

# Exploring The Frameworks Of Splunk Enterprise Security

Dave Herral

Security Architect, Splunk

Kyle Champlin

Senior Sales Engineer, Splunk

.conf2016

splunk>

# Disclaimer

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.

# Agenda

- What Is Splunk Enterprise Security?
- A Look At Security Operations & Toolchains
- Architecture Of Enterprise Security
- A Deep Dive Into The Frameworks Of ES

# Splunk Solutions > Easy To Adopt

Across Data Sources, Use Cases & Consumption Models

## Splunk Premium Solutions



Security



IT Svc Int



VMware



Exchange



PCI



UBA

## Rich Ecosystem of Apps



splunk>enterprise

splunk>cloud

splunk>light

Hunk®

splunk> Platform for Machine Data



Forwarders



Syslog/TCP



Mobile



IoT  
Devices



Network  
Wire Data



Hadoop  
& NoSQL



Relational  
Databases



Mainframe  
Data

# Splunk Solutions > Easy To Adopt

Across Data Sources, Use Cases & Consumption Models

## Splunk Premium Solutions



IT Svc Int



VMware



Exchange



PCI



UBA

## Rich Ecosystem of Apps



splunk>enterprise

splunk>cloud

splunk>light

Hunk®

**splunk>** Platform for Machine Data



Forwarders



Syslog/TCP



Mobile



IoT  
Devices



Network  
Wire Data



Hadoop  
& NoSQL



Relational  
Databases



Mainframe  
Data

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

Adaptive  
Response

# What Is Enterprise Security?

A collection of Frameworks

# Enterprise Security

**Asset and  
Identity  
Correlation**

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

Adaptive  
Response

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

**Notable  
Event**

Threat  
Intelligence

Risk  
Analysis

Adaptive  
Response

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

Adaptive  
Response

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

Adaptive  
Response

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

**Adaptive  
Response**

# What Is Enterprise Security?

A collection of Frameworks

## Enterprise Security

Asset and  
Identity  
Correlation

Notable  
Event

Threat  
Intelligence

Risk  
Analysis

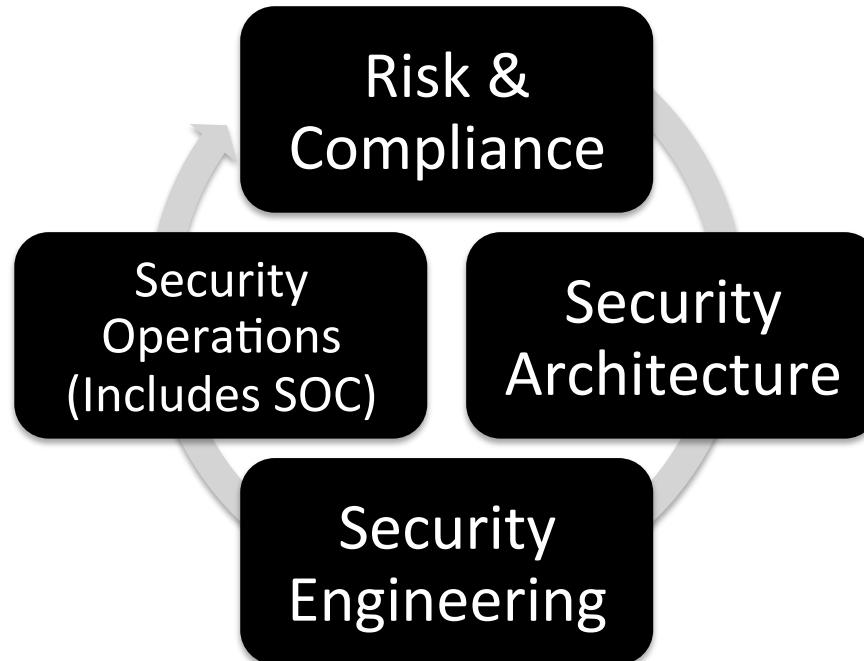
Adaptive  
Response

# Security Operations



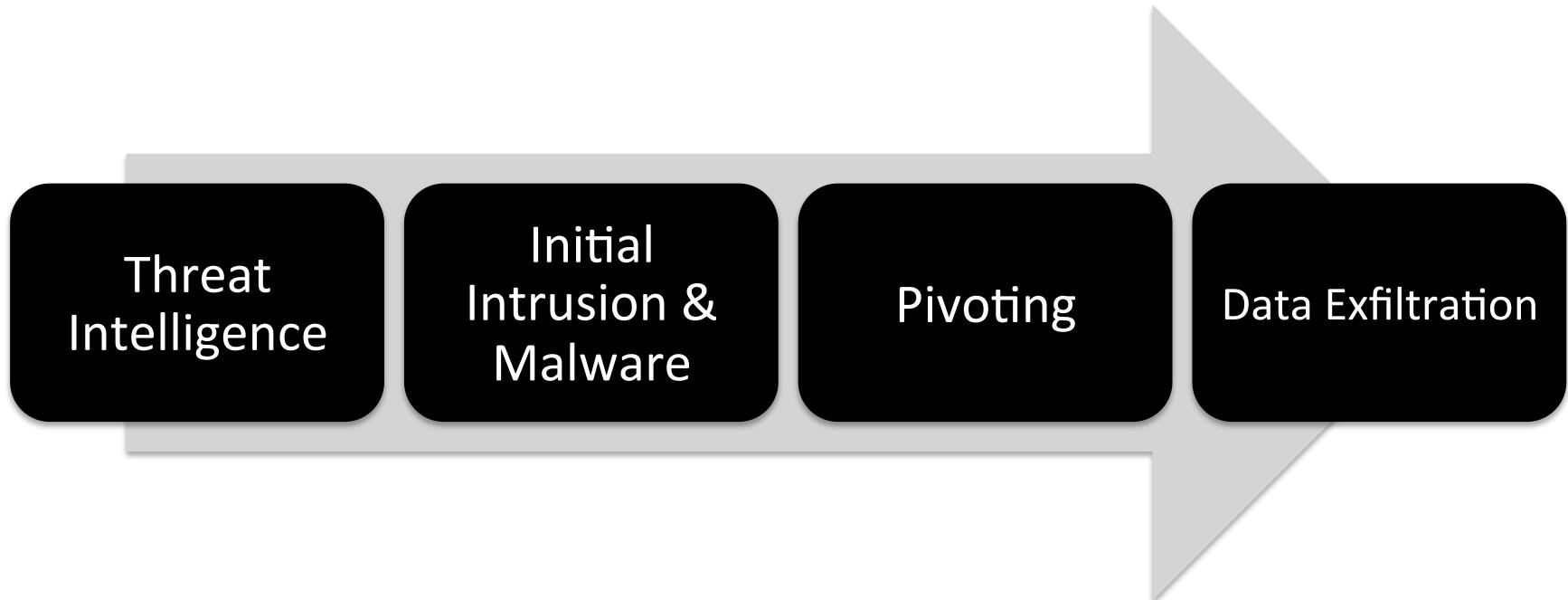
# Traditional?

Security Operations: an important part of a bigger security picture...

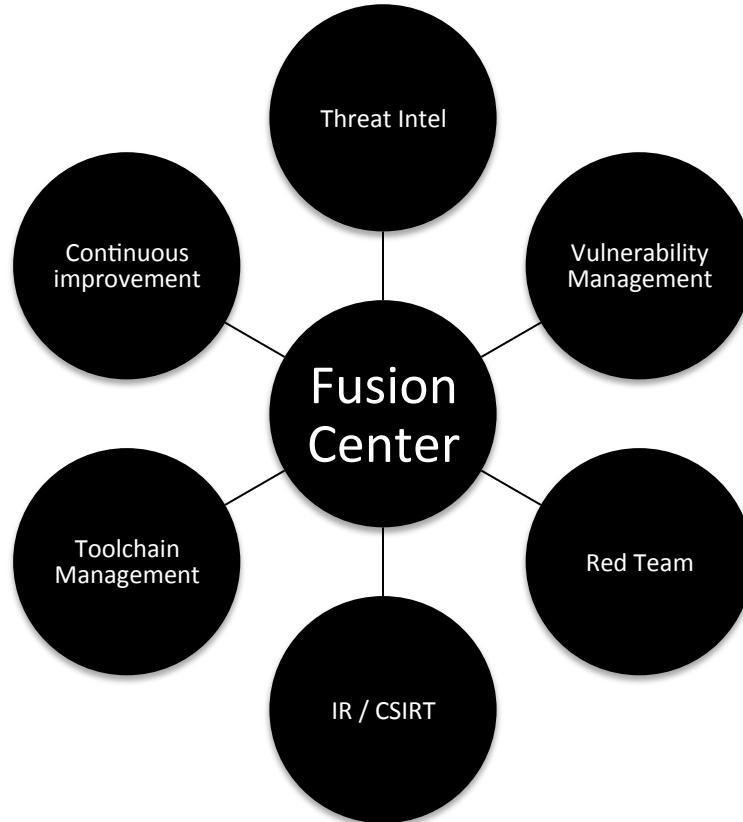


# Kill Chain Based

This is how you are attacked, why not organize to defend?



# Cyber Fusion Center



# What Customers Tell Us...

# What Customers Tell Us...

"I always choose a brain  
over a product."

# What Customers Tell Us...

"I always choose a brain  
over a product."

"We want to build our own  
tooling on Splunk"

# What Customers Tell Us...

"I always choose a brain  
over a product."

"We want to build our own  
tooling on Splunk"

"Can we integrate <security  
tool X> with ES?"

# The Architecture Of ES

It's just Splunk!

Splunk Apps	Alert Actions	Tags	Saved Searches	Python Scripts	Regex	Data Model Acceleration
Lookups	REST Endpoints	Summary Indexes	SPL	Modular Inputs	SHC	Transforms
Macros	Field Extractions	Eventtypes	Sourcetypes	KV Store Collections	Dashboards	

Enterprise Security (SA, DA, TA)

splunk>

# Asset And Identity Correlation System Inventory in ES

The screenshot shows the Splunk Enterprise Security interface with the 'Edit Lookup' page open. The page title is 'Edit Lookup' and the sub-section is 'Edit Lookup File' for 'demo\_asset\_lookup'. The table contains 14 rows of asset data:

1	ip	mac	nt_host	dns	owner	priority	lat	long	city
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183	Istanbul
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington
4				CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167	Dallas
6	2.0.0.0/8					low	50.84436	-0.98451	Havant
7	192.168.15.8-192.168.15.10					medium	38.959405	-77.04	Washington
8	192.168.0.0/16					high	37.694452	-121.894461	Pleasanton
9	5.6.7.8	00:12:cf:30:27:b5	millenium-falcon			critical	32.931277	-96.818167	Dallas
10	192.168.15.9-192.168.15.9		acmefileserver			low	50.84436	-0.98451	Havant
11	192.168.15.9-192.169.15.27					medium	38.959405	-77.04	Washington
12	9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton
13		00:25:bc:42:f4:60-00:25:bc:42:f4:6f				critical	32.931277	-96.818167	Dallas
14		00:25:bc:42:f4:60-00:25:bc:42:f4:60				low	50.84436	-0.98451	Havant

# Asset And Identity Correlation

## System Inventory in ES

ip	dns	nt_host	dns	owner	long	city	category	pci_domain	ls_expected	should_timesync	should_update	requires_AV
6.0.0.1-9.0.0	00:15:70-91:df:6c			CORP1.acmetech.com	41.040855	Istanbul	low	38.959405	-77.04	-121.894461	Pleasanton	Dallas
1.2.3.4				storefront	50.84436	Havant	medium	32.931277	-96.818167	-121.894461	Pleasanton	Dallas
192.168.12.9-192.168.12.9					50.84436	Washington	critical	37.694452	-121.894461	-96.818167	Havant	Washington
2.0.0.0/8					50.84436	Havant	low	32.931277	-96.818167	-121.894461	Pleasanton	Dallas
192.168.15.8-192.168.16.8					50.84436	Washington	medium	38.959405	-77.04	-121.894461	Havant	Washington
192.168.0.0/16					50.84436	Havant	high	37.694452	-121.894461	-96.818167	Pleasanton	Dallas
5.6.7.8	00:15:cf:01:27:b5		millenium-falcon		50.84436	Washington	critical	37.694452	-121.894461	-96.818167	Havant	Washington
192.168.15.9-192.169.15.27				acmefileserver	50.84436	Havant	medium	38.959405	-77.04	-121.894461	Pleasanton	Dallas
9.10.11.12	00:15:10:08:9c				50.84436	Washington	high	37.694452	-121.894461	-96.818167	Pleasanton	Dallas
	4:60-00:25:bc:42:f4:6f				50.84436	Havant	low	32.931277	-96.818167	-121.894461	Pleasanton	Dallas
	00:25:bc:42:f4:60-00:25:bc:42:f4:60				50.84436	Havant						
14												

# Asset And Identity Correlation

## Available throughout ES

splunk > App: Enterprise Security

Administrator Messages Settings Activity Help

Enterprise Security

### Asset Center

Asset Priority Business Unit Category Owner

Assets By Priority

Priority	Events
high	~24
informational	~17
low	~8
medium	~35

Assets By Business Unit

Business Unit	Percentage
americas	~55%
apac	~25%
emea	~10%
sox	~10%

Assets By Category

Category	Count
billing	~45%
cardholder	~10%
other (6)	~10%
virtual	~10%
pci	~25%

### Asset Information

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync
5.6.7.8	00:12:cf:30:27:b5	millennium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerc	untrust	true	true
1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas	sox	untrust	false	true
9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers	untrust	false	true
	00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas		untrust	false	true

No investigation is currently loaded. Please create (+) or load an existing one (≡).

# Asset And Identity Correlation

## Available throughout ES

Asset data

The screenshot shows the Splunk Enterprise Security Asset Center. At the top, there are search and filter fields for Asset, Priority, Business Unit, Category, and Owner, along with a Submit button. Below these are three main visualizations: a horizontal bar chart titled 'Assets By Priority' showing the count of events for low and medium priority assets; a pie chart titled 'Assets By Business Unit' showing the distribution across emea, apac, and americas; and another pie chart titled 'Assets By Category' showing the distribution across billing, cardholder, other, virtual, sox, and pci categories. At the bottom, a table titled 'Assets' lists specific asset details such as IP, MAC, NT Host, DNS, Owner, Priority, Latitude, Longitude, City, Country, Business Unit, Category, PCI Domain, Is Expected, and Should Timesync. A note at the bottom states 'No investigation is currently loaded. Please create (+) or load an existing one (=)'.

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync
5.6.7.8	00:12:cf:30:27:b5	millennium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerc	untrust	true	true
1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas	sox	untrust	false	true
9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers	untrust	false	true
	00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas		untrust	false	true

# Asset And Identity Correlation

## Available throughout ES

The screenshot shows the Splunk Enterprise Security Asset Center interface. At the top, there are search and filter fields for Asset, Priority, Business Unit, Category, and Owner. Below these are three main visualizations: a horizontal bar chart titled 'Assets By Priority' showing event counts for low and medium priority; a pie chart titled 'Assets By Business Unit' showing proportions for emea, apac, and americas; and another pie chart titled 'Assets By Category' showing proportions for cardholder, other (virtual), and pci. A callout bubble labeled 'Visualization & filters' points to the top right of the interface. Another callout bubble labeled 'Asset data' points to the bottom left, where a table titled 'Assets' displays detailed information for several assets, including IP, MAC, and various metadata fields like owner, priority, and location.

Asset data

Visualization & filters

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync
5.6.7.8	00:12:cf:30:27:b5	millennium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerc sox	untrust	true	true
1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas		untrust	false	true
9.10.11.12	00:16:5d:10:08:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers	untrust	false	true
	00:25:ac:42:f4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas		untrust	false	true

No investigation is currently loaded. Please create (+) or load an existing one (≡).

# Asset And Identity Correlation

## Available in core Splunk, too

The screenshot shows the Splunk Enterprise Security interface with the following details:

- Search Bar:** sourcetype=nessus\*
- Event Count:** 26,618 events (before 8/19/16 10:42:58.000 AM) | No Event Sampling
- Selected Fields:** host 1, source 1, sourcetype 3
- Interesting Fields:** control 1, count 14, dest 100, dest\_asset\_id 54, dest\_asset\_tag 12, dest\_bunit 3, dest\_category 5, dest\_city 6, dest\_country 4
- Dest Asset Tag Distribution:** A histogram titled "dest\_asset\_tag" showing 12 values across 90.86% of events. The top 10 values are: should\_timesync (24,192), should\_update (24,192), pci (19,590), emea (13,153), americas (11,008), expected (10,908), cardholder (4,518), OracleDB (1,320), splunk (452), and requires\_av (123). The chart has a "1 hour per column" scale.
- Event Examples:** Three event snippets are shown:
  - :34 2016" dest\_dns=SJCDCSV012ERP01 dest\_nt\_host=SJCDCSV012ERP01 dest\_port\_proto="someapp(2212/tcp)" severity\_id=5 signature\_id=1154 3"
  - :13 2016" dest\_dns=SJCDCSV012ERP01 dest\_nt\_host=SJCDCSV012ERP01 dest\_port\_proto="someapp(1957/tcp)" severity\_id=5 signature\_id=1868 execution (903235)"
  - :40 2016" dest\_dns=SJCDCSV012ERP01 dest\_nt\_host=SJCDCSV012ERP01 dest\_port\_proto="microsoft-ds(445/tcp)" severity\_id=3 signature\_id=
- Footer:** host = 127.0.0.1 : source = eventgen : sourcetype = nessus\*

# Asset And Identity Correlation

## Available in core Splunk, too

Nessus vulnerabilities

The screenshot shows the Splunk Enterprise Security interface with a search bar containing "sourcetype=nessus\*". The search results show 26,618 events from August 19, 2016. A modal window titled "dest\_asset\_tag" displays a histogram of 12 asset tags, with "should\_timesync" and "should\_update" being the top values at 100% count. Below the histogram, a table lists the top 10 asset tags with their counts and percentages. The table data is as follows:

Top 10 Values	Count	%
should_timesync	24,192	100%
should_update	24,192	100%
pci	19,590	80.977%
emea	13,153	54.369%
americas	11,008	45.503%
expected	10,908	45.089%
cardholder	4,518	18.676%
OracleDB	1,320	5.456%
splunk	452	1.868%
requires_av	123	0.508%

Below the histogram, several event snippets are shown, such as:

```
:34 2016" dest_dns=SJCDCSV012ERP01 dest_nt_host=SJCDCSV012ERP01 dest_port_proto="someapp(2212/tcp)" severity_id=5 signature_id=11543"
```

```
:13 2016" dest_dns=SJCDCSV012ERP01 dest_nt_host=SJCDCSV012ERP01 dest_port_proto="someapp(1957/tcp)" severity_id=5 signature_id=1868 execution (903235)"
```

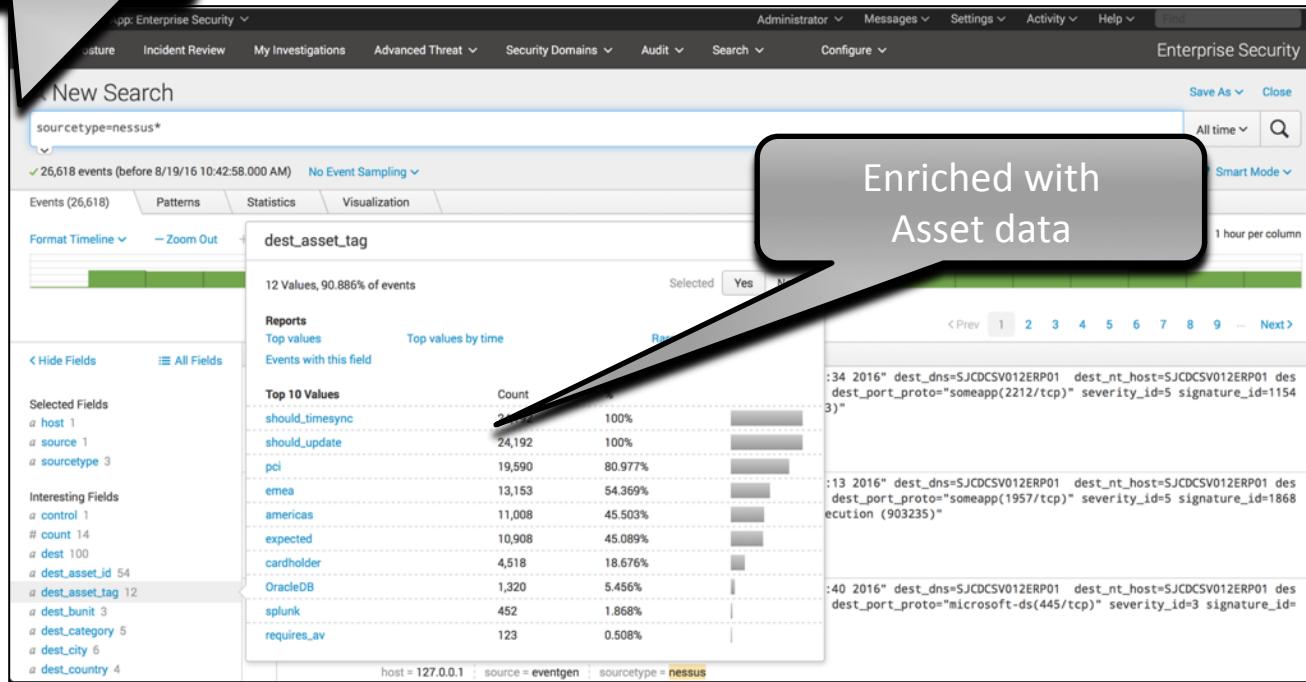
```
:40 2016" dest_dns=SJCDCSV012ERP01 dest_nt_host=SJCDCSV012ERP01 dest_port_proto="microsoft-ds(445/tcp)" severity_id=3 signature_id=
```

At the bottom of the search results, there is a footer with the text "host = 127.0.0.1 : source = eventgen : sourcetype = nessus\*".

# Asset And Identity Correlation

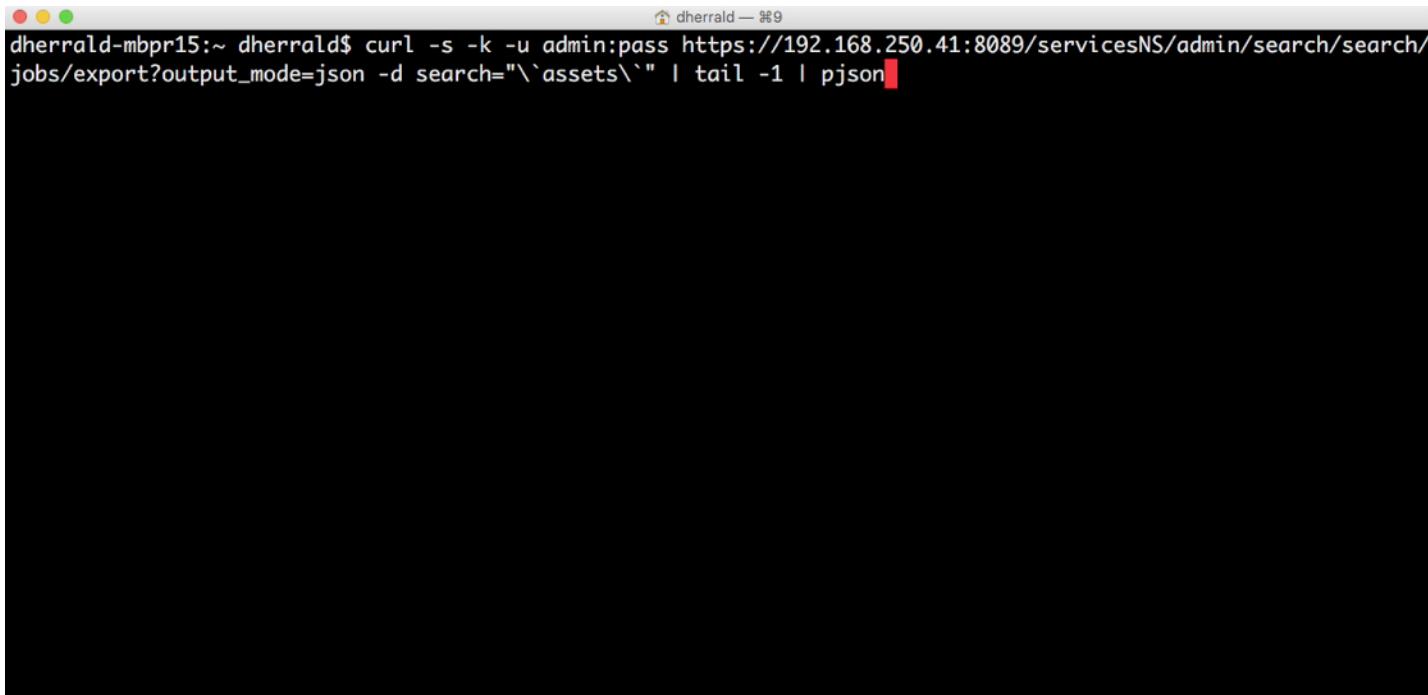
## Available in core Splunk, too

Nessus vulnerabilities



# Asset And Identity Correlation

## Available via API, too



```
dherrald:~ dherrald$ curl -s -k -u admin:pass https://192.168.250.41:8089/servicesNS/admin/search/search/jobs/export?output_mode=json -d search="\`assets\`" | tail -1 | pjson
```

```
curl -s -k -u admin:pass https://192.168.250.41:8089/servicesNS/admin/search/search/jobs/export?output_mode=json -d search="\`assets\`" | tail -1 | pjson
```

# Asset And Identity Correlation

## User List ES

The screenshot shows the Splunk Enterprise Security interface with the 'Edit Lookup' page for 'demo\_identity\_lookup'. The table displays user data with columns for identity, prefix, nick, first, last, suffix, email, phone, phone2, managedBy, priority, bunit, and category. Status indicators are shown as colored cells: green for low, yellow for medium, orange for high, red for critical, and grey for americas.

1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category
34				Gordon	Clough		gclough@acmetech.com	+1 (800)555-5530	+1 (800)555-7083	lietzow.tim		americas	
35		Mr.		Emile	Gamm		egamm@acmetech.com	+1 (800)555-8152	+1 (800)555-4527		low	americas	
36		Dr.		Paul	Faurote		pfaurote@acmetech.com	+1 (800)555-8822	+1 (800)555-5168		medium	americas	
37	pineapple			Forrest	Glaviano		fglaviano@acmetech.com	+1 (800)555-8904	+1 (800)555-1053		high	americas	sox
38		Mr.	Bobby	Robert	Linebaugh		blinebaugh@acmetech.com	+1 (800)555-1708	+1 (800)555-9342		critical	americas	
39		Dr.		Ian	Doiley		idoiley@acmetech.com	+1 (800)555-5475	+1 (800)555-3981	lietzow.tim		americas	intern
40				Julio	Newberg	II	jnewberg@acmetech.com	+1 (800)555-6611	+1 (800)555-6015			americas	
41		Mr.		Wilfred	Groce		wgroce@acmetech.com	+1 (800)555-4409	+1 (800)555-7116		low	americas	
42	bakeryohlerw	Dr.		Wendell	Ohler		wohler@acmetech.com	+1 (800)555-7179	+1 (800)555-1374		medium	americas	pcicardholder
43				Sebastian	Mamone		smamone@acmetech.com	+1 (800)555-6790	+1 (800)555-3276		high	americas	
44	hax0r	Mr.		Hershel	Trapper		htrapper@acmetech.com	+1 (800)555-3039	+1 (800)555-3154		critical	americas	
45		Dr.		Efrain	Cudan		ecudan@acmetech.com	+1 (800)555-9049	+1 (800)555-3814			americas	
46			Nathan	Nathanael	Pernesky		npernesky@acmetech.com	+1 (800)555-1713	+1 (800)555-5253			americas	

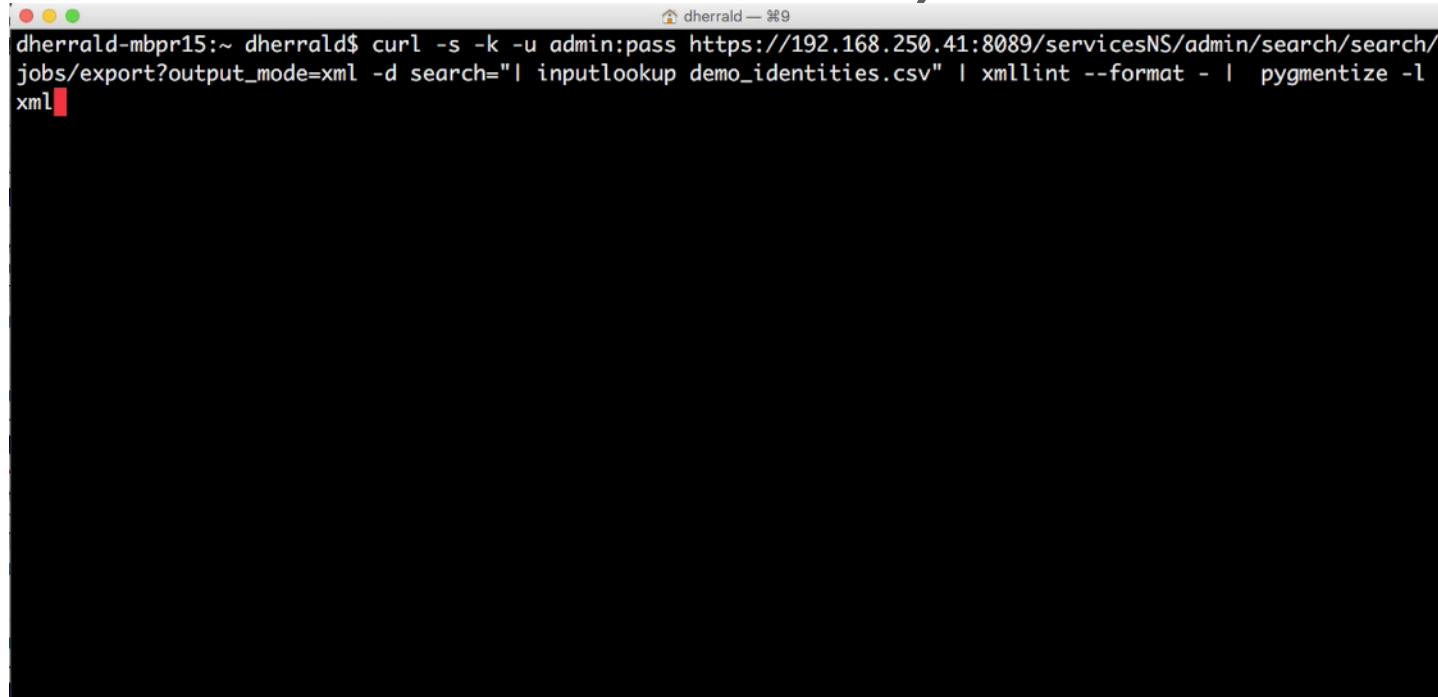
# Asset And Identity Correlation

## User List ES

1	identity	Priority	Name	Business unit	Email	Category*	Phone	Watchlist	Manager	Start/end dates
34		high	gclough	americas	gclough@acmetech.com	high	+1 (800)555-1234	low	John	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
35		medium	Emile	americas	egamm@acmetech.com	medium	+1 (800)555-8152	high	Emile	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
36		medium	Paul	americas	pfaurote@acmetech.com	medium	+1 (800)555-8822	medium	Paul	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
37	pineapple	high	Forrest	americas	fglaviano@acmetech.com	high	+1 (800)555-1052	high	Forrest	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
38		medium	Ian	americas	blinebaugh@acmetech.com	medium	+1 (800)555-1545	medium	Ian	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
39		medium	Dr.	americas	idooley@acmetech.com	medium	+1 (800)555-8475	medium	Dr.	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
40		high	Julio	americas	jnewberg@acmetech.com	high	+1 (800)555-6611	high	Julio	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
41		medium	Wilfred	americas	wgroce@acmetech.com	medium	+1 (800)555-4049	medium	Wilfred	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
42	bakeryjohn	medium	Groce	americas	wohler@acmetech.com	medium	+1 (800)555-1949	medium	Groce	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
43		medium	smamone	americas	smamone@acmetech.com	medium	+1 (800)555-5577	medium	smamone	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
44	hax0r	high	Hershel	americas	htrapper@acmetech.com	high	+1 (800)555-3039	high	Hershel	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
45		medium	Trapper	americas	ecudan@acmetech.com	medium	+1 (800)555-9049	medium	Trapper	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z
46		medium	Nathan	americas	npernesky@acmetech.com	medium	+1 (800)555-1713	medium	Nathan	2016-01-01T00:00:00Z/2016-12-31T23:59:59Z

# Asset And Identity Correlation

## Available via API, too



```
dherrald-mbpr15:~ dherrald$ curl -s -k -u admin:pass https://192.168.250.41:8089/servicesNS/admin/search/search/jobs/export?output_mode=xml -d search="| inputlookup demo_identities.csv" | xmllint --format - | pygmentize -l xml
```

```
curl -s -k -u admin:pass https://192.168.250.41:8089/servicesNS/admin/search/search/jobs/export?output_mode=xml -d search="| inputlookup demo_identities.csv"
```

# Asset And Identity Correlation

## Handle multiple systems of record easily

The screenshot shows a Splunk interface titled "Edit Lookup" for "demo\_identity\_lookup". The interface includes a navigation bar with links like Security Posture, Incident Review, My Investigations, Advanced Threat, Security Domains, Audit, Search, and Configure. The main area displays a table of data with columns: 1, identity, prefix, nick, first, last, suffix, email, phone, phone2, managedBy, priority, bunit, and category. Overlaid on this table is large blue text reading "Active Directory", "LDAP", "Provisioning System (Sailpoint)", and "Custom".

1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category
34				Gordon	Clough		gclough@acmetech.com	+1 (800)555-5530	+1 (800)555-7083	lietzow.tim		americas	
35		Mr.		Emile	Gamm		egamm@acmetech.com	+1 (800)555-8152	+1 (800)555-4527		low	americas	
36				Paul	Eurote		peurote@acmetech.com	+1 (800)555-8822	+1 (800)555-5168		medium	americas	
37				Isaac	Glouc		iglouc@acmetech.com	+1 (800)555-3000	+1 (800)555-7083	lietzow.tim	critical	americas	internal
38				Ian	Dolley		idooley@acmetech.com	+1 (800)555-5475	+1 (800)555-3981	lietzow.tim		americas	intern
39		Dr.		Julio	Newberg	II	jnewberg@acmetech.com	+1 (800)555-6611	+1 (800)555-6015			americas	
40				Wilfred	Groce		wgroce@acmetech.com	+1 (800)555-4409	+1 (800)555-7116		low	americas	
41		Mr.		Wendell	Ohler		wohler@acmetech.com	+1 (800)555-7179	+1 (800)555-1374		medium	americas	pci cardholder
42	bakery ohlerw	Dr.		Sebastian	Mamone		smamone@acmetech.com	+1 (800)555-6790	+1 (800)555-3276		high	americas	
43				Hershel	Trapper		htrapper@acmetech.com	+1 (800)555-3039	+1 (800)555-3154		critical	americas	
44	hax0r	Mr.		Efrain	Cudan		ecudan@acmetech.com	+1 (800)555-9049	+1 (800)555-3814			americas	
45		Dr.		Nathan	Nathanael	Pernesky	npernesky@acmetech.com	+1 (800)555-1713	+1 (800)555-5253			americas	
46													

# Asset And Identity Correlation

## Category field is multi-valued

splunk > App: Enterprise Security

Administrator Messages Settings Activity Help Find

Enterprise Security

Security Posture Incident Review My Investigations Advanced Threat Security Domains Audit Search Configure

### Edit Lookup

[Back to Lookups List](#)

**Edit Lookup File**

**demo\_asset\_lookup**

	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_upd
1				low	41.040855	28.986183	Istanbul	TR	apac			true	true	
2				medium	38.959405	-77.04	Washington D.C.	USA	americas			true	true	
3	f:6c			high	37.694452	-121.894461	Pleasanton	USA	americas	pci cardholder	trust	true	true	
4		CORP1.acmetech.com		critical	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	
5		storefront		low	50.84436	-0.98451	Havant	UK	emea	pci sox	dmz	true	true	
6				medium	38.959405	-77.04	Washington D.C.	USA	americas	pci hipaa	trust	true	true	
7				high	37.694452	-121.894461	Pleasanton	USA	americas	iso27002		true	true	
8				critical	32.931277	-96.818167	Dallas	USA	americas	nerc sox		true	true	
9	7:b5	millenium-falcon		low	50.84436	-0.98451	Havant	UK	emea	pci	trust	true	true	
10		acmefilesserver		medium	38.959405	-77.04	Washington D.C.	USA	americas			true	true	
11				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers		true	true	
12	8:9c			critical	32.931277	-96.818167	Dallas	USA	americas	virtual		true	true	
13	4:60-00:25:bc:42:f4:6F			low	50.84436	-0.98451	Havant	UK	emea	pci	wireless	true	true	
14	4:60-00:25:bc:42:f4:60			medium	38.959405	-77.04	Washington D.C.	USA	americas			true	true	
15	4:60-00:25:cc:42:f4:60			high	50.84436	-0.98451	Havant	UK	emea	pci cardholder		true	true	
16		PA-dC02		high	37.694452	-121.894461	Pleasanton	USA	americas	pci cardholder		true	true	
17		ACMEapp		critical	32.931277	-96.818167	Dallas	USA	americas	pci cardholder		true	true	
18		NCoRPNoDE1		high	50.84436	-0.98451	Havant	UK	emea	pci cardholder		true	true	
19		AcMEDC01		high	38.959405	-77.04	Washington D.C.	USA	americas	pci cardholder		true	true	
20		macFISH		high	37.694452	-121.894461	Pleasanton	USA	americas	pci cardholder		true	true	

# Asset And Identity Correlation

## Category field is multi-valued

The screenshot shows the Splunk interface for editing a lookup file named 'demo\_asset\_lookup'. The left sidebar lists hosts with their IP addresses and names: 192.168.1.6c, storefront, 192.168.1.7.b5, millenium, acmefiles, 192.168.1.8.9c, 192.168.1.60-00:25:bc:42:f4:6F, 192.168.1.60-00:25:bc:42:f4:60, 192.168.1.60-00:25:cc:42:f4:60, AcMEDCO, and macFISH. The main area displays a table titled 'Edit Lookup' with the following data:

category	pci_domain	is_expected	should_timesync	should_update
pci cardholder	trust	true	true	true
pci	trust	true	true	true
pci sox	dmz	true	true	true
pci hipaa	trust		true	true
iso27002			true	true
nerc sox		true	true	true
pci	trust		true	true
			true	true

A preview pane on the right shows the same data with the columns 'expected', 'should\_timesync', and 'should\_update' added. A 'Save' button is located at the bottom right of the main table area.

# Asset And Identity Correlation

## Category field is multi-valued

The screenshot shows the Splunk interface for editing a lookup file named 'demo\_asset\_lookup'. The 'category' column is highlighted with a red border, indicating it is a multi-valued field. The table data is as follows:

category	pci_domain	is_expected	should_timesync	should_update
pci cardholder	trust	true	true	true
pci	trust	true	true	true
pci sox	dmz	true	true	true
pci hipaa	trust		true	true
iso27002			true	true
nerc sox		true	true	true
pci	trust		true	true
			true	true

# Asset And Identity Correlation

## Category field is multi-valued

The screenshot shows a Splunk interface for 'Enterprise Security' with a 'Lookup' table titled 'demo\_asset\_lookup'. The table has columns: 'category', 'pci\_domain', 'is\_expect', and 'should\_update'. A red box highlights the 'category' column, which contains values like 'pci|cardholder', 'pci', 'pci|sox', 'pci|hipaa', 'iso27002', 'nerc|sox', and 'pci'. A callout bubble points to this column with the text 'Multiple values separated by pipes'. The 'pci\_domain' column shows 'trust' for most entries, except for 'pci|sox' which shows 'dmz'. The 'is\_expect' and 'should\_update' columns are mostly 'true'.

category	pci_domain	is_expect	should_update
pci cardholder	trust	true	true
pci	trust	true	true
pci sox	dmz	true	true
pci hipaa	trust	true	true
iso27002		true	true
nerc sox		true	true
pci	trust	true	true
		true	true

# Notable Events

## Where Correlation Searches are Surfaced

### Incident Review

Urgency

CRITICAL	4
HIGH	125
MEDIUM	123
LOW	6
INFO	0

Status

x All	<input type="text"/>
-------	----------------------

Name

<input type="text"/>	<input type="text"/>
----------------------	----------------------

Owner

x All	<input type="text"/>
-------	----------------------

Search

<input type="text"/>	<input type="text"/>
----------------------	----------------------

Security Domain

x All	<input type="text"/>
-------	----------------------

Time

Last 24 hours
---------------

Tag

<input type="text"/>	<input type="button" value="Submit"/>
----------------------	---------------------------------------

✓ 258 events (8/18/16 1:00:00.000 PM to 8/19/16 1:45:21.000 PM)

Format Timeline ▾   Zoom Out   + Zoom to Selection   × Deselect

1 hour per column

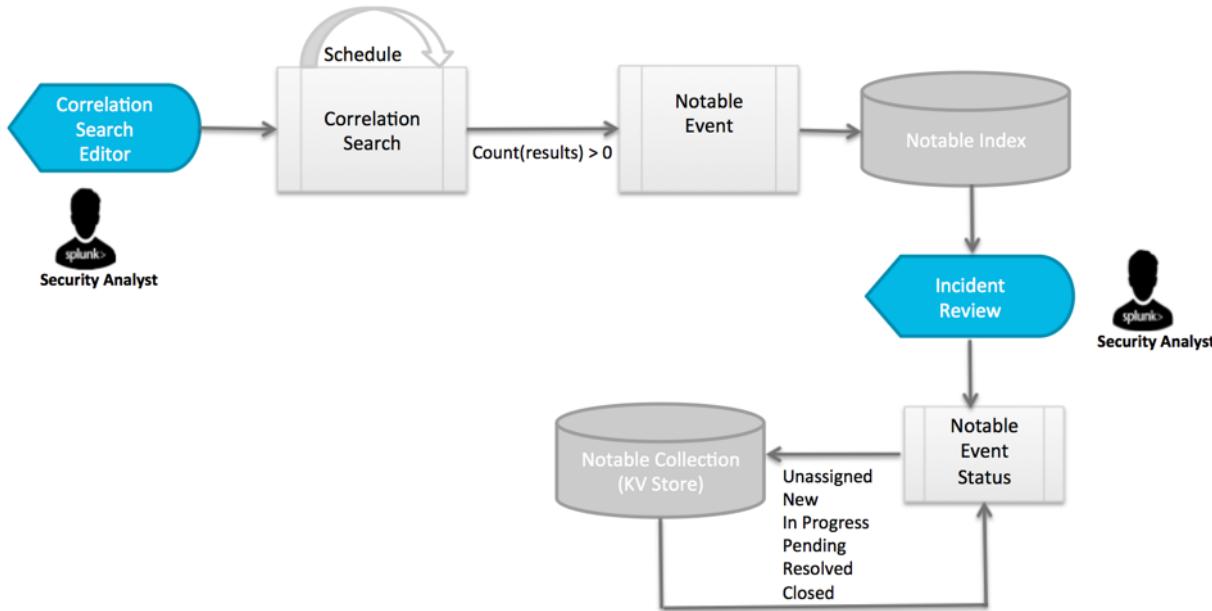
90  
50  
0

6:00 PM Thu Aug 18 2016  
12:00 AM Fri Aug 19  
6:00 AM  
12:00 PM

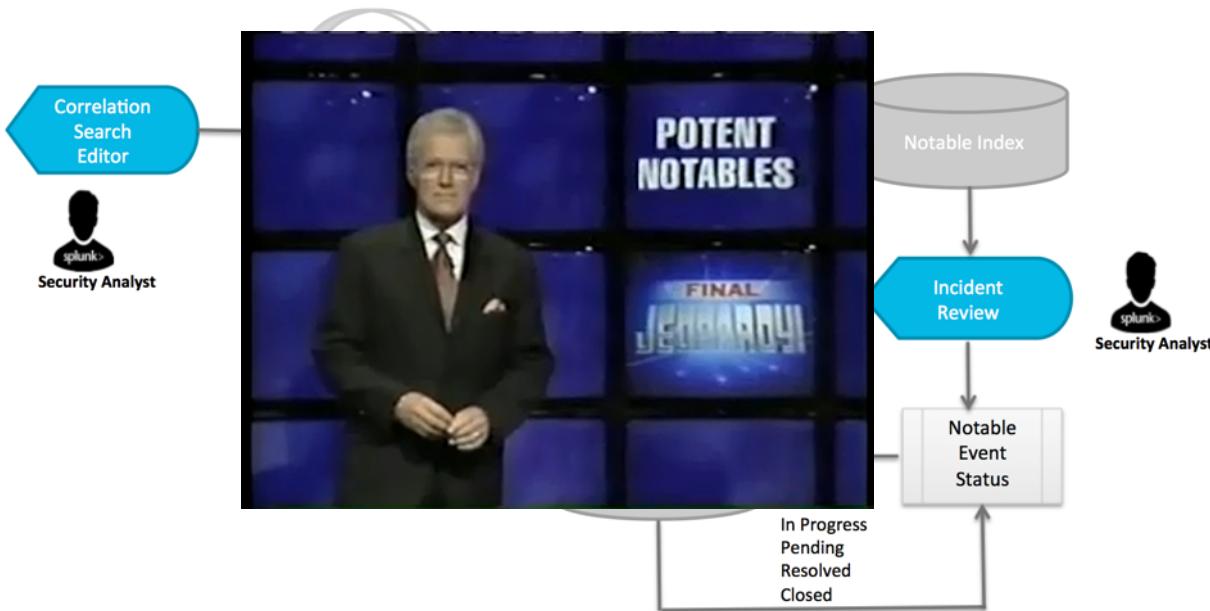
prev 1 2 3 4 5 6 7 8 9 10 next

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	8/19/16 1:03:54.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	! High	Identification	unassigned	▼
>	8/19/16 12:20:21.000 PM	Endpoint	Host With Multiple Infections (10.11.36.43)	! Medium	Identification	unassigned	▼
>	8/19/16 12:20:18.000 PM	Endpoint	Host With Multiple Infections (10.11.36.36)	! High	Identification	unassigned	▼
>	8/19/16 12:10:05.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	! High	Identification	unassigned	▼
>	8/19/16 12:03:53.000 PM	Endpoint	High Or Critical Priority Host With Malware Detected	! High	Identification	unassigned	▼
>	8/19/16 12:00:34.000 PM	Endpoint	High Number Of Infected Hosts (137)	! Medium	Identification	unassigned	▼

# Notable Events Architecture Diagram



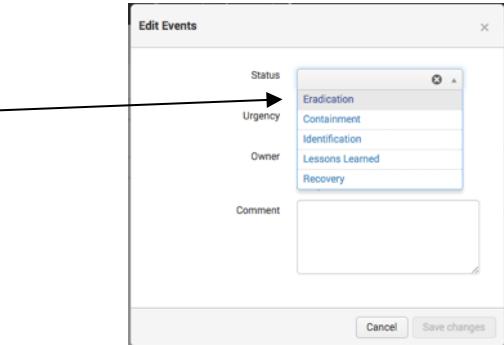
# Notable Events Architecture Diagram



# Notable Event Entry Points

- Populated By Correlation Searches
- Notable (summary) Index
  - Uses a custom alert action to populate
  - Augmented w/KVStore (owner, status, etc.)
  - **`notable` | search NOT `suppression` is your friend**
- **log\_review.conf**
  - Lets you change what's displayed in Incident Review
- **reviewstatuses.conf**
  - Lets you create custom statuses
- There is a REST API
  - [Blog Post by Luke Murphey](#)

i	Time	Security Domain	Title
8/19/16 10:10:30.000 AM		Threat	Threat Act
<b>Description:</b> Threat activity (05cc052686fbdf25fb610c1fe120195f) was discovered in the "file_hash" field based on file_intel collection			
<b>Additional Fields</b>			
Destination	127.0.0.1	Value	
Destination Expected	false	Value	
Destination PCI Domain	untrust	Value	
Destination Requires Antivirus	false	Value	
Destination Should Time Synchronize	false	Value	
Destination Should Update	false	Value	
PC Load Letter	What The Splunk Does That Mean	Value	560
Source	unknown	Value	
Source Expected	false	Value	
Source PCI Domain	untrust	Value	
Source Requires Antivirus	false	Value	



# Notable Events Example + Demo

- Lots of good stuff lives in SA-ThreatIntelligence
  - Did I mention macros?
    - Affords a good amount of abstraction
    - Do you want this? 
    - Or This?
      - ▶ `curl -k -u 'demoadmin:changeme' https://localhost:8089/services/search/jobs/export?output_mode=json -d search="search \`notable\` | search NOT \`suppression\`" -d earliest_time=-1h`
  - Demo:
    - Send A Notable To Slack
    - Update A Notable Status From Slack



# Threat Intelligence

Enterprise Security

Threat Activity

Threat Group Threat Category Search Threat Match Value Last 24 hours Submit Advanced Filter...

**THREAT MATCHES** Unique Count **5** **+1**

**THREAT COLLECTIONS** Unique Count **4** **+1**

**THREAT CATEGORIES** Unique Count **2** **+1**

**THREAT SOURCES** Unique Count **2** **+1**

**THREAT ACTIVITY** Total Count **7** **+1**

Threat Activity Over Time

time

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
file_intel	File Hash Matches File Name Matches		4	4
ip_intel	Source And Destination Matches		1	1
process_intel	Process Matches		1	1
service_intel	Service Matches		1	1

Most Active Threat Sources

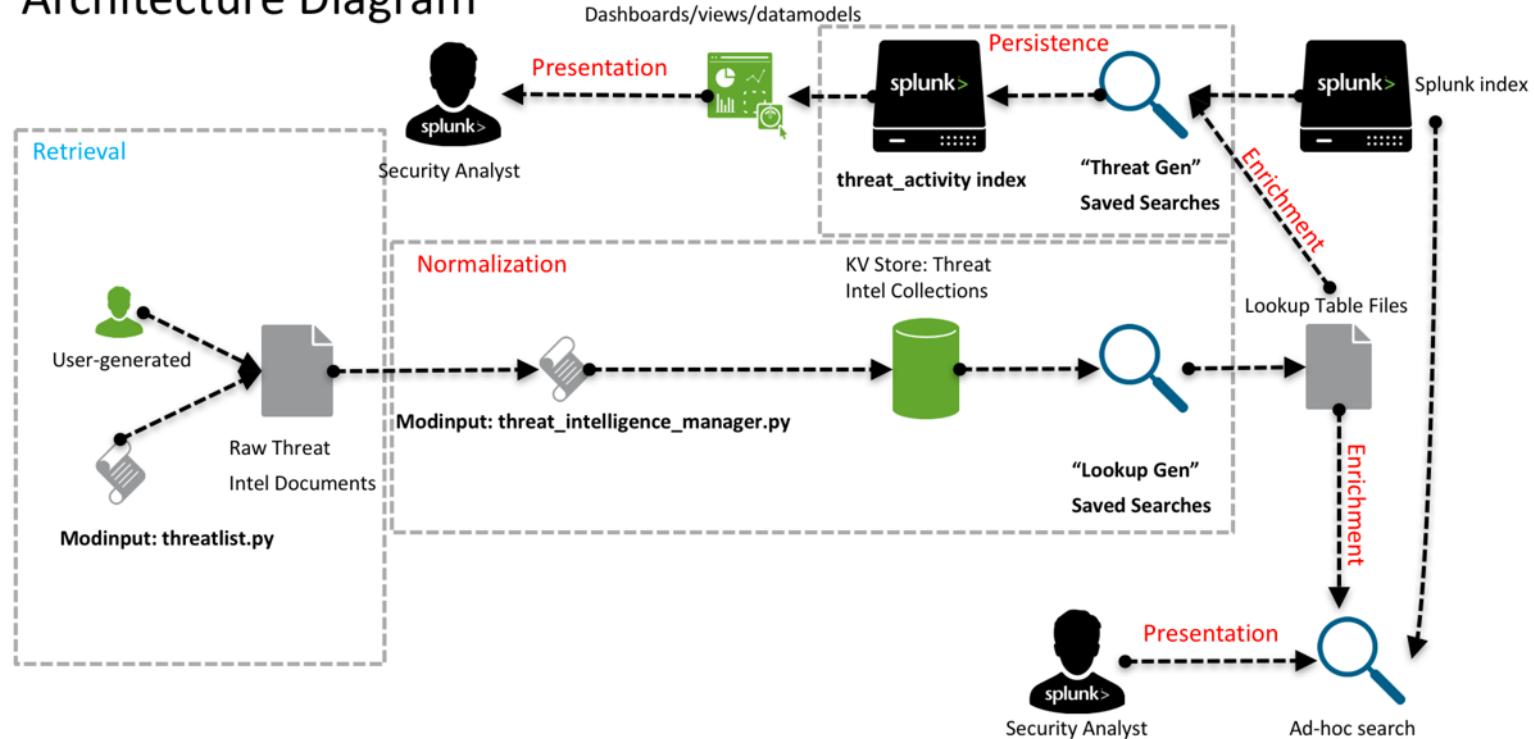
source_id	source_path	source_type	count
mandiant-package-100583d6-1861-4cfe-b212-c016fce1e240	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_JOCs_No_OpenIOC.xml	stix	6
iblocklist_logmein	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blocklist_logmein.csv	csv	1

Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourceType	src	dest	threat_collection	threat_group	threat_category
2016-08-19 10:20:00	process	updatasched.exe		WMI:LocalProcesses	unknown	127.0.0.1	process_intel	undefined	undefined
2016-08-19 10:10:00	service	OSEASV		WMI:Service	unknown	127.0.0.1	service_intel	undefined	undefined

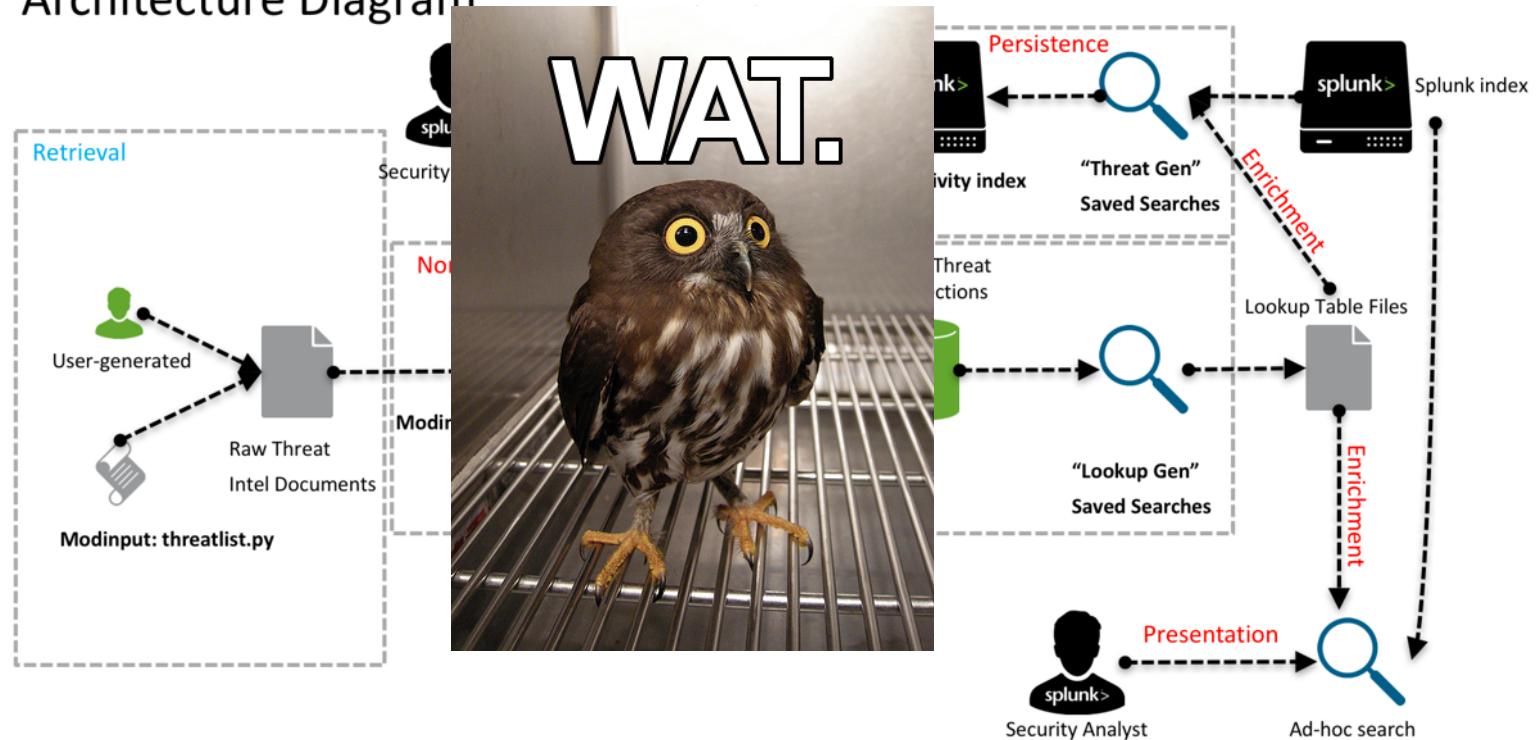
# Threat Intelligence Architecture

## Architecture Diagram



# Threat Intelligence Architecture

Architecture Diagram



# Threat Intelligence Framework

- Composed of: mod-input, scheduled searches, indexes, and lookups.
- You get:
  - flexible input processing (mod-input)
  - deduplication
  - datamodels
  - lookup creation/management
  - high-volume/high-speed matching for free (correlation searches)
- Handy One Liners:
  - What fields are supported for each collection type? | **rest /services/data/transforms/lookups | table title fields\_array | search title=local\*intel**
  - What indicators are in collection “X” (where x = ip\_intel)? | **inputlookup ip\_intel | eval key=\_key**
  - What are all my lookup table files? | **rest /services/data/transforms/lookups | search title="threatintel\_by\*" | table**

# Threat Intelligence Framework Demo



Threat Artifacts																																																																							
Threat Artifact	Threat Category	Threat Group	Malware Alias																																																																				
Threat ID	All	All																																																																					
<hr/>																																																																							
Threat Overview	Network	Endpoint	Certificate	Email																																																																			
<h4>Threat Overview</h4> <table border="1"><thead><tr><th>source_id</th><th>source_path</th></tr></thead><tbody><tr><td>fireeye.stix-b7b16e67-4292-46a3-ba64-60c1a491723d</td><td>/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-res</td></tr><tr><td>iblocklist_logmein</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv</td></tr><tr><td>iblocklist_piratebay</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.cs</td></tr><tr><td>iblocklist_proxy</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.cs</td></tr><tr><td>iblocklist_rapidshare</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.cs</td></tr><tr><td>iblocklist_spyware</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.cs</td></tr><tr><td>iblocklist_tor</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.cs</td></tr><tr><td>iblocklist_web_attacker</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attack</td></tr><tr><td>malware_domains</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.cs</td></tr><tr><td>sans</td><td>/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv</td></tr></tbody></table>					source_id	source_path	fireeye.stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-res	iblocklist_logmein	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	iblocklist_piratebay	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.cs	iblocklist_proxy	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.cs	iblocklist_rapidshare	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.cs	iblocklist_spyware	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.cs	iblocklist_tor	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.cs	iblocklist_web_attacker	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attack	malware_domains	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.cs	sans	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv																																													
source_id	source_path																																																																						
fireeye.stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-res																																																																						
iblocklist_logmein	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv																																																																						
iblocklist_piratebay	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.cs																																																																						
iblocklist_proxy	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.cs																																																																						
iblocklist_rapidshare	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.cs																																																																						
iblocklist_spyware	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.cs																																																																						
iblocklist_tor	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_tor.cs																																																																						
iblocklist_web_attacker	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attack																																																																						
malware_domains	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.cs																																																																						
sans	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv																																																																						
<hr/>																																																																							
<h4>Endpoint Artifacts</h4> <table border="1"><thead><tr><th>threat_collection</th><th>source_type</th><th>threat_group</th><th>threat_category</th><th>malware_alias</th><th>count</th></tr></thead><tbody><tr><td>file_intel</td><td>stix</td><td>undefined</td><td>undefined</td><td></td><td>1356</td></tr><tr><td>file_intel</td><td>stix</td><td>F</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>admin338</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>japanorus</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>menupass</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>nitro</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>th3bug</td><td>APT</td><td></td><td>194</td></tr><tr><td>file_intel</td><td>stix</td><td>wl</td><td>APT</td><td></td><td>194</td></tr><tr><td>process_intel</td><td>stix</td><td>undefined</td><td>undefined</td><td></td><td>15</td></tr><tr><td>registry_intel</td><td>stix</td><td>undefined</td><td>undefined</td><td></td><td>9</td></tr></tbody></table> <td data-kind="ghost"></td> <td data-kind="ghost"></td> <td data-kind="ghost"></td> <td data-kind="ghost"></td> <td data-kind="ghost"></td>	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	file_intel	stix	menupass	APT		194	file_intel	stix	nitro	APT		194	file_intel	stix	th3bug	APT		194	file_intel	stix	wl	APT		194	process_intel	stix	undefined	undefined		15	registry_intel	stix	undefined	undefined		9					
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																																																																		
file_intel	stix	menupass	APT		194																																																																		
file_intel	stix	nitro	APT		194																																																																		
file_intel	stix	th3bug	APT		194																																																																		
file_intel	stix	wl	APT		194																																																																		
process_intel	stix	undefined	undefined		15																																																																		
registry_intel	stix	undefined	undefined		9																																																																		
<hr/>																																																																							
<p style="text-align: right;">« prev 1 2 next »</p>																																																																							

# Risk Analysis Adds context...

Edit Selected | Edit All 8 Matching Events | Add Selected to investigation

	Time	Security Domain	Title	Urgency	Status	Count																														
<input type="checkbox"/>	8/19/16 9:55:24.000 AM	Endpoint	Host Sending Excessive Email (10.11.36.20)	<span style="color: red;">⚠ Critical</span>	New	un																														
<p>Description: The device 10.11.36.20 was detected making 24 SMTP connections to 24 destinations.</p> <p>Additional Fields</p> <table><thead><tr><th>Value</th><th>Action</th></tr></thead><tbody><tr><td>Source</td><td>▼</td></tr><tr><td>Source Business Unit</td><td>▼</td></tr><tr><td>Source Category</td><td>▼</td></tr><tr><td>Source City</td><td>▼</td></tr><tr><td>Source Country</td><td>▼</td></tr><tr><td>Source IP Address</td><td>▼</td></tr><tr><td>Source Expected</td><td>▼</td></tr><tr><td>Source Latitude</td><td>▼</td></tr><tr><td>Source Longitude</td><td>▼</td></tr><tr><td>Source Owner</td><td>▼</td></tr><tr><td>Source PCI Domain</td><td>▼</td></tr><tr><td>Source Requires Antivirus</td><td>▼</td></tr><tr><td>Source Should Time Synchronize</td><td>▼</td></tr><tr><td>Source Should Update</td><td>▼</td></tr></tbody></table> <p>Correlation Search: Endpoint - Host Sending Excessive Email - Rule</p> <p>History: <a href="#">View all review activity for this Notable Event</a></p> <p>Contributing Events: <a href="#">View email-related traffic for source 10.11.36.20 for this event</a></p>							Value	Action	Source	▼	Source Business Unit	▼	Source Category	▼	Source City	▼	Source Country	▼	Source IP Address	▼	Source Expected	▼	Source Latitude	▼	Source Longitude	▼	Source Owner	▼	Source PCI Domain	▼	Source Requires Antivirus	▼	Source Should Time Synchronize	▼	Source Should Update	▼
Value	Action																																			
Source	▼																																			
Source Business Unit	▼																																			
Source Category	▼																																			
Source City	▼																																			
Source Country	▼																																			
Source IP Address	▼																																			
Source Expected	▼																																			
Source Latitude	▼																																			
Source Longitude	▼																																			
Source Owner	▼																																			
Source PCI Domain	▼																																			
Source Requires Antivirus	▼																																			
Source Should Time Synchronize	▼																																			
Source Should Update	▼																																			
<input type="checkbox"/>	8/19/16 8:05:44.000 AM	Network	High Volume of Traffic from 10.12.34.56 to 199.9.251.78	<span style="color: red;">⚠ Critical</span>	New	un																														
<p>Description: A large volume of traffic was observed from 10.12.34.56 to 199.9.251.78.</p> <p>Additional Fields</p> <table><thead><tr><th>Value</th><th>Action</th></tr></thead><tbody><tr><td>Bytes Out</td><td>▼</td></tr><tr><td>Destination</td><td>▼</td></tr><tr><td>Destination Expected</td><td>▼</td></tr><tr><td>Destination PCI Domain</td><td>▼</td></tr><tr><td>Destination Requires Antivirus</td><td>▼</td></tr><tr><td>Destination Should Time Synchronize</td><td>▼</td></tr><tr><td>Destination Should Update</td><td>▼</td></tr><tr><td>Source</td><td>▼</td></tr><tr><td>Source Business Unit</td><td>▼</td></tr></tbody></table> <p>Correlation Search: Network - High Volume of Traffic from High or Critical Host - Rule</p> <p>History: <a href="#">View all review activity for this Notable Event</a></p> <p>Contributing Events: <a href="#">View network communication involving 10.12.34.56 to 199.9.251.78</a></p>							Value	Action	Bytes Out	▼	Destination	▼	Destination Expected	▼	Destination PCI Domain	▼	Destination Requires Antivirus	▼	Destination Should Time Synchronize	▼	Destination Should Update	▼	Source	▼	Source Business Unit	▼										
Value	Action																																			
Bytes Out	▼																																			
Destination	▼																																			
Destination Expected	▼																																			
Destination PCI Domain	▼																																			
Destination Requires Antivirus	▼																																			
Destination Should Time Synchronize	▼																																			
Destination Should Update	▼																																			
Source	▼																																			
Source Business Unit	▼																																			

# Risk Analysis Adds context...

Edit Selected | Edit All 8 Matching Events | Add Selected to investigation

Time	Security Domain	Title	Urgency	Status															
8/19/16 9:55:24.000 AM	Endpoint	Host Sending Excessive Email (10.11.36.20)	Critical	New															
<p>Description: The device 10.11.36.20 was detected making 24 SMTP connections to 24 destinations.</p> <p>Additional Fields</p> <table border="1"><thead><tr><th>Value</th></tr></thead><tbody><tr><td>Source</td></tr><tr><td>Source Business Unit</td></tr><tr><td>Source Category</td></tr><tr><td>Source City</td></tr><tr><td>Source Country</td></tr><tr><td>Source IP Address</td></tr><tr><td>Source Expected</td></tr><tr><td>Source Latitude</td></tr><tr><td>Source Longitude</td></tr><tr><td>Source Owner</td></tr><tr><td>Source PCI Domain</td></tr><tr><td>Source Requires Antivirus</td></tr><tr><td>Source Should Time Synchronize</td></tr><tr><td>Source Should Update</td></tr></tbody></table> <p>Action</p> <p>Correlation Search: Endpoint - Host Sending Excessive Email - Rule</p> <p>History: <a href="#">View all review activity for this Notable Event</a></p> <p>Contributing Events: <a href="#">View email-related traffic for source 10.11.36.20 for this event</a></p>					Value	Source	Source Business Unit	Source Category	Source City	Source Country	Source IP Address	Source Expected	Source Latitude	Source Longitude	Source Owner	Source PCI Domain	Source Requires Antivirus	Source Should Time Synchronize	Source Should Update
Value																			
Source																			
Source Business Unit																			
Source Category																			
Source City																			
Source Country																			
Source IP Address																			
Source Expected																			
Source Latitude																			
Source Longitude																			
Source Owner																			
Source PCI Domain																			
Source Requires Antivirus																			
Source Should Time Synchronize																			
Source Should Update																			
8/19/16 8:05:44.000 AM	Network	High Volume of Traffic from 10.12.34.56 to 199.9.251.78	Critical	New															
<p>Description: A large volume of traffic was observed from 10.12.34.56 to 199.9.251.78.</p> <p>Additional Fields</p> <table border="1"><thead><tr><th>Value</th></tr></thead><tbody><tr><td>Bytes Out</td></tr><tr><td>Destination</td></tr><tr><td>Destination Expected</td></tr><tr><td>Destination PCI Domain</td></tr><tr><td>Destination Requires Antivirus</td></tr><tr><td>Destination Should Time Synchronize</td></tr><tr><td>Destination Should Update</td></tr><tr><td>Source</td></tr><tr><td>Source Business Unit</td></tr></tbody></table> <p>Action</p> <p>Correlation Search: Network - High Volume of Traffic from High or Critical Host - Rule</p> <p>History: <a href="#">View all review activity for this Notable Event</a></p> <p>Contributing Events: <a href="#">View network communication involving 10.12.34.56 to 199.9.251.78</a></p>					Value	Bytes Out	Destination	Destination Expected	Destination PCI Domain	Destination Requires Antivirus	Destination Should Time Synchronize	Destination Should Update	Source	Source Business Unit					
Value																			
Bytes Out																			
Destination																			
Destination Expected																			
Destination PCI Domain																			
Destination Requires Antivirus																			
Destination Should Time Synchronize																			
Destination Should Update																			
Source																			
Source Business Unit																			

Risk score displayed in Incident Review

# Risk Analysis

*...and threads to pull*



# Risk Analysis

## but not this kind of risk...



Credit @j4vv4d Host Unknown presents: I'm a C I Double S P

# Risk Analysis

## but not this kind of risk...



Credit @j4vv4d Host Unknown presents: I'm a C I Double S P

# Risk Analysis

## but not this kind of risk...



Credit @j4vv4d Host Unknown presents: I'm a C I Double S P

# Risk Analysis

Risk as an aggregation of suspicious events...



NaturalNews.com

# Risk Analysis

## View risk scores in ES

splunk > App: Enterprise Security

Administrator Messages Settings Activity Help Find

Enterprise Security

### Risk Analysis

Source: All Risk Object Type: All Risk Object: Last 24 hours Submit Edit More Info + Create Ad-Hoc Risk Entry

**DISTINCT MODIFIER SOURCES** Object Count: 29 +29

**DISTINCT RISK OBJECTS** Object Count: 879 +879

**MEDIAN RISK SCORE** Overall Median Risk: medium ↗ increasing extreme  
Currently is: 73k

**AGGREGATED SYSTEM RISK** Total System Risk: extreme ↗ increasing extreme  
Currently is: 73k

**AGGREGATED USER RISK** Total User Risk: high ↗ increasing extreme  
Currently is: 78k

**AGGREGATED OTHER RISK** Total Other Risk: minimal ↗ increasing extreme  
Currently is: 4k

#### Risk Modifiers Over Time

The chart displays two metrics over time: 'risk\_score' (blue line) and 'count' (orange line). Both metrics show significant spikes around 4:00 AM on Aug 19, with the count reaching approximately 400 and the score peaking at about 25,000.

time

risk\_score count

4:00 PM Thu Aug 18 2016

8:00 PM

12:00 AM Fri Aug 19

4:00 AM

8:00 AM

12:00 PM

#### Risk Score By Object

risk_object	risk_object_type	risk_score	source_count	count
127.0.1	system	2320	6	47
ACME-002	system	880	3	11
HOST-003	system	800	4	10
HOST-005	system	800	4	10
10.11.36.20	system	740	6	11
ACME-006	system	720	3	9
HOST-004	system	720	2	9
ACME-003	system	640	2	8
ACME-004	system	640	2	8
HOST-002	system	640	2	8

< prev 1 2 3 4 5 6 7 8 9 10 next >

#### Most Active Sources

source	risk_score	risk_objects	count
Web - Abnormally High Number of HTTP Method Events By Src - Rule	25560	321	426
Endpoint - Host With Multiple Infections - Rule	14800	185	185
Access - Concurrent App Accesses - Rule	2460	123	123
Access - Geographically Improbable Access Detected - Rule	9680	121	121
Access - Excessive Failed Logins - Rule	6720	60	112
Threat - Brute Force Access Behavior Detected - Rule	7440	93	93
Threat - Threat List Activity - Rule	87	87	87
Network - Unroutable Host Activity - Rule	6560	80	82
Endpoint - High Or Critical Priority Host With Malware - Rule	6320	14	79
Change - Abnormally High Number of Endpoint Changes By User - Rule	2080	50	52

< prev 1 2 3 next >

# Risk Analysis

## View risk scores in ES

The screenshot displays the Splunk Enterprise Security Risk Analysis interface. At the top, there are navigation links: Security Posture, Incident Review, My Investigations, Advanced Threat, Security Domains, Audit, Search, and Configure. On the right, there are links for Administrator, Messages, Settings, Activity, and Help.

The main area is titled "Risk Analysis". It features several sections:

- Distinct MODIFIER SOURCES:** Shows a count of 29 with a red "+29" badge.
- Distinct RISK OBJECTS:** Shows a count of 879 with a red "+879" badge.
- Risk Modifiers Over Time:** A line chart showing risk scores over time, with a specific point highlighted at 4:00 PM on Thursday, August 18, 2016.
- Risk Score By Object:** A table listing risk scores for various objects. The table includes columns for risk\_object, risk\_object\_type, risk\_score, source\_count, and count.

risk_object	risk_object_type	risk_score	source_count	count
127.0.0.1	system	2320	6	47
ACME-002	system	880	3	11
HOST-003	system	800	4	10
HOST-005	system	800	4	10
10.11.36.20	system	740	6	11
ACME-006	system	720	3	9
HOST-004	system	720	2	9
ACME-003	system	640	2	8
ACME-004	system	640	2	8
HOST-002	system	640	2	8

A green arrow points from the "Risk Score By Object" table towards the "Risk Score By Object" section in the bottom-left corner of the dashboard.

# Risk Analysis Or in core Splunk

The screenshot shows the Splunk interface for the Enterprise Security app. At the top, there's a navigation bar with links like Security Posture, Incident Review, My Investigations, Advanced Threat, Security Domains, Audit, Search, Configure, and Help. Below the navigation is a search bar with a placeholder "enter search here...". To the right of the search bar are filters for "All time" and a search icon. Underneath the search bar, there's a section titled "How to Search" with links to "Documentation" and "Tutorial". Another section titled "What to Search" displays statistics: 29,114,348 Events INDEXED, 3 years ago EARLIEST EVENT, and Now LATEST EVENT. There's also a "Data Summary" button. On the left, under "Search History", there's a link to "Expand your search history". At the bottom, there are links for "About", "Support", "File a Bug", "Documentation", and "Privacy Policy". The footer includes a copyright notice: "© 2005-2016 Splunk Inc. All rights reserved."

index=risk app=\* | timechart count by app

# Risk Analysis

## Set risk parameter statically or dynamically in CS

### Edit Correlation Search

[◀ Back to Content Management](#)

#### Correlation Search

Search Name \*

Activity from Expired User Identity



Application Context

SA-IdentityManagement



Description

Alerts when an event is discovered from a user ass

Describes what kind of issues this search is intended to detect

Search \*

```
| datamodel "Identity_Management" "Expired_Identity_Activity" search | stats max(_time) as "lastTime",latest(_raw) as "orig_raw",count by "Expired_Identity_Activity.expired_user" | rename "Expired_Identity_Activity.expired_user" as "user"  
| eval risk_score = calculated_field  
| eval risk_object = user
```

[Edit search in guided mode](#)

Time Range

# Risk Analysis

## Set risk parameter statically or dynamically in CS

### Edit Correlation Search

[Back to Content Management](#)

#### Correlation Search

Search Name \*

Activity from Expired User Identity



Application Context

SA-IdentityManagement



Description

Alerts when an event is discovered from a user ass

Describes what kind of issues this search is intended to detect

Search \*

```
| datamodel "Identity_Management" "Expired_Identity_Activity" search | stats max(_time) as "lastTime",latest(_raw) as "orig_raw",count by "Expired_Identity_Activity.expired_user" as "user" | eval risk_score = calculated_field | eval risk_object = user
```



[Edit search in guided mode](#)

Time Range

# Risk Analysis

## Set risk parameter statically or dynamically in CS

Edit Correlation Search

◀ Back

Create Correlation Search

**Risk Scoring**

Create risk modifier

Score \*  Indicates how much to adjust the score for the given risk object

Risk object field \*  Indicates what field in the results indicates the risk object (such as the system or the user) that the score applies to

Risk object type \*  Indicates the type of risk object this applies to (usually 'system' or 'user')

[Actions](#)

[Edit search in guided mode](#)

Time Range

The screenshot shows the 'Edit Correlation Search' interface in Splunk. A modal window titled 'Risk Scoring' is open. It contains three configuration fields: 'Create risk modifier' (checked), 'Score' (set to 80), and two dropdowns for 'Risk object field' and 'Risk object type', both set to 'user'. Below each field is a descriptive text label. At the bottom of the modal are 'Actions' and 'Edit search in guided mode' buttons. The background shows a partially visible search bar with 'Correlation Search' and a 'Time Range' section.

# Adaptive Response Framework

Modular Action Center

Action Mode Action Name Action Status User Search ID (sid) Edit More Info [Submit](#)

All All All All Last 24 hours

**Edit**

ACTION INVOCATIONS Count	ACTION NAMES Distinct Count	ACTION SEARCH NAMES Distinct Count	ACTION USERS Distinct Count	ACTION SEARCHES Distinct Count	ACTION DURATION Average (Ms)
<b>27k</b> -236	<b>5</b> 0	<b>12</b> -2	<b>3</b> 0	<b>674</b> -64	<b>530</b> -3.6

Action Invocations Over Time By Name

count

time

4:00 PM  
Thu Aug 18  
2016

8:00 PM

12:00 AM  
Fri Aug 19

4:00 AM

8:00 AM

12:00 PM

4:00 PM

Legend:

- acnapsnow\_incident
- checkphish
- eshook
- notable
- risk

Top Actions By Name

action_name	tag	action_mode	search_name	user	search_count	result_count	avg_duration (ms)
checkphish		adhoc (and 1 more)	CheckPhish02 (and 3 more)	admin (and 1 more)	431	16988	568
notable	passive	saved	Access - Account Deleted - Rule (and 7 more)	admin	78	243	272
risk	passive	saved	Access - Account Deleted - Rule (and 6 more)	admin	77	242	280
acnapsnow_incident				nobody	92	0	381
eshook				admin	53	0	125

# Adaptive Response Framework

- Components
  - You can use components for different parts of your search
- This way you can reuse components
- ES template (ES template is a search)
- Leveraging components



# Adaptive Response Framework

- Composed of: mod-alerts, python lib, datamodel, “CAM”, magic
  - You get:
    - ▶ Search and response “glue”,
    - ▶ First-class set of core hooks,
    - ▶ Nice abstraction for creating raw “events”
- This will live in Splunk\_SA\_CIM
  - ES tested, Core approved
- Leverages workflow actions (ad-hoc) and mod-alerts (linked to a search)

# Adaptive Response Framework Demo

```
def factorial(n):
    if n == 0:
        return 1
    else:
        print n
        return n * factorial(n - 1)

factorial(10)
~/SPLUNK_ENV/demo/splunk/etc/apps/TA-vt/default @ kchamplin-mbp15
(kchamplin) >>> python recursion
10
9
8
7
6
5
4
3
2
1
```

# THANK YOU

.conf2016

splunk®