Enterprise Security Biology Part 2

Asset & Identity Framework

John Stoner | Principal Security Strategist

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a høliday in Sweden this yër? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON Including the majestik møøse A Møøse once bit my Marcus... No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møvies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Mølars of Horst Nordfink"... In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.

whoami > John Stoner

CISSP, GCIA, CISA, GCIH, GCTI

Principal Security Strategist

@stonerpsu

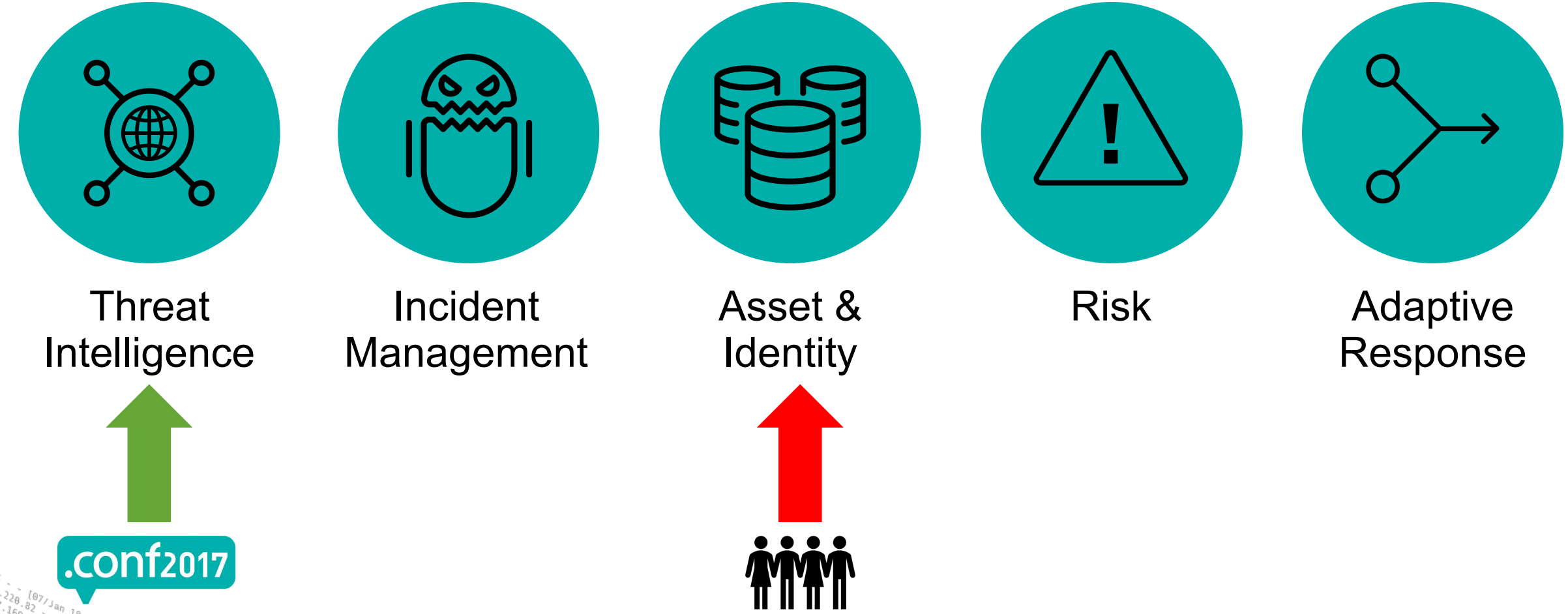
- 20+ Years kicking around databases, ISPs and cyber
- 3.5 Years at Splunk
- Creator of SA-Investigator
- Co-editor and author Hunting with Splunk: The Basic blog series
- Assist in steering the BOTS ship
- Enjoys writing workshops on hunting and investigating with Splunk
- Listening to The Smiths

Agenda

Asset & Identity Framework

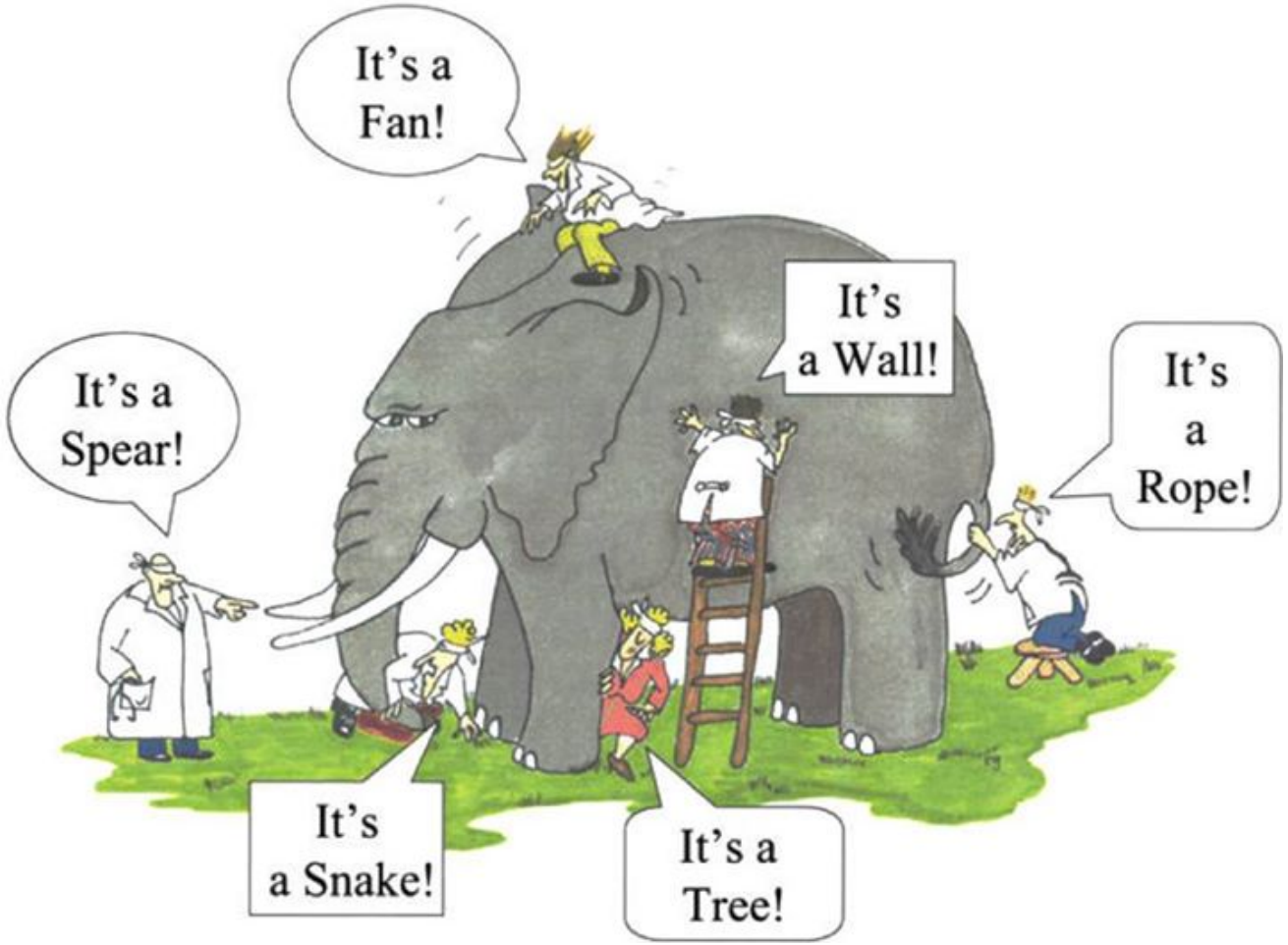
- Enterprise Security Frameworks
- Collection
- Processing
- Troubleshooting
- Adding A New Field to the Asset & Identity Framework

Enterprise Security Frameworks



Why Should I Care About Asset & Identity?

Context



Why Should I Care About Asset & Identity

Practical Application of Context

8/23/17 2:59:57.000 PM | Threat | Threat Activity Detected (nc.exe) | Low | New | unassigned

Description:

Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelligence available in the file collection

Additional Fields	Value	Action
Destination	160.153.91.7	
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
Source	10.0.2.109	
Source Category	workstation	
	windows	
Source City	San Francisco	
Source Country	US	
Source DNS	wrk-klagerf.frothly.local	
Source IP Address	10.0.2.109	
Source Expected	false	
Source MAC Address	00:0c:29:f5:5e:8e	
Source NT Hostname	wrk-klagerf	
Source Owner	Kevin Lagerfield	
Source PCI Domain	untrust	
Source Requires Antivirus	TRUE	
Source Should Time Synchronize	false	
Source Should Update	TRUE	
Threat Category	undefined	
Threat Collection	file	
Threat Group	undefined	
Threat Match Field	file_name	
Threat Match Value	nc.exe	

Related Investigations:

Investigation (No Permission)

Correlation Search:

Threat - Threat List Activity - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View all threat activity involving file_name="nc.exe"

Original Event:

```
08/23/2017 21:59:57 +0000, search_name="Threat - File Name Matches - Threat Gen", search_now=1505071997.000, info_search_time=1505071997.110, dest="160.153.91.7", file_name="nc.exe", info_max_time="1503547198.000000", info_min_time="1503521597.000000", info_search_time="1503525597.000000", orig_sourcetype="stream:ftp", src="10.0.2.109", tag="", threat_collection=file, threat_description="This file was detected and reported by John Stoner in the FRPCENK report", threat_match_field=file_name, threat_match_value="nc.exe"
```

View original event

Adaptive Responses:

Response	Mode	Time	User	Status
Risk Analysis	adhoc	2017-09-10T12:33:20-0700	system	✓ success
Notable	adhoc	2017-09-10T12:33:19-0700	system	✓ success

View Adaptive Response Invocations

Next Steps:

No Next Steps defined.

Why Should I Care About Asset & Identity

Practical Application of Context

8/23/17 2:59:57.000 PM Threat Threat Activity Detected (nc.exe) Low New unassigned

Description:

Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelliger

Additional Fields	Value
Destination	160.153.91.7
Destination Expected	false
Destination PCI Domain	untrust
Destination Requires Antivirus	false
Destination Should Time Synchronize	false
Destination Should Update	false
Source	10.0.2.109
Source Category	workstation
	windows
Source City	San Francisco
Source Country	US
Source DNS	wrk-klagerf.frothly.local
Source IP Address	10.0.2.109
Source Expected	false
Source MAC Address	00:0c:29:f5:5e:8e
Source NT Hostname	wrk-klagerf
Source Owner	Kevin Lagerfield
Source PCI Domain	untrust
Source Requires Antivirus	TRUE
Source Should Time Synchronize	false
Source Should Update	TRUE
Threat Category	undefined
Threat Collection	file
Threat Group	undefined
Threat Match Field	file_name
Threat Match Value	nc.exe

Source	10.0.2.109
Source Category	workstation
	windows
Source City	San Francisco
Source Country	US
Source DNS	wrk-klagerf.frothly.local
Source IP Address	10.0.2.109
Source Expected	false
Source MAC Address	00:0c:29:f5:5e:8e
Source NT Hostname	wrk-klagerf
Source Owner	Kevin Lagerfield
Source PCI Domain	untrust
Source Requires Antivirus	TRUE
Source Should Time Synchronize	false
Source Should Update	TRUE

Our Goal Today?

- Better understand how Splunk processes assets and identities in Enterprise Security
- Better insight = Better Troubleshooting = Better Use

Why Dissection?

dis·sect

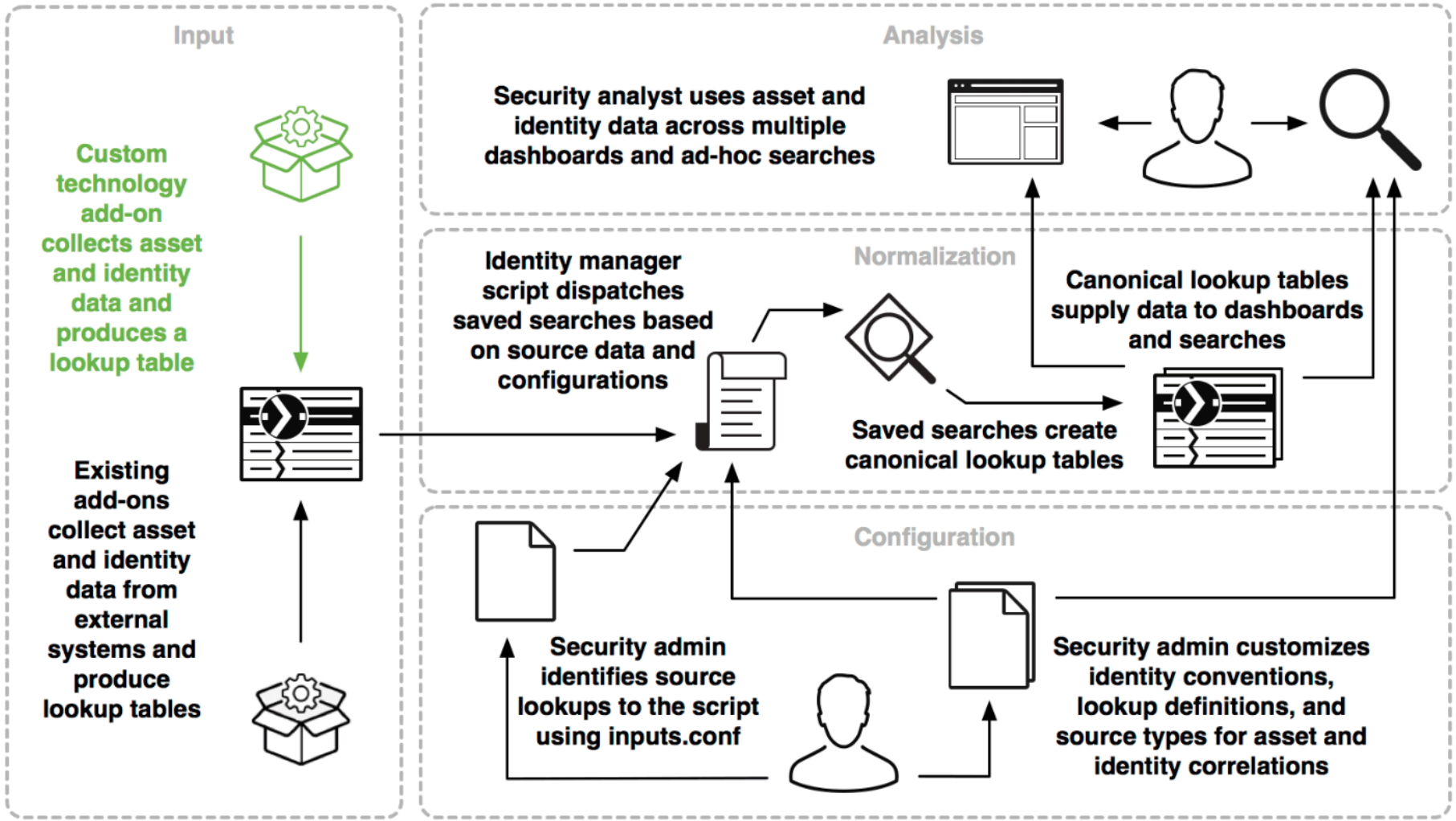
/dəˈsekt,dīˈsekt/

verb

- methodically cut up (a body, part, or plant) in order to study its internal parts
  - synonyms: anatomize, cut up/open, dismember, vivisect
- analyze (something) in minute detail
  - synonyms: analyze, examine, study, scrutinize, pore over, investigate, go over with a fine-tooth comb

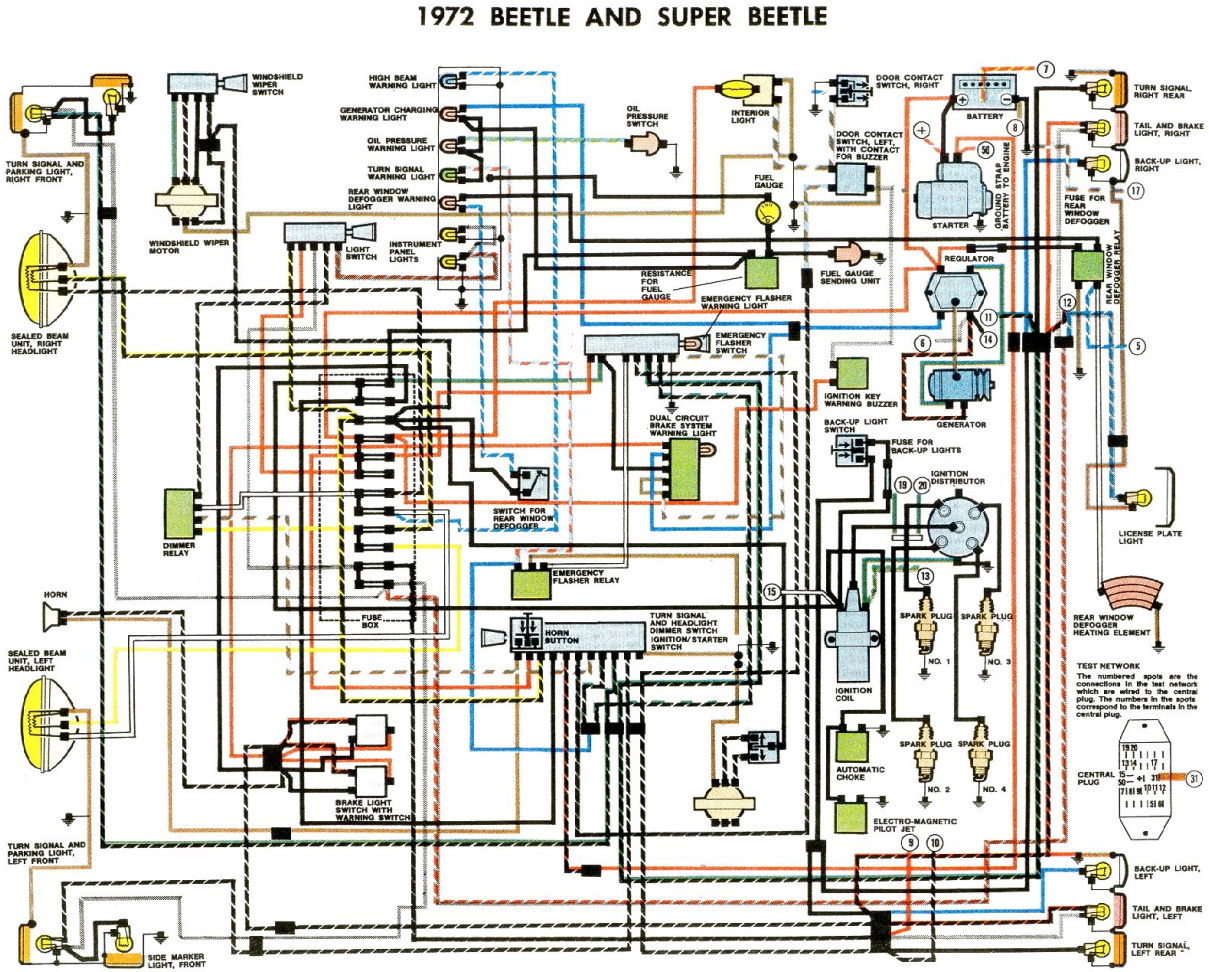
Asset & Identity Framework

http://dev.splunk.com/view/enterprise-security/SP-CAAAFBB

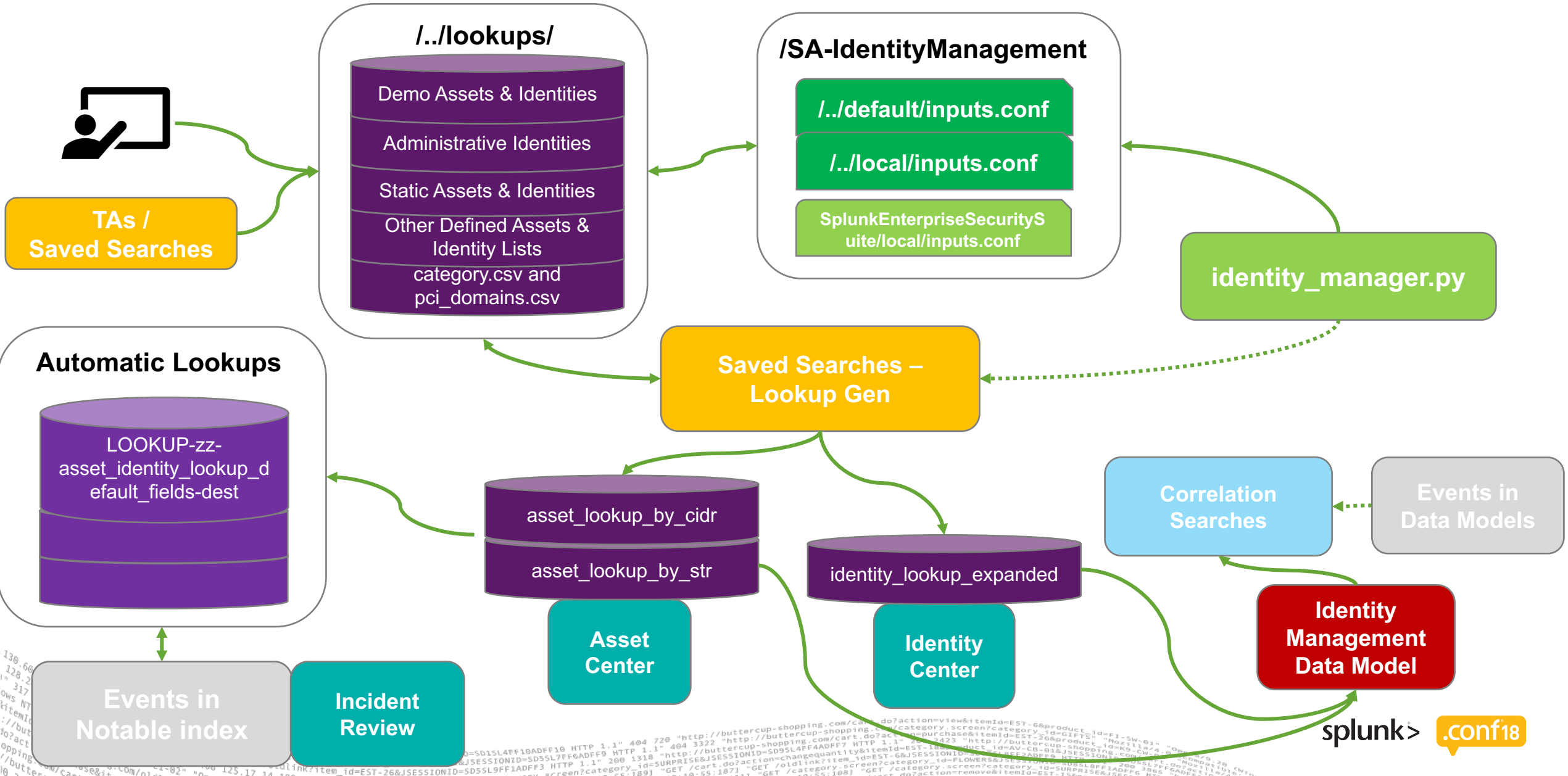


splunk> .conf18

Why This Presentation...

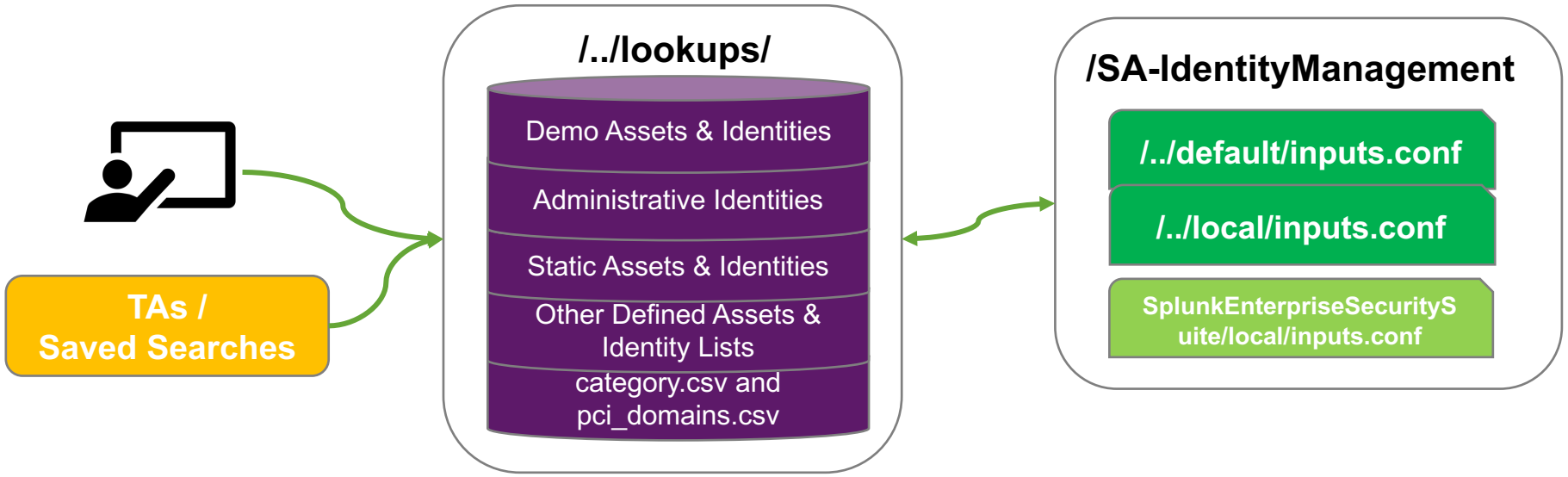


Asset & Identity Framework Data Flow

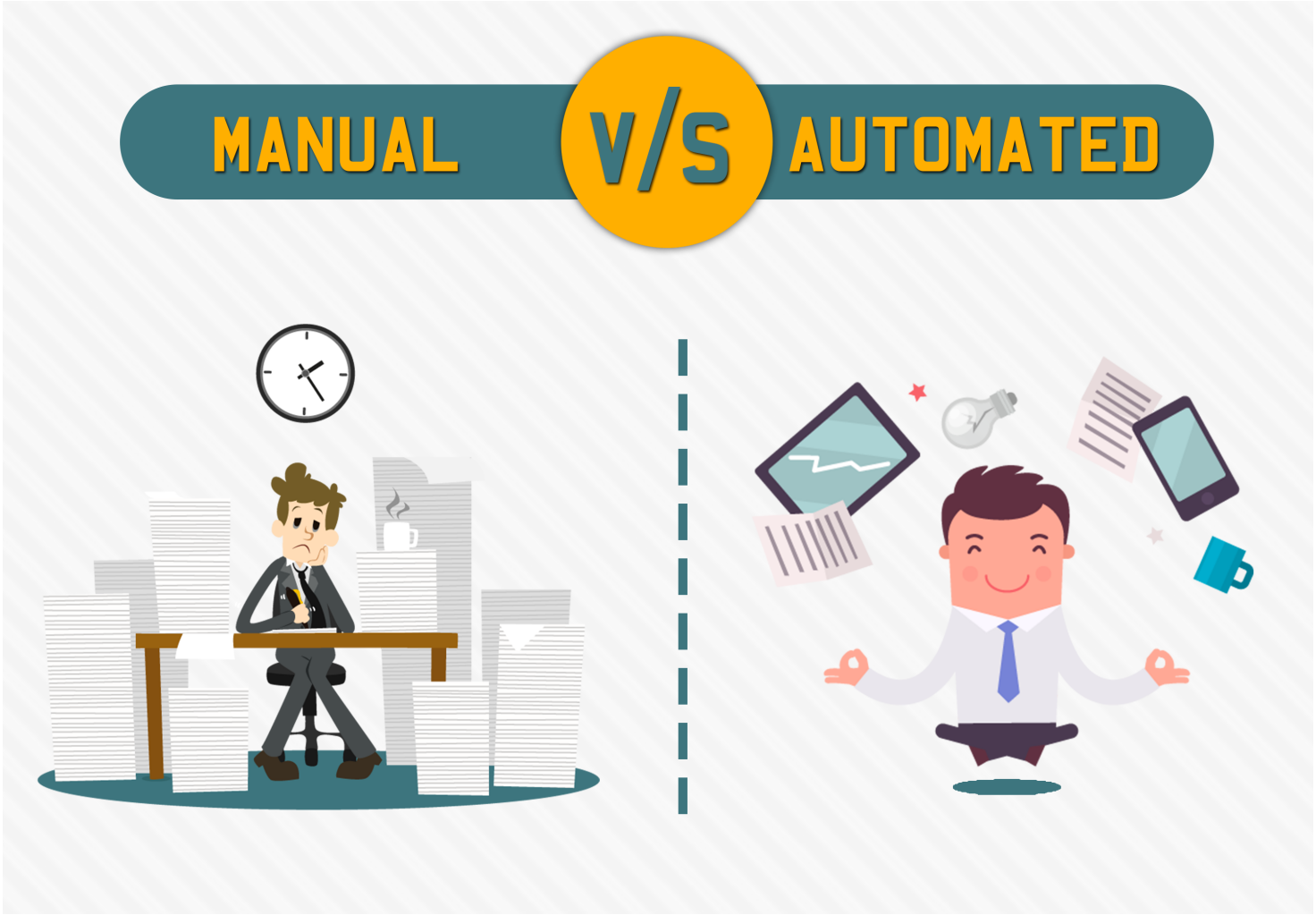


Collection

Asset & Identity Framework - Collection



Getting Data Into A&I



- Active Directory
- LDAP
- CMDB (DBX)
- Other Technical-Add Ons

The Manual Method

Configure > Content Management

Edit Lookup File

administrative_identity_lookup

1	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category
2	3comcso												default|privileged
3	adfexc												default|privileged
4	adm												default|privileged
5	admin|administrator												default|privileged

demo_asset_lookup

1	ip	mac	nt_host	dns	owner	priority	lat	long
2	6.0.0.1-9.0.0.0					low	41.040855	28.986183
3	1.2.3.4	00:15:70:91:df:6c				medium	38.959405	-77.04
4				CORP1.acmetech.com		high	37.694452	-121.894461
5	192.168.12.9-192.168.12.9		storefront			critical	32.931277	-96.818167
6	2.0.0.0/8					low	50.84436	-0.98451

frothly_ids

1	identity	prefix	nick	first	last	suffix	email	phone
2	ghoppy|grace.hoppy|FROTHLY\grace.hoppy|frothly.local\ grace.hoppy|grace.hoppy@FROTHLY.LOCAL	Ms.		Grace	Hoppy		ghoppy@froth.ly	+1 (800)555-1562
3	fyodor|fyodor.malteskesko|FROTHLY\fyodor.malteskesko|frothly.local\fyodor.malteskesko|fyodor.malteskesko@FROTHLY.LOCAL	Mr.		Fyodor	Malteskesko		fyodor@froth.ly	+1 (800)555-8762
4	btun|billy.tun|FROTHLY\billy.tun|frothly.local\billy.tun|billy.tun@FROTHLY.LOCAL	Mr.		Billy	Tun		btun@froth.ly	+1 (800)555-7388

splunk> .conf18

The Automated Method

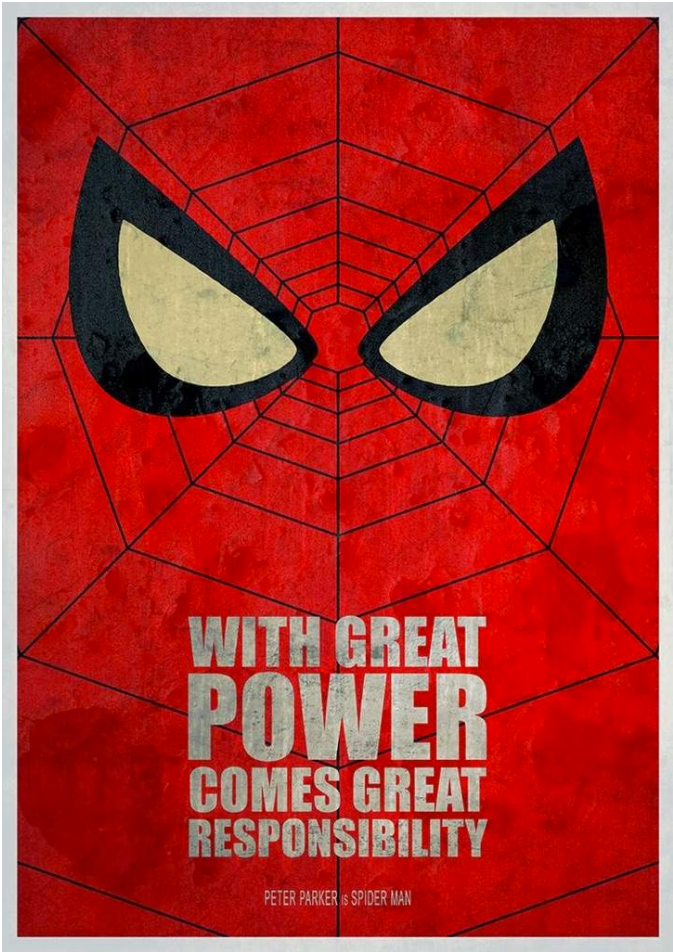
Technology	Asset/ Identity	App	URL
Active Directory	Both	SA-ldapsearch *	https://splunkbase.splunk.com/app/1151/
	Both	SecKit Windows Add On for ES Asset and Identities	https://splunkbase.splunk.com/app/3059/
LDAP	Both	SA-ldapsearch *	https://splunkbase.splunk.com/app/1151/
CMDB	Asset	DB Connect *	https://splunkbase.splunk.com/app/2686/
		SecKit Common Assets Add-on for Splunk Enterprise Security	https://splunkbase.splunk.com/app/3055/
ServiceNow	Both	Splunk Add-on for ServiceNow	https://splunkbase.splunk.com/app/1928/
Asset Discovery	Asset	Splunk for Asset Discovery	https://splunkbase.splunk.com/app/662/
Bit9	Asset	Splunk Add-on for Bit9 *	https://splunkbase.splunk.com/app/2790/
Cisco ISE	Both	Splunk Add-on for Cisco ISE *	https://splunkbase.splunk.com/app/1915/
Microsoft SCOM	Asset	Splunk Add-on for Microsoft SCOM *	https://splunkbase.splunk.com/app/2729/
Okta	Identity	Splunk Add-on for Okta *	https://splunkbase.splunk.com/app/2806/
Sophos	Asset	Splunk Add-on for Sophos *	https://splunkbase.splunk.com/app/1854/
Symantec Endpoint Protection	Asset	Splunk Add-on for Symantec Endpoint Protection *	https://splunkbase.splunk.com/app/2772/
Splunk Enterprise	Asset	Add asset data from indexed events in Splunk platform	http://docs.splunk.com/Documentation/ES/5.1.0/Admin/Examplemethodsofaddingassetandidentitydata#Add_asset_data_from_indexed_events_in_the_Splunk_platform
Amazon Web Services (AWS)	Asset	SecKit AWS Add On for ES Asset and Identities	https://splunkbase.splunk.com/app/3586/

http://docs.splunk.com/Documentation/ES/5.1.0/Admin/Collectandextractassetandidentitydata * = Custom Search Needed

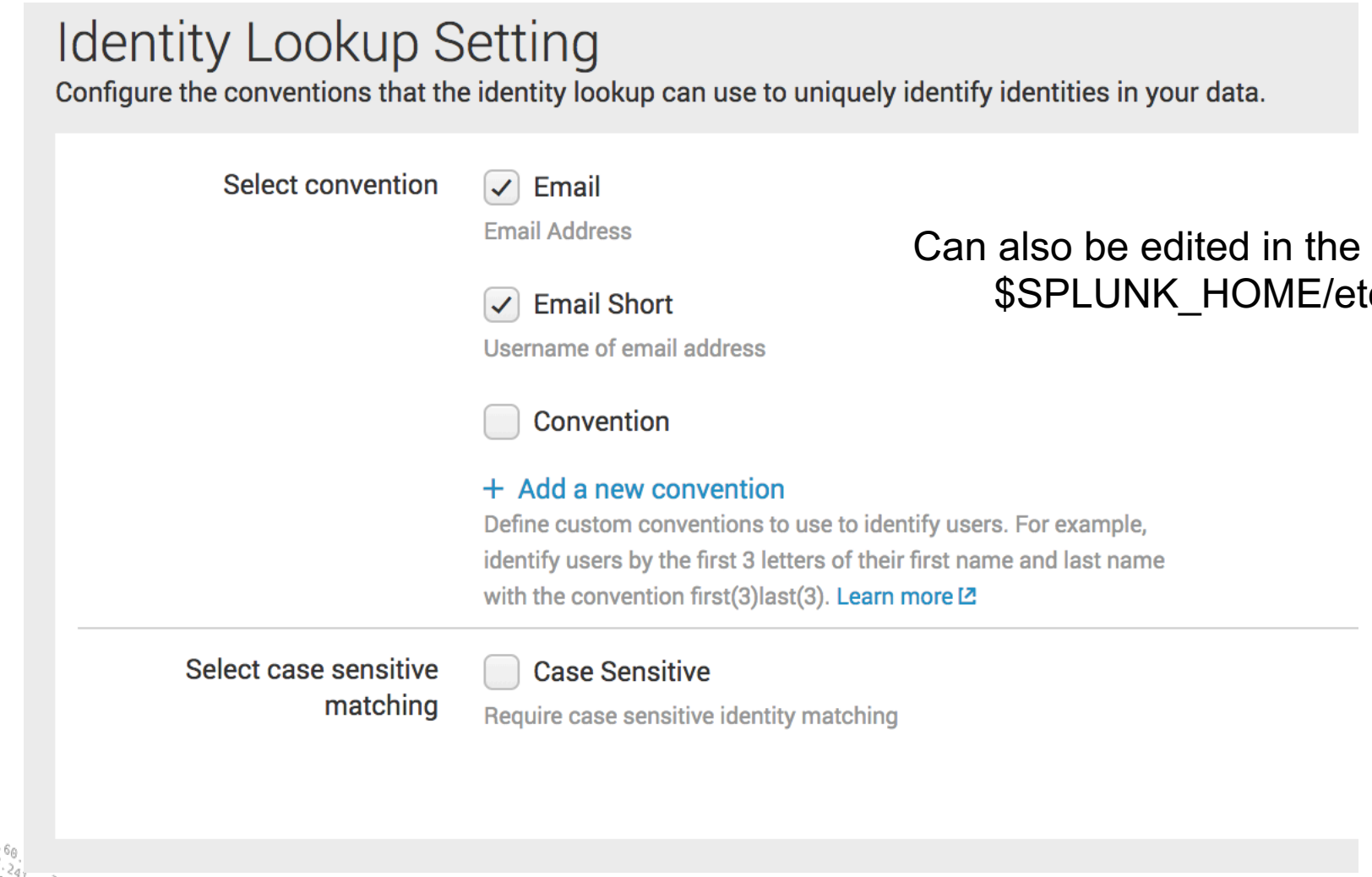
Identity Ingest (1/2)

Requires Some Thought...

- **From Enterprise Security**
  - **Configure > Data Enrichment > Identity Lookup Configuration**.
  - **Email** - email address identifies users
  - **Email short -** username of an email address identifies users
  - **Convention** - custom convention(s) used to identify users
    - Example: First 6 letters of their last name and the first 2 letters of their first name – last(6)first(2)
  - **Case Sensitive** - require case sensitivity for matching



Identity Ingest (2/2)



Can also be edited in the identityLookup.conf
$SPLUNK_HOME/etc/apps/SA-IdentityManagement/default/

```
[identityLookup]
exact = 1
email = 1
email_short = 1
convention = 0
case_sensitive = 0
```

splunk> .conf18

Formatting for Ingest

csv

- Asset Headers

```
ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should
_timesync,should_update,requires_av
```

- Identity Headers

```
identity,prefix,nick,first,last,suffix,email,phone,phone2,managedBy,priority,bunit,category,watchlis
t,startDate,endDate,work_city,work_country,work_lat,work_long
```

- http://docs.splunk.com/Documentation/ES/latest/Admin/Formatassetoridentitylist

The Bare Minimum for Assets

- Address – ip, mac, nt_host, dns
  - At least one
- Priority
  - Used to calculate Urgency in Notable Events
  - Combined with Correlation Search - Severity
- bunit (Business Unit)
  - Common filter in dashboards in ES
- Category
  - Common filter in dashboards in ES
  - Multivalue field, separated with pipes

The Bare Minimum for Identity

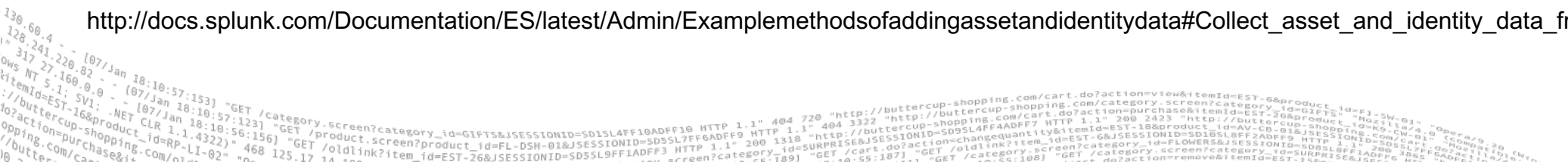
- Identity
  - Multivalue field, separated with pipes
- Priority
  - Used to calculate Urgency in Notable Events
  - Combined with Correlation Search - Severity
- bunit (Business Unit)
  - Common filter in dashboards in ES
- Category
  - Common filter in dashboards in ES
  - Multivalue field, separated with pipes

Using a Saved Search To Prep Your Data

Asset

```
|ldapsearch domain=<domain name> search="(&(objectClass=computer))"
|eval city=""
|eval country=""
|eval priority="medium"
|eval category="normal"
|eval dns=dNSHostName
|eval owner=managedBy
|rex field=sAMAccountName mode=sed "s/\$//g"
|eval nt_host=sAMAccountName
|makemv delim="," dn
|rex field=dn "(OU|CN)\=(?<bunit>.+)"
|table ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should_timesy
nc,should_update,requires_av
| outputlookup create_empty=false createinapp=true my_asset_lookup
```

http://docs.splunk.com/Documentation/ES/latest/Admin/Examplemethodsofaddingassetandidentitydata#Collect_asset_and_identity_data_from_Active_Directory



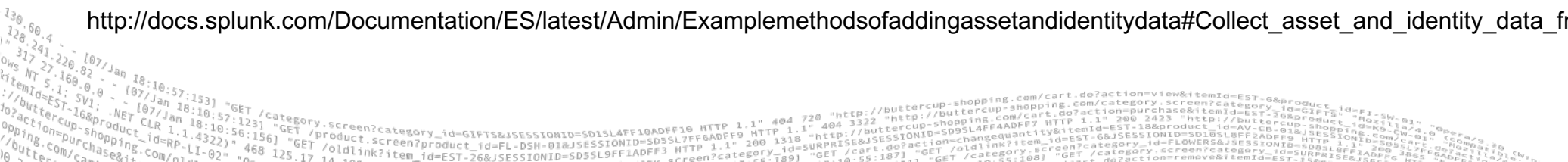
splunk> .conf18

Using a Saved Search To Prep Your Data

Identity

```
|ldapsearch domain=<domain_name> search="(&(objectclass=user)(!(objectClass=computer)))" attrs="userAccountContro
l,sAMAccountName,personalTitle,displayName,givenName,sn,mail,telephoneNumber,mobile,manager,department,whenCreate
d,accountExpires"
|makemv userAccountControl
|search userAccountControl="NORMAL_ACCOUNT"
|eval suffix=""
|eval priority="medium"
|eval category="normal"
|eval watchlist="false"
|eval endDate=""
|table sAMAccountName,personalTitle,displayName,givenName,sn,suffix,mail,telephoneNumber,mobile,manager,priority,d
epartment,category,watchlist,whenCreated,endDate
|rename sAMAccountName as identity, personalTitle as prefix, displayName as nick, givenName as first, sn as last,
mail as email, telephoneNumber as phone, mobile as phone2, manager as managedBy, department as bunit, whenCreated
as startDate
|outputlookup my_identity_lookup
```

http://docs.splunk.com/Documentation/ES/latest/Admin/Examplemethodsofaddingassetandidentitydata#Collect_asset_and_identity_data_from_Active_Directory



splunk> .conf18

Adding a New List

- Enterprise: Settings > Data Inputs > Identity Management
- In ES: Configure > Data Enrichment > Identity Management
- Can have multiple csvs for Asset & Identity

Identity Management

Merges asset and identity information into Splunk lookup tables.

Name	Category	Description	Type	Source	Blacklist	Status	Actions
administrative_identities	administrative_identities	List of commonly-used administrative or privileged identities.	identity	lookup://administrative_identity_lookup	Enabled	Disabled | Enable	Clone
demo_assets	demo_assets	Demonstration asset list.	asset	lookup://demo_asset_lookup	Enabled	Disabled | Enable	Clone
demo_identities	demo_identities	Demonstration identity list.	identity	lookup://demo_identity_lookup	Enabled	Disabled | Enable	Clone
frothly_assets	frothly_assets	All of Frothly's Cloud and On Prem Assets	asset	lookup://frothly_assets	Enabled	Enabled | Disable	Clone | Delete
frothly_ids	frothly_identities	All of the frothly identities	identity	lookup://frothly_ids	Disabled	Enabled | Disable	Clone | Delete
static_assets	static_assets	List containing static assets.	asset	lookup://simple_asset_lookup	Enabled	Enabled | Disable	Clone
static_identities	static_identities	List containing static identities.	identity	lookup://simple_identity_lookup	Enabled	Enabled | Disable	Clone

splunk> .conf18

Pro Tip

Don’t Rely On Configure > Lists and Lookups to Get Your Assets & Identities

46 Objects | Edit selection | Type: Lookup | App: All | Status: All | filter | Clear filters

Name	Type	App	Next Scheduled Time
Action History Search Tracking Whitelist	Lookup	Enterprise Security	
Administrative Identities	Lookup	SA-IdentityManagement	
Application Protocols	Lookup	SA-NetworkProtection	
Assets	Lookup	SA-IdentityManagement	
Cloud Domains	Lookup	Splunk Common Information Model	
Corporate Email Domains	Lookup	Splunk Common Information Model	
Corporate Web Domains	Lookup	Splunk Common Information Model	

Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.

< Back to ES Configuration

5 Objects | Edit selection | Type: Lookup | App: SA-IdentityManagement | Status: All | filter | Clear filters

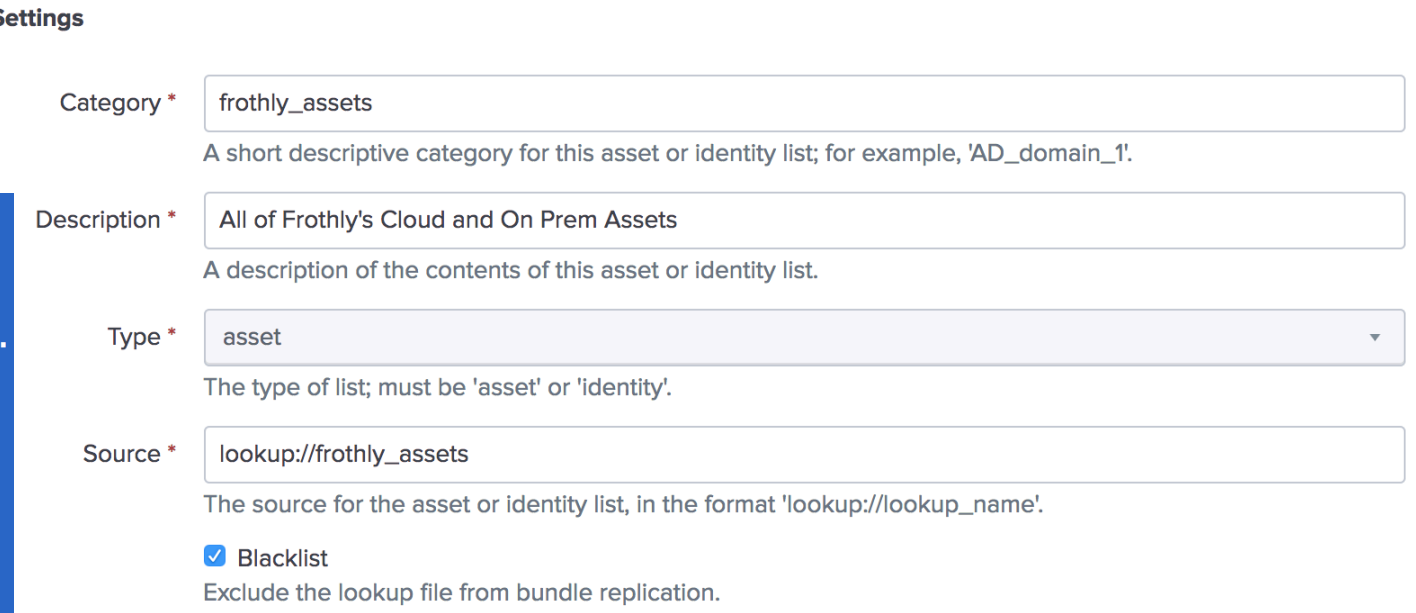
Name	Type	App	Next Scheduled Time
Administrative Identities	Lookup	SA-IdentityManagement	
Assets	Lookup	SA-IdentityManagement	
Demonstration Assets	Lookup	SA-IdentityManagement	
Demonstration Identities	Lookup	SA-IdentityManagement	
Identities	Lookup	SA-IdentityManagement	

splunk> .conf18

Setting A&I Lookups for Ingest

- $SPLUNK_HOME/etc/apps/SA-IdentityManagement/default/inputs.conf
  - Modifications get written to local but you already knew that

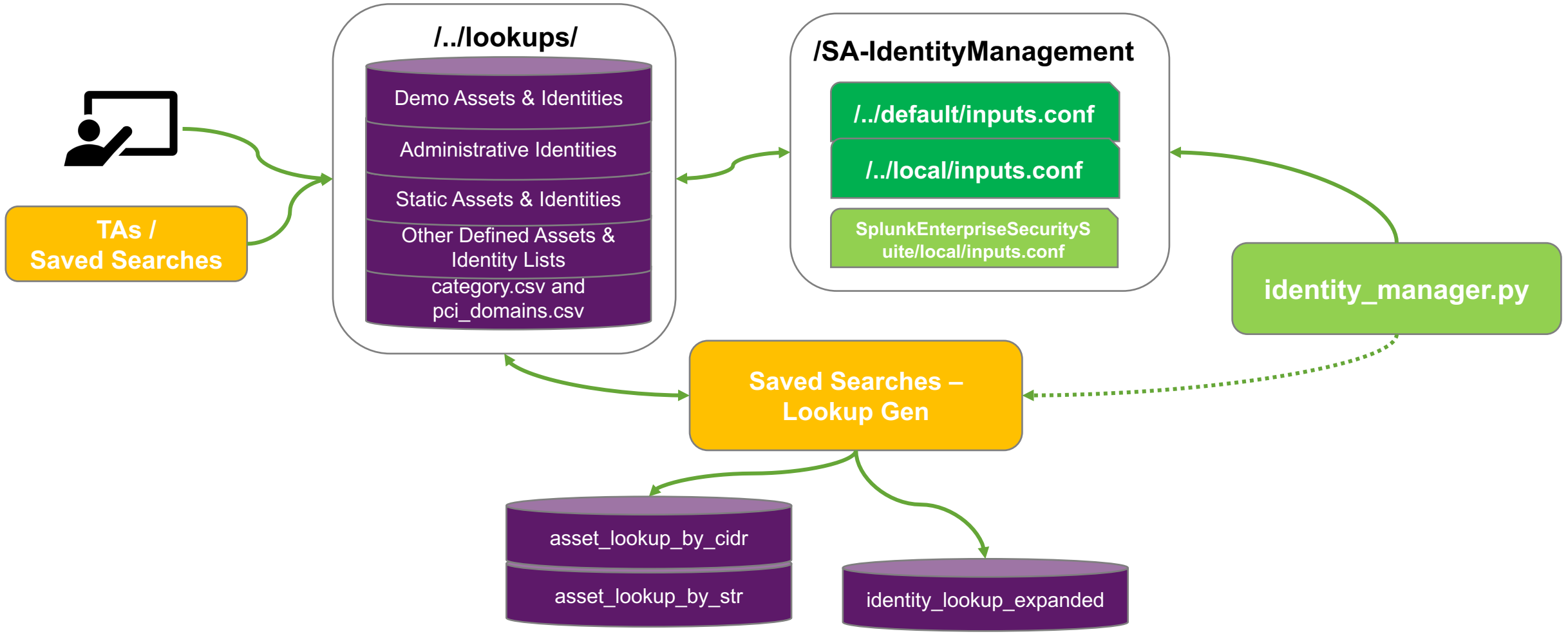
```
# Identity lists

[identity_manager://administrative_identities]
category = administrative_identities
description = List of commonly-used administrative or privileged identities.
disabled = true
target = identity
url = lookup://administrative_identity_lookup

[identity_manager://demo_identities]
category = demo_identities
description = Demonstration identity list.
disabled = true
target = identity
url = lookup://demo_identity_lookup

[identity_manager://static_identities]
category = static_identities
description = List containing static identities.
disabled = true
target = identity
url = lookup://simple_identity_lookup
```



splunk> .conf18

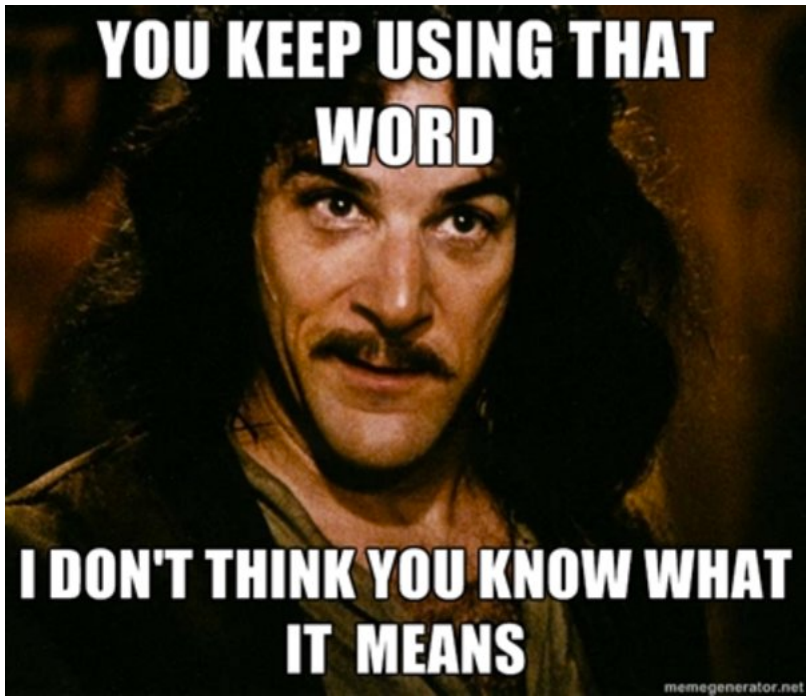
Processing

Asset & Identity Framework - Processing



What Do These Words Mean?

- String-based asset correlation
- CIDR subnet-based asset correlation
- String-based identity correlation



String-based Asset Correlation

Very Straightforward

- Found in lookup asset_lookup_by str

asset_id	asset_tag	bunit	category	city	country	dns	ip	is_expected	key
2ad5b713caa38ffd254d8a67c5d3abdf5937bf13	workstation windows		workstation windows	San Francisco	US	wrk-klagerf.frothly.local	10.0.2.109	false	10.0.2.109 00:0c:29:f5:5e:8e wrk-klagerf wrk-klagerf.frothly.local

lat	long	mac	nt_host	owner	pci_domain	priority	requires_av	should_timesync	should_update
		00:0c:29:f5:5e:8e	wrk-klagerf	Kevin Lagerfield	untrust	low	TRUE	false	TRUE

splunk> .conf18

CIDR Subnet-based Asset Correlation

Very Similar to String Matching

- Found in lookup asset_lookup_by cidr

asset_id	asset_tag	bunit	category	city	country	dns	ip	is_expected	key
d60aae2d1862e96b529840071e60e81ebef33282	workstation		workstation	San Francisco	US		10.0.2.0/24	false	10.0.2.0/24

lat	long	mac	nt_host	owner	pci_domain	priority	requires_av	should_timesync	should_update
					untrust	low	false	false	false

splunk> .conf18

String-based Identity Correlation

- Found in lookup identities_expanded.csv

bunit	category	email	endDate	first	identity	identity_id	identity_tag	key	last
americas		klagerfield@froth.ly		Kevin	FROTHLY\kevin.lagerfield frothly.local\kevin.lagerfield kevin.lagerfield kevin.lagerfield@FROTHLY.LOCAL klager klagerfield klagerfield@froth.ly	90b0149965d02b328f81c3df18c59847e9468884	americas	klagerfield klager kevin.lagerfield FROTHLY\kevin.lagerfield frothly.local\kevin.lagerfield kevin.lagerfield@FROTHLY.LOCAL klagerfield@froth.ly	Lagerfield

managedBy	nick	phone	phone2	prefix	priority	startDate	suffix	watchlist	work_city	work_country	work_lat	work_long
		+1 (800)555-8072	+1 (800)555-2031	Mr.	critical	436174020.000000		false	San Francisco	USA	37.78N	122.41W

splunk> .conf18

How Did We Get There?

- $SPLUNK_HOME/etc/apps/SA-IdentityManagement/bin/identity_manager.py
- Merge process runs every 5 minutes by default
  - | from savedsearch:"Identity - Asset String Matches - Lookup Gen”
  - | from savedsearch:"Identity - Asset CIDR Matches - Lookup Gen”
  - | from savedsearch:"Identity - Identity Matches - Lookup Gen”

Identity - Asset String Matches - Lookup Gen

Very Straightforward

| `asset_sources` | `make_assets_str` | outputlookup output_format=splunk_mv_csv asset_lookup_by_str

`make_assets` | eval `asset_key_field`=mvfilter(**!match**(`asset_key_field`, `ipv4_cidr_regex`)) | where isnotnull(`asset_key_field`)

fillnull value="false" `extra_asset_fields` | `split_mv_asset_fields` | `gen_asset_id(asset_id)` | dedup asset_id | where isnotnull(asset_id) | expandiprange ip | eval `pci_category_meval(category)`, `pci_domain_meval(pci_domain, category)`, `tag_assets_meval` | `generate_asset_key` | fields `asset_key_field`,`asset_fields`

inputlookup append=t **frothly_assets** | inputlookup append=t **simple_asset_lookup**

Identity - Asset CIDR Matches - Lookup Gen

Very Similar to String Matching

| `asset_sources` | `make_assets_cidr` | outputlookup output_format=splunk_mv_csv asset_lookup_by_cidr

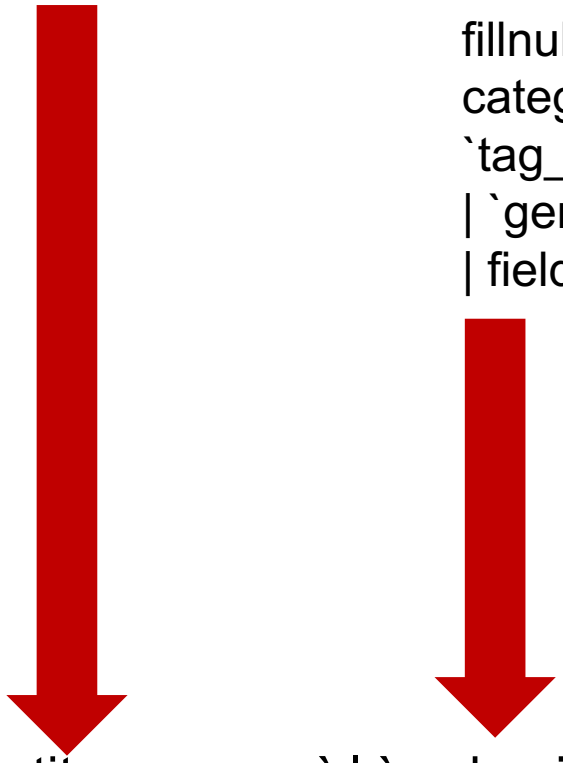
`make_assets` | eval `asset_key_field`=mvfilter(**match**(`asset_key_field`, `ipv4_cidr_regex`)) | where isnotnull(`asset_key_field`)

fillnull value="false" `extra_asset_fields` | `split_mv_asset_fields` | `gen_asset_id(asset_id)` | dedup asset_id | where isnotnull(asset_id) | expandiprange ip | eval `pci_category_meval(category)`, `pci_domain_meval(pci_domain, category)`, `tag_assets_meval` | `generate_asset_key` | fields `asset_key_field`,`asset_fields`

inputlookup append=t **frothly_assets** | inputlookup append=t **simple_asset_lookup**

Identity - Identity Matches - Lookup Gen

inputlookup append=t **frothly_ids** | inputlookup append=t **simple_identity_lookup**



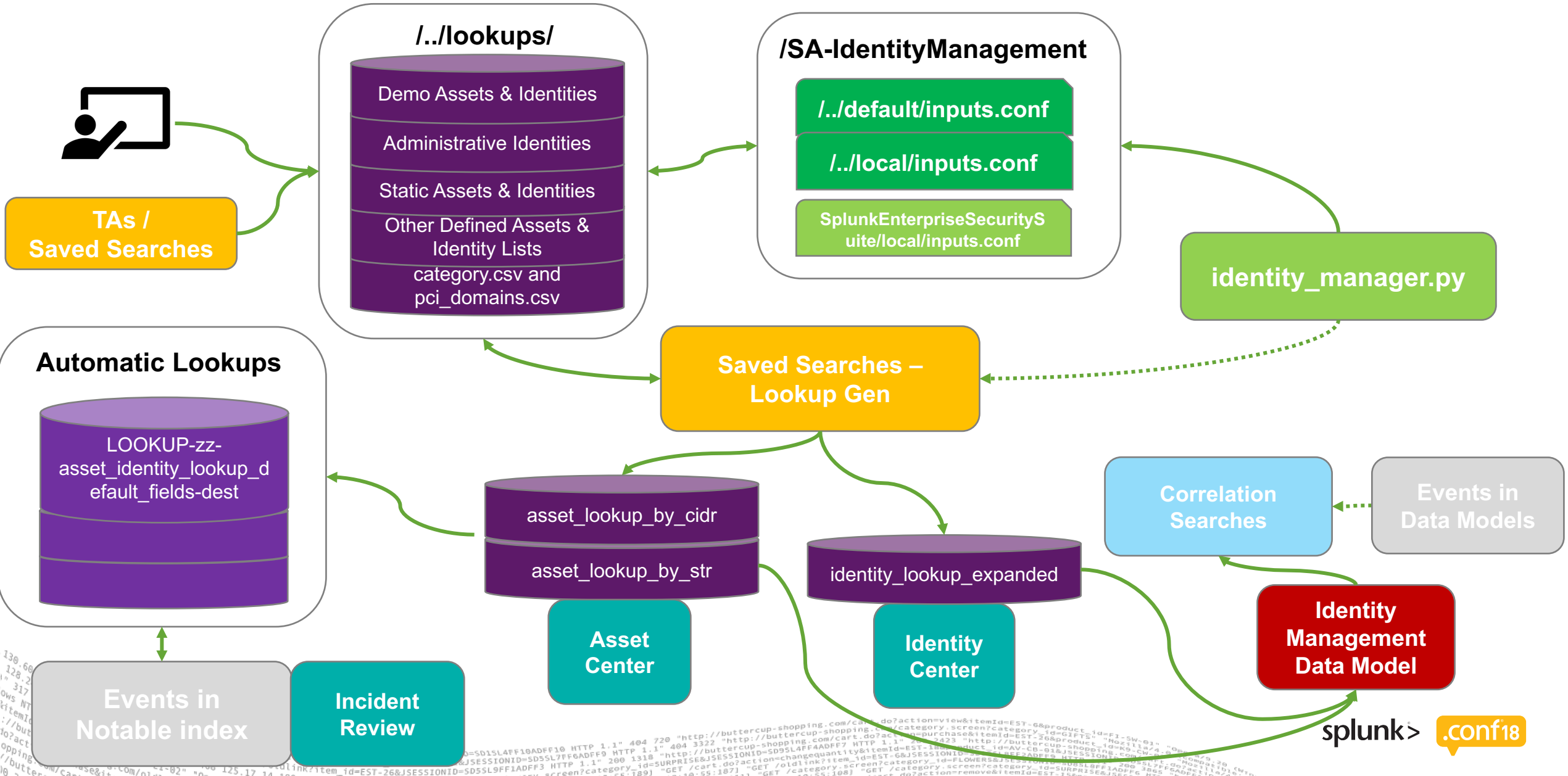
fillnull value="false" watchlist | `str_to_bool(watchlist)` | eval category=split(category, "|"), `pci_category_meval(category)`, `tag_identities_meval` | `gen_identity_id(identity_id)` | where isnotnull(identity_id) | `generate_identities` | eval identity=mvdedup(identity) | `generate_identity_key` | fields `identity_key_field`,`identity_fields`

| `identity_sources` | `make_identities` | eval `iden_mktime_meval(startDate)`,`iden_mktime_meval(endDate)`,identity=mvsort(identity) | sort 0 +identity | outputlookup output_format=splunk_mv_csv identity_lookup_expanded

splunk> .conf18

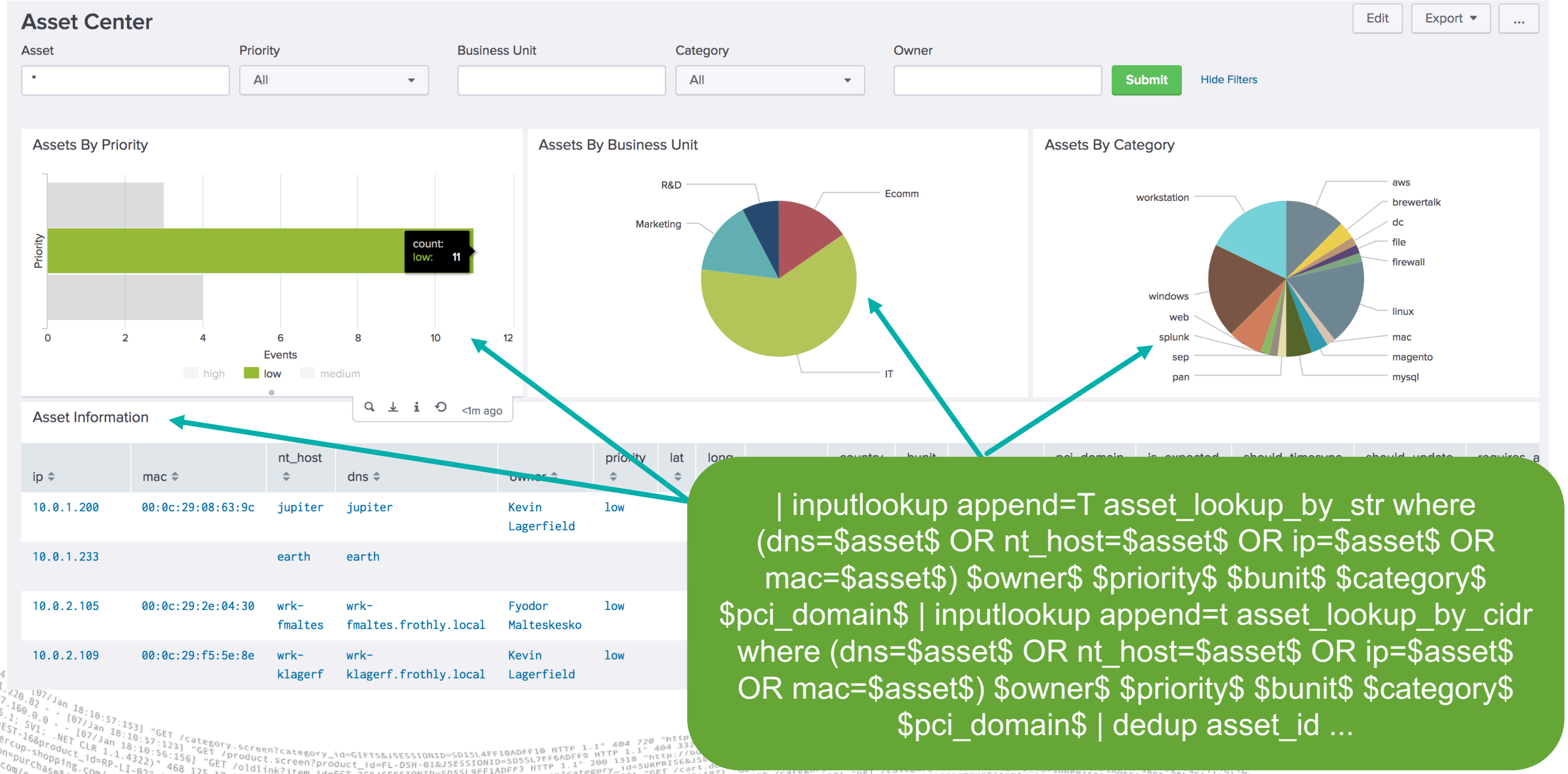
Consuming

Asset & Identity Framework - Consuming



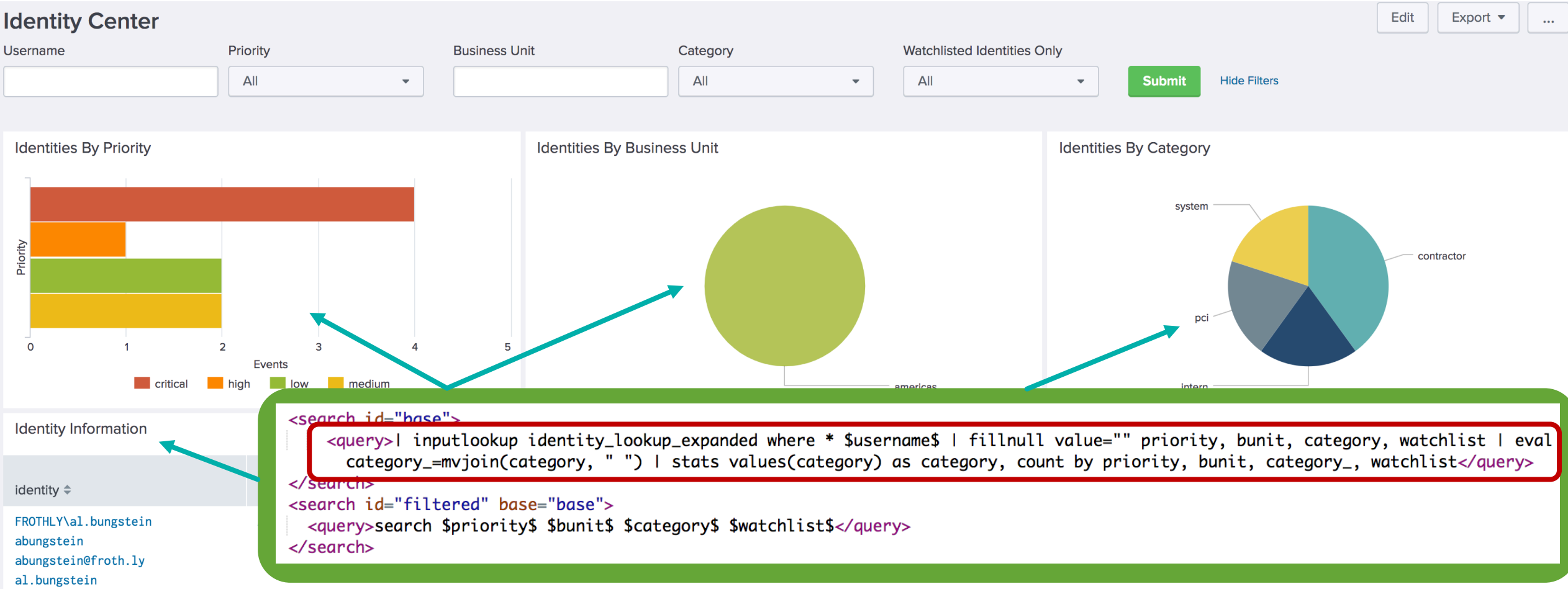
splunk> .conf18

Asset Center




```
| inputlookup append=T asset_lookup_by_str where (dns=$asset$ OR nt_host=$asset$ OR ip=$asset$ OR mac=$asset$) $owner$ $priority$ $bunit$ $category$ $pci_domain$ | inputlookup append=t asset_lookup_by_cidr where (dns=$asset$ OR nt_host=$asset$ OR ip=$asset$ OR mac=$asset$) $owner$ $priority$ $bunit$ $category$ $pci_domain$ | dedup asset_id ...
```

Identity Center




```
<search id="base">
  <query>| inputlookup identity_lookup_expanded where * $username$ | fillnull value="" priority, bunit, category, watchlist | eval
    category_=mvjoin(category, " ") | stats values(category) as category, count by priority, bunit, category_, watchlist</query>
</search>
<search id="filtered" base="base">
  <query>search $priority$ $bunit$ $category$ $watchlist$</query>
</search>
```

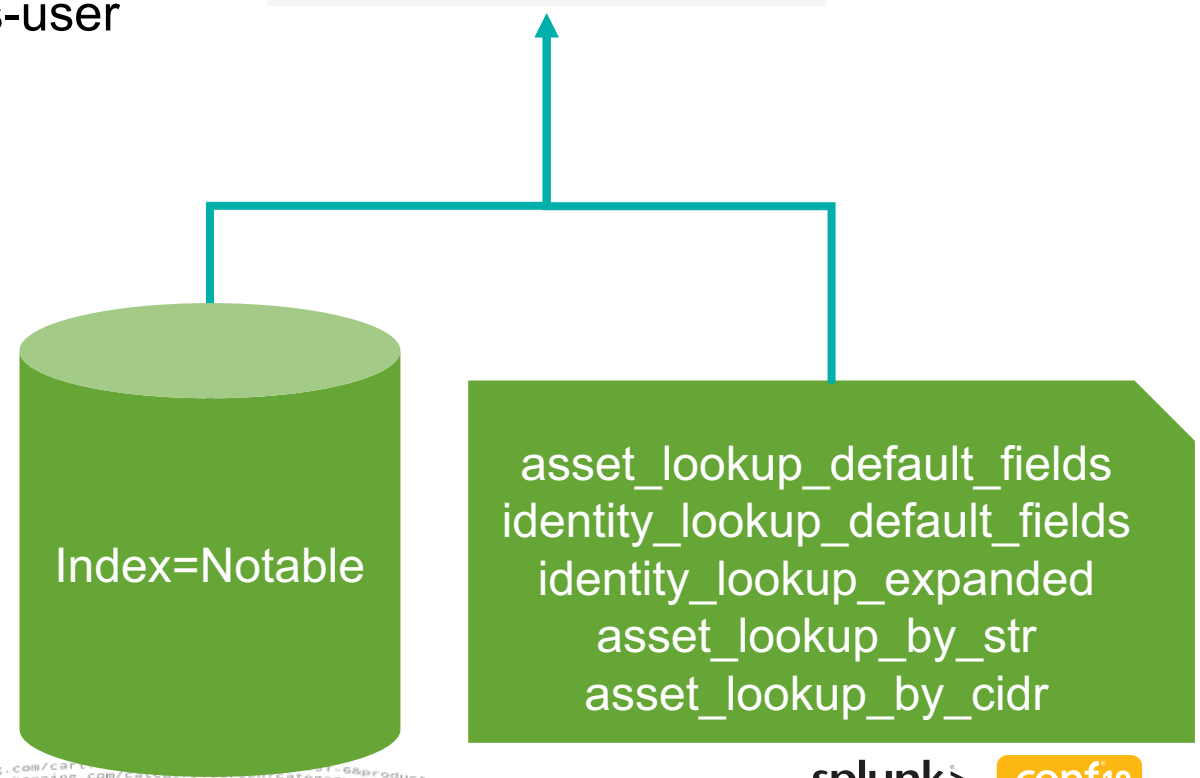
splunk> .conf18

Merging of Data

Automatic Lookups

- Default field correlation
  - LOOKUP-zz-asset_identity_lookup_default_fields-dest
    LOOKUP-zz-asset_identity_lookup_default_fields-dvc
    LOOKUP-zz-asset_identity_lookup_default_fields-src
    LOOKUP-zz-asset_identity_lookup_default_fields-src_user
    LOOKUP-zz-asset_identity_lookup_default_fields-user
- String-based asset correlation
  - LOOKUP-zu-asset_lookup_by_str-dest
    LOOKUP-zu-asset_lookup_by_str-dvc
    LOOKUP-zu-asset_lookup_by_str-src
- CIDR subnet-based asset correlation
  - LOOKUP-zv-asset_lookup_by_cidr-dest
    LOOKUP-zv-asset_lookup_by_cidr-dvc
    LOOKUP-zv-asset_lookup_by_cidr-src
- String-based identity correlation
  - LOOKUP-zy-identity_lookup_expanded-src_user
    LOOKUP-zy-identity_lookup_expanded-user

Source	10.0.2.109
Source Category	workstation windows
Source City	San Francisco
Source Country	US
Source DNS	wrk-klagerf.frothly.local
Source IP Address	10.0.2.109
Source Expected	false
Source MAC Address	00:0c:29:f5:5e:8e
Source NT Hostname	wrk-klagerf
Source Owner	Kevin Lagerfield
Source PCI Domain	untrust
Source Requires Antivirus	TRUE
Source Should Time Synchronize	false
Source Should Update	TRUE



splunk> .conf18

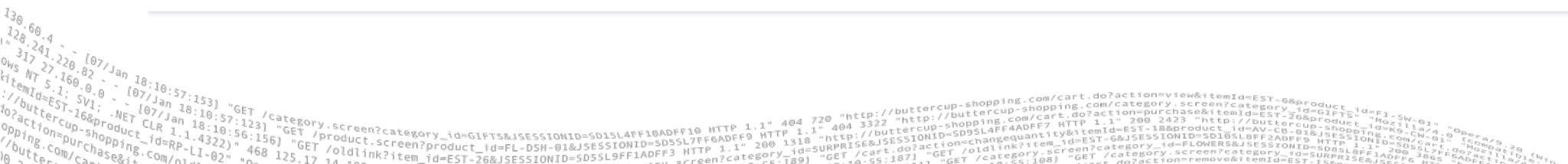
Default Field Correlation

- asset_lookup_default_fields.csv

is_expected	key	pci_domain	requires_av	should_timesync	should_update
false	*	untrust	false	false	false

- identity_lookup_default_fields.csv

key	watchlist
*	false



splunk> .conf18

Default Field Correlation

Automatic Lookup

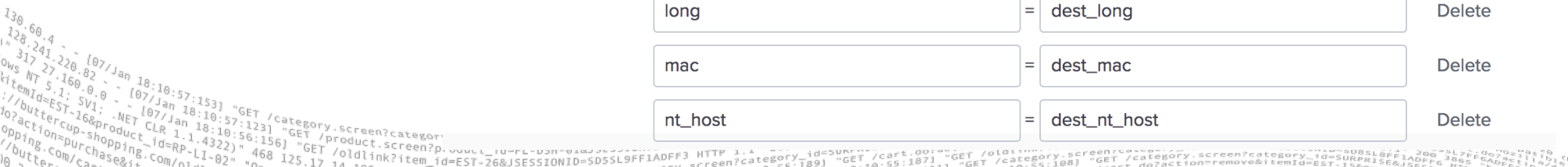
Lookup table *	asset_lookup_default_fields			
Lookup input fields	key	=	dest	Delete
		=		Delete
	+ Add another field			
Lookup output fields	is_expected	=	dest_is_expected	Delete
	pci_domain	=	dest_pci_domain	Delete
	requires_av	=	dest_requires_av	Delete
	should_timesync	=	dest_should_timesync	Delete
	should_update	=	dest_should_update	Delete

splunk> .conf18

Asset Automatic Lookup

LOOKUP-zv-asset_lookup_by_cidr-dest

Lookup table *	asset_lookup_by_cidr		
Lookup input fields	key	= dest	Delete
		=	Delete
	+ Add another field		
Lookup output fields	asset_id	= dest_asset_id	Delete
	asset_tag	= dest_asset_tag	Delete
	bunit	= dest_bunit	Delete
	category	= dest_category	Delete
	city	= dest_city	Delete
	country	= dest_country	Delete
	dns	= dest_dns	Delete
	is_expected	= dest_is_expected	Delete
	lat	= dest_lat	Delete
	long	= dest_long	Delete
	mac	= dest_mac	Delete
	nt_host	= dest_nt_host	Delete



splunk> .conf18

Identity Automatic Lookup

LOOKUP-zy-identity_lookup_expanded-src_user

Lookup table *	identity_lookup_expanded			
Lookup input fields	key	=	src_user	Delete
		=		Delete
	+ Add another field			
Lookup output fields	bunit	=	src_user_bunit	Delete
	category	=	src_user_category	Delete
	email	=	src_user_email	Delete
	endDate	=	src_user_endDate	Delete
	first	=	src_user_first	Delete
	identity	=	src_user_identity	Delete
	identity_tag	=	src_user_identity_tag	Delete
	last	=	src_user_last	Delete
	managedBy	=	src_user_managedBy	Delete
	nick	=	src_user_nick	Delete
	phone	=	src_user_phone	Delete

splunk> .conf18

Automatic Lookup with a Search

Focusing on src assets...

```
index=notable | table src_asset_tag src_bunit src_category src_city src_country src_dns src_ip src_is_expected src_mac src_nt_host src_owner src_pci_domain src_priority
```

All time

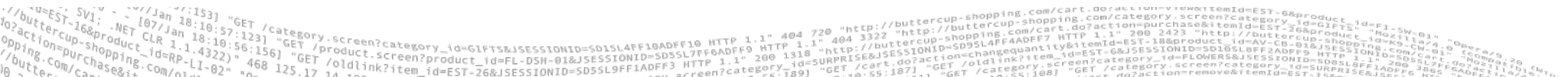
✓ 61 events (12/23/16 10:01:04.000 AM to 8/27/18 11:42:49.000 AM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (61)** Visualization

100 Per Page Format Preview

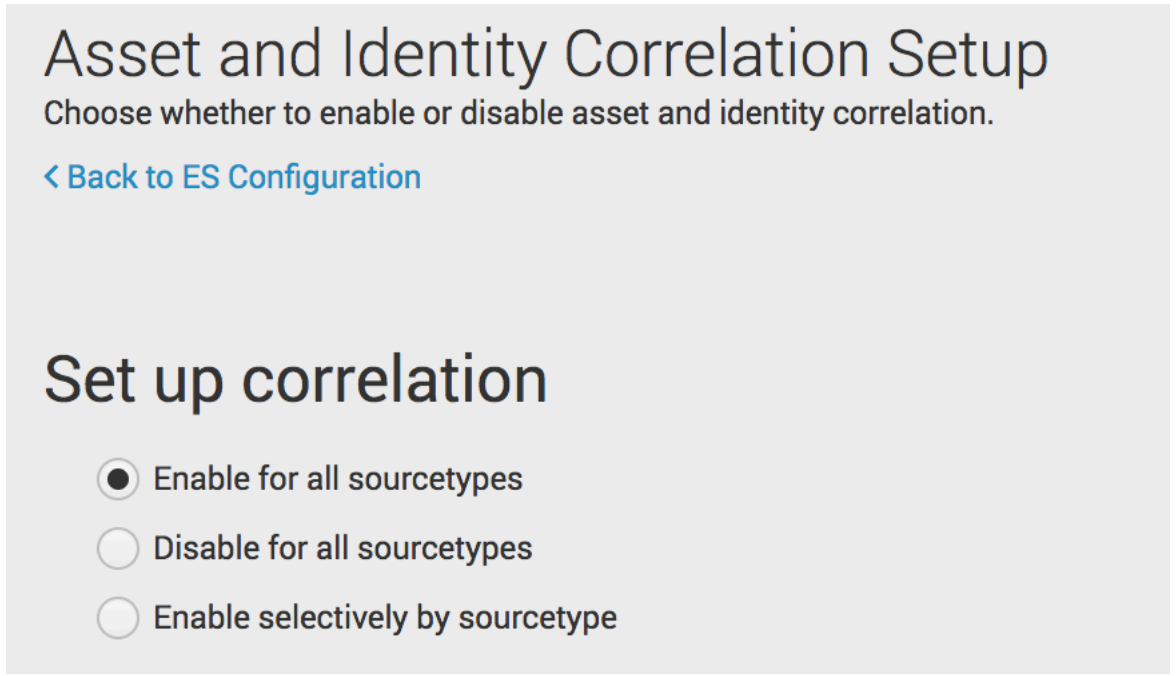
src_asset_tag	src_bunit	src_category	src_city	src_country	src_dns	src_ip	src_is_expected	src_mac	src_nt_host	src_owner	src_pci_domain	src_priority
workstation mac Marketing	Marketing	workstation mac	San Francisco	US	maclory-air13	10.0.4.4	false	02:50:41:00:01:01	maclory-air13	Mallory Kraeusen	untrust	low
workstation mac Marketing	Marketing	workstation mac	San Francisco	US	maclory-air13	10.0.4.4	false	02:50:41:00:01:01	maclory-air13	Mallory Kraeusen	untrust	low
workstation mac Marketing	Marketing	workstation mac	San Francisco	US	maclory-air13	10.0.4.4	false	02:50:41:00:01:01	maclory-air13	Mallory Kraeusen	untrust	low
workstation windows		workstation windows	San Francisco	US	wrk-ghoppy.frothly.local	10.0.2.103	false	00:0c:29:19:b6:74	wrk-ghoppy	Grace Hoppy	untrust	low
workstation windows		workstation windows	San Francisco	US	wrk-ghoppy.frothly.local	10.0.2.103	false	00:0c:29:19:b6:74	wrk-ghoppy	Grace Hoppy	untrust	low
workstation windows		workstation windows	San Francisco	US	wrk-btun.frothly.local	10.0.2.107	false	00:0c:29:6f:d0:2f	wrk-btun	Billy Tun	untrust	low
workstation windows		workstation windows	San Francisco	US	wrk-klagerf.frothly.local	10.0.2.109	false	00:0c:29:f5:5e:8e	wrk-klagerf	Kevin Lagerfield	untrust	low

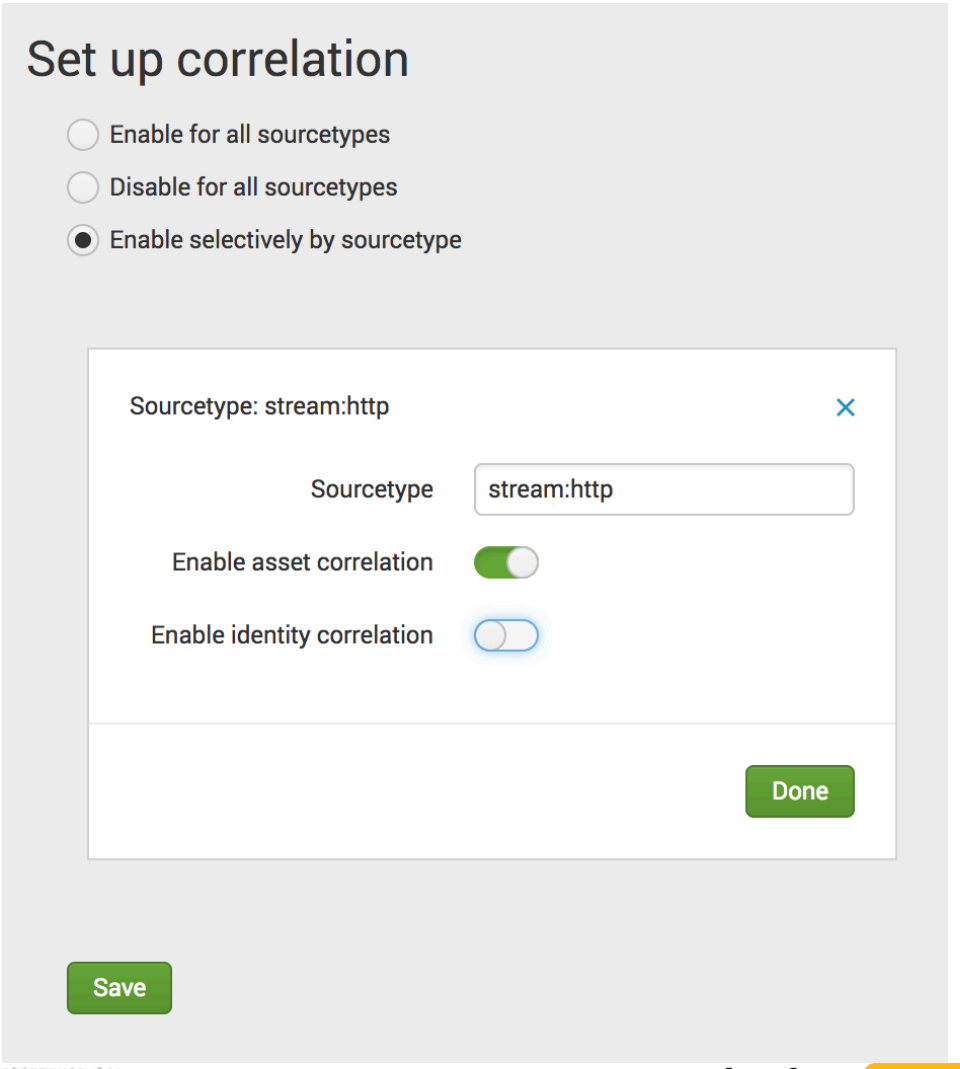


splunk> .conf18

What Else Could I Do?

Limit Correlation to Specific sourcetype





splunk> .conf18

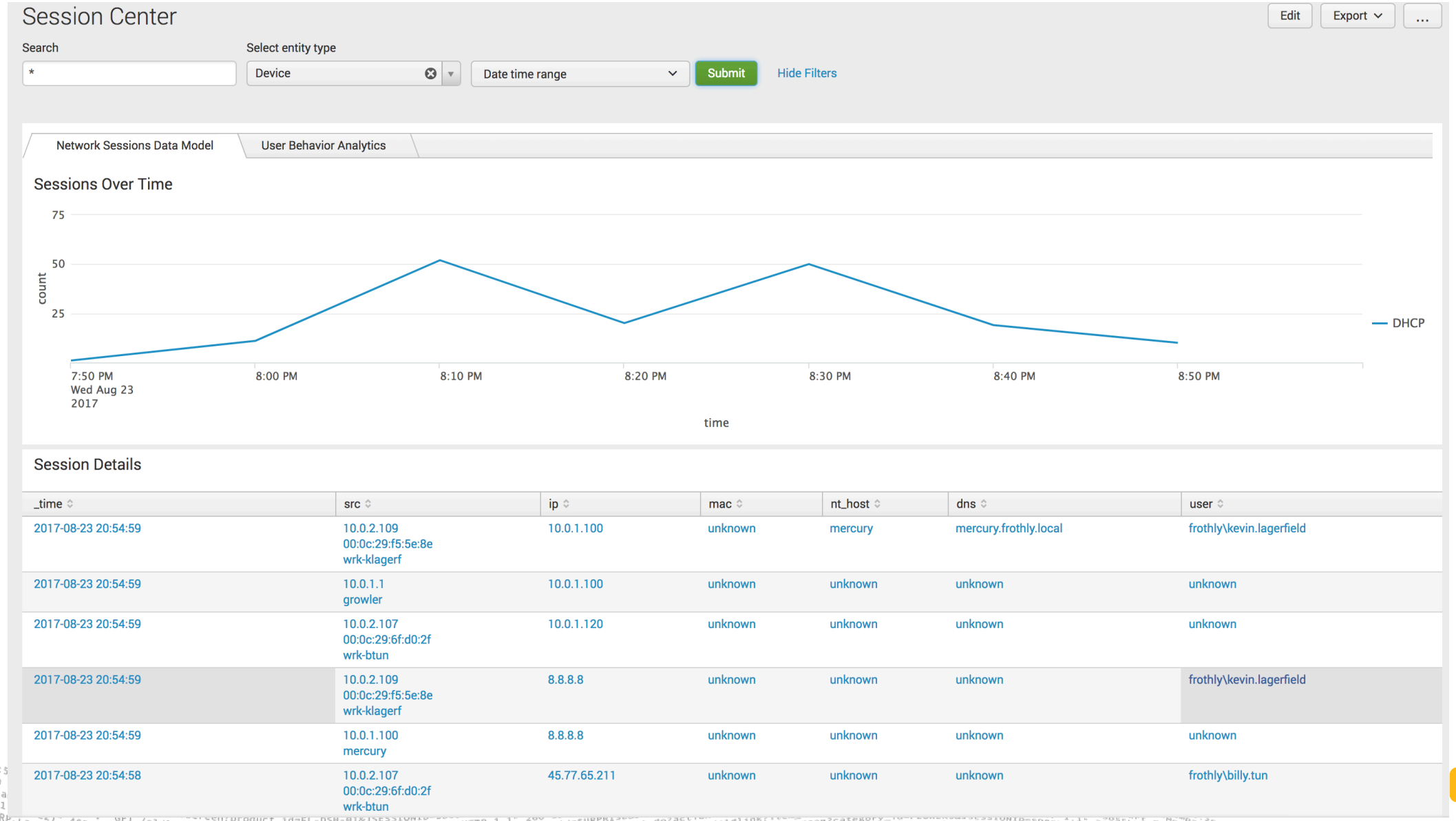
Additional Knowledge Objects Leveraging A&I

Not Exhaustive...

- Data Model
  - Assets & Identities
- Correlation Searches
  - Activity from Expired User Identity*
  - Asset Ownership Unspecified*
  - High Volume Email Activity to Non-corporate Domains by User
  - Web Uploads to Non-corporate Sites by Users
- Search Driven Lookups
  - Asset/Identity Categories
  - PCI Domain Lookup
- Saved Searches
  - Identity - Email Activity to Non-corporate Domains by Users Per 1d - Context Gen
  - Identity - Web Uploads to Non-corporate Domains by Users Per 1d - Context Gen
- KSIs
  - High Risk Users
  - Noncorporate Email Activity
- Swimlanes
  - Asset Investigator
  - Identity Investigator
    - Identity - Tickets by User - Swimlane

splunk> .conf18

Session Center



If I Can Find A UBA Sample to Show for That Tab Show It Here

splunk> .conf18

Troubleshooting

All Is Well

```
index=_internal sourcetype="identity_correlation:modular_input"
```

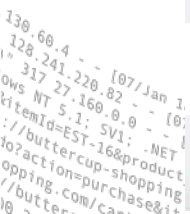
>	8/27/18 12:49:19.151 PM	2018-08-27 19:49:19,151+0000 INFO pid=12787 tid=MainThread file=identity_manager.py:run_threads:387 | status="no action required" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:49:18.181 PM	2018-08-27 19:49:18,181+0000 INFO pid=12787 tid=MainThread file=identity_manager.py:run_threads:314 | last run: 1535399058.02 (2018-08-27 19:44:18+0000) host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:49:18.011 PM	2018-08-27 19:49:18,011+0000 INFO pid=12787 tid=MainThread file=identity_manager.py:<module>:404 | status="Executing modular input" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:44:19.076 PM	2018-08-27 19:44:19,076+0000 INFO pid=3520 tid=MainThread file=identity_manager.py:run_threads:387 | status="no action required" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:44:18.185 PM	2018-08-27 19:44:18,185+0000 INFO pid=3520 tid=MainThread file=identity_manager.py:run_threads:314 | last run: 1535398758.03 (2018-08-27 19:39:18+0000) host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:44:18.014 PM	2018-08-27 19:44:18,014+0000 INFO pid=3520 tid=MainThread file=identity_manager.py:<module>:404 | status="Executing modular input" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:39:19.209 PM	2018-08-27 19:39:19,209+0000 INFO pid=26044 tid=MainThread file=identity_manager.py:run_threads:387 | status="no action required" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input

splunk> .conf18

Change an Asset Value (1/2)

Criticality of a Server

>	8/27/18 12:59:21.983 PM	2018-08-27 19:59:21,983+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:285 | status="saved search completed" search="Identity - Asset String Matches - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD5ddd8f0d71f1f93e2_at_1535399959_2819" state="DONE" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:20.925 PM	2018-08-27 19:59:20,925+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:271 | status="monitoring for saved search completion" timeout="30" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:20.925 PM	2018-08-27 19:59:20,925+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:373 | status="dispatched primary saved search" target="asset" search="Identity - Asset CIDR Matches - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD527d75a5ca50fe8fc_at_1535399960_2820 host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:20.344 PM	2018-08-27 19:59:20,344+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:370 | status="dispatching primary saved search" target="asset" search="Identity - Asset CIDR Matches - Lookup Gen" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:20.344 PM	2018-08-27 19:59:20,344+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:373 | status="dispatched primary saved search" target="asset" search="Identity - Asset String Matches - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD5ddd8f0d71f1f93e2_at_1535399959_2819 host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:19.469 PM	2018-08-27 19:59:19,469+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:370 | status="dispatching primary saved search" target="asset" search="Identity - Asset String Matches - Lookup Gen" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:19.469 PM	2018-08-27 19:59:19,469+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:366 | status="running primary saved searches" targets="set([u'asset']) host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:18.190 PM	2018-08-27 19:59:18,190+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:314 | last run: 1535399658.08 (2018-08-27 19:54:18+0000) host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:59:18.021 PM	2018-08-27 19:59:18,021+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:<module>:404 | status="Executing modular input" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:54:19.226 PM	2018-08-27 19:54:19,226+0000 INFO pid=22580 tid=MainThread file=identity_manager.py:run_threads:387 | status="no action required" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
>	8/27/18 12:54:18.262 PM	2018-08-27 19:54:18,262+0000 INFO pid=22580 tid=MainThread file=identity_manager.py:run_threads:314 | last run: 1535399358.02 (2018-08-27 19:49:18+0000) host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input



Change an Asset Value (2/2)

Criticality of a Server

8/27/18 12:59:22.961 PM	2018-08-27 19:59:22,961+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:285 | status="saved search completed" search="Identity - Make PCI Domains - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD589fedf987e06eb10_at_1535399962_2822" state="DONE" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:22.961 PM	2018-08-27 19:59:22,961+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:285 | status="saved search completed" search="Identity - Make Categories - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD5baf75cf640726cb2_at_1535399961_2821" state="DONE" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:22.944 PM	2018-08-27 19:59:22,944+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:271 | status="monitoring for saved search completion" timeout="30" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:22.944 PM	2018-08-27 19:59:22,944+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:383 | status="dispatched ancillary saved search" search="Identity - Make PCI Domains - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD589fedf987e06eb10_at_1535399962_2822 host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:22.469 PM	2018-08-27 19:59:22,469+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:381 | status="dispatching ancillary saved search" search="Identity - Make PCI Domains - Lookup Gen" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:22.469 PM	2018-08-27 19:59:22,469+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:383 | status="dispatched ancillary saved search" search="Identity - Make Categories - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD5baf75cf640726cb2_at_1535399961_2821 host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:21.984 PM	2018-08-27 19:59:21,984+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:381 | status="dispatching ancillary saved search" search="Identity - Make Categories - Lookup Gen" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:21.984 PM	2018-08-27 19:59:21,984+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:run_threads:379 | status="running ancillary saved searches" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input
8/27/18 12:59:21.984 PM	2018-08-27 19:59:21,984+0000 INFO pid=32585 tid=MainThread file=identity_manager.py:monitor:285 | status="saved search completed" search="Identity - Asset CIDR Matches - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_U0EtSWRlbnRpdHlNYW5hZ2VtZW50__RMD527d75a5ca50fe8fc_at_1535399960_2820" state="DONE" host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/identity_manager.log | sourcetype = identity_correlation:modular_input

When I Don't Have A Lookup To Go With My Identity Management List

Name	Category	Description	Type	Source	Blacklist	Status	Actions
administrative_identities	administrative_identities	List of commonly-used administrative or privileged identities.	identity	lookup://administrative_identity_lookup	Enabled	Disabled | Enable	Clone
demo_assets	demo_assets	Demonstration asset list.	asset	lookup://demo_asset_lookup	Enabled	Disabled | Enable	Clone
demo_identities	demo_identities	Demonstration identity list.	identity	lookup://demo_identity_lookup	Enabled	Disabled | Enable	Clone
frothly_assets	frothly_assets	All of Frothly's Cloud and On Prem Assets	asset	lookup://frothly_assets	Enabled	Enabled | Disable	Clone | Delete
frothly_ids	frothly_identities	All of the frothly identities	identity	lookup://frothly_ids	Disabled	Enabled | Disable	Clone | Delete
my_empty_list	my_empty_list	Does this create a shell csv or is it just a placeholder?	asset	lookup://my_empty_list	Enabled	Enabled | Disable	Clone | Delete
static_assets	static_assets	List containing static assets.	asset	lookup://simple_asset_lookup	Enabled	Enabled | Disable	Clone
static_identities	static_identities	List containing static identities.	identity	lookup://simple_identity_lookup	Enabled	Enabled | Disable	Clone

9/4/18 6:24:52.733 AM
2018-09-04 13:24:52,733+0000 ERROR pid=29560 tid=MainThread file=lookup_modinput.py:collect_files:114 | status="Lookup table file error" err="unknown path or update time" name=my_empty_list category=asset
host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/python_modular_input.log | sourcetype = python_modular_input

9/4/18 6:19:52.381 AM
2018-09-04 13:19:52,381+0000 ERROR pid=19730 tid=MainThread file=lookup_modinput.py:collect_files:114 | status="Lookup table file error" err="unknown path or update time" name=my_empty_list category=asset
host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/python_modular_input.log | sourcetype = python_modular_input

9/4/18 6:14:53.235 AM
2018-09-04 13:14:53,235+0000 ERROR pid=8864 tid=MainThread file=lookup_modinput.py:collect_files:114 | status="Lookup table file error" err="unknown path or update time" name=my_empty_list category=asset
host = OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com | source = /four/splunk/var/log/splunk/python_modular_input.log | sourcetype = python_modular_input

splunk> .conf18

What's Really Happening

Asset

```
index=_internal sourcetype="identity_correlation:modular_input"  | table _time file status search
```

Date time range

✓ 18 events (8/27/18 12:58:42.000 PM to 8/27/18 1:01:42.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (18)** Visualization

100 Per Page Format Preview

_time	file	status	search
2018-08-27 12:59:22.961	identity_manager.py:monitor:285	saved search completed	Identity - Make PCI Domains - Lookup Gen
2018-08-27 12:59:22.961	identity_manager.py:monitor:285	saved search completed	Identity - Make Categories - Lookup Gen
2018-08-27 12:59:22.944	identity_manager.py:monitor:271	monitoring for saved search completion	
2018-08-27 12:59:22.944	identity_manager.py:run_threads:383	dispatched ancillary saved search	Identity - Make PCI Domains - Lookup Gen
2018-08-27 12:59:22.469	identity_manager.py:run_threads:381	dispatching ancillary saved search	Identity - Make PCI Domains - Lookup Gen
2018-08-27 12:59:22.469	identity_manager.py:run_threads:383	dispatched ancillary saved search	Identity - Make Categories - Lookup Gen
2018-08-27 12:59:21.984	identity_manager.py:run_threads:381	dispatching ancillary saved search	Identity - Make Categories - Lookup Gen
2018-08-27 12:59:21.984	identity_manager.py:run_threads:379	running ancillary saved searches	
2018-08-27 12:59:21.984	identity_manager.py:monitor:285	saved search completed	Identity - Asset CIDR Matches - Lookup Gen
2018-08-27 12:59:21.983	identity_manager.py:monitor:285	saved search completed	Identity - Asset String Matches - Lookup Gen
2018-08-27 12:59:20.925	identity_manager.py:monitor:271	monitoring for saved search completion	
2018-08-27 12:59:20.925	identity_manager.py:run_threads:373	dispatched primary saved search	Identity - Asset CIDR Matches - Lookup Gen
2018-08-27 12:59:20.344	identity_manager.py:run_threads:370	dispatching primary saved search	Identity - Asset CIDR Matches - Lookup Gen
2018-08-27 12:59:20.344	identity_manager.py:run_threads:373	dispatched primary saved search	Identity - Asset String Matches - Lookup Gen
2018-08-27 12:59:19.469	identity_manager.py:run_threads:370	dispatching primary saved search	Identity - Asset String Matches - Lookup Gen
2018-08-27 12:59:19.469	identity_manager.py:run_threads:366	running primary saved searches	
2018-08-27 12:59:18.190	identity_manager.py:run_threads:314		
2018-08-27 12:59:18.021	identity_manager.py:<module>:404	Executing modular input	

Identity Change

```
index=_internal sourcetype="identity_correlation:modular_input"  | table _time file status search
```

2018-08-27 13:39:21.960	identity_manager.py:monitor:285	saved search completed	Identity - Make PCI Domains - Lookup Gen
2018-08-27 13:39:21.960	identity_manager.py:monitor:285	saved search completed	Identity - Make Categories - Lookup Gen
2018-08-27 13:39:21.960	identity_manager.py:monitor:271	monitoring for saved search completion	
2018-08-27 13:39:21.960	identity_manager.py:run_threads:383	dispatched ancillary saved search	Identity - Make PCI Domains - Lookup Gen
2018-08-27 13:39:21.425	identity_manager.py:run_threads:381	dispatching ancillary saved search	Identity - Make PCI Domains - Lookup Gen
2018-08-27 13:39:21.425	identity_manager.py:run_threads:383	dispatched ancillary saved search	Identity - Make Categories - Lookup Gen
2018-08-27 13:39:20.826	identity_manager.py:run_threads:381	dispatching ancillary saved search	Identity - Make Categories - Lookup Gen
2018-08-27 13:39:20.826	identity_manager.py:run_threads:379	running ancillary saved searches	
2018-08-27 13:39:20.825	identity_manager.py:monitor:285	saved search completed	Identity - Identity Matches - Lookup Gen
2018-08-27 13:39:20.795	identity_manager.py:monitor:271	monitoring for saved search completion	
2018-08-27 13:39:20.795	identity_manager.py:run_threads:373	dispatched primary saved search	Identity - Identity Matches - Lookup Gen
2018-08-27 13:39:20.194	identity_manager.py:run_threads:370	dispatching primary saved search	Identity - Identity Matches - Lookup Gen
2018-08-27 13:39:20.193	identity_manager.py:run_threads:366	running primary saved searches	
2018-08-27 13:39:18.259	identity_manager.py:run_threads:314		
2018-08-27 13:39:18.076	identity_manager.py:<module>:404	Executing modular input	

What's Really Happening

Identity - Make PCI Domains - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Make PCI Domains - Lookup Gen

Identity - Make PCI Domains - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Asset CIDR Matches - Lookup Gen

Identity - Asset String Matches - Lookup Gen

Identity - Asset CIDR Matches - Lookup Gen

Identity - Asset CIDR Matches - Lookup Gen

Identity - Asset String Matches - Lookup Gen

Identity - Asset String Matches - Lookup Gen

Identity - Make PCI Domains - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Make PCI Domains - Lookup Gen

Identity - Make PCI Domains - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Make Categories - Lookup Gen

Identity - Identity Matches - Lookup Gen

Identity - Identity Matches - Lookup Gen

Identity - Identity Matches - Lookup Gen

Adding A New Field to the Asset & Identity Framework

splunk> .conf18

Initial Setup

- Cloned csv structure for assets
- Added a column called classification
- Added a new asset with value of TOPSECRET in classification field
- Added csv to Data Inputs > Identity Management
  - Insert of Asset worked as expected but no Classification column in Asset Center

Name	Category	Description	Type	Source	Blacklist	Status	Actions
administrative_identities	administrative_identities	List of commonly-used administrative or privileged identities.	identity	lookup://administrative_identity_lookup	Enabled	Disabled | Enable	Clone
demo_assets	demo_assets	Demonstration asset list.	asset	lookup://demo_asset_lookup	Enabled	Disabled | Enable	Clone
demo_identities	demo_identities	Demonstration identity list.	identity	lookup://demo_identity_lookup	Enabled	Disabled | Enable	Clone
frothly_assets	frothly_assets	All of Frothly's Cloud and On Prem Assets	asset	lookup://frothly_assets	Enabled	Enabled | Disable	Clone | Delete
frothly_ids	frothly_identities	All of the frothly identities	identity	lookup://frothly_ids	Disabled	Enabled | Disable	Clone | Delete
one_more_assets	asset_2	My new asset with an additional column	asset	lookup://one_more_assets	Enabled	Enabled | Disable	Clone | Delete
static_assets	static_assets	List containing static assets.	asset	lookup://simple_asset_lookup	Enabled	Enabled | Disable	Clone
static_identities	static_identities	List containing static identities.	identity	lookup://simple_identity_lookup	Enabled	Enabled | Disable	Clone

splunk> .conf18

Lookup Generating Searches

- Asset Information view and search is straightforward
  - asset_lookup_by_str and asset_lookup_by_cidr are missing the new column
- Lookup Generating Saved Searches are run by the modular input to finesse the data

Name	Actions		Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
Identity - Asset CIDR Matches - Lookup Gen	Edit Run		none	none	admin	SA-IdentityManagement	0	Global	✓ Enabled
Identity - Asset String Matches - Lookup Gen	Edit Run		none	none	admin	SA-IdentityManagement	0	Global	✓ Enabled

Macro Modifications to Capture New Field

- Need to modify macros
  - asset_sources is updated automatically to accommodate my new csv as a data source (no action required)
  - make_assets_str relies on make_assets macro
    - which relies on asset_fields macros
      - which relies on asset_attributes macro – Add our new field here

```
| `asset_sources` | `make_assets_str` | outputlookup output_format
    =splunk_mv_csv asset_lookup_by_str
```

Name	Definition
asset_attributes	owner,priority,lat,long,city,country,bunit,category,pci_domain,`extra_asset_fields`,classification
asset_fields	`asset_id_fields`,`asset_attributes`,asset_tag,asset_id

Asset Center Tweaks to View

- With those changes classification is now being captured in the converged lookup
  - Present in asset_by_str lookup but not in Asset Center
- Add to Asset Center by modifying the asset information saved search in pane
  - Optional achievement to unlock: Make it a tokenized field if desired!
  - In Asset Information panel, go into SimpleXML mode and add the field
    - <fields>ip,mac,nt_host,dns,owner,priority,lat,long,city,country,bunit,category,pci_domain,is_expected,should_timesync,should_update,requires_av,**classification**</fields>

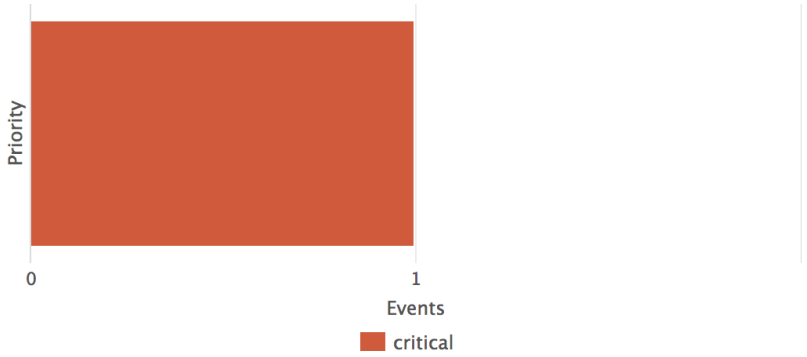
Asset Center

Asset Center

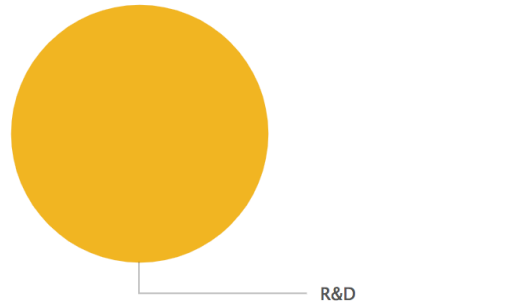
Edit | Export | ...

Asset: *
Priority: critical
Business Unit:
Category: All
Owner:
Submit | Hide Filters

Assets By Priority

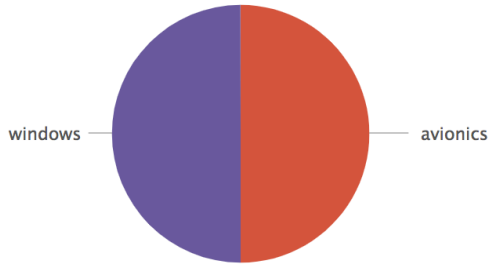


Assets By Business Unit



<1m ago

Assets By Category



Asset Information

ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	category	pci_domain	is_expected	should_timesync	should_update	requires_av	classification
192.168.50.50	ff:ff:ff:ff:ff:ff	orange		John Stoner	critical	37.7953849	-116.7775061	Tonopah Test Range	US	R&D	avionics windows	FALSE	TRUE	TRUE	TRUE	TRUE	TOPSECRET

Now What?

- Build correlation searches that leverage the new column
- Update dashboards and tokenize value to filter
- Add to Incident Review

Adding to Incident Review

- In ES, Configure > Incident Management > Incident Review Settings

Incident Review Settings

Configuration settings for Incident Review.

- Add new entry
  - Add label and field name both src and dest, in this case could also be dvc

Incident Review - Event Attributes

List of available attributes for notable event details.

Add new entry

Label	Field	Action
Source Country	src_country	Edit | Remove
Destination Classification	dest_classification	Edit | Remove
Source Classification	src_classification	Edit | Remove
Command Line	cmdline	Edit | Remove
Decoded URI	decoded_uri	Edit | Remove

splunk> .conf18

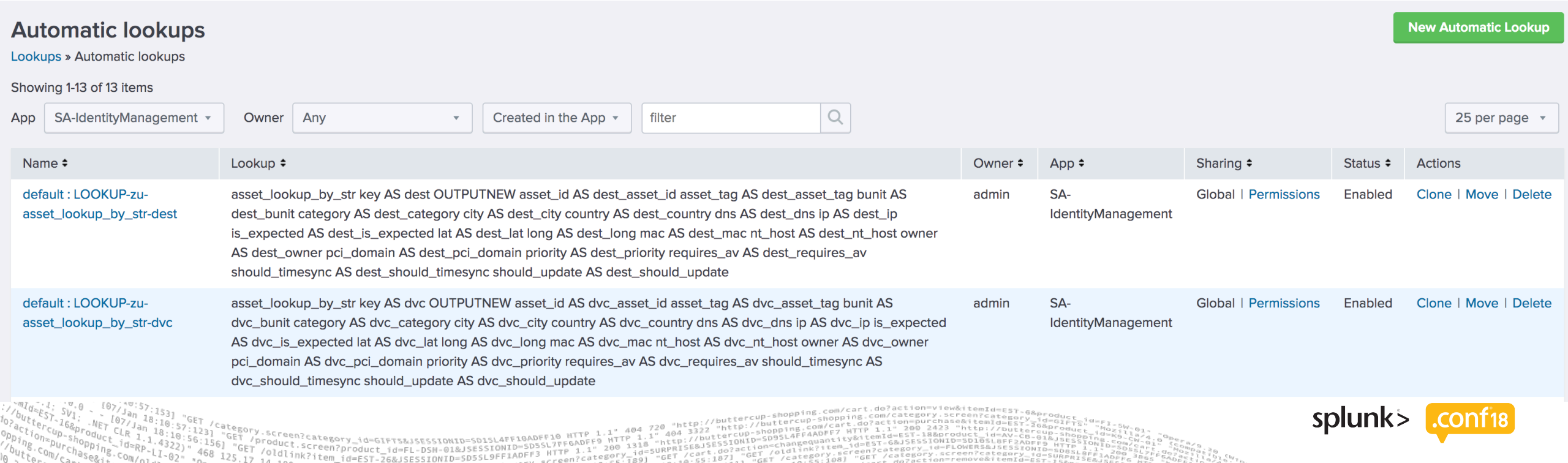
Update Macros

- This is not imperative for Notable Event but this is a frequently used macro to get asset values
  - Adding the field here is a good idea

get_asset_by(2)	lookup update=true asset_lookup_by_key key as "$subject$" OUTPUTNEW asset_id as "$subject$_asset_id",ip as "$subject$_ip",mac as "$subject$_mac", nt_host as "$subject$_nt_host",dns as "$subject$_dns",owner as "$subject$_owner",priority as "$subject$_priority",lat as "$subject$_lat",long as "$subject$_long",city as "$subject$_city",country as "$subject$_country",bunit as "$subject$_bunit",category as "$subject$_category",classification as "$subject$_classification",pci_domain as "$subject$_pci_domain",is_expected as "$subject$_is_expected",should_timesync as "$subject$_should_timesync",should_update as "$subject$_should_update",requires_av as "$subject$_requires_av",asset_tag as "$subject$_asset_tag"

Automatic Lookups

- At this point, if we run index=notable or any similar search, we get all metadata except our new field
- Settings > Lookups > Automatic Lookups
  - Select SA-IdentityManagement



splunk> .conf18

Automatic Lookups

- Add the new field in all 6 auto lookups

Name	Lookup
default : LOOKUP-zu-asset_lookup_by_str-dest	PUTNEW asset_id AS dest_asset_id asset_tag AS dest_asset_tag bunit AS dest_bunit category AS dest_category city AS dest_city classification AS dest_classification country AS dest_country dns AS dest_dns ip AS dest_ip is_expected AS dest_is_expected lat AS dest_lat long AS dest_long mac AS dest_mac owner pci_domain AS dest_pci_domain priority AS dest_priority requires_av AS dest_requires_av should_timesync AS dest_should_timesync should_update AS dest_should_update
default : LOOKUP-zu-asset_lookup_by_str-dvc	key AS dvc OUTPUTNEW asset_id AS dvc_asset_id asset_tag AS dvc_asset_tag bunit AS dvc_bunit category AS dvc_category city AS dvc_city classification AS dvc_classification country AS dvc_country dns AS dvc_dns ip AS dvc_ip is_expected AS dvc_is_expected lat AS dvc_lat long AS dvc_long mac AS dvc_mac nt_host owner pci_domain AS dvc_pci_domain priority AS dvc_priority requires_av AS dvc_requires_av should_timesync AS dvc_should_timesync should_update AS dvc_should_update
default : LOOKUP-zu-asset_lookup_by_str-src	key AS src OUTPUTNEW asset_id AS src_asset_id asset_tag AS src_asset_tag bunit AS src_bunit category AS src_category city AS src_city classification AS src_classification country AS src_country dns AS src_dns ip AS src_ip is_expected AS src_is_expected lat AS src_lat long AS src_long mac AS src_mac nt_host owner pci_domain AS src_pci_domain priority AS src_priority requires_av AS src_requires_av should_timesync AS src_should_timesync should_update AS src_should_update
default : LOOKUP-zv-asset_lookup_by_cidr-dest	PUTNEW asset_id AS dest_asset_id asset_tag AS dest_asset_tag bunit AS dest_bunit category AS dest_category city AS dest_city classification AS dest_classification country AS dest_country dns AS dest_dns is_expected AS dest_is_expected lat AS dest_lat long AS dest_long mac AS dest_mac nt_host AS dest_nt_host owner AS dest_owner domain AS dest_pci_domain priority AS dest_priority requires_av AS dest_requires_av should_timesync AS dest_should_timesync should_update AS dest_should_update
default : LOOKUP-zv-asset_lookup_by_cidr-dvc	asset_lookup_by_cidr key AS dvc OUTPUTNEW asset_id AS dvc_asset_id asset_tag AS dvc_asset_tag bunit AS dvc_bunit category AS dvc_category city AS dvc_city classification AS dvc_classification country AS dvc_country dns AS dvc_dns is_expected AS dvc_is_expected lat AS dvc_lat long AS dvc_long mac AS dvc_mac nt_host AS dvc_nt_host owner AS dvc_pci_domain priority AS dvc_priority requires_av AS dvc_requires_av should_timesync AS dvc_should_timesync should_update AS dvc_should_update
default : LOOKUP-zv-asset_lookup_by_cidr-src	asset_lookup_by_cidr key AS src OUTPUTNEW asset_id AS src_asset_id asset_tag AS src_asset_tag bunit AS src_bunit category AS src_category city AS src_city classification AS src_classification country AS src_country dns AS src_dns is_expected AS src_is_expected lat AS src_lat long AS src_long mac AS src_mac nt_host AS src_nt_host owner AS src_owner pci_domain AS src_pci_domain priority AS src_priority requires_av AS src_requires_av should_timesync AS src_should_timesync should_update AS src_should_update

Here's How

Lookup table *

asset_lookup_by_str

Lookup input fields

key	=	dest	Delete
	=		Delete

Add another field

Lookup output fields

asset_id	=	dest_asset_id	Delete
asset_tag	=	dest_asset_tag	Delete
bunit	=	dest_bunit	Delete
category	=	dest_category	Delete
city	=	dest_city	Delete
classification	=	dest_classification	Delete

Splunk Search

```
index=notable
```

src_asset_id	4a362a1c0f4dd1b62c52c9d7371dbce3989695f5
src_asset_tag	workstation
	windows
src_category	workstation
	windows
src_city	San Francisco
src_classification	SECRET
src_country	BR
src_dns	wrk-btun.frothly.local
src_ip	10.0.2.107
src_is_expected	false
src_mac	00:0c:29:6f:d0:2f
src_nt_host	wrk-btun
src_owner	Billy Tun
src_pci_domain	untrust
src_priority	low
src_requires_av	TRUE
src_should_timesync	false
src_should_update	TRUE

splunk> .conf18

Notable Event

☐	8/23/17 2:36:15.000 PM	Threat	Threat Activity Detected (nc.exe)

Description:

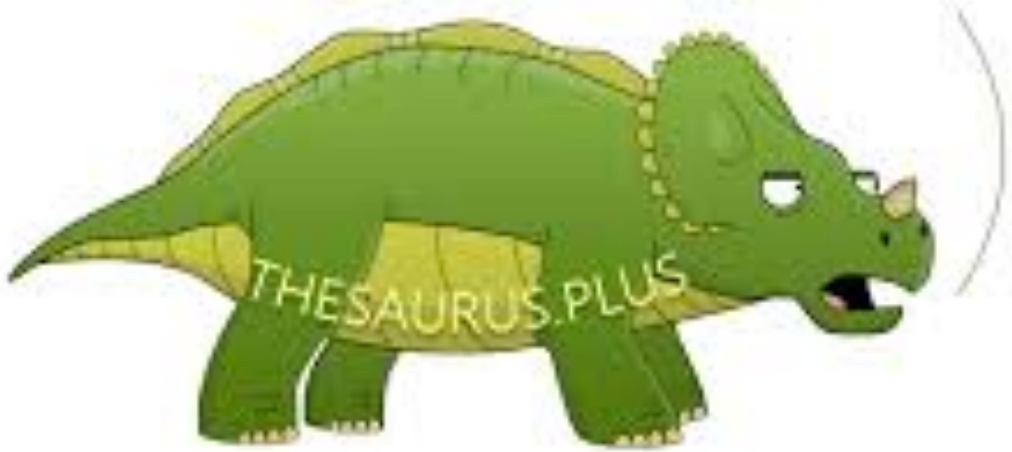
Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelligence available in the file collection

Additional Fields	Value	Action
Destination	160.153.91.7	
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
Source	10.0.2.107	
Source Category	workstation	
	windows	
Source City	San Francisco	
Source Classification	SECRET	
Source Country	BR	
Source DNS	wrk-btun.frothly.local	
Source IP Address	10.0.2.107	
Source Expected	false	
Source MAC Address	00:0c:29:6f:d0:2f	
Source NT Hostname	wrk-btun	
Source Owner	Billy Tun	
Source PCI Domain	untrust	
Source Requires Antivirus	TRUE	
Source Should Time Synchronize	false	
Source Should Update	TRUE	
Threat Category	undefined	
Threat Collection	file	
Threat Group	undefined	
Threat Match Field	file_name	
Threat Match Value	nc.exe	

A Caveat (or Two)

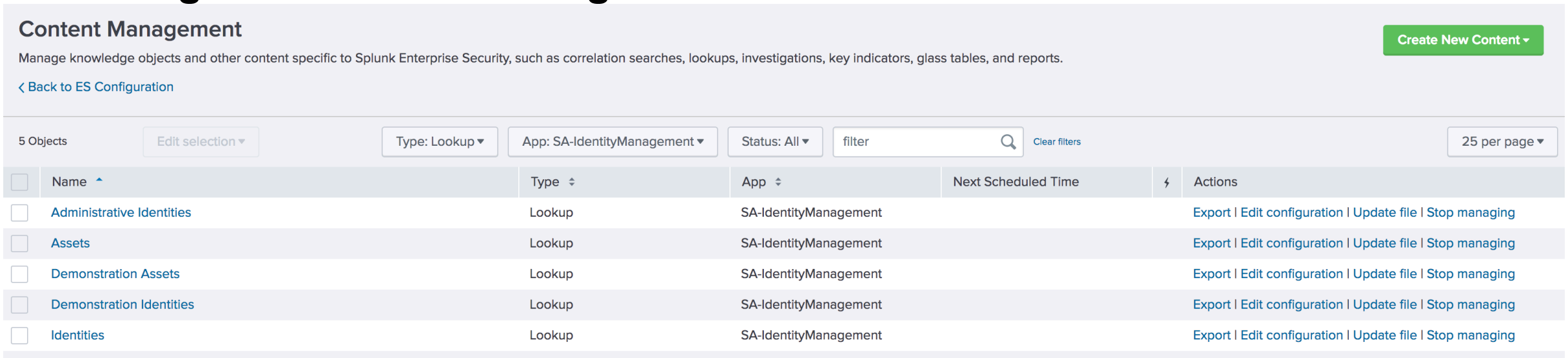
- Depending on how far you want to go with this
  - The underlying python scripts identity_correlation_rest_handler.py and identityLookup_rest_handler.log will require some love to accommodate these additional fields
  - Data model will need to be updated to accommodate additional fields

synonyms for caveat:
caution, admonition, warning, monition, qualification,
proviso, condition, stipulation, forewarning,
provision



Toys To Play With

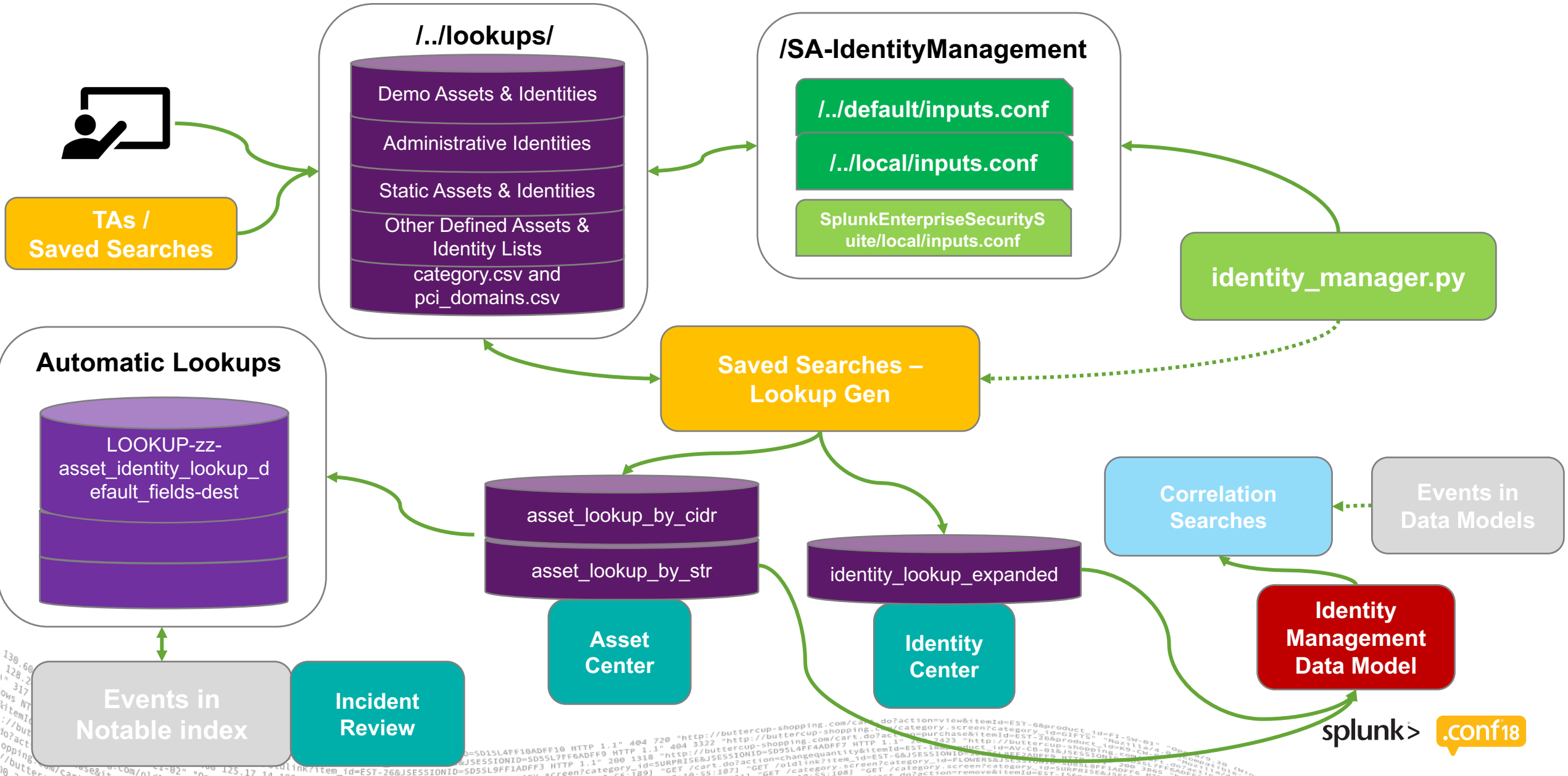
- **Configure > Content Management**



- $SPLUNK_HOME/etc/apps/SA-IdentityManagement/lookups/demo_assets.csv
- $SPLUNK_HOME/etc/apps/SA-IdentityManagement/lookups/demo_identities.csv

splunk> .conf18

Asset & Identity Framework Data Flow



Conclusion

- Asset & Identity Framework Provides Much Needed Context
- Reasonably straightforward to use
- Couple of early decision points to make around correlation of sourcetypes and naming convention around identities
- Scaling across large customer bases is something that needs to be thought through and planned with professional services
- Adding additional fields is possible but not as straightforward as you might expect so plan accordingly

Thank You

Don't forget to rate this session in the .conf18 mobile app