Exploring The Frameworks Of Splunk Enterprise Security

Dave Herrald

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 the 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

ES — Security
ITSI — IT Svc Int
VM — VMware
EX — Exchange
PCI — PCI
UBA — 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

- ES — Security
- ITSI — IT Svc Int
- VM — VMware
- EX — Exchange
- PCI — PCI
- UBA — 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

What Is Enterprise Security?

A collection of Frameworks

What Is Enterprise Security?

A collection of Frameworks

What Is Enterprise Security?

A collection of Frameworks

What Is Enterprise Security?

A collection of Frameworks

What Is Enterprise Security?

A collection of Frameworks

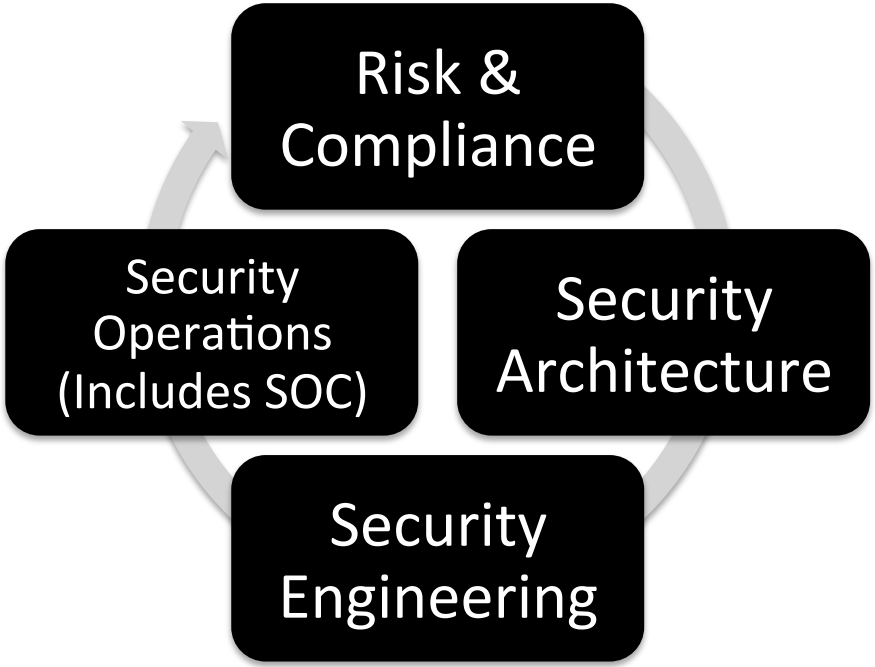
What Is Enterprise Security?

A collection of Frameworks

Security Operations

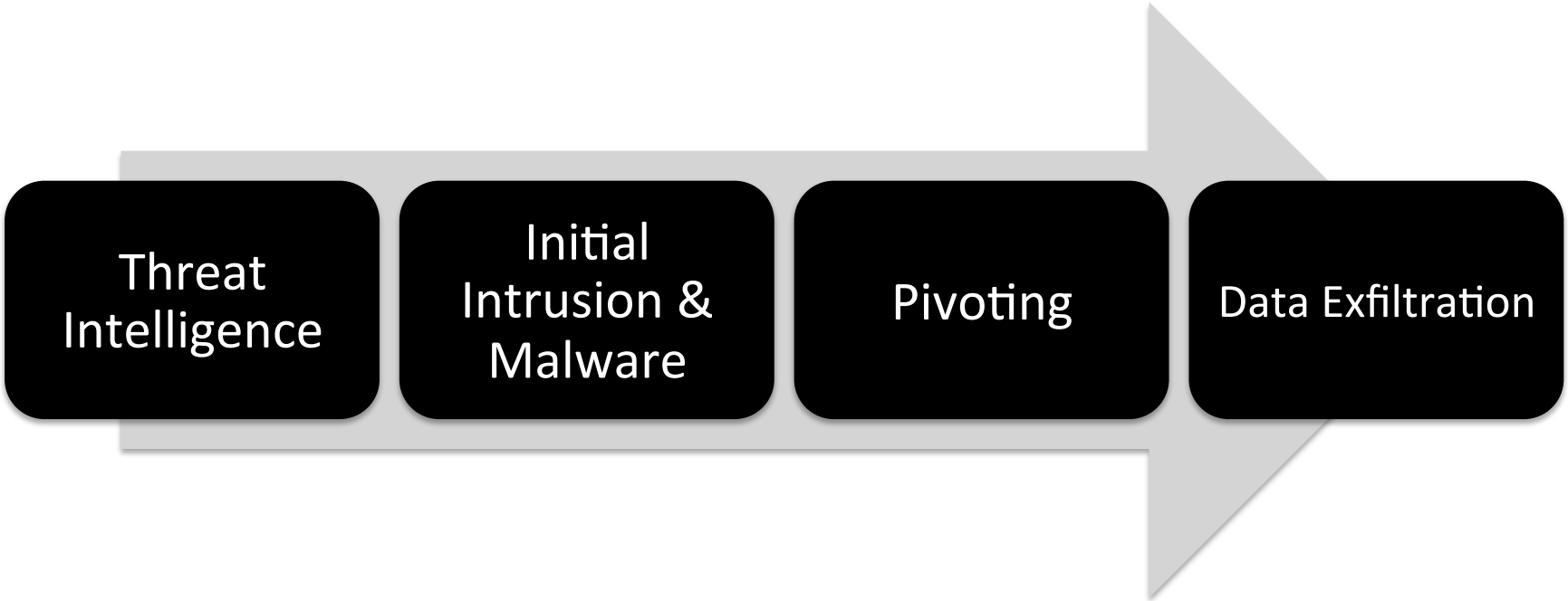
Traditional?

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

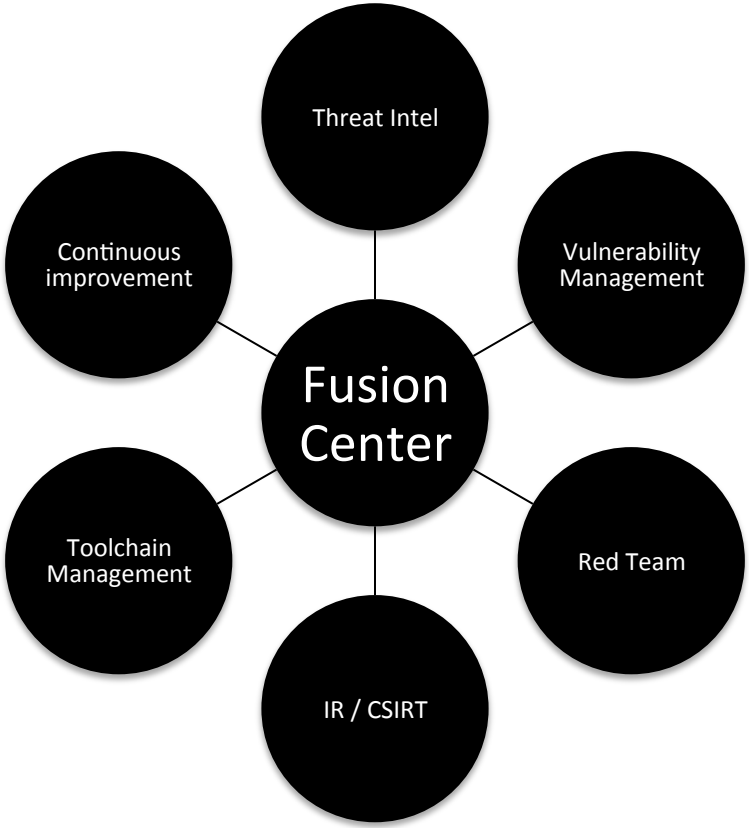


Kill Chain Based

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…

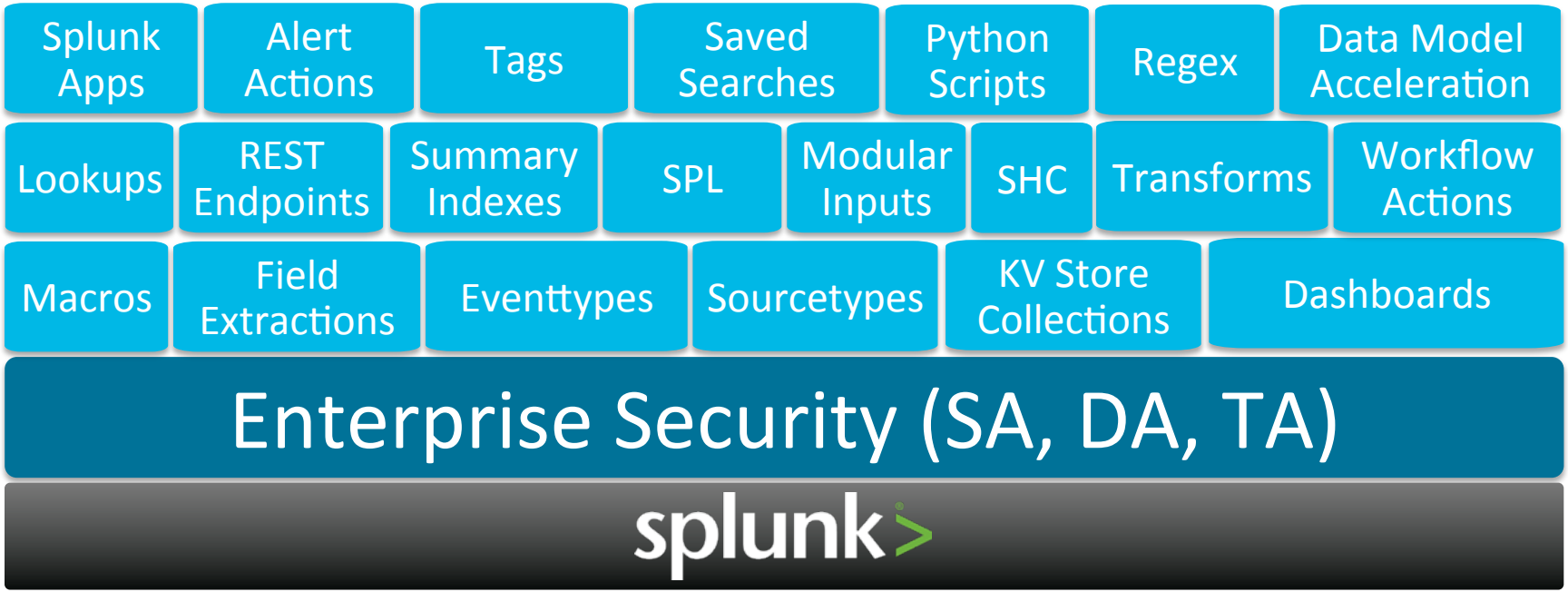
"I always choose a brain over a product."

"We want to build our own tooling on Splunk"

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

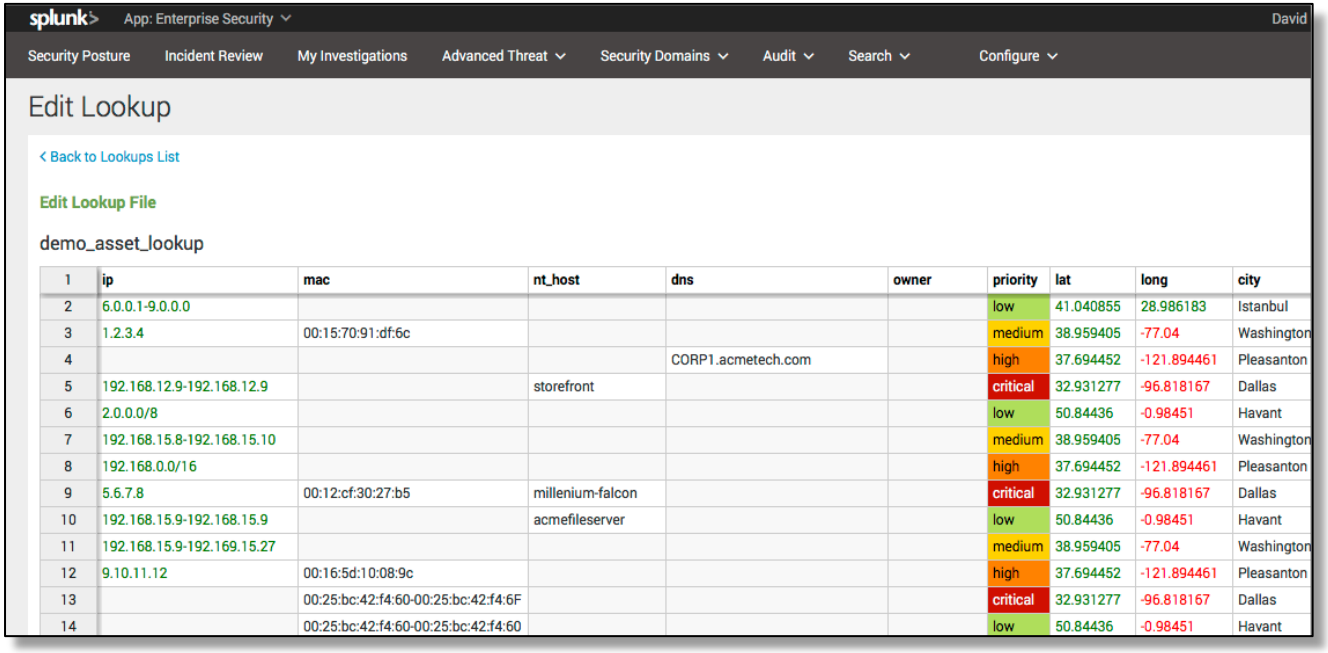
The Architecture Of ES

It's just Splunk!



Asset And Identity Correlation

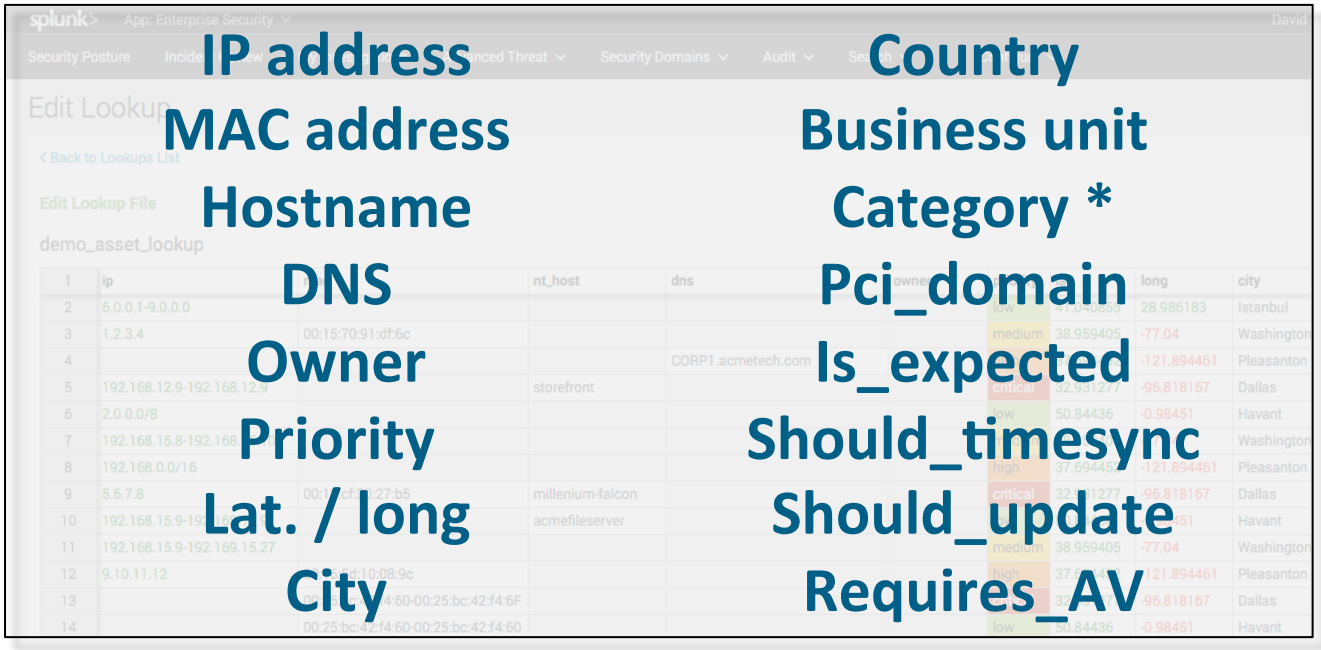
System Inventory in ES



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

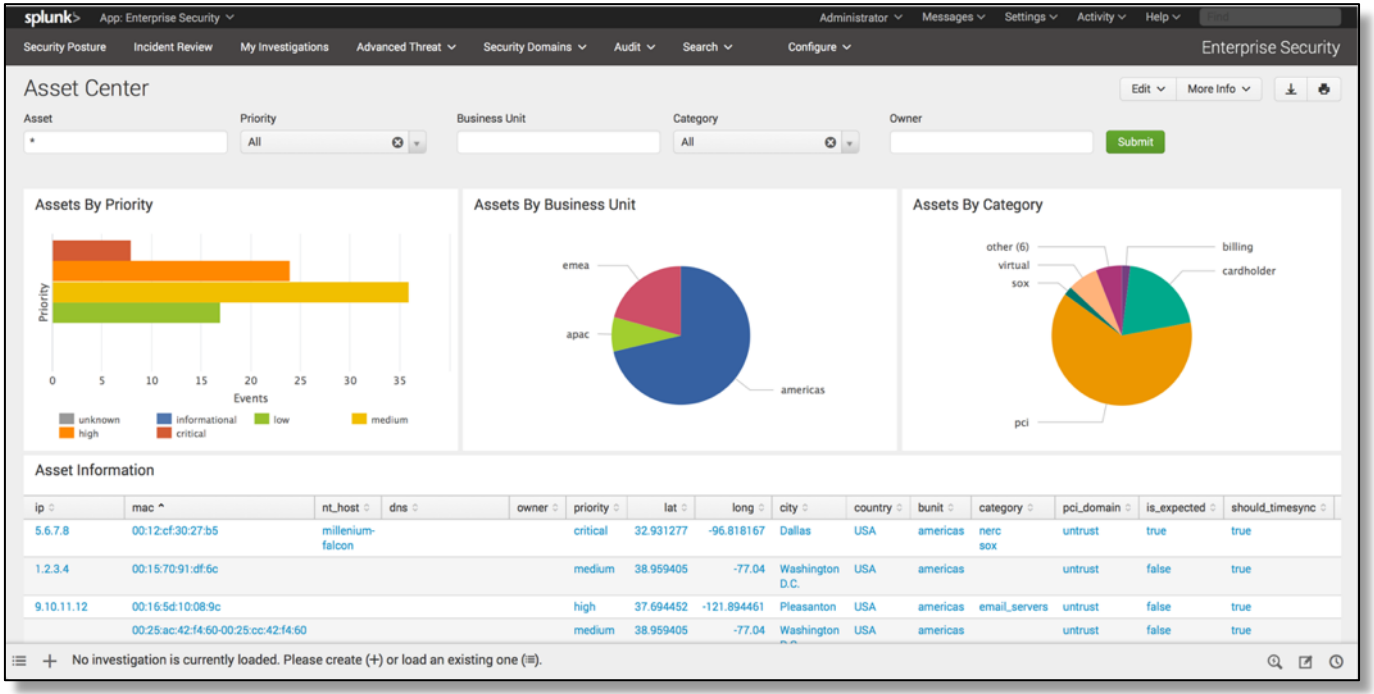
Asset And Identity Correlation

System Inventory in ES



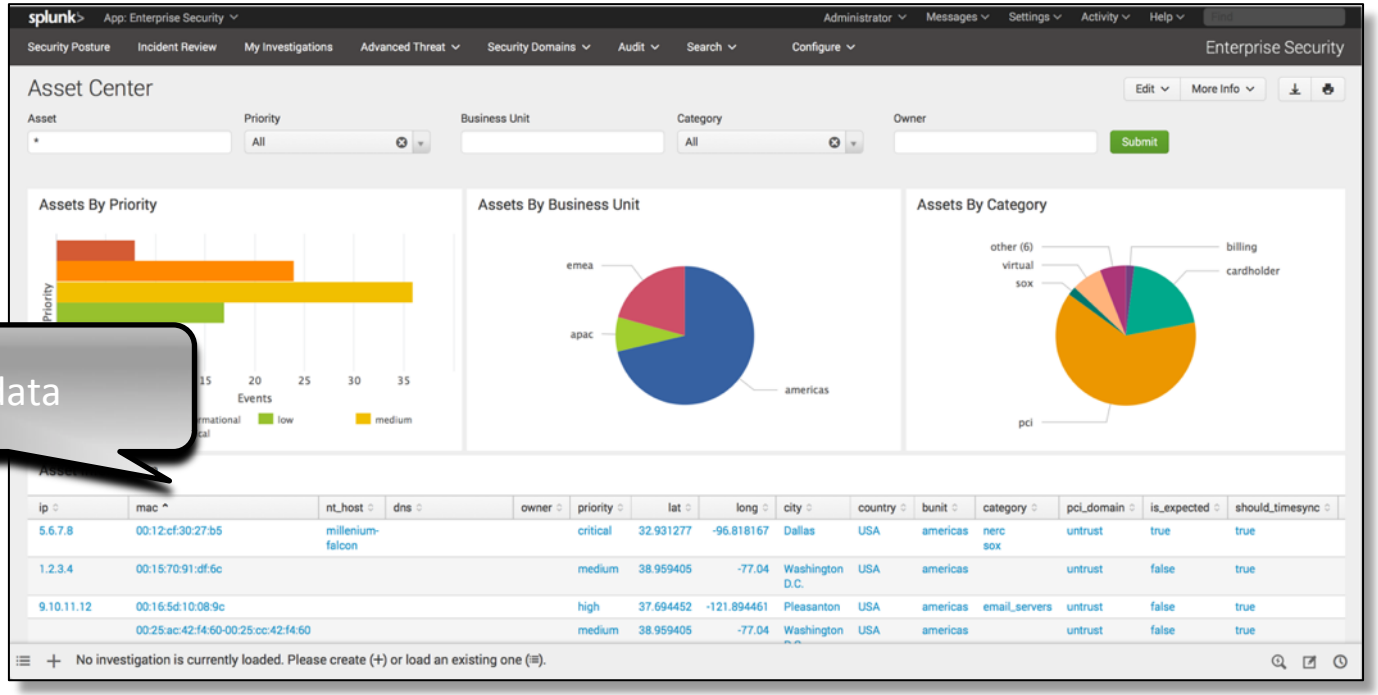
Asset And Identity Correlation

Available throughout ES



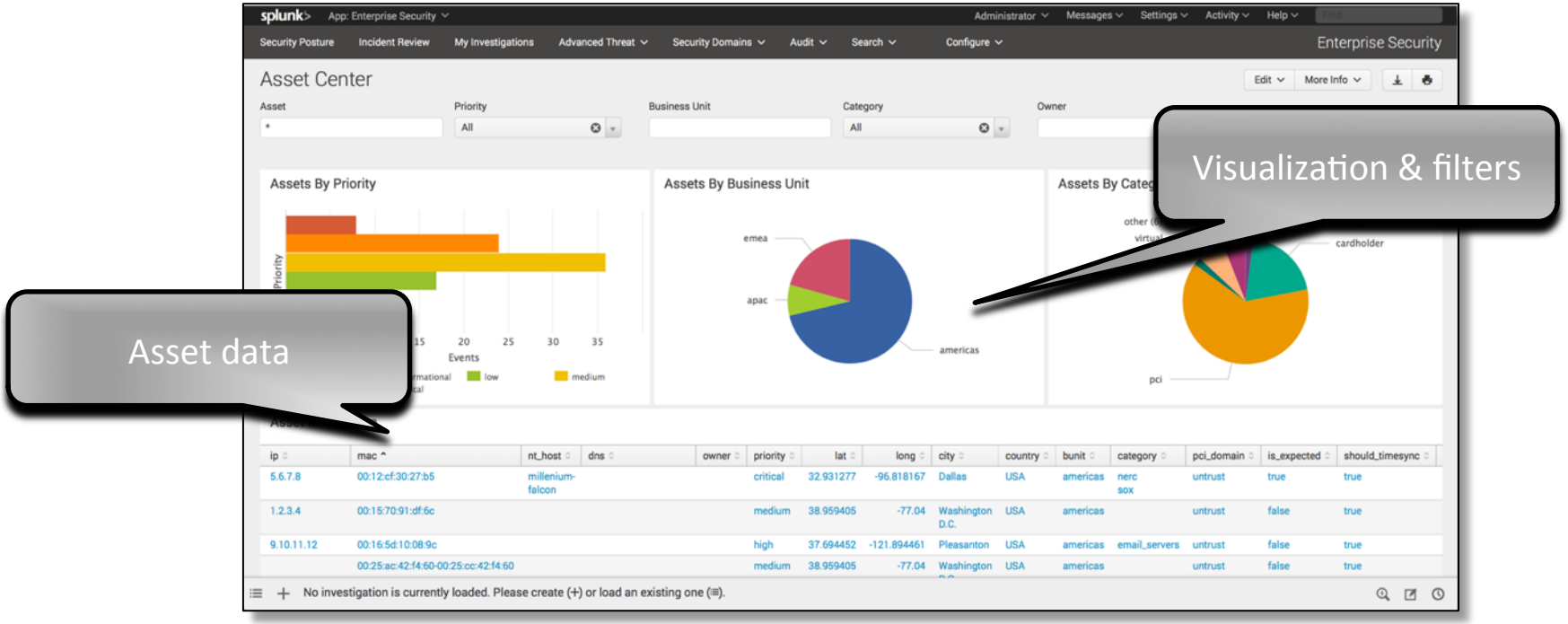
Asset And Identity Correlation

Available throughout ES



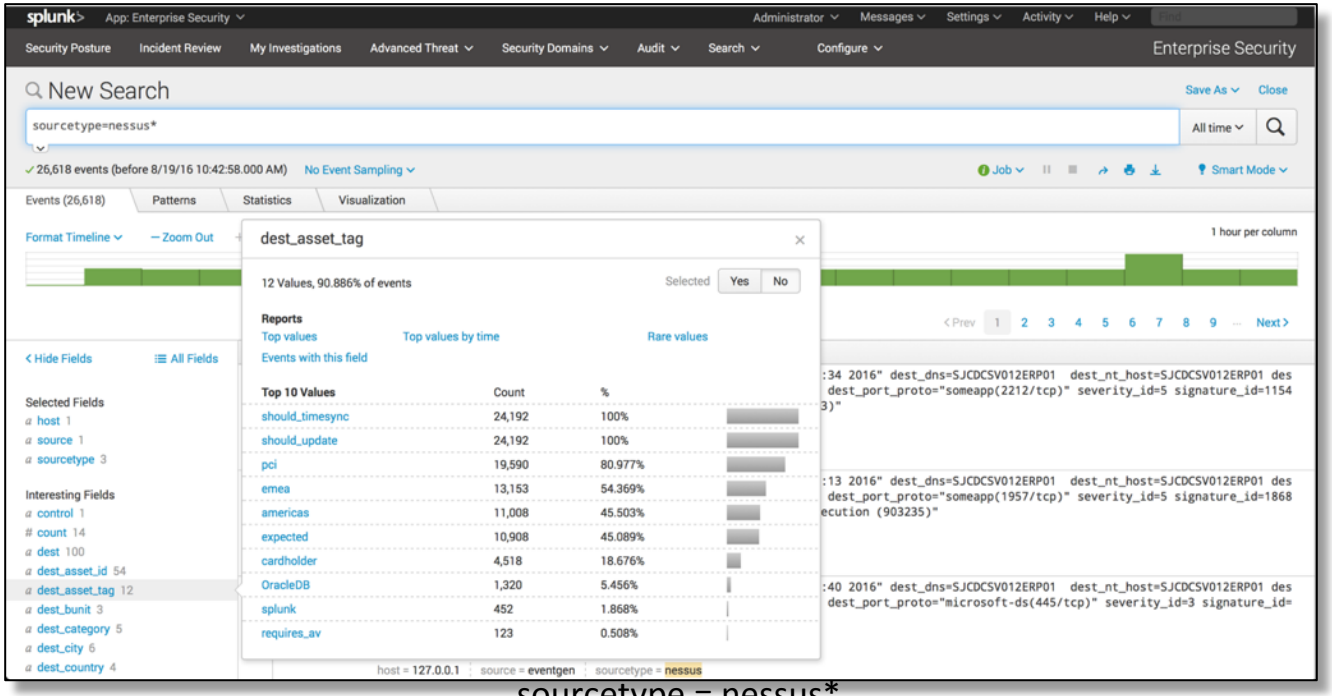
Asset And Identity Correlation

Available throughout ES



Asset And Identity Correlation

Available in core Splunk, too

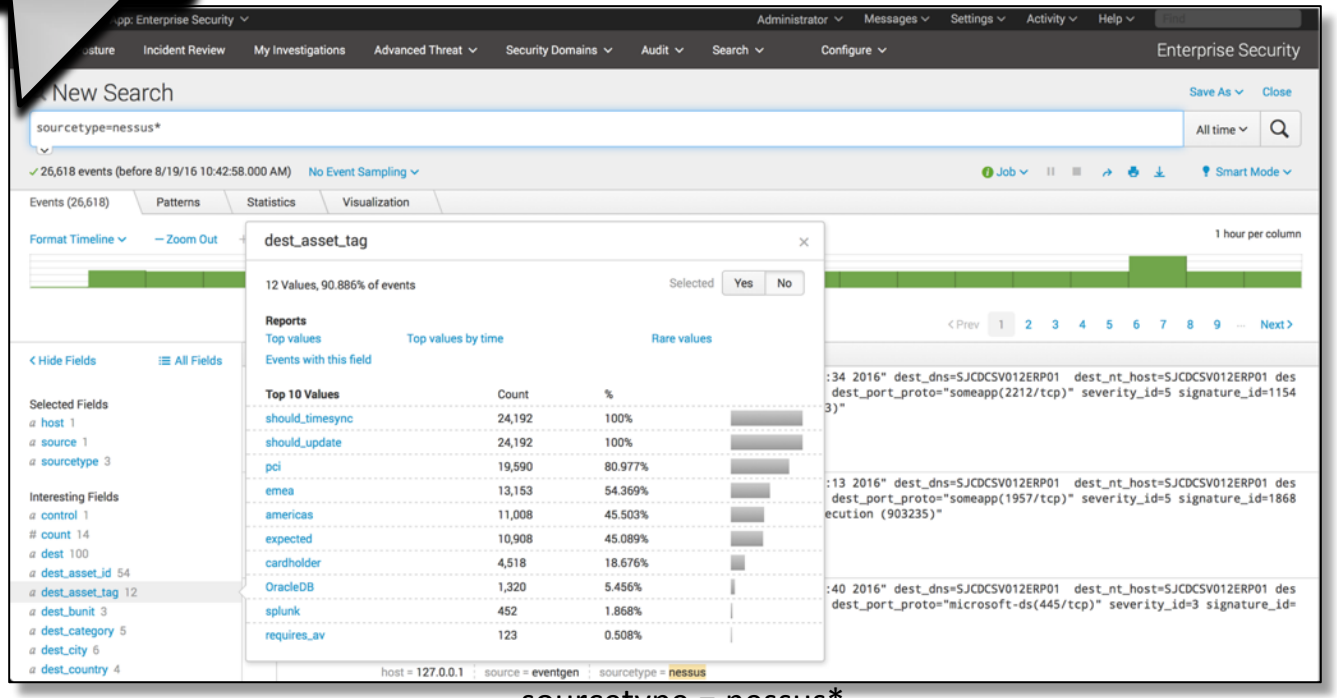


sourcetype = nessus*

Asset And Identity Correlation

Available in core Splunk, too

Nessus vulnerabilities

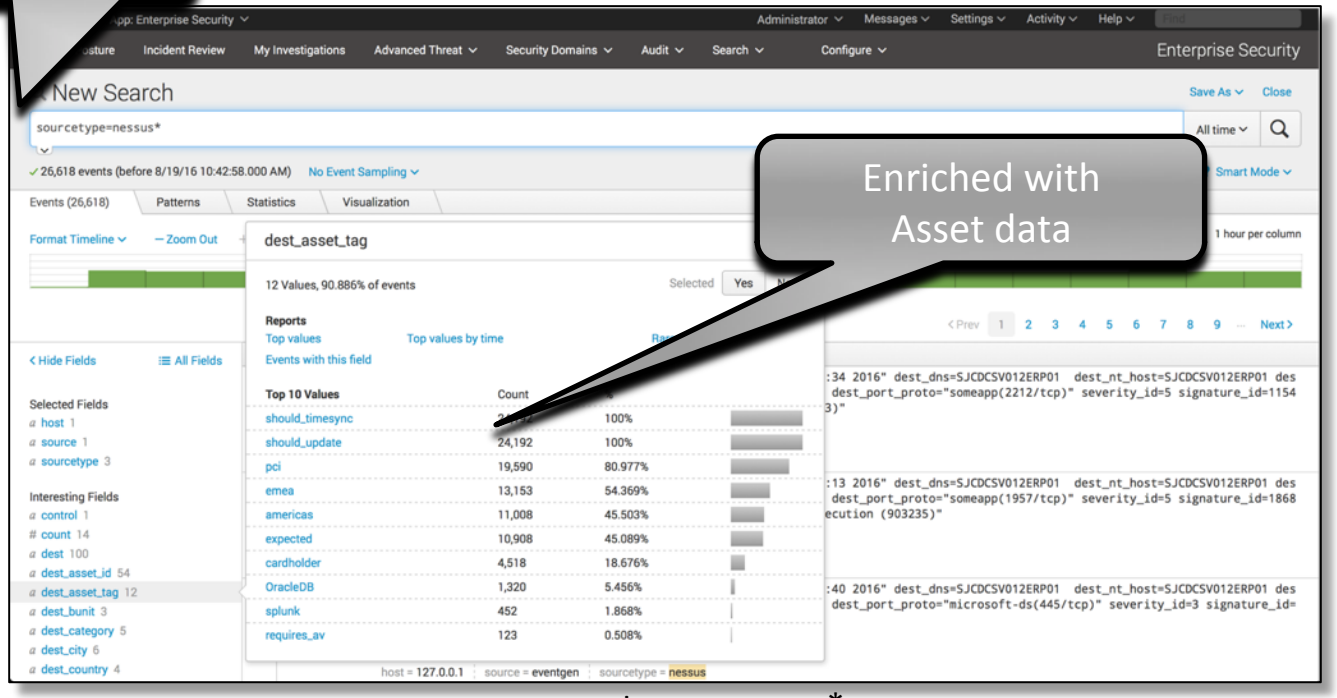


sourcetype = nessus*

Asset And Identity Correlation

Available in core Splunk, too

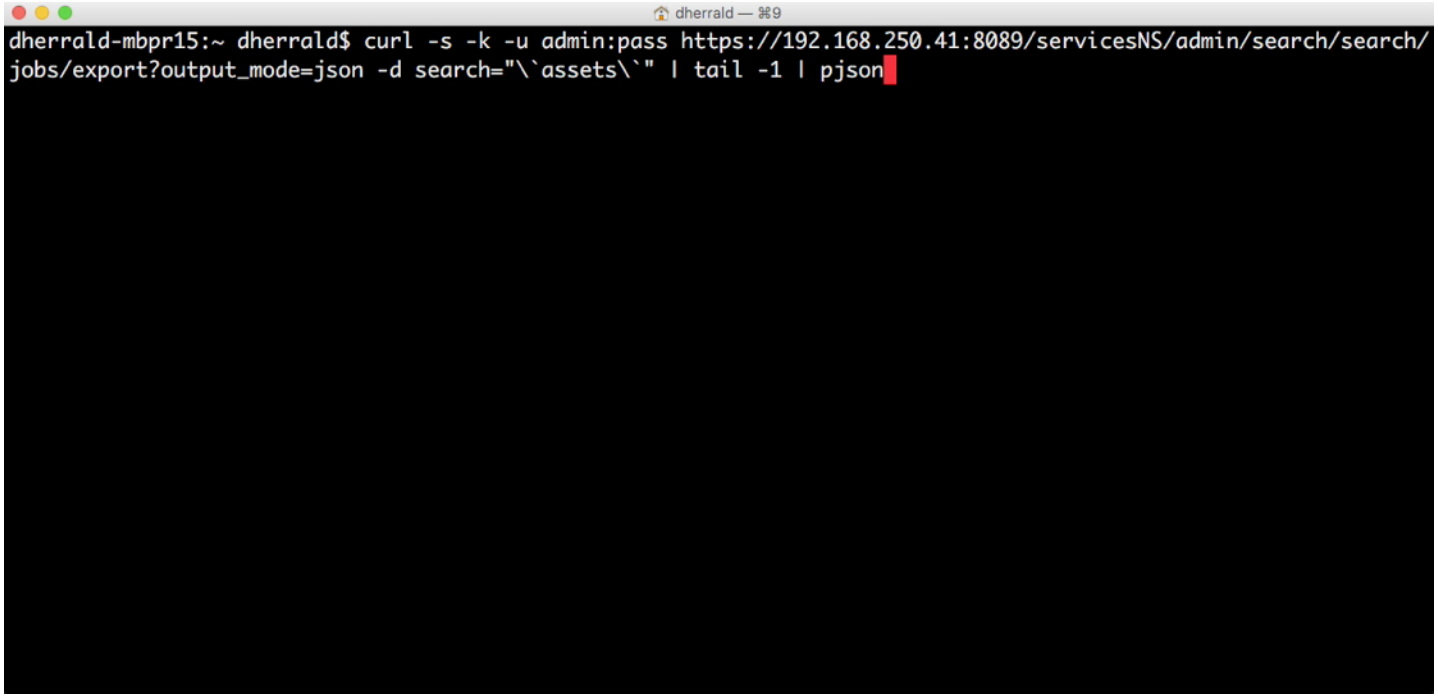
Nessus vulnerabilities



sourcetype = nessus*

Asset And Identity Correlation

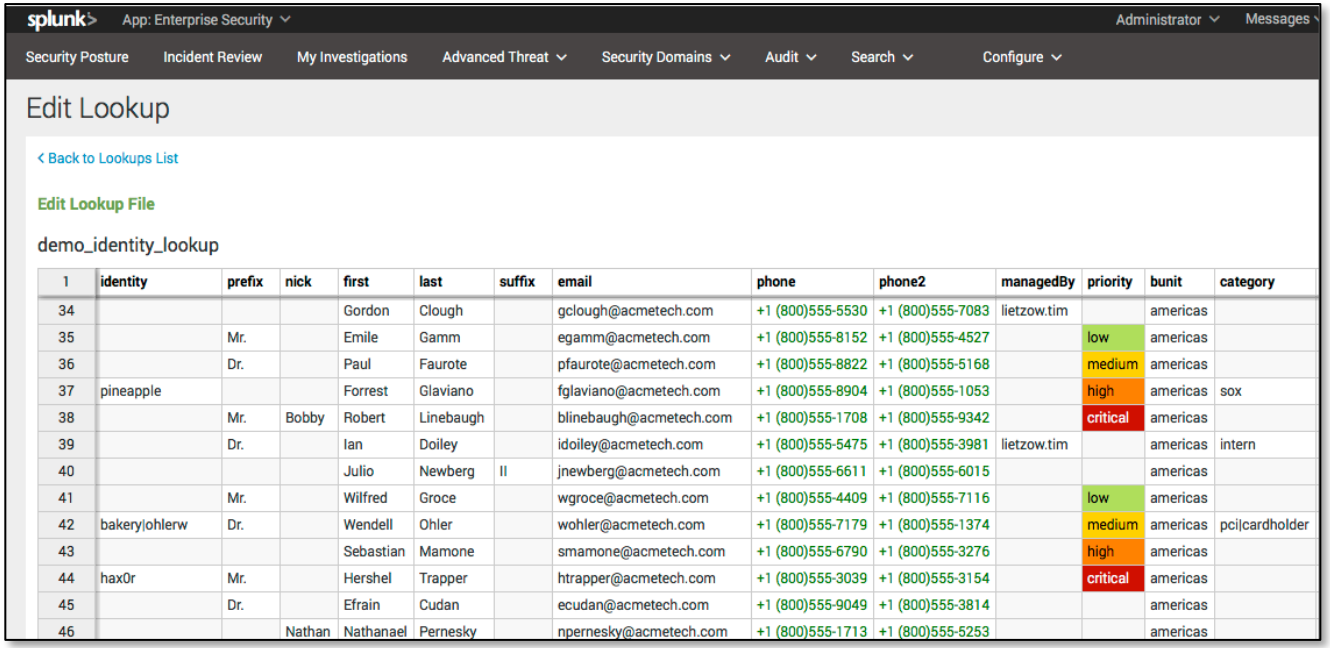
Available via API, too



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



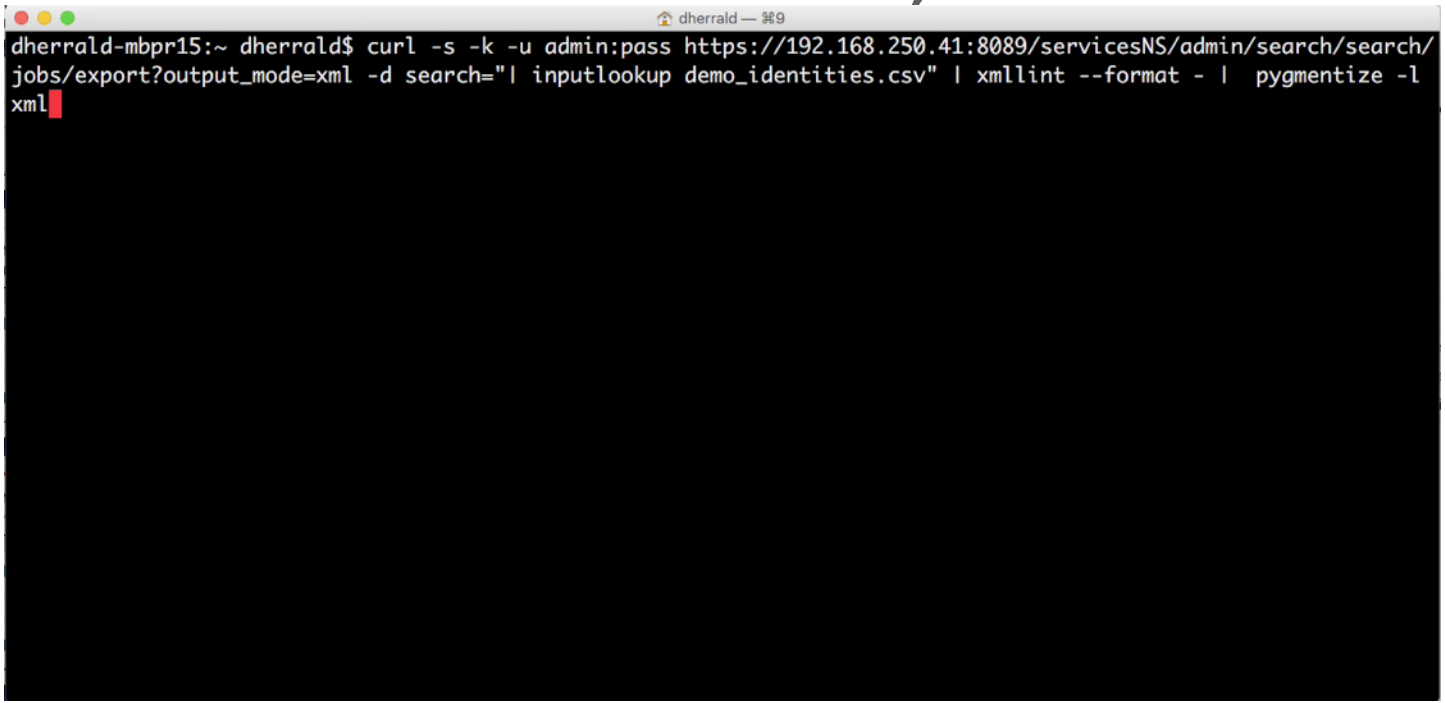
1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category
34				Gordon	Clough		gclough@acmetech.com	+1 (800)555-5530	+1 (800)555-7083	lietzow.tim		americas	
35		Mr.		Emile	Gamm		egamm@acmetech.com	+1 (800)555-8152	+1 (800)555-4527		low	americas	
36		Dr.		Paul	Faurote		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	bakery|ohlerw	Dr.		Wendell	Ohler		wohler@acmetech.com	+1 (800)555-7179	+1 (800)555-1374		medium	americas	pci|cardholder
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

Asset And Identity Correlation

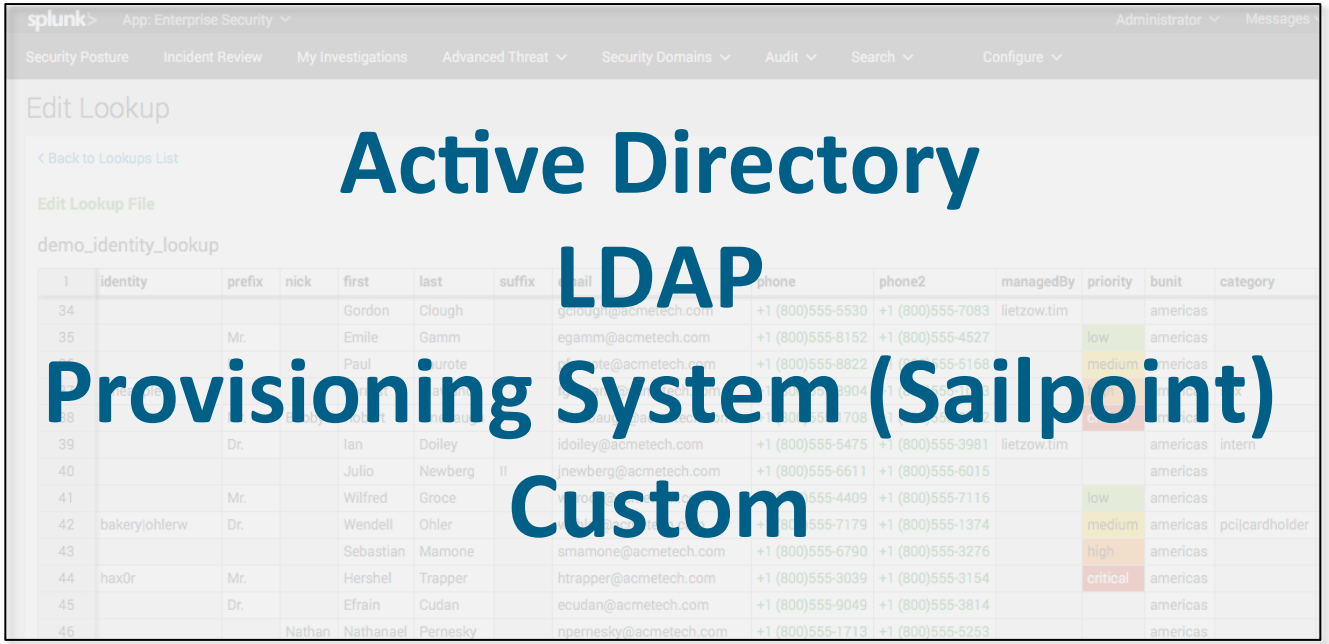
Available via API, too



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"

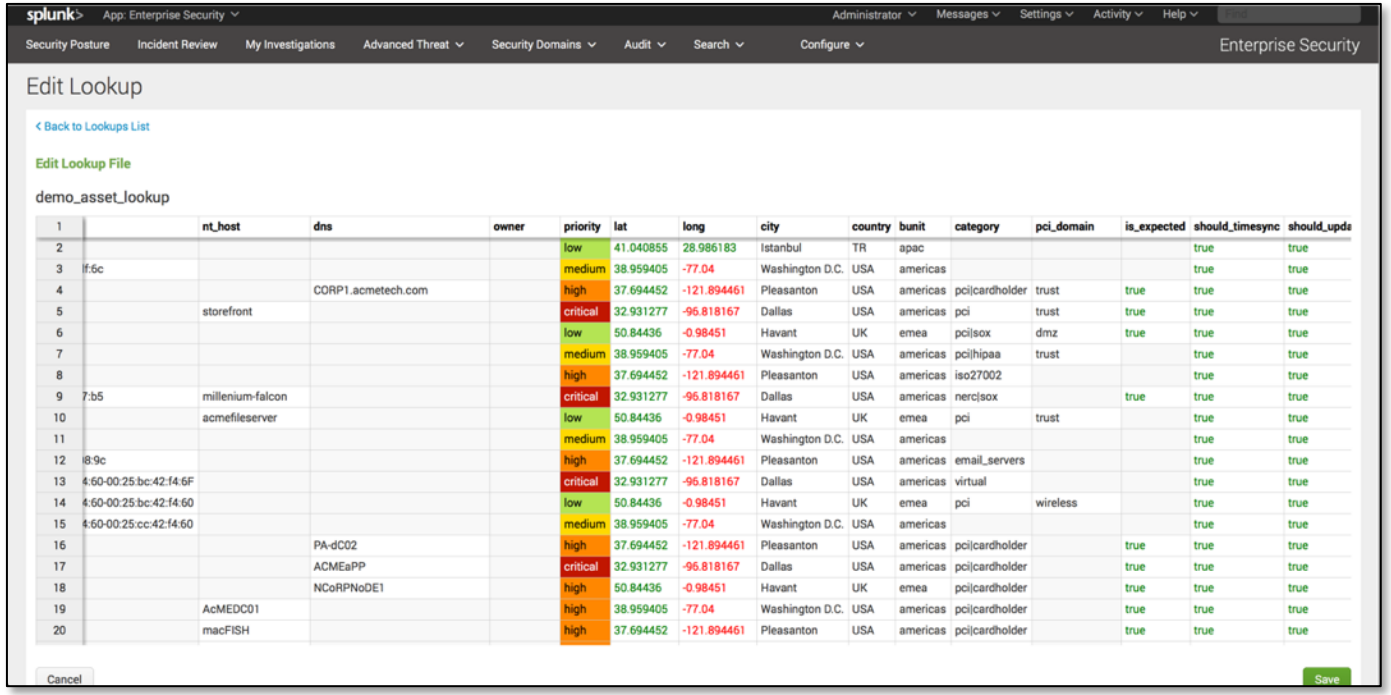
Asset And Identity Correlation

Handle multiple systems of record easily



Asset And Identity Correlation

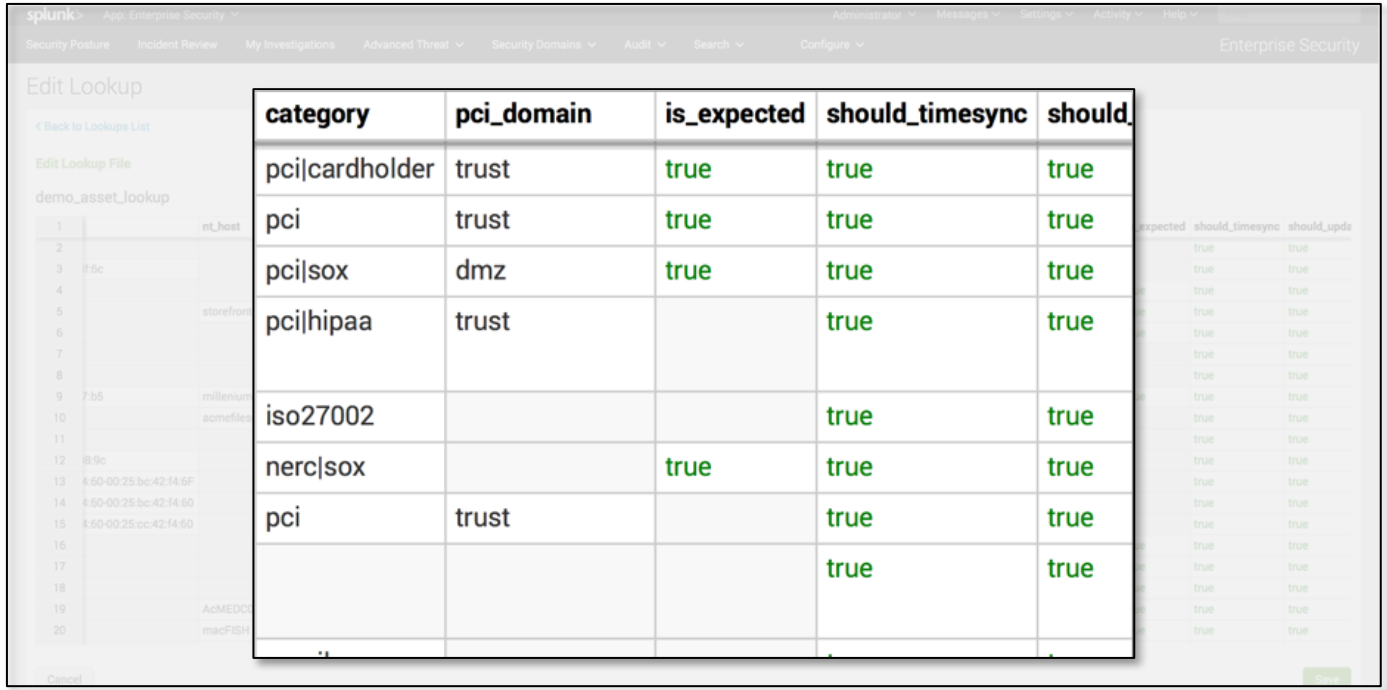
Category field is multi-valued



		nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_upda
2					low	41.040855	28.986183	Istanbul	TR	apac				true	true
3	lf:6c				medium	38.959405	-77.04	Washington D.C.	USA	americas				true	true
4			CORP1.acmetech.com		high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder	trust	true	true	true
5		storefront			critical	32.931277	-96.818167	Dallas	USA	americas	pci	trust	true	true	true
6					low	50.84436	-0.98451	Havant	UK	emea	pci|sox	dmz	true	true	true
7					medium	38.959405	-77.04	Washington D.C.	USA	americas	pci|hipaa	trust		true	true
8					high	37.694452	-121.894461	Pleasanton	USA	americas	iso27002			true	true
9	7:b5	millenium-falcon			critical	32.931277	-96.818167	Dallas	USA	americas	nerc|sox		true	true	true
10		acmefileserver			low	50.84436	-0.98451	Havant	UK	emea	pci	trust		true	true
11					medium	38.959405	-77.04	Washington D.C.	USA	americas				true	true
12	i8:9c				high	37.694452	-121.894461	Pleasanton	USA	americas	email_servers			true	true
13	4:60-00:25:bc:42:f4:6F				critical	32.931277	-96.818167	Dallas	USA	americas	virtual			true	true
14	4:60-00:25:bc:42:f4:60				low	50.84436	-0.98451	Havant	UK	emea	pci	wireless		true	true
15	4:60-00:25:cc:42:f4:60				medium	38.959405	-77.04	Washington D.C.	USA	americas				true	true
16			PA-dC02		high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder		true	true	true
17			ACMEaPP		critical	32.931277	-96.818167	Dallas	USA	americas	pci|cardholder		true	true	true
18			NCoRPNoDE1		high	50.84436	-0.98451	Havant	UK	emea	pci|cardholder		true	true	true
19		AcMEDC01			high	38.959405	-77.04	Washington D.C.	USA	americas	pci|cardholder		true	true	true
20		macFISH			high	37.694452	-121.894461	Pleasanton	USA	americas	pci|cardholder		true	true	true

Asset And Identity Correlation

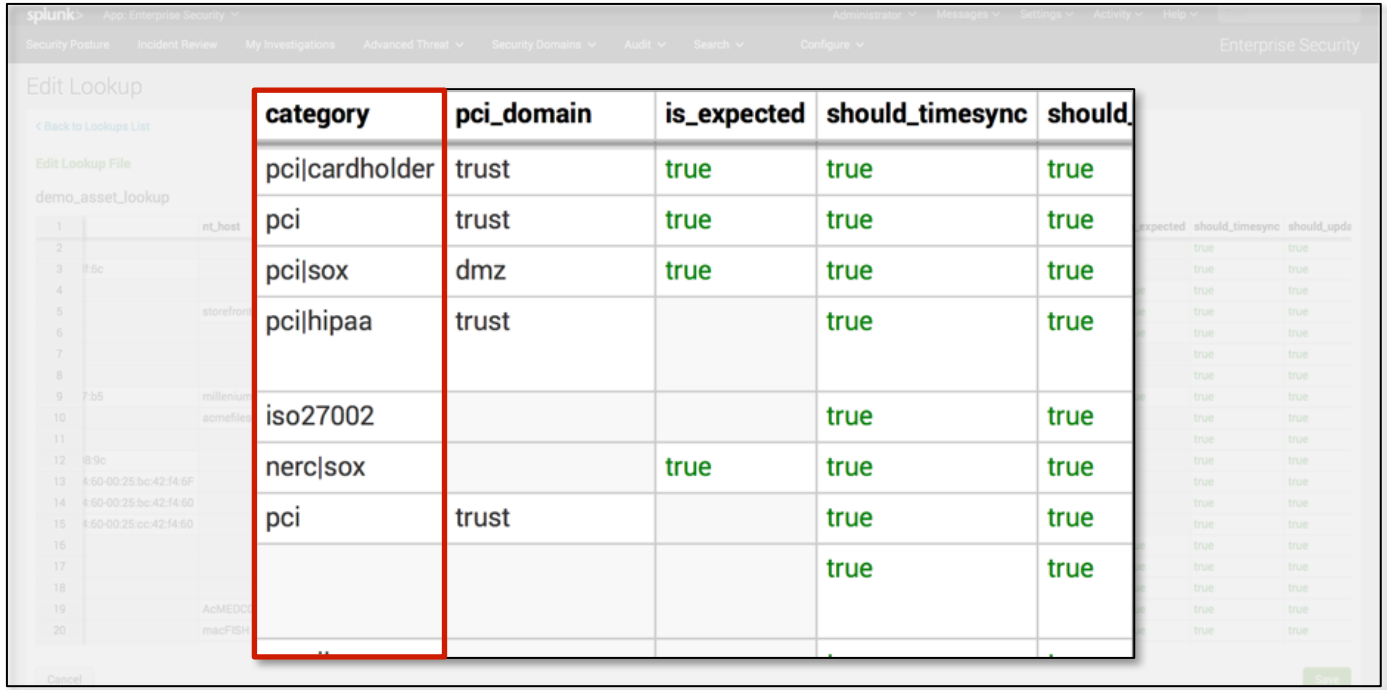
Category field is multi-valued



category	pci_domain	is_expected	should_timesync	should_
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

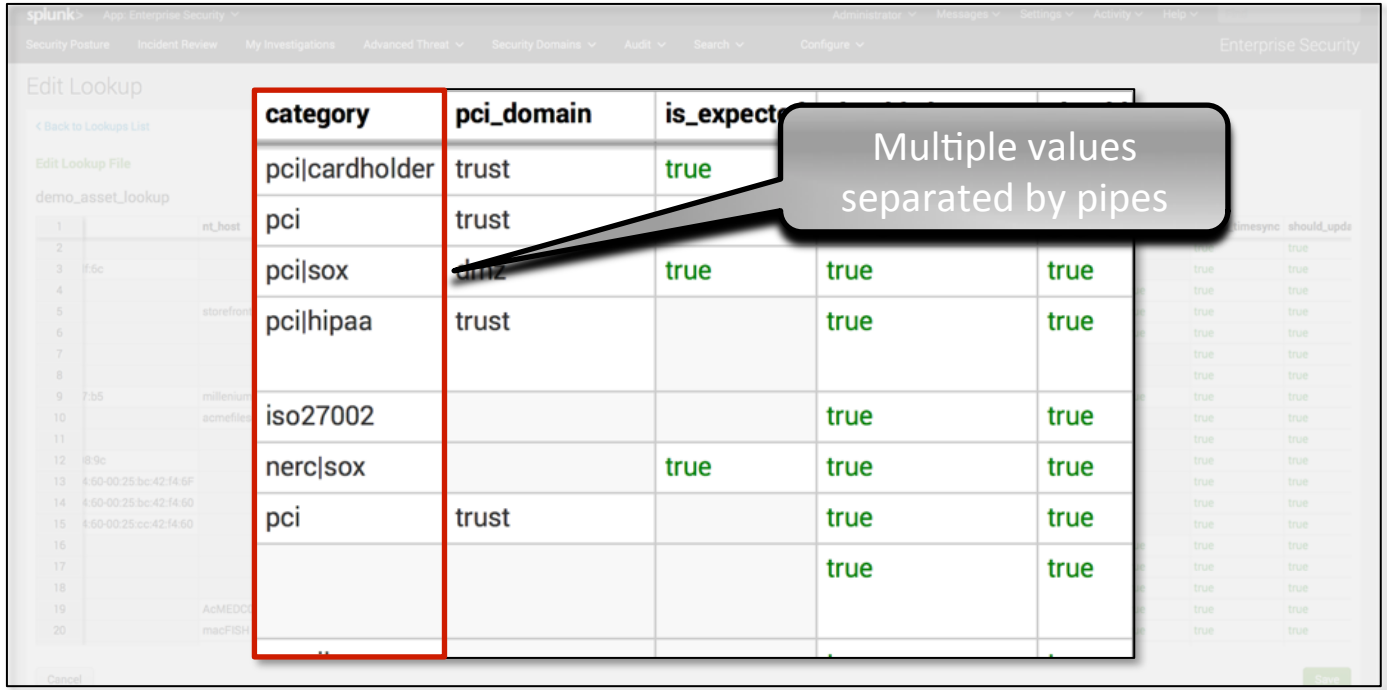
Category field is multi-valued



category	pci_domain	is_expected	should_timesync	should_
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

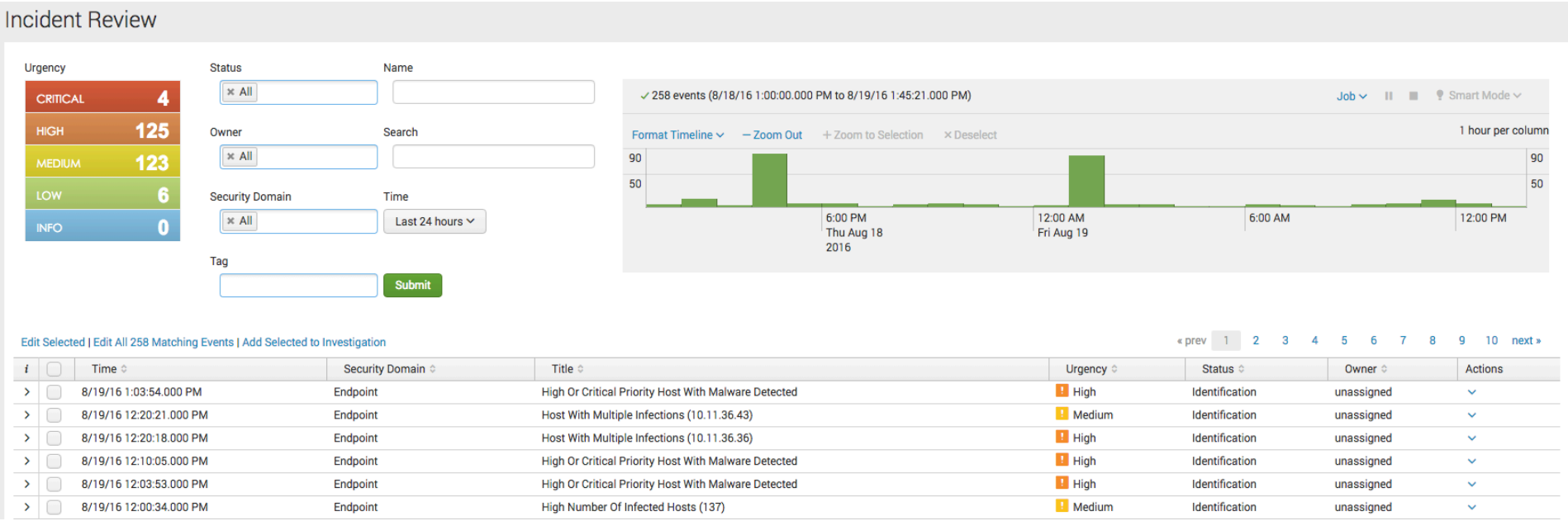
Category field is multi-valued



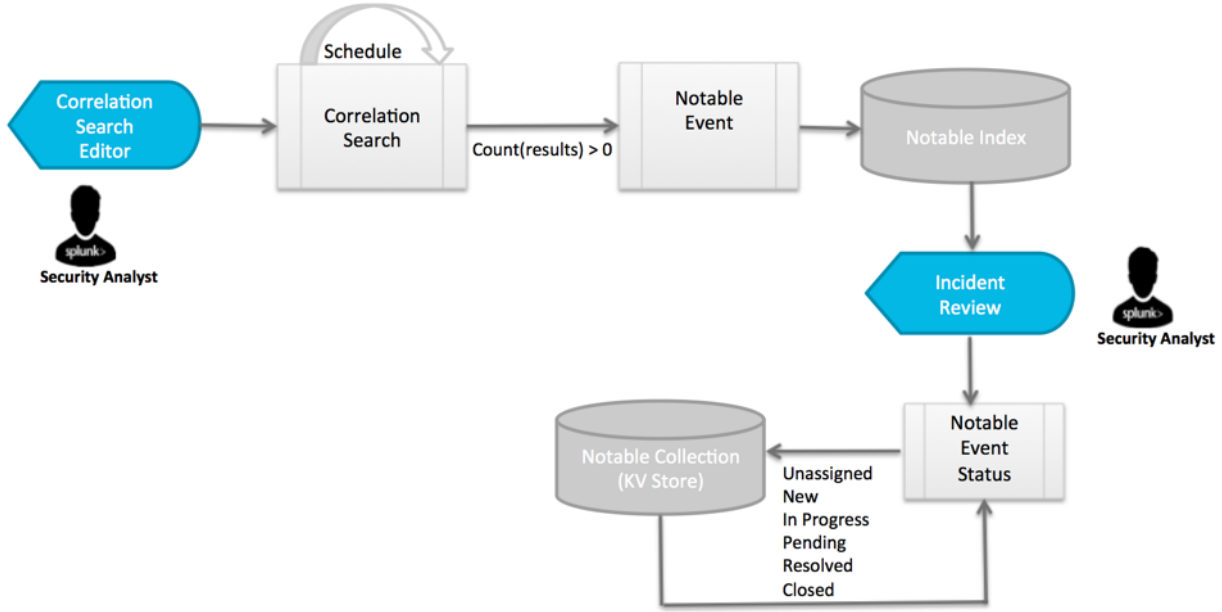
category	pci_domain	is_expect		
pci|cardholder	trust	true		
pci	trust			
pci|sox	dmz	true	true	true
pci|hipaa	trust		true	true
iso27002			true	true
nerc|sox		true	true	true
pci	trust		true	true
			true	true

Notable Events

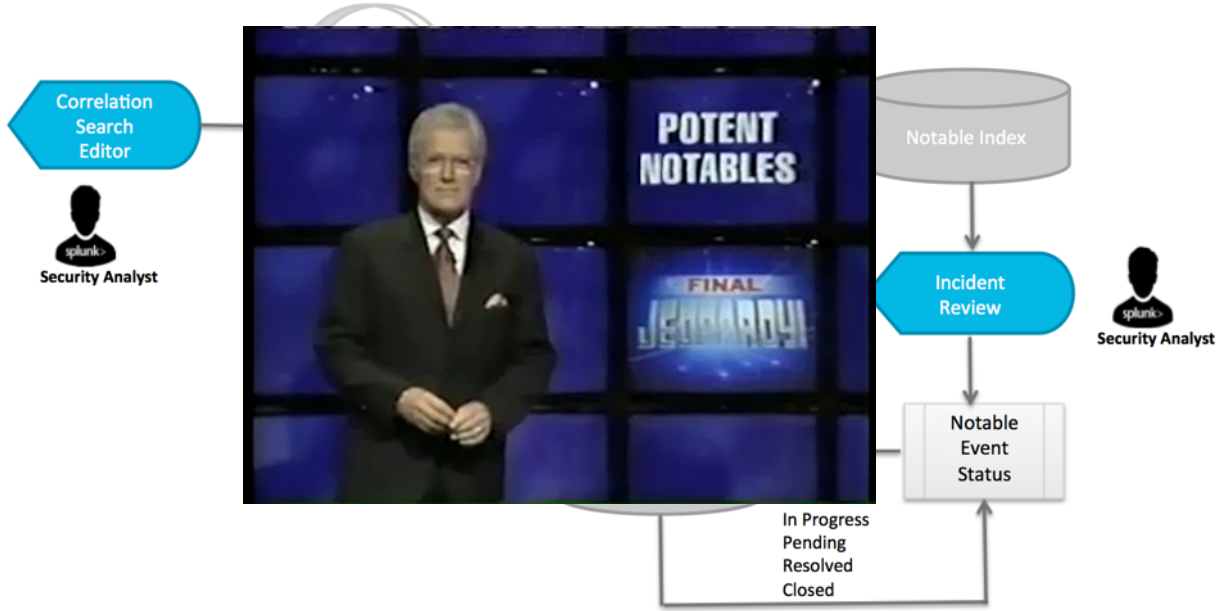
Where Correlation Searches are Surfaced



Notable Events Architecture Diagram

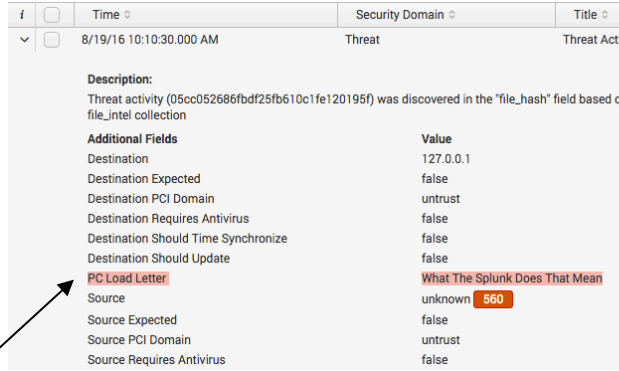


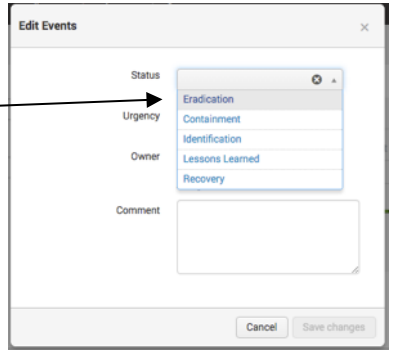
Notable Events Architecture Diagram



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]

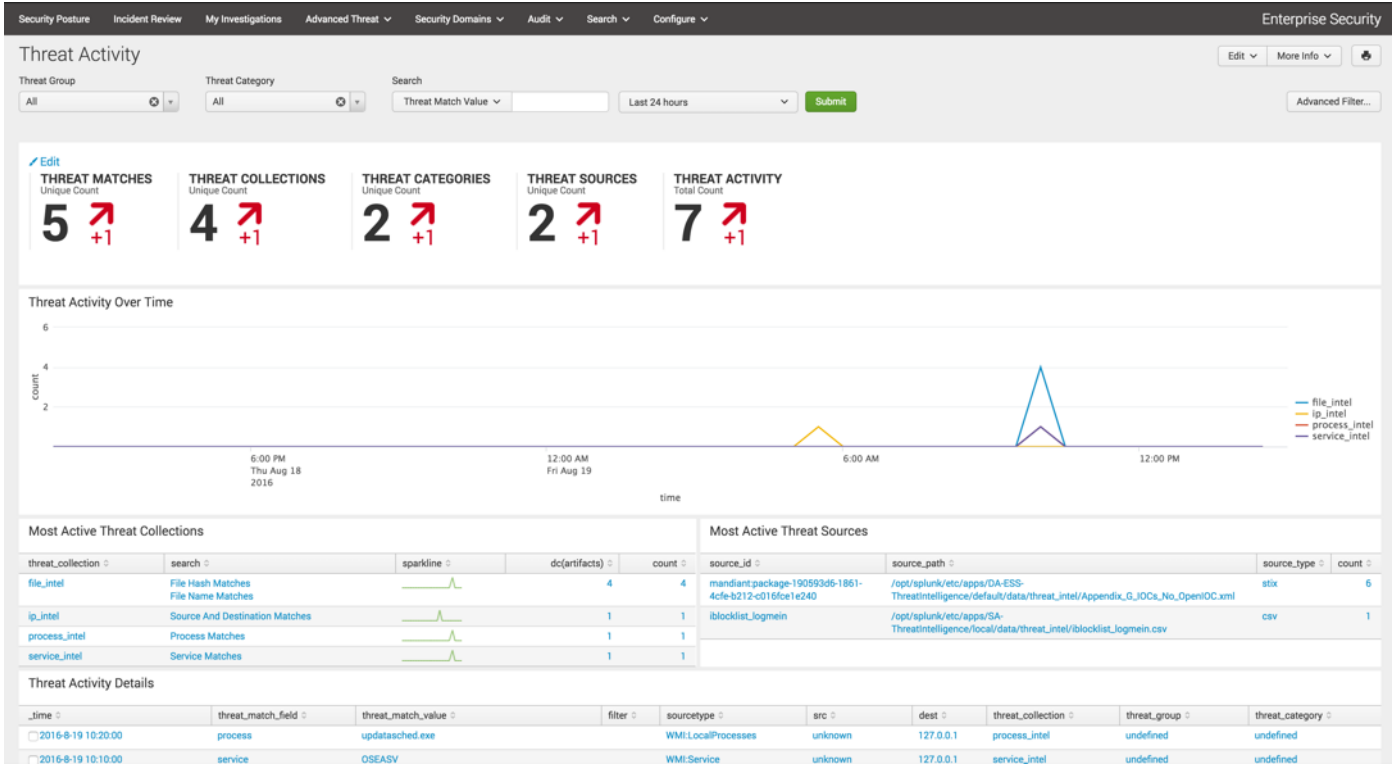




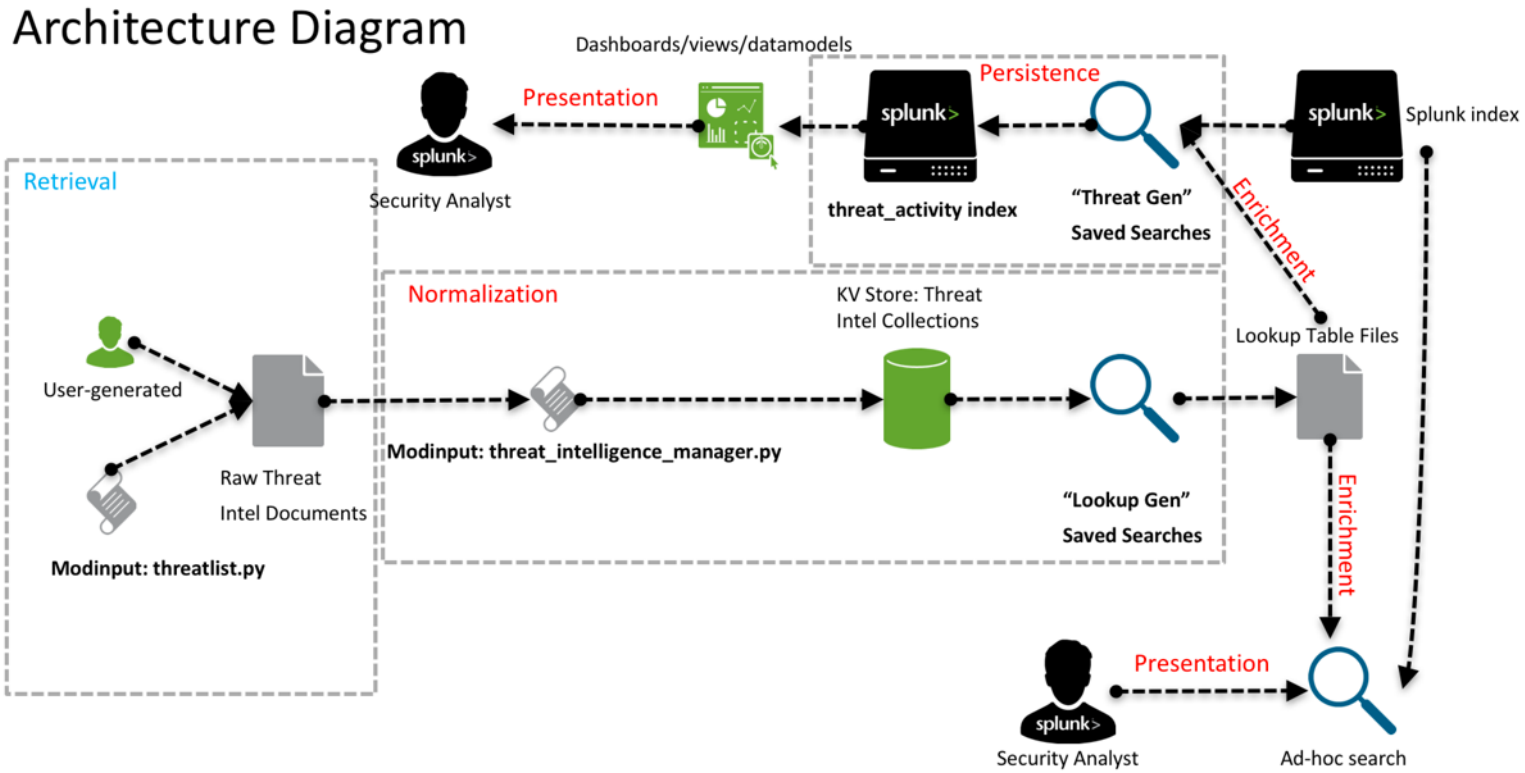
Notable Events Example + Demo

- 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

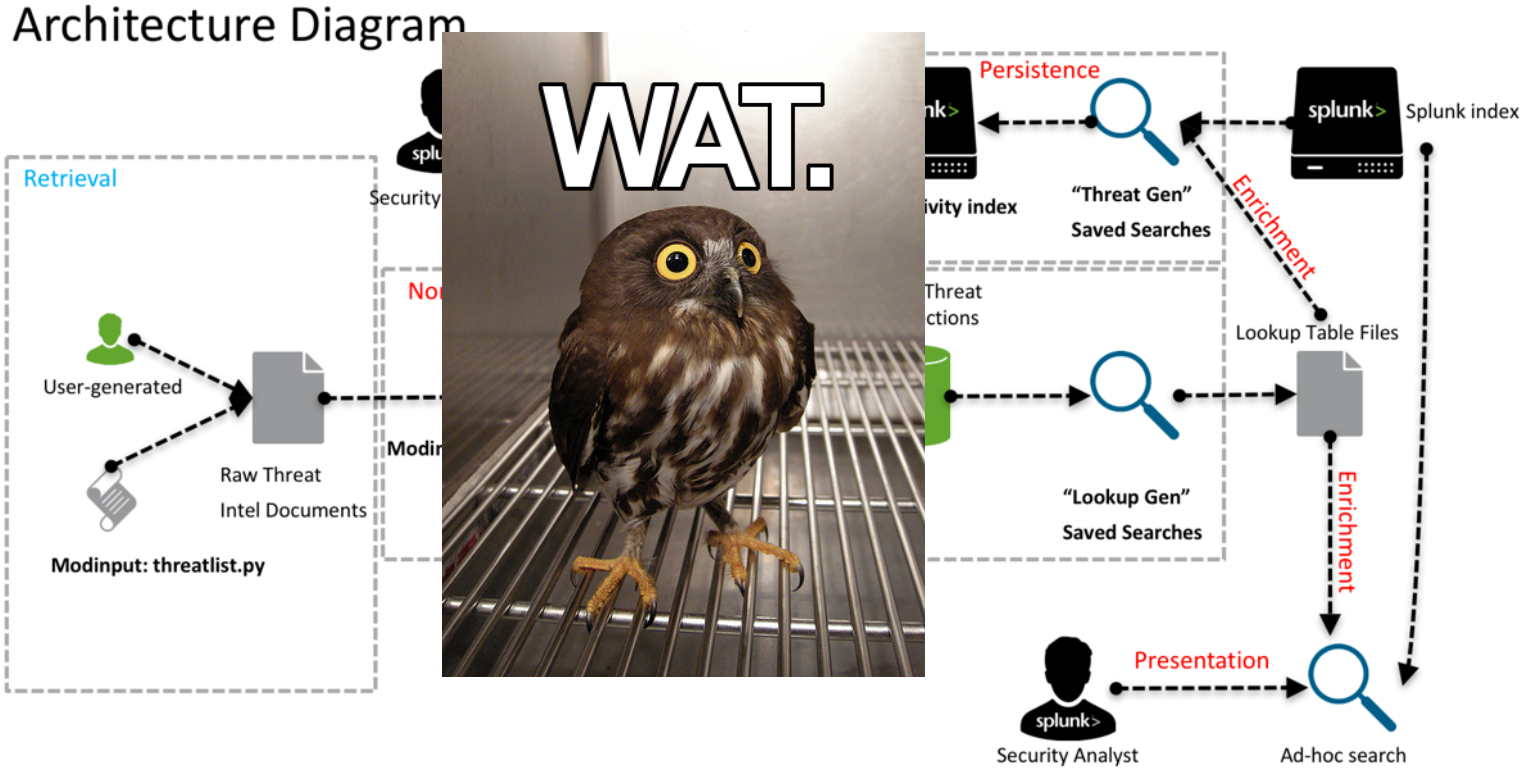
Threat Intelligence



Threat Intelligence Architecture



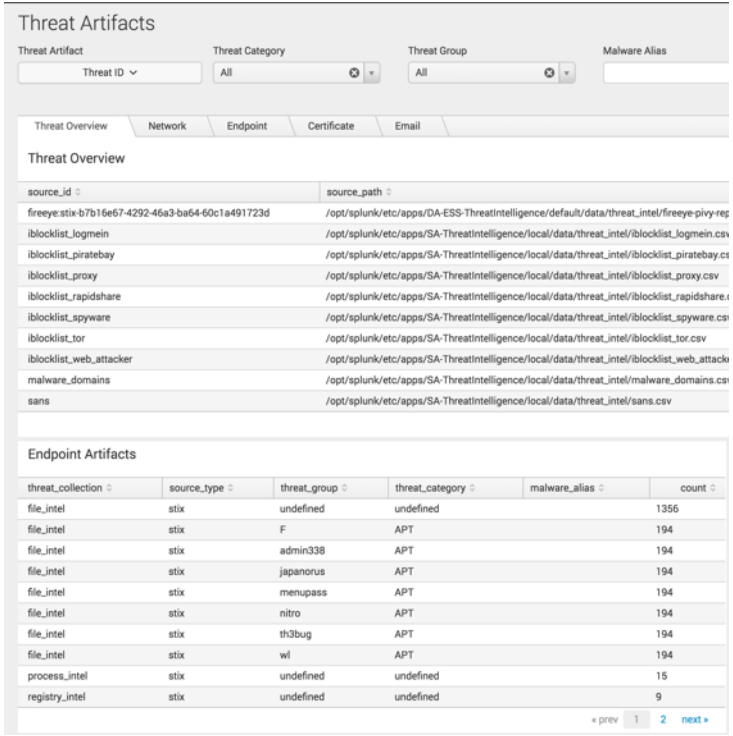
Threat Intelligence Architecture



Threat Intelligence Framework

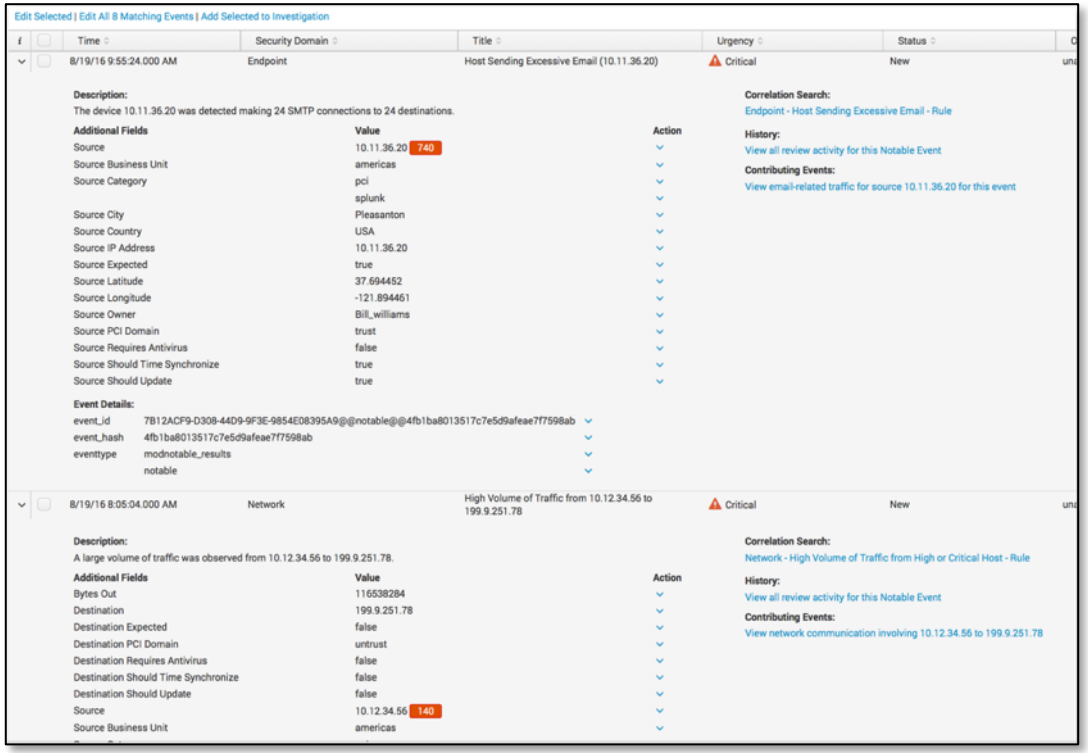
- Composed of: mod-input, scheduled searches, indexes, and lookups.
- You get:
  - flexible input processing (mod-input)
  - deduplication
  - datamodels
  - lookup creation/management
  - high-volume/high-speed matching for free (correlation searches)
- Handy One Liners:
  - What fields are supported 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



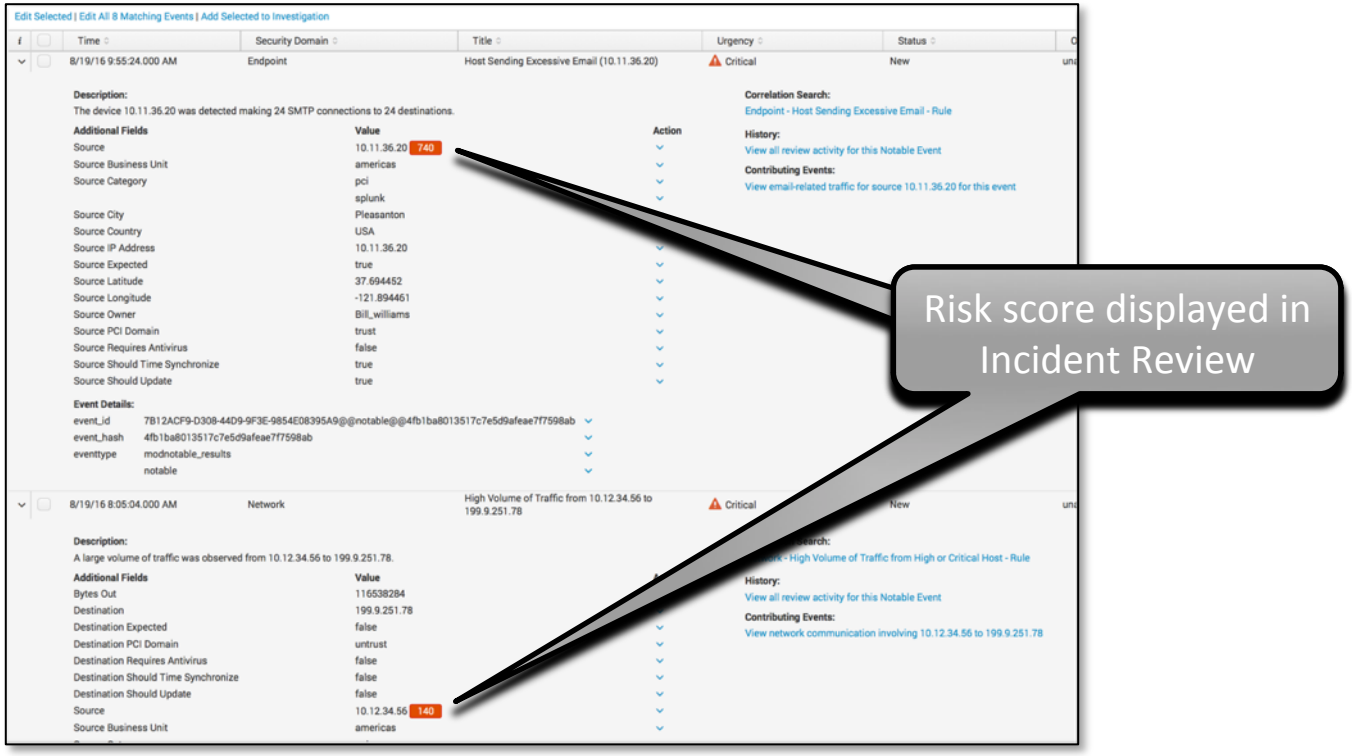
Risk Analysis

Adds context…



Risk Analysis

Adds context…



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…

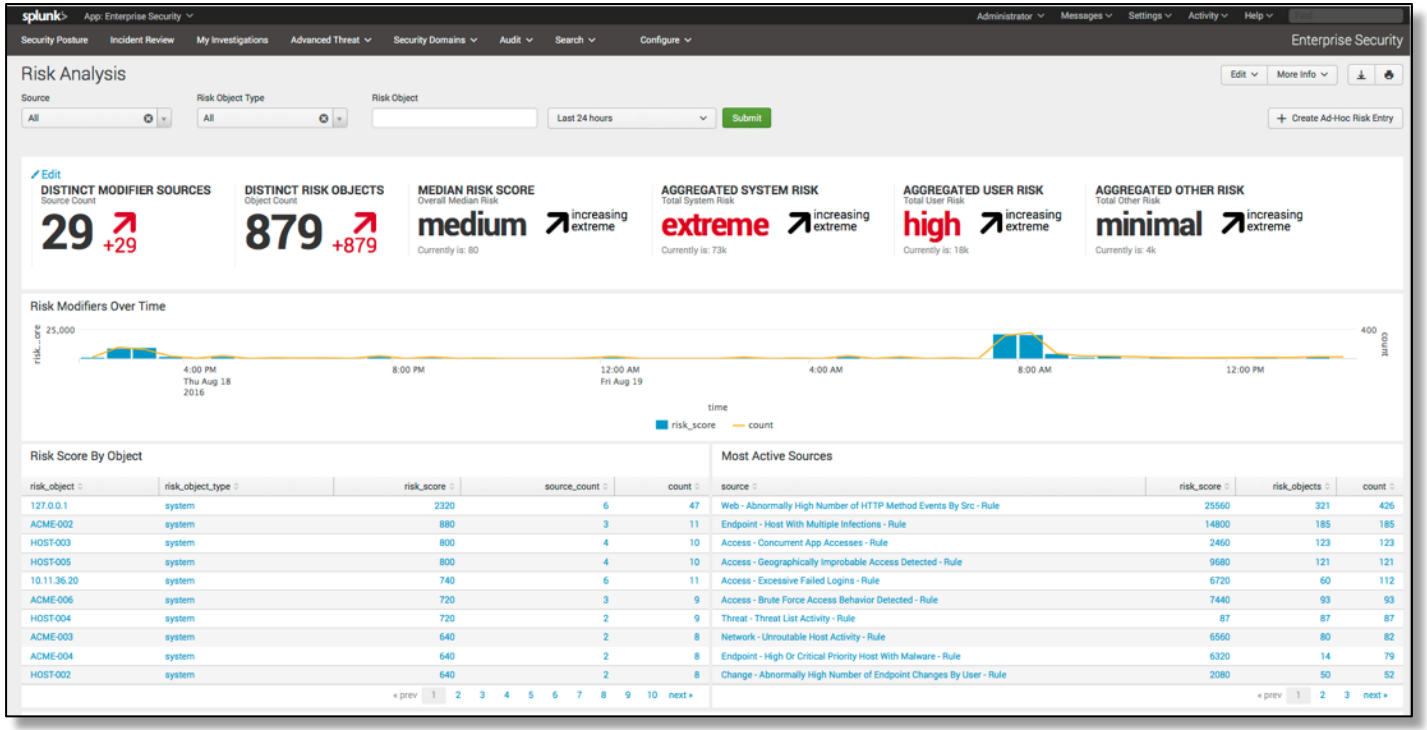
Credit @j4vv4d **Host Unknown presents: I'm a C I Double S P**

Risk Analysis

Risk as an aggregation of suspicious events…

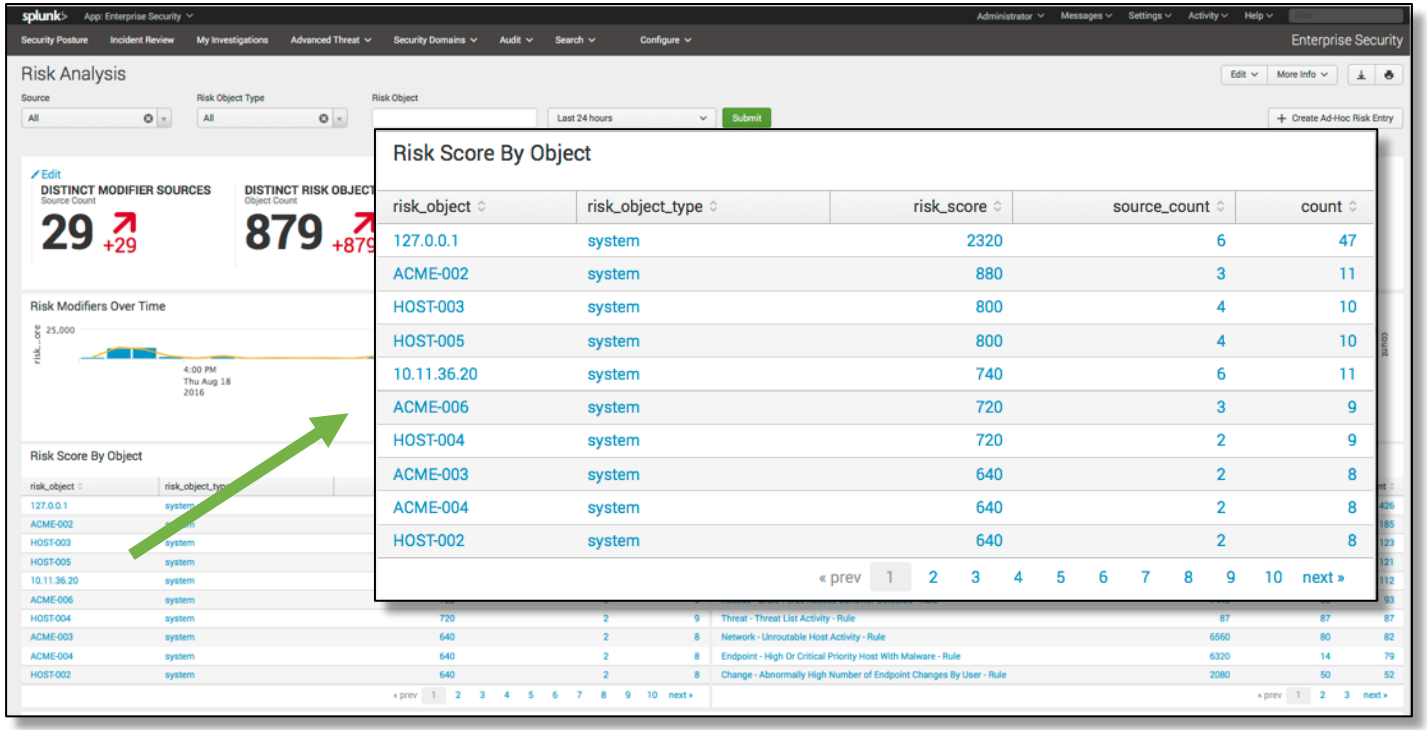
Risk Analysis

View risk scores in ES

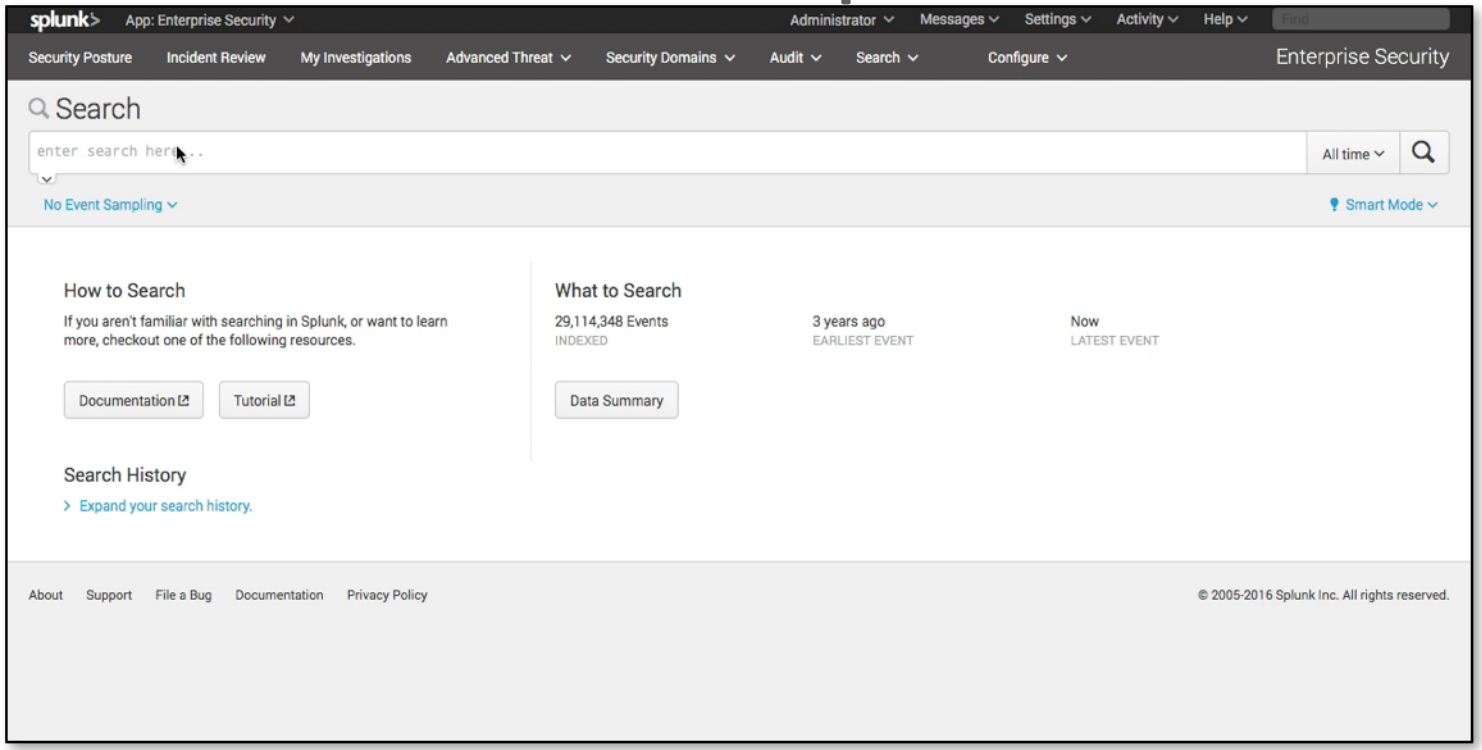


Risk Analysis

View risk scores in ES



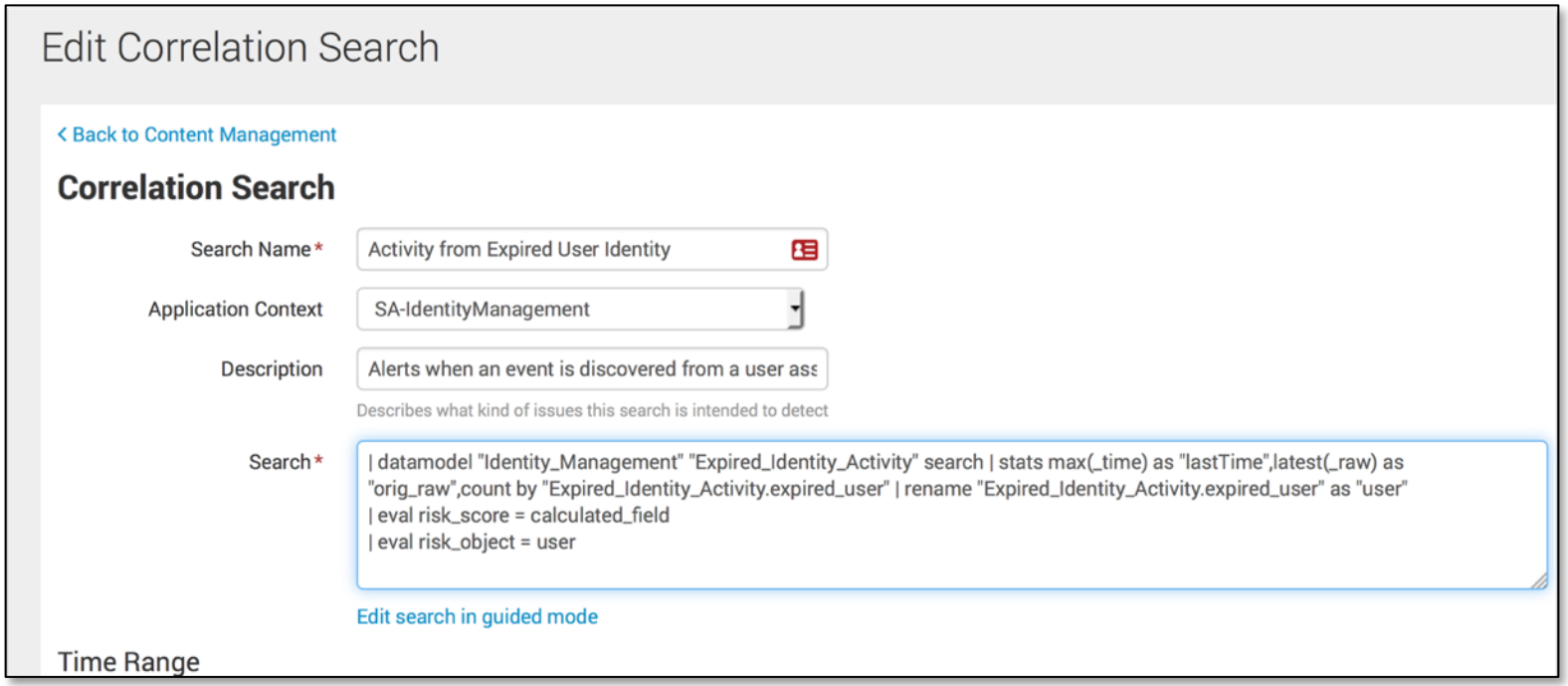
Risk Analysis
Or in core Splunk



index=risk app=* | timechart count by app

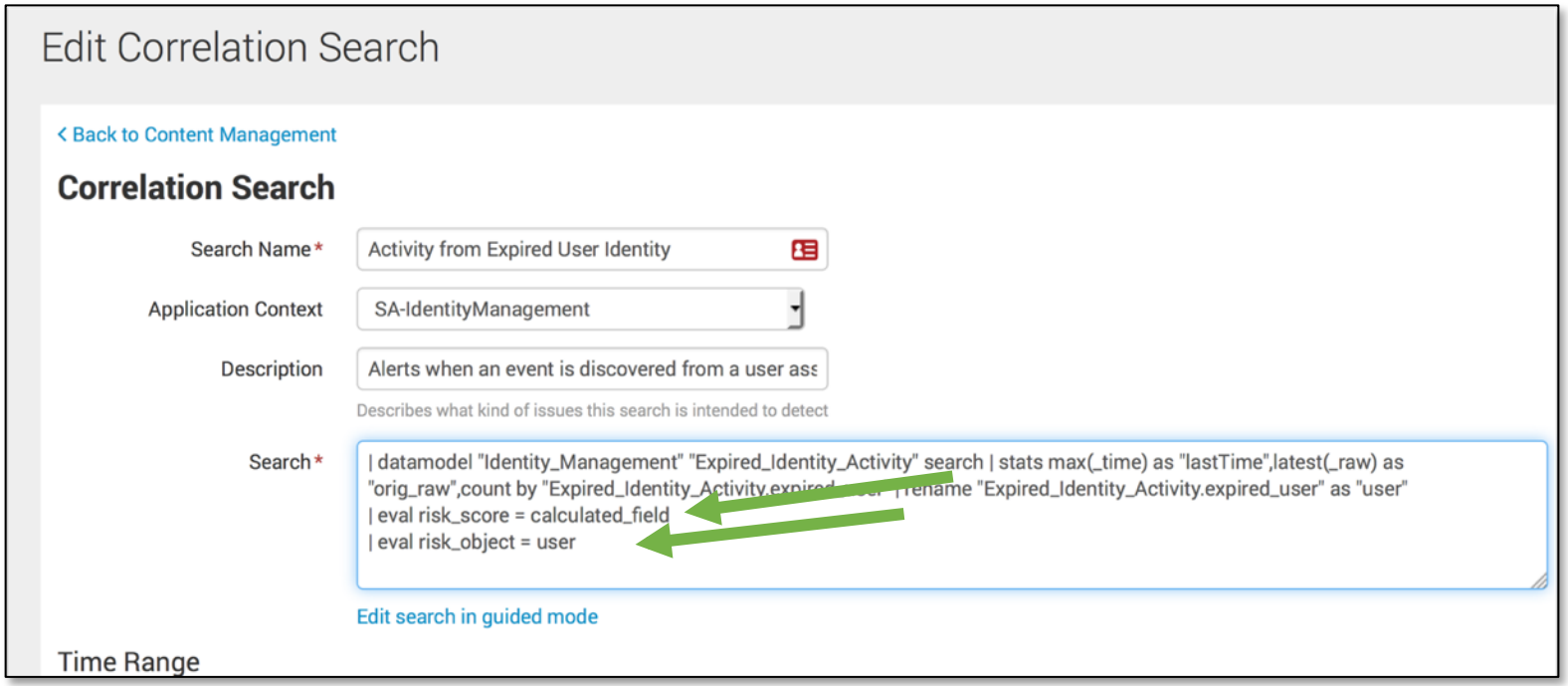
Risk Analysis

Set risk parameter statically or dynamically in CS



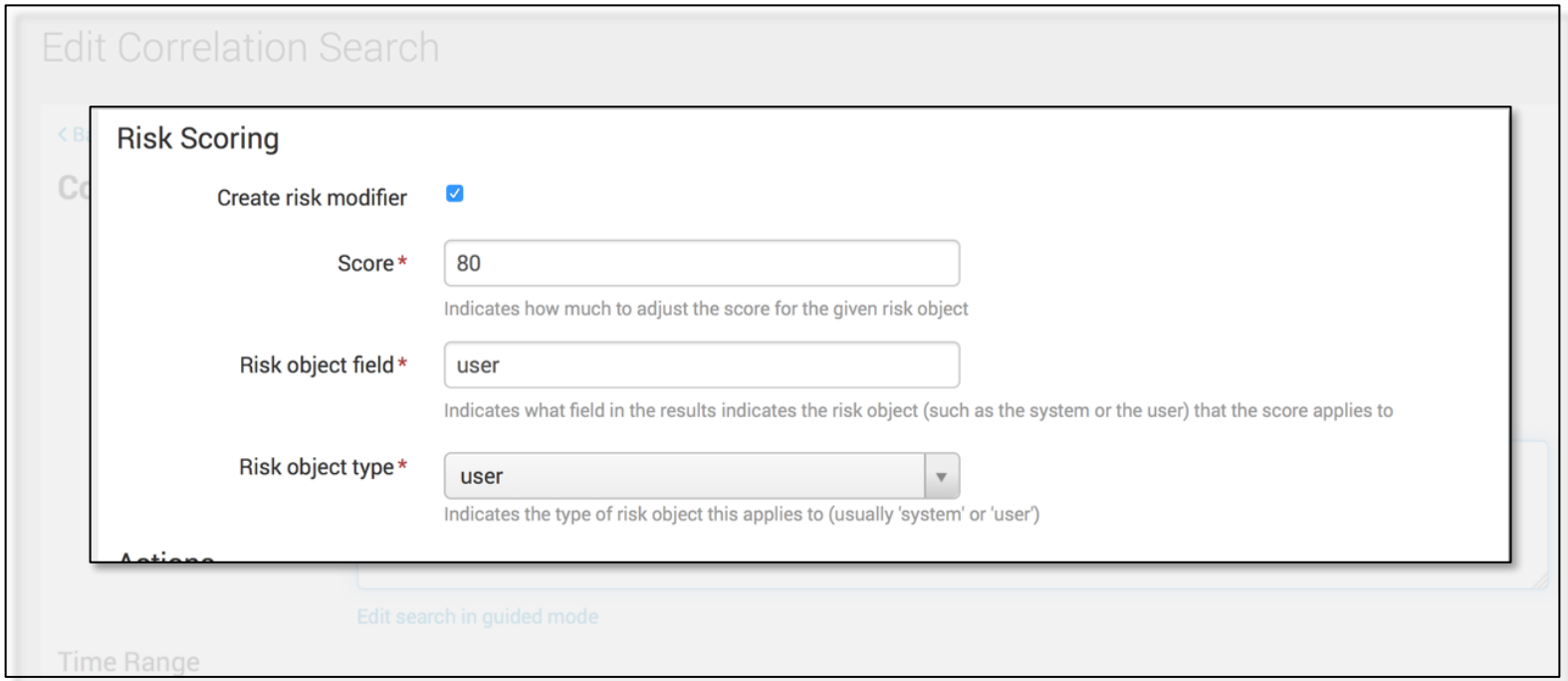
Risk Analysis

Set risk parameter statically or dynamically in CS

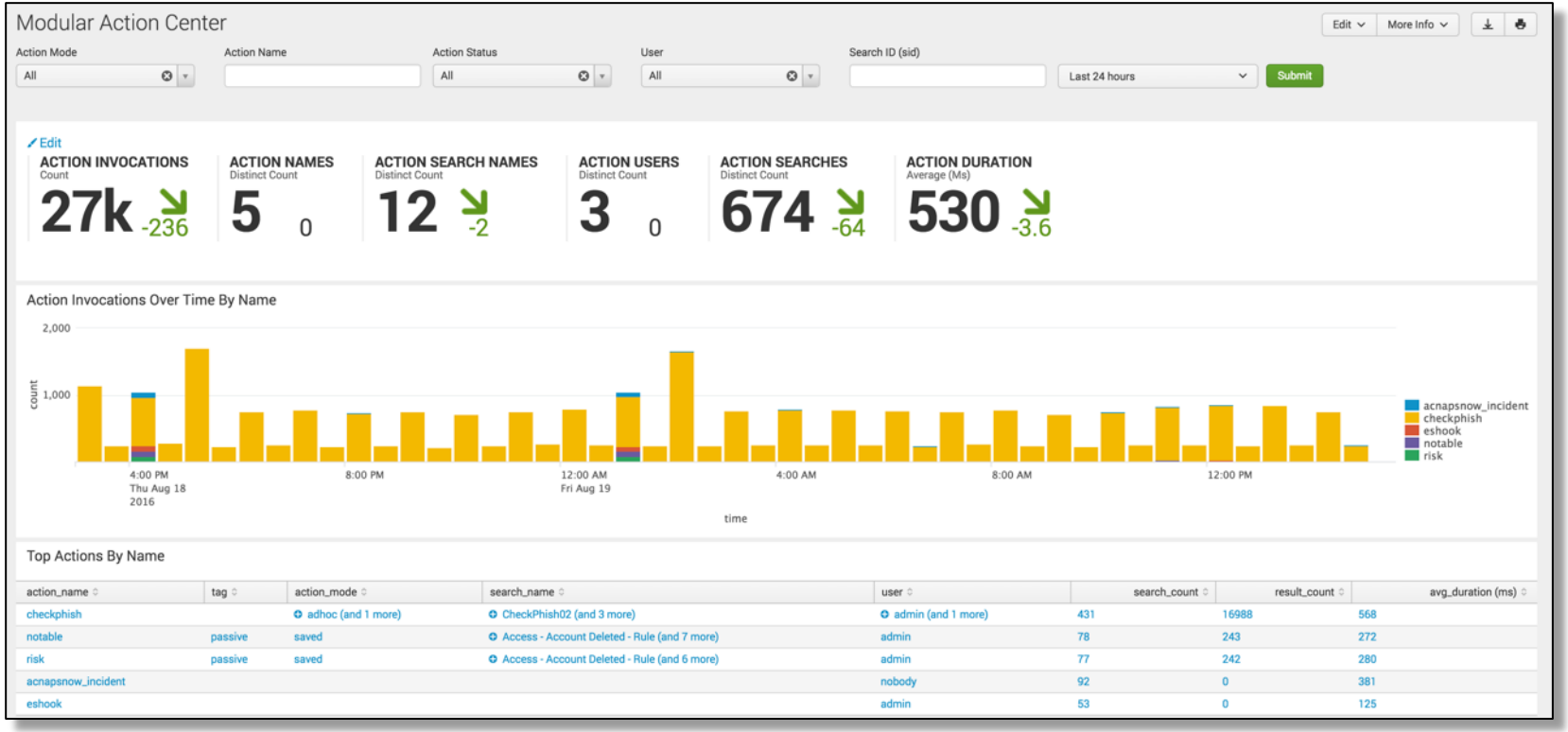


Risk Analysis

Set risk parameter statically or dynamically in CS



Adaptive Response Framework



Adaptive Response Framework

- Comp ic
  - You nice abstraction for c
- This w
  - ES te
- Lever a search)

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

splunk>