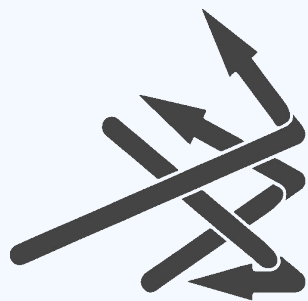




**UNDER  
DEFENSE**  
CyberSecurity Solutions  
Protecting your business

**splunk**>



**Catch them!**

**Splunk Secrets to Detect Attackers**



# Agenda

1. Splunk As **Google** for (un)structured data
2. AD infrastructure monitoring
3. IT Service Intelligence
4. Cloud monitoring
5. PCI DSS monitoring
6. Know your Defense Arsenal: Splunk for Layered Security
7. Practical Example: 30 minutes in the Life of security analyst
8. Hands-On Workshop

# splunk>partner+

UnderDefense is [Splunk partner](#) and our team is holding the following Splunk certifications:

- Splunk Certified Consultant I
- Splunk architect
- Splunk Administrator
- Splunk Power User
- Splunk Sales engineer 1
- Splunk User
- Splunk Sales Rep 1
- Splunk Sales Rep 2
- Splunk Sales IT & App
- Splunk UBA User



# Trusted security professionals

ISO-27001  
Lead Auditor

Ph.D. in Security





# Recognitions, Awards & Partnerships



<https://www.owasp.org/index.php/Lviv>



## Awards

1. [Cybersecurity Educator of the Year - EMEA 2017](#),
2. [Cybersecurity Consultant of the Year 2016](#)



# Winners of Competition in 2018

**SecOps**  
**EUROPE** **2018**

International  
Exercise  
& Conference  
on Security  
Operations



15 Leaders

Reviews

Leaders Matrix

<https://clutch.co/it-services/cybersecurity/leaders-matrix>



## Clutch Leaders Matrix

Rollover to see company insights or click a company below for more details.

584 Firms

- 1 ELEKS
- 2 RiskIQ
- 3 FRSecure
- 4 UnderDefense
- 5 RiskVision
- 6 Fluid Attacks
- 7 A1QA
- 8 Switchfast Technologies
- 9 Fidelis Cybersecurity
- 10 TechMD
- 11 The Vietnam Security Network
- 12 Berezha Security
- 13 UkrInSoT
- 14 TestArmy
- 15 OnDefend





Attackers

VS.

Defenders

**TRUE SECURITY NEED PRACTICE**

- **Process**
- **People**
- **Tools**

# UnderDefense SOC



“Incident Response needs people, because successful Incident Response requires thinking.”  
— Bruce Schneier



Security is not from Mon-Fri 8 hours job. Hackers don't sleep. It's 24x7x365 eyes on target. 24x7x365 readiness to detect and block new threat. Today excellent and experienced security professionals are hard to find on the market.



Proactively Detect & Stop attacker before he get into the network. Modern business require really quick reaction on Security Incidents



Evolving Compliance and Regulatory Requirement increase responsibility and penalties for failure with Security Program and user data leakage.



Lack of in-house highly skilled security professionals in very high

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (December 2017)



# Why Splunk?

## General causes

- Turn Machine Data Into Answers
- **Analytics** Platform
- Monitor service health
- Log **collection**
- Conduct **investigations**
- Detect malicious actions and malware
- Detect ransomware source
- **Reconstruct** events
- **Anomalies** detection

## Client's specific causes

- Compliance
- Security Monitoring
- Fraud Detection
- Get visibility on organization from security perspective
- Response to Incidents
- Understand problem root cause
- Log collection
- Data visualization/analytics
- Product performance monitoring

# Splunk Portfolio + acquisitions (e.g. Voice control)



Search and Investigate



Dashboards and Reports



Incident & Breach Response



Monitoring & Alerting



Threat Detection



Security Operations



Automation & Orchestration



Discover Anomalous Behavior

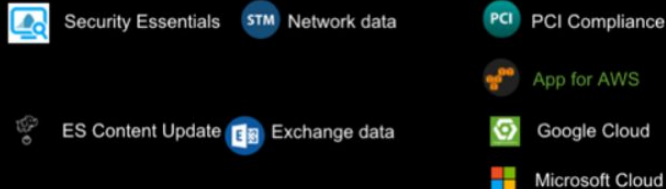


Detect Unknown Threats

## 3<sup>rd</sup> Party Apps & Add-ons (700+)



## Splunk Security Apps & Add-ons



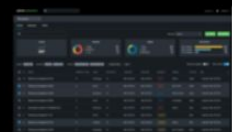
## Premium Solutions



Enterprise Security



User Behavior Analytics



Phantom

# DIFFERENTIATORS



Splunk Enterprise  
Security™

## Technology Approach

## Competitors



Big Data, extensible platform



Integrated user behavior & machine learning  
analytics



End-to-end visibility using all machine data



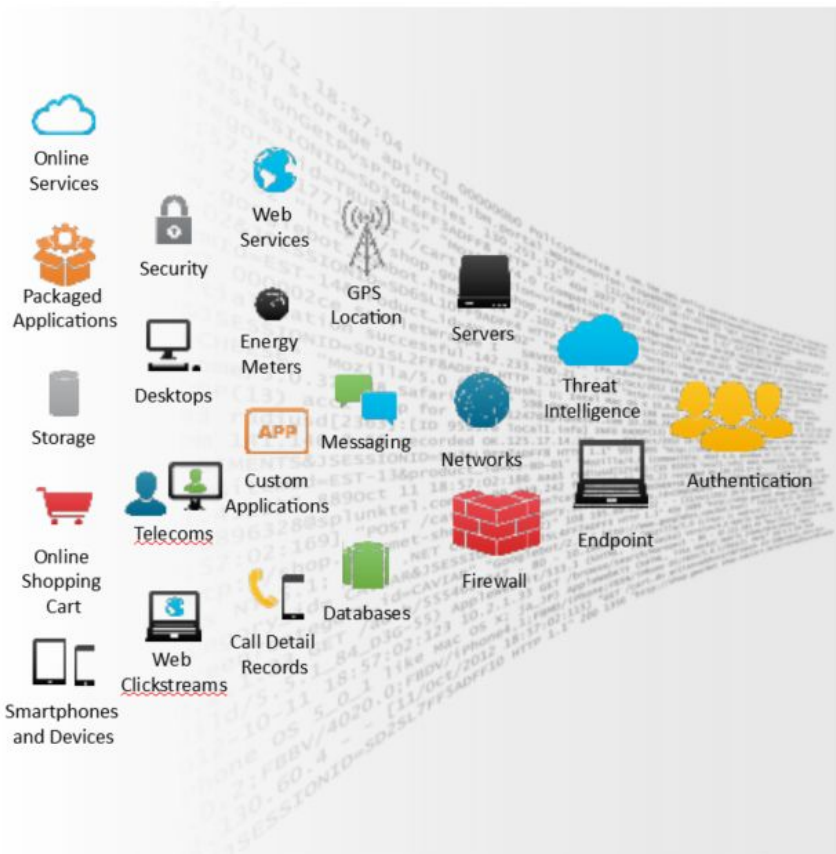
Single solution to detect, investigate and  
respond



Support for a wide range of security use cases



# You can monitor almost everything



**Ad hoc search**



**Monitor and alert**



**Report and analyze**



**Custom dashboards**



**Developer Platform**

**splunk**



**External Lookups**

**Asset & CMDB**



**Employee Info**



**Threat Intelligence**



**Applications**



**Data Stores**



**Key Features**

Performance, Scale, and Manageability

- SmartStore**  
Scale to exponentially growing volumes of machine data by scaling compute and storage independently, while achieving high availability, longer data retention and significant TCO reduction.
- Workload Manager**  
Policy-based management resources for critical workloads, ensuring optimal resource handling to meet business needs.
- Splunk on Docker Support**  
Easily scale Splunk deployments on containers in their culture while lowering the total cost of ownership.
- Splunk Cloud Active Archive**  
Ready and use-it data for only for regulatory and compliance, CI


>  Splunk Built


## Splunk Essentials for Cloud and Enterprise 7.2


Release 7.2 is the latest version of Splunk Enterprise and Splunk Cloud. We have developed an app to guide you through the powerful new features. This is not an in-depth tutorial, rather a guide to help you understand the new

> Splunk Essentials for

 Palo Alto Networks App

 Splunk ES Content Update

 Splunk App for AWS

 Splunk Machine Learning Toolkit

### Browse by Category



**DevOps**  
108 Apps



**Security, Fraud & Compliance**  
850 Apps



**IT Operations**  
876 Apps



**Utilities**  
673 Apps



**Business Analytics**  
129 Apps



**IoT & Industrial Data**  
112 Apps

# Splunk for Application Delivery

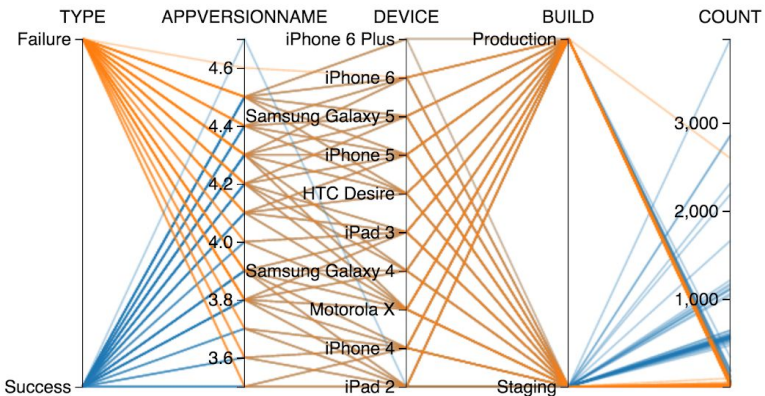
Edit ▾ More Info ▾  

## Dev - Builds

**312** Errors **1,827** Errors

IN STAGING IN PRODUCTION

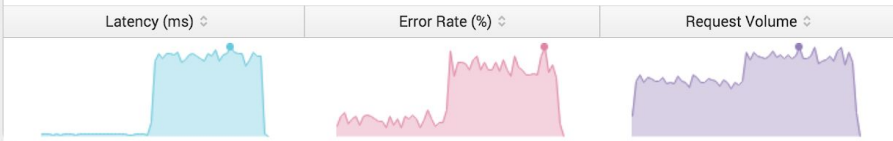
Choose a View: [Dev Errors Parallel Coordinates](#) [Dev Errors Stacked Chart](#) [Hide All](#)




### Latest Commits

user ▾	priority ▾	message ▾	repo ▾	created ▾	type ▾
billy	low	My first production commit as an intern!	acme	1442442551	commit
david	low	Fueled by grape soda.	acme	1442444201	commit
david	low	What could go wrong?.	acme	1442444218	commit
david	low	I love Sublime	acme	1442443855	commit

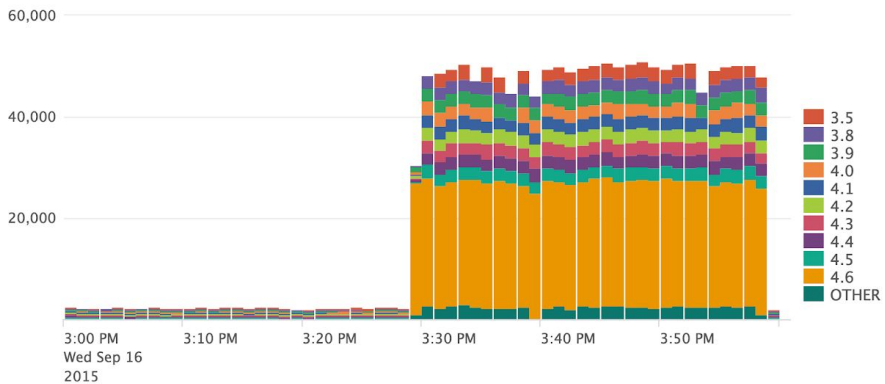
## Ops - Performance



Select Split-by Field

App Version  ▾

Mobile Performance Views: [Latency \(ms\)](#) [Request Volume](#) [Error Rate \(%\)](#) [Hide All](#)



userIdentifier ▾	url ▾	Country ▾	Connection ▾	Version ▾	Platform ▾	Device ▾	Latency ▾
hax0r	/search/=1 AND (SELECT * FROM hr_employee_info)	North Korea	WIFI	4.6	iOS	iPhone 6	25000.469349
hax0r	/search/  (SELECT password FROM	North Korea	WIFI	4.6	iOS	iPhone 6	24738.945402



# Performance Monitoring

Edit | Export | ...

Perfmon Hosts | Perfmon Hosts (text search) | All x | \* | Last 15 minutes | Hide Filters

Instance: All | Counter: % C1 Time

## CPU Metrics

Host	Trend	Average	Peak	Current	Last Updated
coredev-002		23.00	23.00	23.00	11/07/2018 18:26:54.486
WIN-6LR3JNJ6LVD		17.23	23.70	16.88	11/07/2018 18:40:01.911
busdev-002		15.00	15.00	15.00	11/07/2018 18:35:11.486
coredev-006		13.00	13.00	13.00	11/07/2018 18:30:01.486
acme-005		8.00	8.00	8.00	11/07/2018 18:30:51.486
ops-sys-004		8.00	8.00	8.00	11/07/2018 18:36:57.486

Instance: All | Counter: % Disk Read Time

## PhysicalDisk Metrics

Host	Trend	Average	Peak	Current	Last Updated
prod-mfs-003		96.00	96.00	96.00	11/07/2018 18:32:56.170
busdev-003		93.00	93.00	93.00	11/07/2018 18:38:19.170
coredev-001		65.50	96.00	92.00	11/07/2018 18:34:37.170
coredev-006		78.50	92.00	92.00	11/07/2018 18:30:55.170
prod-mfs-006		92.00	92.00	92.00	11/07/2018 18:30:24.170
exch-mbx-den-00-b		52.20	90.00	90.00	11/07/2018 18:40:29.170
exch-mbx-pla-00-a		68.40	88.00	88.00	11/07/2018 18:40:29.170
exch-mbx-den-01-a		70.40	87.00	87.00	11/07/2018 18:40:29.170
exch-mbx-den-01-b		58.80	88.00	87.00	11/07/2018 18:40:29.170

Instance: All | Counter: Bytes Received/sec

## Network Metrics

Host	Trend	Average	Peak	Current	Last Updated
exch-mbx-pla-00-a		174234.86	196721.00	196721.00	11/07/2018 18:39:29.170
exch-mbx-cup-00-b		107965.00	191851.00	191851.00	11/07/2018 18:39:29.071
exch-mbx-cup-00		88190.58	194387.00	188936.00	11/07/2018 18:39:29.170
exch-mbx-cup-00-a		58972.57	185357.00	185357.00	11/07/2018 18:39:29.071
exch-hub-pla-01		117622.00	183436.00	157743.00	11/07/2018 18:39:29.170
exch-mbx-pla-01		93935.43	148837.00	148837.00	11/07/2018 18:39:29.170
exch-mbx-pla-00		85317.14	153144.00	147990.00	11/07/2018 18:39:29.170
exch-mbx-den-00-a		103633.13	188547.00	147933.00	11/07/2018 18:39:29.071
exch2010		118555.71	194308.00	139462.00	11/07/2018 18:39:29.170
exch-hub-cup-01		124994.71	168083.00	138335.00	11/07/2018 18:39:29.071

Counter: %Committed Bytes In Use

## Memory Metrics

Host	Trend	Average	Peak	Current	Last Updated
prod-pos-002		8798521.00	8798521.00	8798521.00	11/07/2018 18:37:25.498
ops-sys-006		7308801.00	8072430.00	8072430.00	11/07/2018 18:35:55.498
host0201		6064548.00	6064548.00	6064548.00	11/07/2018 18:31:04.498
same-ad		4811041.00	6028829.00	6028829.00	11/07/2018 18:31:24.498
prod-pos-006		5870547.00	5870547.00	5870547.00	11/07/2018 18:30:16.498
busdev-003		5291116.00	5291116.00	5291116.00	11/07/2018 18:35:35.498
same-ad3		5007527.00	5007527.00	5007527.00	11/07/2018 18:28:52.498
busdev-002		4659425.00	4659425.00	4659425.00	11/07/2018 18:31:55.498
host-001		4063195.00	4063195.00	4063195.00	11/07/2018 18:34:59.498
coredev-002		3360937.00	3360937.00	3360937.00	11/07/2018 18:26:56.498



# Windows Update

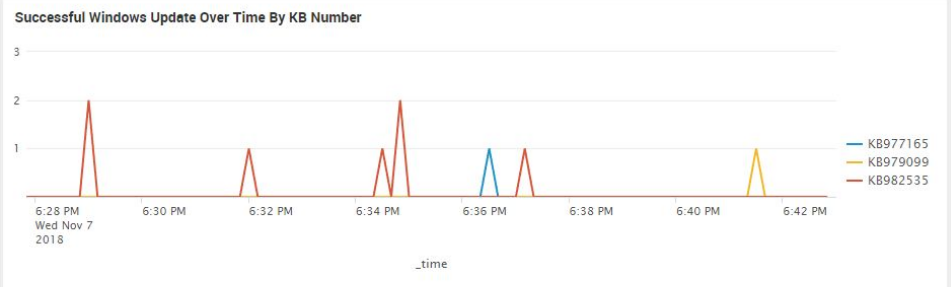
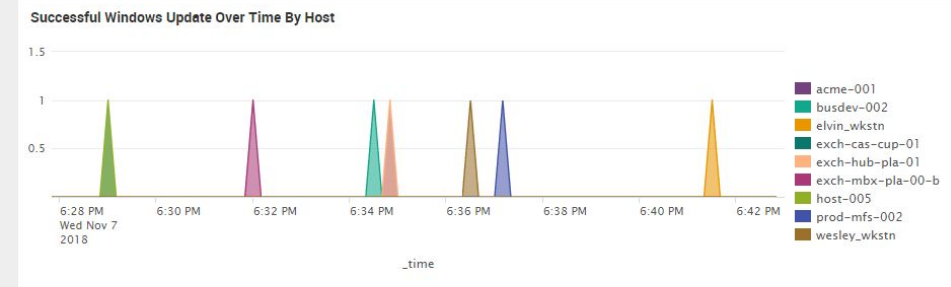
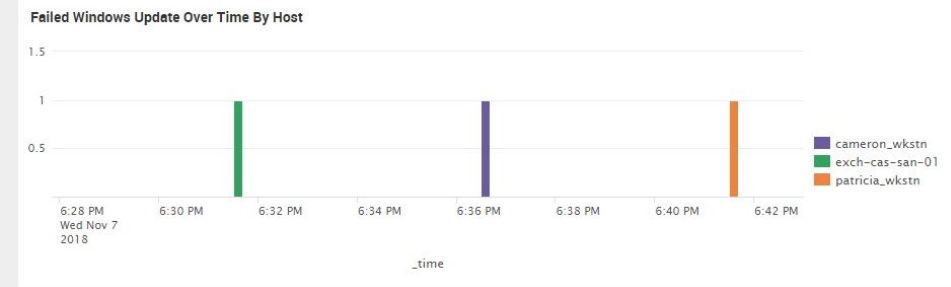
Edit Export ...

Event Host

All

Last 15 minutes

Hide Filters



### Failed Windows Update By Host

host	Trend	count
cameron_wkstn		1
exch-cas-san-01		1
patricia_wkstn		1

### Failed Windows Update By KB Number

package_title	Trend	count
"Security Update for Windows Server 2008 x64 Edition (KB975560)";		1
"Security Update for Windows Server 2008 x64 Edition (KB979482)";		1
"Update for Internet Explorer 8 Compatibility View List for Windows Server 2008 x64 Edition (KB978506)";		1

### Successful Windows Update By Host

### Successful Windows Update By KB Number

## Active Directory Overview

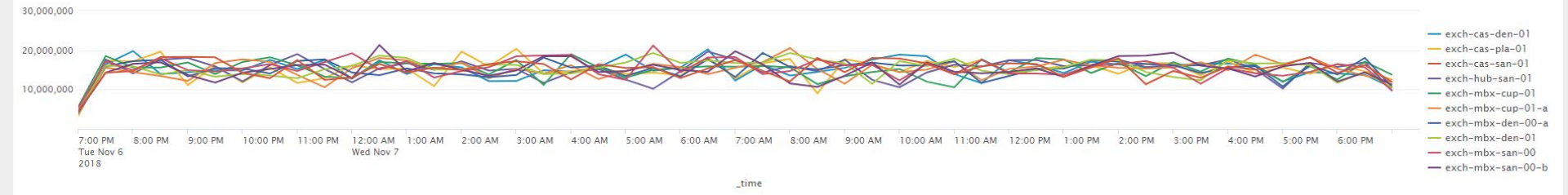
Edit Export ▾ ...

Forest:  Site:  Domain:  Server:  Last 15 minutes ▾ Hide Filters

### Topology Report

Host ▾	Enabled ▾	Site ▾	Operating System ▾	Version ▾	Master Roles ▾	Global Catalog ▾	RODC ▾	Services ▾	DNS Registration ▾	SYSVOL Shared ▾
same-ad	✓	Default-First-Site-Name	Windows Server 2008 R2 Datacenter	6.1 (7601)	Schema DomainNaming PDCEmulator RIDMaster Infrastructure	✓	✗	✓	✓	✓
same-ad3	✓	Default-Second-Site-Name	Windows Server 2008 R2 Datacenter	6.1 (7601)	Schema DomainNaming PDCEmulator RIDMaster Infrastructure	✓	✗		✓	
127.0.0.1	✓	Default-First-Site-Name	Windows Server 2012 R2 Datacenter Evaluation	6.3 (9600)	Schema DomainNaming PDCEmulator RIDMaster Infrastructure	✓	✗	✓	✓	✓

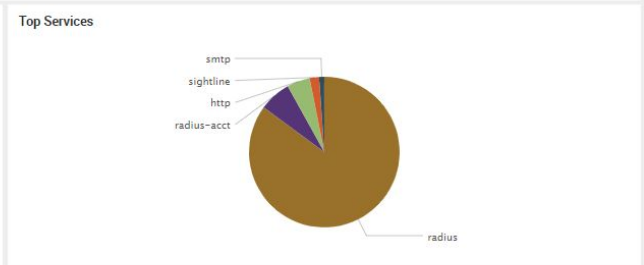
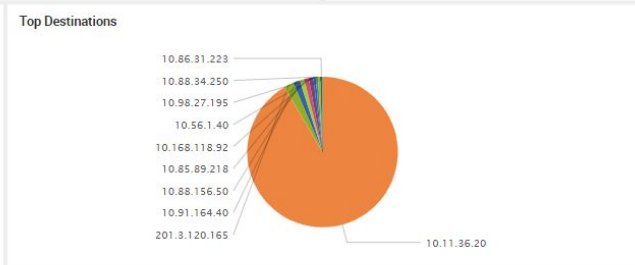
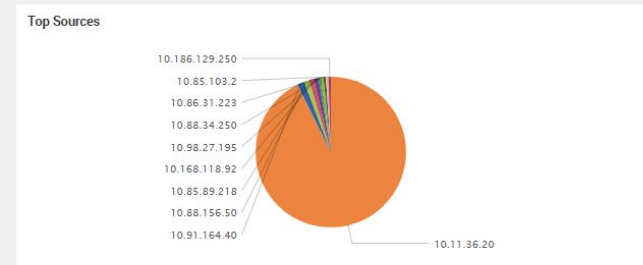
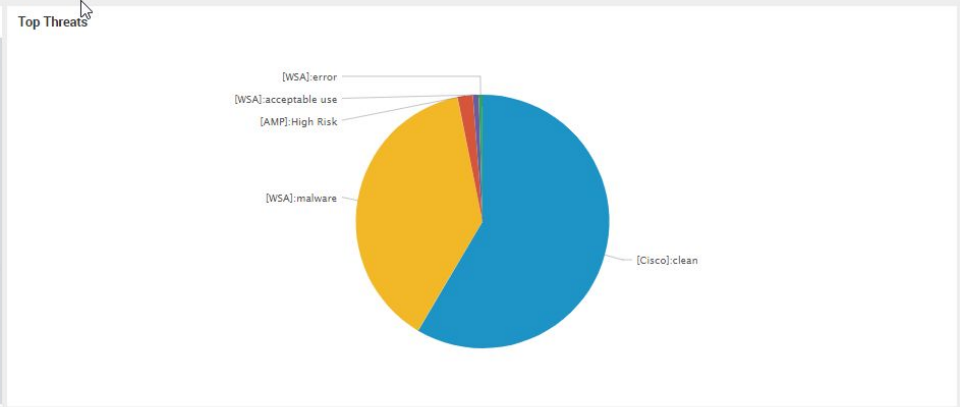
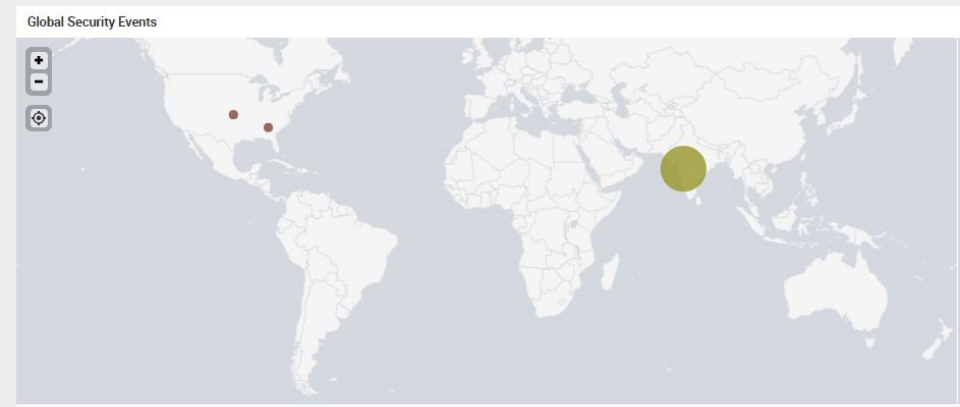
### All Hosts Memory



# Cisco Security Overview

Your dashboard for all things Cisco... Security.

Export ...



### Security Event Statistics by Sourcetype

rank	sourcetype	count	Trend
1	Cisco:ISE:Syslog	65688	
2	cisco:esa	16084	
3	cisco:fwsm	1084	
4	cisco:asa	1044	
5	cisco:wsa:squid	892	
6	cisco:wsa:squid copy-too_small	890	
7	@streamer	67	

### Security Event Statistics by Host

rank	host	count	Trend
1	127.0.0.1	81804	
2	ch-demo-cisco.hod.cloud	4000	

# ISE User Investigation

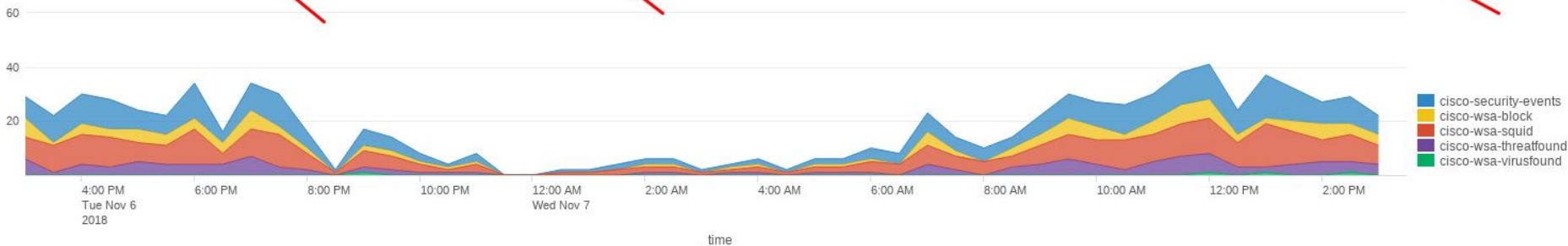
Export | ...

Username:  Client IP:  Last 24 hours  [Hide Filters](#)

## User Information

FirstName	LastName	SystemName	Location	UserGroup	latest(PostureStatus)	latest(OperatingSystem)	latest(AntiVirusInstalled)	latest(AntiSpywareInstalled)	latestLocation	Control
Josef	Martinez	JMartinez-W764	SJ	IT Admins	Compliant	Windows 7 64	McAfeeAV	Windows Defender	San Jose CA	Quarantine
		JMiPhone5s			Compliant	iOS7.2	Lookout 2.3.2		San Jose CA	Quarantine
		JMiPad			Unknown	iOS7.2	Lookout 2.3.1		Hong Kong	Quarantine

## Network Utilization



## ISE User Investigation

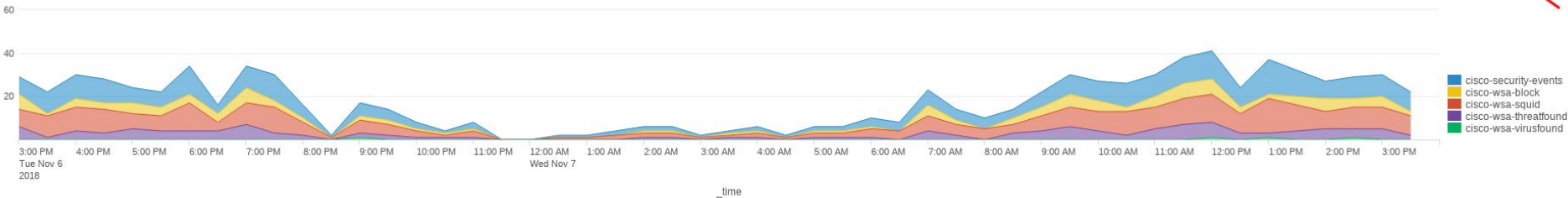
Export | ...

Username:  Client IP:  Last 24 hours  [Hide Filters](#)

### User Information

FirstName	LastName	SystemName	Location	UserGroup	latest(PostureStatus)	latest(OperatingSystem)	latest(AntiVirusInstalled)	latest(AntiSpywareInstalled)	latestLocation	Control
Josef	Martinez	JMartinez-W764	SJ	IT Admins	Compliant	Windows 7 64	McAfeeAV	Windows Defender	San Jose CA	Locked
		JMiPhone5s			Compliant	iOS7.2	Lookout 2.3.2		San Jose CA	Locked
		JMiPad			Unknown	iOS7.2	Lookout 2.3.1		Hong Kong	Locked

### Network Utilization



### Username in Use

_time	Username
2018-11-07 15:49:06.166	<u>josef@demo.com</u>

### Threat Count

X-ThreatName	count
Trojan-Backdoor-Zbot	7
Trojan-Downloader.Gen	4
Unknown	11
Virus-Otwyca1	8
zhongsou zstoolbar	4

### External Traffic

dest_ip	count
<u>201.3.120.165</u>	176
74.55.85.122	10
164.109.50.111	3
174.129.97.79	3
194.150.231.55	3
67.20.106.129	3
72.21.91.13	3
72.52.222.117	3
169.207.67.12	2
184.168.221.79	2

### Internal Traffic

src_ip	SrcUserName	dest_ip	dest_user	count
10.2.3.4	josef	10.120.208.207	alfonso	6
10.2.3.4	josef	10.120.109.82	hollis	2
10.2.3.4	josef	10.120.12.226	angela	2
10.2.3.4	josef	10.120.137.110	rodger	2
10.2.3.4	josef	10.120.220.21	jordan	2
10.2.3.4	josef	10.120.251.250		2
10.2.3.4	josef	10.105.159.56	blake	1

### Top 10 Destination Domains

dest_ip	dest_domain	count
<u>201.3.120.165</u>	<u>damtare.by.ru</u>	62
201.3.120.165	er18.com	43
201.3.120.165	zhongsou.com	16
201.3.120.165	lyred.com	15
201.3.120.165	mymailsignature.com	15
201.3.120.165	201.3.120.165	14
201.3.120.165	bewfsnfwka.net	11
74.55.85.122	fftoday.com	7
164.109.50.111	cosmogirl.com	3
174.129.97.79	thenewsroom.com	3

### IP Addresses in Use

_time	Client IP
2018-11-07 15:49:06.166	172.20.16.106
2018-11-07 15:49:06.166	172.20.14.157
2018-11-07 15:44:27.830	172.20.16.112
2018-11-07 15:41:18.635	172.20.16.111
2018-11-07 15:40:31.570	172.20.16.112
2018-11-07 15:38:46.431	172.20.12.136
2018-11-07 15:36:21.304	172.20.16.120
2018-11-07 15:35:11.239	172.20.14.153
2018-11-07 15:32:32.134	172.20.14.159
2018-11-07 15:23:57.515	172.20.16.116

### Top 10 Web Categories

Category	count	percent
Unknown	109	36.333333
Society and Culture	67	22.333333
Shopping	17	5.666667
Computers and Internet	17	5.666667
Advertisements	16	5.333333
Sports and Recreation	13	4.333333
Arts	11	3.666667
Business and Industry	9	3.000000
News	7	2.333333
Health and Nutrition	6	2.000000



# Profile an IP

Export [ ]

IP Address

Sourcetype

201.3.120.165

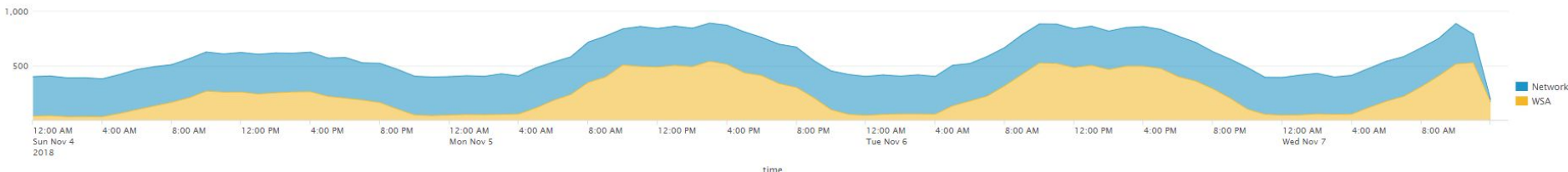
\* [ ]

Last 3 days [ ]

Submit

Hide Filters

## Product Usage: \* / 201.3.120.165



## Events: \* / 201.3.120.165

#	Time	Event
>	11/7/18 12:18:47.920 PM	1541593127.920440 327 172.20.16.113 TCP_DENIED/403 1921 GET http://sdelaem.cn/ZsC/cfg.bin "josef@demo.com" NONE/- - BLOCK_AWQ-REQ-DefaultGroup-Demo_Clients-NONE-NONE-NONE-NONE <nc,-9,23,"Trojan-Backdoor-Zbot",100,12714,582243,...,nc,-> - "Opera/7.50 (Windows XP; U)" - "Unknown" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:45.920 PM	1541593125.920440 486 172.20.10.229 TCP_DENIED/403 1893 GET http://www.mymailsignature.com/"zachary@demo.com" NONE/- - BLOCK_AWQ-REQ-DefaultGroup-Demo_Clients-NONE-NONE-NONE-NONE <IW_comp,-7,9,13,"Unknown",100,11269,37876,...,IW_comp,-> - "Mozilla/5.0 (iPad; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.10" - "Computers and Internet" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:40.920 PM	1541593120.920440 16922 172.20.12.182 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt "lamont@demo.com" DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-NONE-DefaultRouting <IW_scty,-6,9,0,...,IW_scty,-> - "Mozilla/5.0 (Linux; U; Android 1.5; de-de; Galaxy Build/CUPCAKE) AppleWebKit/528.5 (KHTML, like Gecko) Version/3.1.2 Mobile Safari/525.20.1" - "Society and Culture" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:33.920 PM	1541593113.920440 486 172.20.12.72 TCP_DENIED/403 1893 GET http://www.mymailsignature.com/"clark@demo.com" NONE/- - BLOCK_AWQ-REQ-DefaultGroup-Demo_Clients-NONE-NONE-NONE-NONE <IW_comp,-7,9,13,"Unknown",100,11269,37876,...,IW_comp,-> - "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; Trident/7.0; .NET4.0E; .NET4.0C) - "Computers and Internet" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:29.920 PM	1541593109.920440 16922 172.20.11.93 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt "christian@demo.com" DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-NONE-DefaultRouting <IW_scty,-6,9,0,...,IW_scty,-> - "Mozilla/5.0 (Maemo; Linux armv7l; rv:10.0.1) Gecko/20100101 Firefox/10.0.1 Fennec/10.0.1" - "Society and Culture" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:29.920 PM	1541593109.920440 93 172.20.14.231 TCP_DENIED/403 1873 GET http://www.lyred.com/"augustus@demo.com" NONE/- - BLOCK_AWQ-REQ-DefaultGroup-Demo_Clients-NONE-NONE-NONE-NONE <IW_adv,-7,13,"Unknown",100,11269,37782,...,IW_adv,-> - "Mozilla/5.0 (compatible; Koleror/3.3; Linux 2.6.8-gentoo-r3; X11; " - "Advertisements" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:10.920 PM	1541593090.920440 16922 172.20.12.205 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt "royce@demo.com" DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-NONE-DefaultRouting <IW_scty,-6,9,0,...,IW_scty,-> - "Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; en) AppleWebKit/534.1 (KHTML, like Gecko) Version/6.0.0.141 Mobile Safari/534.1" - "Society and Culture" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:18:06.920 PM	1541593086.920440 110 172.20.12.117 TCP_DENIED/403 1901 GET http://444.er18.com/config.txt "alonzo@demo.com" NONE/- - BLOCK_AWQ-REQ-DefaultGroup-Demo_Clients-NONE-NONE-NONE-NONE <nc,-7,1,25,"Virus-Otwycal",100,15453,405880,...,nc,-> - "Mozilla/5.0 (Macintosh; PPC Mac OS X; en) AppleWebKit/125.2 (KHTML, like Gecko) Safari/125.8" - "Unknown" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid
>	11/7/18 12:17:51.920 PM	1541593071.920440 16922 172.20.12.178 TCP_REFRESH_HIT/200 474 GET http://damtare.by.ru/id.txt "emanuel@demo.com" DIRECT/damtare.by.ru text/html DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-NONE-DefaultRouting <IW_scty,-6,9,0,...,IW_scty,-> - "Mozilla/5.0 (BB10; Touch) AppleWebKit/537.10- (KHTML, like Gecko) Version/10.1.0.2342 Mobile Safari/537.10" - "Society and Culture" 201.3.120.165 host = ch-demo-cisco.hod.cloud source = /four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid sourcetype = cisco.wsa.squid



Q New Search Save As Close

sourcetype=\*\*\* (src\_ip=201.3.120.165 OR dest\_ip=201.3.120.165) | eval product=case(sourcetypes="Network:Generic","Network",sourcetypes="cisco.wsa:squid","WSA") | search product=WSA Date time range

20,058 events (11/4/18 12:00:00.000 AM to 11/7/18 12:18:52.000 PM) No Event Sampling Job Visualization

Events (20,058) Patterns Statistics Visualization

Format Timeline Zoom Out CS\_username 1 hour per column

>100 Values, 100% of events Selected Yes No

Reports Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
josef@demo.com	482	2.403%
elliott@demo.com	27	0.135%
eldon@demo.com	27	0.135%
darrel@demo.com	26	0.13%
jeff@demo.com	26	0.13%
asron@demo.com	26	0.13%
adolfo@demo.com	26	0.13%
augustus@demo.com	26	0.13%
geraldo@demo.com	25	0.125%
bruno@demo.com	25	0.125%

Time	Source	Destination	Method	Request	Response	User-Agent	CS Username	Host	Source	CS Username
11/7/18 12:18:29.920 PM	1541593109.920440	93.172.20.14	231 TCP_DENIED/403	1873 GET http://www.lyred.com/	403	AppleWebKit/537.101 (KHTML, like Gecko) Version/10.0.11.0 Mobile Safari/10.0.11.0	christian@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	christian@demo.com
11/7/18 12:18:10.920 PM	1541593090.920440	16922.172.20.12	205 TCP_REFRESH_HIT/200	474 GET http://damtare.by.ru/id.txt	200	Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; en) AppleWebKit/534.1 (KHTML, Like Gecko) Version/6.0.0.141 Mobile Safari/534.1	royce@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	royce@demo.com
11/7/18 12:18:06.920 PM	1541593086.920440	110.172.20.12	117 TCP_DENIED/403	1901 GET http://444.er18.com/config.txt	403	AppleWebKit/537.101 (KHTML, like Gecko) Version/10.0.11.0 Mobile Safari/10.0.11.0	alonso@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	alonso@demo.com
11/7/18 12:17:51.920 PM	1541593071.920440	16922.172.20.12	178 TCP_REFRESH_HIT/200	474 GET http://damtare.by.ru/id.txt	200	Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/534.1 (KHTML, like Gecko) Safari/125.8	emmanuel@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	emmanuel@demo.com
11/7/18 12:17:45.837 PM	1541593065.837745	16922.172.20.13	103 TCP_REFRESH_HIT/200	474 GET http://damtare.by.ru/id.txt	200	Mozilla/5.0 (Windows NT 6.2; rv:19.0.0) Gecko/20121129 Firefox/19.0	monty@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	monty@demo.com
11/7/18 12:17:43.837 PM	1541593063.837745	16922.172.20.13	64 TCP_REFRESH_HIT/200	474 GET http://damtare.by.ru/id.txt	200	Mozilla/5.0 (Meego; NokiaN950-00/00) AppleWebKit/534.13 (KHTML, like Gecko) NokiaBrowser/8.5.0 Mobile Safari/534.13	roscoe@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	roscoe@demo.com
11/7/18 12:17:41.837 PM	1541593061.837745	16922.172.20.13	116 TCP_REFRESH_HIT/200	474 GET http://damtare.by.ru/id.txt	200	Opera/9.80 (Android 4.0.4; Linux; Opera Mobi/ADR-1205181138; U; pl) Presto/2.10.254 Version/12.00	alexis@demo.com	ch-demo-cisco.hod.cloud	/four/splunk/var/spool/splunk/samplelog/cisco-wsa-squid	alexis@demo.com

New Search

Save As | Close

sourcetype="\*" (src\_ip="201.3.120.165" OR dest\_ip="201.3.120.165") | eval product=case(sourcetype="Network:Generic","Network",sourcetype="cisco:wsa:squid","WSA") | search product=Network

Date time range | Search

182 events (11/7/18 3:27:00.000 PM to 11/7/18 4:27:55.000 PM) No Event Sampling

Job | Smart Mode

Events (182) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

1 minute per column

List | Format | 20 Per Page

Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Next

Hide Fields | All Fields

Selected Fields

- host 1
- source 1
- sourcetype 1

Interesting Fields

- date\_hour 2
- date\_mday 1
- date\_minute 51
- date\_month 1
- date\_second 57
- date\_wday 1
- date\_year 1
- date\_zone 1
- dest\_ip 1
- EndPointMatchedProfile 1
- eventtype 2
- index 1
- linecount 1
- product 1
- punct 1
- splunk\_server 1
- src\_ip 1
- timeendpos 1
- timestartpos 1

i	Time	Event
>	11/7/18 4:22:42.000 PM	11/07/2018 16:22:42 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:21:10.000 PM	11/07/2018 16:21:10 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:21:02.000 PM	11/07/2018 16:21:02 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:20:51.000 PM	11/07/2018 16:20:51 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:20:45.000 PM	11/07/2018 16:20:45 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:13:55.000 PM	11/07/2018 16:13:55 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:12:54.000 PM	11/07/2018 16:12:54 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic

**EndPointMatchedProfile** [X]

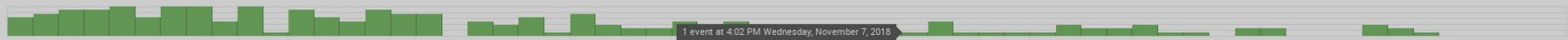
1 Value, 100% of events Selected Yes No

**Reports**

- Top values
- Events with this field
- Rare values

**Values**

Values	Count	%
Network-Printer	182	100%



List | Format | 20 Per Page

< Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Next >

< Hide Fields | All Fields

Selected Fields

- a host 1
- a source 1
- a sourcetype 1

Interesting Fields

- # date\_hour 2
- # date\_mday 1
- # date\_minute 51
- a date\_month 1
- # date\_second 57
- a date\_wday 1
- # date\_year 1
- a date\_zone 1
- a dest\_ip 1
- a EndPointMatchedProfile 1
- a eventtype 2
- a index 1
- # linecount 1
- a product 1
- a punct 1
- a splunk\_server 1
- a src\_ip 1
- # timeendpos 1
- # timestartpos 1

+ Extract New Fields

i	Time	Event
∨	11/7/18 4:22:42.000 PM	11/07/2018 16:22:42 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer"

Event Actions

Type	Field	Value	Actions
<input checked="" type="checkbox"/>	Build Event Type	127.0.0.1	▼
<input type="checkbox"/>	Extract Fields	eventgen	▼
<input checked="" type="checkbox"/>	Quarantine in ISE	Network:Generic	▼
<input type="checkbox"/>	Show Source	Profile ▾ Network-Printer	▼
<input type="checkbox"/>	eventtype ▾	201.3.120.165	▼
<input type="checkbox"/>	product ▾	cisco-ise-dc-devices	▼
<input type="checkbox"/>	src_ip ▾	generic-network-traffic	▼
<input type="checkbox"/>	Time ⌲	Network	▼
<input type="checkbox"/>	index ▾	10.2.3.7	▼
<input type="checkbox"/>	linecount ▾	2018-11-07T16:22:42.000+00:00	▼
<input type="checkbox"/>	punct ▾	main	▼
<input type="checkbox"/>	splunk_server ▾	ch-demo-cisco.hod.cloud	▼

>	11/7/18 4:21:10.000 PM	11/07/2018 16:21:10 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:21:02.000 PM	11/07/2018 16:21:02 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:20:51.000 PM	11/07/2018 16:20:51 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:20:45.000 PM	11/07/2018 16:20:45 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:20:41.000 PM	11/07/2018 16:20:41 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:16:43.000 PM	11/07/2018 16:16:43 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:16:04.000 PM	11/07/2018 16:16:04 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic
>	11/7/18 4:15:20.000 PM	11/07/2018 16:15:20 - src_ip="10.2.3.7" dest_ip="201.3.120.165" EndPointMatchedProfile="Network-Printer" host = 127.0.0.1   source = eventgen   sourcetype = Network:Generic

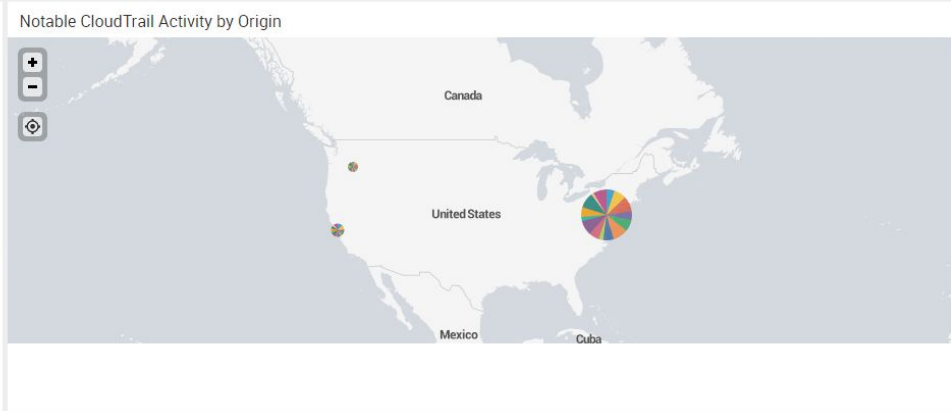
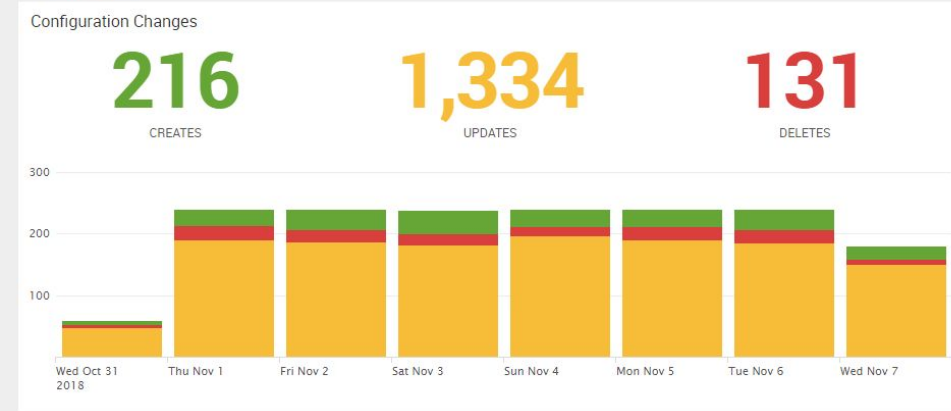
# Overview

Edit Export ...

Account ID:  Regions:  Tags:  Time Range:  [Hide Filters](#)

**i** Some panels may not be displayed correctly because the following inputs have not been configured: CloudWatch, Config, CloudTrail, Description. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. [Learn more](#)

[Hide Messages](#)





# Historical Monthly Bills

Edit Export ...

Account ID:  Currency:  Tags:  Billing report from:  To:   Include Onetime Payments [Hide Filters](#)

Some panels may not be displayed correctly because the following inputs have not been configured: Billing. Or, the saved search 'Addon Metadata - Summarize AWS Inputs' is not enabled on Add-on instance. [Learn more](#) Hide Messages

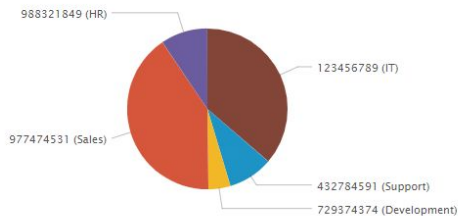
## Total Cost

477,679,847 \$

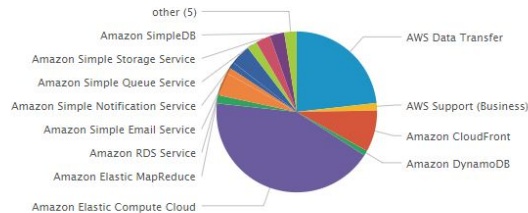
## Total Onetime Payments Cost

0 \$

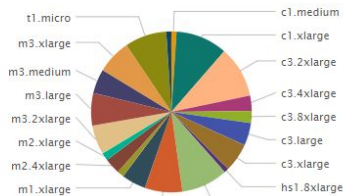
## Cost by Account



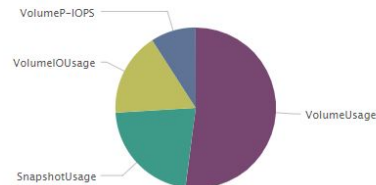
## Cost by Service



## EC2 Cost by Instance Type



## EBS Cost by Usage Type



### Reserved Instance Planner Details

Edit Export ...

Some panels may not be displayed correctly because the following inputs have not been configured: Billing. Or, the saved search "Addon Metadata - Summarize AWS Inputs" is not enabled on Add-on instance. [Learn more](#)

[Hide Messages](#)

Summary  
Account ID: 729374374  
Region: Asia Pacific (Tokyo)  
Platform: Linux/UNIX  
Tenancy: default  
Family: d2

Basis for insight  
 History  Prediction

Payment option(one-year term)  
 All upfront  Partial upfront  No upfront

#### Existing Reserved Instances

# N/A

Count

#### Optimal Reserved Instances

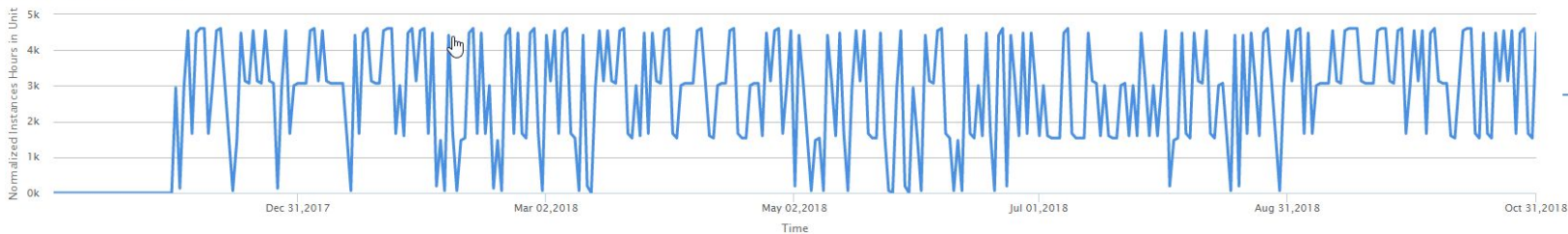
# 128.00

Unit

#### Estimated Cost

# \$80,223 ↓ 21%

#### Running instances over time



Reset

The past year  
Nov 01, 2017–Oct 31, 2018  
Adjust the history time range by horizontal dragging

### Reserved Instance Planner Details

Edit Export ...

Some panels may not be displayed correctly because the following inputs have not been configured: Billing. Or, the saved search 'Addon Metadata - Summarize AWS Inputs' is not enabled on Add-on instance. [Learn more](#)

[Hide Messages](#)

Summary  
Account ID: 729374374  
Region: Asia Pacific (Tokyo)  
Platform: Linux/UNIX  
Tenancy: default  
Family: d2

Basis for insight

Payment option(one-year term)

#### Existing Reserved Instances

**N/A**  
Count

#### Optimal Reserved Instances

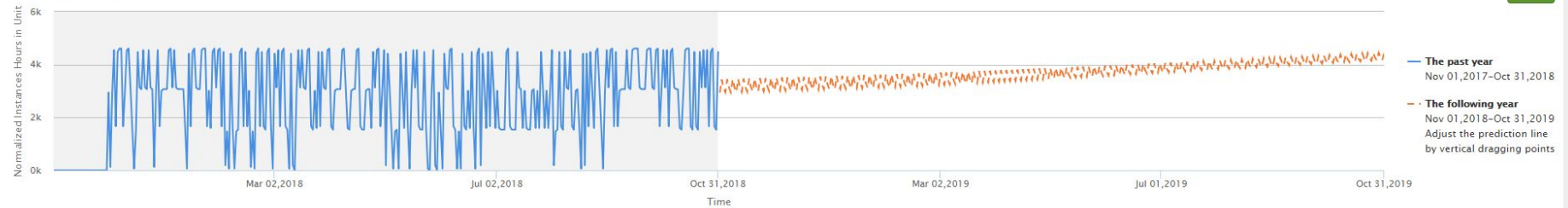
**152.00**  
Unit

#### Estimated Cost

**\$80,987** 43%

#### Running instances over time

[Reset](#)





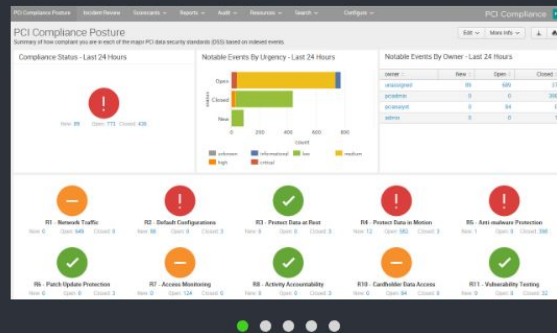


# Splunk App for PCI Compliance - Splunk Enterprise

★★★★★ 20 ratings

Splunk Built

# NOW FREE ]:)



## Overview

## Details

The Splunk App for PCI Compliance (for Splunk Enterprise) is a Splunk developed and supported App designed to help organizations meet PCI DSS 3.2 requirements. It reviews and measures the effectiveness and status of PCI compliance technical controls in real time. It can also identify and prioritize any control areas that may need to be addressed and let you quickly address any auditor report or data request.

The App provides out-of-the-box searches, dashboards, reports, an incident response framework, and integration with employee and asset information to give you visibility into system, application, and device activity relevant to PCI compliance.

NOTE: There are two installer options for this App. If you are installing the App on Splunk Enterprise 6.4+ use the installer on this page. But if you are installing the App on Splunk Enterprise Security, use the installer at <https://splunkbase.splunk.com/app/2897/>

2

Installs

2,470

Downloads

Download

Rate this App

## VERSION

3.70 ▾

# PCI Compliance Posture

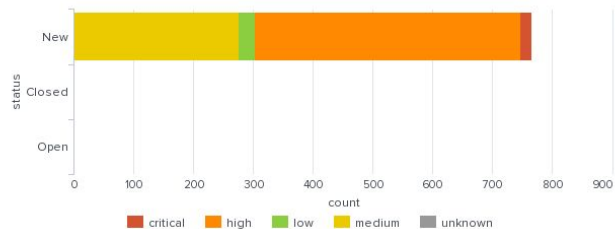
Export ...

Summary of how compliant you are in each of the major PCI data security standards (DSS) based on indexed events.

Compliance Status - Last 24 Hours



Notable Events By Urgency - Last 24 Hours



Notable Events By Owner - Last 24 Hours

owner	New	Open	Closed
unassigned	766	0	0



**R1 - Network Traffic**

New: 45 Open: 0 Closed: 0



**R2 - Default Configurations**

New: 54 Open: 0 Closed: 0



**R3 - Protect Data at Rest**

New: 2 Open: 0 Closed: 0



**R4 - Protect Data in Motion**

New: 21 Open: 0 Closed: 0



**R5 - Anti-malware Protection**

New: 303 Open: 0 Closed: 0



**R6 - Patch Update Protection**

New: 66 Open: 0 Closed: 0



**R7 - Access Monitoring**

New: 121 Open: 0 Closed: 0



**R8 - Activity Accountability**

New: 94 Open: 0 Closed: 0



**R10 - Cardholder Data Access**

New: 141 Open: 0 Closed: 0



**R11 - Vulnerability Testing**

New: 24 Open: 0 Closed: 0

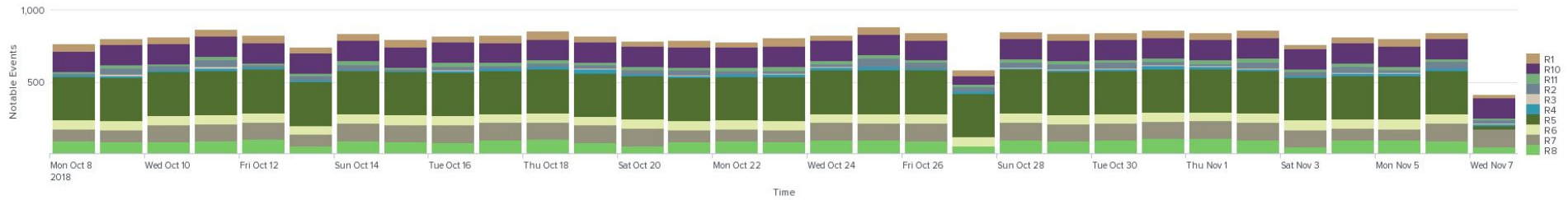
## Notable Event History

Last 30 days



## Notable Event History By Requirements

Last 30 days



Search, Download, Info, Refresh, 1h ago

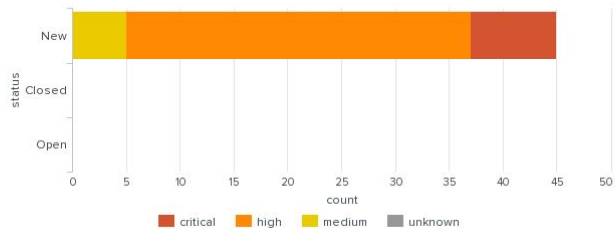
# PCI Scorecard: Requirement 1

Export ...

Compliance Status - Last 24 Hours



Notable Events By Urgency - Last 24 Hours



Notable Events By Owner - Last 24 Hours

owner	New	Open	Closed
unassigned	45	0	0

Views - Last 24 Hours

view	user	viewed_today
Firewall Rule Activity	mfaizal	Yes
Network Traffic Activity		No
Prohibited Services		No

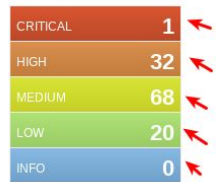
Notable Event History

Last 30 days



# Incident Review

## Urgency



## Status

New X

## Owner

All X

## Security Domain

All X

## Tag

Select...

## Correlation Search Name

Select...

## Search

governance="pci" control="7.1"

Time Associations

Last 24 hours

Submit



Edit Selected | Edit All 121 Matching Events | Add Selected to Investigation

prev 1 2 3 4 5 6 7 next

i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	11/7/18 8:00:00 AM	Access	<u>Brute Force Access Behavior Detected From 10.1136.9</u>	High	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.8	High	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.7	High	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.6	High	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.50	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.5	High	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.49	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.48	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.47	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.46	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.45	Medium	New	unassigned	▼
>	<input type="checkbox"/>	11/7/18 7:59:57 AM	Access	Brute Force Access Behavior Detected From 10.1136.44	Medium	New	unassigned	▼



Description:

The system 10.11.36.20 has failed authentication 755 times and successfully authenticated 22 times in the last hour

Additional Fields

Additional Fields	Value
Application	login sshd win.local win.remote
Source	10.11.36.20 3940
Source Business Unit	americas
Source Category	pci splunk Pleasanton
Source City	
Source Country	USA
Source IP Address	10.11.36.20
Source Expected	true
Source Latitude	37.694452
Source Longitude	-121.894461
Source Owner	Bill_williams
Source PCI Domain	trust
Source Requires Antivirus	false
Source Should Time Synchronize	true
Source Should Update	true

Event Details:

event_id	AFE39A99-CD65-4740-83E7-FD33B2388180@@@notable@@@7adc72ff6b3a0f3b3ac8cfbe3889fd0d
event_hash	7adc72ff6b3a0f3b3ac8cfbe3889fd0d
eventtype	modnotable_results
	nix-all-logs
	pci
	suppress_src
	notable
	google_pci

Related Investigations:

Currently not investigated.

Correlation Search:

Access - Brute Force Access Behavior Detected - Rule

Compliance

Governance	Control
pci	7.1
pci	7.2

History:

View all review activity for this Notable Event

Contributing Events:

View all login attempts by system 10.11.36.20

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2018-11-07T07:59:57+0000	admin	✓ success
Risk Analysis	saved	2018-11-07T07:59:57+0000	admin	✓ success
Notable	saved	2018-11-06T08:01:35+0000	admin	✓ success
Risk Analysis	saved	2018-11-06T08:01:35+0000	admin	✓ success

View Adaptive Response Invocations

Next Steps:

No Next Steps defined.

Urgency

CRITICAL	1
HIGH	32
MEDIUM	68
LOW	20
INFO	0

Status

New x

Owner

All x

Security Domain

All x

Tag

Select...

Correlation Search Name

Select...

Search

governance="pci" control="7\*\*

Time Associations

Last 24 hours

Submit



Edit Selected | Edit All 121 Matching Events | Add Selected to Investigation

i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input checked="" type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.20				
>	<input type="checkbox"/>	11/7/18 8:00:00.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.9				
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.8				
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.7				
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.6				
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.5				
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.4				
i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	11/7/18 8:00:00.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.9	High	In Progress	demo_owner	
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.8	High	In Progress	demo_owner	
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.7	High	In Progress	demo_owner	
>	<input type="checkbox"/>	11/7/18 7:59:57.000 AM	Access	Brute Force Access Behavior Detected From 10.11.36.6	High	In Progress	demo_owner	

### Edit Events

**i** You are editing all events matching the search (768 events)

Status: In Progress

Urgency: Medium

Owner: demo\_owner

Assign to me

Comment:



### R1 - Network Traffic

New: 40 Open: 0  
Closed:  
0



### R2 - Default Configurations

New: 47 Open: 0  
Closed:  
0



### R3 - Protect Data at Rest

New: 2 Open: 0  
Closed:  
0



### R4 - Protect Data in Motion

New: 21 Open: 0  
Closed:  
0



### R5 - Anti-malware Protection

New:  
304 Open: 0  
Closed:  
0



### R6 - Patch Update Protection

New: 66 Open: 0  
Closed:  
0



### R7 - Access Monitoring

Open:  
New: 0 121  
Closed:  
0



### R8 - Activity Accountability

New: 94 Open: 0  
Closed:  
0



### R10 - Cardholder Data Access

New: 60 Open: 81  
Closed:  
0



### R11 - Vulnerability Testing

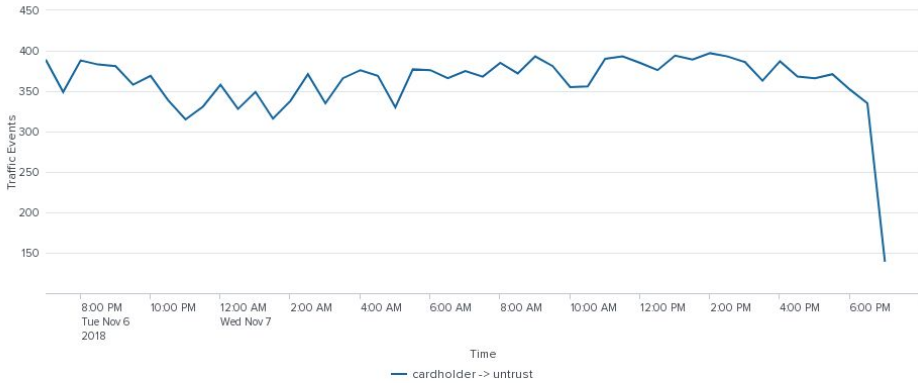
New: 20 Open: 0  
Closed:  
0

## Network Traffic Activity

Export ...

Source Domain: 
 Destination Domain: 
 Category: 
 Action: 
 Security: 
 Authorization: 
 Time Range:

Traffic By Source And Destination Domain



Recent Notable Events - Last 24 Hours

No results found.

### Traffic Detail

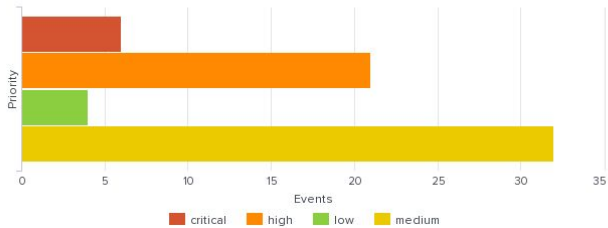
src	src_pci_domain	dest	dest_pci_domain	port	is_secure	is_prohibited	count
10.252.2.6	trust cardholder	66.235.133.3	untrust	tcp/80	false	true	17
10.11.36.43	trust cardholder	188.241.9.99	untrust	udp/12355	false	true	13
10.11.36.41	trust cardholder	69.55.54.17	untrust	udp/123	false	true	11
10.11.36.45	trust cardholder	69.55.54.17	untrust	udp/123	false	true	11

# Asset Center

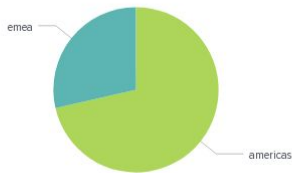
Export ...

Asset:  Priority: All Business Unit:  Category: pci X PCI Domain: All Owner:  Submit Hide Filters

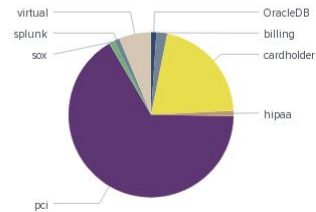
Assets By Priority



Assets By Business Unit



Assets By Category



## Asset Information

2m ago

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av
		ACME-006			high	50.84436	-0.98451	Havant	UK	emea	pci	trust wireless	false	true	true	true
		ops-sys-005			medium	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	true	true
		BUSDEV-007			medium	37.694452	-121.894461	Pleasanton	USA	americas	cardholder pci	cardholder trust	true	true	true	true
		PROD-POS-001		mbcgown	medium	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	true	true
		AcMEFW			high	38.959405	-77.04	Washington D.C.	USA	americas	cardholder pci	cardholder trust	true	true	true	false
		BUSDEV-001			medium	37.694452	-121.894461	Pleasanton	USA	americas	cardholder pci	cardholder trust	true	true	true	true
		HOST-006			high	50.84436	-0.98451	Havant	UK	emea	pci	trust wireless	false	true	true	false
		PROD-POS-002		gclough	medium	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	true	true

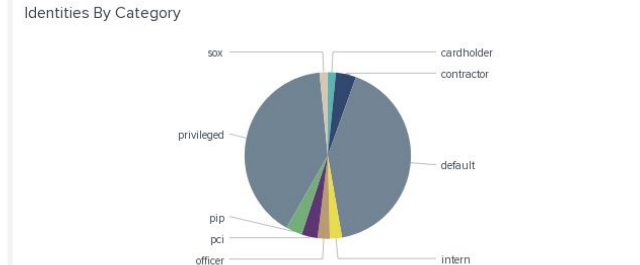
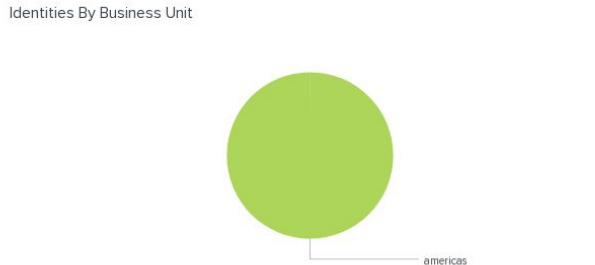
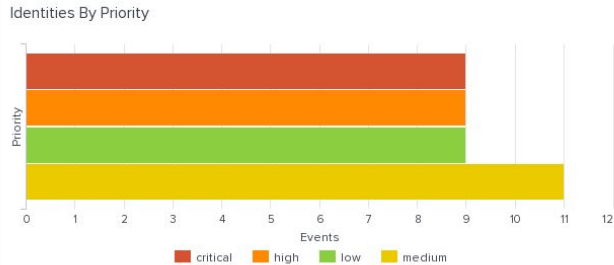


# Identity Center

Export ...

Username: 
 Priority: 
 Business Unit: 
 Category: 
 Watchlisted Identities Only:

[Hide Filters](#)



## Identity Information

identity	first	last	email	phone	phone2	managedBy	priority	bunit	category	watchlist	startDate	endDate	work_city	work_country	work_lat	work_long
3comcso									default privileged	false						
Bill_williams Bill_williams@acmecorp.com	William	Williams	Bill_williams@acmecorp.com	+1 (800)555-1212	+1 (800)555-3814		medium	americas	officer	true	03/08/2002 00:00:00		San Jose	USA	37.3382N	121.8863W
Joy joy_rence joy_rence@bankofvulcan.com	Joy	Rence	joy_rence@bankofvulcan.com	+1 (800)555-6931	+1 (800)555-3814	joy_rence	low	americas		false	02/08/2003 14:38:00	09/22/2015 08:29:00	London	UK	51.507N	0.1275W
a.koski aseykoski aseykoski@acmetech.com pepper	Allen	Seykoski	aseykoski@acmetech.com	+1 (800)555-2111	+1 (800)555-9996		high	americas		true	07/12/2003 15:30:00	07/12/2008 19:49:00	San Francisco	USA	37.78N	122.41W
adfexc									default privileged	false						



**BREAK**

10 MINUTES



Splunk Enterprise  
Security™



# Splunk as Security Nerve Center

© 2018 SPLUNK INC.

**paloalto** NETWORKS Booz | Allen | Hamilton

**ATLASSIAN**

**ALMAIL** illumio

Corvil **AWAKE**

**DEMISTO** **TANIUM**

**Symantec** **COFENSE**

**CYBERRESPONSE** ADAPTIVE SECURITY

**FORTINET**

**SailPoint** VMRAY

**REDSEAL** INTERNET STORM CENTER

**RESOLVE** SYSTEMS **dataphy**

**Resilient** an IBM Company **ziftēn** **zscaler**

**amazon** Web Services **ForeScout** Recorded Future **QUALYS**

**DomainTools** **SWIMLANE** **CISCO** Cisco Umbrella

**CYLANCE**

**CYBERARK** **Signal Sciences** **THREATCONNECT**

**LogicHub** **ANOMALI**

**netskope** **CROWDSTRIKE**

**Pinn AuthX** **CISCO**

**SHODAN** **CARBON BLACK**

**SYNCRITY** **Phantom**

**okta** **ACALVIO**

**TCELL** **SentinelOne** **Gigamon**

**tenable** **algosec** **proofpoint**

**graphistry** **accenture** **CISCO** Cisco Cloudlock



**splunk** > listen to your data

# Typical Data Sources



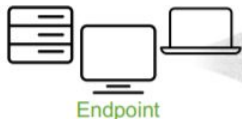
- Third-party threat intel
- Open-source blacklist
- Internal threat intelligence

Attacker, know relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution



- Firewall, IDS, IPS
- DNS
- Email
- Web proxy
- NetFlow
- Network

Where they went, who talked to whom, attack transmitted, abnormal traffic, malware download



- Endpoint (AV/IPS/FW)
- Malware detection
- PCLM
- DHCP
- OS logs
- Patching

What process is running (malicious, abnormal, etc.)  
Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility



- Active Directory
- LDAP
- CMDB
- Operating system
- Database
- VPN, AAA, SSO

Access level, privileged users, likelihood of infection, where they might be in kill chain



# Stream Investigations – Choose Your Data Wisely



Threat Intelligence



Email



Web



Desktops



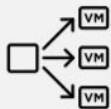
Servers



DHCP/ DNS



CMDB



Hypervisor



Badges



Firewall



Authentication



Vulnerability  
Scans



Custom Apps



Network  
Flows



Storage



Mobile



Intrusion  
Detection



Data Loss  
Prevention



Anti-Malware



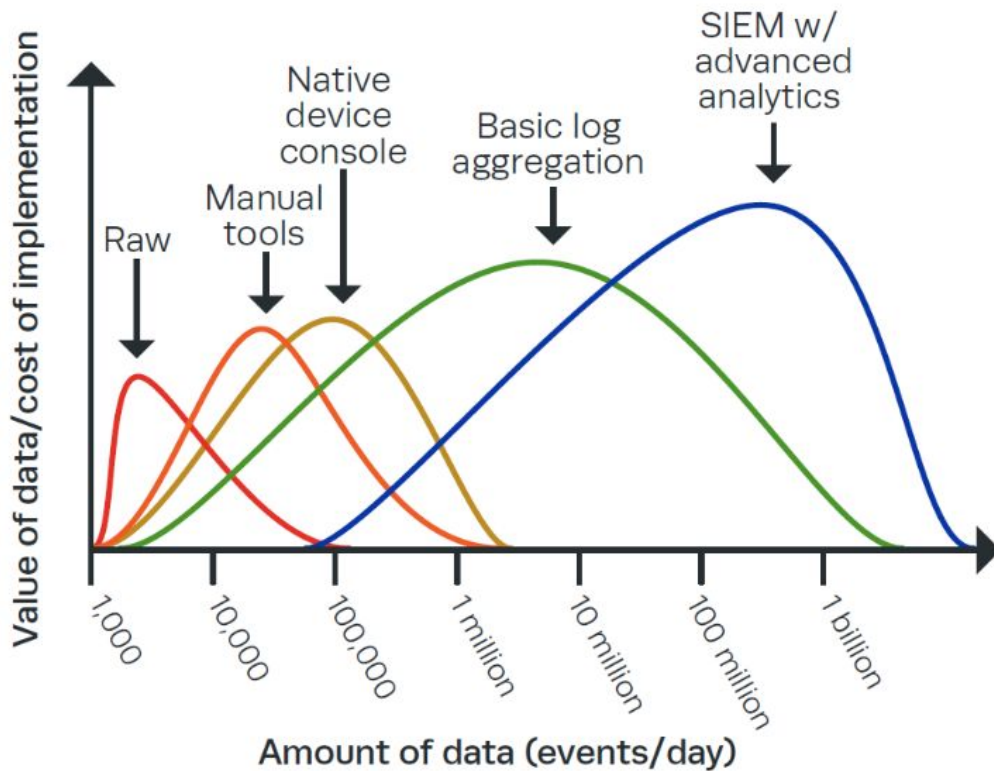
Physical  
Access



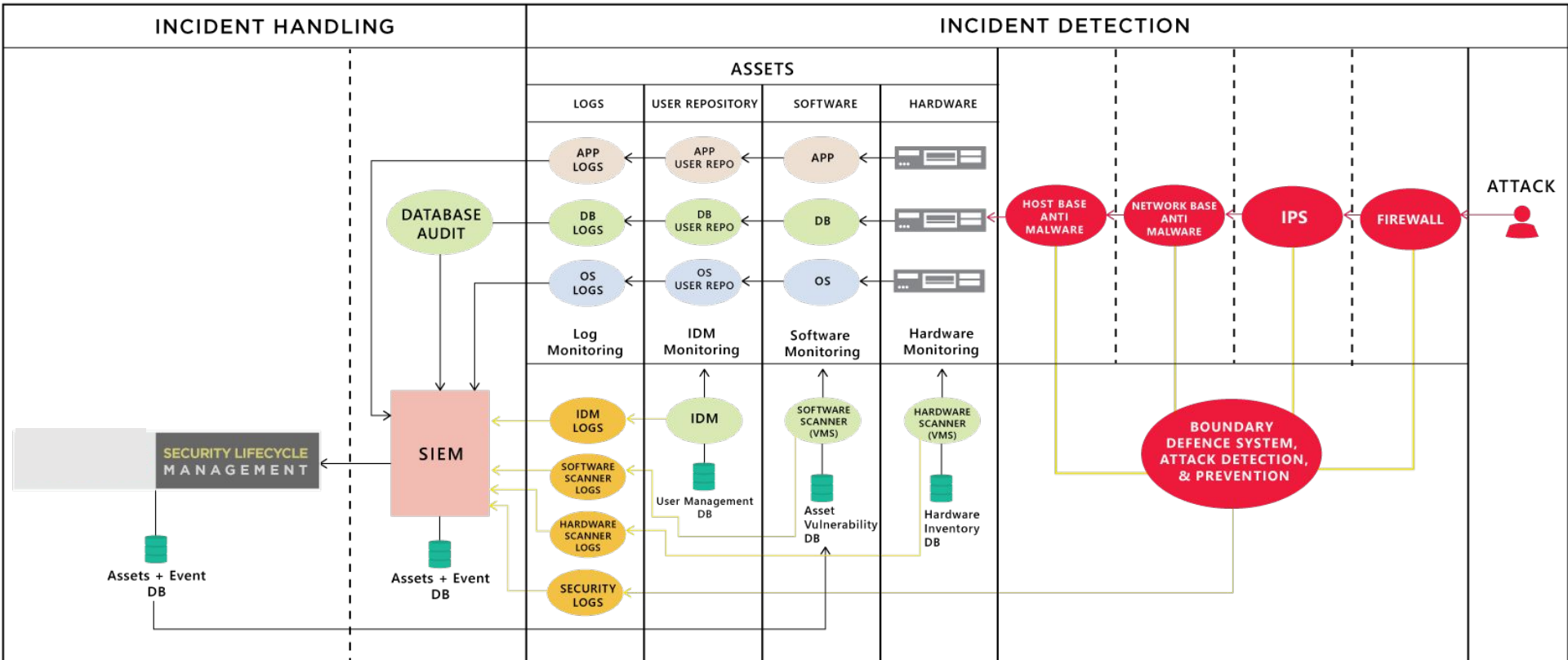
Transaction  
Records

## Traditional

# SOC Fundamentals: amount of data



# Know yourself: Your arsenal, toolset and processes. Layered security



# Security Pyramid



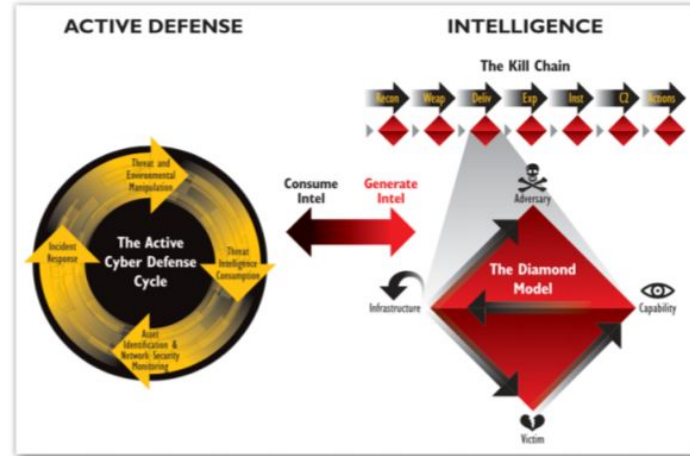
# What is Threat Hunting, Why do You Need it?

## What?

Threat hunting - the act of aggressively intercepting, tracking and eliminating cyber adversaries as early as possible in the Cyber Kill Chain<sup>2</sup>

## Why?

Threats are human. Focused and funded adversaries will not be countered by security boxes on the network alone. Threat hunters are actively searching for threats to prevent or minimize damage [before it happens]<sup>1</sup>



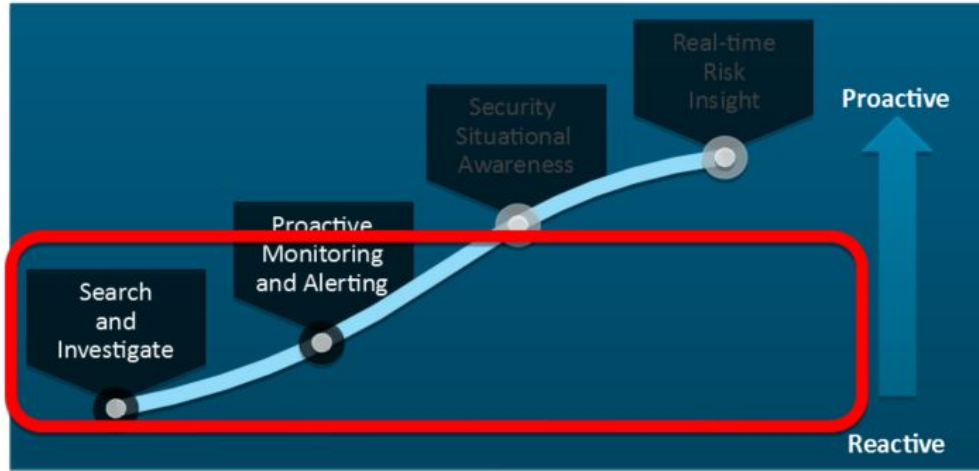
*"Threat Hunting is not new, it's just evolving!"*

<sup>1</sup> The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS Feb 2016

<sup>2</sup> Cyber Threat Hunting - Samuel Alonso blog, Jan 2016



# Everyone Performs Security Investigation



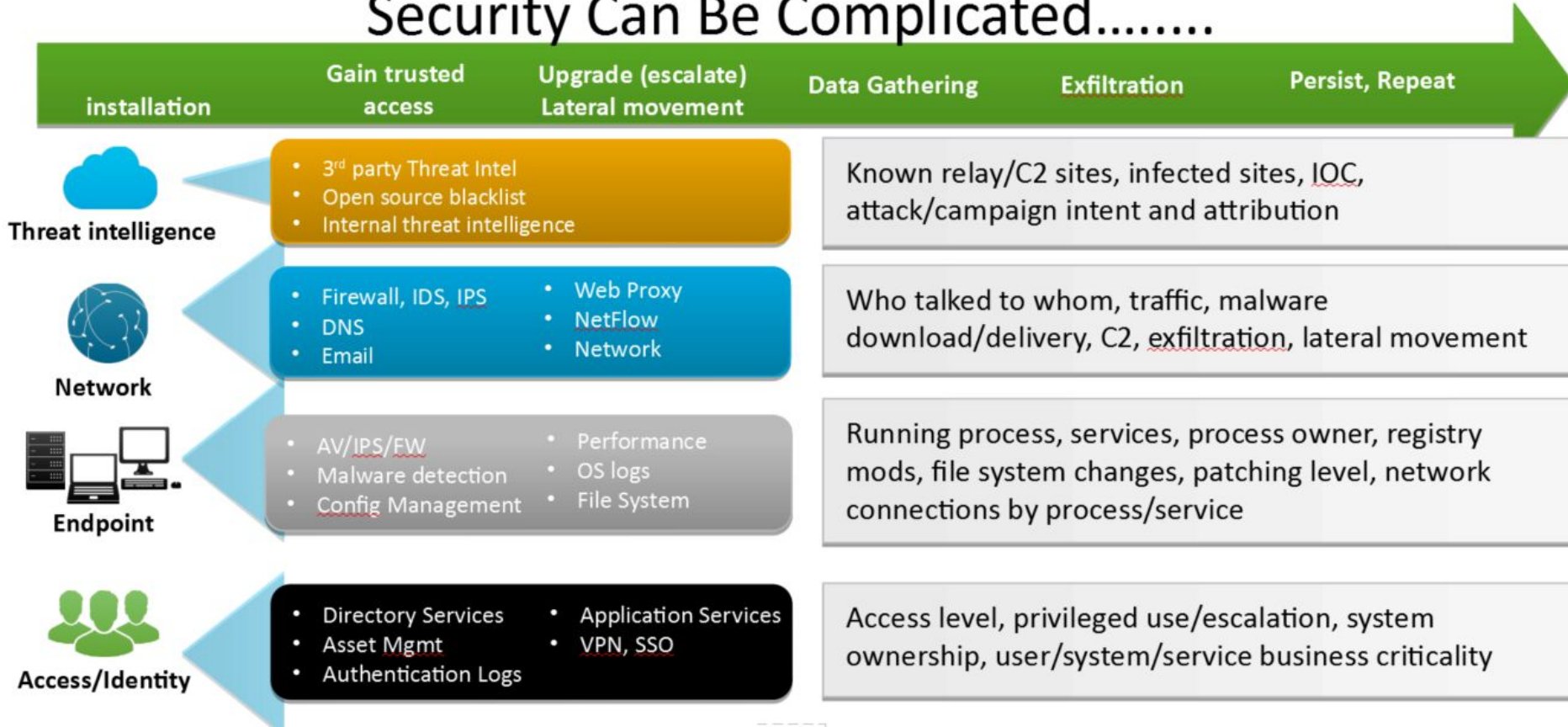
- Continuous monitoring/evaluation
- Incident response and forensic investigation
- Event searching, reporting, monitoring & correlation
- Rapid learning loop, shorten discover/detect cycle
- Rapid insight from all data

Progress to hunting, SIEM, advanced analytics, machine learning, risk-based approach

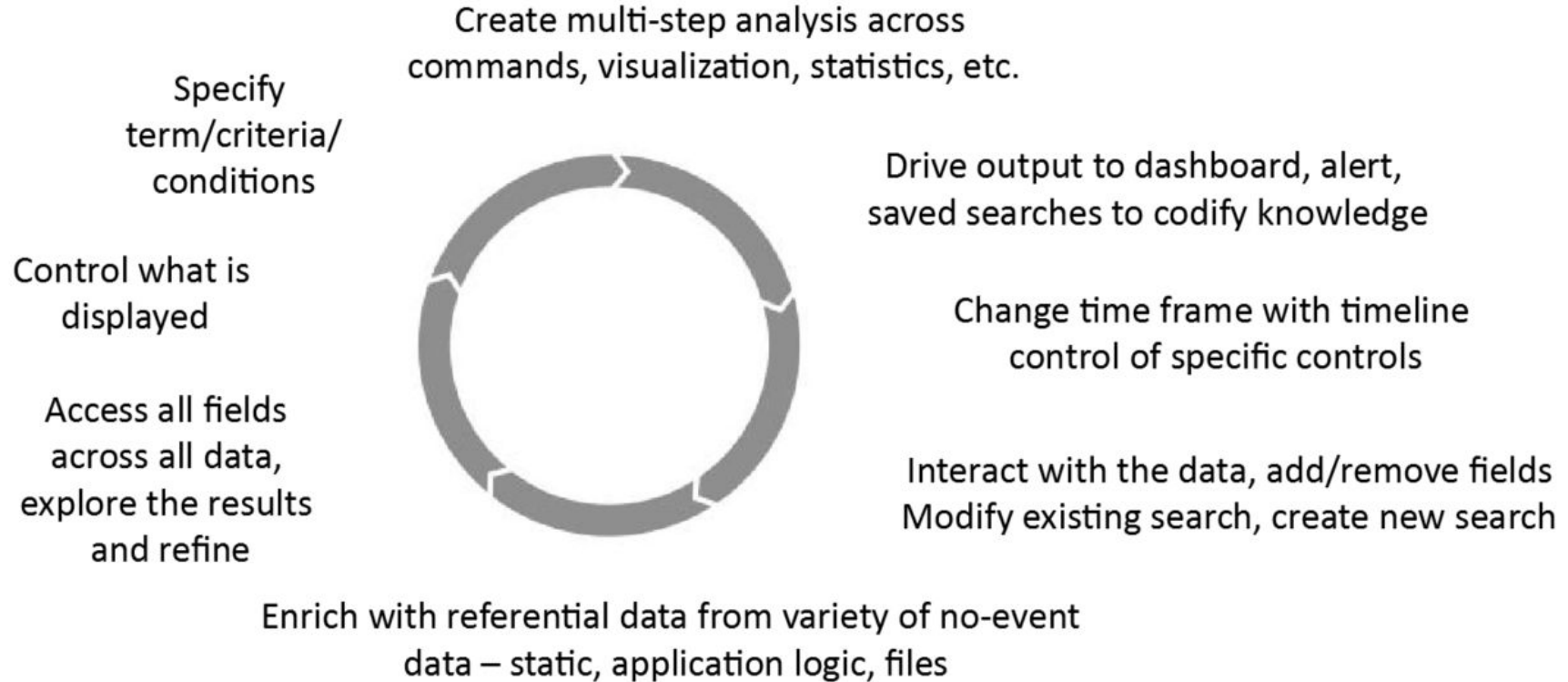


Splunk helps organizations start, evolve and grow their Information Security skill and maturity

# Security Can Be Complicated.....



# The Optimized Analytics Cycle



# SANS Threat Hunting Maturity

splunk>enterprise



**Ad Hoc  
Search**

**Statistical  
Analysis**

**Visualization  
Techniques**

**Aggregation**

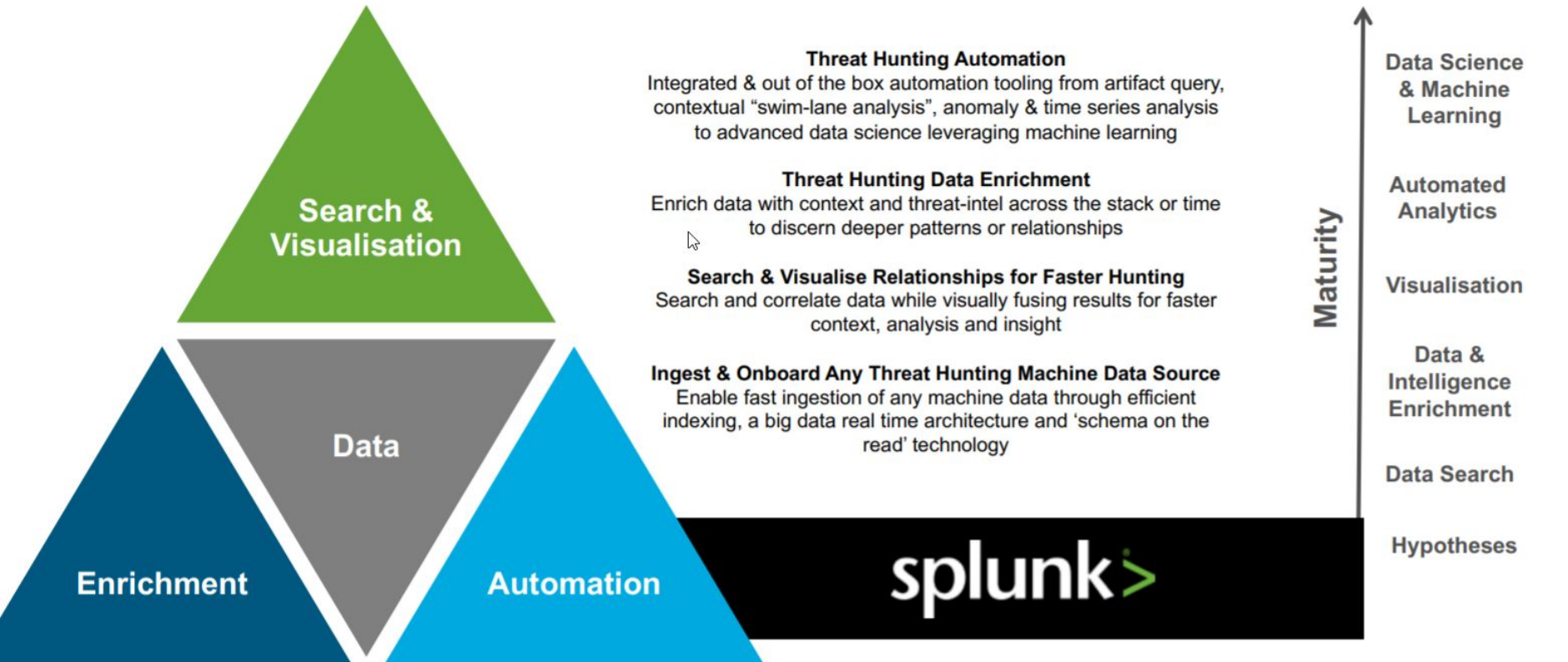
**Machine Learning/  
Data Science**



Source: SANS IR & Threat Hunting Summit 2016

130.60.4 - - [07/Jun 18:10:57:153] "GET /category/screen?category\_id=GIFTS&SESSIONID=5055LAPF1GADFF10 HTTP/1.1" 404 720 "http://buttkrcep-shopping.com/cart.do?action=removeItem&id=55-68product\_id=2-5w-03-  
130.241.230.82 - - [07/Jun 18:10:57:131] "GET /product/screen?product\_id=FL-DSH-01&SESSIONID=5055LAPF1GADFF10 HTTP/1.1" 404 1323 "http://buttkrcep-shopping.com/category/screen?category\_id=55-68product\_id=2-5w-03-  
317.27.160.9 - - [07/Jun 18:10:57:121] "GET /product/screen?product\_id=FL-DSH-01&SESSIONID=5055LAPF1GADFF10 HTTP/1.1" 200 1318 "http://buttkrcep-shopping.com/cart.do?action=removeItem&id=55-188product\_id=2-5w-03-  
//buttkrcep-shopping.com/.NET CLR 1.1.4322) 468 135 "GET /oldlink!item\_session\_id=5055LAPF1GADFF10 HTTP/1.1" 200 1318 "http://buttkrcep-shopping.com/cart.do?action=removeItem&id=55-188product\_id=2-5w-03-  
action=removeItem&id=55-188product\_id=2-5w-03-  
buttkrcep-shopping.com/.NET CLR 1.1.4322) 468 135 "GET /oldlink!item\_session\_id=5055LAPF1GADFF10 HTTP/1.1" 200 1318 "http://buttkrcep-shopping.com/cart.do?action=removeItem&id=55-188product\_id=2-5w-03-  
buttkrcep-shopping.com/.NET CLR 1.1.4322) 468 135 "GET /oldlink!item\_session\_id=5055LAPF1GADFF10 HTTP/1.1" 200 1318 "http://buttkrcep-shopping.com/cart.do?action=removeItem&id=55-188product\_id=2-5w-03-

# How Splunk Helps You Drive Threat Hunting Maturity

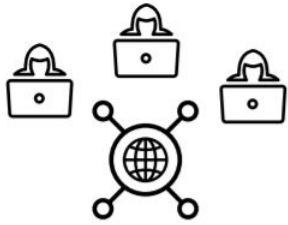
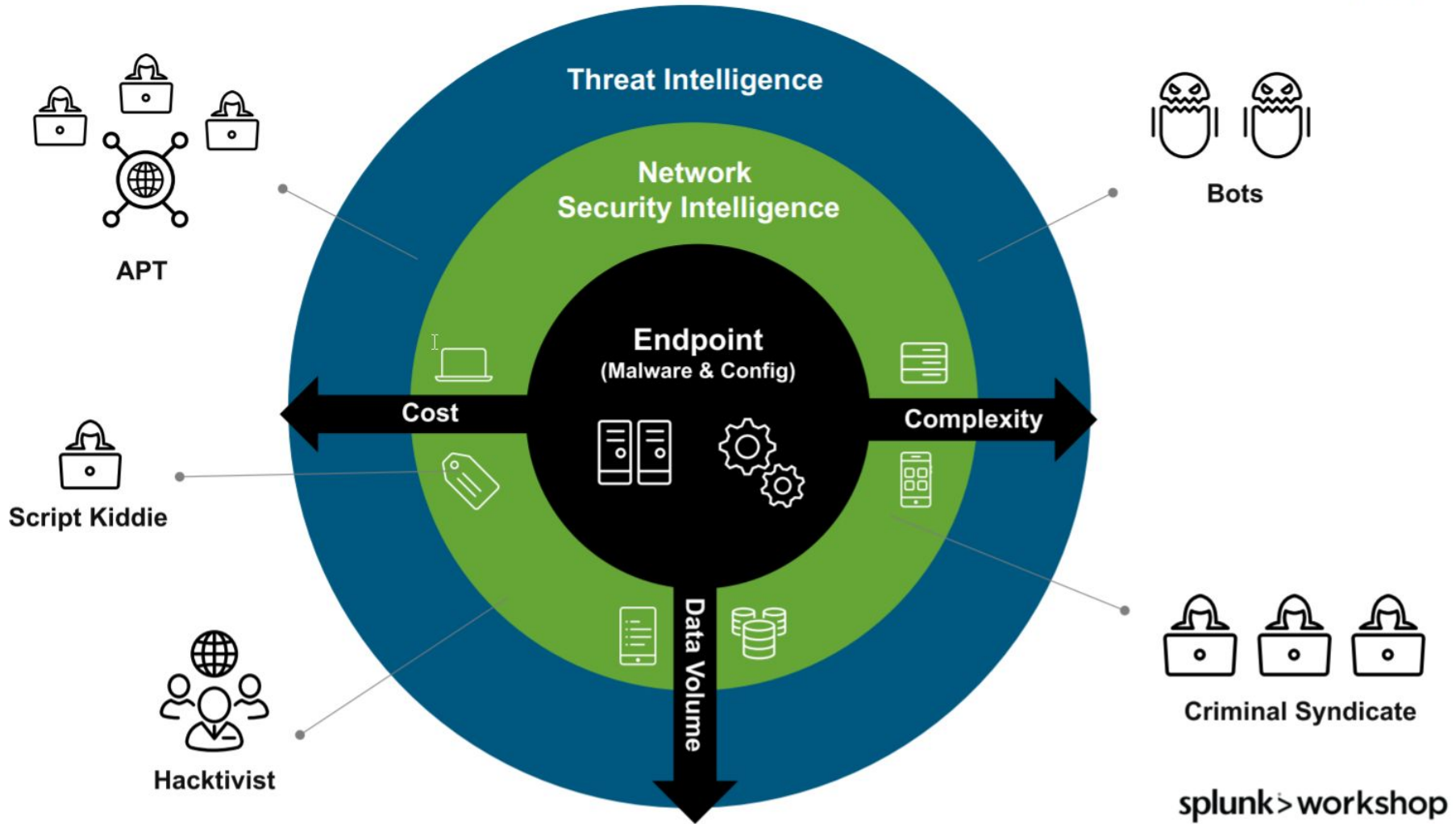




# Hunting Tools: Internal Data

- ▶ **IP Addresses:** threat intelligence, blacklist, whitelist, reputation monitoring  
Tools: Firewalls, Proxies, Splunk Stream, Bro, IDS
- ▶ **Network Artifacts and Patterns:** network flow, packet capture, active network connections, historic network connections, ports and services  
Tools: Splunk Stream, Bro IDS, FPC, Netflow
- ▶ **DNS:** activity, queries and responses, zone transfer activity  
Tools: Splunk Stream, Bro IDS, OpenDNS
- ▶ **Endpoint – Host Artifacts and Patterns:** users, processes, services, drivers, files, registry, hardware, memory, disk activity, file monitoring: hash values, integrity checking and alerts, creation or deletion  
Tools: Windows/Linux, Carbon Black, Tanium, Tripwire, Active Directory
- ▶ **Vulnerability Management Data**  
Tools: Tripwire IP360, Qualys, Nessus
- ▶ **User Behavior Analytics:** TTPs, user monitoring, time of day location, HR watchlist  
Splunk UBA, (All of the above)





APT



Bots



Script Kiddie



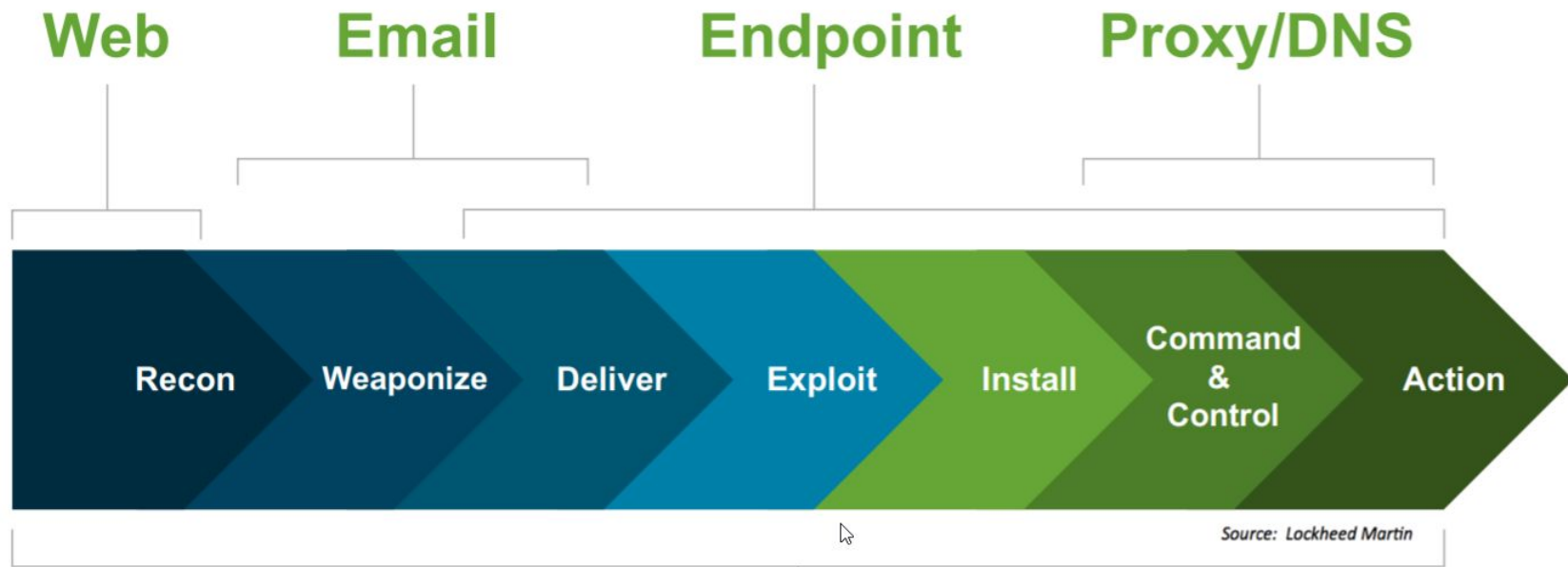
Hacktivist



Criminal Syndicate

splunk > workshop

# Data Source Mapping



**CMDB and Threat Intelligence**

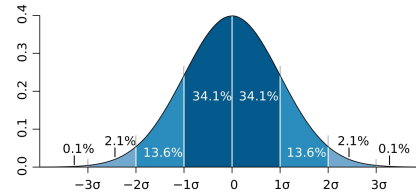
130.60.4 - - [07/Jan/18:14:30] "GET / HTTP/1.1" 200 220 82 317 27 160 14

# Correlation rules is not hard

1. Correlation/ Patterns

A and B and C not D = FRAUD

2. Anomalies/ outliers off baseline



3. Risk Scoring



\*\*\*Correlation with external feed of data in KV- Store for scale

# ES Features provided:



Threat Intelligence



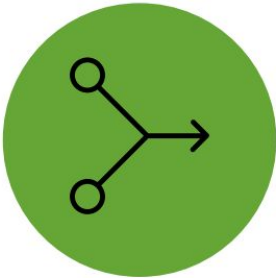
Incident Management



Asset & Identity



Risk



Adaptive Response



Security & Compliance Reporting



Incident Investigations & Forensics



Monitor & Detect Known/Unknown Threats



Security Analytics



Insider Threat



Fraud Detection

# Security Posture

Export ...

[Edit](#)

**ACCESS NOTABLES**  
Total Count

**22** ↘  
-3

**ENDPOINT NOTABLES**  
Total Count

**1.4k** ↘  
-15

**NETWORK NOTABLES**  
Total Count

**36** ↘  
-2

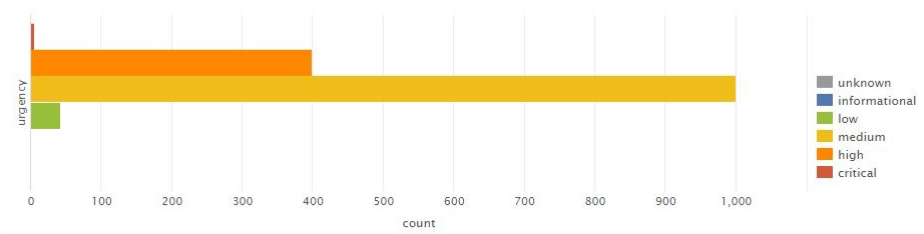
**IDENTITY NOTABLES**  
Total Count

**4** 0

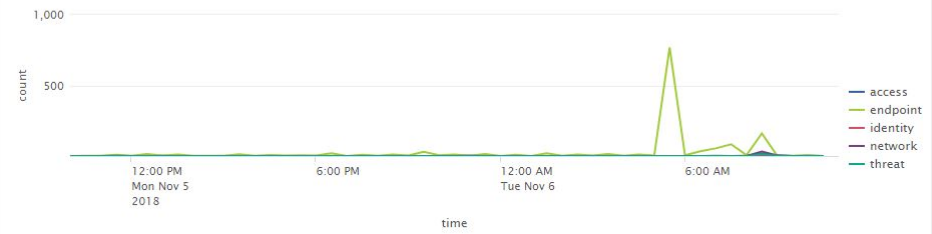
**THREAT NOTABLES**  
Total Count

**17** ↘  
-9

## Notable Events By Urgency



## Notable Events Over Time



## Top Notable Events

rule_name	sparkline	count
Host With A Recurring Malware Infection		1017
Host With Multiple Infections		180
Host With Old Infection Or Potential Re-Infection		128
Outbreak Detected		28
Unroutable Activity Detected		21
Threat Activity Detected		17
Default Account Activity Detected		15
Network Change Detected		10
Host Sending Excessive Email		9
High Or Critical Priority Host With Malware Detected		6

## Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
192.168.56.102		1	1	3
0.0.145.77		1	1	1
0.115.192.36		1	1	1
0.115.204.201		1	1	1
0.124.146.255		1	1	1
0.129.169.127		1	1	1
0.135.109.171		1	1	1
0.163.116.224		1	1	1
0.185.190.169		1	1	1
0.194.69.56		1	1	1

# Incident Review

**Urgency**

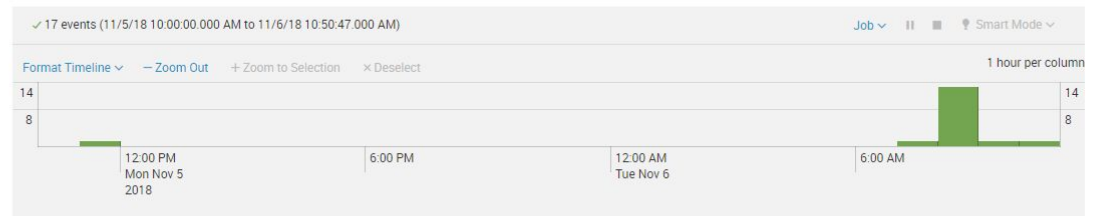
- CRITICAL 2
- HIGH 0
- MEDIUM 1
- LOW 14
- INFO 0

**Status**  Threat Activity Detected

**Owner**

**Security Domain**  **Time**

**Tag**



[Edit Selected](#) | [Edit All 17 Matching Events](#) | [Add Selected to Investigation](#)

i	<input type="checkbox"/>	Time	Security Domain	Title	Risk	Urgency	Status	Owner	Actions
	<input checked="" type="checkbox"/>	11/6/18 10:06:17.000 AM	Threat	Threat Activity Detected (115.29.46.99)		<span style="color: red;">▲</span> Critical	New	unassigned	[v]

**Description:**

Threat activity (115.29.46.99) was discovered in the 'dest' field based on threat intelligence available in the ip\_intel collection

Additional Fields	Value	Action
Destination	115.29.46.99	[v]
Destination Expected	false	[v]
Destination PCI Domain	untrust	[v]
Destination Requires Antivirus	false	[v]
Destination Should Time Synchronize	false	[v]
Destination Should Update	false	[v]
Source	192.168.56.102	[v]
Source Business Unit	Sales	[v]
Source Category	Laptop	[v]
Source City	San Francisco	[v]
Source Country	USA	[v]
Source DNS	cgilbert-DC3A297.buttercupgames.com	[v]
Source IP Address	192.168.56.102	[v]
Source Expected	TRUE	[v]
Source Latitude	37.782955	[v]
Source Longitude	-122.390978	[v]
Source NT Hostname	cgilbert-DC3A297	[v]

**Correlation Search:**

[Threat - Threat List Activity - Rule](#)

**History:**  
[View all review activity for this Notable Event](#)

**Contributing Events:**  
[View all threat activity involving dest='115.29.46.99'](#)

**Adaptive Responses:** [v]

**Next Steps:**



# cris qilbert station

(no description defined)

[Back to My Investigations](#)

Timeline | List | Type: All | Filter

Add Investigator

Search

- A Administrator
- AG Alain Gutknecht
- BM Beau Morgan
- BS Burch Simon
- CC Christopher Craft
- CL Chris Ladd
- CS Chris Shobert
- DD Dominique Dessy

### Web Search

Time	Host	Source	Destination	AS	Event Count	View
11:59:00.000	chrome	chrome	115.29.46.99	chrome	4	View

Time	Host	Source	Destination	AS	Event Count	View
11:59:00.000	chrome	chrome	115.29.46.99	chrome	4	View

chrome\_2018-11-07\_13-59-26.png

1:59 PM November 7, 2018  
4 connection to the IP 115.29.46.99(from TI)  
[chrome\\_2018-11-07\\_13-59-26.png](#)

4 connection to the IP 115.29.46.99(from TI)



## Adaptive Response Actions



Select actions to run.

+ Add New Response Action ▾

Category All ▾

Show only recommended actions



Anti-Virus

Category: anti-virus | Task: Update Virus Definition | Subject: Update Virus | Vendor: SEC



AWS : Start Instance

Category: Permissions Control | Task: allow | Subject: endpoint.server | Vendor: AWS



Verify latest patch status

Verify latest patch status

Category: Information Gathering | Task: update | Subject: endpoint.workstation | Vendor: TAN



Deep Forensics Data Collect

Category: forensics | Task: collect | Subject: collect | Vendor: Deep Forensics



Dominos : Order Pizza

Category: Device Control | Task: create | Subject: splunk.event | Vendor: Dominos



Endpoint : Check for new Hash

Endpoint : Check for new Hash

Category: Device Control | Task: create | Subject: endpoint | Vendor: Generic

Run

# Adaptive Response Action Center

Export | ...

Action Mode: All | Action Name: | Action Status: All | User: All | Search ID (sid): | Last 24 hours | [Submit](#) | [Hide Filters](#)

**ACTION INVOCATIONS**  
Count

**3.2k** ↑ +18

**ACTION NAMES**  
Distinct Count

**7** ↑ +3

**ACTION SEARCH NAMES**  
Distinct Count

**18** ↓ -1

**ACTION USERS**  
Distinct Count

**2** ↑ +1

**ACTION SEARCHES**  
Distinct Count

**109** **0**

**ACTION DURATION**  
Average (Ms)

**240** ↓ -13.4

## Action Invocations Over Time By Name



## Top Actions By Name

action_name	tag	action_mode	search_name	user	search_count	result_count	avg_duration (ms)
notable	passive	saved	Access - Default Account Usage - Rule Access - Excessive Failed Logins - Rule Access - Insecure Or Cleartext Authentication - Rule Endpoint - High Number Of Infected Hosts - Rule Endpoint - High Number of Hosts Not Updating Malware Signatures - Rule Endpoint - High Or Critical Priority Host With Malware - Rule Endpoint - Host Sending Excessive Email - Rule Endpoint - Host With Multiple Infections - Rule Endpoint - Old Malware Infection - Rule Endpoint - Outbreak Observed - Rule Endpoint - Recurring Malware Infection - Rule Identity - Activity from Expired User Identity - Rule Network - High Volume of Traffic From High or Critical Host - Rule Network - Policy Or Configuration Change - Rule Network - Substantial Increase in an Event - Rule Network - Unroutable Host Activity - Rule Network - Vulnerability Scanner Detection (by targets) - Rule Threat - Threat List Activity - Rule	admin	108	1451	155
risk	passive	saved	Access - Default Account Usage - Rule Access - Excessive Failed Logins - Rule	admin	106	1449	140

# ES Deployment Status



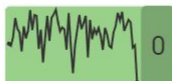
Search Head



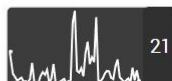
Avg Page Load Time



Average Search Time



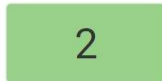
Skipped Searches Over Time



Searches Over Time



Data Models



Incomplete Datamodels



Currently Accelerating



Average Size (MB)



Avg Run Duration (s)



Indexers



Enabled TAs



Average EPD



Maximum EPD



Recent EPD



Forwarders



Forwarder Count



Average Event Count



Average CPU Load (%)



Average Memory Used (MB)

# Risk Analysis

Export ...

Source: All Risk Object: All Last 24 hours Submit Hide Filters + Create Ad-Hoc Risk Entry

**16** 0

**DISTINCT MODIFIER SOURCES**  
Source Count

**322** ↓ -13

**DISTINCT RISK OBJECTS**  
Object Count

**extreme** no change (delta is zero)

**MEDIAN RISK SCORE**  
Overall Median Risk

Currently is: 240

**low** ↓ decreasing minimally

**AGGREGATED SYSTEM RISK**  
Total System Risk

Currently is: 110.9k

**low** ↓ decreasing minimally

**AGGREGATED USER RISK**  
Total User Risk

Currently is: 400

**30** ↓ -5

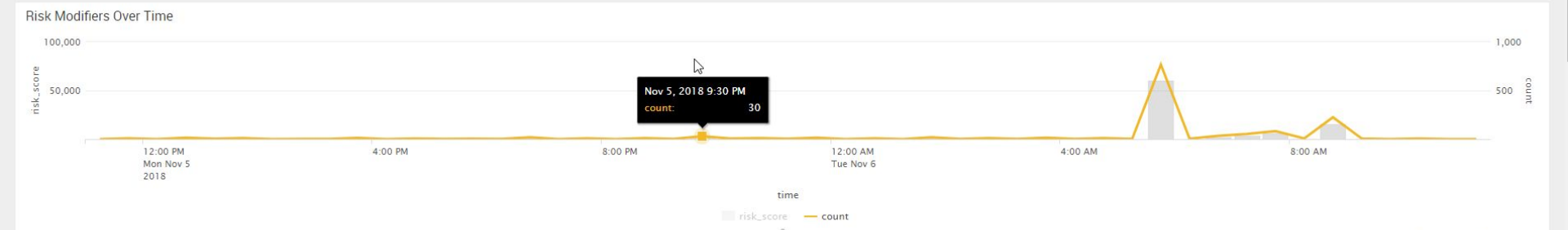
**DISTINCT RISK OTHER OBJECTS**  
Other Object Count

**288** ↓ -11

**DISTINCT RISK SYSTEM OBJECTS**  
System Object Count

**5** ↓ -2

**DISTINCT RISK USER OBJECTS**  
User Object Count



Risk Score By Object					Most Active Sources			
risk_object	risk_object_type	risk_score	source_count	count	source	risk_score	risk_objects	count
#COMPUTERNAME#	system	640	3	8	Endpoint - Recurring Malware Infection - Rule	81360	238	1017
0.0.145.77	system	80	1	1	Endpoint - Host With Multiple Infections - Rule	14320	179	179
0.23.10.164	system	80	1	1	Endpoint - Old Malware Infection - Rule	10240	85	128

# Threat Artifacts

Export ▾ ...

Threat Artifact: Threat ID ▾ | Threat Category: All | Threat Group: All | Malware Alias: | Intel Source ID: | Intel Source Path: Submit Hide Filters

- Threat Overview
- Network
- Endpoint
- Certificate
- Email

## Threat Overview

i	source_id	source_path	source_type	threat_group	threat_category	malware_alias
>	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F admin338 japanorus nitro th3bug wl menupass	APT APT APT	
>	bad_ips	/four/splunk/etc/apps/SA-zeus-demo/lookups/bad_ips.csv	csv	bad_ips	malicious	
>	emerging_threats_compromised_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_compromised_ip_blocklist.csv	csv	emerging_threats_compromised_ip_blocklist	threatlist	
>	emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	emerging_threats_ip_blocklist	threatlist	
>	iblocklist_logmein	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	iblocklist_logmein	threatlist	
>	iblocklist_piratebay	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.csv	csv	iblocklist_piratebay	threatlist	
>	iblocklist_proxy	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv	csv	iblocklist_proxy	threatlist	
>	iblocklist_rapidshare	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.csv	csv	iblocklist_rapidshare	threatlist	
>	iblocklist_spyware	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv	csv	iblocklist_spyware	threatlist	
>	iblocklist_tor	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.csv	csv	iblocklist_tor	threatlist	

« prev 1 2 3 next »

## Endpoint Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
file_intel	stix	undefined	undefined		1356
file_intel	stix	F	APT		194
file_intel	stix	admin338	APT		194
file_intel	stix	japanorus	APT		194

## Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group
ip_intel	csv	337613	0	0	0	337613	iblocklist_tor
ip_intel	csv	0	131136	0	0	131136	malware_domains
ip_intel	csv	42961	0	0	0	42961	emerging_threats_compromised_ip_blocklist
http_intel	csv	0	0	22421	0	22421	phishtank



# Asset management

## Edit Lookup

[< Back to Lookups List](#)

### Edit Lookup File

simple\_asset\_lookup

1	bunit	category	city	country	dns	ip	is_expected	lat	long	mac	nt_host	owner	pci_domain	priority	requires_en
2	apac		Istanbul	TR		6.0.0.1-9.0.0.0		41.040855	28.986183					low	
3	americas		Washington D.C.	USA		1.2.3.4		38.959405	-77.04	00:15:70:91:df:6c				medium	
4	americas	pci cardholder	Pleasanton	USA	CORP1.acmetech.com		true	37.694452	-121.894461				trust	high	
5	americas	pci	Dallas	USA		192.168.12.9-192.168.12.9	true	32.931277	-96.818167		storefront		trust	critical	
6	emea	pci sox	Havant	UK		2.0.0.0/8	true	50.84436	-0.98451				dmz	low	
7	americas	pci hipaa	Washington D.C.	USA		192.168.15.8-192.168.15.10		38.959405	-77.04				trust	medium	
8	americas	iso27002	Pleasanton	USA		192.168.0.0/16		37.694452	-121.894461					high	
9	americas	nerc sox	Dallas	USA		5.6.7.8	true	32.931277	-96.818167	00:12:cf:30:27:b5	millenium-falcon			critical	
10	emea	pci	Havant	UK		192.168.15.9-192.168.15.9		50.84436	-0.98451		acmefileserv		trust	low	
11	americas		Washington D.C.	USA		192.168.15.9-192.169.15.27		38.959405	-77.04					medium	
12	americas	email_servers	Pleasanton	USA		9.10.11.12		37.694452	-121.894461	00:16:5d:10:08:9c				high	
13	americas	virtual	Dallas	USA				32.931277	-96.818167	00:25:bc:42:f4:60-00:25:bc:42:f4:6f				critical	
14	emea	pci	Havant	UK				50.84436	-0.98451	00:25:bc:42:f4:60-00:25:bc:42:f4:60			wireless	low	
15	americas		Washington D.C.	USA				38.959405	-77.04	00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	
16	americas	pci cardholder	Pleasanton	USA	PA-dC02		true	37.694452	-121.894461					high	
17	americas	pci cardholder	Dallas	USA	ACMEaPP		true	32.931277	-96.818167					critical	
18	emea	pci cardholder	Havant	UK	NCORPN0DE1		true	50.84436	-0.98451					high	
19	americas	pci cardholder	Washington D.C.	USA			true	38.959405	-77.04		AcMEDC01			high	
20	americas	pci cardholder	Pleasanton	USA			true	37.694452	-121.894461		macFISH			high	

Cancel

Save

# Asset Investigator

## 10.11.36.20

country: USA  
ip: 10.11.36.20  
owner: Bill\_williams  
priority: critical

category: pci, splunk  
bunit: americas  
long: -121.894461  
pci\_domain: trust

\_time: 2018-11-06T15:10:28-0600  
should\_update: true  
requires\_av: false  
city: Pleasanton

lat: 37.694452  
is\_expected: true  
should\_timesync: true

10/31/2018

11/1/2018

11/2/2018

11/3/2018

11/4/2018

11/5/2018

11/6/2018

All Authentication



All Changes

Search returned no results

Threat List Activity

Search returned no results

Exec File Activity

Search returned no results

Malware Attacks



IDS Attacks



Notable Events



UEBA Threats

Search returned no results

Risk Modifiers



UBA Anomalies

Search returned no results

Last 7 days ▾



10/30

11/06

# Access Anomalies

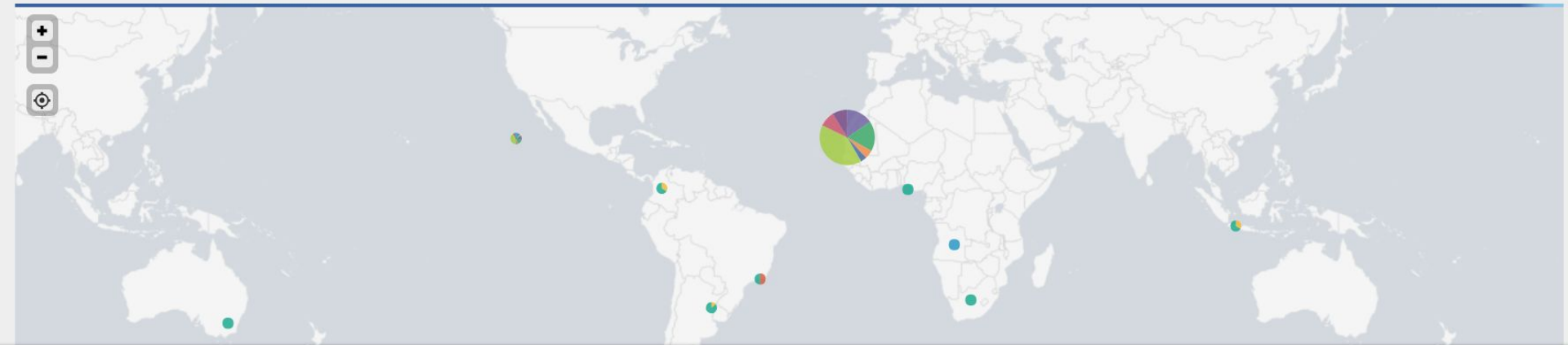
Export > ...

Action: All App: All User: Business Unit: Last 7 days Submit [Hide Filters](#)

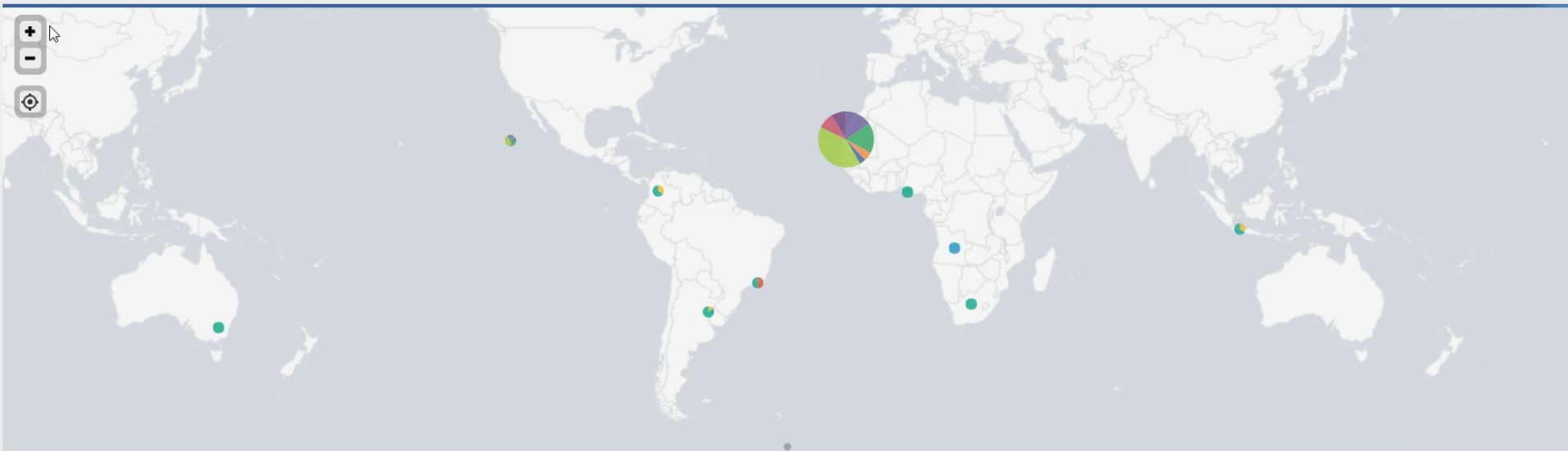
## Geographically Improbable Accesses

user	user_bunit	src	_time	session_city	session_country	app	prev_src	prev_time	prev_city	prev_country	prev_app	distance	speed
ACMEDC01\$		10.11.36.6	2018-11-02 07:57:34	Havant	UK	win:local	10.11.36.23	11/02/2018 07:57:14	Dallas	USA	win:local	7610.90	1369962.00
administrator		10.11.36.40	2018-11-02 07:58:43	Washington D.C.	USA	win.remote	10.11.36.20	11/02/2018 07:58:31	Pleasanton	USA	win.remote	3877.00	1163100.00
administrator		10.11.36.20	2018-11-02 07:58:51	Pleasanton	USA	win.remote	10.11.36.40	11/02/2018 07:58:43	Washington D.C.	USA	win.remote	3877.00	1744650.00
administrator		10.11.36.21	2018-11-02 07:59:07	Dallas	USA	win.remote	10.11.36.20	11/02/2018 07:58:56	Pleasanton	USA	win.remote	2329.20	762283.64
administrator		10.11.36.35	2018-11-02 07:59:30	Washington D.C.	USA	win.remote	10.11.36.21	11/02/2018 07:59:07	Dallas	USA	win.remote	1898.00	297078.26

« prev 1 2 3 4 5 6 7 8 9 10 next »



# Concurrent application Accesses



Concurrent Application Accesses



user	app	src	_time	prev_src	prev_time	time_diff	count
test	sshd	10.11.36.4	2018-10-30 15:00:25	10.11.36.19	10/30/2018 15:00:25	0	1
test3	sshd	10.11.36.30	2018-10-30 15:00:45	10.11.36.24	10/30/2018 15:00:45	0	1
test	sshd	10.11.36.47	2018-10-30 15:01:16	10.11.36.39	10/30/2018 15:01:16	0	1
unknown	oracle	__jdbc__	2018-10-30 15:01:52	Oracle10gR2_linux	10/30/2018 15:01:52	0	12
test	sshd	10.11.36.28	2018-10-30 15:02:00	10.11.36.26	10/30/2018 15:02:00	0	1

# Malware Center

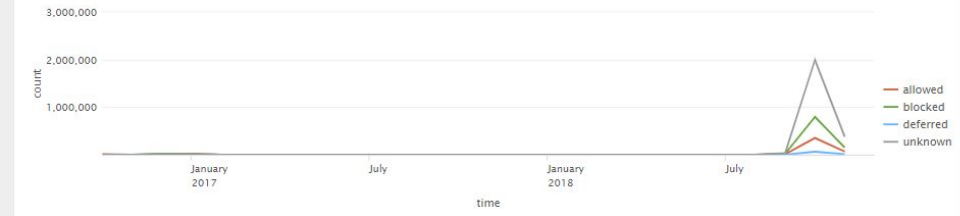
Export ...

Action:  Business Unit:  Category:  All time  [Hide Filters](#)

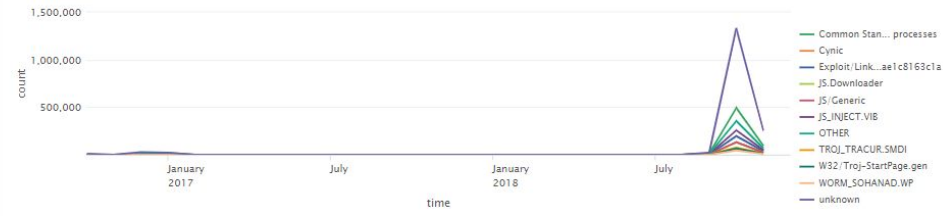
[Edit](#)

<b>NEW INFECTIONS</b> Count <b>0</b>	<b>MULTIPLE INFECTIONS</b> System Count <b>105</b> <span>↓ -15</span>	<b>UNIQUE MALWARE</b> Unique Count <b>61</b>	<b>INFECTED SYSTEMS</b> System Count <b>228</b> <span>↓ -2</span>	<b>TOTAL INFECTIONS</b> Count <b>medium</b> <span>↓ decreasing minimally</span> Currently is: 450
--	---	--	---	--

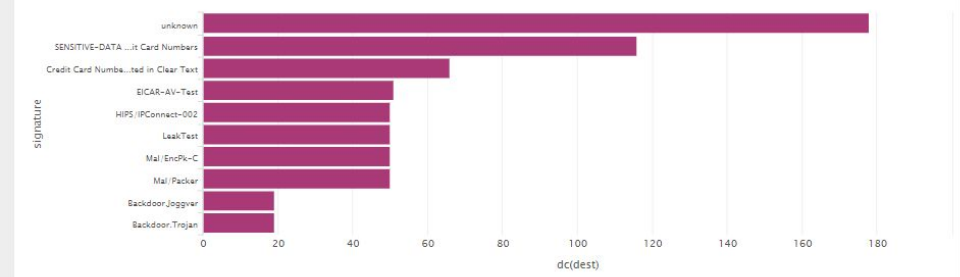
### Malware Activity Over Time By Action



### Malware Activity Over Time By Signature



### Top Infections



### New Malware - Last 30 Days

No results found.

# Vulnerability Center

Export ...

Severity:  Business Unit:  Category:  Last 90 days  [Hide Filters](#)

**VULNS PER SYSTEM**  
Average Count

**29.5** ↑  
+1.2

**VULNERABLE SYSTEMS**  
Percent Vulnerable

**100%**

**VULNERABLE SYSTEMS**  
System Count

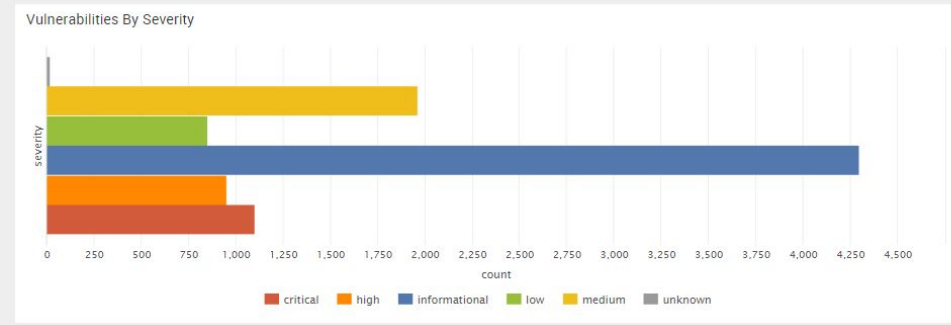
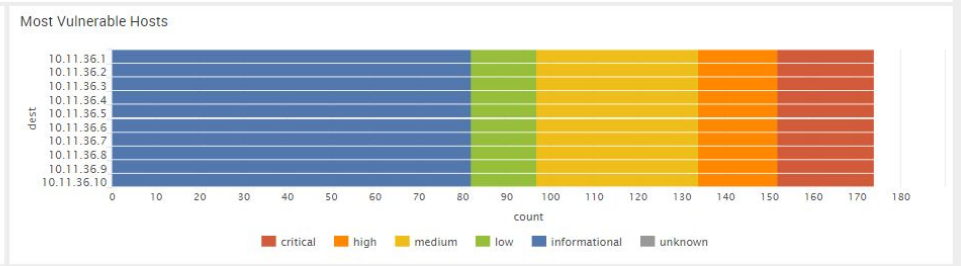
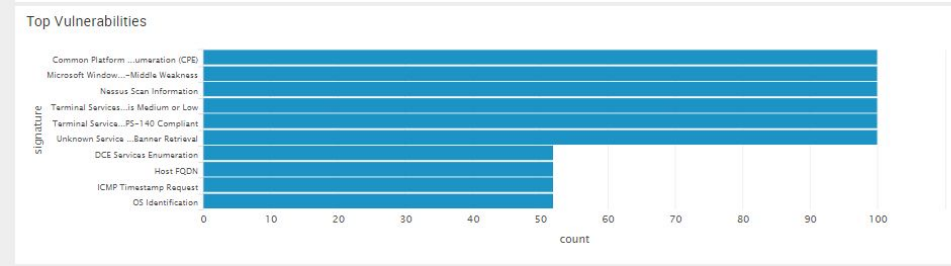
**103** ↑  
+1

**TOTAL VULNS**  
Count

**3k** ↑  
+151

**VULNERABILITY AGE**  
Average Days

**34.9**



### New Vulnerabilities

No results found.



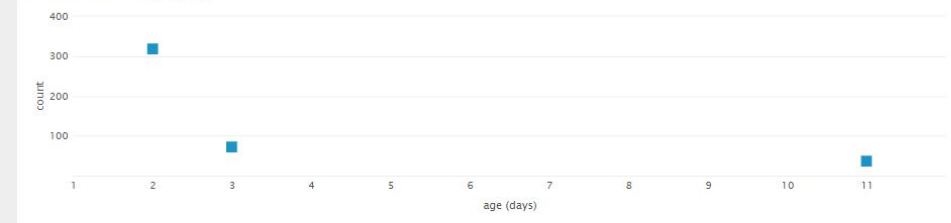
# New Domain Analysis

Domain:  Domain Type:  Maximum Age (days):  Last 24 hours  Hide Filters

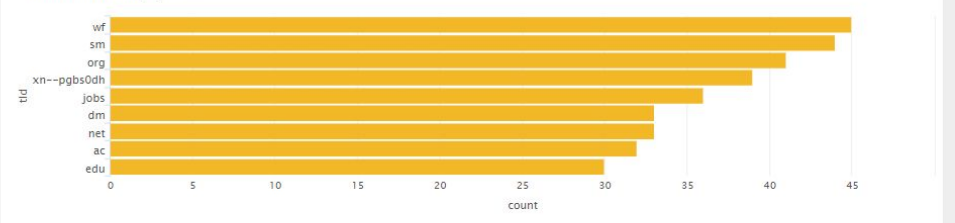
## New Domain Activity

_time	dest	domain	filter	created	Age (days)	alexa_rank	count
2018-11-06T17:09:57.000-06:00	vasfegizezfrhin.net	vasfegizezfrhin.net		11/05/2018 00:00:00	3	below 1 million	33
2018-11-06T17:06:24.000-06:00	grrwgyrtrupmf.ac	grrwgyrtrupmf.ac		11/06/2018 00:00:00	2	below 1 million	32
2018-11-06T17:03:24.000-06:00	ttbxwberpilcpjt.dm	ttbxwberpilcpjt.dm		11/06/2018 00:00:00	2	below 1 million	33
2018-11-06T17:02:23.000-06:00	zqtpdchgtfaveg.sm	zqtpdchgtfaveg.sm		11/06/2018 00:00:00	2	below 1 million	44
2018-11-06T17:02:12.000-06:00	tfrrmvpxtgsgkgx.org	tfrrmvpxtgsgkgx.org		11/06/2018 00:00:00	2	below 1 million	41
2018-11-06T16:57:55.000-06:00	hmrxdxjzmcjdpug.xn--9t4b11yi5a	hmrxdxjzmcjdpug.xn--9t4b11yi5a		11/06/2018 00:00:00	2	below 1 million	41
2018-11-06T16:38:21.000-06:00	jpmnwefrftqnmjdj.xn--11b5bs3e9ajfg	jpmnwefrftqnmjdj.xn--11b5bs3e9ajfg		11/06/2018 00:00:00	2	below 1 million	52
2018-11-06T16:35:15.000-06:00	zkotiwaewfbsra.jobs	zkotiwaewfbsra.jobs		10/28/2018 00:00:00	11	below 1 million	36
2018-11-06T16:33:25.000-06:00	gqtavlekkdkcryl.xn--pgbs0dh	gqtavlekkdkcryl.xn--pgbs0dh		11/05/2018 00:00:00	3	below 1 million	39
2018-11-06T16:32:42.000-06:00	mpesgkjkrvrttk.edu	mpesgkjkrvrttk.edu		11/06/2018 00:00:00	2	below 1 million	30

## New Domain Activity By Age



## New Domain Activity By TLD



## Registration Details

_time	domain	resolved_domain	filter	created	age	expires	nameservers	registrant	registrar
2018-11-7 13:23:24	hmrxdxjzmcjdpug.xn--9t4b11yi5a			11/06/2018 00:00:00	2	06/11/2017 00:00:00	ns1.hmrxdxjzmcjdpug.xn--9t4b11yi5a ns2.hmrxdxjzmcjdpug.xn--9t4b11yi5a ns3.hmrxdxjzmcjdpug.xn--9t4b11yi5a	Malicious Domain Operators, LLC.	Malicious Domain Operators, LLC.
2018-11-7 13:23:24	tlcficjhlotbnw.gov			11/06/2018 00:00:00	2	06/11/2017 00:00:00	ns1.tlcficjhlotbnw.gov ns2.tlcficjhlotbnw.gov ns3.tlcficjhlotbnw.gov	Malicious Domain Operators, LLC.	Malicious Domain Operators, LLC.
2018-11-7 13:23:24	ovuroahuiqgsth.info			11/06/2018 00:00:00	2	06/11/2017 00:00:00	ns1.ovuroahuiqgsth.info ns2.ovuroahuiqgsth.info ns3.ovuroahuiqgsth.info	Malicious Domain Operators, LLC.	Malicious Domain Operators, LLC.

# Practical Exercise: Test your Skills

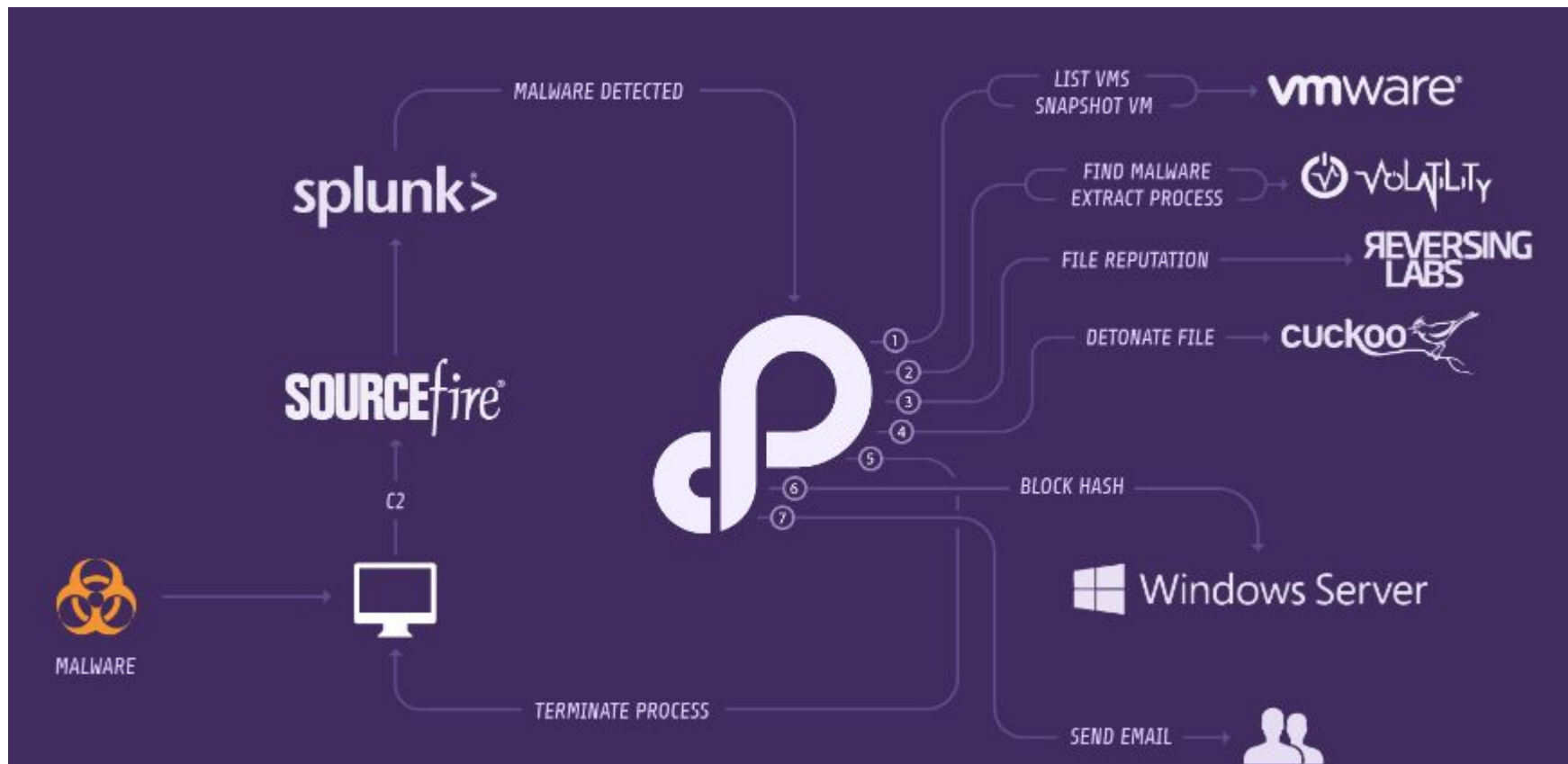
## Access

Web: <https://warroom.underdefense.com/>

User: analyst[1-20]

Password: password1

# IR Playbooks Automation



# IR Playbooks Automation

The screenshot displays the Demisto interface for an incident response (IR) playbook. The main window shows a flowchart titled "Enrichment IOC" with the following steps:

- Incident** (Step #25) - Green box with checkmark.
- Fetch IP reputation** (Step #26) - Green box with checkmark.
- Fetch URL Reputation** (Step #27) - Green box with checkmark.
- Bad url found?** (Step #31) - Green box with checkmark.
- Enrich Domain** (Step #32) - Blue box, currently selected.
- Whois Domain Information** (Step #33) - Grey box.
- Domain GeoLocation** (Step #34) - Grey box.
- Domain Category** (Step #35) - Grey box.
- Collect Hashes from incident** (Step #36) - Green box with checkmark.
- Check for Hashes** (Step #37) - Green box with checkmark.
- Fetch MD5 Reputation** (Step #38) - Green box with checkmark.
- Bad hash found?** (Step #39) - Green box with checkmark and a "Follow" checkbox.
- Malicious Indicators found?** (Step #40) - Green box with checkmark.

The interface includes a left sidebar with navigation options: Home, Incidents, Jobs, Dashboard, Reports, Indicators, Playbooks, Automation, and Settings. A top navigation bar shows the event ID "#5038 Event from Splunk 06-16-17 Alert - sus..." and a search bar. A bottom status bar contains the text "Focus on the CLI field using 'cmd+',".

Invest into your **Training.**  
**Get Prepared!**



СПОРТИВНИ

ИМЯ: \_\_\_\_\_  
ФАМИЛИЯ: \_\_\_\_\_  
ГРУППА: \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_  
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР \_\_\_\_\_

№	Имя	Фамилия	Группа
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

УЭРАИОТИНИ









**I KNOW**

**SPLUNK**

# We resolve the lack of security resources

Augment your team with experts who deliver results beyond expectations in terms of costs, savings and speed

[SEE OUR WORK](#)

## Experts as a Service (EaaS)



Security Operations Center  
Analyst



Risk and Compliance  
Analyst



Penetration  
Tester



# Thank you for your trust

**V2 Version 2** | 二版  
www.version-2.com  
Hong Kong | Taiwan | Singapore | Macau | Mainland China

**Hong Kong & Macau**  
Tel : (852) 2893 8860  
Email : sales@version-2.com.hk

**Taiwan**  
Tel : (886) 02 7722 6899  
Email : sales@version-2.com.tw

**Singapore, Malaysia & SEA**  
Tel : (65) 6296 4268  
Email : sales@version-2.com.sg