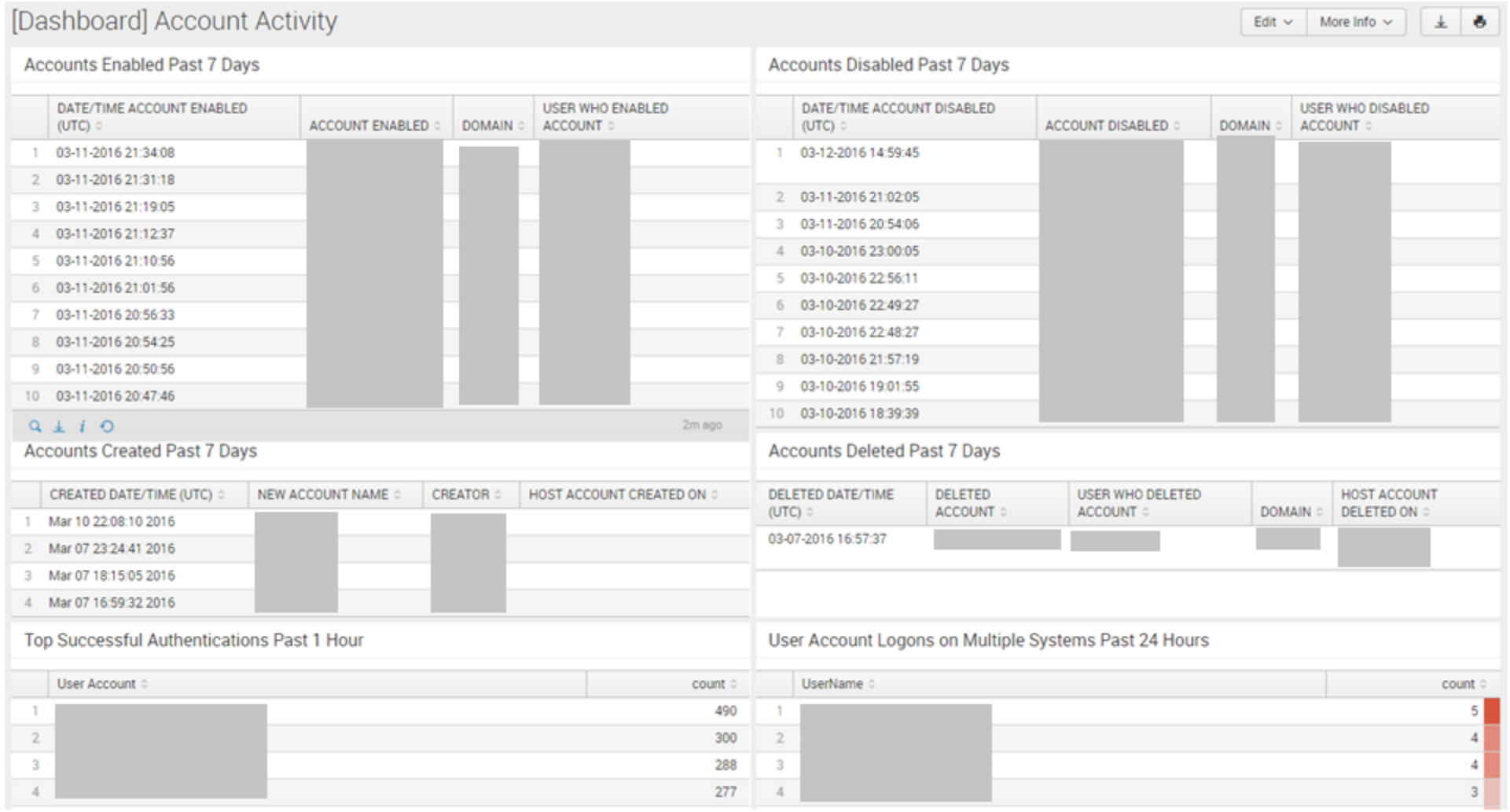
The alert condition for '[Real Time Alert] - Windows Executable Launched' was triggered.

DATE/TIME INSTALLER LAUNCHED(UTC)	HOSTNAME	HOST IP	ACCOUNT INSTALLING SOFTWARE	EXECUTABLE
Feb 16 18:49:36 2016				C:\Users\ AppData\LocalLow\Oracle\Java\AU\au.msi.
Feb 16 18:48:34 2016				C:\Users AppData\LocalLow\Oracle\Java\jre1.8.0_74\jre1.8.0_74.msi.
Feb 16 18:32:35 2016				C:\Users\ \AppData\Local\dell\drivers\APP_WIN_R312259\dellsysmgr.msi.

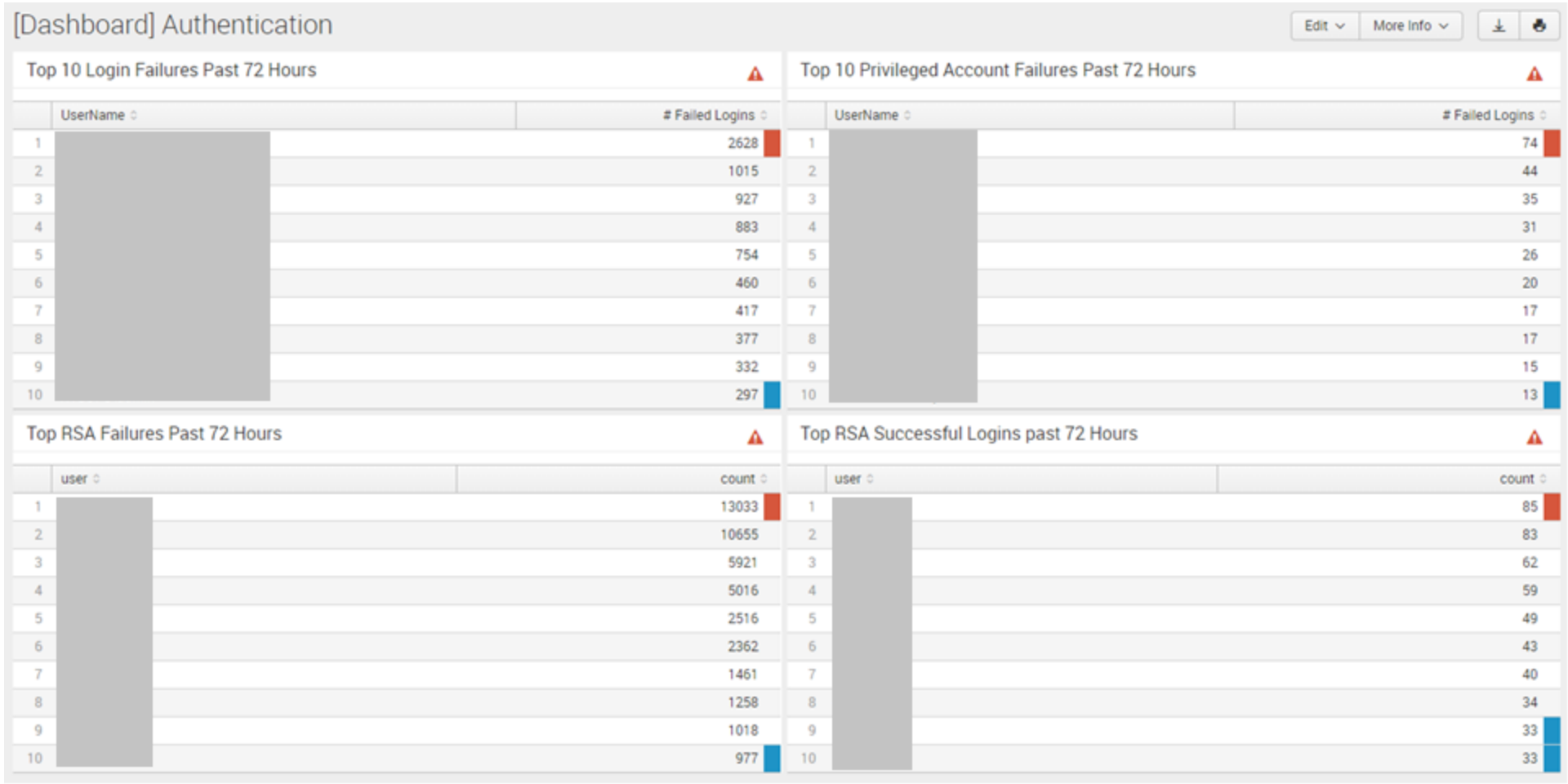
National Nuclear Security Administration
US Department of Energy
Nevada National Security Site

splunk> .conf2017

Account Activity Dashboard

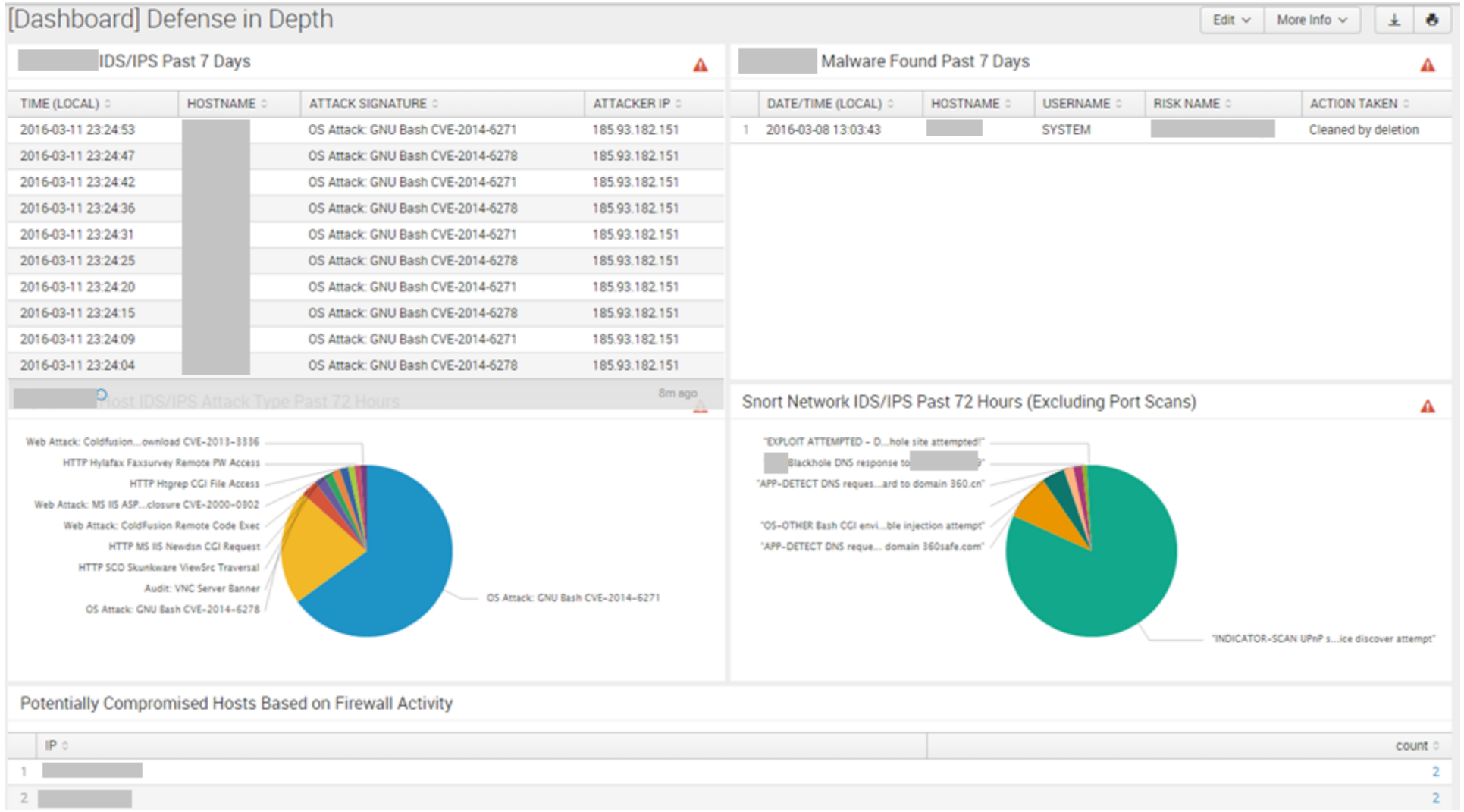


Authentication Dashboard



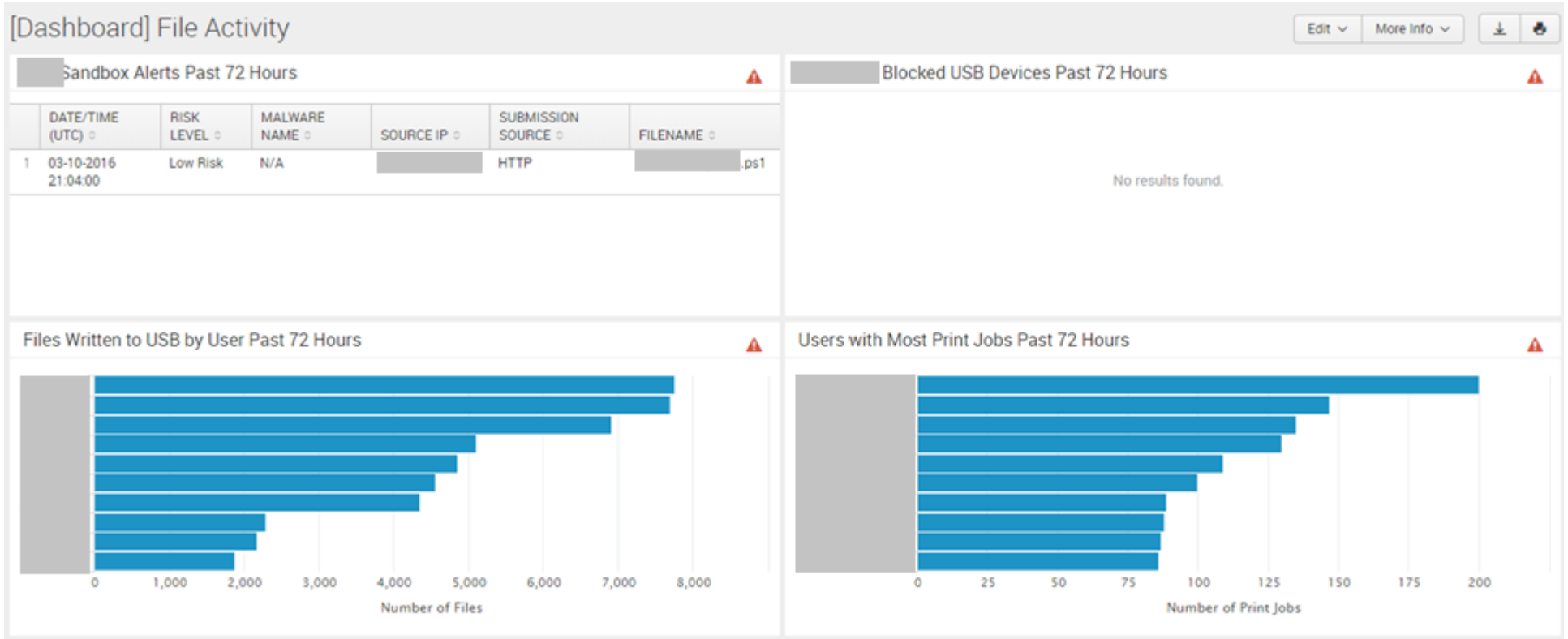
splunk> .conf2017

Defense in Depth Dashboard



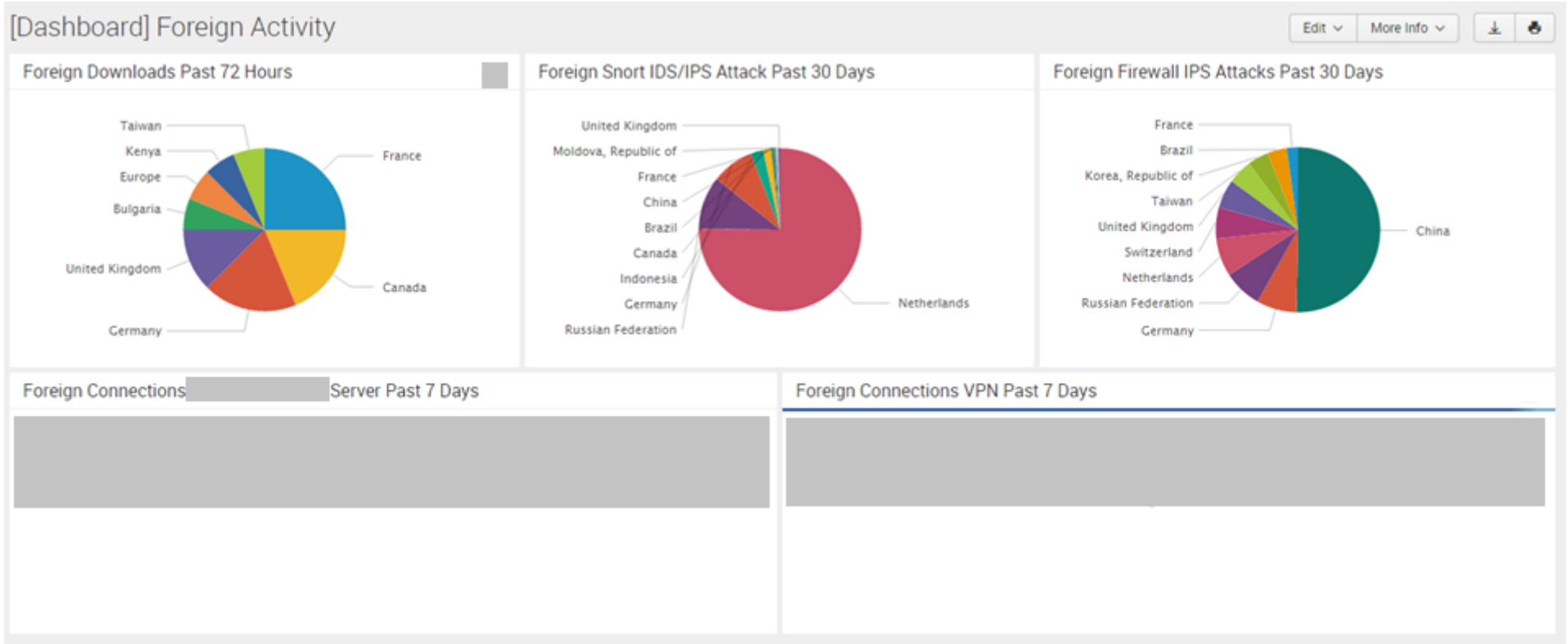
splunk> .conf2017

File Activity Dashboard

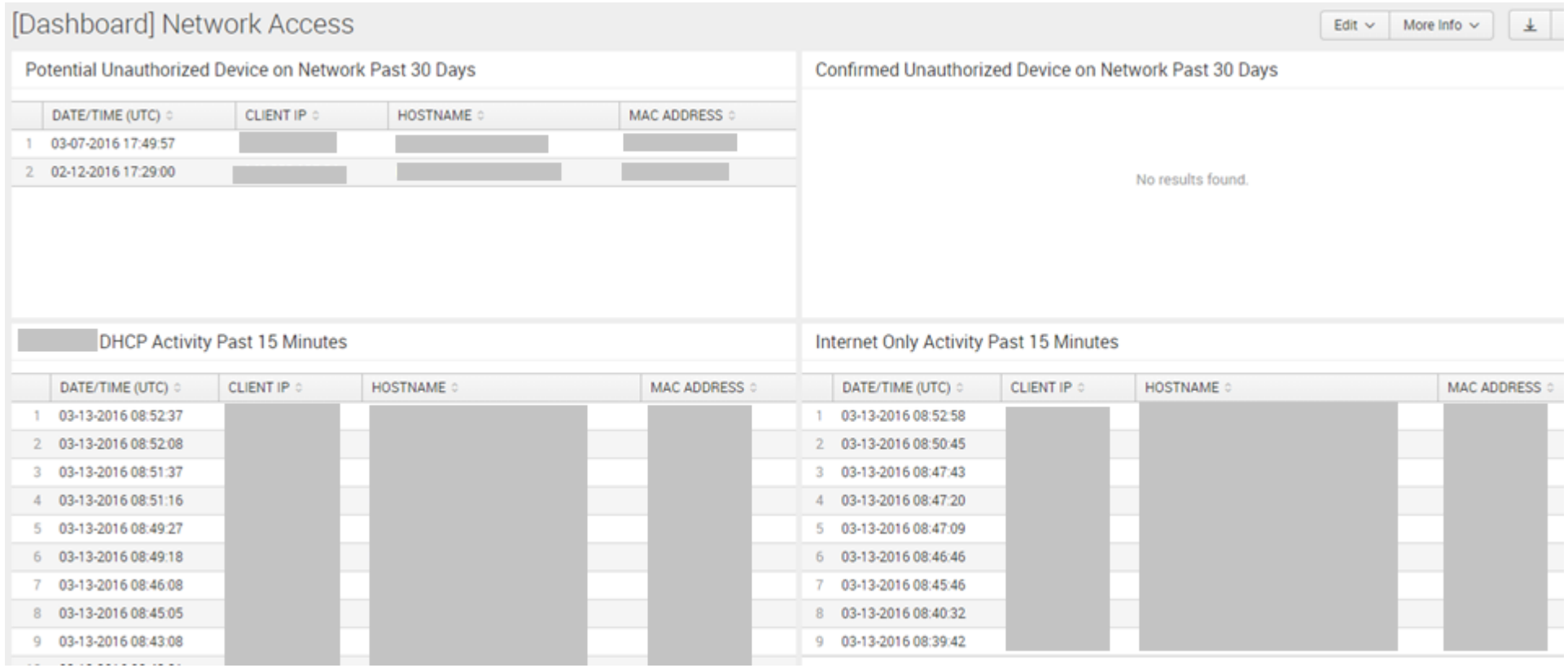


splunk> .conf2017

Foreign Activity Dashboard

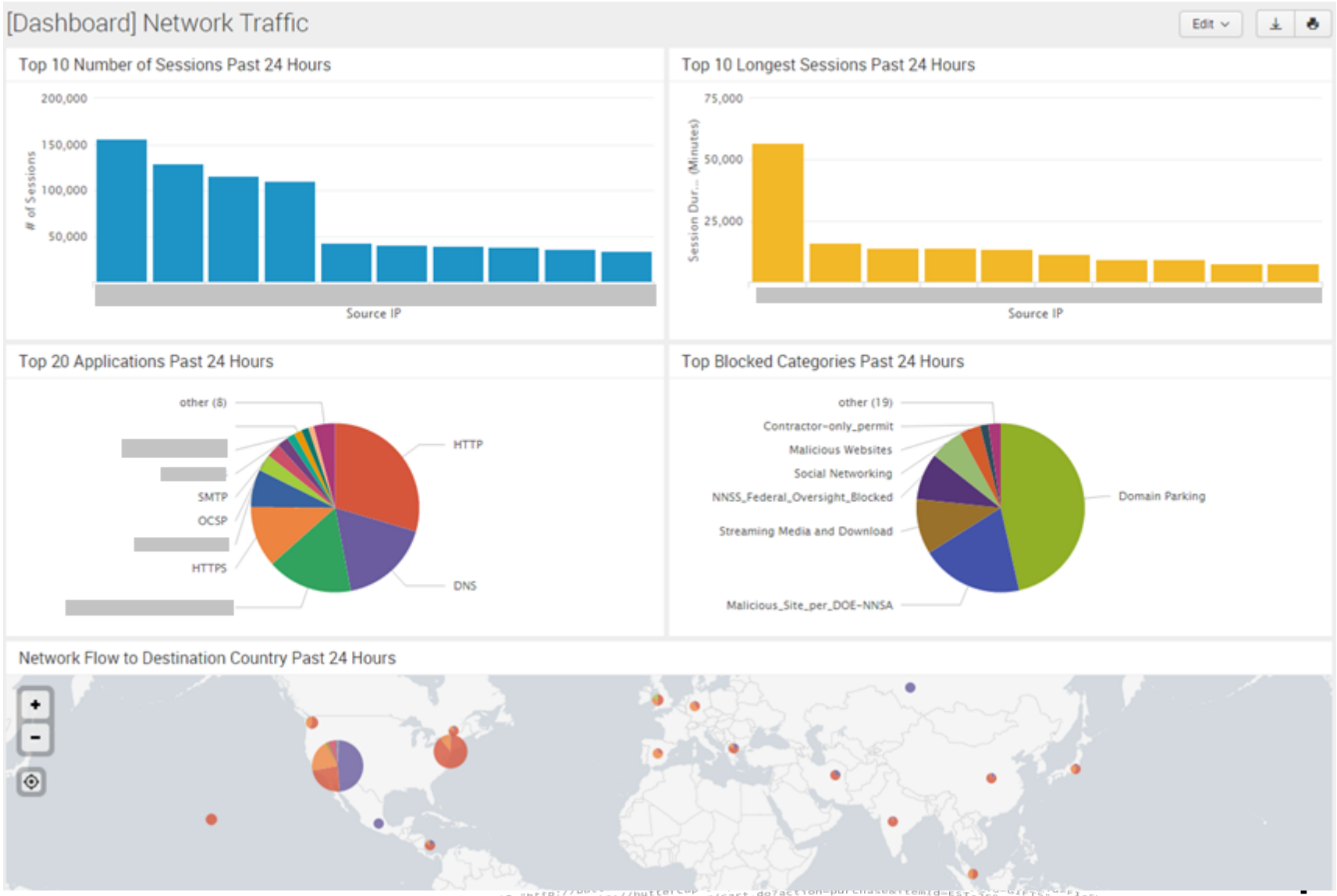


Network Access Dashboard



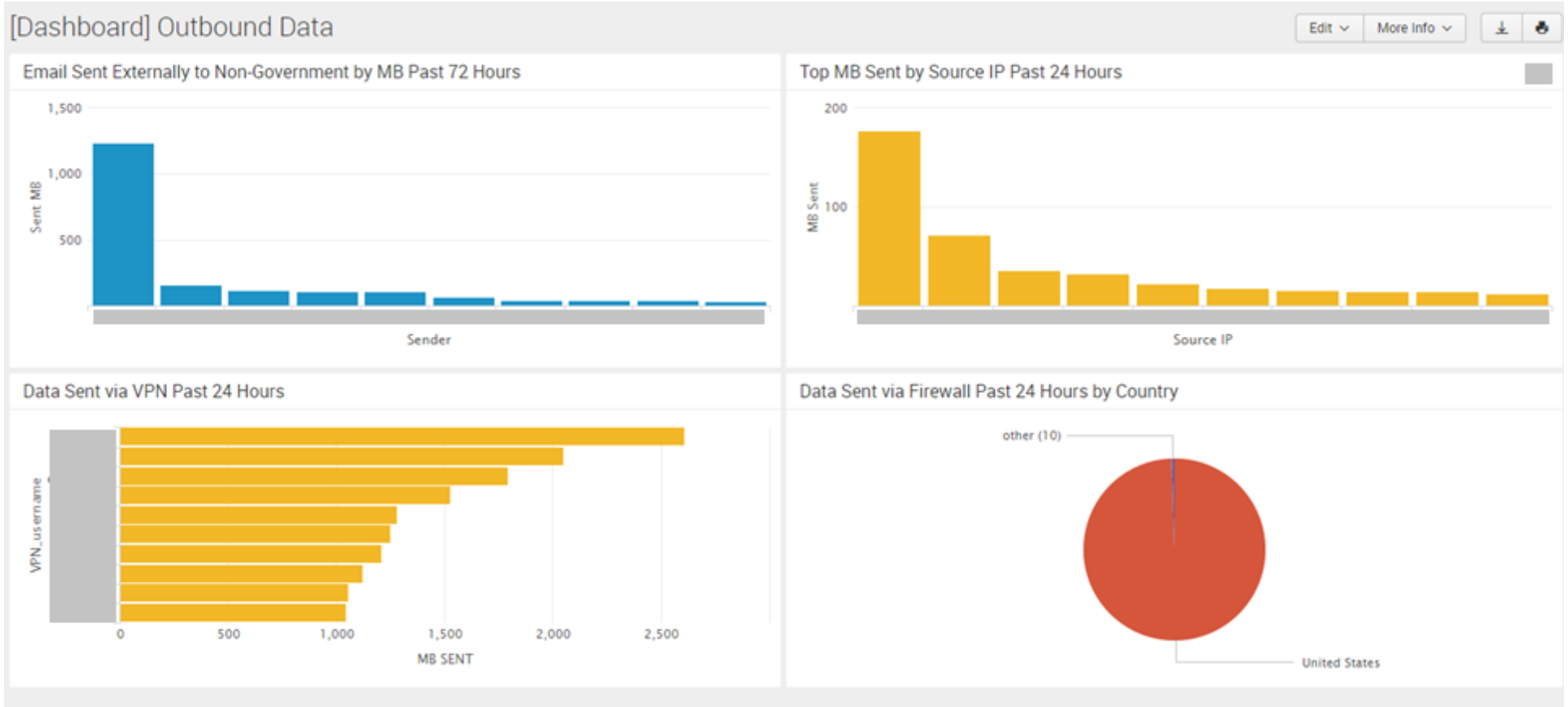
splunk> .conf2017

Network Traffic Dashboard



unk> .conf2017

Outbound Data Dashboard



Key Takeaways

1. Identify all of your logging sources
2. Identify what information from those sources can indicate malicious behavior
3. Prepare alerts and dashboards based upon those indicators
4. Prepare and save searches for repetitive, common searches
5. ACT ON THE INFORMATION!!!!