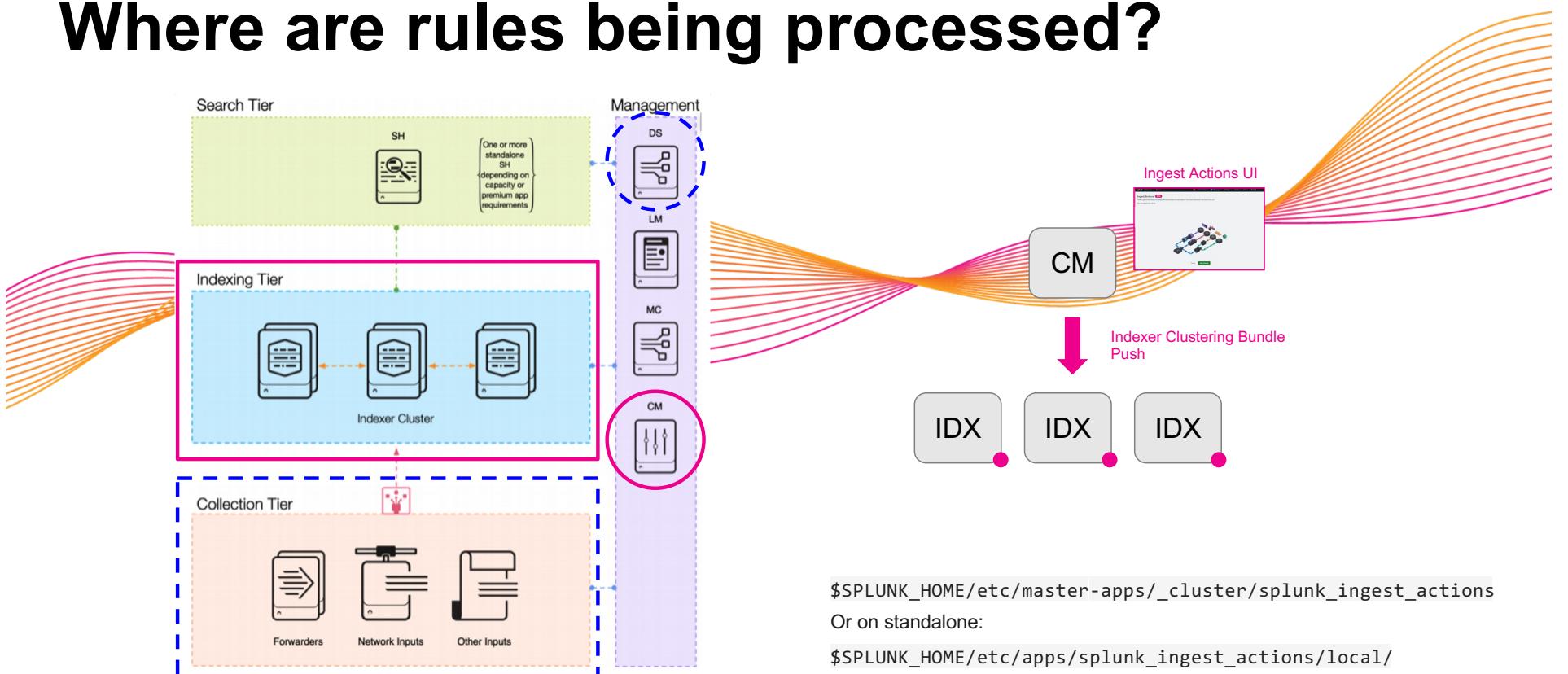


Where are rules being processed?



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)

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

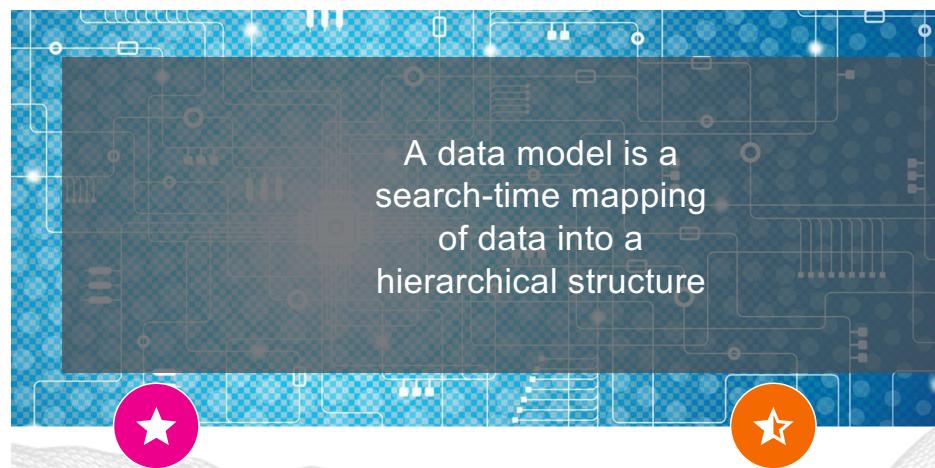
splunk>

Data Models

Standardize your data

splunk®

What are Data Models?



A collection of objects

That have constraints and attributes

JVM
JVM

- Alerts
- Application State
- Authentication
- Certificates
- Databases
- Data Loss Prevention
- Email
- Interprocess Messaging
- Intrusion Detection
- Inventory

- Java Virtual Machines
- Malware
- Network Resolution (DNS)
- Network Sessions
- Network Traffic
- Performance
- Ticket Management
- Updates
- Vulnerabilities
- Web

Building
Library

Where child objects inherit those constraints and attributes

splunk>

Why Use Data Models?

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>

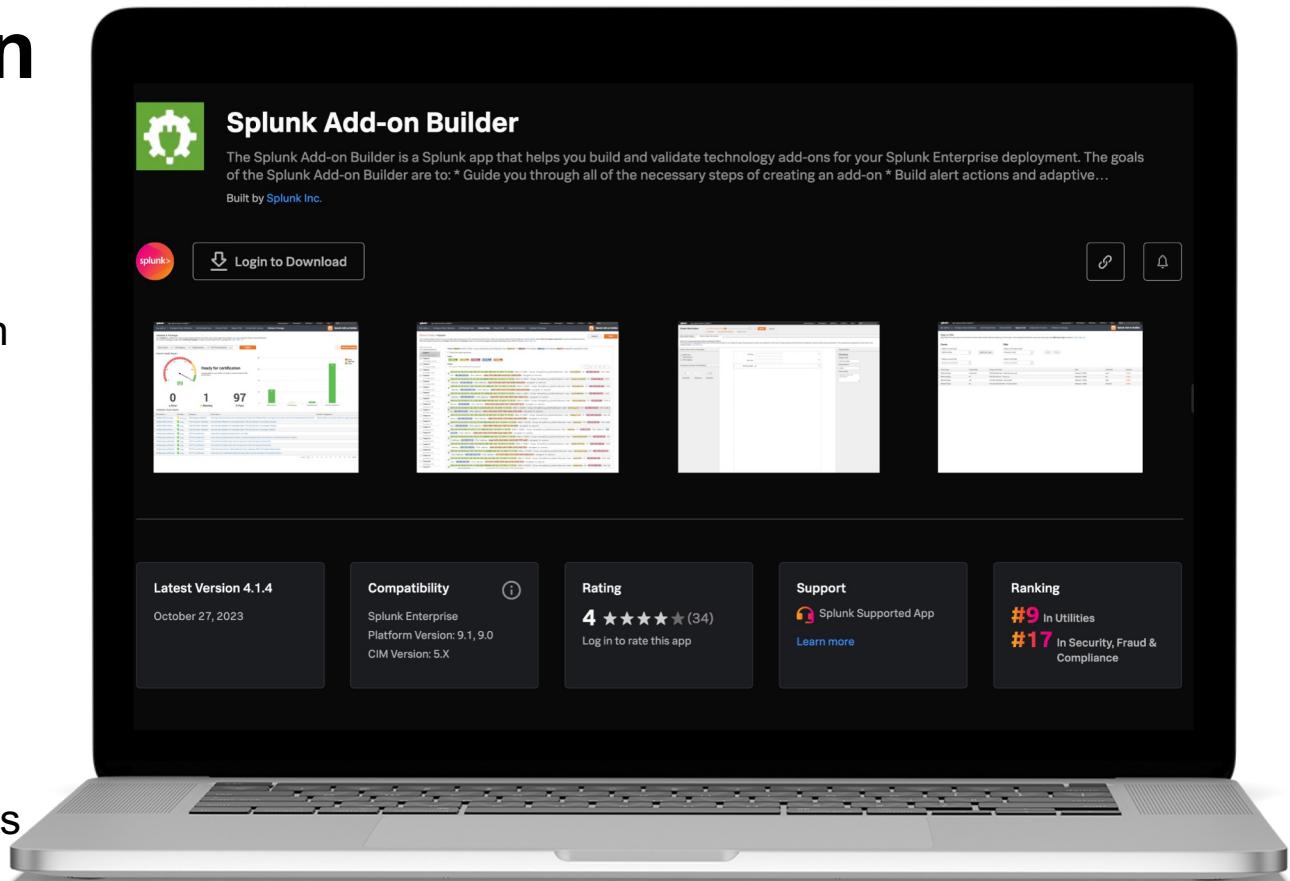


Splunk Add-on Builder

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.



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
 - o Each device has a dedicated folder
2. Adjust input settings
 - o host to match the folder name
3. Confirm Input

Goal:

Review

Input Type Directory Monitor
 Source Path /opt/data/syslog
 IncludeList N/A
 ExcludeList N/A
 Source Type ftg_traffic
 App Context DataOnboarding4Ninjas
 Host Source path segment number: 4
 Index firewall



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:

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More [\[?\]](#)

File or Directory [Browse](#)

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www0/var/log.

Input Settings
Optionally set additional input parameters for this data input as follows:

Source type
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type	<input type="button" value="Automatic"/> <input type="button" value="Select"/> <input type="button" value="New"/>
Source Type Category	<input type="button" value="Custom"/> [?]
Source Type Description	

App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More [\[?\]](#)

App Context	<input type="button" value="DataOnboarding4Ninjas (DataOnboarding4Ninjas)"/> [?]
-------------	--

Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More [\[?\]](#)

Host	<input type="radio"/> Constant value <input type="radio"/> Regular expression on path <input checked="" type="radio"/> Segment in path
Segment number	<input type="text" value="4"/> [?]

Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More [\[?\]](#)

Index	<input type="button" value="firewall"/> [?] <input type="button" value="Create a new index"/>
-------	---

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

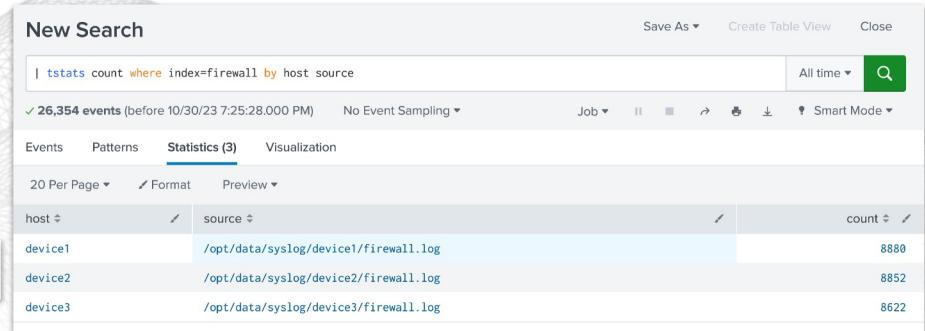
```
| tstats count where index=firewall by host source
```

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:

Review

Input Type File Monitor
 Source Path /opt/data/badge.log
 Continuously Monitor No, index once
 Source Type badge1
 App Context DataOnboarding4Ninjas
 Host show-demo-i-01f71d9ecd9e5a646
 Index badge

Source Type Name	Input Name	Events	Parsed Format	Actions
badge	-	52	(Unparsed Data)	Edit Delete

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:

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ?

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

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:

The goal is to collect and parse badge data from a log file named /opt/data/badge.log. The data consists of event logs with various fields and timestamps. The goal is to define a source type for this data and then use it to parse the logs correctly.

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /opt/data/badge.log

Event Breaks

Time Event

1 1/9/18 4:06:52,000 PM ##Nov 19 16:00:52 127.0.0.1 1/9/18 9:02,buttercup,front_badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 1:06:52 127.0.0.1 1/9/18 9:02,ceo,private_bathroom,badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 9:03,bob,netwrcloset,badge_hours_ineffectiv##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,guest4,netwrcloset,badge_type_not_allowed##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,buttercup,conference,badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,ceo,private_bathroom,badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,bob,netwrcloset,badge_hours_ineffectiv##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,guest56,netwrcloset,badge_type_not_allowed##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,buttercup,conference,badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,ceo,private_bathroom,badge_accepted##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,bob,netwrcloset,badge_hours_ineffectiv##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,guest55,netwrcloset,badge_type_not_allowed##Nov 19 16:00:52 127.0.0.1 1/9/18 9:04,buttercup,private_bathroom,badge_accepted

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /opt/data/badge.log

Advanced

Name	Value
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

New setting

Copy to clipboard

Apply settings

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:

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context: DataOnboarding4Ninjas (DataOnboarding4Ninjas)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Host field value: show-demo-i-0ff7d9ecd9e5a646

Constant value
Regular expression on path
Segment in path

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your

Index: badge

Create a new index

source="/opt/data/badge.log" host="show-demo-i-067bc6892005879f1" index="badge" sourcetype="badge"

52 events (before 10/31/23 3:38:34.000 PM) No Event Sampling

Events (52) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

1 day per column

List Format 20 Per Page < Prev 1 2 3 Next >

Time	Event
2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,guest65,networkcloset,badge type not allowed host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,bob,networkcloset,badge hours ineffective host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
2/16/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,one,beardedcom,badge accepted

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

splunk>



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:

Source Type	Time	Event
Event Breaks		
Timestamp		
Advanced		
Time		
Event		

splunk>



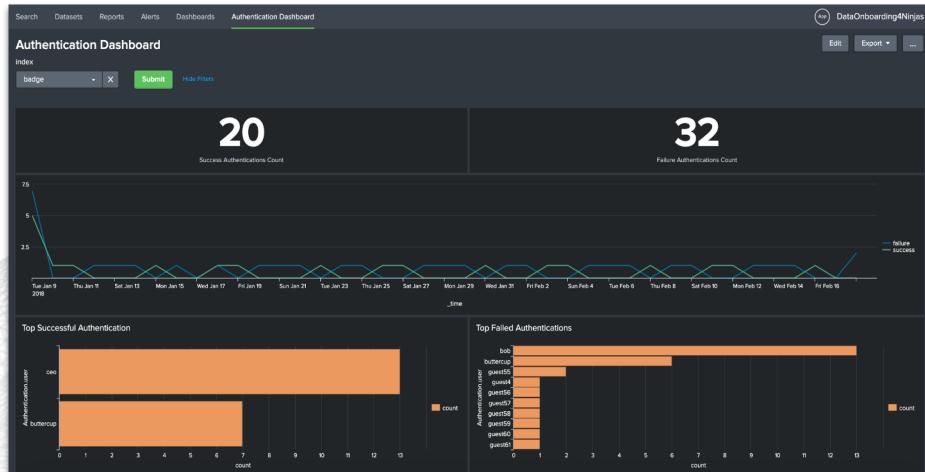
Lab 3: Field Extraction and CIM Compliance

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:



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:

The screenshot shows the Splunk Authentication Dashboard. At the top, there's a search bar with 'badge' typed in, a 'Submit' button, and a 'Hide Filters' link. Below the search bar, there are two large numerical displays: '0' under 'Success Authentications Count' and another '0' under 'Failure Authentications Count'. Underneath each '0' is a small button labeled 'Open In Search'. A red arrow points to the 'Open In Search' button under the 'Success Authentications Count'. At the bottom of the dashboard, it says 'No results found.'

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:

Please select the format you want to parse.

Table

Cancel Submit

_time	employee	door	result
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	guest65	networkcloset	badge type not allowed
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	bob	networkcloset	badge hours ineffective
Nov 19 16:06:52 127.0.0.1 2/16/18 9:04	ceo	boardroom	badge accepted
Nov 19 16:06:52 127.0.0.1 2/15/18 9:04	buttercup	private bathroom	badge type not allowed

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:

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
badge	FIELDALIAS	door	dest	Edit Delete
badge	EVAL	if(result=="badge accepted","success_","failure_") action		Edit Delete

splunk>



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:

Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More [More](#)

27 Data Models App: DataOnboarding4Ninjas (DataOnboarding4Ninjas) • Visible in the App • Owner: Any • filter Q

Type	Actions	App	Owner	Sharing
data model	Edit ▾ Pivot	Splunk_SA_CIM	nobody	Global
data model	Edit ▾ Pivot	Splunk_SA_CIM	nobody	Global
data model	Edit ▾ Pivot	Splunk_SA_CIM	nobody	Global
data model	Edit Datasets	Splunk_SA_CIM	nobody	Global
data mode	Edit Permissions	Splunk_SA_CIM	nobody	Global
data mode	Edit Acceleration	Splunk_SA_CIM	nobody	Global
data mode	Clone	Splunk_SA_CIM	nobody	Global
data mode	Clone	Splunk_SA_CIM	nobody	Global

Authentication Dashboard

Success authentications count: 20

Failure authentications count: 32

Line chart showing Success authentications count over time from Jan 9, 2018, to Feb 16, 2018. The count starts at approximately 25 and fluctuates between 2 and 5.

Bar charts showing Top Successful Authentication and Top Failed Authentications.

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 Events

<https://events.splunk.com>

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



<https://conf.splunk.com>

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

The laptop screen displays the Splunk Events website. The header includes the Splunk logo and navigation links for Products, Solutions, Why Splunk, and Resources. A sidebar on the left provides filtering options for Search, Filter all (39 Results), Clear All, Regions, Event Types, and Solutions. The main content area features a "Splunk Events" section with a sub-headline: "Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community." Below this are sections for "Featured Events" and "Upcoming Events". The "Featured Events" section highlights three events: "Gartner IT SYMPOSIUM Xpo Orlando" (Industry Event, Mandalay Bay / Las Vegas, Virtual, Oct 16, 2023 - Oct 19, 2023), "KubeCon + CloudNativeCon North America 2023" (Industry Event, Chicago, IL, Nov 06, 2023 - Nov 09, 2023), and "AWS re:Invent" (Partner Event, Las Vegas, NV, Nov 27, 2023 - Dec 01, 2023). The "Upcoming Events" section lists "KubeCon" (Industry Event, Chicago, IL, Nov 06, 2023 - Nov 09, 2023) and "AWS re:Invent" (Partner Event, Las Vegas, NV, Nov 27, 2023 - Dec 01, 2023). A "Register Now" button is present for each event listing.

Thank You



splunk>