

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

Got Assets?

Defending Your Assets Part Two: You Asked for It!

SEC1219B

Megan Parsons

Security Strategist | Splunk

Scott McCarthy

Senior SOAR Engineer | National Grid



splunk> .conf22



Scott McCarthy

Senior SOAR Engineer | National Grid



Megan Parsons

Staff Security Strategist | Splunk

Finding Last Year's Presentation

Got Assets? Part 1: SEC1689C

- <https://conf.splunk.com/files/2021/recordings/SEC1689C.mp4>
- <https://conf.splunk.com/files/2021/slides/SEC1689C.pdf>



Why Should You Care?

After all it is just Assets

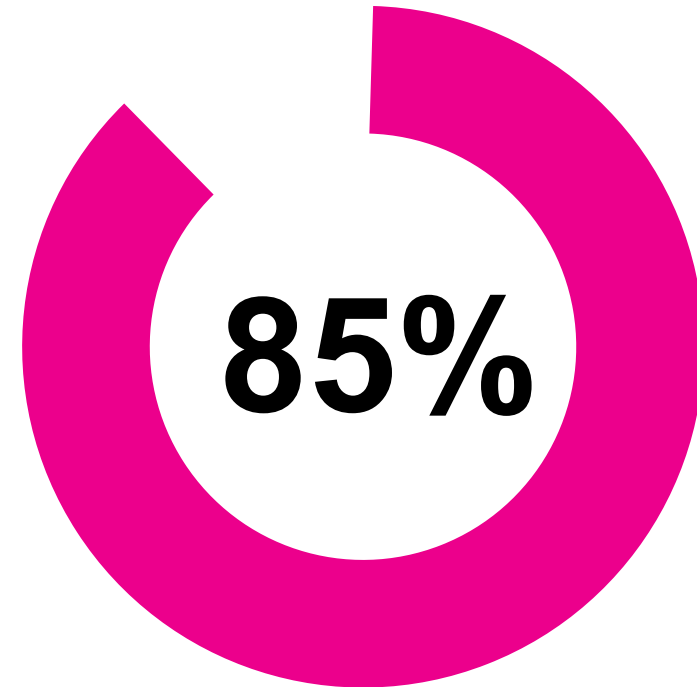


Don't Stop at CMDB

Configuration Management
Databases are incomplete

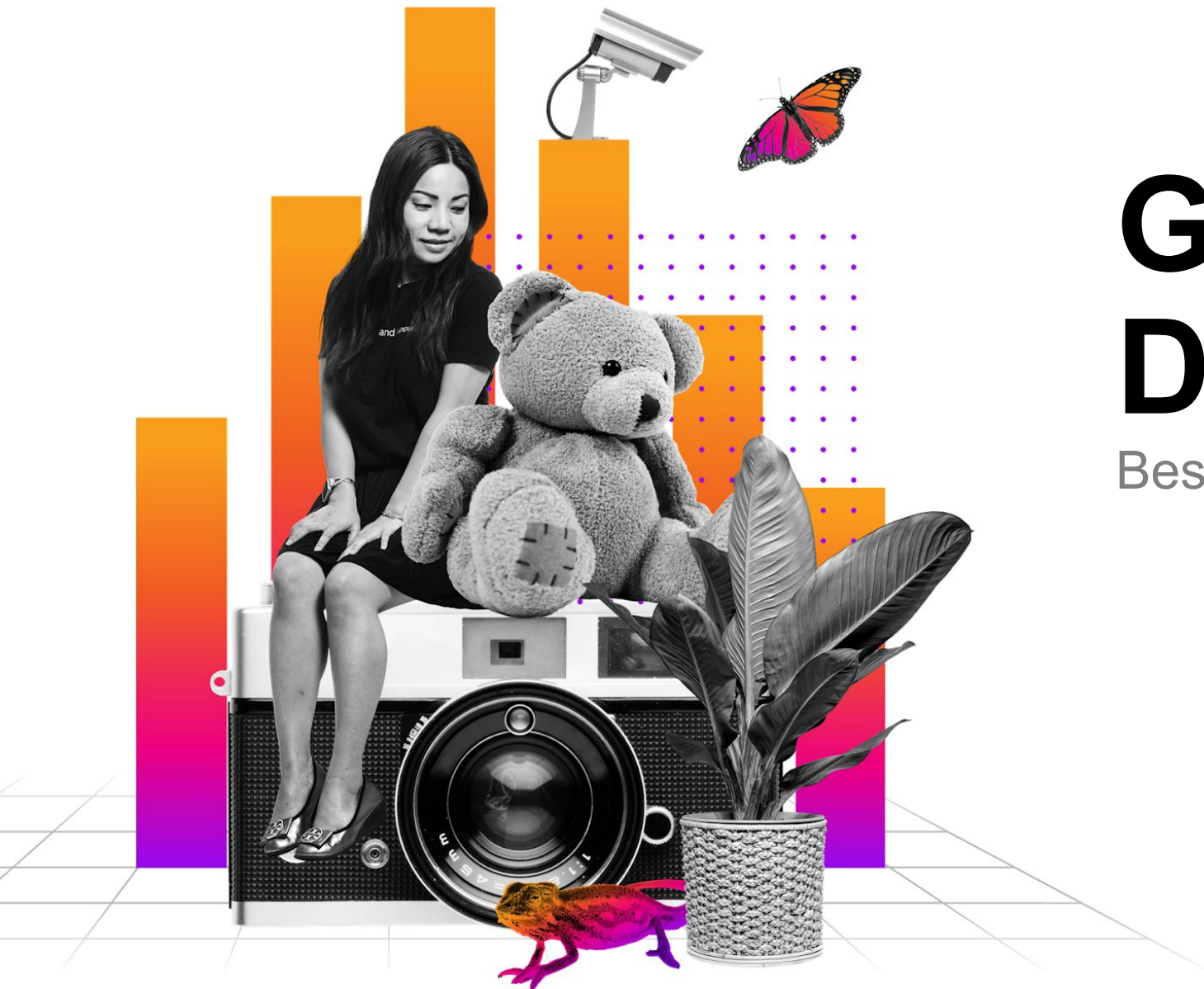
According to Forbes most companies fail at creating a CMDB. This is probably true at your company. What can we do about it?

Companies Failing At
Creating A CMDB



See what data you are missing...

Let's check that notable that just fired



Getting Data In

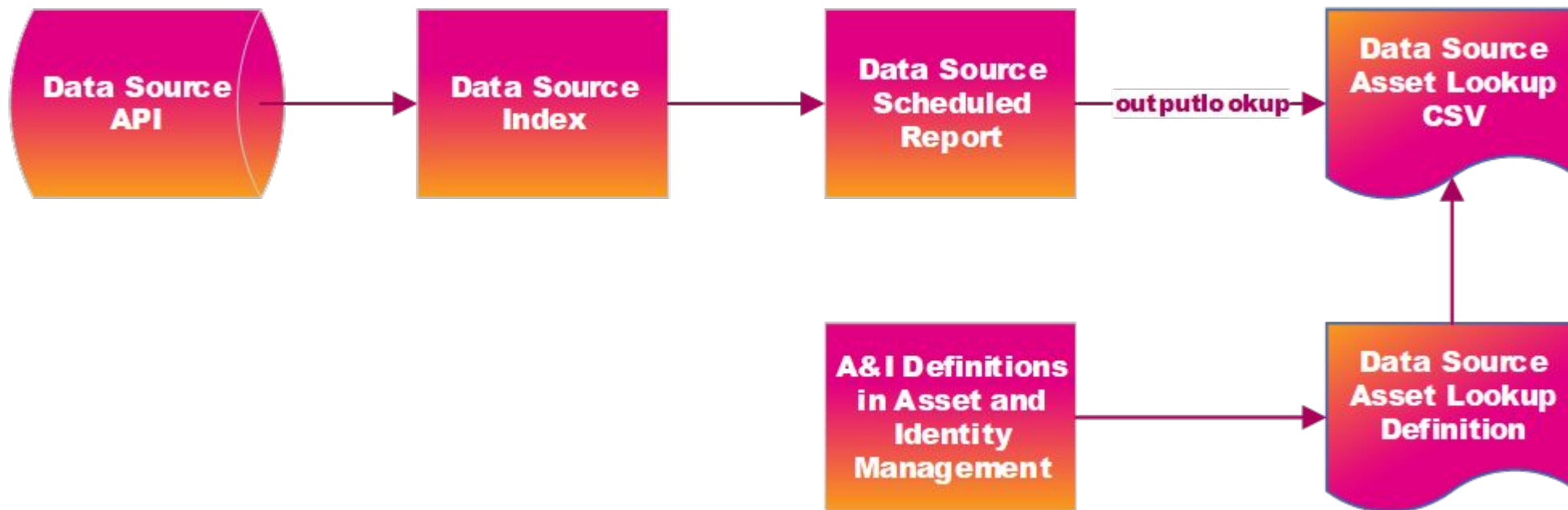
Best Practices

splunk>

.conf22

Bringing data into A&I

The process outlined



Standardization

Keeping names easy for future edits and reporting

Naming conventions to make it easier to identify reports, CSVs, and lookups that ingest into Assets and Identity

Assets_Identities_**DataSourceName**_lookup Report

Assets_Identities_**DataSourceName**_lookup.csv

Assets_Identities_**DataSourceName**_lookup

Schedule at off hours and stagger them

```
Interval = 6 2 * * *
```

Use Macros to standardize data cleanup

This macro formats the multi-value fields so they can be stored in lookups

```
`multivalue_fields_for_lookup`
```

This macro is design to remove invalid IPs (home IPs) and you can edit this macro to match your needs

```
`remove_home_ip`
```

This macro is designed to deduplicate multivalue fields

```
`remove_duplicates`
```

Append vs. Overwrite

- Depends on the data source
- Depends on how far you wish to go back on each search

```
| inputlookup lookup_name.csv  
| append  
  [ search index=sourcedata ...  
    | stats ...]  
| stats max(time) as time by nt_host  
| outputlookup lookup_name.csv|
```

NOTE: If you are looking for the “latest” and put a `_time` somewhere in the lookup you must convert both to epoch and use `max()`

Normalizing Data with Macros

add_meta(2)	eval meta="\$field_name\$: ".strftime(\$time\$,"%Y-%m-%d %H:%M:%S")	field_name,time
extract_meta(1)	rex field=meta "\$field_name\$\s(?:<\$field_name\$>\d{4}\-\d{2}\-\d{2}\s\d{2}\:\d{2}\:\d{2})"	field_name
multivalue_fields_for_lookup	foreach * [eval <<FIELD>> = mvjoin(mvdedup(mvappend(mvfilter(NOT match(<<FIELD>>,".[a-zA-Z]+\$")),<<FIELD>>)), "I")]	
os_filter	search NOT (OS="*cisco*" OR OS="*vmware*" OR OS="*no os*" OR OS="*emc*" OR OS="*switch*" OR OS="*openvms*")	
remove_duplicates	foreach * [eval <<FIELD>>=mvdedup(<<FIELD>>)]	
remove_home_ip	eval ip=if(match(ip,"192\.168\..*"),null(),ip) eval ip=if(match(ip,"169\.254\..*"),null(),ip) eval ip=if(match(ip,"0\.0\..*"),null(),ip)	
remove_ip_based_on_os	eval ip=if(match(OS,"Windows (?!Server).*(Business Enterprise Pro.*)."),null(),ip) eval ip=if(match(OS,"macOS.*"),null(),ip) eval ip=if(match(OS,"Mac.*"),null(),ip)	
splunk_data_indexes	index=os	

Auditing A&I Data

- Reports to identify the Sources and Searches/schedule of A&I
- Audit dashboard to identify problem assets or identities

Considerations for Customization

- Max custom fields = 20
- Reuse fields that aren't needed - (lat, lon)
- Create metadata field **meta** to use for additional context
- Use | in fields that support | - use multi-value fields!
- Don't use non-ascii characters



A&I Searches and IR Dashboard

splunk> **.conf22**

Search Assets

Assets

To make an ad-hoc query you just need an event with any field that contains an IP address, MAC address, hostname, or DNS name

```
| makeresults  
| eval hostname="host"  
| `get_asset(hostname)`
```

If you have a list of assets or events you can cross-reference the details very easily

```
| inputlookup hostlookup  
| `get_asset(hostnames)`
```

OR if you have a non-CIM compliant search

```
index="endpoint"  
| `get_asset("Computer Name")`
```

If you have a list of assets or events you can cross-reference the details very easily

```
| `assets`
```

Search Identities

Identities

To make an ad-hoc query you just need an event with any field that contains a username, sid, or email address.

```
| makeresults  
| eval user="someuser@buttercupgames.com"  
| `get_identity4events(user)`
```

OR a list of users

```
| makeresults  
| eval user="someuser@buttercupgames.com,someotheruser@buttercupgames.com"  
| makemv delim="," user  
| mvexpand user  
| `get_identity4events(user)`
```

Or you can just make it part of any search, but the field must be an approved identity field:

```
index="email"  
| eval user='recipient'  
| `get_identity4events(user)`
```

If you want to get a list of all identities:

```
| `identities`
```

Correlation Search A&I Extraction

- CIM Compliant – fields usually automatically lookup
- Edit which fields are used

The screenshot shows the configuration interface for Identity and Asset Extraction in Splunk. It features two main sections: 'Identity Extraction' and 'Asset Extraction'. Each section contains a list of fields with an 'X' icon to toggle their selection.

Identity Extraction

- src_user X
- user X
- src_user_id X
- src_user_role X
- user_id X
- user_role X
- vendor_account X
- src_user_email X
- recipient X

Asset Extraction

- src X
- dest X
- dvc X
- orig_host X

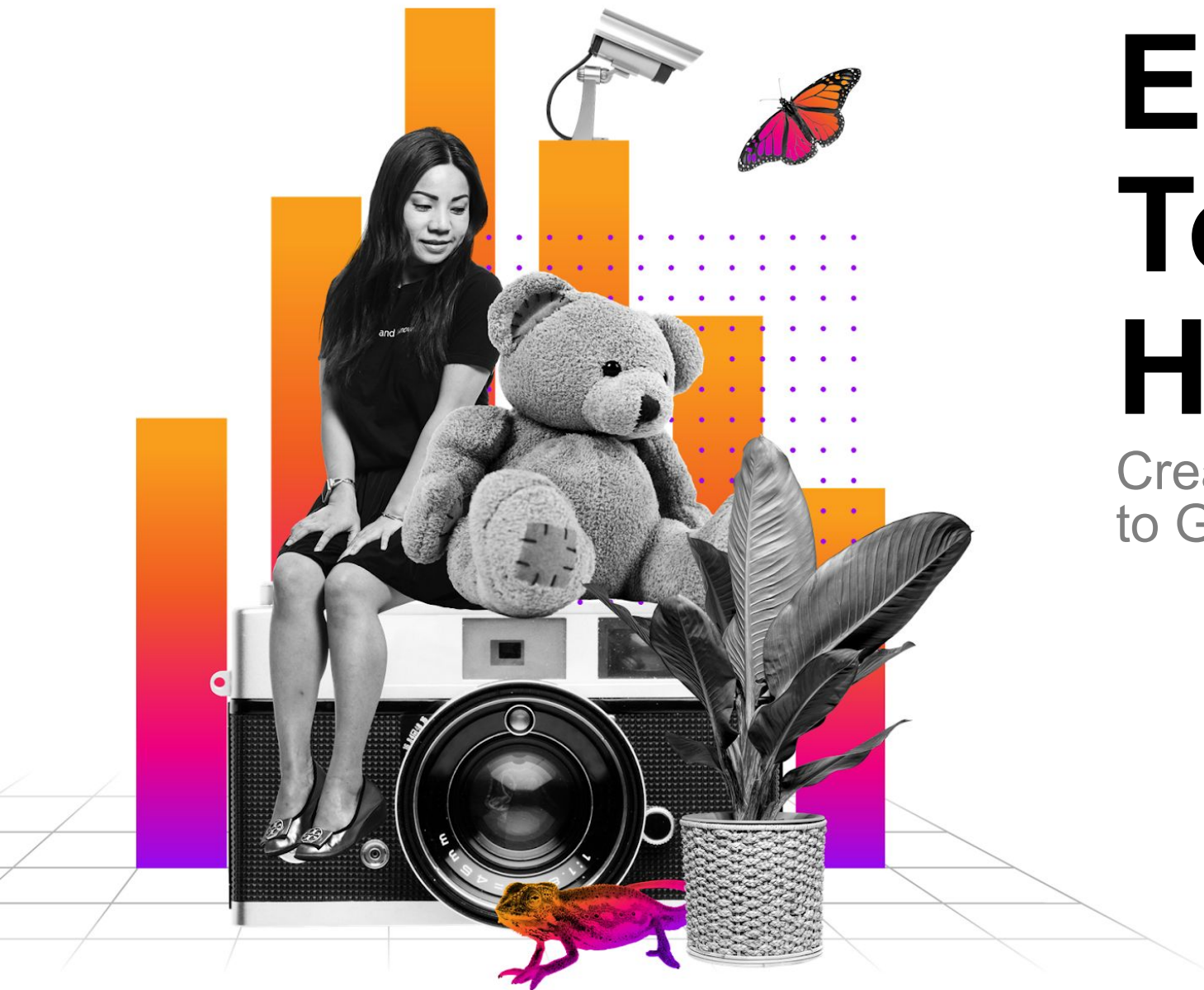
IR Dashboard Fields

Incident Review - Event Attributes

< Prev 1 2 3 4 5 ... 13 Next >

Field	Label	
Computer IP	Computer IP	Edit Remove
Intel Name	Intel Name	Edit Remove
Computer Name	Computer Name	Edit Remove
num_hosts	Number of hosts	Edit Remove
id	Alert ID	Edit Remove
body	Alert Body	Edit Remove



Endpoint Tooling Helper

Creating Metadata to Gain Better Insights

splunk>

.conf22

Security Tooling field

Use this to indicate the source of the data you are bringing into the A&I Framework

This is helpful to identify hosts which have Splunk and other endpoint tooling enabled.

```
index="endpoint"
| rename hostname as nt_host, os AS OS
| stats values(domain) as domain, values(OS) as OS, values(ip) as ip, values(mac) as mac latest(_time) as last_checked_in by nt_host
| eval security_tooling="endpoint"
  add_meta(ep_last_discovered,last_checked_in)`
| search NOT ip=*ip*
  `remove_home_ip`
  `remove_ip_based_on_os`
  `multivalue_fields_for_lookup`
| outputlookup Assets_Identity_Endpoint_lookup.csv|
```

Metadata field - Assets


Create the Metadata field

Standardize formats for data ingestion

Use date stamps to record the last interaction with the tooling being checked.

Example of endpoint checking dates

```
index="endpoint"
| rename hostname as nt_host, os AS OS
| stats values(domain) as domain, values(OS) as OS, values(ip) as ip, values(mac) as mac latest(_time) as last_checked_in by nt_host
| eval security_tooling="endpoint"
| add_meta(ep_last_discovered,last_checked_in)
| search NOT ip=*ip*
  `remove_home_ip`
  `remove_ip_based_on_os`
  `multivalue_fields_for_lookup`
| outputlookup Assets_Identity_Endpoint_lookup.csv
```



A diagram consisting of two rectangular boxes with red borders. The left box contains the text `'add_meta(ep_last_discovered,last_checked_in)'`. A red arrow points from this box to the right box, which contains the text `| eval meta="$field_name$: ".strftime($time$,"%Y-%m-%d %H:%M:%S")`. This illustrates the internal implementation of the `add_meta` function.

Extracting Metadata

New Search

```
| `assets`  
| `extract_meta(ep_last_discovered)`  
| `extract_meta(sp_data_last_ingested)`  
| table nt_host ep_last_discovered sp_last_discovered sp_data_last_ingested
```

```
| rex field=meta "$field_name$:\s(?:<$field_name$>\d{4}\-\d{2}\-\d{2}\s\d{2}:\d{2}:\d{2})"
```





✓ 4,967 results (before 4/18/22 4:54:33.000 PM) No Event Sampling ▾

Job ▾

Events (0) Patterns **Statistics (4,967)** Visualization

20 Per Page ▾  Format Preview ▾

< Prev 1

nt_host ⇅ 	ep_last_discovered ⇅ 	sp_last_discovered ⇅ 	sp_data_last_ingested ⇅ 
canada_dev_03mdpy0z	2022-04-11 20:24:56		
canada_dev_04swmm01	2022-04-12 16:54:02		
canada_dev_0rmqh8dh	2022-04-12 16:54:02		2022-02-28 15:02:53
canada_dev_0u3qzss0	2022-04-12 16:54:02		
canada_dev_11pirjdo	2022-04-12 16:54:02		2022-02-26 04:16:11
canada_dev_16sacai	2022-04-11 20:24:56		2022-03-05 13:44:27
canada_dev_1d1qktyj	2022-04-11 20:24:56		2022-04-05 17:16:18
canada_dev_1es6n8n6	2022-04-11 20:24:56		
canada_dev_1gfzpb9b	2022-04-11 20:24:56		
canada_dev_1k4kurpm	2022-04-11 20:24:56		



Dashboards

splunk>

.conf22

A&I Sources Dashboard

Assets and Identities Sources

Edit

Export ▾

...

Name

splunk

Submit

[Hide Filters](#)

Lookups

title ↕	fields_array ↕	filename ↕
Assets_Identity_SplunkData_lookup	nt_host last_data_ingested meta security_tooling	Assets_Identity_SplunkData_lookup.csv
Assets_Identity_SplunkDS_lookup	security_tooling nt_host meta	Assets_Identity_SplunkDS_lookup.csv

Reports

title ↕	search ↕	disabled ↕	is_scheduled ↕	next_scheduled_time ↕	cron_schedule ↕	dispatch.earliest_time ↕	ear:acl.app ↕	id ↕
Assets_Identity_SplunkData_lookup Report	<pre> tstats latest(_time) as last_data_ingested where `splunk_data_indexes` by host eval security_tooling="splunk" rename host AS nt_host `add_meta(sp_data_last_ingested,last_data_ingested)` `remove_home_ip` `multivalued_fields_for_lookup` outputlookup Assets_Identity_SplunkData_lookup.csv</pre>	0	0			0	DA_Assets_Helper	https://es.soar.ssn.ngrid.net:8089/servicesNS/mccars3/DA_Assets_He

Debug Asset Data Dashboard

Debug Asset Data

Edit

Export ▾

...

This is designed to debug issues with the A&I Framework sources. You can enter a hostname, IP, dns, or SID in the asset field and see the current set up in A&I and each feed from each source to identify issues. The source_of_data in the input panel shows which lookup is feeding that row of data.

Asset

germany_dev_ou5sf6ge

Submit

[Hide Filters](#)

Asset Search

asset ▾	asset_id ▾	bunit ▾	category ▾	country ▾	dns ▾	ip ▾	lat ▾	long ▾	mac ▾	meta ▾	nt_host ▾	owner ▾	pci_dorr ▾
germany_dev_ou5sf6ge.extdomain.com 10.185.108.157 da:b6:a8:84:34:76 germany_dev_ou5sf6ge	6259c908357f871391136378	services	server	germany	germany_dev_ou5sf6ge.extdomain.com	10.185.108.157	51.165691	10.451526	da:b6:a8:84:34:76	ep_last_discovered: 2022-04-12 16:54:02 sp_data_last_ingested: 2022-04-06 17:35:51 sp_last_checked_in: 2022-04-06 17:35:51	germany_dev_ou5sf6ge	sean payne	untrust

Get the Source of your Data

Inputs															
OS ⌵	bunit ⌵	category ⌵	country ⌵	dns ⌵	domain ⌵	ip ⌵	last_checked_in ⌵	last_data_ingested ⌵	lat ⌵	long ⌵	mac ⌵	meta ⌵	nt_host ⌵	os ⌵	owner ⌵
solaris 8					extdomain	10.185.108.157	1649782442				da:b6:a8:84:34:76	ep_last_discovered: 2022-04-12 16:54:02	germany_dev_OU5SF6GE		
	Services	server	germany	germany_dev_OU5SF6GE.extdomain.com	extdomain	10.185.108.157			51.165691	10.451526	da:b6:a8:84:34:76		germany_dev_OU5SF6GE	solaris 8	Sean Payne
								1649266551				sp_data_last_ingested: 2022-04-06 17:35:51	germany_dev_OU5SF6GE		
												sp_last_checked_in: 2022-04-06 17:35:51	germany_dev_OU5SF6GE		

Asset Search

Search for asset details

Edit

Export ▾

...

Asset

germany_dev_ou5sf6ge

Submit

[Hide Filters](#)

Splunk Installed

True

Splunk Data

active

Splunk Internal Data Status

inactive

Splunk Last Checked In

0

Splunk Data Last Ingested

2022-04-06 17:35:51

Splunk Internal Data Last Ingested

0

asset ▾	asset_id ▾	bunit ▾	category ▾	country ▾	dns ▾	ip ▾	lat ▾	long ▾	mac ▾	meta ▾	nt_host ▾	owner ▾	pci_dom ▾
germany_dev_ou5sf6ge.extdomain.com 10.185.108.157 da:b6:a8:84:34:76 germany_dev_ou5sf6ge	6259c908357f871391136378	services	server	germany	germany_dev_ou5sf6ge.extdomain.com	10.185.108.157	51.165691	10.451526	da:b6:a8:84:34:76	ep_last_discovered: 2022-04-12 16:54:02 sp_data_last_ingested: 2022-04-06 17:35:51 sp_last_checked_in: 2022-04-06 17:35:51	germany_dev_ou5sf6ge	sean payne	untrust

Identity Search

Identity Search

Identity

andrew.mackenzie

Submit

Hide Filters

Edit

Export ▾

...

Results

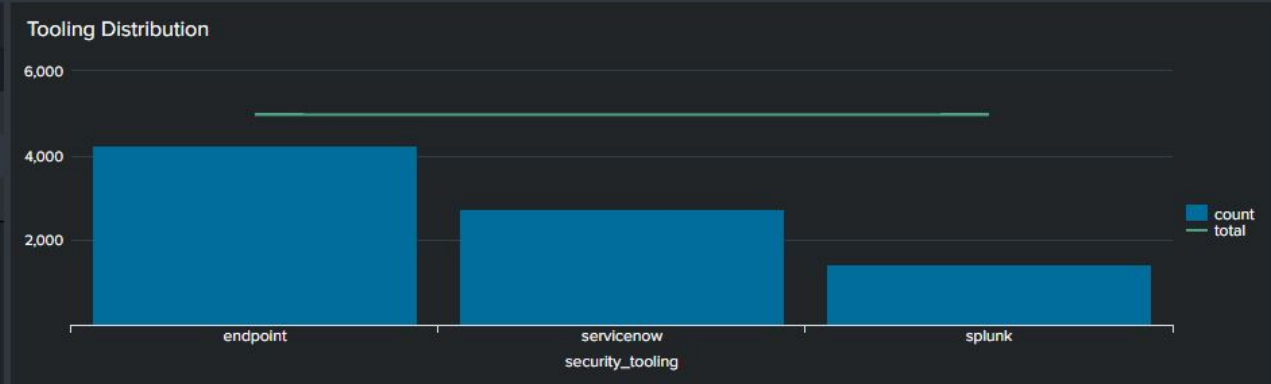
identity_id ▾	UUID ▾	bunit ▾	category ▾	email ▾	endDate ▾	first ▾	identity ▾	identity_tag ▾	last ▾	managedBy ▾	nick ▾	phone ▾	prefix ▾	priority ▾	startDate ▾	suffix ▾	watchl ▾
6259a62bc12a7464e77a1481	b478c76c-1057-4a99-9d0a-f965f05825ce	human resources		andrew.mackenzie@buttercupgames.com		andrew	b478c76c-1057-4a99-9d0a-f965f05825ce andrew.mackenzie andrew.mackenzie@buttercupgames.com	human resources	mackenzie					critical			

Tooling Visibility

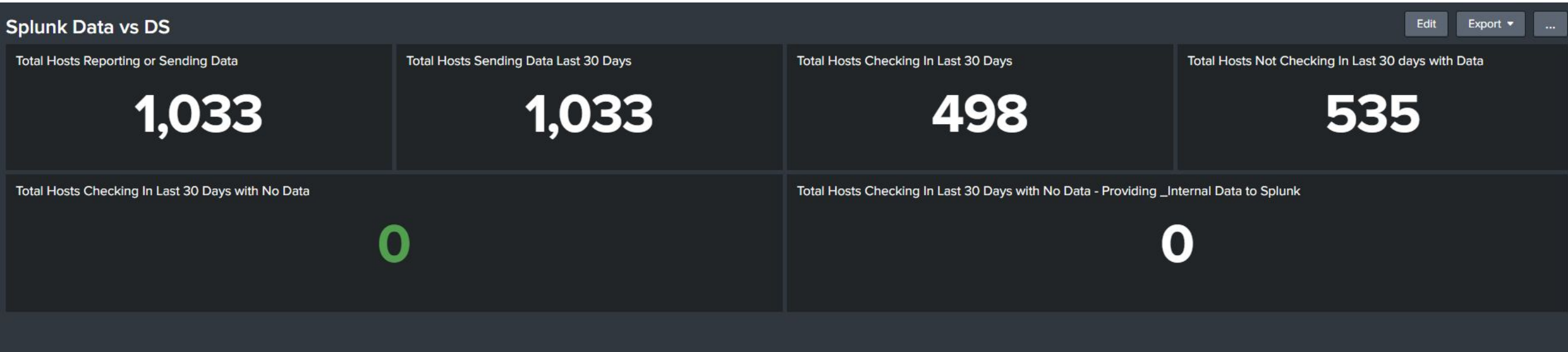
Asset Visibility Tooling

Tooling Distribution			
security_tooling ▾	count ▾	total ▾	percent ▾
endpoint	4,237	4,967	85.30%
servicenow	2,743	4,967	55.22%
splunk	1,447	4,967	29.13%

Q ⬇ i ↺ <1m ago



Splunk DS/UF Data Trends





Demo

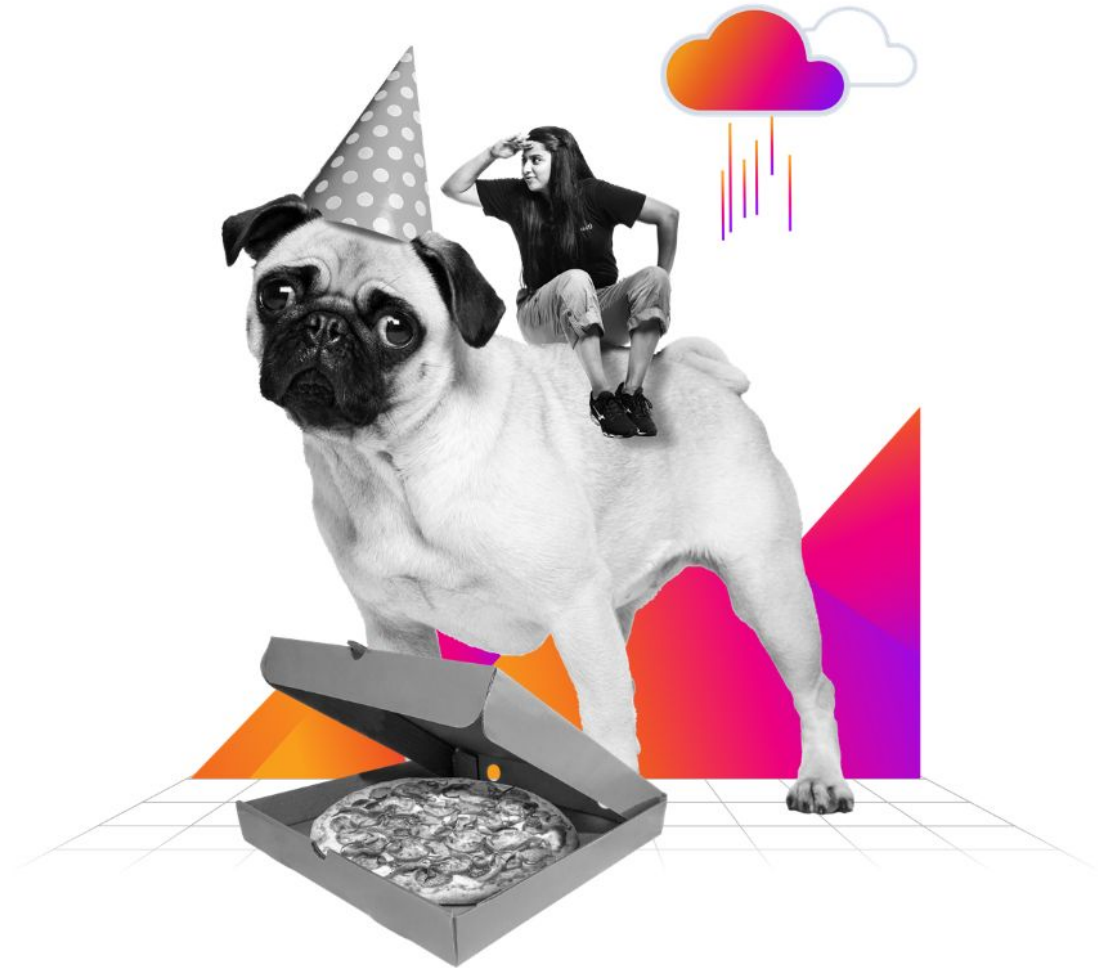


Next Steps



- Risk Based Alerts
- VIP
- Priority-based
- Watch List

- Manage new assets/identities
- Age out old assets/identities





Download the helper app

<https://splunkbase.splunk.com/app/6406/>

Thank You

