

Splunk4Ninjas - Common Information Model (CIM)

An introduction to Splunk CIM Data Models and
making data CIM compliant

splunk>



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. © 2025 SPLUNK LLC All rights reserved.

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Workshop Agenda

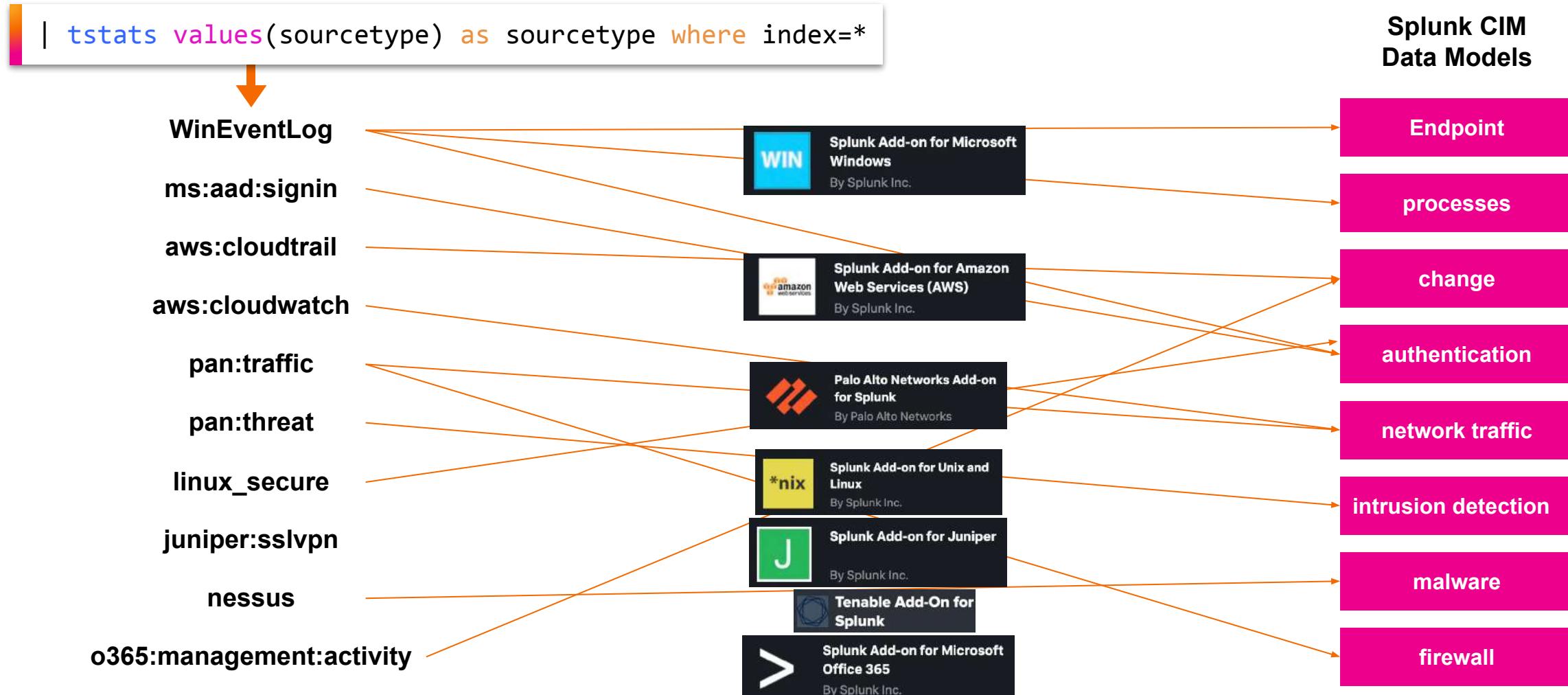
- Overview of Splunk data sources and Splunkbase add-ons roles
- What is the Splunk Common Information Model (CIM)?
- Splunk data models and data model acceleration overview
- CIM compliance process walkthrough
- Hands-on Practice lab exercises: 

Lab 1: Onboarding CIM compliant data (firewall traffic logs) using the FortiGate add-on

Lab 2: Onboarding custom data (badge data) and manually mapping to the CIM Authentication data model

Lab 3: Dashboarding CIM data using the `tstats` command

Overview of Splunk Data Sources



Discover Splunk Apps: <https://splunkbase.splunk.com/>

What's “CIM”?

CIM = Common Information Model

(DTMF's CIM)



Distributed Management Task Force

is a nonprofit industry standards organization that creates open manageability standards.

DTMF's CIM provides a **common definition** of management information for systems, networks, applications and services.

The CIM standard **includes a specification and a schema**, as well as a Metamodel

Learn more: <https://www.dmtf.org/standards/cim>

!= **Splunk's CIM**) = compatibility



The Splunk CIM helps you to **normalize your data to match a common taxonomy** for data from multiple source vendors

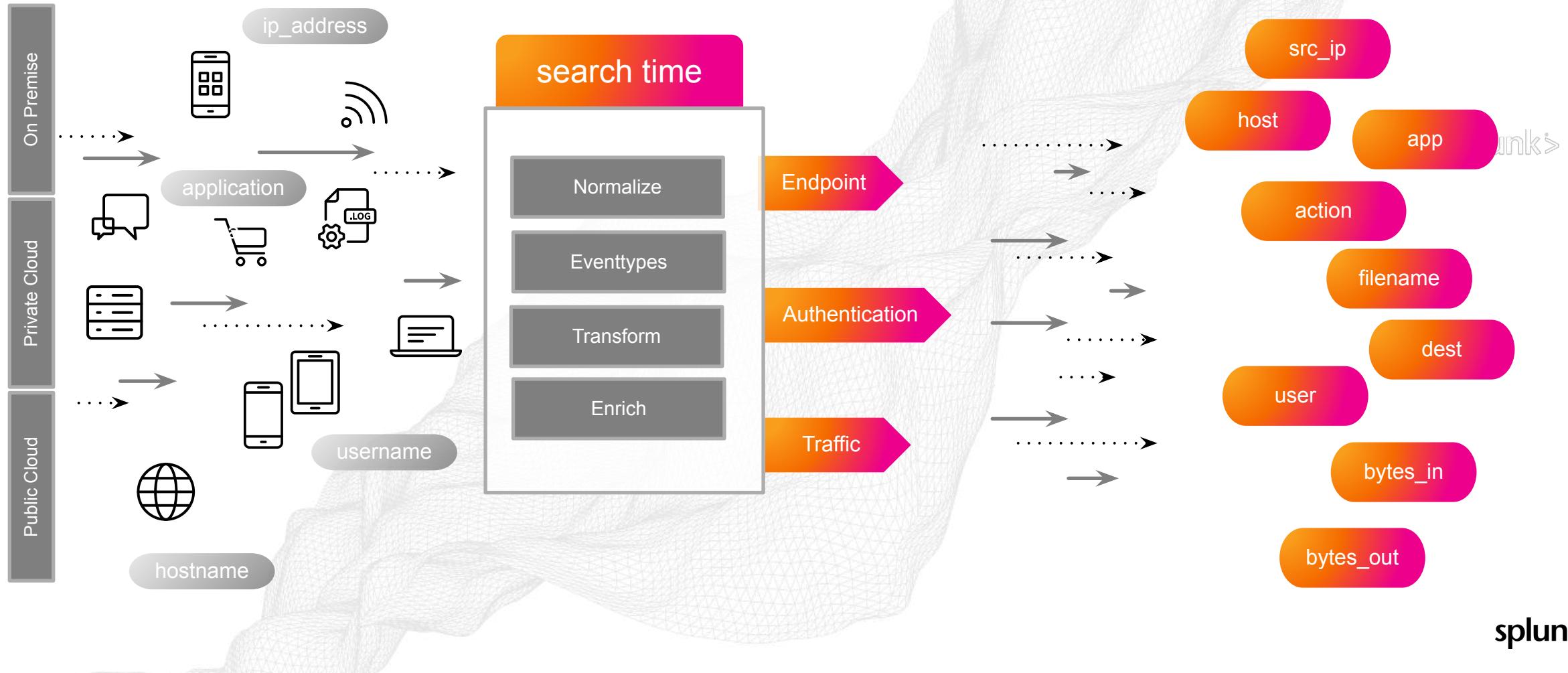
The **Splunk CIM** is packaged as an add-on and comes with **pre-configured data models with a schema** in the form of tables that help you **parse your data at search time**

Learn more:

<https://docs.splunk.com/Documentation/CIM/latest/User/Overview>

Splunk Common Information Model

Normalize fields and events across all data sources





Splunk Common Information Model (CIM)

The What and Why of CIM



CIM: common information model for normalizing data across disparate data sources; allows for **easy correlations**/mapping to data models

<https://docs.splunk.com/Documentation/CIM/latest/User/Overview>

- The CIM helps you to normalize your data to match a common standard, using the **same field names and event tags** for equivalent events from different sources or vendors. The CIM acts as a search-time schema ("schema-on-the-fly") to allow you to define relationships in the event data while leaving the raw machine data intact.
- Normalized data from multiple different source types, allows Splunk users to develop reports, correlation searches, and dashboards to present a **unified view of a data domain**.
- The Splunk Common Information Model add-on **is packaged with Splunk Enterprise Security**.
- The app can be downloaded/installed from here: <https://splunkbase.splunk.com/app/1621>

Why Splunk CIM?

Common taxonomy: Simpler searches

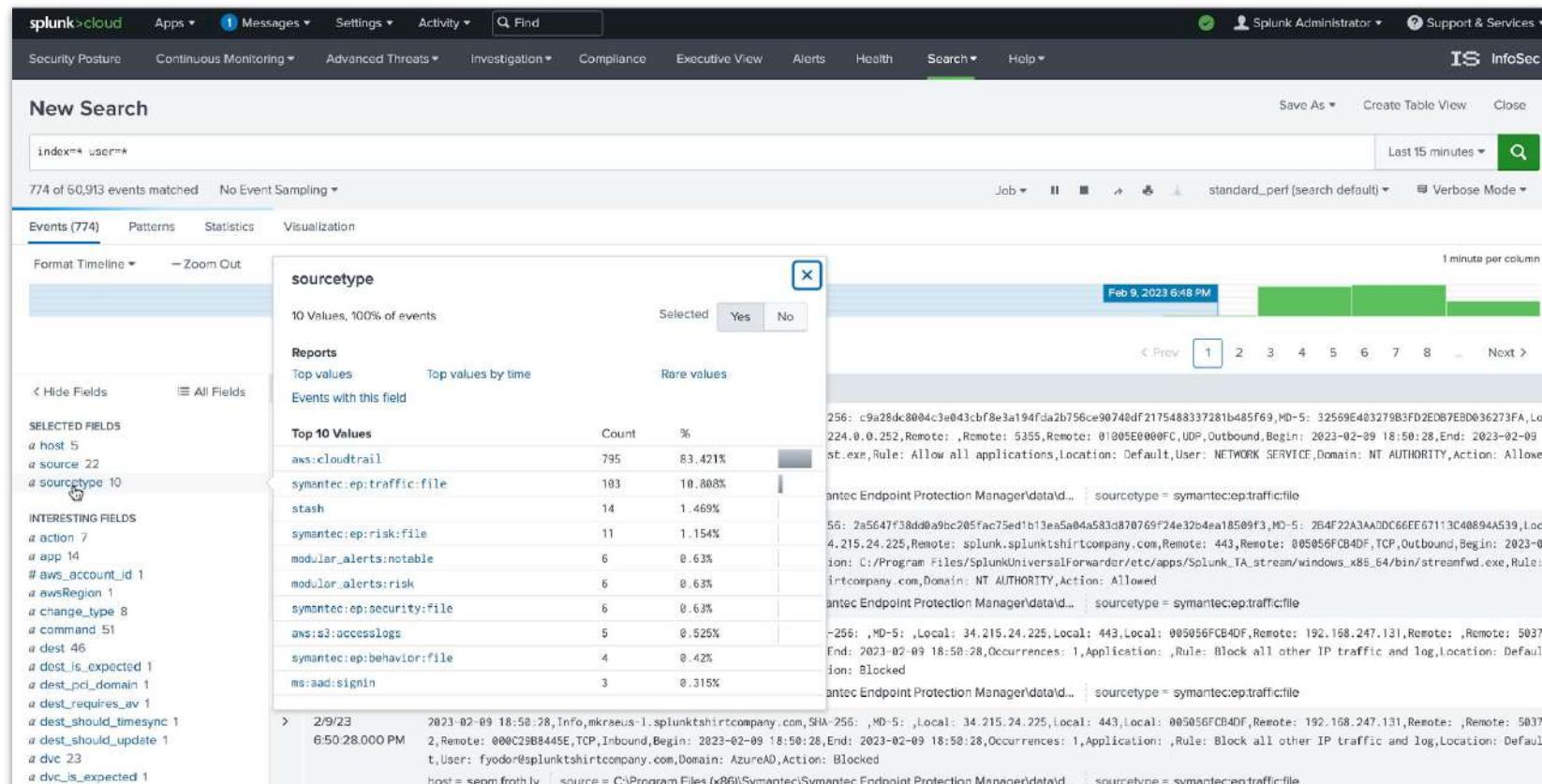
`index=* user=*`

vs

`index=* (Username=* OR username=* OR user_name=* OR user_=*)`

Splunk CIM Authentication
 data model → **user** to identify
 an entity using a particular
 system, the “user.”

Cisco ASA → **Username**
 WinEventLog → **userName**
 Linux Secure → **user_name**
 Duo → **username**



Why Splunk CIM?

Searching the data model automatically correlates multiple data sources

The screenshot shows the Splunk CIM interface with a search bar at the top containing the query `| datamodel Authentication search`. Below the search bar, it displays 80,754 events from March 22, 2023, to March 23, 2023, with no event sampling applied. The interface includes tabs for Events (80,754), Patterns, Statistics, and Visualization, with the Events tab selected. Below the tabs are buttons for Format Timeline, Zoom Out, Zoom to Selection, and Deselect.

A modal window titled "sourcetype" is open, showing a table of values. The table has columns for Values, Count, and %. The data is as follows:

Values	Count	%
WinEventLog	75,661	93.693%
oracle:audit:xml	3,184	3.943%
oracle:audit:unified	1,026	1.27%
XmlWinEventLog	481	0.596%
oracle:audit:text	363	0.45%
aws:cloudtrail	25	0.031%
audittrail	14	0.017%

The modal also includes sections for Reports (Top values, Top values by time, Rare values) and Events with this field. On the left side of the interface, there are sections for Selected Fields (host 100+, source 6, sourcetype 7, highlighted with a pink box and cursor), Interesting Fields (Authentication.action 3, Authentication.app 6, Authentication.dest 100+, #Authentication.is_Default_Authentication 2, #Authentication.is_Failed_Authentication 2, #Authentication.is_Insecure_Authentication 2), and a status message at the bottom: HOST = 127.0.0.1 | source = /var/app/oracle/admin/orcl/adump/orcl_m001_2.

Why Splunk CIM?

Faster and more performant searches: data models can be accelerated

Searching against an **accelerated data model**:

```
| tstats summariesonly=true distinct_count(Authentication.user) from datamodel=Authentication by sourcetype
```

 Takes **0.6 seconds** to run

vs searching against the **index**:

```
index=* sourcetype=wineventlog | stats dc(userName) as count by sourcetype
| append
[ search index=* sourcetype=cisco:asa | stats dc(Username) as count by sourcetype
| append
[ search index=* sourcetype=linux_secure | stats dc(user_name) as count by sourcetype
| append
[ search index=* sourcetype=duo | stats dc(username) as count by sourcetype ] ] ]
```

 Takes **over 65 seconds** to run (<100x)

Intro to (CIM) Data Models

What is a data model?

- A data model is a **hierarchically structured search-time mapping** of your data, and can be composed by one or more datasets.

What is data model acceleration?

- It is a Splunk **feature** used to **speed up data models** that represent extremely large datasets
- Using searches that query accelerated Data Models in dashboards improves search performance
- When enabled, it will create a *summary* table with the key=value pairs
- Searches against a data model that is accelerated, e.g.

```
| tstats summariesonly=true from datamodel=Malware...
```

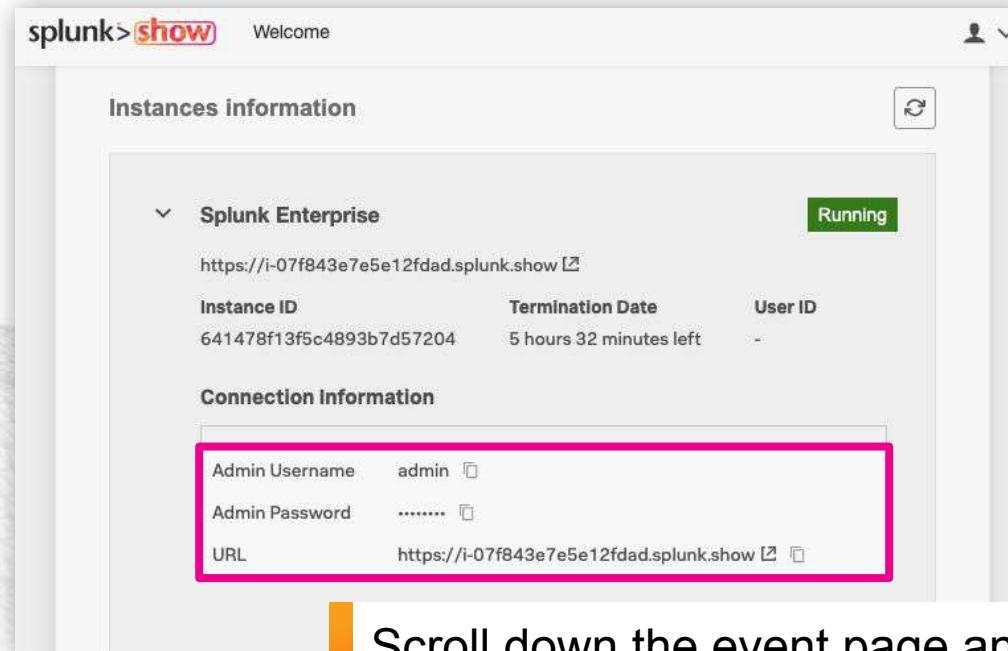
will search against the *summary* table, and will run faster.

- Requires index whitelisting
- This is set up in the CIM add-on



Task 2: Log in to Splunk

Locate your instance URL and credentials
in the Splunk Show event
<https://show.splunk.com>



The screenshot shows the Splunk Show event page. In the 'Instances information' section, there is a collapsed 'Splunk Enterprise' item. When expanded, it reveals the following details:

- Instance URL: <https://i-07f843e7e5e12fdad.splunk.show>
- Instance ID: 641478f13f5c4893b7d57204
- Termination Date: 5 hours 32 minutes left
- User ID: -

In the 'Connection Information' section, the Admin Username ('admin') and URL ('https://i-07f843e7e5e12fdad.splunk.show') are highlighted with a pink box.

Scroll down the event page and
expand the **Splunk Enterprise**
section to view your login
details

Log in to your Splunk instance



The screenshot shows the Splunk instance login page. The URL is 'splunk>enterprise'. It features a 'Username' field containing 'admin', a 'Password' field with a masked password, and a green 'Sign In' button. The background of the page is filled with a dark, grainy texture of log data.

Login using the credentials
from Splunk Show



Task 3: Explore the CIM add-on

Explore CIM Set up, view objects, and explore CIM data models under settings

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Common Information Model	Splunk_SA_CIM	4.13.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit properties View objects View details on Splunkbase

Learn more:

<https://docs.splunk.com/Documentation/CIM/latest/User/Howtousethesreferencetables>

<https://docs.splunk.com/Documentation/CIM/latest/User/CIMfields>

<https://docs.splunk.com/Documentation/CIM/latest/User/Authentication>

Index whitelisting
acceleration settings

splunk>

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

KNOWLEDGE

- Searches, reports, and alerts
- Data models**
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management

USERS AND AUTHENTICATION

- Access controls
- Tokens

Add Data

Explore Data

Monitoring Console

Data Models

Data models enable users to easily create reports in the

27 Data Models App: Search & Reporting (search) ▾

i	Title
>	Alerts
>	Application State (Deprecated)
>	Authentication (highlighted)
>	Certificates
>	Change
>	Change Analysis (Deprecated)
>	CIM Validation (S.o.S.)
>	Data Loss Prevention
>	Databases
>	Email
>	Endpoint
>	Interprocess Messaging
>	Intrusion Detection
>	Inventory
>	JVM
>	Malware
>	Network Resolution (DNS)
>	Network Sessions
>	Network Traffic

Authentication

Authentication

< All Data Models

⚠ This object has no explicit index constraint. Consider adding one for better performance.

Datasets Add Dataset ▾

EVENTS

Authentication

- Failed Authentication
- Successful Authentication
- Default Authentication
 - Failed Default Authentication
 - Successful Default Authentication
- Insecure Authentication
- Privileged Authentication
 - Failed Privileged Authentication
 - Successful Privileged Authentication

CONSTRAINTS

(cim_Authentication_indexes) tag=authentication NOT (action=success user="\$")

Bulk Edit ▾

INHERITED

_time		Time
<input type="checkbox"/> host		String
<input type="checkbox"/> source		String
<input type="checkbox"/> sourcetype		String

EXTRACTED

<input type="checkbox"/> dest_bunit		String
<input type="checkbox"/> dest_category		String
<input type="checkbox"/> dest_nt_domain		String
<input type="checkbox"/> dest_priority		String
<input type="checkbox"/> duration		Number
<input type="checkbox"/> response_time		Number
<input type="checkbox"/> signature		String
<input type="checkbox"/> signature_id		String
<input type="checkbox"/> src_bunit		String
<input type="checkbox"/> src_category		String
<input type="checkbox"/> src_nt_domain		String
<input type="checkbox"/> src_priority		String
<input type="checkbox"/> src_user_bunit		String



Task 4: Explore the data model using SPL

Explore the data model's data sets and schema in json format using the Search app

| datamodel "Authentication"

New Search

1 | datamodel Authentication

✓ 1 event (8/7/23 8:00:00.000 AM to 8/8/23 8:57:02.000 AM) No Event Sampling ▾

Save As ▾ Create Table View Close

Last 24 hours ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out ▾ Zoom to Selection ▾ Detailed ▾

1 hour per column

List ▾ Format 20 Per Page ▾

< Hide Fields + Extract New Fields

Time	Event
	{ [-] description: Authentication Data Model displayName: Authentication modelName: Authentication objectNameList: [[-] Authentication Failed_Authentication Successful_Authentication Default_Authentication Failed_Default_Authentication Successful_Default_Authentication Insecure_Authentication Privileged_Authentication Failed_Privileged_Authentication Successful_Privileged_Authentication] objectSummary: { [-] Event-Based: 10 Search-Based: 0 Transaction-Based: 0 } objects: [[-] { [-] calculations: [[-] { [-] calculationID: Authentication_Fillnull_action calculationType: Eval comment: editable: true expression: if(isnull(action) OR action=='','unknown',action) outputFields: [[-] { [-] name: action type: String }] }] }

Learn more:

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Datamodel>



Task 4: Explore the data model using SPL

Explore the data model's data sets' fields in table view using the search app

```
| datamodelsimple type=attributes object=Authentication datamodel=Authentication
```

attribute	lineage
_time	_time
_raw	_raw
source	source
sourcetype	sourcetype
host	host
authentication_method	Authentication.authentication_method
authentication_service	Authentication.authentication_service
dest_bunit	Authentication.dest_bunit
dest_category	Authentication.dest_category
dest_nt_domain	Authentication.dest_nt_domain
dest_priority	Authentication.dest_priority
duration	Authentication.duration
reason	Authentication.reason
response_time	Authentication.response_time
signature	Authentication.signature
signature_id	Authentication.signature_id
src_bunit	Authentication.src_bunit
src_category	Authentication.src_category
src_nt_domain	Authentication.src_nt_domain
src_priority	Authentication.src.priority

Learn more:

https://docs.splunk.com/Documentation/CIM/latest/User/UsetheCIMtovalidateyourdata#Use_the_datamodelsimple_command

Practice Lab





Lab 1: GDI CIM-compliant Data

CIM-compliant Add-on from Splunkbase

Fortinet FortiGate Firewall Traffic Logs

splunk>

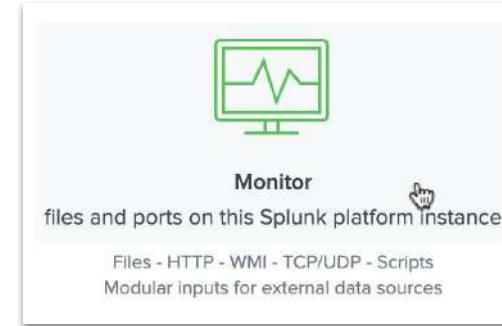
LAB 1



Task 5: Ingest Fortinet Traffic Logs

1. Create a monitoring input for firewall.log

The screenshot shows the Splunk web interface. The top navigation bar includes 'Administrator', 'Messages', 'Settings' (which is highlighted with a pink box), 'Activity', 'Help', and 'Find'. On the left, there's a sidebar with icons for 'Explore Data', 'Monitoring Console', and several sections: KNOWLEDGE (Searches, reports, and alerts, Data models - highlighted with a pink box, Event types, Tags, Fields, Lookups, User interface, Alert actions, Advanced search, All configurations), SYSTEM (Server settings, Server controls, Health report manager, Instrumentation, Licensing, Workload management), and USERS AND AUTHENTICATION (Access controls, Tokens). A large orange arrow points from this screen to the next one.



This screenshot shows the 'Add Data' configuration page for a file-based modular input. The title is 'Add Data' with a progress bar. The first step, 'Select Source', is active. The 'File & Directories' section is highlighted with a red oval. Below it, there's a note about monitoring files and directories. The 'File or Directory' field contains '/opt/data/syslog' (also highlighted with a red oval), with a 'Browse' button next to it. A note below says 'Data preview will be skipped, it is not supported for directories.' The 'Input Settings' tab is selected, showing fields for 'Whitelist' and 'Blacklist', both marked as optional.

This screenshot shows a 'Select source' dialog box. It displays a hierarchical tree of log file paths under the 'data' directory. Under 'syslog', three devices are listed: 'device1', 'device2', and 'device3', each with its own 'firewall.log' file. Other log files like 'badge.log', 'splunk.log', and 'splunkd.log' are also visible. At the bottom right are 'Cancel' and 'Select' buttons. A large orange arrow points from the 'Add Data' screen to this dialog.

splunk>



Task 5: Ingest Fortinet Traffic Logs

2. Create a monitoring input for firewall.log

Add Data Select Source Input Settings Review Done < Back Review >

Input Settings

Optionaly 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.

Automatic **Select** New
fortigate_traffic

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 Search & Reporting (search) *

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](#)

Constant value
 Regular expression on path
 Segment in path
Host field value ip-172-31-21-113.eu-west-1.compute.inte

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 **firewall** * Create a new index



Task 5: Ingest Fortinet Traffic Logs

3a. Check your data!

```
index="firewall" sourcetype="fortigate_traffic"
```

New Search Save As ▾ Create Table View Close

All time Search

✓ 17,474 events (before 3/28/23 4:21:52.000 PM) No Event Sampling ▾ Job ▾

Events (17,474) Patterns Statistics Visualization Verbose Mode ▾

Format Timeline ▾ – Zoom Out + Zoom to Selection ✖ Deselect 1 second per column



List ▾ ✖ Format 20 Per Page ▾ ◀ Prev 1 2 3 4 5 6 7 8 ... Next >

◀ Hide Fields	☰ All Fields	i Time	Event	
SELECTED FIELDS		> 11/20/18 6:08:59.000 PM	Nov 20 18:08:59 device3 date=2015-08-11 time=19:19:43 devname=device3 devid=FG800C3912801080 logid=0004000017 type=traffic subtype=sniffer level=notice vd=root srcip=208.91.115.10 srcport=60832 srcintf="port1" dstip=74.125.170.175 dstport=443 dstintf="port1" sessionid=12512 proto=17 action=accept policyid=1 dstcountry="United States" srccountry="United States" trandisp=snat transip=0.0.0.0 transport=0 service="udp/443" duration=10 sentbyte=202281 rcvbyte=3089 sentpkt=0 rcvdpkt=0 appcat="unscanned" devtype="Windows PC" osname="Windows" osversion="7" mastersrcmac=00:09:0f:97:ef:e4 srcmac=00:09:0f:97:ef:e4 host = Domane-Demo-i-030d03b04fa3cc549 source = /opt/data/syslog/device3/firewall.log sourcetype = fortigate_traffic	
INTERESTING FIELDS		> 11/20/18 6:08:59.000 PM	Nov 20 18:08:59 device3 date=2015-08-11 time=19:19:43 devname=device3 devid=FG800C3912801080 logid=0004000017 type=traffic subtype=sniffer level=notice vd=root srcip=208.91.115.12 srcport=62176 srcintf="port1" dstip=161.202.72.147 dstport=1194 dstintf="port1" sessionid=3364 proto=17 action=accept policyid=1 dstcountry="Japan" srccountry="United States" trandisp=snat transip=0.0.0.0 transport=0 service="udp/1194" duration=46 sentbyte=187792 rcvbyte=17758 sentpkt=0 rcvdpkt=0 appcat="unscanned" devtype="Windows PC" osname="Windows" osversion="7" mastersrcmac=00:09:0f:97:ef:e4 srcmac=00:09:0f:97:ef:e4	



Task 5: Ingest Fortinet Traffic Logs

3b. Another method to check your data!

| `datamodel Network_Traffic search`

New Search

Save As ▾ Create Table View Close

All time ▾

✓ 26,354 events (before 3/29/23 10:41:53.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (26,354) Patterns Statistics Visualization

Format Timeline ▾ 1 second per column

List ▾ 20 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	☰ All Fields	i Time	Event
SELECTED FIELDS		11/20/18 1:08:59.000 PM	Nov 20 18:08:59 device3 date=2015-08-11 time=19:19:43 devname=device3 devid=FG800C3912801080 logid=0004000017 type=traffic subtype=sniffer level=notice vd=root srcip=208.91.115.10 srcport=60832 srcintf="port1" dstip=74.125.170.175 dstport=443 dstintf="port1" sessionid=12512 proto=17 action=accept policyid=1 dstcountry="United States" srccountry="United States" trandisp=snat transip=0.0.0.0 transport=0 service="udp/443" duration=10 sentbyte=202281 rcvbyte=3089 sentpkt=0 rcvdpkt=0 appcat="unscanned" devtype="Windows PC" osname="Windows" osversion="7" mastersrcmac=00:09:0f:97:ef:e4 srcmac=00:09:0f:97:ef:e4 host = Domane-Demo-i-0f469783f321c6313 source = /opt/data/syslog/device3/firewall.log sourcetype = fortigate_traffic
INTERESTING FIELDS		11/20/18 1:08:59.000 PM	Nov 20 18:08:59 device3 date=2015-08-11 time=19:19:43 devname=device3 devid=FG800C3912801080 logid=0004000017 type=traffic subtype=sniffer level=notice vd=root srcip=208.91.115.12 srcport=62176 srcintf="port1" dstip=161.202.72.147 dstport=1194 dstintf="port1" sessionid=3364 proto=17 action=accept policyid=1 dstcountry="Japan" srccountry="United States" trandisp=snat transip=0.0.0.0 transport=0 service="udp/1194" duration=46 sentbyte=187792 rcvbyte=17758 sentpkt=0 rcvdpkt=0 appcat="unscanned" devtype="Windows PC" osname="Windows" osversion="7" mastersrcmac=00:09:0f:97:ef:e4 srcmac=00:09:0f:97:ef:e4 host = Domane-Demo-i-0f469783f321c6313 source = /opt/data/syslog/device3/firewall.log sourcetype = fortigate_traffic



Task 6: Accelerate the Network_Traffic Data Model in CIM

1. Set the data model's indexes

1. Click on **Settings**

2. Click on **Advanced search**

3. Click on **Search macros**

4. Filter by the **cim_Network_Traffic_indexes** macro

cim_Network_Traffic_indexes

Advanced search > Search macros > cim_Network_Traffic_indexes

Definition *

Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: \$arg1\$

Use eval-based definition?



Task 6: Accelerate the Network_Traffic Data Model in CIM

2. Edit the data model's acceleration settings

1. Browse to the Data models settings

2. Click Edit Acceleration for the Network Traffic data model

Edit Acceleration

Data Model **Network Traffic**

Accelerate Acceleration may increase storage and processing costs.

Summary Range ? **3 Months**

Advanced Settings

Change the following settings only if you are experiencing summary creation issues. [Learn More](#)

Backfill Range ? **Match Summary Range**

Max Summarization Search Time ? **1 Hour**

Maximum Concurrent Summarization Searches ? **3**

Poll Buckets For Data To Summarize ?

Summarization Period ? **1-56/5 ******
Examples: */5 ****, */30 **** [Learn More](#)

Automatic Rebuilds ?

Cancel **Save**



Task 7: Search for Traffic...

So...what's the difference between...?

```
index=firewall sourcetype="fortigate_traffic" | stats count
```

```
| datamodel Network_Traffic search | stats count
```

```
| tstats count from datamodel=Network_Traffic
```

```
| tstats summariesonly=true count from datamodel=Network_Traffic
```

CIM Compliance

How do we do it ?

1

**Get the right CIM
fields/values**



2

**Create an
eventtype to
regroup our
events**



3

**Tag our
eventtypes**

Learn more:

<https://docs.splunk.com/Documentation/CIM/latest/User/UsetheCIMtonormalizedataatsearchtime>

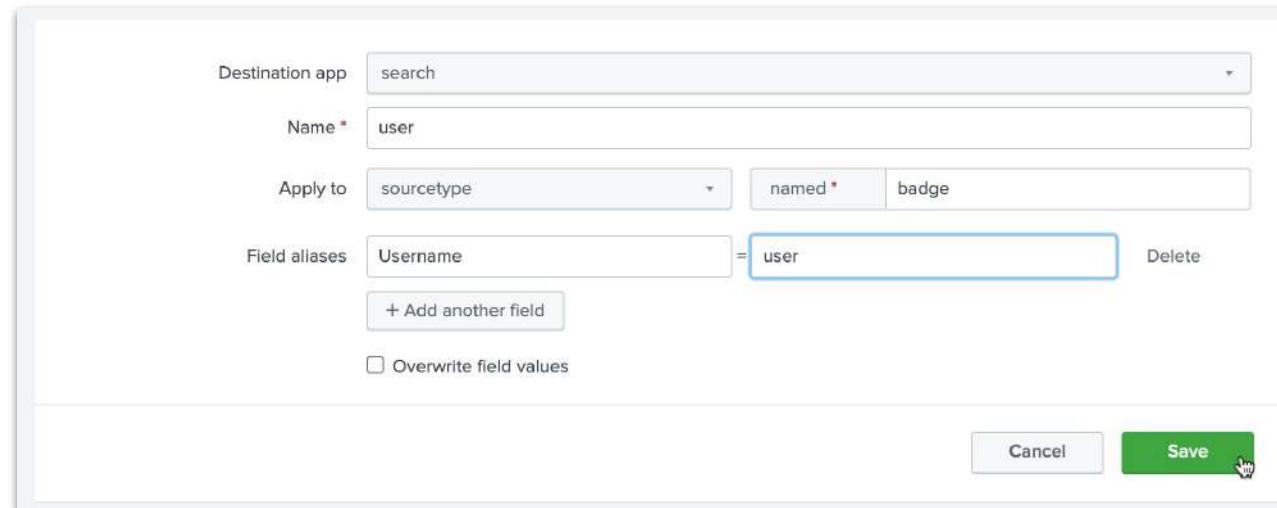
CIM Compliance

Get the right CIM fields/values

My field name is different?



Use field alias: **Settings > Fields > Field Alias**



props.conf →

```
[badge]
FIELDALIAS-user = Username as user
```

splunk>

CIM Compliance

Get the right CIM fields/values

I don't have this field in my event



Use calculated fields: **Settings > Fields > Calculated Field**

The screenshot shows the "Calculated Field" configuration interface. The "Destination app" is set to "search". Under "Apply to", "sourcetype" is selected and "named" is checked with the value "fgt_traffic". The "Name" field is set to "vendor_product", described as "Name of the field whose value will be calculated". The "Eval expression" field contains the string "'Fortigate Fortinet Firewall'" with the note "A valid eval expression, e.g. x + 3". At the bottom are "Cancel" and "Save" buttons, with "Save" being highlighted.

props.conf →

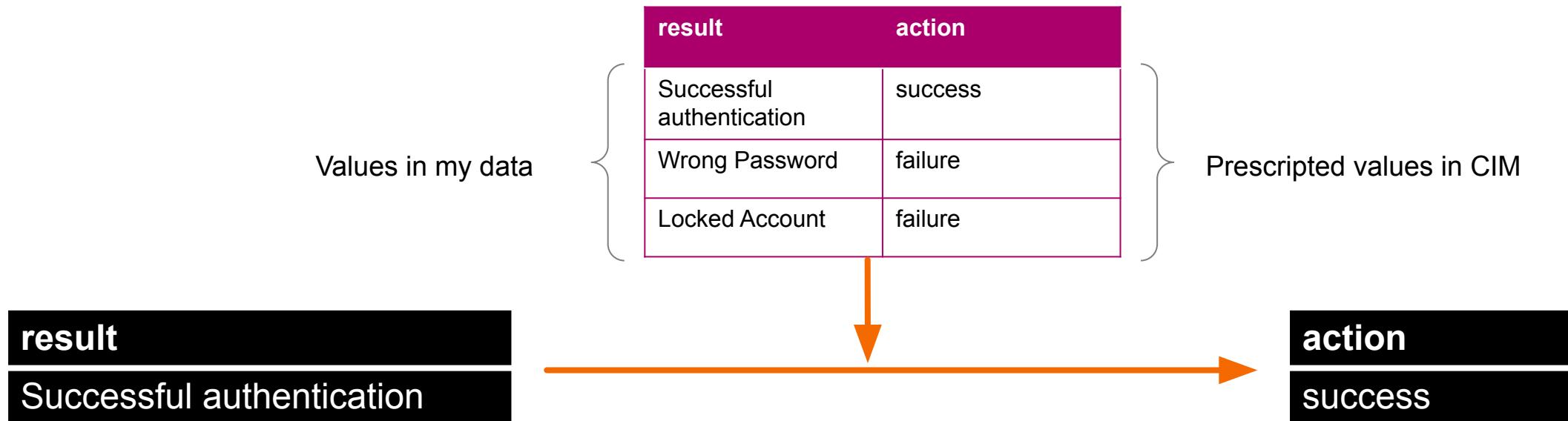
```
[fgt_traffic]
EVAL-vendor_product = "Fortinet Fortigate Firewall"
```

splunk>

CIM Compliance

Get the right CIM fields/values

My field value is not CIM compliant? Use a lookup!



```
<your base search> | lookup result OUTPUTNEW action
```

Need Help ?

Build: Splunk Add-on Builder

<https://splunkbase.splunk.com/app/2962/>

The screenshot shows the Splunk Add-on Builder interface. At the top, there's a navigation bar with links like 'My Add-on', 'Configure Data Collection', 'Add Sample Data', 'Extract Fields', 'Map to CIM', 'Create Alert Actions', 'Validate & Package', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a section titled 'Validate & Package' with a note: 'Click Validate to validate your add-on against best practices and other rules, and to determine whether your app is ready for Splunk App Certification. Your add-on package is ready. Click Download Package to create and download the SPL package file. Learn more'.

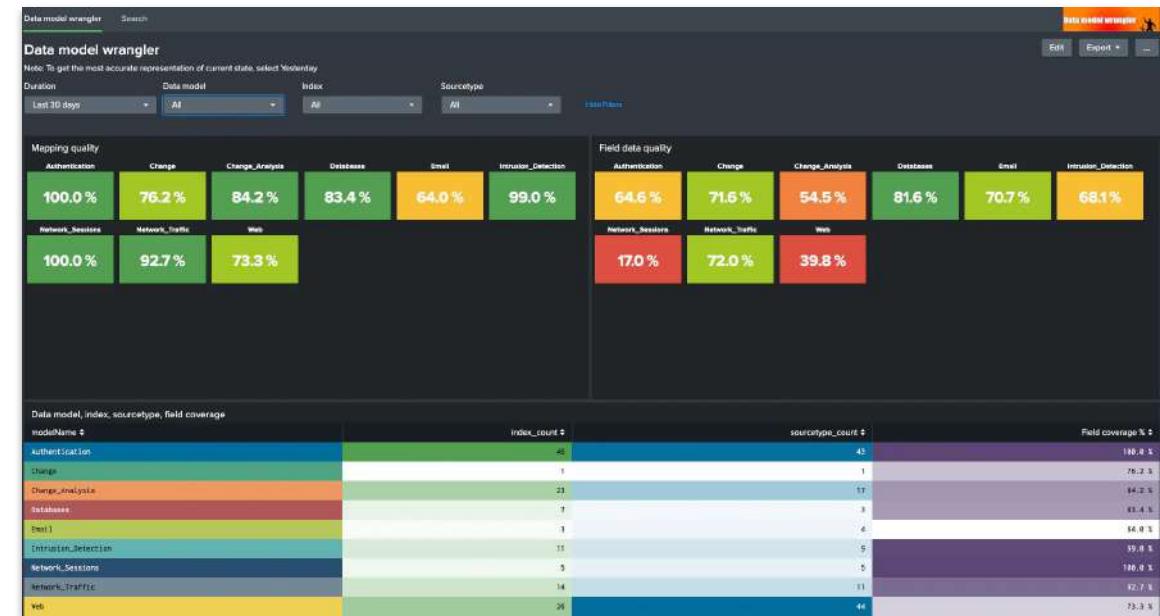
The main area features a large circular 'Overall Health Report' gauge with a scale from 0 to 100. An arrow points to the value '99', which is highlighted in green. Below the gauge, the text 'Ready for certification' is displayed. A bar chart shows the distribution of validation results: 0 Errors (red), 1 Warning (yellow), and 97 Passes (green). To the right of the chart is a single green bar reaching the value 70.

Below these metrics is a table titled 'Validation Rule Details' with 14 rows, each containing a rule name, severity, category, description, and a 'Solution Suggestion' column. For example, the first row is 'Validate field coverage' with a yellow warning icon, 'CIM Mapping Validation', and the description 'Coverage of the "[network, communicate] action" field in the "MyEventType" event type is 0.0, which is lower than the threshold value of 0.6. Check whether you should add more regular expression'.

At the bottom of the page, there are navigation links: '< prev 1 2 3 4 5 6 7 8 9 10 next >'.

Validate: Data Model Wrangler

<https://splunkbase.splunk.com/app/6286/>



Practice Lab





Lab 2: GDI Badge Data

Custom “badge” sourcetype

Create a custom app for the “badge” sourcetype

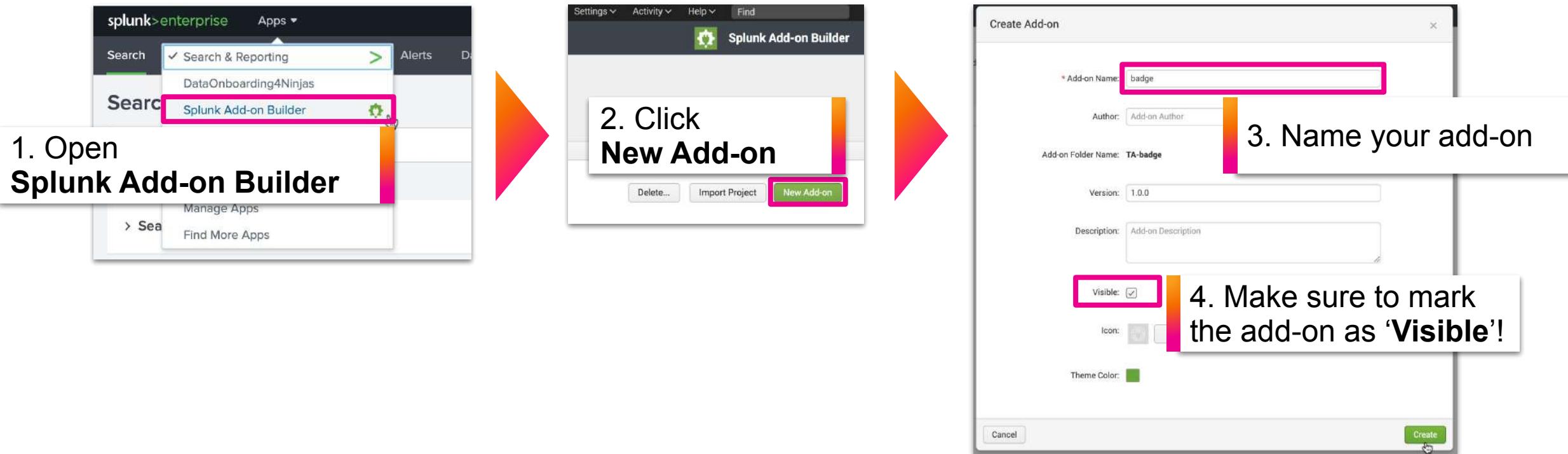


splunk>



Task 8: Create a Custom Add-on

1. Go to the **Splunk Add-on Builder** app. We need to create a custom add-on for the new custom sourcetype



LAB 2



Task 9: Add Badge Data

2. Click on **Settings > Add Data > Monitor > File & Directories (index once)**

1. Click on **Settings**
2. Click on **Add Data**
3. Click on **Monitor**

Settings

- Administrator
- Messages
- Settings**
- Activity
- Help
- Find

KNOWLEDGE

- Searches, reports
- Data models
- Event types
- Tags

Add Data

Report acceleration summaries

Monitor

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

1. Click on **Settings**
2. Click on **Add Data**
3. Click on **Monitor**
4. Select **Files & Directories**
5. Select the location of your badge data
6. Click on **Index Once**

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to receive data via TCP or UDP.

Scripts

Get data from any API, script, or other source.

Splunk Add-on Builder field extraction modular input

Splunk Add-on Builder field extraction modular input

Modular Action Relay

Relay modaction from remote splunk search head.

Splunk Add-on Builder validation modular input

Splunk Add-on Builder validation modular input

/opt/data/badge.log

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

Continuously Monitor

Index Once

Whitelist?

Blacklist?

FAQ

- What kinds of files can the Splunk platform index?
- I can't access the file that I want to index. Why?



Task 9: Add Badge Data

Set a Custom Source Type

splunk>enterprise Apps ▾

Administrator 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

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 [View Event Summary](#)

Source type:	Select Source Type	Save As
<ul style="list-style-type: none">> Event Breaks> Timestamp> Advanced		

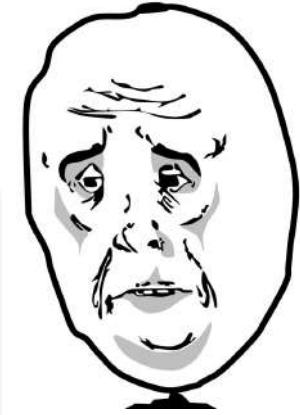
List ▾ Format 20 Per Page ▾

	Time	Event
1	11/19/18 4:06:52.000 PM	##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest55,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,private bathroom,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest55,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/10/18 9:04,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1 1/11/18 9:04,ceo,private bathroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/12/18 9:04,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/13/18 9:04,guest56,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/14/18 9:04,buttercup,private bathroom,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/15/18 9:04,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/16/18 9:04,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,guest57,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1



Task 9: Add Badge Data

Event breaking failed... why ?



Use the Advanced section to edit the sourcetype attributes

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.

Source: /opt/data/badges.log

Event Breaks

Timestamp

Advanced

Name	Value
CHARSET	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n +)
NO_BINARY_CHECK	true

New setting

Copy to clipboard

Apply settings

Format: 20 Per Page ▾

time	Event
11/19/18 4:06:52.000 PM	##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge pted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest55,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,pr e bathroom,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted##Nov 19 06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,t55,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/10/18 9:04,buttercup,conference ,badge pted##Nov 19 16:06:52 127.0.0.1 1/11/18 9:04,ceo,private bathroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/13/18 9:04,guest56,networkclo age type not allowed##Nov 19 16:06:52 127.0.0.1 1/14/18 9:04,buttercup,private bathroom,badge type not allow Nov 19 16:06:52 127.0.0.1 1/15/18 9:04,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/16/18 9:04,b etworkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,guest57,networkcloset,badge type allowed##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0



Task 9: Add Badge Data

3. Set custom source type: Remove the default settings

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

View Event Summary

Event Breaks

Timestamp

Advanced

Name	Value
CHARSET	
SHOULD_LINEMERGE	true
LINE_BREAKER	(\r\n]+)
NO_BINARY_CHECK	true

New setting

Copy to clipboard

Apply settings

Time Event

1 11/19/18 ##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,o,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge 9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,pr #Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,tworkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,allowed##Nov 19 16:06:52 127.0.0.1 1/10/18 9:04,buttercup,conference ,badg pted##Nov 19 16:06:52 127.0.0.1 1/11/18 9:04,ceo,private bathroom,badge accepted##Nov 19 16:06:52 127.0.0.1 18 9:04,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/13/18 9:04,guest56,networkclo adge type not allowed##Nov 19 16:06:52 127.0.0.1 1/14/18 9:04,buttercup,private bathroom,badge type not allow Nov 19 16:06:52 127.0.0.1 1/15/18 9:04,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/16/18 9:04,etworkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,guest57,networkcloset,badge type allowed##Nov 19 16:06:52 127.0.0.1 1/18/18 9:04,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0

Remove CHARSET and NO_BINARY_CHECK



Task 9: Add Badge Data

4. Set custom attributes: Edit **SHOULD_LINEMERGE** and **LINE_BREAKER**

Splunk>enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data Next >

Set Source Type < Back

Select Source Set Source Type Input Settings Review Done

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 View Event Summary

Source type: Select Source Type ▾ Save As

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

	Time	Event
1	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted
2	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted
3		ob,networkcloset,badge hours ineffective
4		uest4,networkcloset,badge type not allowed
5	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted
6	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted

SHOULD_LINEMERGE → false

LINE_BREAKER: → (##)

New setting Apply settings

Copy to clipboard

SHOULD_LINEMERGE → false

LINE_BREAKER: → (##)



Task 9: Add Badge Data

Line breaking is ok...do you notice something weird ?

The screenshot shows the Splunk interface for adding data. The top navigation bar includes 'splunk>enterprise', 'Apps ▾', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below the navigation is a progress bar with five steps: 'Select Source' (green), 'Set Source Type' (green), 'Input Settings' (light gray), 'Review' (light gray), and 'Done' (light gray). Buttons for '< Back' and 'Next >' are at the bottom of the bar.

The main content area is titled 'Set Source Type'. It displays the following text:

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".

Below this text, the 'Source' is set to '/opt/data/badge.log'. On the left, there's a sidebar with 'Event Breaks', 'Timestamp', and 'Advanced' sections. Under 'Advanced', there are two settings: 'SHOULD_LINEMERGE' (Value: false) and 'LINE_BREAKER' (Value: '##'). Buttons for 'Save As' and 'Apply settings' are also present.

The main panel shows a table of events with columns 'Time' and 'Event'. The first event is highlighted with a pink border. The text 'Splunk is using the first timestamp it detected in the raw data' is overlaid on the event table. The event details are as follows:

Time	Event
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted
11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted

On the right side of the event table, there are buttons for 'View Event Summary', 'List ▾', 'View Event Summary', and a page navigation bar with buttons for '< Prev', '1' (selected), '2', '3', and 'Next >'. A watermark text 'Splunk is using the first timestamp it detected in the raw data' is overlaid on the event table.



Task 9: Add Badge Data

The right timestamp is the second one

splunk>enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data ◀ Back Next ▶

Select Source Set Source Type Input Settings Review Done

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

Source type: Select Source Type ▾ Save As

Event Breaks

Timestamp

Advanced

Name	Value
SHOULD_LINEMERGE	false
LINE_BREAKER	(##)

New setting

Copy to clipboard Apply settings

List ▾ Format 20 Per Page ▾

View Event Summary 1 2 3 Next >

But this is the timestamp we actually need

	Time	Event
1	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02 buttercup,front,badge accepted
2	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted
3	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective
4	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed
5	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted
6	11/19/18 4:06:52.000 PM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted

LAB 2



Task 9: Add Badge Data

6. Set custom source type: Add best practice time stamp settings

1. Set the following attributes:

TIME_PREFIX: \d+\.\d+\.\d+\.\d+\s
TIME_FORMAT: %m/%d/%y %H:%M
MAX_TIMESTAMP_LOOKAHEAD: 14
TRUNCATE: 1000

TIME_PREFIX	\d+\.\d+\.\d+\.\d+\s
TIME_FORMAT	%m/%d/%y %H:%M
MAX_TIMESTAMP_LOC	14
TRUNCATE	1000

2. Click on Apply settings

3. Verify that Splunk is now using the second timestamp

4. Click on Next



Task 9: Add Badge Data

7. Set custom source type: Save sourcetype, pick app context & index, & review

1. Name your source type 'badge'

Save Source Type

Name: badge

Description: custom badge data

Category: Custom

App: badge

2. Select the badge app

3. Click on Save

Cancel Save

Add Data

Select Source Set Source Type Input Settings Review Done

Review >

Input Settings

Optionaly set additional input parameters for this data input as follows:

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: badge (TA-badge)

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: Domane-Demo-i-07fb24207ac10a294

Constant value (selected)

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

Index: badge

Create a new index

4. Select the badge index



Task 9: Add Badge Data

8. Check your data with a search:

```
index="badge" sourcetype="badge"
```

Search over All time

All time ▾ Q

New Search

Save As ▾ Create Tab

52 events (before 3/29/23 5:11:23.000 PM) No Event Sampling ▾

Events (52) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × 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 = Domane-Demo-i-0926027bd9fab477e 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 = Domane-Demo-i-0926027bd9fab477e source = /opt/data/badge.log sourcetype = badge
2/16/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/16/18 9:04,ceo,boardroom,badge accepted host = Domane-Demo-i-0926027bd9fab477e source = /opt/data/badge.log sourcetype = badge
2/15/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/15/18 9:04,buttercup,private bathroom,badge type not allowed host = Domane-Demo-i-0926027bd9fab477e source = /opt/data/badge.log sourcetype = badge
2/14/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/14/18 9:04,guest64,networkcloset,badge type not allowed host = Domane-Demo-i-0926027bd9fab477e source = /opt/data/badge.log sourcetype = badge
2/13/18	Nov 19 16:06:52 127.0.0.1 2/13/18 9:04,bob,networkcloset,badge hours ineffective

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
date_hour 1
date_mday 30
date_minute 3
a date_month 2
a date_wday 7
date_year 1
a date_zone 1
a index 1
linecount 1

Dashboards & Reports Best Practices

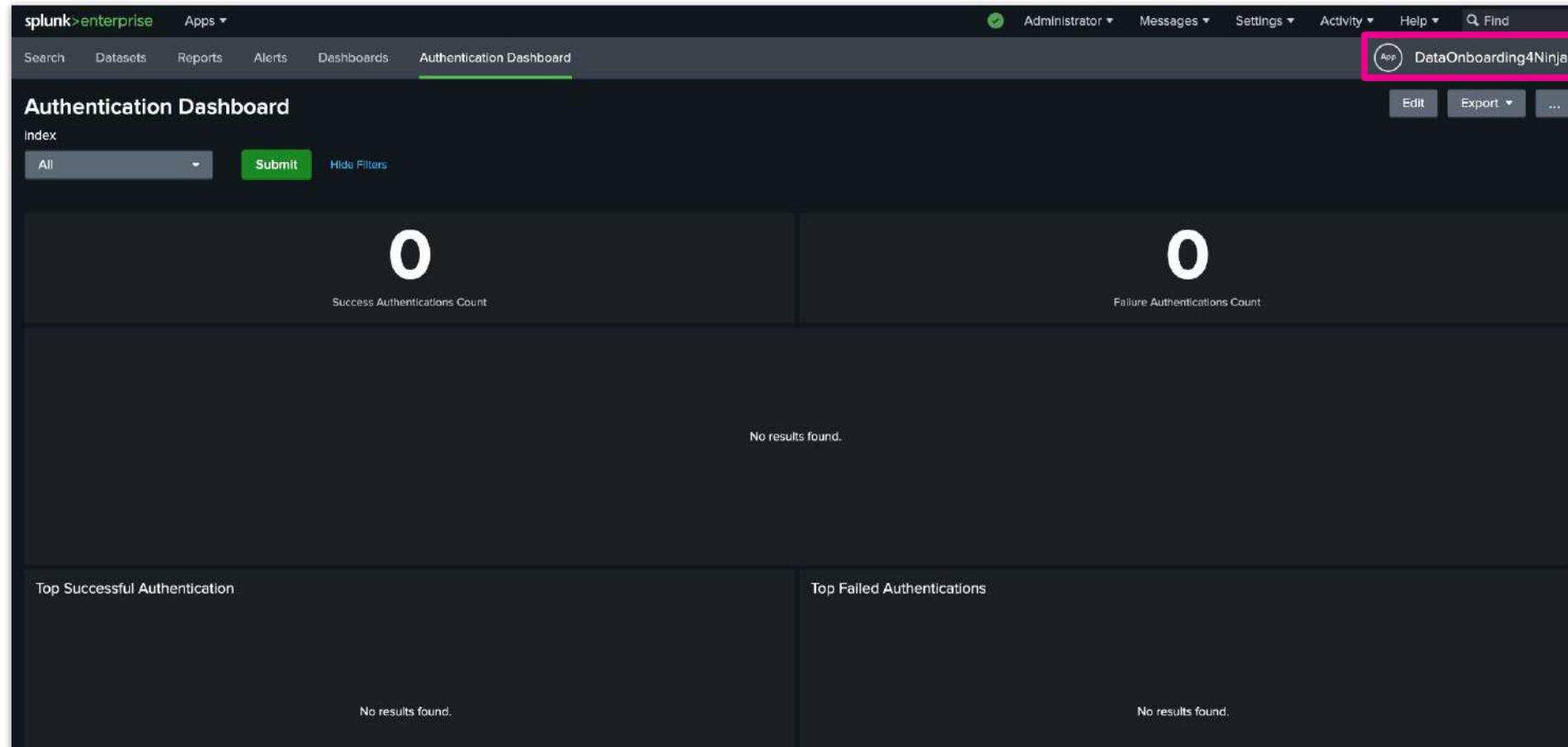
Use SPL queries that search against the data models

- The goal is to understand the data (i.e. extract fields), apply some best practices and make it CIM compliant
- You have already indexed badge system data, can you do reports on it?
- Why?

Final Objective of the Day:

Display Badge Data on the Authentication Dashboard

1. Locate the Authentication Dashboard in the DataOnboarding4Ninjas app



The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation bar, the 'Authentication Dashboard' is selected in the 'Dashboards' menu. On the left, there's a sidebar with 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'Authentication Dashboard' and has a sub-section 'Index'. It features two large numerical displays: 'Success Authentications Count' (0) and 'Failure Authentications Count' (0). Below these counts, it says 'No results found.' In the bottom left, there's a section for 'Top Successful Authentication' which also says 'No results found.'. In the bottom right, there's a section for 'Top Failed Authentications' which also says 'No results found.' On the far right of the dashboard, there are buttons for 'Edit', 'Export', and three dots for more options.

Practice Lab





Lab 3: Create Reports on Badge Data

splunk>



Task 10: Create Reports on Badge Data

1. Go to the DataOnboarding4Ninjas App

The screenshot shows the Splunk interface with the 'splunk>enterprise' logo at the top left. The top navigation bar includes 'App: Search & Reporting ▾'. A dropdown menu is open under 'Search & Reporting', with the 'DataOnboarding4Ninjas' option highlighted by a pink rectangle. Other options in the dropdown include 'Splunk Add-on Builder', 'Manage Apps', and 'Find More Apps'. The main search area on the left has a 'Search' title and a search bar containing 'enter search here'. Below the search bar is a 'No Event Sampling' section. The bottom left contains 'How to Search' and 'Documentation ↗' and 'Tutorial ↗' buttons. The bottom right corner features the 'splunk>' logo.



Task 10: Create Reports on Badge Data

2. Check the Authentication Dashboard

1. Select the badge index

2. Click on Submit

Success Authentications Count

Failure Authentications Count

No results found.

Top Successful Authentication

Top Failed Authentifications



Task 10: Create Reports on Badge Data

3. Choose one panel and click on the Open in Search icon

Nothing is displayed ... why?

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise App: DataOnboarding4Ninjas ▾
- Top Navigation:** Administrator ▾, 3 Messages ▾, Settings ▾, Activity ▾, Help ▾, Find ▾
- Left Sidebar:** Search, Datasets, Reports, Alerts, Dashboards
- Current Dashboard:** Authentication Dashboard
- Search Bar:** index badge ▾ X Submit Hide Filters
- Metrics:** Success Authentications Count (0), Failure Authentications Count (0)
- Bottom Navigation:** Open in Search, Search icon (highlighted with a pink box), Refresh, Help, 1m ago
- Callout:** Click on the search icon (with a pink box highlighting the search icon in the bottom navigation bar).



Task 10: Create Reports on Badge Data

Notice the search. We are doing a query against the Authentication data model

The screenshot shows the Splunk Enterprise interface. The top navigation bar includes 'splunk>enterprise' and 'App: DataOnboarding4Ninjas'. The main menu has tabs for 'Search', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'Authentication Dashboard'. The 'Search' tab is selected. The search bar contains the following query:

```
| tstats summariesonly=f count from datamodel=Authentication.Authentication where index=badge Authentication.action="success"
```

The search results section shows '1 result (before 4/18/19 1:28:52.000 PM)'. The 'Statistics (1)' tab is selected, displaying a single row:

count
0



Task 10: Create Reports on Badge Data

4. Go to the Splunk Add-on Builder app

The screenshot shows the Splunk Enterprise search interface. At the top, the URL is 'splunk>enterprise' and the 'App: Search & Reporting' dropdown is selected. Below the header, there are tabs for 'Search' and 'Database'. A sub-menu is open under 'Search & Reporting' with the following options: 'Search & Reporting' (selected), 'DataOnboarding4Ninjas', 'Splunk Add-on Builder' (highlighted with a red box), 'Manage Apps', and 'Find More Apps'. The main search area has a placeholder 'enter search here'. On the left, there's a section titled 'How to Search' with links to 'Documentation' and 'Tutorial', and a 'Search History' section. On the right, there's a 'What to Search' section with a 'Data Summary' button and the message 'Waiting for data...'. The bottom right corner features the Splunk logo.



Task 10: Create Reports on Badge Data

5. Click on the add-on you created before

The screenshot shows the Splunk Add-on Builder interface. At the top, there's a navigation bar with the Splunk logo, the text "App: Splunk Add-on Builder", and user information like "Administrator". Below the navigation is a header with "Home" and "Configuration" buttons and a gear icon.

The main area is titled "Add-on List" and contains a welcome message: "Welcome to Splunk Add-on Builder. The list below displays the add-ons that are installed on this instance of Splunk Enterprise." There are two view options: "Card View" (selected) and "Table View".

Below the welcome message, there are two tabs: "Created with Add-on Builder" (selected) and "Other apps and add-ons". There are also search and sort filters: "Search Add-on" and "Sort by Last Modified". On the right side of the card list, there are "Delete..." and "Import" buttons.

The list of add-ons includes one item:

Icon	Name	Owner	Last Modified	Actions
	badge	Nabil	2019/04/18	Validate & Package Export Properties

The "badge" row is highlighted with a red border. At the bottom left of the card, it says "V1.0.0".



Task 10: Create Reports on Badge Data

6. Click on Extract fields

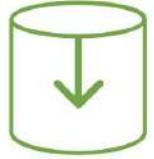
Splunk > App: Splunk Add-on Builder >

badge | Configure Data Collection Manage Source Types Extract Fields Map to Data Models Create Alert Actions Validate & Package

Add-on: badge

Welcome to the home page for your add-on project!

Start with the options below to begin adding components to your add-on. The summary shows your progress. [Learn more](#)

Configure Data Collection
Click to add new data inputs.

Create Alert Actions
Click to create alert actions.

Add-on Summary

Validation Score	Data Inputs	Extracted Fields	Event Types
-	0	0	0



Task 10: Create Reports on Badge Data

7. Click on Assisted Extraction

Field Extraction

Splunk Add-on Builder provides you three ways to build the field extractions.

- **Assisted Extraction.** Splunk Add-on Builder will detect the format of the data and provide you the recommended regex to parse your data.

If you have complex field extractions or field transformations in the existing add-ons which cannot be supported by Splunk Add-on Builder, you can also

- **Manual Extraction.** Configure the field extraction manually in Splunk platform.
- **Manual Transformation.** Configure the field transformation manually in Splunk platform.

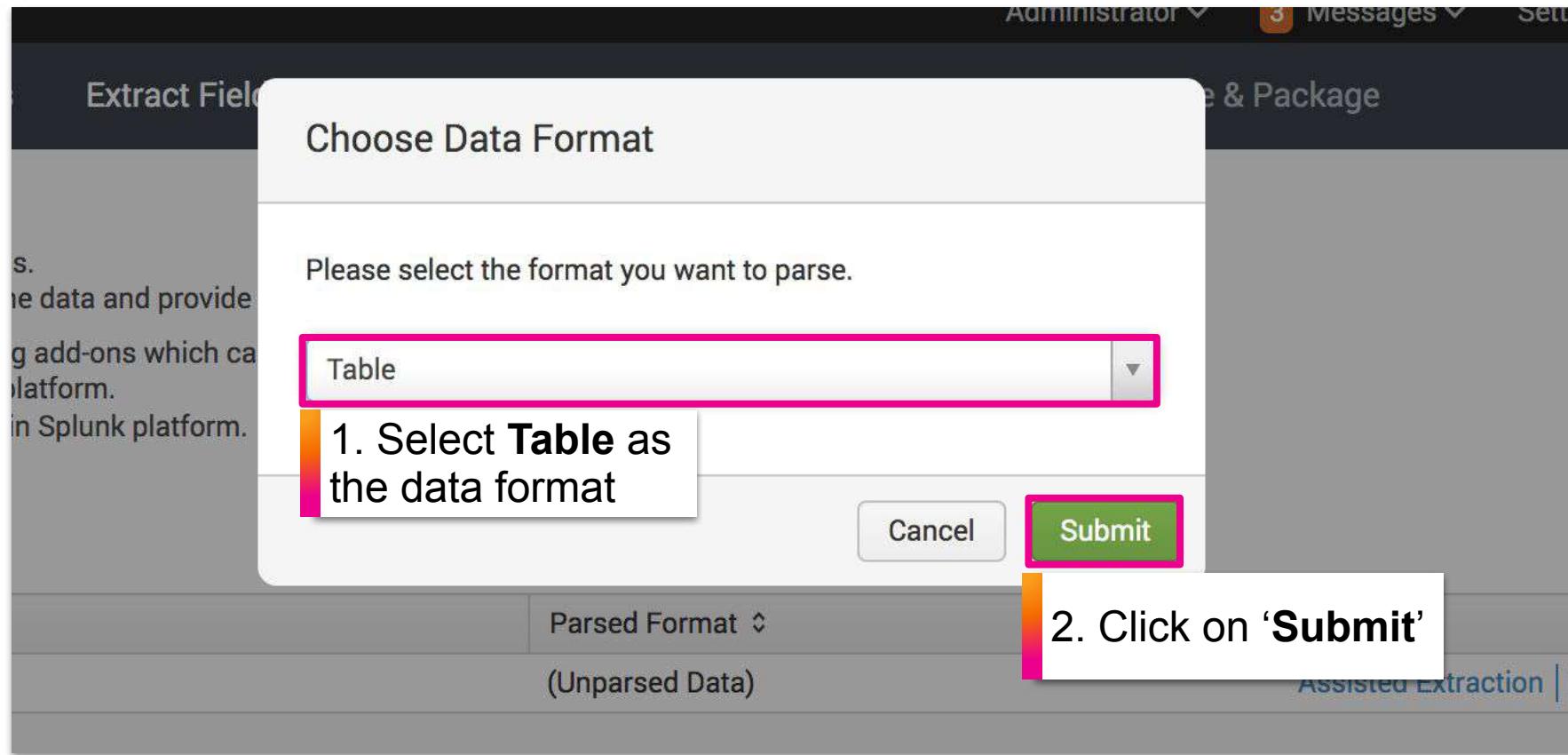
[Learn more](#)

Source Type Name	Events	Parsed Format	Actions
badge	52	(Unparsed Data)	Assisted Extraction Manual Extraction Manual Transformation



Task 10: Create Reports on Badge Data

8. Choose Table and click on Submit





Task 10: Create Reports on Badge Data

9. Choose Comma as the delimiter character

Extract Fields >> badge

The summary below shows how your sample data was parsed for the Table format. Select the column delimiter character, or click Other to enter a different one. When the results look correct, click Save. Otherwise, click Cancel to return to the previous page to try parsing the data using a different format. [Learn more](#)

Data Summary

Source type: badge Column: 10
Format: Table Row: 52

Space Comma Tab Pipe Other... < 1 2 3 >

field_0	field_1	field_2	field_3	field_4	field_5	field_6	field_7	field_8	field_9
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
Nov	19	16:06:52	127.0.0.1	2/14/18	9:04,guest64,networkcloset,badge	type	not	allowed	
Nov	19	16:06:52	127.0.0.1	2/13/18	9:04,bob,networkcloset,badge	hours	ineffective		
Nov	19	16:06:52	127.0.0.1	2/12/18	9:04,ceo,private	bathroom,badge	accepted		
Nov	19	16:06:52	127.0.0.1	2/11/18	9:04,buttercup,conference	,badge	accepted		
Nov	19	16:06:52	127.0.0.1	2/10/18	9:04,guest63,networkcloset,badge	type	not	allowed	

Cancel Save



Task 10: Create Reports on Badge Data

10. Rename the fields: user, door, result

splunk > App: Splunk Add-on Builder >

Administrator > 3 Messages > Settings > Activity > Help > Find

badge | Configure Data Collection Manage Source Types Extract Fields Map to Data Models Create Alert Actions Validate & Package Splunk Add-on Builder

Extract Fields > badge

The summary below shows how your sample data was parsed for the Table format. Select the column delimiter character, or click Other to enter a different one. When the results look correct, click Save. Otherwise, click Cancel to return to the previous page to try parsing the data using a different format. Learn more.

Data Summary

Source type: badge Column: 4
Format: Table Row: 52

Space Comma Tab Pipe Other...

field_0 field_1 field_2 field_3

Nov 19 16:06:52 127.0.0.1 2/18/18 9:04

Nov 19 16:06:52 127.0.0.1 2/18/18 9:04

Nov 19 16:06:52 127.0.0.1 2/16/18 9:04

Nov 19 16:06:52 127.0.0.1 2/15/18 9:04

Nov 19 16:06:52 127.0.0.1 2/14/18 9:04

Nov 19 16:06:52 127.0.0.1 2/13/18 9:04

Nov 19 16:06:52 127.0.0.1 2/12/18 9:04

Nov 19 16:06:52 127.0.0.1 2/11/18 9:04

Nov 19 16:06:52 127.0.0.1 2/10/18 9:04

Enter New Field Name: field_1

field_1 ✓ ✕

field_0	field_1	field_2	field_3
workcloset		badge type not allowed	
workcloset		badge hours ineffective	
guardroom		badge accepted	
buttercup		private bathroom	badge type not allowed
guest64		networkcloset	badge type not allowed
bob		networkcloset	badge hours ineffective
ceo		private bathroom	badge accepted
buttercup		conference	badge accepted
guest64		networkcloset	badge type not allowed

< 1 2 3 >

Cancel Save



Task 10: Create Reports on Badge Data

11. Check the fields names and click **Save**

Splunk > App: Splunk Add-on Builder >

badge | Configure Data Collection Manage Source Types Extract Fields Map to Data Models Create Alert Actions Validate & Package Administrator > 3 Messages > Settings > Activity > Help > Find

Extract Fields >> badge

The summary below shows how your sample data was parsed for the Table format. Select the column delimiter character, or click Other to enter a different one. When the results look correct, click Save. Otherwise, click Cancel to return to the previous page to try parsing the data using a different format. Learn more ↗

Data Summary

Source type: badge Column: 4
Format: Table Row: 52

Space Comma Tab Pipe Other...

field_0	user	door	result
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	user	door	result
	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
Nov 19 16:06:52 127.0.0.1 2/14/18 9:04	guest64	networkcloset	badge type not allowed
Nov 19 16:06:52 127.0.0.1 2/13/18 9:04	bob	networkcloset	badge hours ineffective
Nov 19 16:06:52 127.0.0.1 2/12/18 9:04	ceo	private bathroom	badge accepted
Nov 19 16:06:52 127.0.0.1 2/11/18 9:04	buttercup	conference	badge accepted
Nov 19 16:06:52 127.0.0.1 2/10/18 9:04	guest63	networkcloset	badge type not allowed

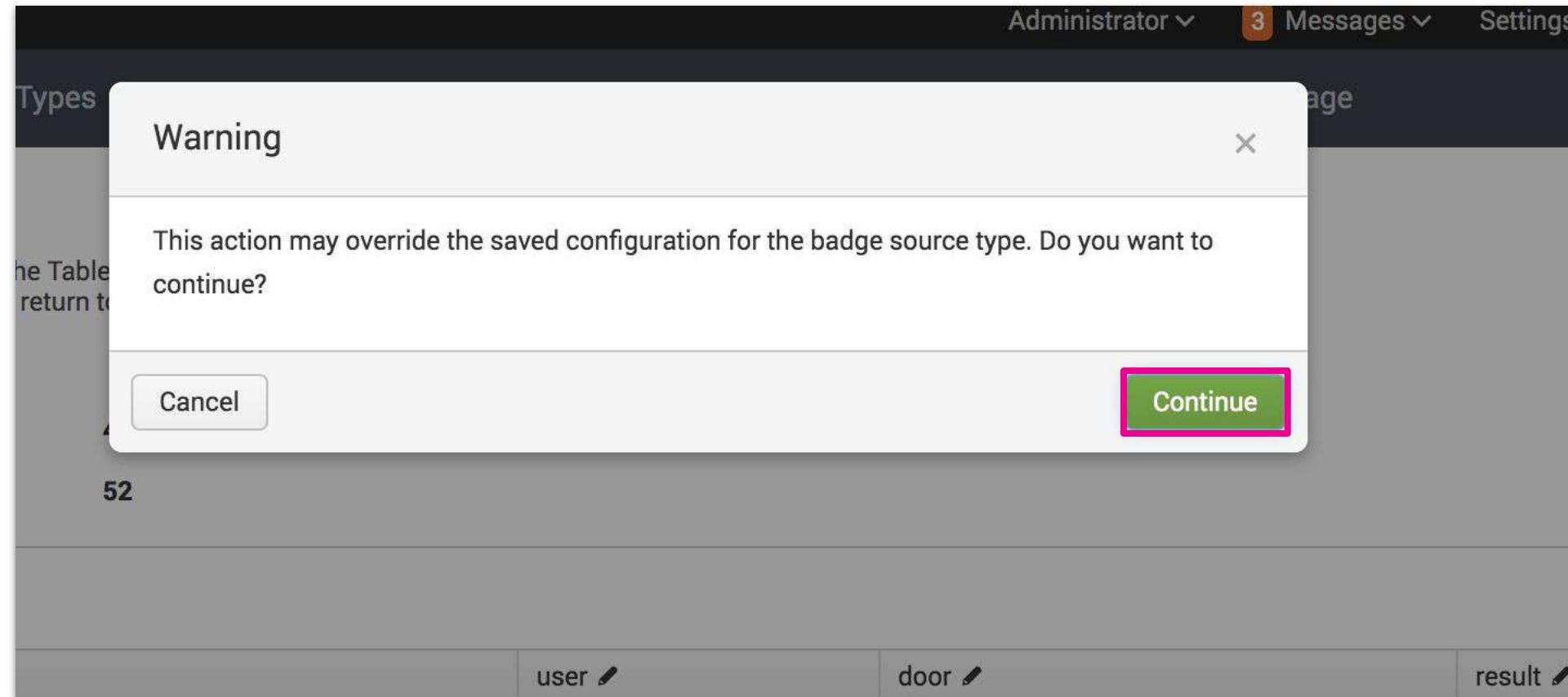
Cancel Save

Save your changes



Task 10: Create Reports on Badge Data

12. Click on **Continue**





Task 10: Create Reports on Badge Data

13. Check that the fields are extracted correctly

index="badge"

The screenshot shows the Splunk interface with the search bar set to "index='badge'". The search results indicate 52 events found before 4/18/19 1:17:40.000 PM. The "Events (52)" tab is selected. A specific event is highlighted, showing the timestamp as Nov 19 16:06:52 2018 and the source as 127.0.0.1. The event details mention "guest65, networkcloset, badge type not allowed". The "Event Actions" dropdown is open. In the bottom right corner of the event details, there is a callout box with the text "Check the field names" overlaid on the table. The table columns are "Type", "Field", and "Value". The "Field" column for the selected row contains "host", "source", and "sourcetype". The "Value" column for these rows shows "ip-172-31-37-209.eu-west-1.compute.internal", "/opt/data/badge.log", and "badge" respectively. The "Event" section of the table lists "door", "field_0", "result", and "user" as event fields.

Type	Field	Value
Selected	host	ip-172-31-37-209.eu-west-1.compute.internal
Selected	source	/opt/data/badge.log
Selected	sourcetype	badge
Event	door	127.0.0.1
Event	field_0	2/18/18 9:04
Event	result	allowed
Event	user	guest65



Task 10: Create Reports on Badge Data

14. Another way to check the fields

```
index=badge | stats values(user) values(door) values(result)
```

The screenshot shows the Splunk interface with a search bar containing the command: `index="badge" | stats values(user) values(door) values(result)`. The search results table displays three columns: `values(user)`, `values(door)`, and `values(result)`. The `values(result)` column includes a tooltip: "Search over All time".

values(user)	values(door)	values(result)
bob	boardroom	badge accepted
buttercup	conference	badge hours ineffective
ceo	front	badge type not allowed
guest4	networkcloset	
guest55	private bathroom	
guest56		
guest57		
guest58		
guest59		
guest60		
guest61		
guest62		
guest63		
guest64		
guest65		



Task 10: Create Reports on Badge Data

15. Go to add on builder app and click on Map to Data Models

splunk > App: Splunk Add-on Builder

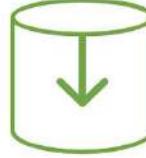
Administrator 3 Messages Settings Activity Help Find

badge | Configure Data Collection Manage Source Types Extract Fields **Map to Data Models** Create Alert Actions Validate & Package Splunk Add-on Builder

Add-on: badge

Welcome to the home page for your add-on project!

Start with the options below to begin adding components to your add-on. The summary shows your progress. [Learn more](#)

Configure Data Collection
Click to add new data inputs.

Create Alert Actions
Click to create alert actions.

Add-on Summary

Validation Score	Data Inputs	Extracted Fields	Event Types	Alert Actions
-	0	1	0	0



Task 10: Create Reports on Badge Data

16. Click on New Data Model Mapping

The screenshot shows the Splunk Add-on Builder interface. At the top, there is a navigation bar with links: Administrator, Messages (with 3 notifications), Settings, Activity, Help, and Find. Below the navigation bar, there are several tabs: Manage Source Types, Extract Fields, Map to Data Models (which is currently selected and highlighted in blue), Create Alert Actions, and Validate & Package. To the right of these tabs is a green gear icon followed by the text "Splunk Add-on Builder". In the main content area, there is a message: "Click **New Data Model Mapping** to define an event type, then map fields from your events to Data Model Fields. If your data is stored outside of this add-on in Splunk platform (for example, data from HTTP Event Collector and syslogs), go to **Manage Source Types** first to add the data to your add-on. [Learn more](#)". Below this message is a table with three columns: "Source Type", "Data Model Source", and "Actions". A green button labeled "New Data Model Mapping" is positioned at the top right of the table area.



Task 10: Create Reports on Badge Data

17. Enter an event type name, select the source type and click on **Save**

The screenshot shows the 'Define Event Type' page in the Splunk Add-on Builder. The top navigation bar includes 'splunk>', 'App: Splunk Add-on Builder', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main content area has the following steps:

1. Enter the name '**badge_data**' in the 'Enter a name for the event type:' field.
2. Select the '**badge**' source type from the 'Select one or more source types:' dropdown.
3. Enter the search query '**(sourcetype=badge)**' in the 'Enter a search:' field.
4. Click the '**Save**' button in the top right corner.

A large callout box on the right side of the interface contains the text '4. Save your changes'.



Task 10: Create Reports on Badge Data

18. Click on Select Data Model(s)

splunk> App: Splunk Add-on Builder ▾

Administrator ▾ 3 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Data Model Mapping > Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#) ⓘ

Done

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions

Event Type Fields

Edit Event Type...
Search event type fields

badge_data

- date_hour
- date_mday
- date_minute
- date_month
- date_wday
- date_year
- date_zone
- door
- field_0
- host
- index

New Knowledge Object ▾

Select Data Model(s)...
Search model fields

Data Model Fields



Task 10: Create Reports on Badge Data

19. Select Authentication Data Model and click on Save

splunk> App: Splunk Add-on Builder > DataModelMapping > Select Data Models

Administrator > 3 Messages > Settings > Activity > Help > Find

From the center panel, select one or more data models to use for mapping. You can select an entire model or individual datasets within it. For reference, your event type fields and selected Data Model Fields are also listed. [Learn more](#)

Event Type Fields Data Models Selected Data Models

Search event type fields Search CIM Model Name

Expand All Close All Select

1. Expand the Authentication data model

2. Check the box next to Authentication(12)

3. Click on Select

Authentication data model selection steps:

1. Expand the Authentication data model.
2. Check the box next to Authentication(12).
3. Click on the Select button.

Selected Data Models:

- Splunk_SA_CIM/Authentication/Authentication(12)

Data Model Fields:

- user
- dest_nt_domain
- duration
- response_time
- signature
- signature_id
- src_nt_domain
- action
- app
- src
- src_user
- dest

Event Type Fields:

- user
- date_hour
- date_mday
- date_minute
- date_month
- date_wday
- date_year
- date_zone
- door
- field_0
- host
- index
- linecount
- punct
- result
- source

Data Models:

- Splunk_SA_CIM
 - Certificates
 - Authentication
 - Authentication(12)
 - Web
 - Alerts
 - Change Analysis (Deprecated)
 - Vulnerabilities
 - Malware
 - Change
 - Databases
 - Application State (Deprecated)
 - Network Sessions
 - Ticket Management



Task 10: Create Reports on Badge Data

20. Click on New Knowledge Object and select FIELDALIAS

The screenshot shows the Splunk Add-on Builder interface with the title "Data Model Mapping > Data Model Mapping Details". The main area displays a "Data Model Mapping List" table with columns: Source Type, Object Type, Event Type Field or Expression, and Data Model Field. On the left, under "Event Type Fields", there is a tree view showing "badge_data" expanded, with various fields like "date_hour", "date_mday", etc. On the right, under "Data Model Fields", there is a list of fields from "Splunk_SA_CIM" such as "dest_nt_domain", "duration", "response_time", etc. A callout box highlights the "FIELDALIAS" option in the "New Knowledge Object" dropdown menu. Another callout box highlights the "badge_data" event type in the tree view. A large callout box on the right contains the text "1. Select FIELDALIAS" and "2. Verify that you see the badge_data event type".

1. Select FIELDALIAS

2. Verify that you see the badge_data event type

Event Type Fields

Source Type Object Type Event Type Field or Expression Data Model Field

New Knowledge Object

FIELDALIAS EVAL

badge_data

date_hour date_mday date_minute date_month date_wday date_year date_zone door field_0 host

Splunk_SA_CIM

Authentication(12)

user dest_nt_domain duration response_time signature signature_id src_nt_domain action app src



Task 10: Create Reports on Badge Data

21. Click on the **door** field on the left panel

splunk > App: Splunk Add-on Builder >

Administrator > 3 Messages > Settings > Activity > Help > Find

Data Model Mapping >> Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#)

Done

Event Type Fields	Data Model Mapping List				Data Model Fields
	Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
badge_data	badge	FIELDALIAS	door		cel

1. Click on the **door** event type

2. 'door' will appear as the Event Type Field

Event Type Fields:

- Edit Event Type...
- Search event type fields
- badge_data
 - user
 - date_hour
 - date_mday
 - date_minute
 - date_month
 - date_wday
 - date_year
 - date_zone
 - door
 - field_0
 - host
 - index

Data Model Fields:

- Select Data Model(s)...
- Search model fields
- Splunk_SA_CIM
 - Authentication(12)
 - user
 - dest_nt_domain
 - duration
 - response_time
 - signature
 - signature_id
 - src_nt_domain
 - action
 - app
 - src



Task 10: Create Reports on Badge Data

22. Click on **dest** field on the right panel, then click on **OK**

Splunk > App: Splunk Add-on Builder >

Administrator > 3 Messages > Settings > Activity > Help > Find

Data Model Mapping > Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. Learn more ↗

Event Type Fields

Edit Event Type...
Search event type fields
badge_data
user
date_hour
date_mday
date_minute
date_month
date_wday
date_year
date_zone
door
field_0
host
index

Data Model Mapping List

New Knowledge Object

Source Type: badge

Data Model Field: dest

Action: OK

Done

1. Click on dest

2. 'dest' will appear as the Data Model Field

3. Click on OK

Data Model Fields

Select Data Model(s)...
user
dest_nt_domain
duration
response_time
signature
signature_id
src_nt_domain
action
app
src
src_user
dest



Task 10: Create Reports on Badge Data

23. Click on **New Knowledge Object** and select **EVAL**

splunk> App: Splunk Add-on Builder ▾ Administrator ▾ 3 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Done

Data Model Mapping >> Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. Learn more ↗

Event Type Fields	Source Type	Object Type	Event Type Field or Expression	Data Model Field
<button>Edit Event Type...</button> <input type="text" value="Search event type fields"/>	badge	FIELDALIAS	door	dest

New Knowledge Object ▾

FIELDALIAS	EVAL
dest	EVAL

Data Model Fields

Select Data Model(s)...
Search model fields

Splunk_SA_CIM

Authentication(12)

- dest
- user
- dest_nt_domain
- duration
- response_time
- signature
- signature_id
- src_nt_domain
- action



Task 10: Create Reports on Badge Data

24. Select **action** on the right panel and enter the expression:

```
if(result=="badge accepted","success","failure")
```

splunk > App: Splunk Add-on Builder >

Administrator > 3 Messages > Settings > Activity > Help > Find

Data Model Mapping >> Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#)

Done

Event Type Fields

Edit Event Type...
Search event type fields
badge_data
dest
user
date_hour
date_mday
date_minute
date_month
date_wday
date_year
date_zone
door
field_0
host

Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Action
badge	EVAL	badge accepted","success","failure")	action	OK

New Knowledge Object >

Data Model Fields

Select Data Model(s)...
Authentication(12)
dest
user
dest_nt_domain
duration
response_time
signature
signature_id
src_nt_domain
action
app

3. Click on OK

2. Enter the expression shown above

1. Click on action



Task 10: Create Reports on Badge Data

25. Click on Done

splunk> App: Splunk Add-on Builder > Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type. Starting by selecting the data models and datasets you want to use, then click New Knowledge Object to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. [Learn more](#)

Data Model Mapping List

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

Event Type Fields

- badges
- action
- dest
- user
- date_hour
- date_mday
- date_minute
- date_month
- date_wday
- date_year
- date_zone
- door
- field_0

Data Model Fields

- Select Data Model(s)...
- Search model fields
- Splunk_SA_CIM
- Authentication(12)
 - action
 - dest
 - user
 - dest_nt_domain
 - duration
 - response_time
 - signature
 - signature_id
 - src_nt_domain
 - app

Done



Task 10: Create Reports on Badge Data

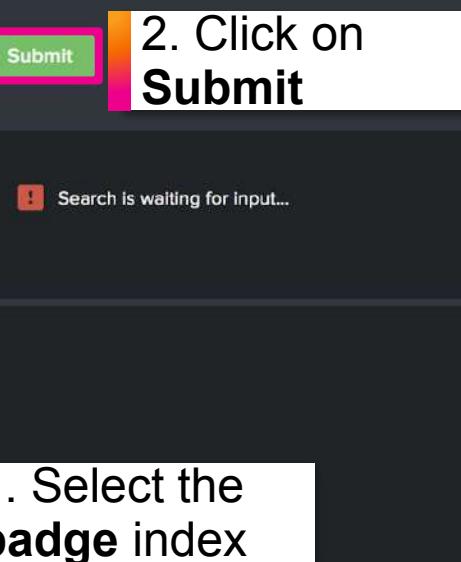
26. Go to the DataOnboarding4Ninjas app

The screenshot shows the Splunk Add-on Builder interface. At the top, there's a navigation bar with the Splunk logo, the text "App: Splunk Add-on Builder", and an "Admin" button. Below the navigation bar, there's a header with tabs: "badge" (which is highlighted with a pink box), "Search & Reporting", "Extract Fields", "Map to Data Models", and "Create Alert Actions". On the left side, there's a sidebar with sections for "Data Model Mapping", "Splunk Add-on Builder" (which has a checked checkbox next to it), "Manage Apps", and "Find More Apps". The main content area contains a section titled "Data Model Mapping" with the following text: "Data Model Mapping to define an event type, then map fields from your events to Data Model Fields. If you want to map data from another source outside of this add-on in Splunk platform (for example, data from HTTP Event Collector and syslogs), go to Manage Apps." Below this, there are three dropdown menus: "Event Type" set to "badge_data", "Source Type" set to "badge", and "Data Model Source" set to "Splunk_SA_CIM(3)".



Task 10: Create Reports on Badge Data

27. Check you dashboard again



1. Select the badge index

2. Click on Submit

index

all

filter

_audit

_internal

_introspection

_telemetry

_thefishbucket

add_on_builder_index

badge

cim_modactions

firewall

history

main

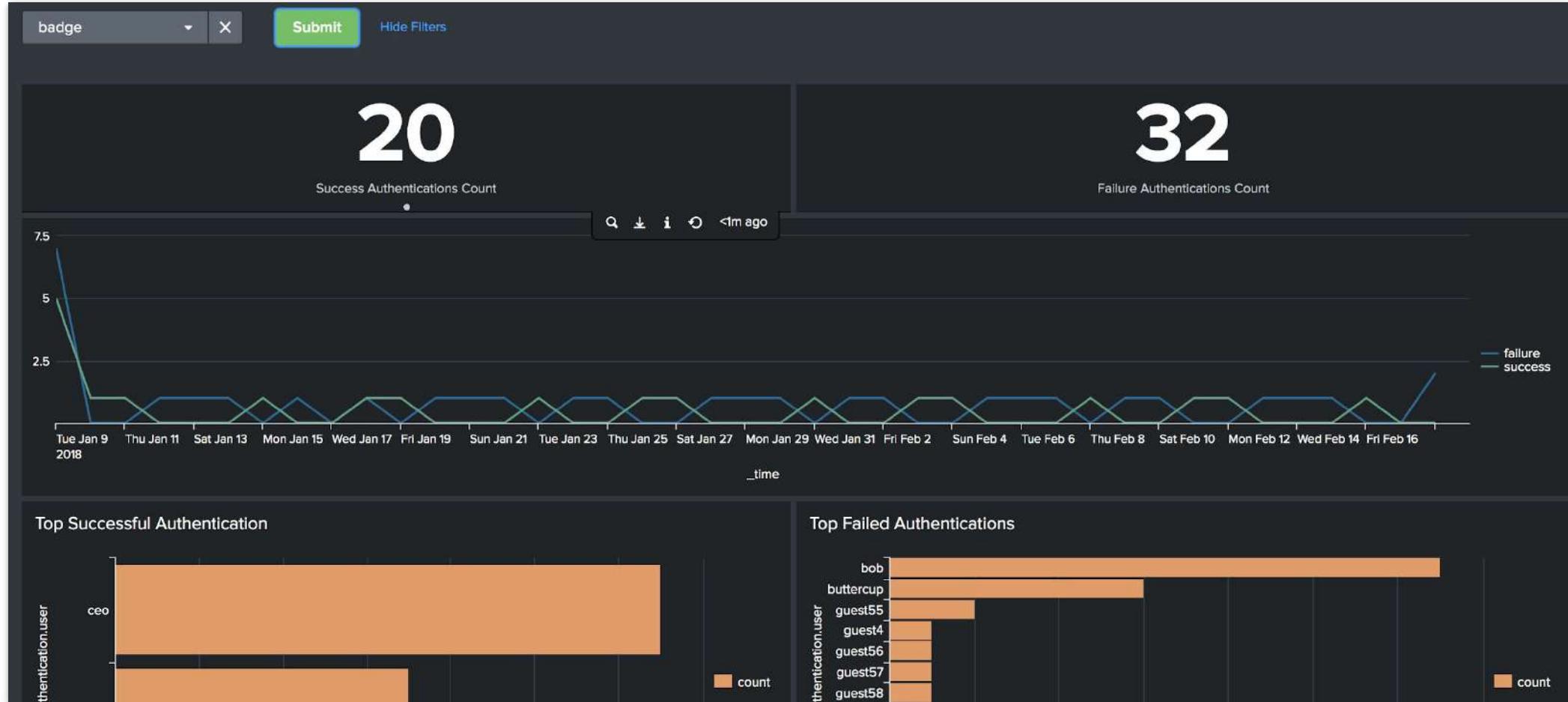
Top Failed Authentications

splunk>



Task 10: Create Reports on Badge Data

Results should now be displayed correctly!



Thank You!

(Extra credit exercises below!)





Extra Credit: Install the Data Model Wrangler App

1. Go to Apps > Find More Apps and search for “wrangler”

The screenshot shows the Splunk interface. On the left, there's a sidebar with various search terms and a 'Find More Apps' button highlighted with a pink box. The main area shows a search bar with 'wrangler' typed in, also highlighted with a pink box. Below the search bar, there's a 'Best Match' section showing one result: 'Data model wrangler'. The result card includes a small icon, the app name, a brief description, and an 'Install' button, which is also highlighted with a pink box.

Enter your splunk.com
credentials

Login

Enter your Splunk.com username and password to download the app.

splunk4cim@grr.la

.....

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app and does not provide any warranty or support. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

CIM Buddy is governed by the following license: [3rd_party_eula](#)

I have read the terms and conditions of the license and agree to be bound by them. I accept that Splunk will securely send my login credentials over the Internet to splunk.com

[Cancel](#) [Login and Install](#)



Extra Credit: Wrangler App Pre-reqs

2. Review the prerequisites

How do I use the app?

- Ensure you have the [Common Information Model](#) app installed and up-to-date
- [Install the CIM Validator app](#), as Data model wrangler relies on a custom search command from the CIM Validator app. There are also drill-downs from panels in the Data model wrangler to the CIM Validator.
- Create an index for the data that will be generated. Default index name is: *data_model_wrangler*
 - If you want to use a custom index name, please update the 'data_model_wrangler_index' search macro in the app with the custom index name
- [Enable the below saved searches](#)
 - *data_model_wrangler_dm_index_sourcetype_field* (default schedule is twice per day, once at 06:00 and again at 14:00. Time range: -4h@h to -3h@h)
 - *data_model_wrangler_field_quality* (default schedule is once per day at 01:00)
 - *data_model_wrangler_mapping_quality* (default schedule is once per day at 01:00)

Over time this will build up a view of mapping and field data quality over time, allowing you to see the current state, find issues and measure the results.

Whenever a CIM mapping requirement comes up, this dashboard provides a quick and easy way to find existing mapped data, or to verify that newly added data has been CIM mapped correctly.



Extra Credit: Install the CIM Validator App

3. Install the SA-cim_vladiator app (search for “cim”)

The image shows two screenshots of the Splunk web interface. On the left, the 'Apps' menu is highlighted. On the right, a search result for 'cim' is shown.

Splunk > enterprise Apps

- Search & Reporting >
- Data model wrangler
- DataOnboarding4Ninjas
- SA-cim_vladiator
- Splunk Add-on Builder
- Splunk Essentials for Cloud and Enterprise 9.0
- Splunk Secure Gateway
- Manage Apps
- [Find More Apps](#)

Browse More Apps

Search: cim

CATEGORY:

- IT Operations
- Security, Fraud & Compliance
- Business Analytics
- Utilities
- IoT & Industrial Data
- DevOps
- Directory Service
- Email
- Endpoint
- Firewall
- Generic
- Identity Management
- Information
- Investigative
- Network Access Control
- Network Device
- Network Security
- Reputation
- Sandbox
- SIEM
- Threat Intel
- Ticketing
- Virtualization

Results:

- CIM Buddy** (Best Match)
 - Category: Utilities | Author: Christian Lauber | Downloads: 606 | Released: a year ago | Last Updated: 5 months ago | [View on Splunkbase](#)
- SA-cim_vladiator**
 - This Splunk app was developed with one goal in mind, reduce amount of time spent validating Splunk Common Information Model (CIM) compliance of technology add-ons (TA's). Use of this app simplifies validation process in several ways:
 - Identifies fields that are required, but missing
 - Validates data confirms to expected CIM values
 - Rapid prototypin... [More](#)
 - Category: Security, Fraud & Compliance, Utilities | Author: Splunk Works | Downloads: 11778 | Released: 2 months ago | Last Updated: 2 months ago | [View on Splunkbase](#)



Extra Credit: Create an Index for the Data Model Wrangler App

4. Create a `data_model_wrangler` index

Messages ▾ **Settings ▾** Activity ▾ Help ▾ Find

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes**
- Report acceleration summaries
- Virtual indexes
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Federated search
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- RapidDiag
- Instrumentation
- Workload management

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password Management
- Authentication Methods

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more ↗

16 Indexes filter 20 per page ▾

New Index

General Settings

Index Name **data_model_wrangler**
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics
The type of data to store (event-based or metrics).

Home Path optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path optional
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thawedb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index 500 GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket auto GB ▾
Maximum target size of buckets. Enter 'auto...high...volume' for high-volume indexes.

Frozen Path optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Data model wrangler ▾

Storage Optimization

Save Cancel

Search macros

Advanced search > Search macros

Showing 1-7 of 7 items

Name	Definition
<code>data_model_wrangler_dm_index_sourcetype_field_search</code>	<code>index='data_model_wrangler_dm_index' sourcetype='field' \$SEARCH</code>
<code>data_model_wrangler_field_quality_search</code>	<code>index='data_model_wrangler' field=\$FIELD quality=\$QUALITY</code>
<code>data_model_wrangler_health_review_lookup</code>	<code>data_model_wrangler_health_review \$SEARCH</code>
data_model_wrangler_index	<code>data_model_wrangler</code>

The **`data_model_wrangler_index`** macro is included in the Data Model Wrangler app and points to this index name



Extra Credit: Run the Data Model Wrangler Saved Searches

5. Run the 3 saved searches (hint: set time to **All time**)

1. Open Searches, reports, and alerts

2. Search for "wrangler"

3. Run each of the 'data_model_wrangler' searches

Run the searches over All time

Name	Type	Next Scheduled Time	Display View	Owner	App	Alerts
data_model_wrangler_dm_in dex_so urcetyp e_field	Report	2023-03-29 09:25:00 EDT	none	nobody	data_model_wrangler	0
data_model_wrangler_field_quality	Report	2023-03-29 09:26:00 EDT	none	nobody	data_model_wrangler	0
data_model_wrangler_mapping_quality	Report	2023-03-29 09:26:00 EDT	none	nobody	data_model_wrangler	0

```

| datamodelsimple
| search datamodel!="*_Validation"
| search datamodel!="internal_audit_logs"
| search datamodel!="internal_server"
| search datamodel IN ('datamodel_wrangler_data_model_list')
    
```



Extra Credit: Install the Data Model Wrangler App

6. Review the Data Wrangler dashboards

enterprise Apps ▾

- Search & Reporting
- Data model wrangler**
- SA-cim_vladiator
- Splunk Add-on Builder
- Splunk Essentials for Cloud and Enterprise 9.0

1. Open Data model wrangler



Data model wrangler

Note: To get the most accurate representation of current state, select Yesterday

Duration	Data model	Index	Sourcetype
All time	All	All	All

Mapping quality score: 100.0 %

Field data quality score: No results found.

Overall quality score: No results found.

Mapping quality per data model: Authentication 100.0 %, Network_Traffic 100.0 %

Field data quality per data model: Authentication 0.0 %, Network_Traffic 0.0 %

Overall quality per data model: 0.0 %

↓ (scroll down)

Indexes, sourcetypes and fields mapped to data models - Splunk DM recommended field coverage

modelName	index	sourcetype	cim_search	splunk_recommended_fields	actual_mapped_fields	rec_field_coverage_pct	reviewed	status
Authentication	audit	audittrail	index=audit sourcetype=audittrail tag=authentication NOT (action=success user=\$)	action app dest index reason sourcetype src src_user user		100.0 %	true	Done
Network_Traffic	firewall	fortigate_traffic	index=firewall sourcetype=fortigate_traffic tag=network tag=communicate	action app bytes bytes_in bytes_out dest dest_port dvc rule src src_port transport user		100.0 %	true	Done

Data model review

Duration: Last 7 days

Data model: All

Index: All

Sourcetype: All

Status: All

Open data_model_wrangler_health_review.csv in Lookup Editor

Reviewed - Done	Reviewed - In Development	Reviewed - Open	To be reviewed - Recommended field coverage < 100%
1	0	0	2