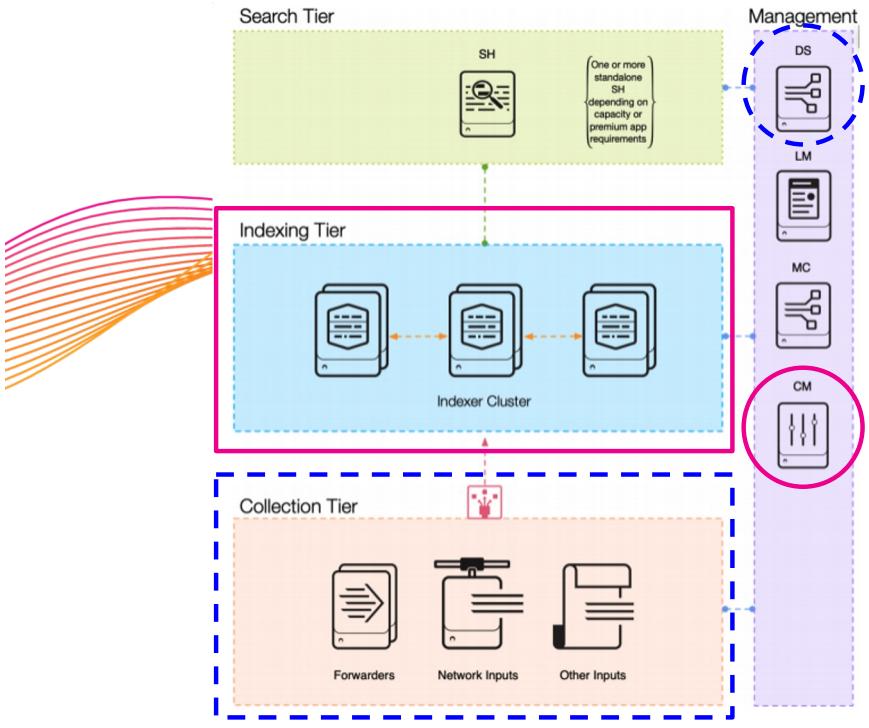
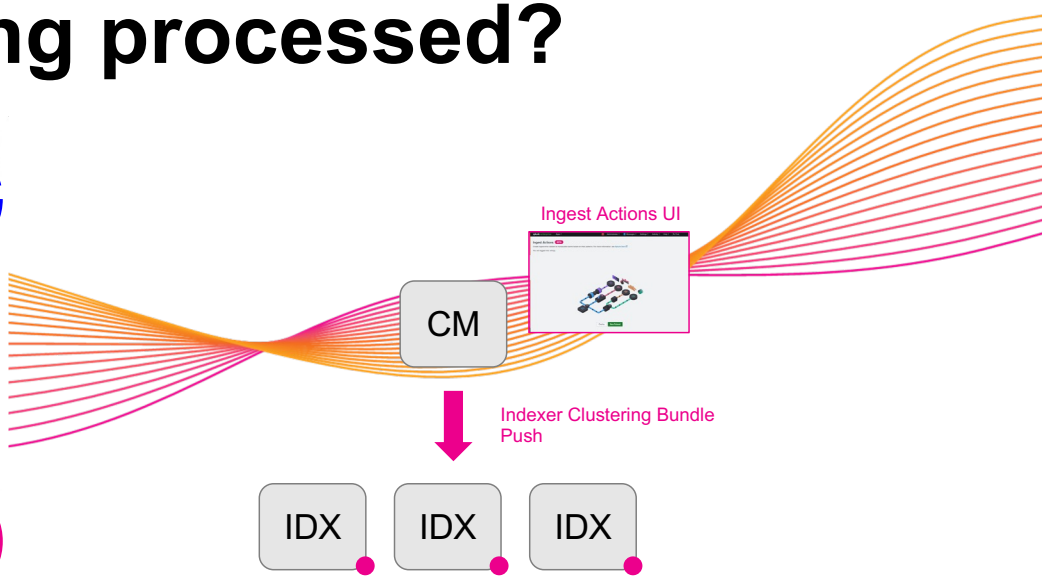
Where are rules being processed?





`$SPLUNK_HOME/etc/master-apps/_cluster/splunk_ingest_actions`

Or on standalone:

`$SPLUNK_HOME/etc/apps/splunk_ingest_actions/local/`

splunk>

Interaction with TRANSFORMS

The `RULESET` setting is similar in behavior to the `TRANSFORMS` setting in props.conf

Considerations when using `RULESET`:

- `TRANSFORMS` is applied first if a source type matches both a `RULESET` and a `TRANSFORMS` stanza configuration on the cluster peers.
- A source type should *only* have one `RULESET` configuration. Additional rulesets is unsupported.
- Only use the Ingest Actions page, or the REST API `/services/data/ingest/rulesets` endpoint to create a `RULESET` configuration.
- A `RULESET` is applied to data streams from a UF and to cooked data from the HF. This represents a change in behavior from using the `TRANSFORMS` setting.

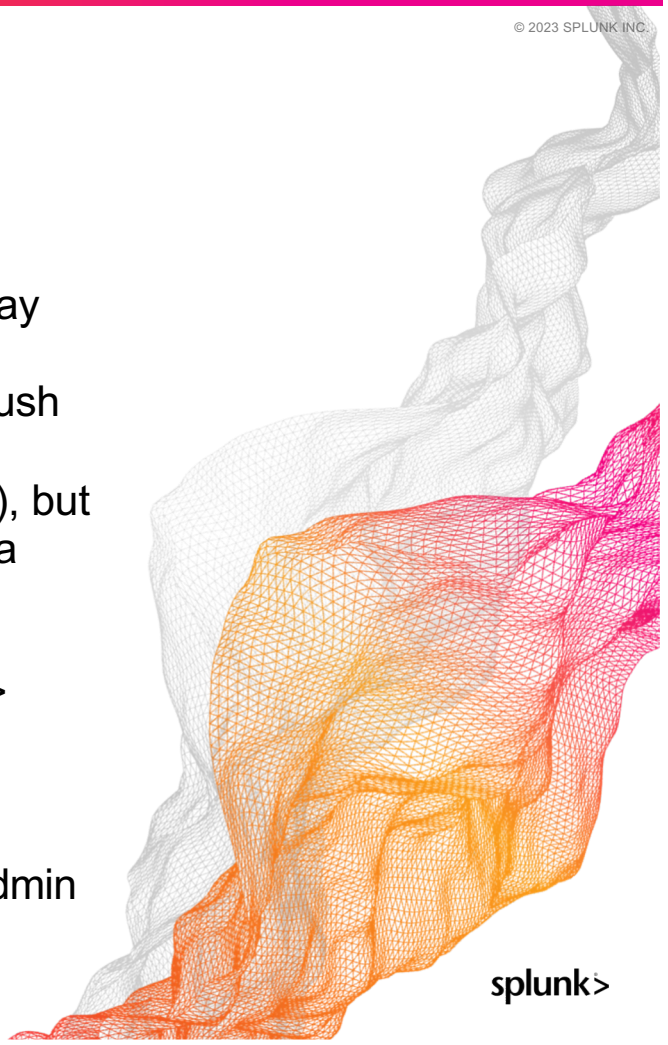
Order of operations for Ingest Actions on a HF:

1. Existing HWF TRANSFORMS
2. Ingest Actions HWF RULESET TRANSFORMS
3. *INDEXER TRANSFORMS (skipped if already touched by HF TRANSFORMS)*
4. Ingest Actions INDEXER RULESET TRANSFORMS (accepts cooked data)

splunk>

Deployment Gotchas

- Saved rulesets will be deployed on the next bundle push, important if you save now but decide not to deploy right away
- Deleted ruleset is only applied to the peers with a bundle push
- Rulesets are hot-reloadable (will not trigger Rolling-Restart), but if there are *other* configuration settings staged that require a RR, a RR will initiate
- Check the Configuration Bundle page for issues (Settings > Distributed Environment > Indexer Clustering > Edit > Configuration Bundle Actions)
- IA requires the *list_ingest_ruleset* and *edit_ingest_ruleset* admin capabilities to run



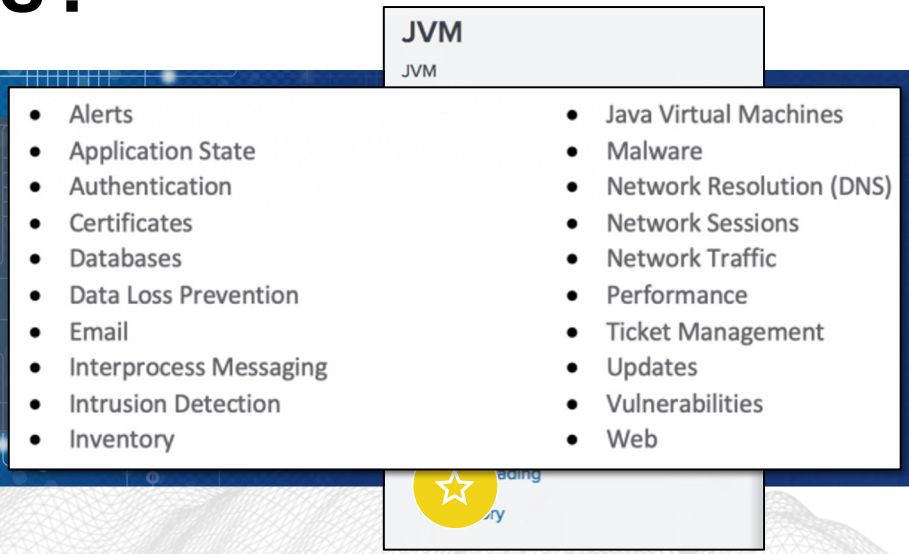
Data Models

Standardize your data

splunk>

What are Data Models?

A data model is a search-time mapping of data into a hierarchical structure



A collection of objects

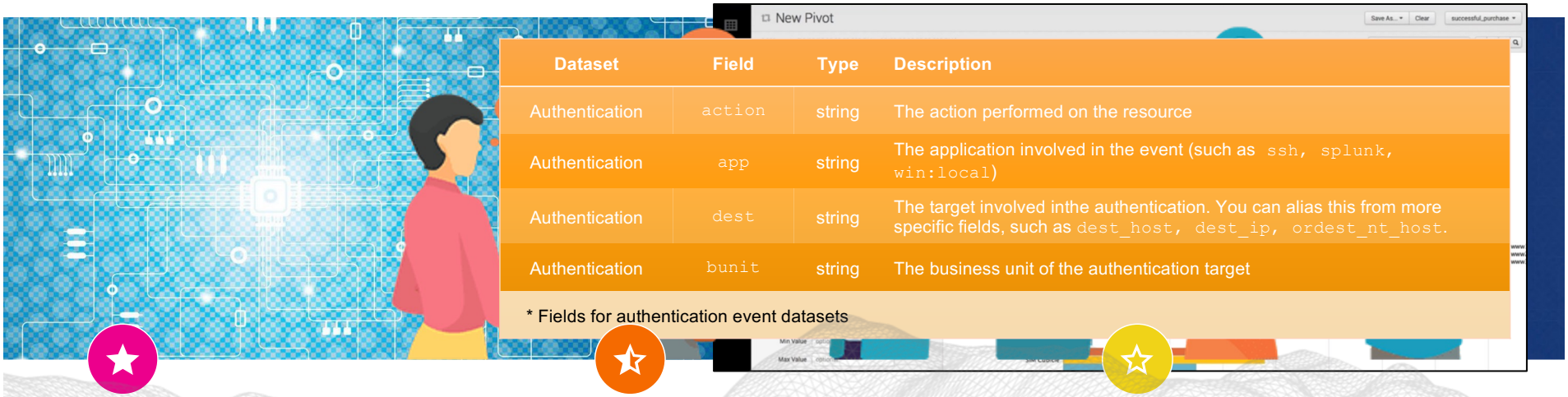
That have constraints and attributes

Where child objects inherit those constraints and attributes

splunk>

SAGEFOX

Why Use Data Models?



Dataset	Field	Type	Description
Authentication	action	string	The action performed on the resource
Authentication	app	string	The application involved in the event (such as ssh, splunk, win:local)
Authentication	dest	string	The target involved inthe authentication. You can alias this from more specific fields, such as dest_host, dest_ip, ordest_nt_host.
Authentication	bunit	string	The business unit of the authentication target

* Fields for authentication event datasets

Fields
Common fields allow for unique insights across many sets of data

Pivot
Allow general users to build reports with an Excel-like interface

Common Language
CIM allows for normalized fields that can be tailored for many use cases

splunk>

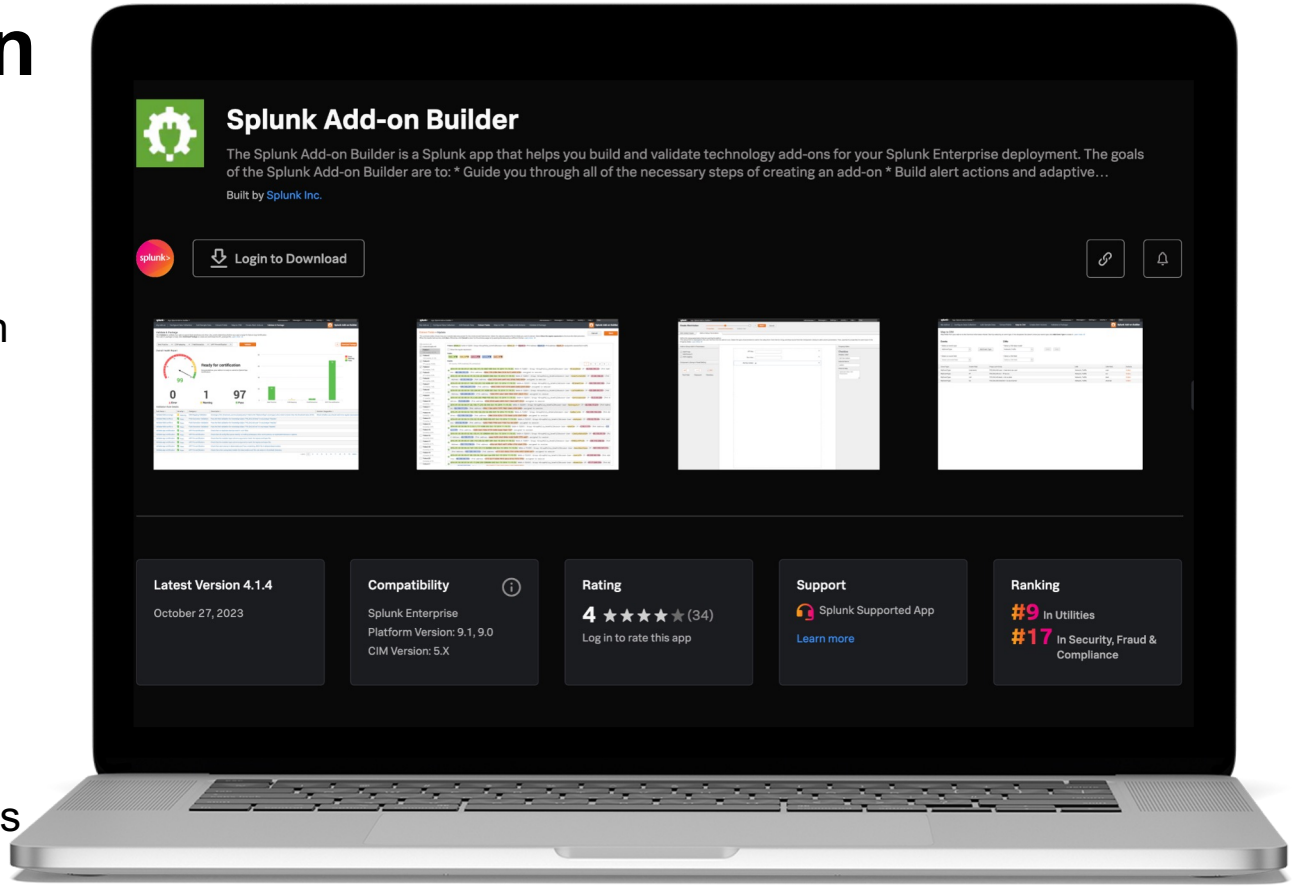
SAGEFOX

Splunk Add-on Builder

splunk>

Splunk Add-on Builder

- Onboard additional data
- Build and validate add-on
- Custom configurations
  - field extractions
  - transforms
- Knowledge mapping
  - event types
  - tags
- Custom views and reports



splunk>

Lab Access

splunk>

Access Class Material

Items of Interest can be found by going to this Google Drive:

1. **This link will have your Lab Guide, Splunk Instance Details and more:**
   https://tinyurl.com/splunkworkshops
2. **Follow the guidance of your instructor on accessing / noting which instance you will use for this workshop, along with getting access to the slides and lab guide.**

splunk>

Lab Exercises

splunk>

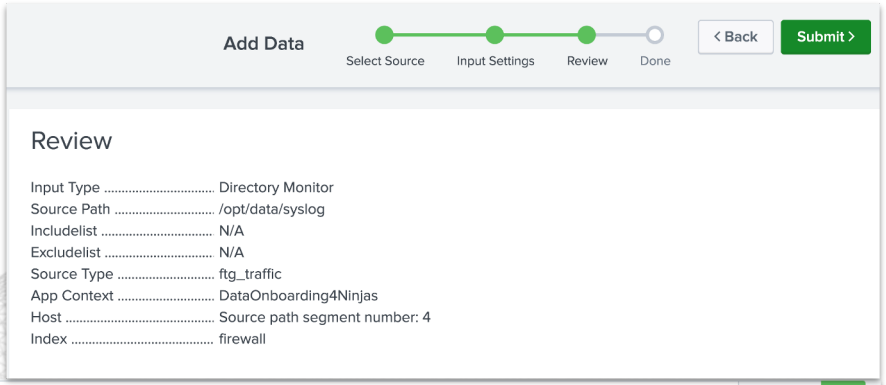
Lab 1: File Monitor

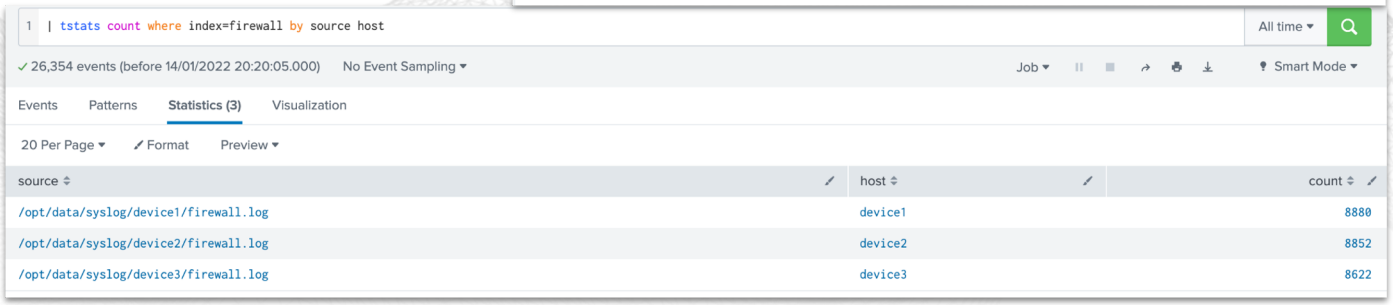
Collect some local files within different folder structure by using inputs.conf

Activity:

1. Monitor the syslog directory on the local machine
   - Each device has a dedicated folder
2. Adjust input settings
   - host to match the folder name
3. Confirm Input

Goal:





splunk>

Break for Lab 1

splunk>

Lab 1: Option 1 - File Monitor: GUIDED

Collect some local files within different folder structure by using inputs.conf

GUI:

Navigate to Settings > Add Data > Files and Directories

Select your firewall logs under /opt/data/syslog/

***KEY:* Choose continuous monitor for this lab!**

 # Input Settings

New Source Type: ftg_ttraffic

App Context: DataOnboarding4Ninjas

Host Value: Set ‘Segment in Path’ to 4

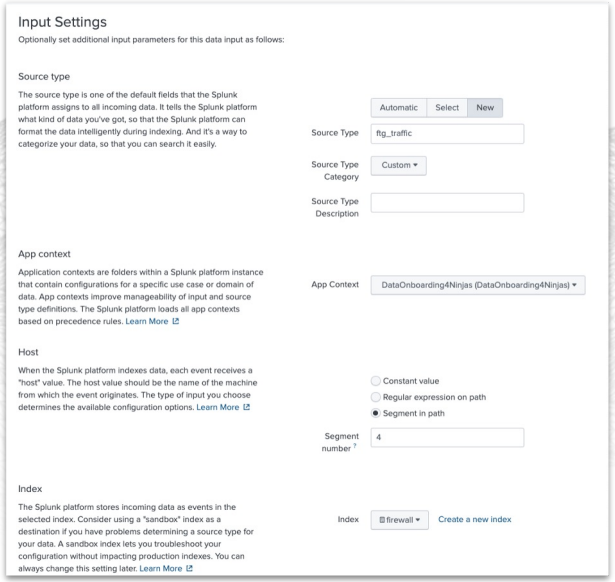
Index: firewall

 # Check result

```
| tstats count where index=firewall by host source
```

***KEY:* Host value now has the device name**

Goal:



splunk>

Lab 1: Option 2 - File Monitor: GUIDED

Collect some local files within different folder structure by using inputs.conf

CLI:

Navigate to /opt/splunk/etc/system/local/inputs.conf

```
[monitor:///opt/data/syslog/*/firewall.log]
sourcetype = fgt_traffic
index = firewall
host_segment = 4
```

 # Reload Monitor

```
/opt/splunk/bin/splunk reload monitor

/opt/splunk/bin/splunk btool inputs list --
debug | grep firewall
```

 # Check result

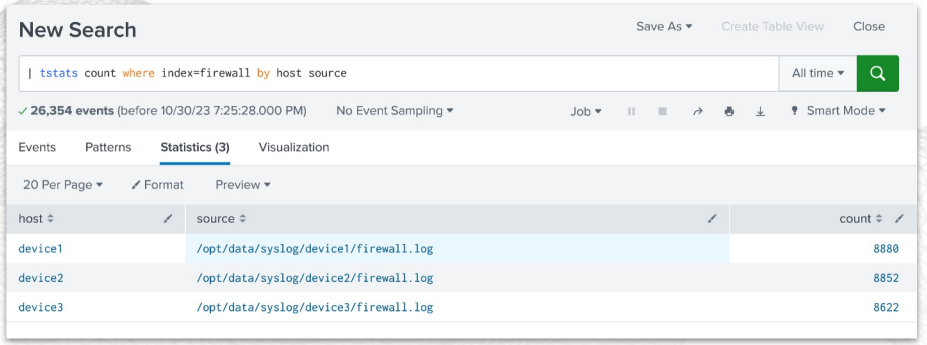
```
| tstats count where index=firewall by host source
```

KEY: Host value now has the device name

Goal:

```
splunk@show-demo-i-05d1683d07b1bccca:~$ sudo su
root@show-demo-i-05d1683d07b1bccca:/home/splunk# cd /opt/splunk/etc/apps/DataOnboarding4Ninjas/
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# mkdir local
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# cd local
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas/local# vi inputs.conf
```

```
[monitor:///opt/data/syslog/*/firewall.log]
sourcetype = fgt_traffic
index = firewall
host_segment = 4
```



splunk>

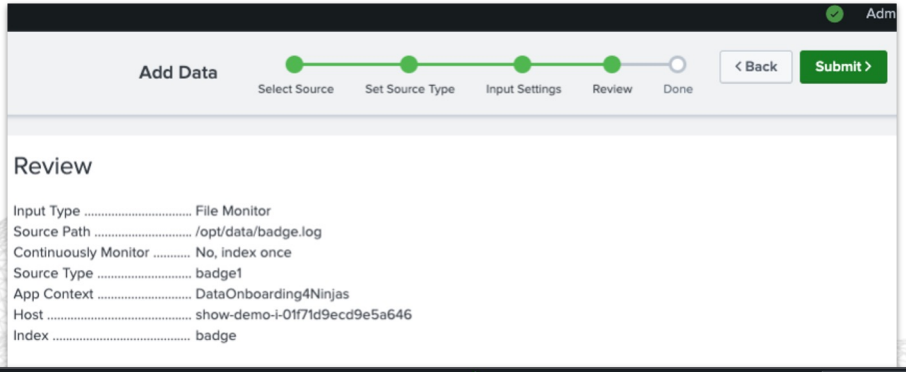
Lab 2: Data Parsing

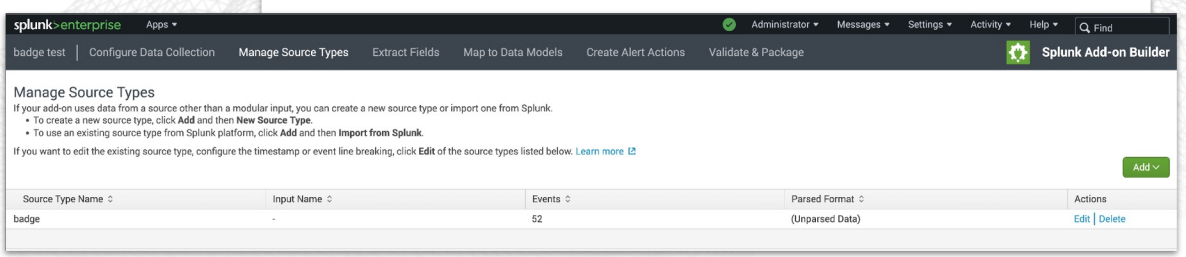
Collect and parse badge data through a sourcetype and create an add-on

Activity:

1. Collect badge data being stored on a local structure
2. Parse out the badge data via a new sourcetype
3. Select our input settings
4. Create a *badge* add-on
5. Import the new sourcetype into the add-on

Goal:





splunk>

Break for Lab 2

splunk>

Lab 2: Option 1- Data Parsing: Guided Steps

Collect and parse badge data through a new sourcetype

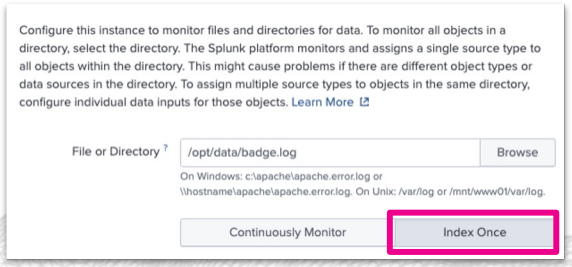
GUI:

Navigate to Settings > Add Data > Files and Directories

Select your badge logs under /opt/data/

***KEY:* Choose index once for this lab!**

Goal:



splunk>

Lab 2: Data Parsing: Guided Steps

Collect and parse badge data through a new sourcetype

GUI:

 # Save Source Type as badge

SHOULD_LINEMERGE = false

LINE_BREAKER = (##)

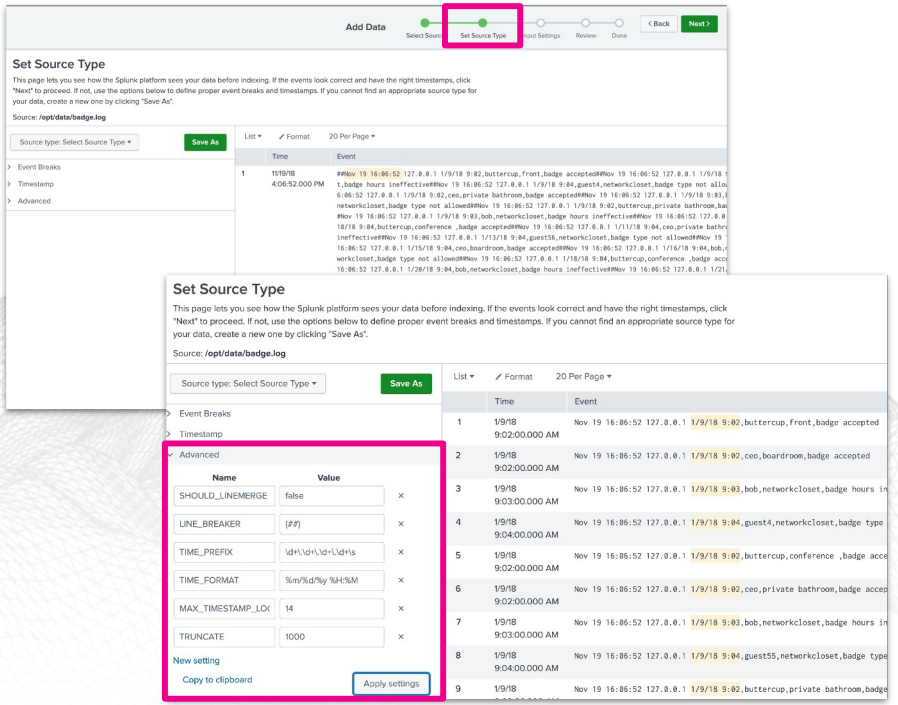
TIME_PREFIX = \d+\.\d+\.\d+\.\d+\s

TIME_FORMAT = %m/%d/%y %H:%M

MAX_TIMESTAMP_LOOKAHEAD = 14

TRUNCATE = 1000

Goal:



splunk>

Lab 2: Data Parsing: Guided Steps

Adjust input settings and check results

GUI:

 # Input Settings

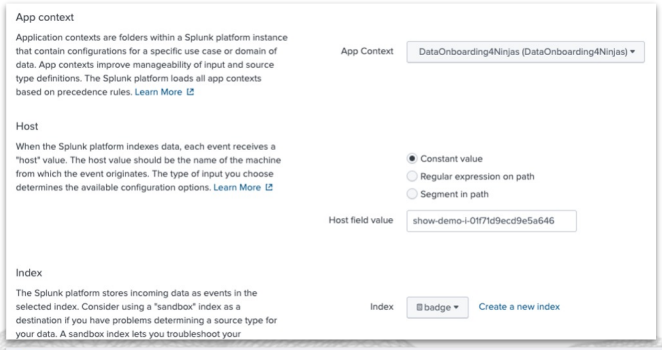
App Context: DataOnboarding4Ninjas

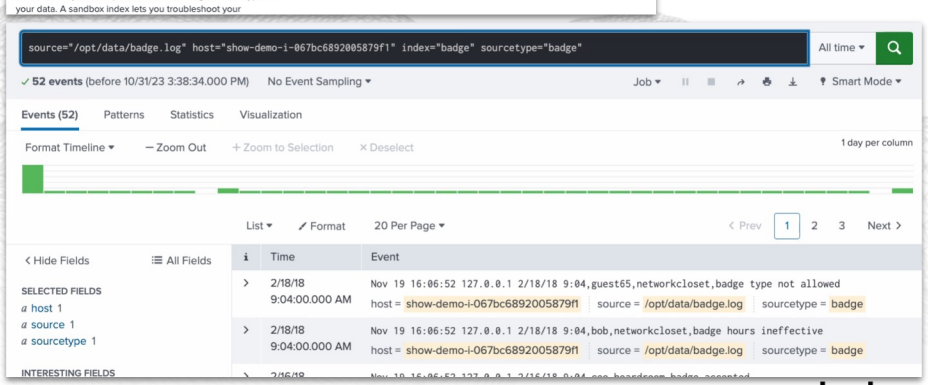
Index: badge

 # Check Results

Start searching after submitting input

Goal:





Lab 2: Data Parsing: Guided Steps

Create an add-on and import the badge source type

GUI:

 # Add-on Builder

Navigate to Apps > Splunk Add-on Builder

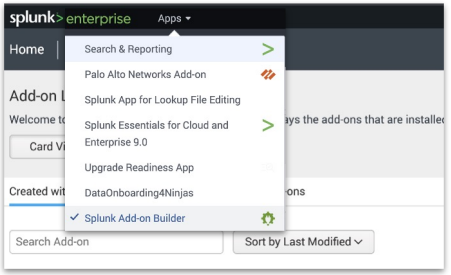
Name a new add-on *badge*

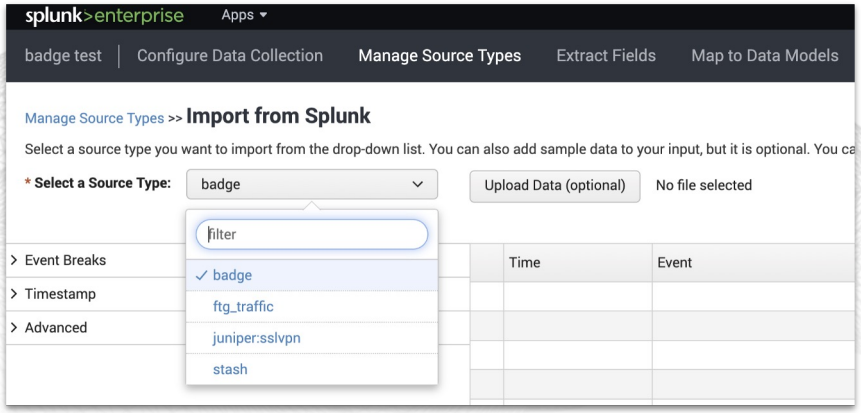
 # Import Source Source type

Navigate to *Manage Source Types*

import *badge* source type from splunk

Goal:





splunk>

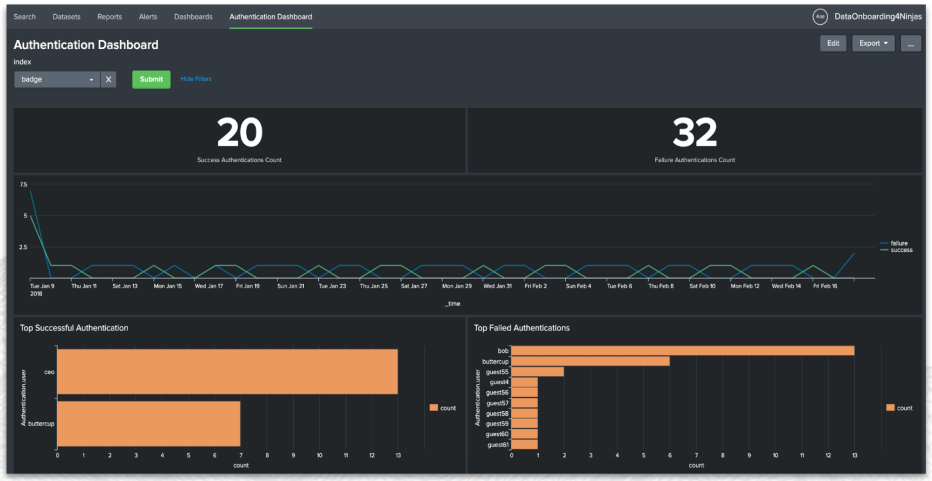
Lab 3: Field Extraction and CIM Compliance

Extract the new fields and make your data CIM compliant

Activities:

1. Extract new fields: employee, door, result
2. Apply badge data to the CIM “Authentication” data model
3. Display the badge data on the “Authentication Dashboard” in the “DataOnboarding4Ninjas” app

Goal:



splunk>

Break for Lab 3

splunk>

Lab 3: Field Extraction and CIM: Guided Steps

Verify the Authentication Dashboard does not populate

Authentication Dashboard:

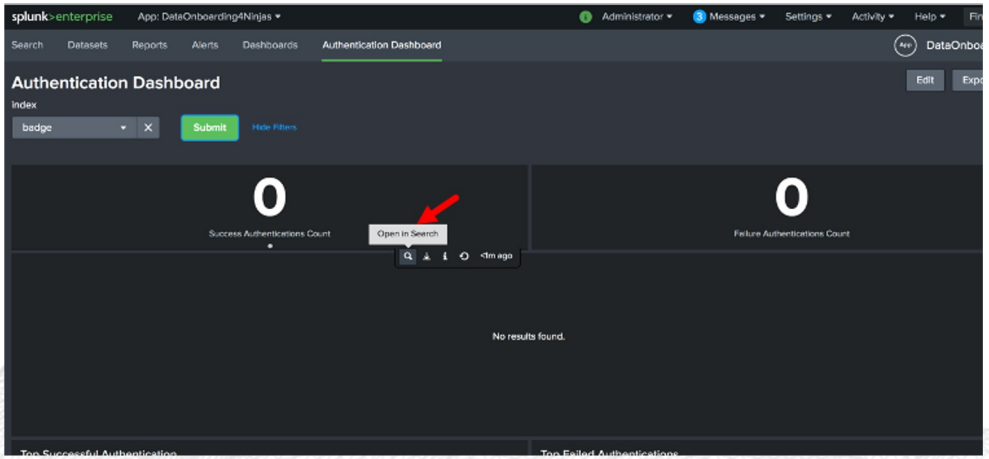
 # Check the Authentication Dashboard

It will not populate

 # WHY?

We need CIM compliant data!

Goal:



splunk>

Lab 3: Field Extraction and CIM: Guided Steps

Extract new fields

Add-on Builder GUI:

 # Extract Fields

Go to Extract Fields in the badge add-on

 # Structure your data

Choose Assisted Extraction

Table Format

Comma Separation

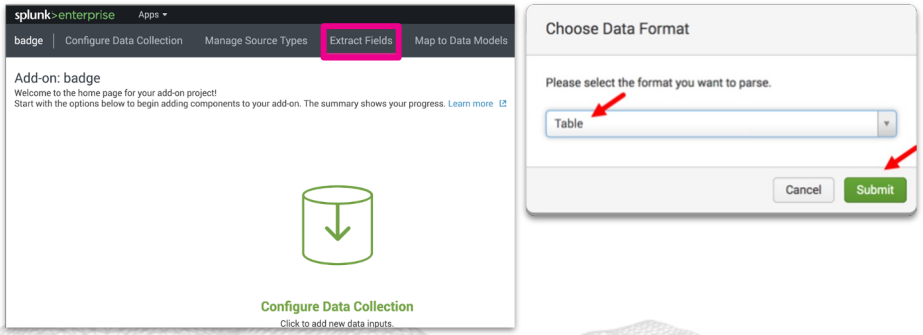
 # Name your fields

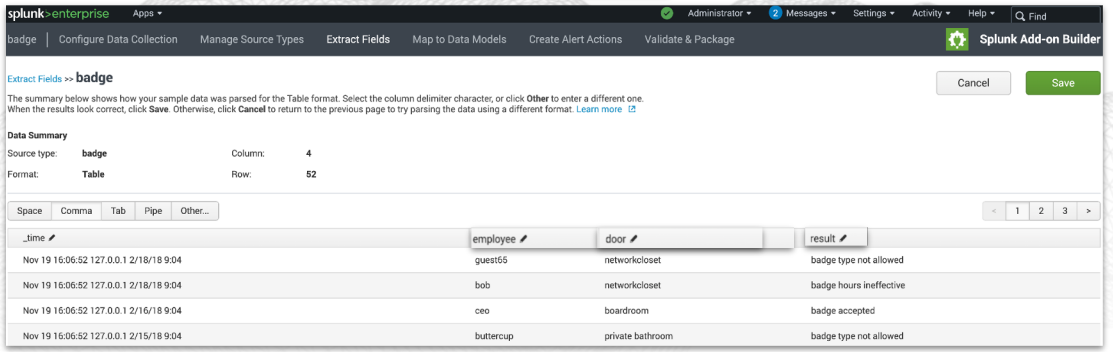
field_1 = employee

field_2 = door

field_3 = result

Goal:





splunk>

Lab 3: Field Extraction and CIM: Guided Steps

Map to the Authentication Data Model

Add-on Builder GUI:

 # Map to Data Models

Go to Map to Data Models in the badge add-on

 # Define the Event Type

Event type name: badge_data

Source type: badge

Search: (sourcetype=badge)

 # Select your Data Model

Splunk_SA_CIM

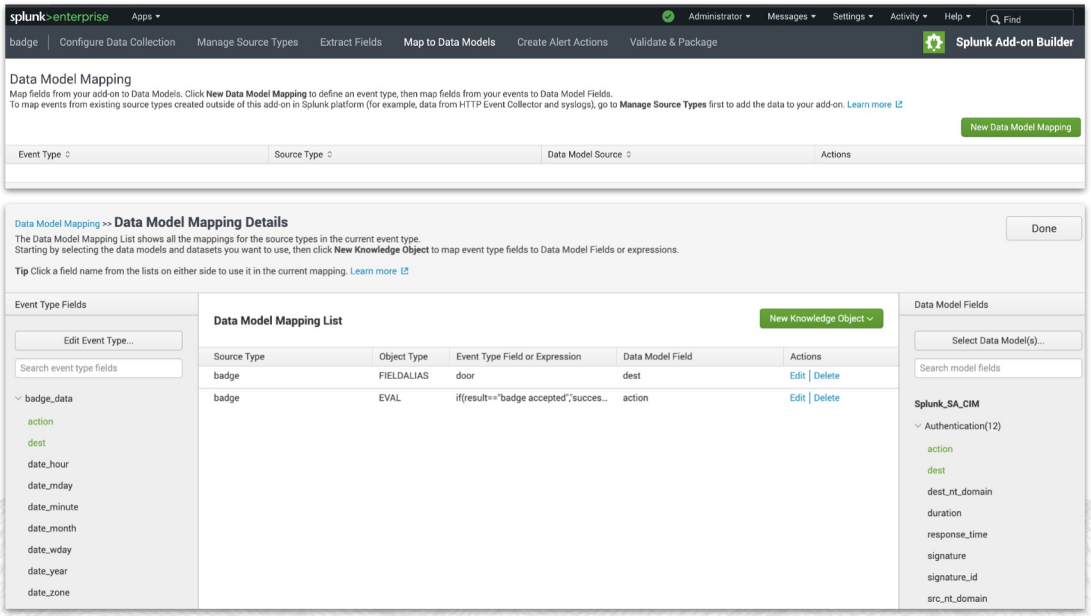
Authentication

 # Create a Field Alias and Eval

Field Alias mapping door to dest

Eval mapping result to success/failure

Goal:



Lab 3: Field Extraction and CIM: Guided Steps

Accelerate and view your dashboard

GUI:

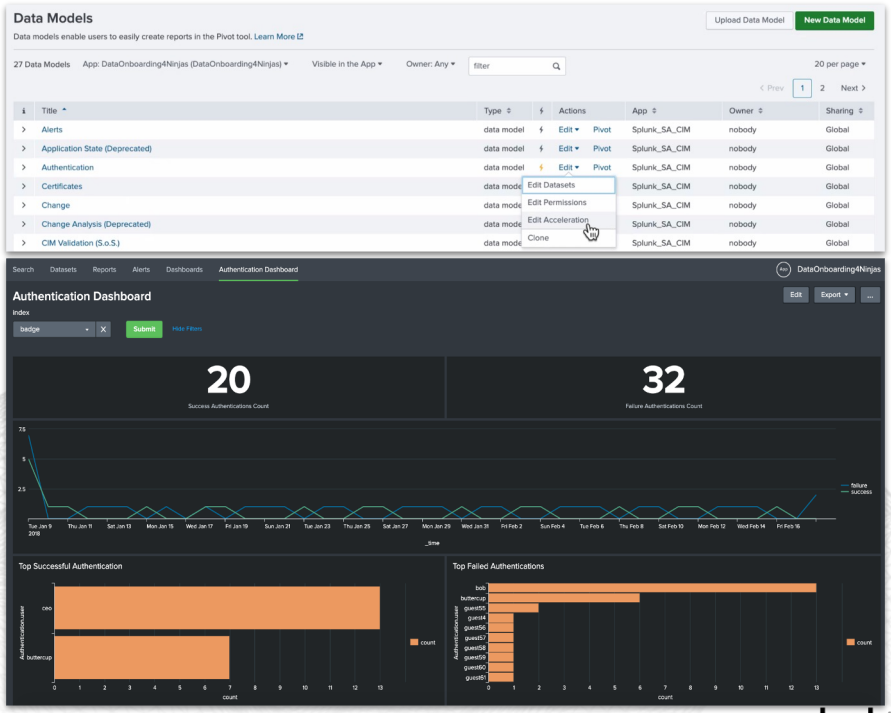
 # Accelerate your Data Models

- Navigate to Settings > Data Models
- Edit the Authentication Data Model
- Restart the Acceleration

 # View your dashboard

- Back in the DataOnboarding4Ninjas App

Goal:



splunk>

What Happens Next?

splunk>

Additional Resources

Want more details?

Content

Splunk .conf session recordings: conf.splunk.com
- SEC1423A - To Data Model or Not to Data Model...
- FN1402 - Best Practises for Forwarder Hierarchies

Splunk Education and Training: education.splunk.com
- Free online courses
- Virtual instructor-led classes

This **slide deck**: splk.it/S4N-DataOnboarding

Help

Splunk Documentation: docs.splunk.com
- Getting Data In, Forwarding Data

Data Onboarding Cheat Sheet
- aplura.com/cheatsheets

Splunk Lantern: lantern.splunk.com

Community: community.splunk.com

Developer: dev.splunk.com

splunk>

Splunk Events

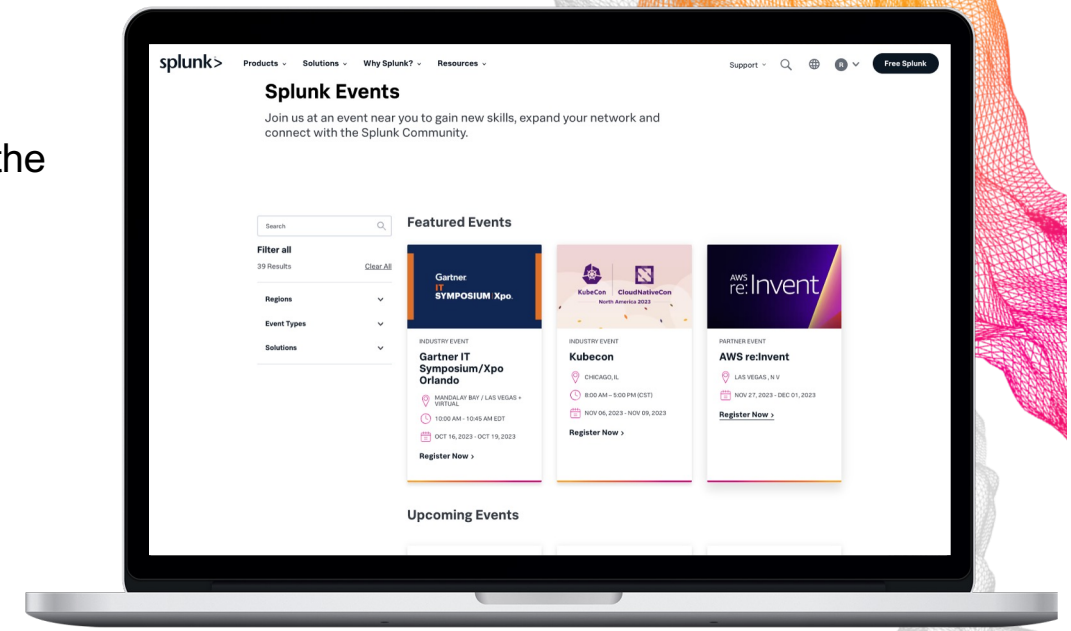
https://events.splunk.com

- Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

- Join us at .conf24!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



splunk>

Thank You