

# Splunk4Industry: Manufacturing

## Lab Guide

### Overview

This lab guide contains the hands-on exercises for the **Splunk4Industry: Manufacturing** workshop. Before proceeding with these exercises, please ensure that you have a copy of the Splunk4Industry slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: <https://splk.it/Manu-Attendee>

### Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the [Splunk Show portal](#) and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one [here](#) before proceeding with the rest of the workshop.



### Registering for a Splunk.com Account

To help reduce any additional identity verification checks during the registration process, please use full names and full company names where possible, avoiding nicknames and abbreviations. Please see [Splunk.com Registration Best Practices](#) for more details.



### Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. <https://show.splunk.com/event/<eventID>>) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

## Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Exercise 1 – Access Your Lab Environment.....</b>	<b>4</b>
Description.....	4
Steps.....	4
<b>Exercise 2 – Create an App and Add Data to Splunk.....</b>	<b>7</b>
Description.....	7
Steps.....	7
<b>Start Exploring Your Data.....</b>	<b>13</b>
Description.....	13
Steps.....	13
<b>Exercise 3 – IT Operations team: Investigate successful vs unsuccessful web server requests over time.....</b>	<b>15</b>
Description.....	15
Steps.....	15
<b>Exercise 4 – DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures.....</b>	<b>18</b>
Description.....	18
Steps.....	18
Extract a New Field.....	18
Show the most common customer operating systems.....	20
Show which web browsers are experiencing the most failures.....	22
<b>Exercise 5 - Manufacturing: exploring additional use cases.....</b>	<b>24</b>
Description.....	24
Steps.....	24
Switch lab instance.....	24
Explore the data.....	24
<b>Exercise 6 - Operational Technology: Security.....</b>	<b>33</b>
Description.....	33
Steps.....	33
Navigating the OT Security Add-on.....	33
Exploring a Notable.....	35
<b>Exercise 7 - Business Service Insights: exploring capability.....</b>	<b>40</b>
Description.....	40
Steps.....	40
Switching lab environment.....	40
Exploring a Glass Table view.....	41
Exploring a Service Analyzer.....	42
Exploring Deep Dive view.....	45
Create a multi-KPI alert.....	48
Exploring Alerts & Episodes View.....	49
<b>Exercise 8 - Business Service Insights: building out a service view.....</b>	<b>53</b>
Description.....	53
Steps.....	53
Expand an existing service for Manufacturing.....	53
Import the service template.....	53

View Service Tree for Splunk Widget Co.....	56
Add a new service to IIoT Monitoring.....	57
Add some KPIs.....	61
Setting Thresholds.....	63
Build custom Glass Tables: Business Services Overview.....	67
Build custom Glass Tables: Infrastructure Overview.....	74
Connecting Glass Tables.....	78
<b>Exercise 9 - Build Your Own Service.....</b>	<b>81</b>
Description.....	81
<b>Answers: Exercise 5.....</b>	<b>82</b>
Final Dashboard.....	82
<b>Answers: Exercise 7.....</b>	<b>83</b>
Glass Tables.....	83
Service Analyzer.....	83
Deep Dive.....	84
Service Creation.....	84

## Exercise 1 – Access Your Lab Environment

### Description

You'll need a Splunk instance to do these hands-on exercises – time to get one!

In this exercise, you will create your own Splunk Enterprise instance using our Splunk Show portal.

---

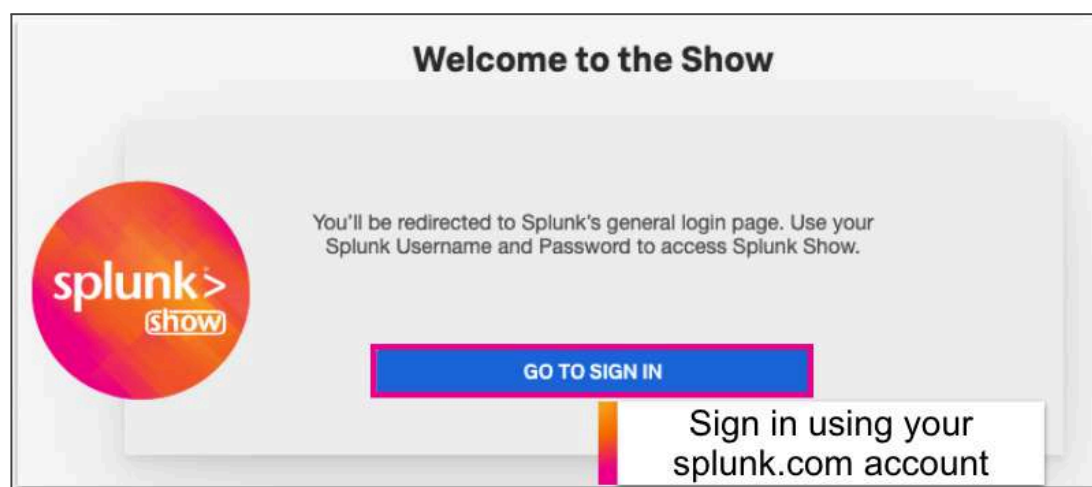
#### Already been given your Splunk instance details?

If your workshop host has already provided you with your instance URL and login details then you do not need to follow the instructions in exercise 1 of this lab guide - you can skip straight to [exercise 2](#)!

---

### Steps

1. Browse to <https://show.splunk.com> and log in using your **Splunk.com account**.



---

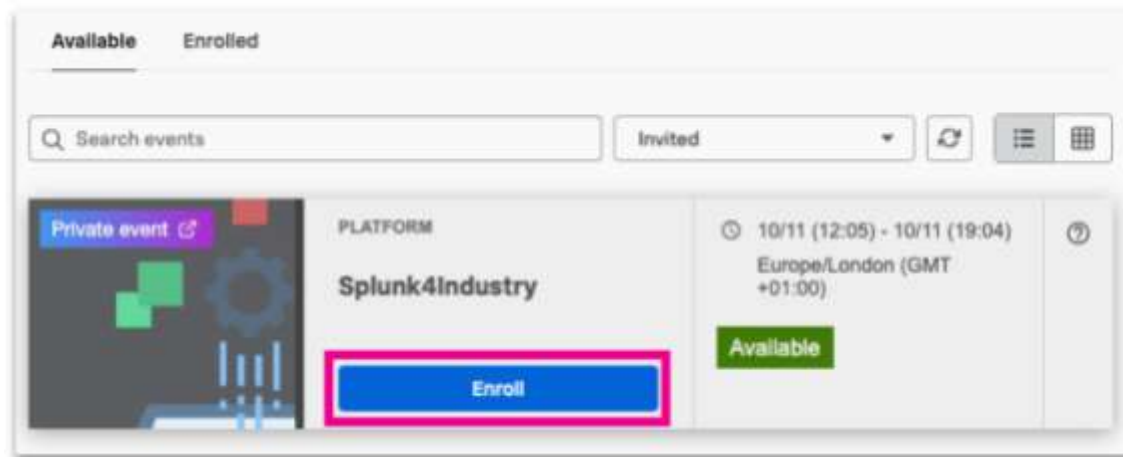
#### Don't have a Splunk.com Account?

To access our hands-on workshop events you will need a Splunk.com account. If you don't already have a Splunk.com account, don't worry - it only takes a few minutes to create one! Please create one [here](#).

---

2. Once logged in to Splunk Show you will see the event page for the event that you have been invited to. If no events are listed, try selecting '**Invited**' from the dropdown list.

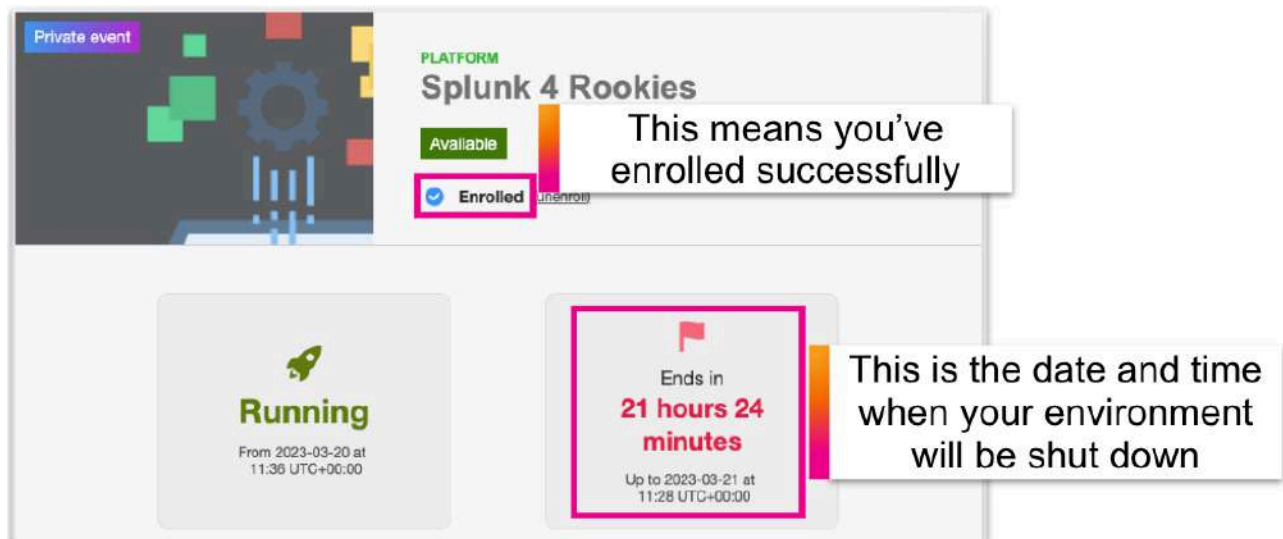
Click on **Enroll** to join the event.



The page will refresh and the event will now display 'Enrolled'.

### Lab environment expiration

All Splunk environments that are part of this workshop event will automatically be shut down at the date and time specified on this screen so feel free to continue to play around with your lab environment until then!



3. Scroll down the page to the **Instances Information** section and expand out the 'Splunk Enterprise' section to locate the user credentials and link to your lab environment.

The screenshot shows the 'Instances information' page in the Splunk Cloud console. At the top, there's a 'splunk>show' header and a 'Welcome' message. A 'Refresh' icon is in the top right. The main content area is titled 'Instances information'. Under this, there's a section for 'Splunk Enterprise' which is currently expanded. A callout box says 'Expand this section'. Below this, the instance is shown as 'Running'. The instance details include a URL, Instance ID (641478f13f5c4893b7d57204), Termination Date (5 hours 32 minutes left), and User ID (-). A 'Connection Information' section is also visible, containing fields for Admin Username (admin), Admin Password (masked), and URL (https://i-07f843e7e5e12fdad.splunk.show). A callout box at the bottom right says 'View your login details'.

---

**! No connection information shown?**

If you don't see any connection information displayed yet it means that your lab environment is currently starting up. Please try refreshing this view in a few minutes.

The screenshot shows the 'Instances information' page in the Splunk Cloud console. The 'Splunk Enterprise' section is expanded, but the instance is in a 'Starting' state. A callout box says 'Your instance may take up to 5 minutes to spin up so please be patient!'. The instance details include a URL, Instance ID (641871fd0b8a20001d52a5dd), Termination Date (23 hours 48 minutes left), and User ID (-). The 'Connection Information' section shows 'No data'. A callout box at the bottom right says 'Connection information will be displayed once your environment is running'.

## Exercise 2 – Create an App and Add Data to Splunk

### Description

Splunk apps and add-ons provide customisable content and capabilities for a variety of technologies and use cases, accelerating the time it takes to get value from your data. They're also a great way to organise and share your content - such as reports and dashboards - to Splunk users. Anyone can build apps and add-ons, and today we're going to create our own app that contains a dashboard.

Since Splunk is a data platform, we'll also need to load some data in before we can do anything!

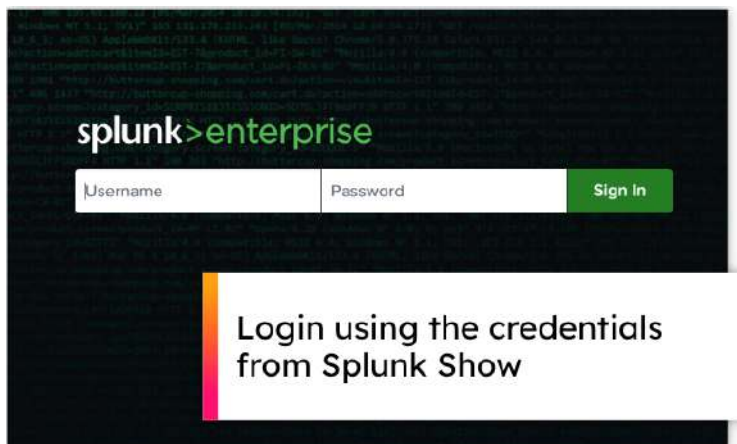
In this exercise, you will create a new app and then add some data to your Splunk Enterprise instance. We will configure Splunk to monitor some sample web server logs, which are currently being generated on the same server that Splunk is running on.

### Steps

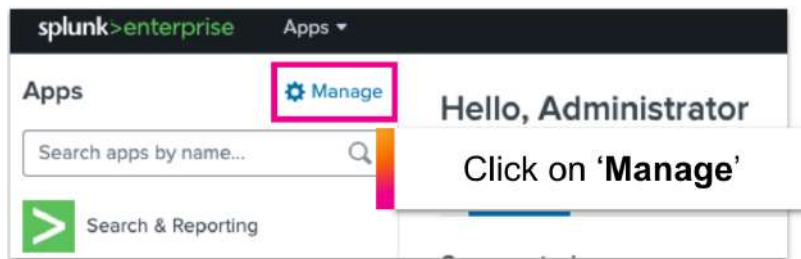
1. Browse to your Splunk instance by using the unique URL link provided in the Splunk Show event (see step 3 of [Exercise 1 - Access Your Lab Environment.](#))

Admin Username	admin	📋
Admin Password	.....	📋
URL	<a href="https://i-07f843e7e5e12fdad.splunk.show">https://i-07f843e7e5e12fdad.splunk.show</a>	🔗 📋

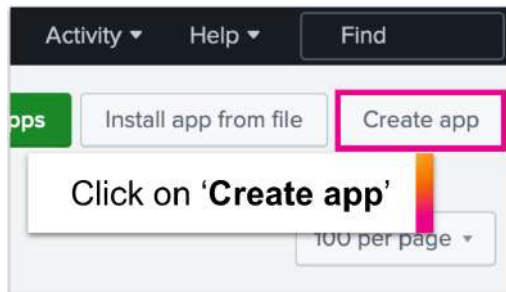
2. Log in using the credentials from the Splunk Show event.



3. On the left side of the page, under the **Apps** section, click on **Manage**.



4. On the top right corner of the screen, click on **Create app**.



5. Give your app a name and enter a folder name. Leave all other values as they are and click on **Save**.



6. Now that our blank app has been created, we need to select the app so that everything we do from now on will be created and saved within the new app.

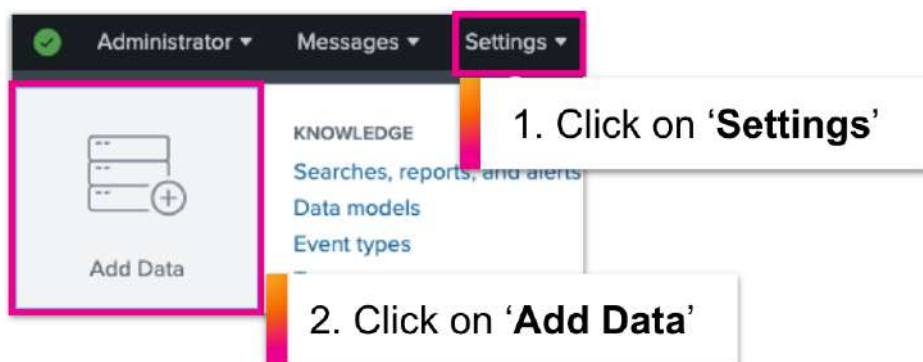
To select your app, click on the **Apps** dropdown list at the top left of the page and select your app.



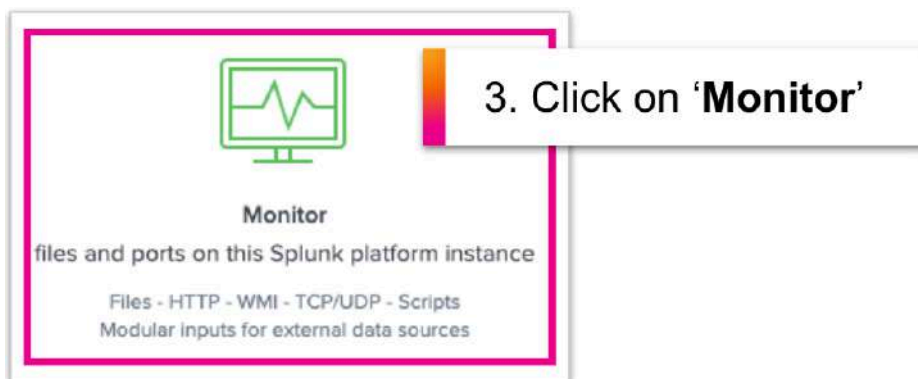
Now let's add some data!



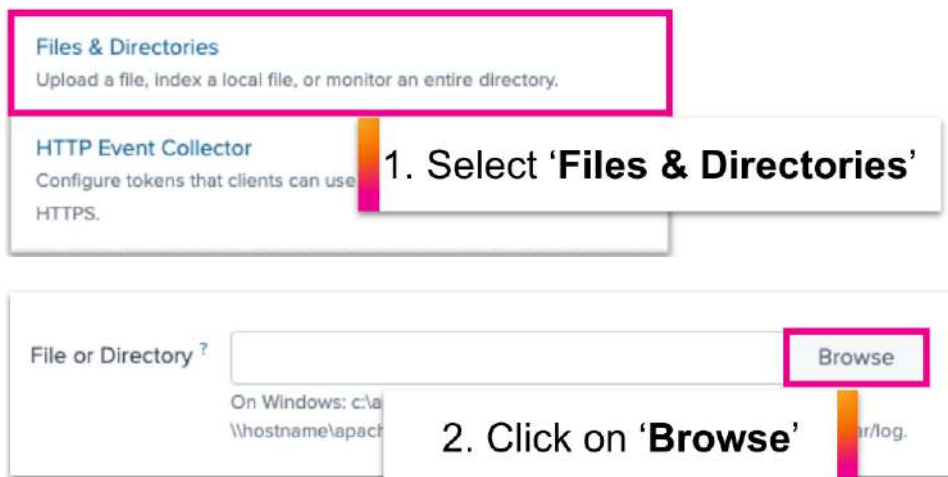
7. With our new app still selected from the dropdown list, go to **Settings > Add Data**.



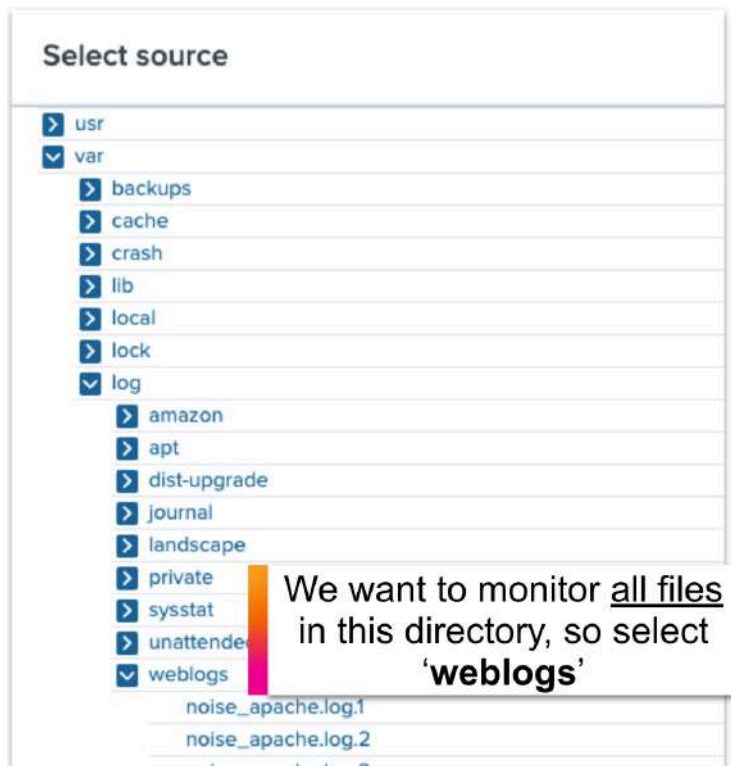
8. For this exercise we will monitor a directory, as this will allow us to pick up new data as it is generated by the web server. To do this, click on **'Monitor'**.



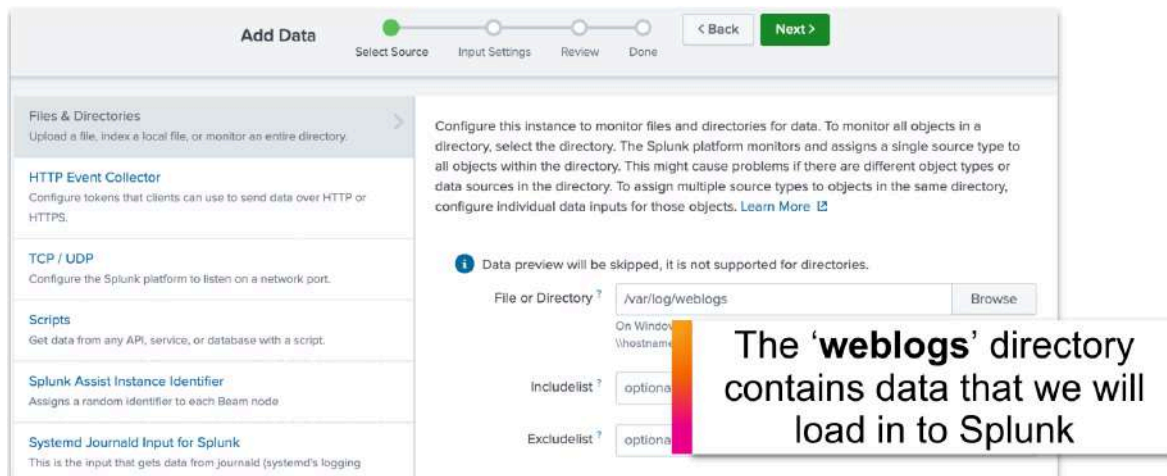
9. Select **'Files & Directories'** and then click **'Browse'**.



10. Browse to `/var/log` and select the **weblogs** directory. Click on **Select** to choose this directory.

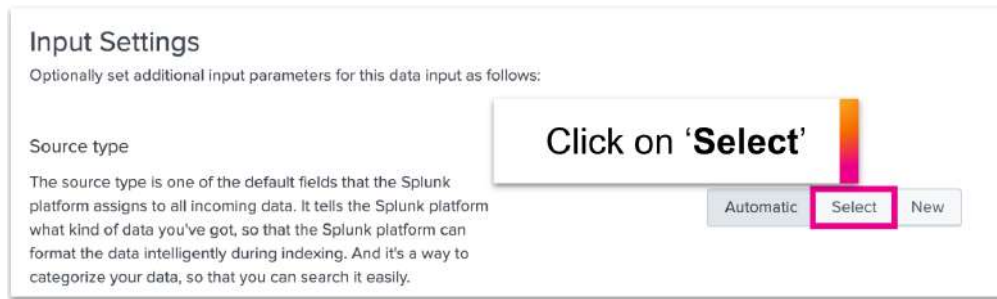


11. Check that the directory path is correct (`/var/log/weblogs`) and click on **Next**.





12. Now we need to select a source type for this data. A source type determines how Splunk formats the data during the indexing process. Splunk comes with a large set of predefined source types and can often detect the source type automatically. However, for this exercise you will specify the source type.


On the **Input Settings** screen, to the right of the **Source type** section, click on **Select**.





Click on **Start Searching** to search the data you have just added to Splunk.


 **File input has been created successfully.**  
Configure your inputs by going to Settings > [Data Inputs](#)

**Start Searching** Search your data now or see [examples and tutorials](#). 

Extract Fields Create search-time field extractions. [Learn more about fields](#). 

Add More Data Add more data inputs now or see [examples and tutorials](#). 

Download Apps Apps help you do more with your data. [Learn more](#). 

Build Dashboards Visualize your searches. [Learn more](#). 

You should now see the raw events being shown in Splunk.

Search

Analytics

Datasets

Reports

Alerts

Dashboards

App

splunk4rookies

New Search

Save As

Create Table View

CLOSE

source="/var/log/weblogs/\*" host="ip-172-31-39-95" sourcetype="access\_combined"

All time

🔍

✓ 1,467 events (before 17/01/2022 16:29:20.000) No Event Sampling

Job

🔧

🔄

📄

📌

🔔 Smart Mode

Events (1,467)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

1 minute per column

List

Format

20 Per Page

Prev

1

2

3

4

5

6

7

8

Next

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

action 5

bytes 100+

clientip 67

date\_hour 2

date\_mday 1

date\_minute 25

date\_month 1

date\_second 60

i	Time	Event
>	12/01/2022 18:09:15.129	194.215.205.19 - - [12/Jan/2022 18:09:15:129] "GET /cart.do?action=view&itemId=EST-78product_id=WPSS-2&JSESSIONID=SD9SL10FF5ADFF9 HTTP/1.1" 403 3490 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" Mozilla/5.0 (Windows; WDM64) AppleWebKit/537.36 Chrome/51.0.2784.106 Safari/537.36 402 host= ip-172-31-39-95   source = /var/log/weblogs/noise_apache_3.log   sourcetype = access_combined
>	12/01/2022 18.09.13.193	141.146.8.66 - - [12/Jan/2022 18:09:13:193] "GET /cart.do?action=changequantity&itemId=EST-26&product_id=MCB-6&JSESSIONID=SD3SL1FF7ADFF5 HTTP/1.1" 200 2278 "http://www.buttercupenterprises.com/cart.do?action=changequantity&itemId=EST-26&product_id=MCB-6" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 Chrome/57.0.2957.0 Safari/537.36 613 host= ip-172-31-39-95   source = /var/log/weblogs/noise_apache_3.log   sourcetype = access_combined
>	12/01/2022 18:09:13:191	128.241.220.82 - - [12/Jan/2022 18:09:13:191] "GET /product.screen?product_id=WPSS-2&JSESSIONID=SD4SL2FF5ADFF8 HTTP/1.1" 400 317 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5 Build/PPR58N) AppleWebKit/537.36 Chrome/52.0.2743.8 Mobile Safari/537.36 818 host= ip-172-31-39-95   source = /var/log/weblogs/noise_apache_3.log   sourcetype = access_combined

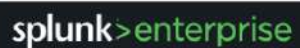
## Start Exploring Your Data

### Description

In this exercise, you will try some basic Splunk searches using the Search section of your new app.

### Steps

1. Click on the Splunk logo in the top left corner of the screen to take you back to the default home screen.



2. Under the **Apps** section on the left of the page, click on the new app that you created in task 2 (Note: the name will be whatever you entered when you created it.)



3. To search, just type any word or phrase into the search bar and Splunk will search for all events that contain those words.

So enough talking – let's try some searches!

Firstly, set the time picker (to the right of the search bar) to **Last 60 minutes**. Your environment has an event generator running in the background, which is constantly creating sample data for you to use. This data started being generated from the moment you registered for your Splunk environment, so let's stick to the last 60 minutes of data...

Try the following search:

```
503 purchase
```

This will return all events from Splunk that contain the number '**503**' and the word '**purchase**'.



#### **Spaces between words in a search**

In Splunk, a space between two words is an implied Boolean '**AND**', meaning that Splunk will automatically search for events containing both words – you don't need to specify it.

---

4. That's great, but what if there are events with the word '*purchased*', '*purchasing*', or '*purchaser*', for example? Well, we can use a wildcard asterisk (\*) to search for any events containing '**503**' and any word beginning with '**pur**':

```
503 pur*
```

A wildcard is useful if we want to be a bit more flexible with what we're searching for.

5. Remember the '**AND**' operator we mentioned in step 3? Well you can also use the other Boolean operators as well: **OR** and **NOT**. Note that these must be in UPPERCASE.

Let's try using one of these operators in a search:

```
503 (purchase OR addtocart)
```

This search will return all events containing the number '**503**' and either the word '**purchase**' or the word '**addtocart**'.

6. So far, we've just been searching for text – those numbers could appear anywhere in our data, so how do we know that we're searching the right values? Depending on our data '**503**' could be a HTTP status code, or it could be part of a session ID or a phone number.

Well, we know we're looking at web logs, so let's include field/value pairs in our search to be more specific with what we're looking for:

```
status=503 action=purchase
```

This will ensure that our results only return web server **purchase** events where the HTTP status code is '**503**'. Always specify field names where possible to ensure that your results are as accurate as possible!

---

### Search Best Practices

In a production environment you will likely have much more data to search through than in today's workshop environment. As a best practice, always specify the index and sourcetype if you know them - it will make your searches MUCH faster!

Example:

```
index=main sourcetype=access_combined
```

For more information please see [Write better searches](#) in the Splunk docs.

---

## Exercise 3 – IT Operations team: Investigate successful vs unsuccessful web server requests over time

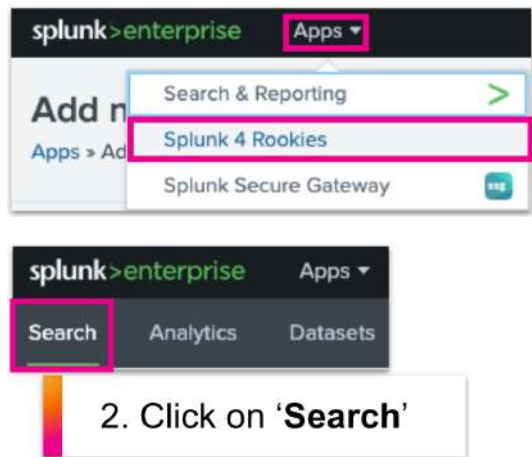
### Description

The IT Operations team currently has no visibility of failures on the Buttercup Enterprises website.

In this exercise, you will produce a dashboard panel for the IT Operations team, showing website successes vs failures over time.

### Steps

1. To start a new search, first make sure your app is selected from the Apps dropdown list and then click Search on the app menu bar.



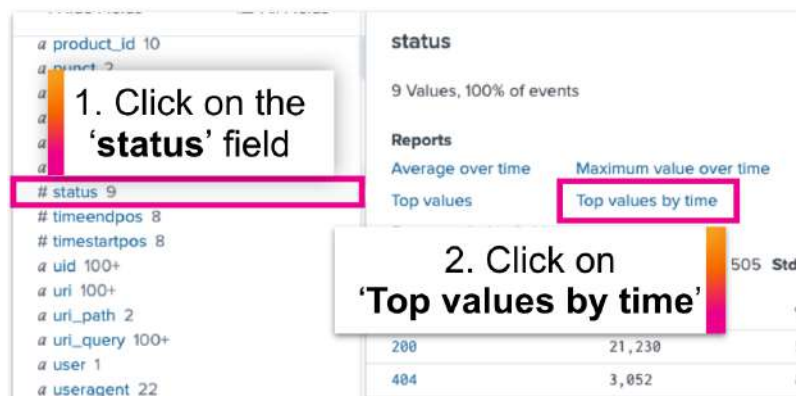
1. Click on the 'Apps' dropdown list and select your new app

2. Click on 'Search'

2. Search the **main** index (i.e. the default index) for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

3. Scroll down the page and find the **status** field. Click on the field name to display the field window and select **Top values by time**.



1. Click on the 'status' field

2. Click on 'Top values by time'

status	Count	Percentage
200	21,230	5
404	3,052	8

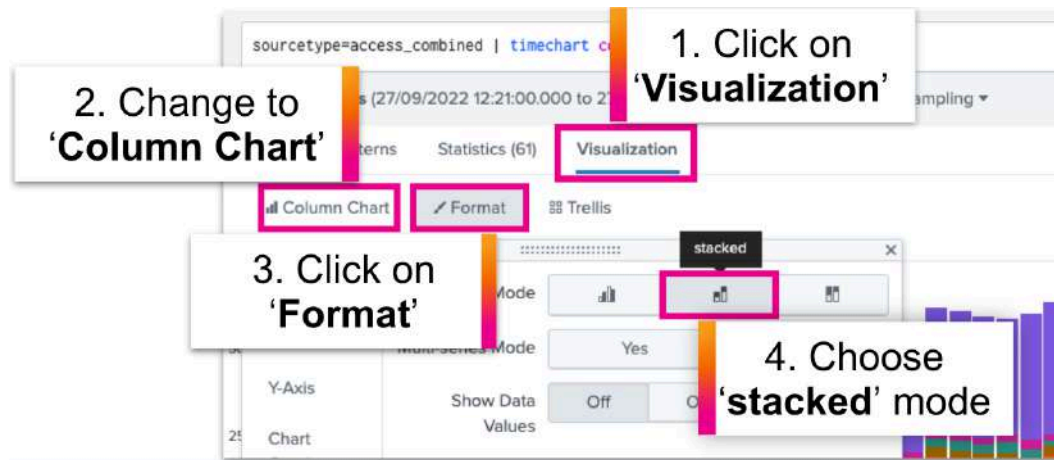


Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined | timechart count by status limit=10
```

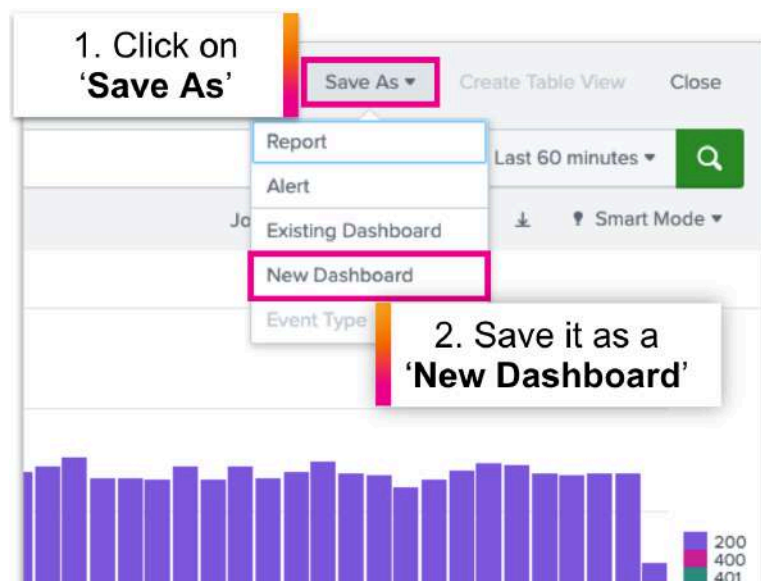
4. A chart will display on the **Visualization** tab. Change the visualization to a **Column Chart**.

Click on **Format** and then on the **General** tab to change the **Stack Mode** to '**stacked**'. Feel free to play around with the formatting until you're happy with the visualization.



5. Now that we have a nice chart visualization, let's add it to a new dashboard so we can share this information with the business.

In the top right corner of the screen, go to **Save As > New Dashboard**.





6. On the **Save Panel to New Dashboard** screen, give your dashboard a suitable title and optionally a description too. If you can't think of a name for your dashboard, call it '**Buttercup Enterprises**, or something else meaningful to you.

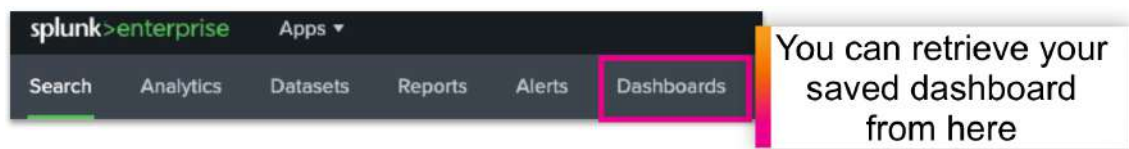
Choose how you want to build your dashboard. For today's workshop we will use **Dashboard Studio**. For your layout mode, select **Absolute**.

Give your panel a title – something that describes what this chart is showing, such as '**IT Ops: Web Server Status Codes Over Time**'.

The screenshot shows the 'Save Panel to New Dashboard' dialog box. It has several sections: 'Dashboard Title' with a text input containing 'Buttercup Enterprises' and an 'Edit ID' link; 'Description' with a text input containing 'Dashboard for Buttercup Enterprises'; 'Permissions' with a dropdown set to 'Shared in App'; 'How do you want to build your dashboard?' with two options: 'Classic Dashboards' and 'Dashboard Studio' (marked with a 'NEW' badge); 'Select layout mode' with 'Absolute' and 'Grid' options; 'Panel Title' with a text input containing 'IT Ops: Web Server Status Codes Over Time'; 'Visualization Type' with 'Column Chart' and 'Statistics' options; and an 'Advanced Panel Settings' link. At the bottom are 'Cancel' and 'Save to Dashboard' buttons. Four numbered callouts are overlaid: 1. 'Give your dashboard a title and description' points to the title and description fields. 2. 'Select 'Dashboard Studio'' points to the 'Dashboard Studio' option. 3. 'Select 'Absolute'' points to the 'Absolute' layout mode option. 4. 'Give your panel a name - make it clear what the chart is showing!' points to the 'Panel Title' field.

7. Click on **Save to Dashboard** and then **View Dashboard**.

Congratulations - you've just created a Splunk dashboard with your first panel!! Anytime you want to access a dashboard, click on **Dashboards** in the menu bar and select the dashboard you wish to display. Go ahead – give it a try!



## Exercise 4 – DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures

### Description

In this exercise, you will need to extract a new field from your events in order to create the report we need. To accomplish this, we will use Splunk's field extractor wizard.

Custom field extractions are useful in a variety of scenarios, such as:

- When you have custom data and Splunk did not recognise/extract a particular field that you need
- When you need to extract a particular part of an event in order to be able to search/report on that value

### Steps

#### Extract a New Field

1. Click **Search** if you don't see the search bar displayed. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Expand out one of the events by clicking on the arrow (>) to the left of the event timestamp. Click on the **Event Actions** dropdown list and select **Extract Fields**:

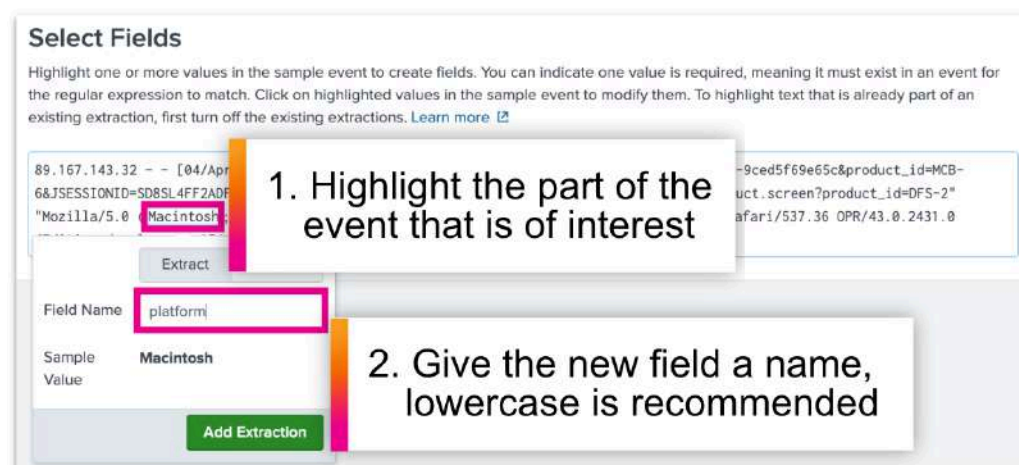


3. We have two options for extracting fields: Regular Expression or Delimiters. For this exercise, we will choose Regular Expression. Click on **Regular Expression** and then click on **Next**.



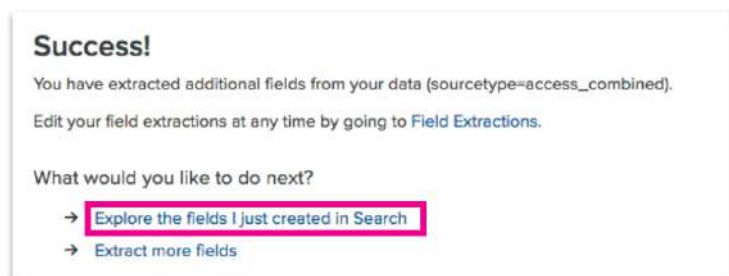
4. You will now be presented with a sample event from which to extract your field. For this exercise, we will need to extract the platform (operating system) information from each event so we can report on it. Look for the platform/operating system information in your event (e.g. Linux, Macintosh, Windows, etc.) contained in the useragent string towards the end of the event and highlight it.

Give the new field the following name: **platform** (field names are case sensitive, so be sure to use all lowercase letters for this to make your life easier!)

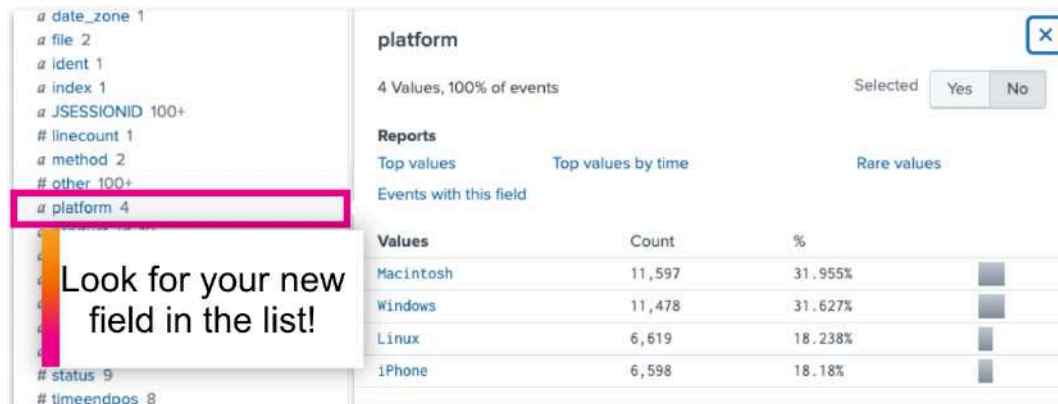


5. Click on **Add Extraction** and then click on **Next**.
6. Click on **Next** again to reach the **Save** screen. On the Save screen, click on **Finish** to save your new field extraction.

7. You should now see a **Success!** page. Click on **Explore the fields I just created in Search.**



8. Splunk will show you search results for all of your web server data over the last 24 hours. Scroll down the page and look for your new field listed on the left – you can now use it in your searches!



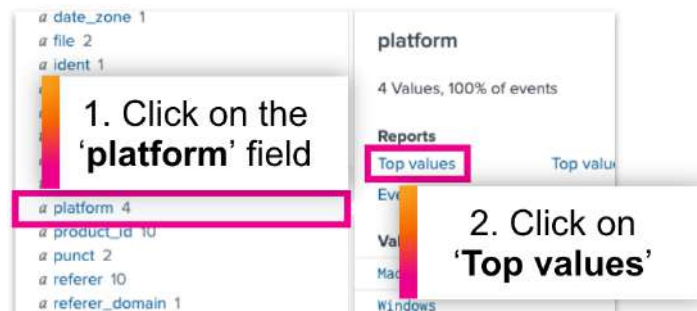
### Show the most common customer operating systems

Now that we have our new field, we can use it to report for the DevOps team!

1. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Scroll down the page and find the **platform** field that you just extracted. Click on the field name to display the field window, and then select **Top values**.



Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined | top limit=20 platform
```

3. Select the **Visualization** tab if not already displayed and change the visualization to a **Bar Chart**.



---

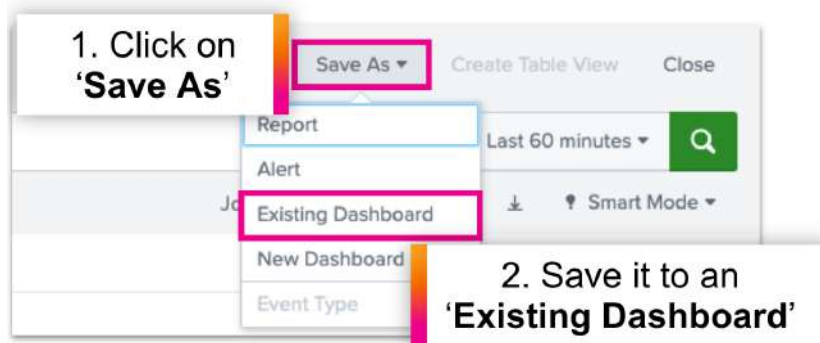
**i Tip for cleaning up your chart**

You can optionally add `showperc=f` to the `top` command to remove the 'percent' column from the table of statistics. This will help to keep the chart nice and clean when we view it on our dashboard later.

```
index=main sourcetype=access_combined | top limit=20 platform showperc=f
```

---

4. When you're happy with your chart, save it to an **'Existing Dashboard'** and select the dashboard you previously created from the list. Finally, give the dashboard panel a suitable title, such as **'DevOps: Most Popular Operating Systems'** and click on **Save to Dashboard**.



Save Panel to Existing Dashboard

Select an Existing Dashboard

Sort: Title (A - Z) ↓

Search By Title

☒ Buttercup Enterprises

1. Select your existing dashboard from the list

Panel Title

Visualization Type

☒ Bar Chart

2. Give your panel a title

> Advanced Panel Settings

Cancel

Save to Dashboard

## Show which web browsers are experiencing the most failures

One DevOps use case down, one more to go! We now need to report on failures by web browser.

1. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Add a search filter to return only events with a status code of 400 or higher (an event with a status value of 400 or higher is considered a failure of some kind.)

```
index=main sourcetype=access_combined status>=400
```

3. Scroll down the page and find the **useragent** field (Note: 'useragent' is a field containing information about the web browsers that are interacting with our website.) Click on the field name to display the field window and then select **Top values by time**.

1. Click on the 'useragent' field

2. Click on 'Top values by time'

useragent

22 Values, 100% of events

Selected

Yes

No

Reports

Top values

Events with this field

Top values by time

Rare values

Top 10 Values

Mozilla/5.0 (Macintosh; Intel

AppleWebKit/537.36 Chrome/56.0.2914.3

Safari/537.36 OPR/43.0.2431.0 (Edition developer)

Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=10
```

4. Select the **Visualization** tab if not already displayed and change the visualization to an **Area Chart**.

To make your chart cleaner, limit your output to the top 5 useragents by changing the “limit” to 5 in your search.

```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5
```

---

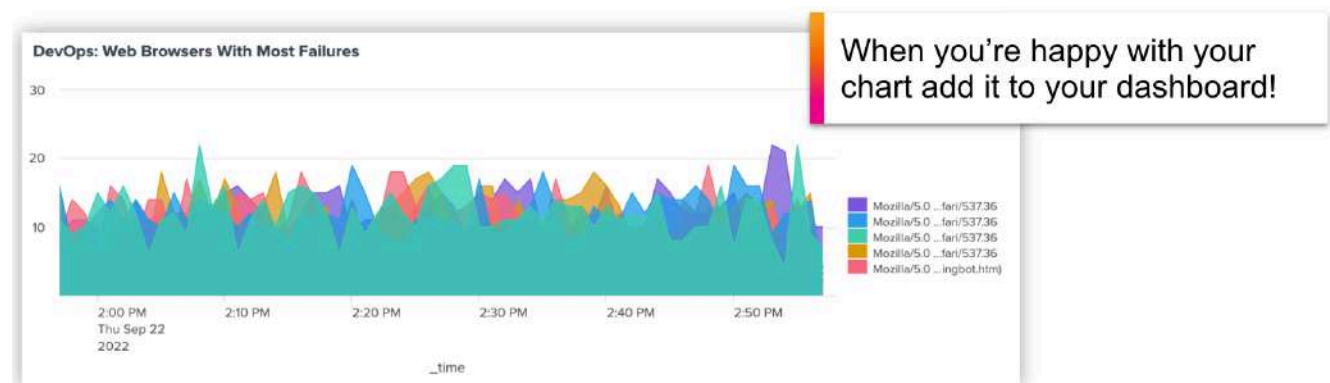
### Tip for cleaning up your chart

You can optionally add `useother=f` to the `timechart` command to remove the ‘OTHER’ value from your chart.

```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5 useother=f
```

---

When you’re happy with your chart, add it to your dashboard and give the panel a title such as ‘**DevOps: Web Browsers With Most Failures**’.



**Note:** Remember to add it to your existing dashboard rather than creating a new one!



## Exercise 5 - Manufacturing: exploring additional use cases

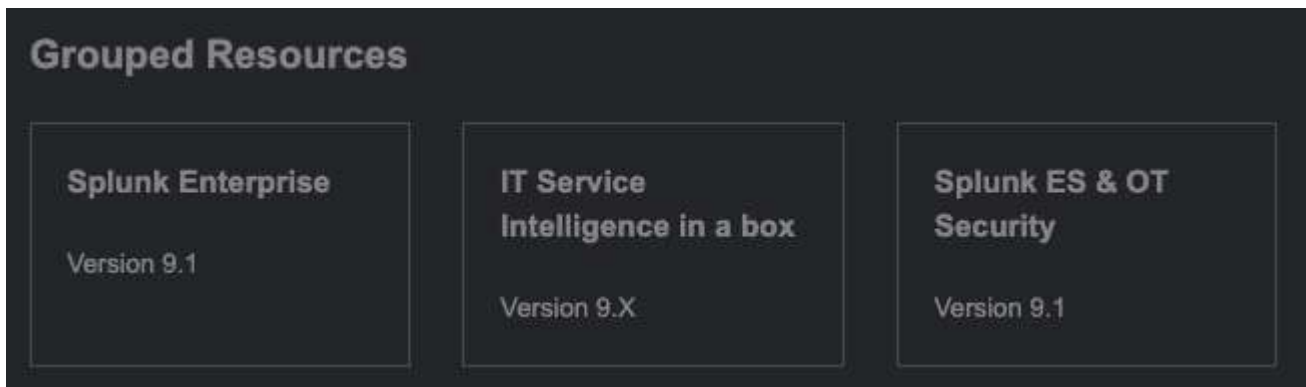
### Description

Now that you have some experience with searching and investigating data in Splunk, we'll take a look at working with some non-traditional IT data. Remember that Splunk can handle any type of machine data, across security, ITOps, IoT and Industrial IoT. For this exercise, we will experiment with insights we can get into data coming from Wind Turbines. Think about how you could apply these techniques across Manufacturing. What data do you have in your organisation that you'd like to explore?

### Steps

#### Switch lab instance

For this exercise, you will need to switch demo instance to "Splunk ES & OT Security". This instance will have its own username and password credentials. Ask for assistance if needed, to locate the demo instance and credentials:



#### Explore the data

Create a new app for this exercise E.g. "Manufacturing Insights"

Name	<input type="text" value="Manufacturing Insights"/>
Give your app a friendly name for display in Splunk Web.	
Folder name *	<input type="text" value="ManufacturingInsights"/>
This name maps to the app's directory in \$SPLUNK_HOME/etc/apps/.	

and save

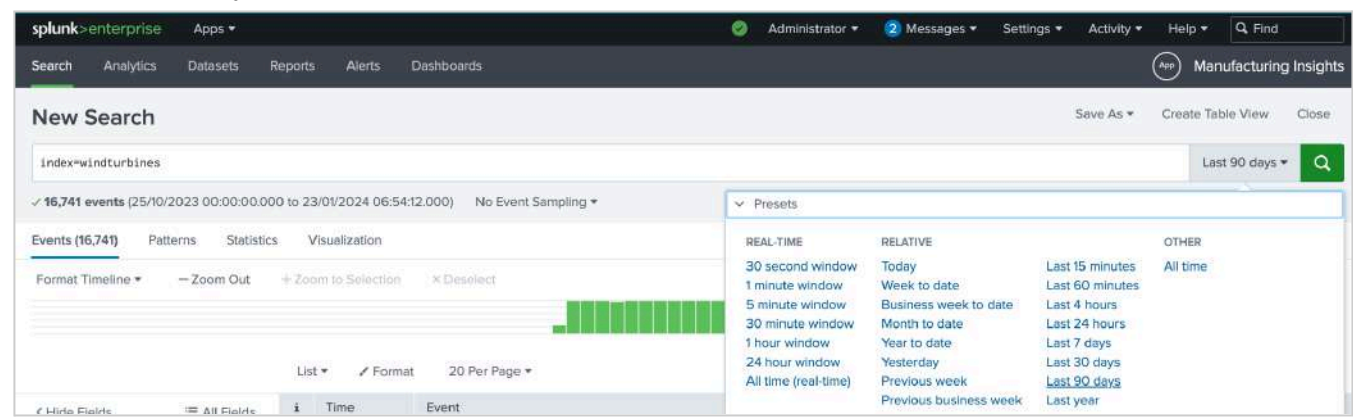
Navigate to the new app, by selecting it from the Apps drop-down menu

The wind turbine data has already been loaded into an index for you, named "windturbines". Search for all available data using:

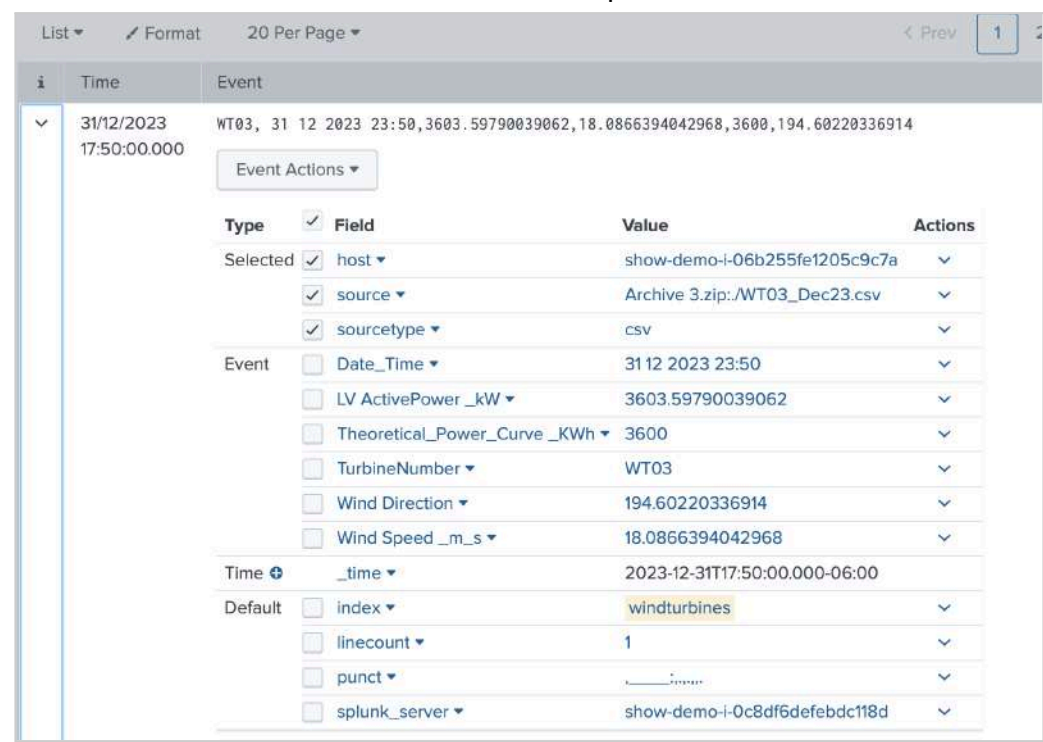


index=windturbines

As this is historical data, you may need to go back 90 days, or more, depending on your results. You should see approximately 16,000 results



Explore one of the events to explore the fields that comprise the event log. You should be able to note around 5 fields that could make the basis of further exploration.



**Q1: Using the “interesting fields” list in the UI, can you determine how many wind turbines there are?**

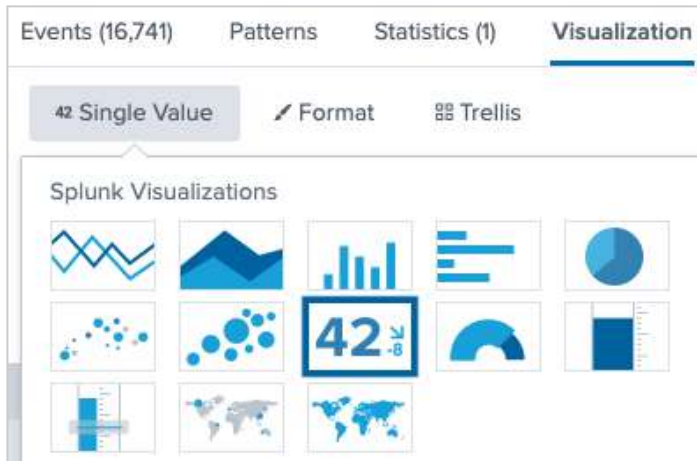
**A:** \_\_\_\_\_

Let’s use this as the basis for a new dashboard.

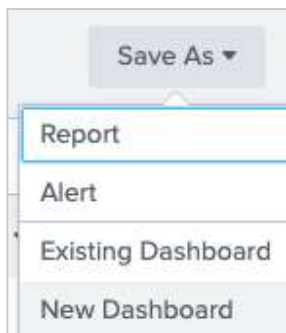
Get a distinct count of number of wind turbines:

```
index=windturbines | stats dc(TurbineNumber)
```

We want this as a **single value** visualisation on our dashboard, so ensure you select that from the choices within **Splunk Visualisations**



Add this to a new dashboard using **Save As** followed by **New Dashboard**, panel name of “Number of Turbines”.



For the dashboard title, we'll use “**Wind Turbine Overview**” to represent what we are building out.

We'll use **Classic** (rather than **Dashboard Studio**) to build this further. Then **Save to Dashboard**.

Save Panel to New Dashboard

Dashboard Title: Wind Turbine Overview  
wind\_turbine\_overview Edit ID

Description: Optional

Permissions: Private

How do you want to build your dashboard? [What's this?](#)

**Classic Dashboards**  
The traditional Splunk dashboard builder.

**Dashboard Studio** **NEW**  
A new builder to create visually-rich, customizable dashboards.

Panel Title: Optional

Visualization Type: Single Value | Statistics Table

> Advanced Panel Settings

Cancel Save to Dashboard

And view the new dashboard

View Dashboard

One of the metrics we can leverage is called **status**. This is an indication of whether a device reports as being online or offline. In this step, we visualise if any devices are currently offline, and also report on how many devices reported as being offline in the last year.

Run a new search using over the last 15 minutes:

```
index=windturbines status=offline | stats count
```

Ensure this is also a single value visualisation

We want to use colour formatting to make it clear if and when this value exceeds our acceptable thresholds

General

Color

Number Format

Use Colors ☒ Yes ☐ No

Color by ☒ Value ☐ Trend

Ranges

from	min	to	
		0	<div style="width: 20px; height: 20px; background-color: green;"></div>
from	0	to 1	<div style="width: 20px; height: 20px; background-color: orange;"></div> x
from	1	to 2	<div style="width: 20px; height: 20px; background-color: red;"></div> x
from	2	to max	<div style="width: 20px; height: 20px; background-color: red;"></div>

+ Add Range

Color Mode ☐ ☒ 42 ☒ 42

As we already have a dashboard created from the previous step, we'll add this to it.

Save As ▾

- Report
- Alert
- Existing Dashboard
- New Dashboard

Name the panel "Current Offline Devices".

Save Panel to Existing Dashboard

Select an Existing Dashboard

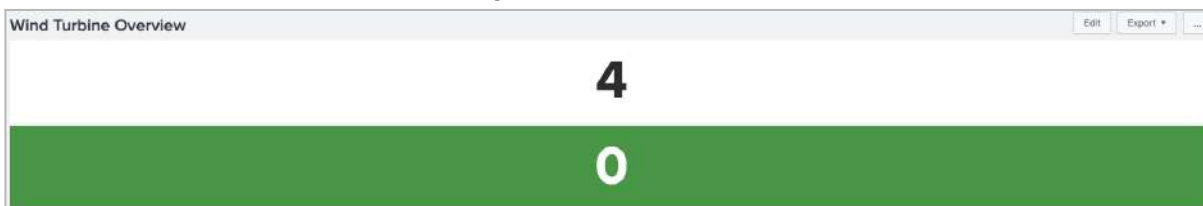
Sort: Title (A - Z) ↓

win

- ✓ Wind Turbine Overview

Ensure you **Save**, and then **View**.

Your dashboard should look something like this:



We'll add another metric to indicate how many turbines reported as being offline over last year. Run a new search, over a time range of "last year" in the time picker.

```
index=windturbines status=offline | stats count
```

Format this as a single value, using the colour formatting below

General

Use Colors ☒ Yes ☐ No

Color by ☒ Value ☐ Trend

Number Format

Ranges

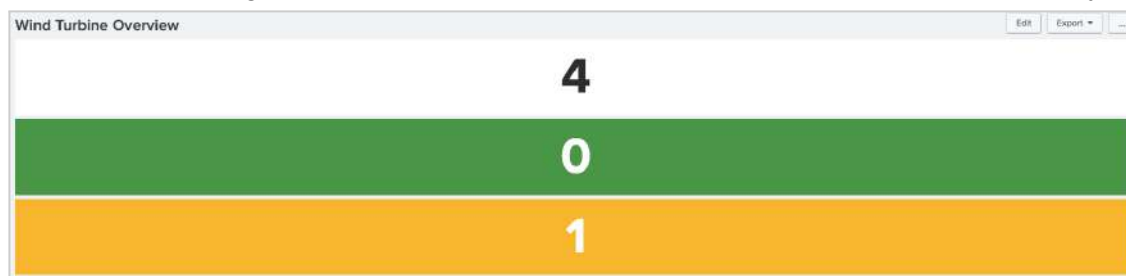
from	min	to	
		0	Green
from	0	to 1	Yellow x
from	1	to 2	Orange x
from	2	to max	Red

+ Add Range

Color Mode ☐ Value ☒ Trend

42

Save to the existing dashboard, and view. Name the panel “Total Offline Devices (1 year)”



We’d like to make better use of space here (as we’ll be adding more items shortly) so we would like these values to appear in one row. Select **Edit** from the dashboard menu.

Using the “drag lines” shown below, move two of the panels alongside each other, in a row.



Now that we know a device was offline at some point, we realise we’d like to have a chart showing when that event happened, as it might happen again.

Return to the search interface and run a search using the *status* field, and using the *timechart* command, over a 90 day period

```
index=windturbines status=offline | timechart count by TurbineNumber
```

Save this as a line chart visualisation to your existing dashboard. Edit the dashboard so it aligns to the other 3 metrics. Use a panel title of “Offline Devices by Time, Turbine Number”

## Q2: On what date did a turbine report being offline? Which turbine?

A: \_\_\_\_\_

It looks like Wind Speed could be an interesting metric to explore further. Create a new visualisation that shows the maximum wind speed over time, for each of the turbines.

**Note:** as our sample data is limited to December 2023, we will use the commands ***earliest*** and ***latest*** to narrow down to that specific time period in our search (we could also do this via the time range picker in the GUI)

```
index=windturbines earliest="11/26/2023:00:00:00" latest="12/31/2023:20:00:00"  
| timechart max("Wind Speed _m_s") by TurbineNumber
```

Save this as a line chart to your existing dashboard.

Because it's possible for IoT devices to stop reporting data (if they went "offline" for example), ensure that you use the appropriate formatting of the chart to capture this, by enabling "null values"



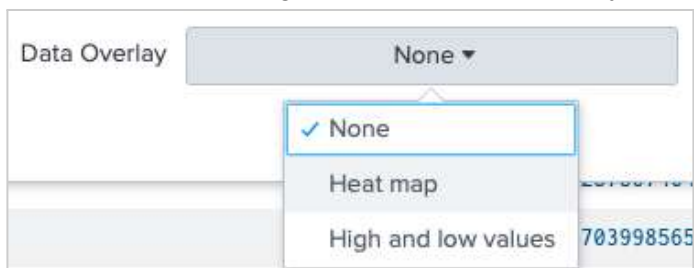
Name the panel "Max Wind Speed"

We can visually see where the peaks and troughs were for the wind speed metric, but let's confirm the top values by using a statistics table. We'll also rename fields for convenience of reporting, and sort speed from fastest to slowest.

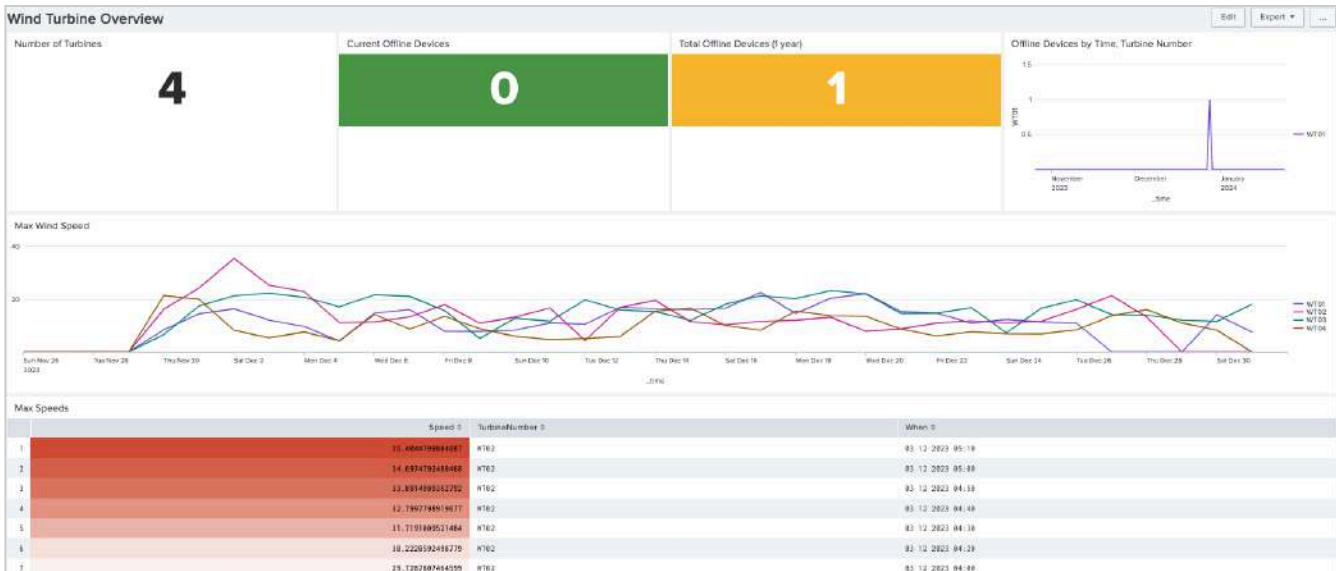
Run a new search:

```
index=windturbines | table "Wind Speed _m_s", TurbineNumber, Date_Time  
| rename Date_Time AS When, "Wind Speed _m_s" AS Speed | sort - Speed
```

Format the table using a **heat map** data overlay, and then save to dashboard.



Your dashboard should now look similar to below



**Q3: Which wind turbine produced the greatest speed? What was the speed and when did it happen?**

**A:** \_\_\_\_\_

We now have a good picture of wind speeds over time, maximum values, and also a view in status (online / offline). Let's correlate what we see...

**Q4: What was significant about the speed of WT01 on Dec 27th/28th? How does it relate to the view of offline devices over time?**

**A:** \_\_\_\_\_

Sometimes in manufacturing and IIoT, we might value seeing the location of devices, or where certain events are happening. We can use the longitude and latitude data in our wind turbine data to plot some information to a map.

Run a new search

```
index=windturbines long=* lat=*
| geostats latfield=lat longfield=long count by TurbineNumber
```

For our visualisation we need to use the **Cluster map**.



Experiment with zooming into the data (pie charts) and moving the map around so you have a good view of the specific wind turbines.

Once you are happy with the view, you can save these settings for when the map is added to the dashboard. Click **populate with current map settings**.

The screenshot shows a 'Format' panel for a 'Cluster Map'. The 'General' tab is selected, showing a 'Zoom on Scroll' toggle set to 'Yes'. Below this are input fields for 'Latitude' (0), 'Longitude' (0), and 'Zoom' (2). A link at the bottom reads 'Populate with current map settings'.

General		
Zoom on Scroll	Yes	No
Latitude	0	
Longitude	0	
Zoom	2	
<a href="#">Populate with current map settings</a>		

Save to your dashboard and view your finished work!

**Q5: What Countries are the turbines located in or near?**

**A:** \_\_\_\_\_



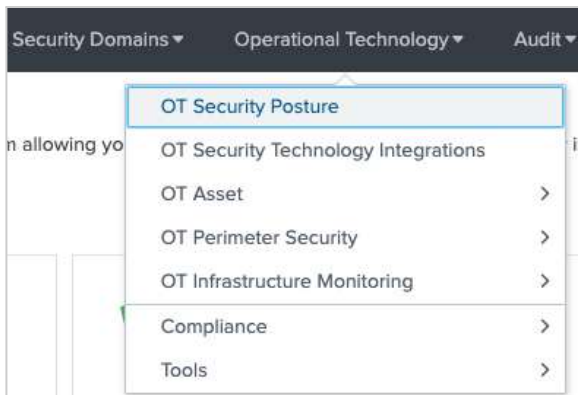
## Exercise 6 - Operational Technology: Security

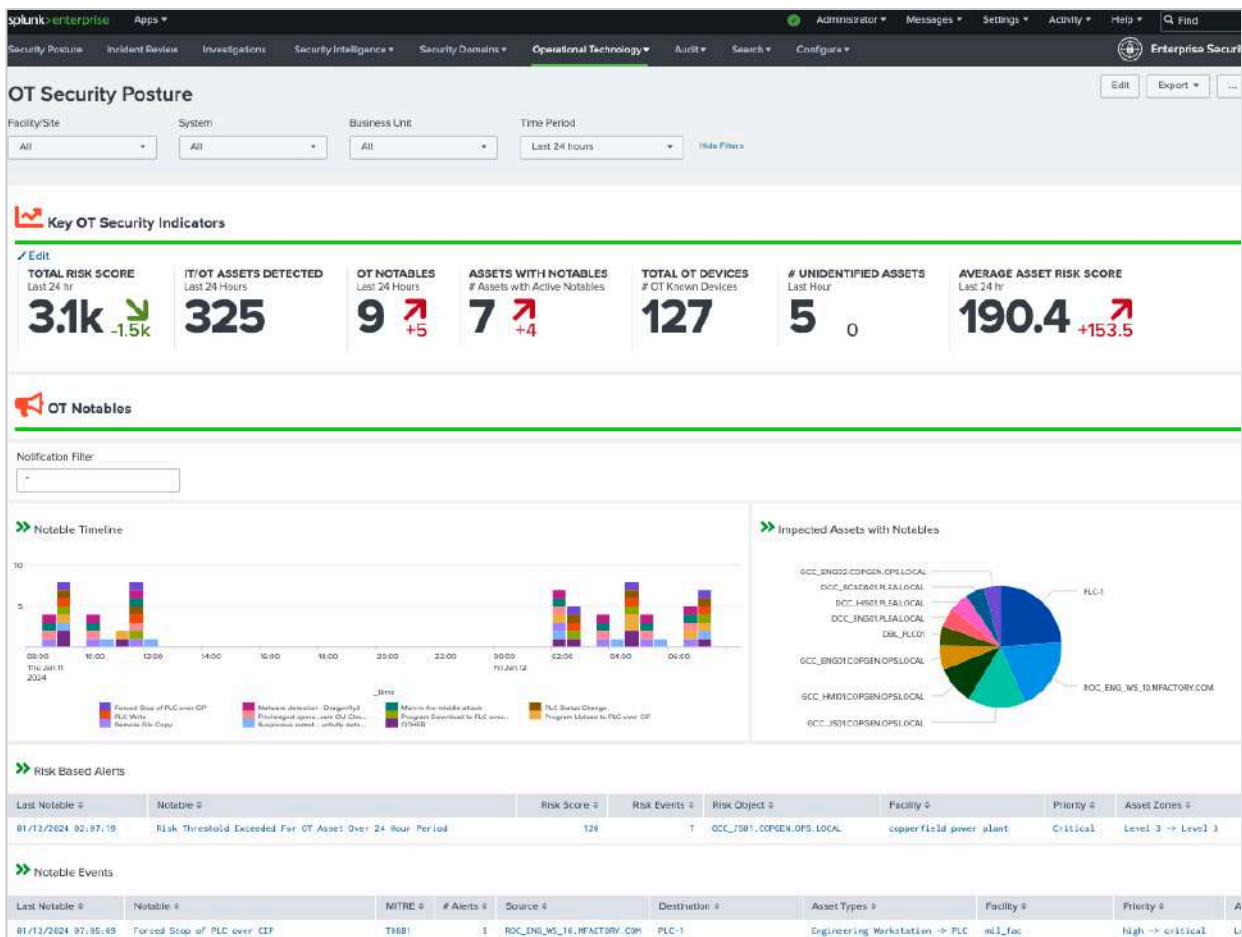
### Description

In this Exercise, you will explore the consolidation of OT data into an existing security view so that a single security team can have complete visibility of all areas of the business, encompassing both traditional IT and also OT.

### Steps

#### Navigating the OT Security Add-on





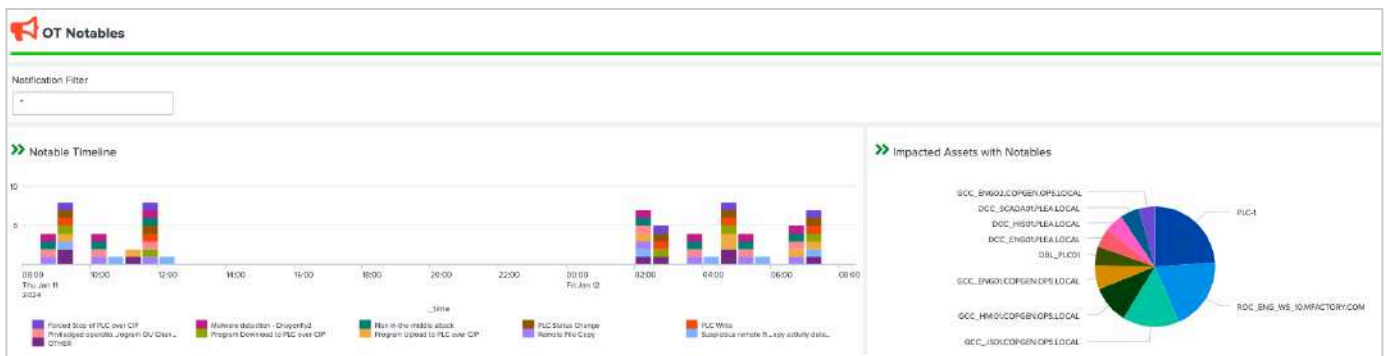
The purpose of this dashboard is to provide a high-level overview of your OT environment. This dashboard is specific only to assets and users that are part of the OT Environment.



Note the filters at the top that allow you to filter down the content at site, system or business unit level. These are completely configurable and allows security teams that may be assigned different responsibilities to find their specific content quickly.



We also provide some Key Security Indicators. These KSIs can be customised, and users can choose to add, remove or create their own, relevant to their needs.



Also provided are insights into Notable Events (Notables), which are our security alerts for the OT environment. We can see how these notables occur over time, as well as the assets that are being impacted.

Last Notable	Notable	MITRE	# Alerts	Source	Destination	Asset Types	Facility	Priority	Asset Zone
01/12/2024 07:05:09	Forced Stop of PLC over CIP	T8881	5	ROC_ENG_WS_10.FACTORY.COM	PLC-1	Engineering Workstation -> PLC	mil_fac	high -> critical	Level 2 -> Level 1
01/12/2024 07:05:09	PLC Status Change	T8816	5	ROC_ENG_WS_10.FACTORY.COM	PLC-1	Engineering Workstation -> PLC	mil_fac	high -> critical	Level 2 -> Level 1
01/12/2024 07:05:09	PLC Write	T8855	5	ROC_ENG_WS_10.FACTORY.COM	PLC-1	Engineering Workstation -> PLC	mil_fac	high -> critical	Level 2 -> Level 1
01/12/2024 07:05:09	Program Download to PLC over CIP	T8845	5	ROC_ENG_WS_10.FACTORY.COM	PLC-1	Engineering Workstation -> PLC	mil_fac	high -> critical	Level 2 -> Level 1
01/12/2024 07:05:09	Program Upload to PLC over CIP	T8808	2	ROC_ENG_WS_10.FACTORY.COM	PLC-1	Engineering Workstation -> PLC	mil_fac	high -> critical	Level 2 -> Level 1
01/12/2024 07:00:34	Suspicious remote file copy activity detected	T8867	7	GCC_JS01.COPSEN.OPS.LOCAL	GCC_HM101.COPSEN.OPS.LOCAL	Remote Access -> HMI	copperfield power plant	critical -> high	Level 3 -> Level 1
01/12/2024 06:55:14	Program Upload to PLC over CIP	T8845	21	GCC_ENG02.COPSEN.OPS.LOCAL	PLC-1	Engineering Workstation -> PLC	copperfield power plant	medium -> critical	Level 3 -> Level 1

Finally, we see the specific notables with a lot of enriched details. These are important because they add valuable context for handling these security alerts.

In this example, we can see the nature of the threat (Remote File Copy), how it relates to MITRE ATT&CK models ([T10867](#) - Lateral Tool Transfer), and the asset type (Human Machine Interface)

Last Notable	Notable	MITRE	# Alerts	Source	Destination	Asset Types	Facility	Priority
01/12/2024 08:20:17	Remote File Copy	T10867	8	GCC_JS01.COPSEN.OPS.LOCAL	GCC_HM101.COPSEN.OPS.LOCAL	Remote Access -> HMI	copperfield power plant	critical -> high

Note, the OT Security Add-on also maps onto MITRE ICS ATT&CK [model](#).

## Exploring a Notable

Drill-down into the “Remote File Copy” notable by clicking on any of the hyperlinks in that row.

Incident Review												
<div> <div> <div>Search: Remote File Copy</div> <div>Source: OT Threat - MITRE ICS Alert</div> <div>Time Range: Custom time</div> </div> <div> <div>20 per page</div> <div>Refresh</div> </div> </div>												
8 Notables	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
<input type="checkbox"/>	Remote File Copy	...	...	...	Notable	Today, 08:20	Undetermined	Threat	Medium	New	unassigned	
<input type="checkbox"/>	Remote File Copy	...	...	...	Notable	Today, 06:50	Undetermined	Threat	Medium	New	unassigned	
<input type="checkbox"/>	Remote File Copy	...	...	...	Notable	Today, 05:20	Undetermined	Threat	Medium	New	unassigned	
<input type="checkbox"/>	Remote File Copy	...	...	...	Notable	Today, 03:50	Undetermined	Threat	Medium	New	unassigned	

Note how we are now leveraging the Incident Review capability within Splunk Enterprise Security, to give a holistic “SOC” experience (IT & OT consolidation).

We can see all the incidents that matched our notable from the OT Security Overview dashboard. Expand the incident to get more information as well as the assets and users involved.

Expand any of the notables by clicking on the “>” icon

8 Notables [Unselect all](#) [Edit Selected](#) [Edit All Matching Events \(8\)](#) [Add Selected to Investigation](#) 20 per page [Refresh](#)

Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
Remote File Copy				Notable	Today, 08:20	Undetermined	Threat	Medium	New	unassigned	

**Description:**  
An indicator of a MITRE ICS Attack was detected by fore scout. IP 172.104.104.98 has initiated SMBv1 remote file copy, its victims are: 172.104.1.104, 172.104.1.103

Additional Fields	Value	Action
Action	allowed	
Application	fore scout	
Category	Remote File Copy	
Description	IP 172.104.104.98 has initiated SMBv1 remote file copy, its victims are: 172.104.1.104, 172.104.1.103	
Destination	f4:54:33:20:20:00 <span>120</span>	
Destination Business Unit	ga plant ops	
Destination Category	nerc	
	workstation	
	windows	
	generation	
	ot	
	hmi	
	bca	
Destination City	atlanta, ga	
Destination Country	us	
Destination DNS	gcc_hmi01.copgen.ops.local	
Destination IP Address	null	

**Related Investigations:**  
Currently not investigated.

**Correlation Search:**  
[Threat - OT Sec - MITRE ICS Alert - Rule 12](#)

**History:**  
[View all review activity for this Notable Event](#)

**Original Event:**

```
{
  "id": "234",
  "type_id": "SIGN:SMB",
  "name": "Remote File Copy",
  "description": "IP 172.104.104.98 has initiated SMBv1 remote file copy, its victims are: 172.104.1.104, 172.104.1.103",
  "severity": 0,
  "mac_src": "08:1e:15:21:21:aa",
  "mac_dst": "f4:54:33:20:20:00",
  "ip_src": null,
  "ip_dst": null,
  "risk": "10.0",
  "protocol": null,
  "src_roles": null,
  "dst_roles": null,
  "time": 1705068384,
  "ack": false,
  "id_src": "08:04:23:e0:04:1c",
  "id_dst": null,
  "synchronized": false,
  "appliance_id": "",
  "port_src": null,
  "port_dst": "137",
  "label_src": null,
  "label_dst": null,
  "trigger_id": null,
  "trigger_type": null,
  "appliance_host": "otsec01",
  "appliance_ip": "10.0.1.45",
  "transport_protocol": "unknown",
  "is_security": true,
  "note": null,
  "appliance_site": null,
  "parents": [],
  "is_incident": false,
  "properties": {
    "is_src_node_learned": true,
    "bad_actor": "08:1e:15:15:d2:d3",
    "remediation_target": "08:1e:15:15:d2:d3",
    "victims": ["172.104.1.104", "172.104.1.103"]
  }
}
```

[View original event](#)

**Adaptive Responses:**

Response	Mode	Time	User	Status
Notable	saved	2024-01-12T08:20:12-0600	admin	success

We can see the description of the alert, and more information about why it was flagged.

Title	Risk Object	Risk Score	Risk Events	Type	Time
Remote File Copy				Notable	Today, 08:20

**Description:**  
An indicator of a MITRE ICS Attack was detected by fore scout. IP 172.104.104.98 has initiated SMBv1 remote file copy, its victims are: 172.104.1.104, 172.104.1.103

Additional Fields	Value	Action
Action	allowed	
Application	fore scout	
Category	Remote File Copy	
Description	IP 172.104.104.98 has initiated SMBv1 remote file copy, its victims are: 172.104.1.104, 172.104.1.103	
Destination	f4:54:33:20:20:00 <span>120</span>	
Destination Business Unit	ga plant ops	
Destination Category	nerc	
	workstation	
	windows	
	generation	
	ot	
	hmi	
	bca	
Destination City	atlanta, ga	
Destination Country	us	
Destination DNS	gcc_hmi01.copgen.ops.local	

We see a categorisation of the asset (various), what type of machine it is. Looking at the source, we can see the mac address that was part of the alert, and its corresponding risk score.

Session Identifier	null	
Severity	unknown	
Signature	Remote File Copy	
Source	0d:1e:15:21:21:aa	240
Source Business Unit	ga plant ops	
Source Category	nerc	
	workstation	

The mac address may not always be helpful to an analyst, but we see also the IP address and hostname, which may be more meaningful. We can learn more about this asset by selecting “OT Asset Investigator” from the action menu (down arrow symbol).

	generation	
	ot	
	jump server	
	pca	
Source City	atlanta, ga	
Source Country	us	
Source DNS	gcc_js01.copgen.ops.local	
Source IP Address	172.104.104.98	
Source Expected	true	
Source Latitude	33.734375	
Source Longitude	-84.372268	
Source MAC Address	0d:1e:15:21:21:aa	
Source NT Hostname	gcc_js01	

Intrusion Search (as destination)  
Intrusion Search (as source)  
Notable Event Search  
Malware Search  
Nbtstat gcc\_js01  
Nslookup gcc\_js01  
OT Asset Investigator  
OT Host Access Monitoring  
Ping gcc\_js01

The OT Asset Investigator is designed to help us understand assets and their behaviours.

### OT Asset Investigator

Specify an asset to populate details

Investigating Asset: gcc\_js01 Time Window: Last 24 hours

#### Asset Details: gcc\_js01

# Detected Vulnerabilities: 0

# Notables: 1

Prohibited Traffic Across Perimeter: 31 35%

Field	Value	Field	Value
ip	172.104.104.98	category	nerc
nt_host	gcc_js01		workstation
dns	gcc_js01.copgen.ops.local		windows
mac	0d:1e:15:21:21:aa		generation
asset_id			ot
priority	critical		jump server
asset_system	cop		pca
description	copperfield plant jump server	asset_model	proliant d1380
bnmt	ga plant ops	asset_vendor	hewlett packard
owner	occ	asset_type	Remote Access
site_id	copperfield power plant	classification	cip:high
city	atlanta, ga		cip:pca

Geographical Info

ip: 172.104.104.98  
host: gcc\_js01  
type: remote access  
description: copperfield plant jump server  
site: copperfield power plant  
city: atlanta, ga (us)

Here we are looking at the asset “gcc\_js01”.

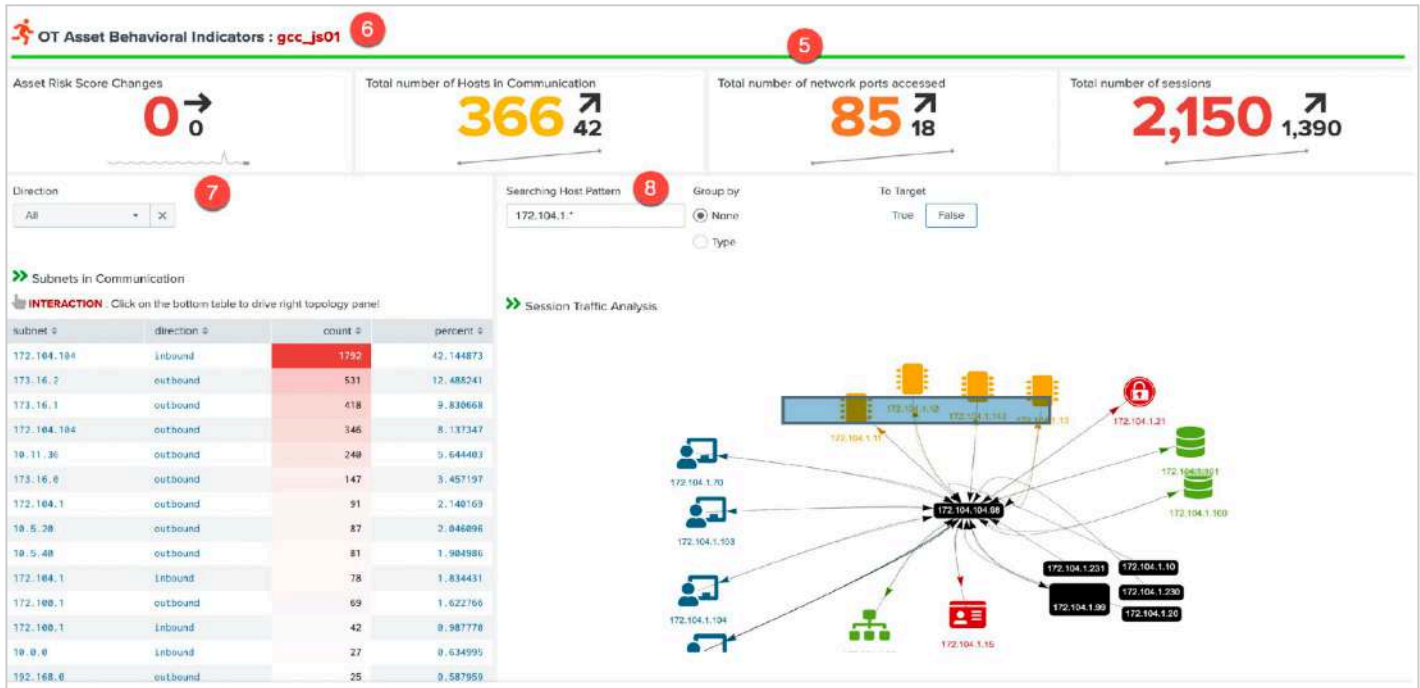
This view provides information about the asset such as IP address, mac address, but also site, description and location.



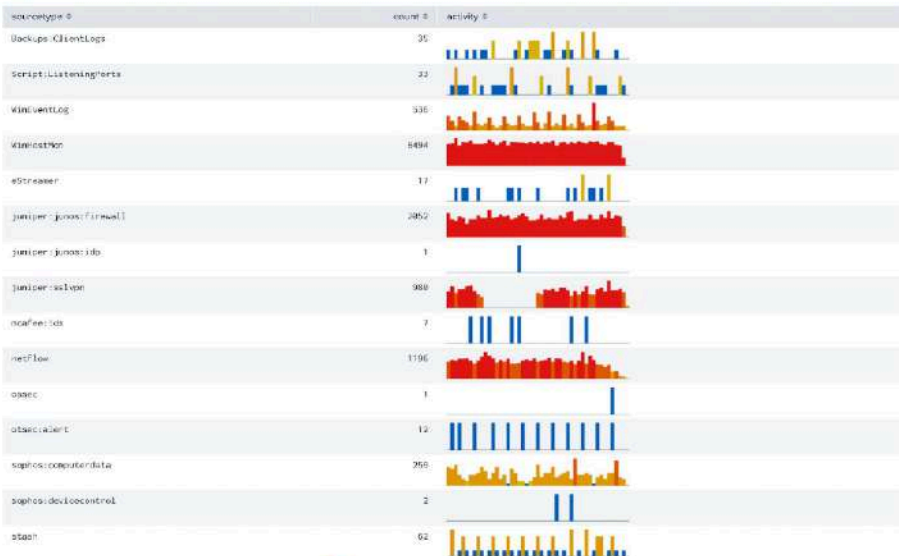
**Q: What is the location of this asset? A:** \_\_\_\_\_

Additionally, we see categories, security classifications, and the physical location of the asset on a map.

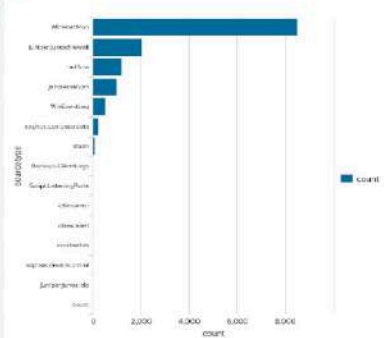
**Q: Where does the asset seem to be located? A:** \_\_\_\_\_



### Activity by Sourcetype

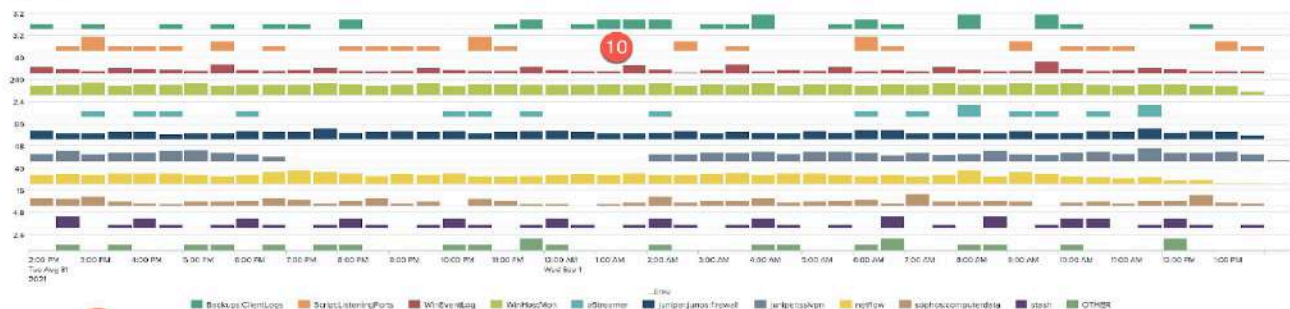


### Activity Volume by Sourcetype



### Sourcetype Timeline Drilldown : gcc\_js01 9

INTERACTION: Click on the bottom timeline to drilldown bottom detail panel



Time	Sourcetype	src	src_port	src_asset_type	dest	dest_port	dest_asset_type	signature	row
2021-09-01 13:58:58	Backups:ClientLogs				gcc_js01		remote access	01-01-2021 13:58:58 GCC_JS01 Info <48862> - GSAH connected via: IPv4, retrieved Data Domain IPv4 hostname = backup01	
2021-09-01 17:37:54	Backups:ClientLogs				gcc_js01		remote access	01-01-2021 17:37:54 GCC_JS01 Info <5010> - Successfully logged into backup server (backup01) (compression enabled)	
2021-09-01 18:19:45	Backups:ClientLogs				gcc_js01		remote access	01-01-2021 18:19:45 GCC_JS01 Info <10480> - Resolved Data Domain Server name "backup01.opconenergy.com" to the IP address "10.23.1.45"	
2021-09-01 18:55:58	Backups:ClientLogs				gcc_js01		remote access	01-01-2021 18:55:58 GCC_JS01 Info <10480> - Resolved Data Domain Server name "backup01.opconenergy.com" to the IP address "10.23.1.45"	
2021-09-01	Backups:ClientLogs				gcc_js01		remote access	01-01-2021 18:55:58 GCC_JS01 Info <7510> - Back up of "/" on server "backup01" for /clients/GCC_JS01	

## Exercise 7 - Business Service Insights: exploring capability

### Description

Service Insights in IT Service Intelligence (ITSI) represents the mapping and monitoring of business and technical services within your organisation. The information derived from Service Insights helps you better detect problems, simplify investigations, triage issues, and accelerate resolutions.

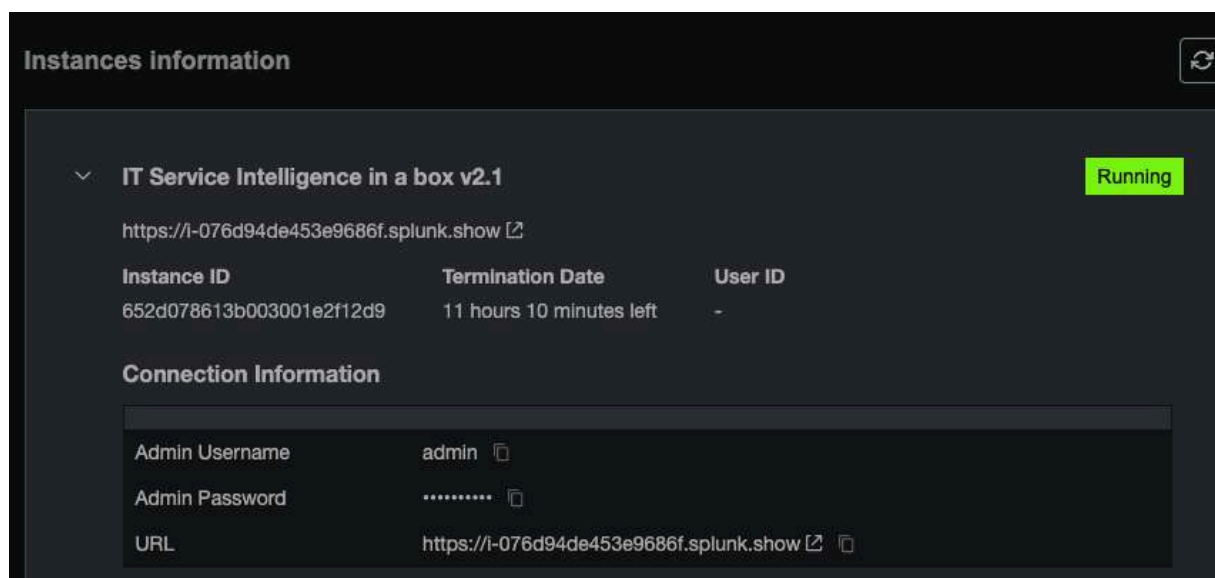
Within ITSI, a service is a set of interconnected applications and hosts that are configured to offer a specific service to the organisation. Services can be internal, like an organisation email system, or customer-facing, like an organisation's website. For example, creating financial reports through a web-based application requires a computer, web server, application server, databases, middleware, and network infrastructure. These applications and hosts are all configured to offer the service of financial reporting.

For the next few steps, we will be using an example service from the Financial Services Industry (to show that any organisation can make use of service monitoring). We will then switch back to some manufacturing use cases.

### Steps

#### Switching lab environment

For the remainder of the labs, you will using the “IT Service Intelligence in box” instance



**Instances information**

IT Service Intelligence in a box v2.1 Running

<https://i-076d94de453e9686f.splunk.show>

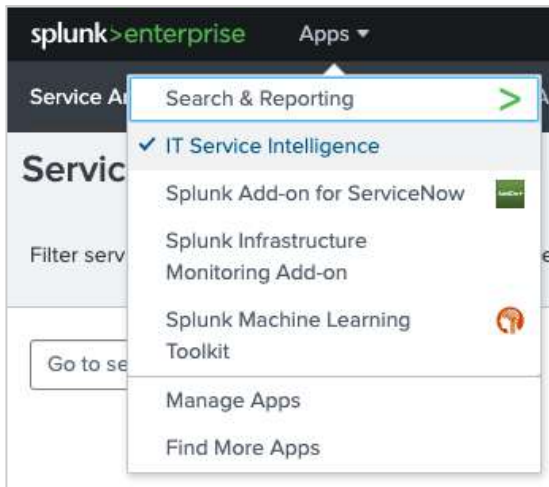
Instance ID	Termination Date	User ID
652d078613b003001e2f12d9	11 hours 10 minutes left	-

**Connection Information**

Admin Username	admin
Admin Password	.....
URL	<a href="https://i-076d94de453e9686f.splunk.show">https://i-076d94de453e9686f.splunk.show</a>

Navigate to the “IT Service Intelligence” app, if not already taken there after logging in



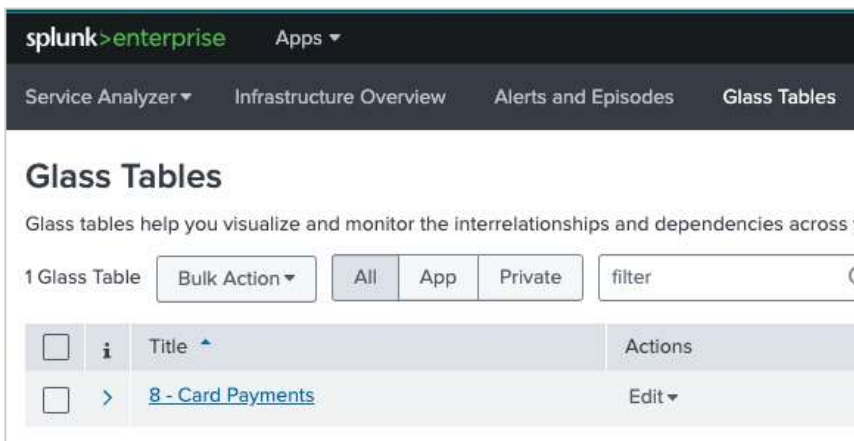


## Exploring a Glass Table view

Glass tables allow users to visualise and monitor the interrelationships and dependencies across your IT and business services. You can use glass tables to create dynamic contextual views of your IT topology or business processes and monitor them in real time. You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

Let's explore an example Glass Table that was built to represent a "Card Payments" process that mirrors what a commercial/retail bank may need to monitor.

Locate the "Card Payments" Glass Table by selecting the **Glass Tables** tab from the ITSI main menu



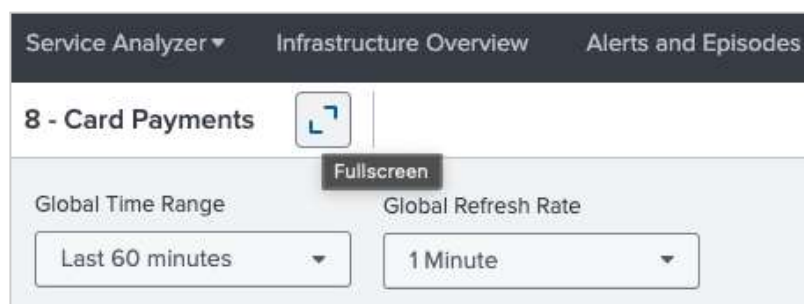
Select the hyperlink "8 - Card Payments" to view the Glass Table

---

Note that there are several other example Glass Tables which you are free to explore throughout today

---

Expand the Glass Table by selecting the **Fullscreen** icon:



Please review the following questions to help identify what we can learn about the information presented to the user. Remember that Glass Tables are completely customisable for all types of audience, so this a demonstration of the “art of the possible” - you are only limited by your imagination!

**Q1: Service Health - which of the 4 services has the lowest/worst health score?**

**A:** \_\_\_\_\_

**Q2: KPIs - how many Fraud alerts have occurred in the last hour?**

**A:** \_\_\_\_\_

**Q3: What’s the main reason that Confirmation has a low score?**

**A:** \_\_\_\_\_

**Q4: What technical components are involved in this degradation? (HINT: Use the lowest layer of the diagram to find this)**

**A:** \_\_\_\_\_

## Exploring a Service Analyzer

The Service Analyzer is the home page for Splunk IT Service Intelligence (ITSI) and serves as your starting point for monitoring your IT operations. The Service Analyzer enables you to see the health of your IT environment at a glance.

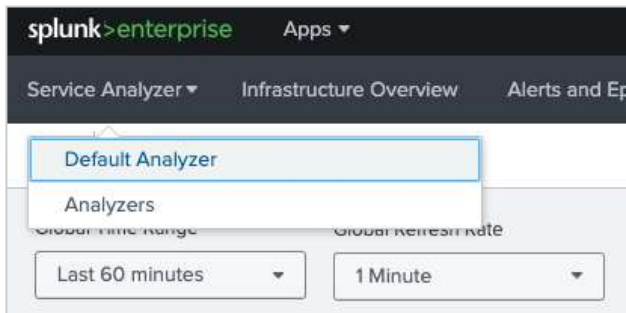
The Service Analyzer provides an overview of ITSI service health scores and KPI search results that are currently trending at the highest severity levels. Use the Service Analyzer to quickly view the status of IT

operations and to identify services and KPIs running outside expected norms. Click on any tile in the Service Analyzer to drill down to the deep dives for further analysis and comparison of search results over time.

There are two service analyzer views: the tile view and the tree view. You can drill down to more detailed information from each view to investigate services with poor health scores.

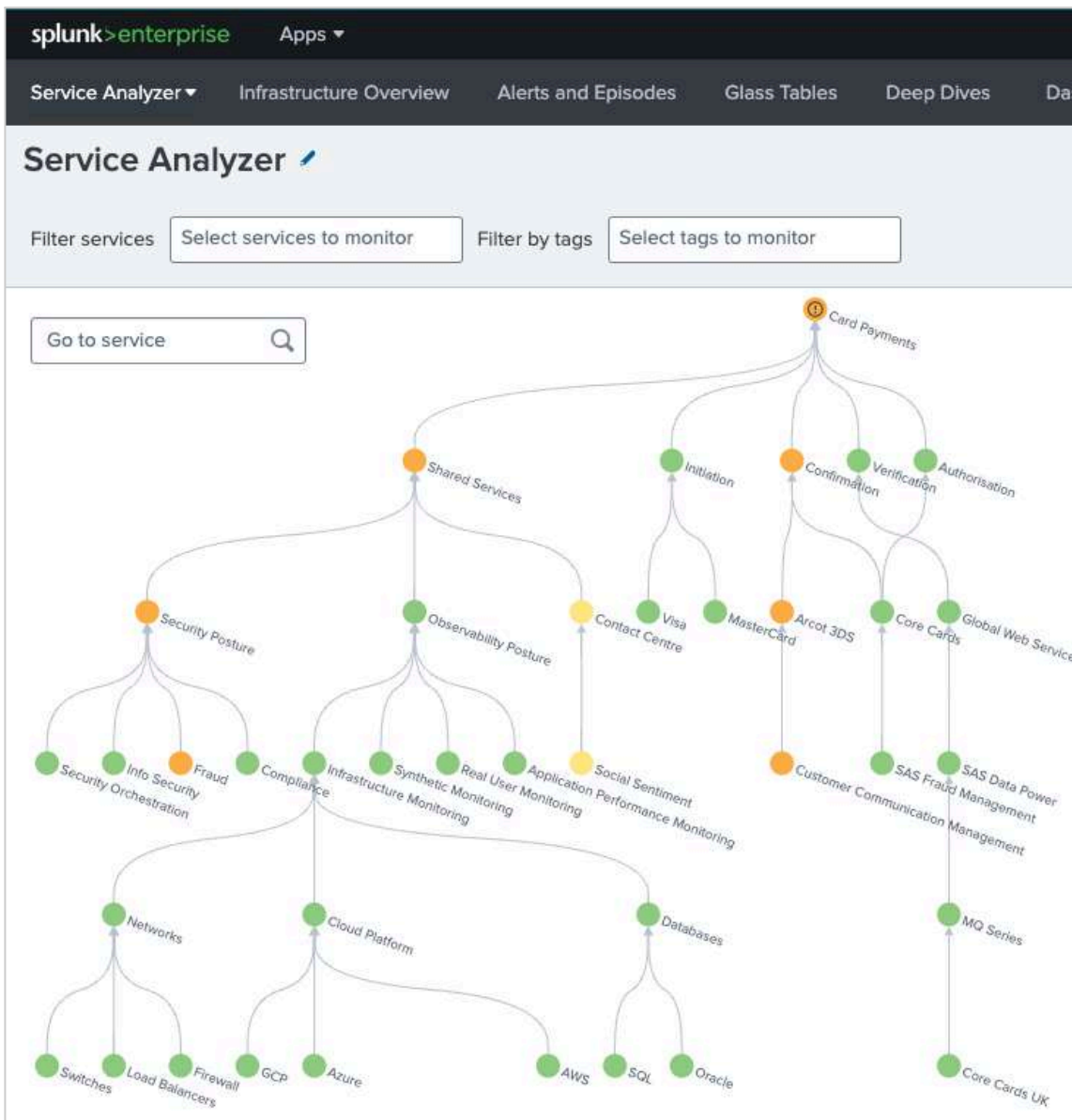
To access the Service Analyzer, click **Service Analyzer > Default Service Analyzer** from the ITSI main menu. The tile view is the default view, but whichever view you last saved loads the next time you open the Service Analyzer.

Navigate to the Default Analyzer via **Service Analyzer** tab:



You should see a service tree diagram similar to below. If you cannot see the whole tree, use the **center** icon and the **zoom in / zoom out** controls to fit everything into your screen. Also use your mouse to zoom in and out:





Please review the following questions to learn how the Service Analyzer can be used to determine likely root causes of issues

**Q5: There are actually a number of services impacting Card Payments - name 2 of them. HINT: focus on the root cause.**

Locate the KPIs for the Card Payment service by selecting the icon below



## Q6: How many KPIs are there and what are their severities?

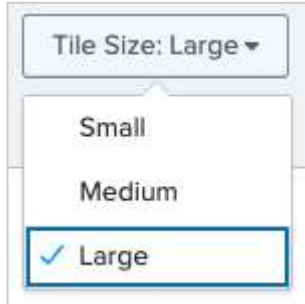
Experiment toggling between Hierarchy view and Tile view:



In the Tile view, use the cog icon, reduce the number of services that appear in the tile view



and experiment with different tile sizes



## Exploring Deep Dive view

Deep dives are an investigative tool to help you identify and troubleshoot issues in your IT environment in IT Service Intelligence (ITSI). Use deep dives to view KPI search results over time, zoom-in on KPI search results, and visually correlate root cause. Stack and organise deep dive lanes to create contextual views of metrics across your services.

You can use deep dives to quickly zoom in on metric and log events, and visually correlate root cause. You can create swim lanes for both KPI and ad hoc searches, and you can customise the look of your swimlanes with unique graph types and colours to differentiate services and metrics.

We need to pivot into an investigative view of what's going using a view called **Deep Dive**.

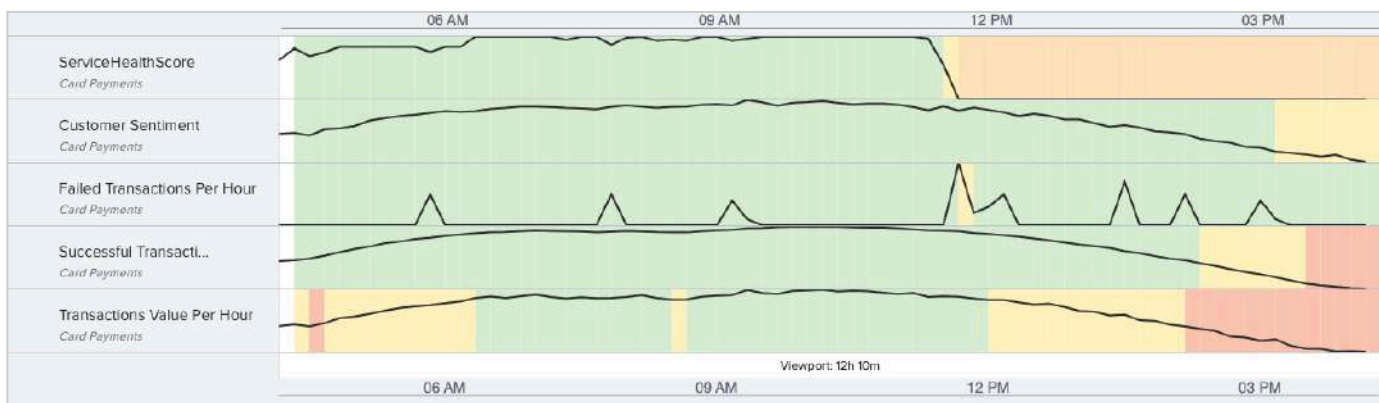
In the Tree view of **Service Analyzer**, access **Deep Dive** via the Card Payment service. Ensure Card Payment icon has been selected.



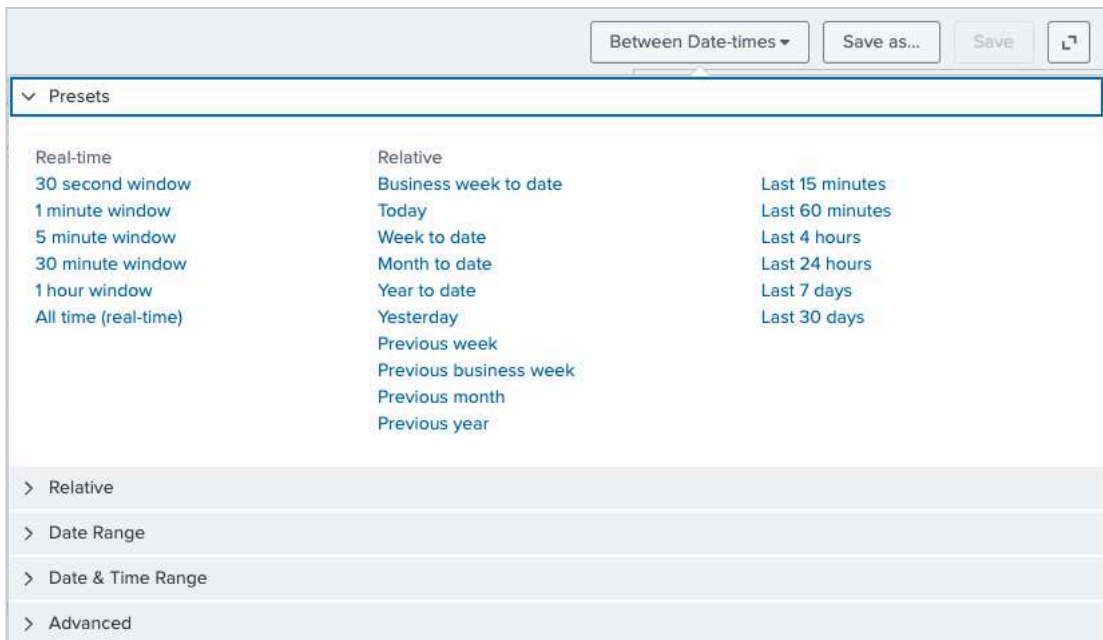
Then select **Open all in Deep Dive** link



Here we see the RAG value of KPIs over any given time range, and we can see their relationship to each other.

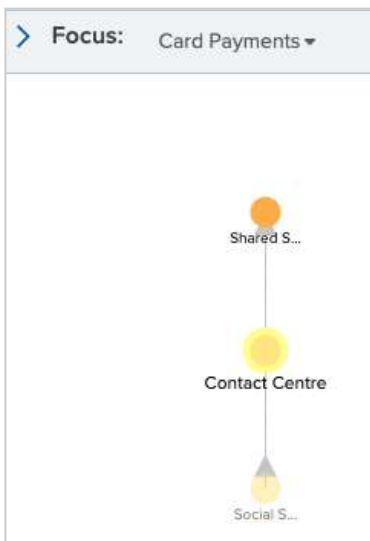


As this is Splunk, we have full control over the time range of the data displayed. Experiment with different settings e.g. 15 mins, 60 mins etc.



Although we are looking at the KPIs for the **Card Payment** service, we can pull in any business or technical KPIs from any other service. Let's add a KPI from the **Social Sentiment** service.

In the Focus view to the right of the swim-lane view, view the Contact Centre KPIs under **Card Payments > Shared Services > Contact Centre**



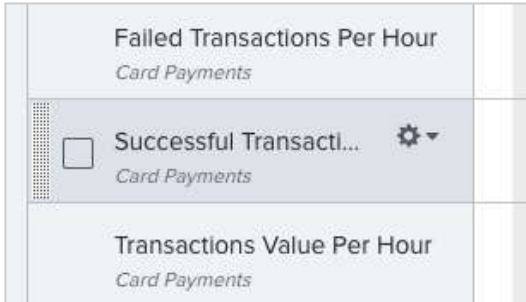
Note the various KPIs available and their individual values (red/amber/green)

### Q7: Which KPIs look particularly problematic?

Add it into the deep dive view (if none stand out, pick one that is red / amber)



As this is a timeline view (from left to right), it would be good to be able to reorder these swimlanes, or lessen the focus on the KPIs that aren't impacting service performance. Experiment with moving the swimlanes around using the "drag" icon. You'll need to mouse over each swimlane name to see this.



## Create a multi-KPI alert

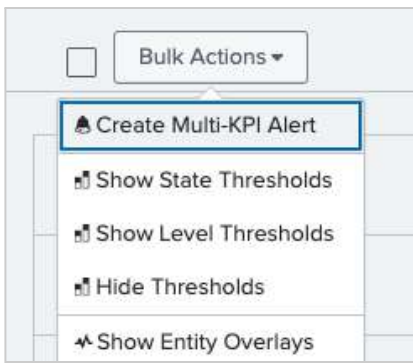
Rather than being alerted when individual thresholds are breached, we want to create a "multi-KPI alert" - something where we will only be alerted if a number of thresholds are breached, using a determination of our own choosing.

Select a couple of KPIs



And then select the Bulk Action button to navigate to the alert config screen





3 KPIs — Remove Selected — View Selected in Deep Dive  10 per page ▾

<input type="checkbox"/>	i	Remove	KPI	Service	Latest Status	Importance
<input checked="" type="checkbox"/>	>	Remove	Customer Sentiment	Card Payments	High	1 <input type="range"/> 11
<input checked="" type="checkbox"/>	>	Remove	Transactions Value Per Hour	Card Payments	High	1 <input type="range"/> 11
<input checked="" type="checkbox"/>	>	Remove	Response Rate	Contact Centre	Low	1 <input type="range"/> 11

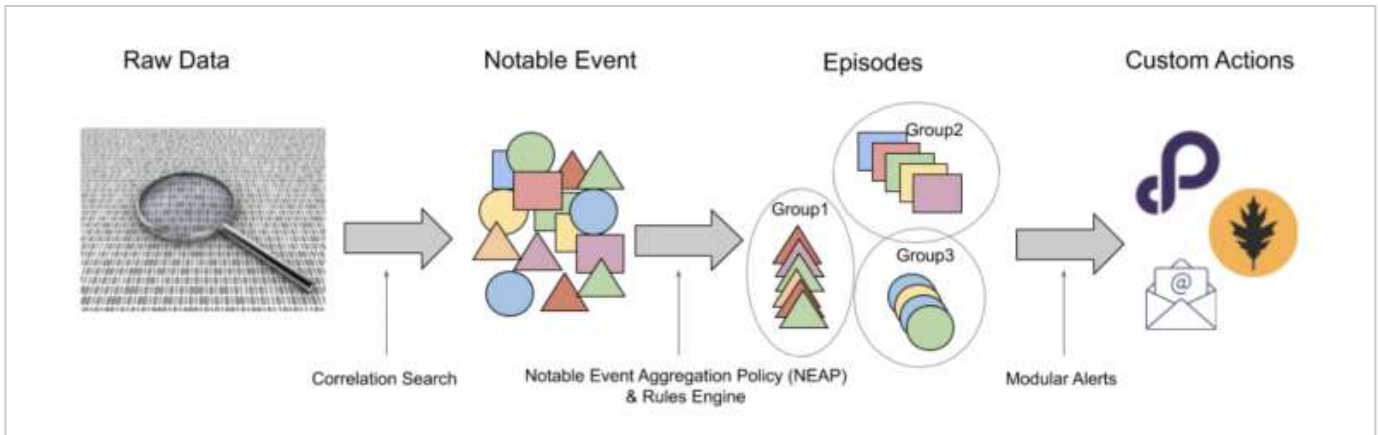
No need to save changes - there are many configurable options in this screen which we will not cover today, but are covered in our in-depth workshops.

## Exploring Alerts & Episodes View

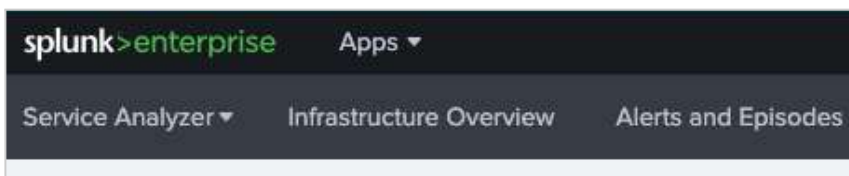
Splunk IT Service Intelligence (ITSI) Event Analytics ingests events from across your IT landscape and from other monitoring silos to provide a unified operational console of all your events and service-impacting issues. You can also integrate with incident management tools and help desk applications to accelerate incident investigation and automate remedial actions.

Event Analytics is equipped to handle huge numbers of events coming into ITSI at once. Because these events might be related to each other, they must be grouped together so you can identify the underlying problem. Event Analytics provides a way to deal with this huge volume and variety of events.

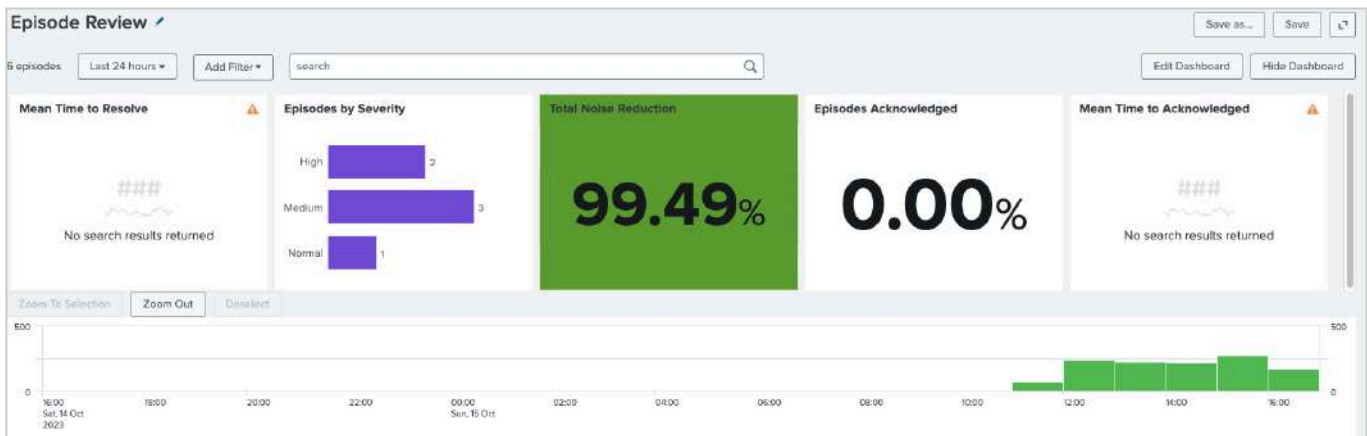
Aggregation policies reduce your event noise by grouping notable events based on their similarity and displaying them in Episode Review. An episode is a collection of notable events grouped together based on a set of predefined rules. An episode represents a group of events occurring as part of a larger sequence, or an incident or period considered in isolation. Aggregation policies let you focus on key event groups and perform actions based on certain trigger conditions, such as consolidating duplicate events, suppressing alerts, or closing episodes when a clearing event is received.



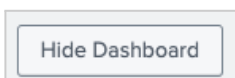
Navigate to the **Alerts and Episode** view via the main menu



The Episode Review dashboard provides insights in high-level metrics around noise reduced through improved filtering and alerting of events



We can hide this for now:



Before proceeding, ensure that **Episode View** is set to **Off** via the configuration cog icon:

Show Dashboard

Toggle the “Episode View” setting as necessary, and click **Done**:

View Settings

Viewing Option

Standard

Episode View

Off

Done

**Q8: How many events have occurred in the last 2 hours (your results may differ from screenshot below)?**

Service Analyzer

Infrastructure Overview

Alerts

> Episode Review

588 events

Last 2 hours

Add Filter

Sorted by Time

+ Add sub-sort

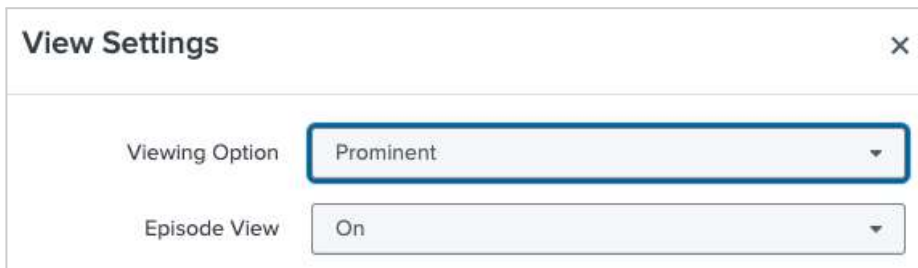
Note that you can change how events are sorted, and add additional sort settings. Try sorting by **Severity**, and then add a **sub-sort** field.

Sorted by Severity Time

+ Add sub-sort

Count	Title
1	"Transactions Value Per Hour" is HIGH for "Card Payments"
1	"Transactions Value Per Hour" is HIGH for "Card Payments"

Now turn on **Episode View** back to **On** and also ensure **Prominent** is selected from **Viewing Option**:

A screenshot of a 'View Settings' dialog box. The dialog has a title bar with 'View Settings' and a close button (X). Inside, there are two settings: 'Viewing Option' with a dropdown menu showing 'Prominent' and a blue border, and 'Episode View' with a dropdown menu showing 'On'.

**Q9: How many are there now? More or Less? Why do you think that is? Hint: click on one of the episodes for more information.**

**Congratulations - you have successfully navigated through IT Service Intelligence.**

---

## Exercise 8 - Business Service Insights: building out a service view

### Description

Now that you have explored some of the key features of ITSI, now is the time for you to start building out a few examples yourself.

### Steps

#### Expand an existing service for Manufacturing

Rather than building out a service completely from scratch, which would mean creating all of the service dependencies by hand, we have created an example for you, based on some possible scenarios in Manufacturing.

**Note:** Splunk has an *import from CSV* feature which means that complex services with many dependencies can be modelled using a pre-defined .csv file template, to save on manual configuration time.

For this lab, we have provided a .csv file for you to import. Navigate to the Splunk google drive repository for the asset needed for this lab: <https://splk.it/Manu-Lab-Assets>. Download to your local machine the file "ITSI\_Manu.csv".

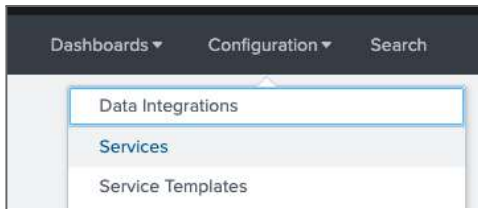
From this file, we are going to create an example manufacturing service tree for our fictional organisation "Splunk Widget Co.".

Open/Edit the file and confirm that the file looks similar to below:

	A	B	C
1	<b>Service</b>	<b>Service Description</b>	<b>Dependent Services</b>
2	Splunk Widget Co.		Product Assembly Line, IIoT Monitoring, Order Management, Warehouse Management, Shipping Management, Inventory
3	Product Assembly Line	Sub-service of Splunk Widget Co.	Robots, Misc Infra, Carts, Conveyor Belts
4	Warehouse Management	Sub-service of Splunk Widget Co.	Forklifts
5	IIoT Monitoring	Sub-service of Splunk Widget Co.	Drones, Turbines, Sensors
6	Robots	Sub-services of Product Assembly Line	Welding Robots, Painting Robots, Automated Inspection
7	Misc Infra	Sub-services of Product Assembly Line	ERP/CRM, 3rdPartyAPIs, 5G, WiFi

#### Import the service template

From within ITSI, navigate to the services configuration via **Configuration** tab in main menu, and select **Services**.



From here, create select the **Create Service** drop-down button and choose the **Import from CSV** option:



The UI will ask you to drop a file into the UI, or allow you to browse a file from your local device. Use the **ITSI\_Manu.csv** you downloaded in the previous step so that you have something similar to:

**Entity/Service Import**

Import CSV | Select Columns | Done

**Import CSV**

Drop your file here or [browse](#)

ITSI\_Manu.csv

**File Preview - 6 total lines**

#	Dependent Services	Service	Service Description
1	Product Assembly Line, IIoT Monitoring, Order Management, Warehouse Management, Shipping Management, Inventory	Splunk Widget Co.	
2	Robots, Misc Infra, Carts, Conveyor Belts	Product Assembly Line	Sub-service of Splunk Widget Co.
3	Forklifts	Warehouse Management	Sub-service of Splunk Widget Co.
4	Drones, Turbines, Sensors	IIoT Monitoring	Sub-service of Splunk Widget Co.
5	Welding Robots, Painting Robots, Automated Inspection	Robots	Sub-services of Product Assembly Line
6	ERP/CRM, 3rdPartyAPIs, 5G, WIFI	Misc Infra	Sub-services of Product Assembly Line

Select Next to proceed to configure the import settings



We need to ensure that each column in the .csv file is correctly interpreted, so copy the settings use in the image below:

### Specify Columns

Select the columns to import and how they should be converted to ITS! object data type (service or entity). If you are importing entities, you must specify one column as the Entity Title. If you are importing services, you must specify one column as the Service Title.

Column Name	Import Column As	Sample Values From Search
Dependent Services	Dependent Services ▼	Product Assembly Line, IIoT Monitoring, Order Management, Warehouse Management, Shipping Management, Inventory
Service	Service Title ▼	Splunk Widget Co.
Service Description	Service Description ▼	

It is useful to select **Import Service As** “Enabled” as that means that the service will effectively be “live” when we start to add KPIs and Health Scores into the configuration.

### Settings

Service Team
Global ▼

Import Services As
Enabled ▼

The preview in the UI should look like this:

### Preview

The preview displays your imported entity and service information. It does not show final merged values.

Services to be Imported
Service Dependency Tree
Entities to be Imported

6 services

Service Title	Service Description	Service Tags	Dependent Services	Link to Service Template
Splunk Widget Co.			Product Assembly Line, IIoT Monitoring, Order Management, Warehouse Management, Shipping Management, Inventory	
Product Assembly Line	Sub-service of Splunk Widget Co.		Robots, Misc Infra, Carts, Conveyor Belts	
Warehouse Management	Sub-service of Splunk Widget Co.		Forklifts	
IIoT Monitoring	Sub-service of Splunk Widget Co.		Drones, Turbines, Sensors	
Robots	Sub-services of Product Assembly Line		Welding Robots, Painting Robots, Automated Inspection	
Misc Infra	Sub-services of Product Assembly Line		ERP/CRM, 3rdPartyAPIs, 5G, WiFi	

When ready, select **Import**

Import

and confirm it completed ok

✓ Import Completed in 3 seconds

Monitor the CSV on disk to set up recurring imports. [Learn more](#)

Services

[View all services](#)

22 services created/updated.

Entities

[View all entities](#)

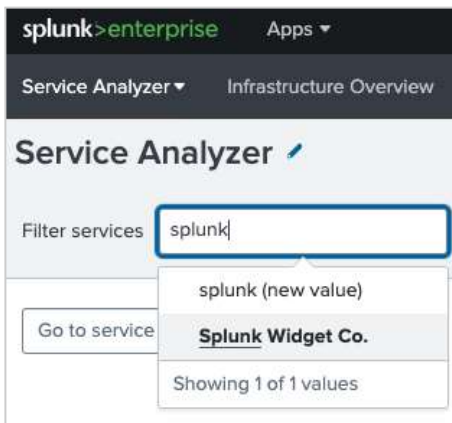
0 entities created/updated.

Let's now confirm everything is set up as needed.

### View Service Tree for Splunk Widget Co.

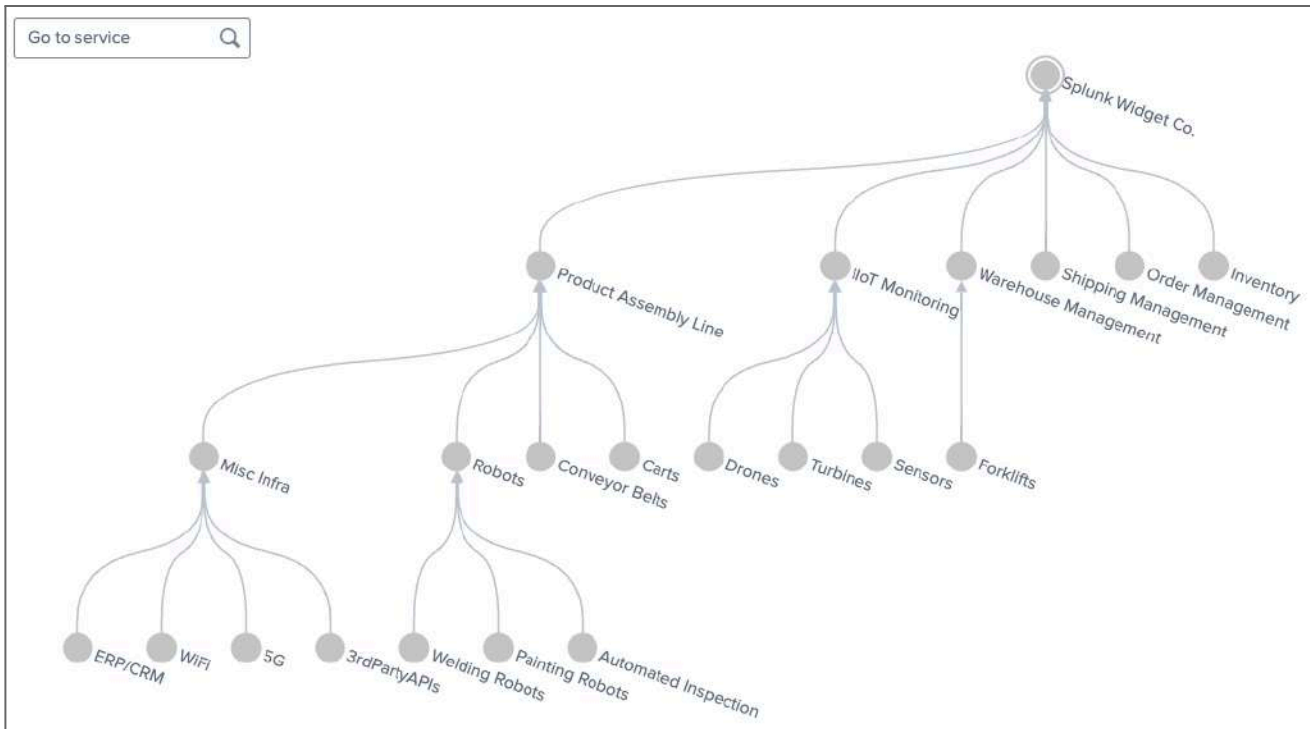
Return to the **Service Analyzer** view. You should see that there are two hierarchies represented, one for **Card Payments**, and one for **Splunk Widget Co.** We are going to filter only on **Splunk Widget Co.** from now on.

Type **splunk** into the **Filter services** input and select **Splunk Widget Co.** when it becomes available to choose.



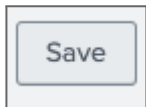
Once filtering is complete, you should see a view of everything contained within the configuration for Splunk Widget Co.





Note: All items will be greyed out because we have not yet created any KPIs for the services involved.

For convenience, we will save this view to become the new **Default Analyzer** view.



## Add a new service to IIoT Monitoring

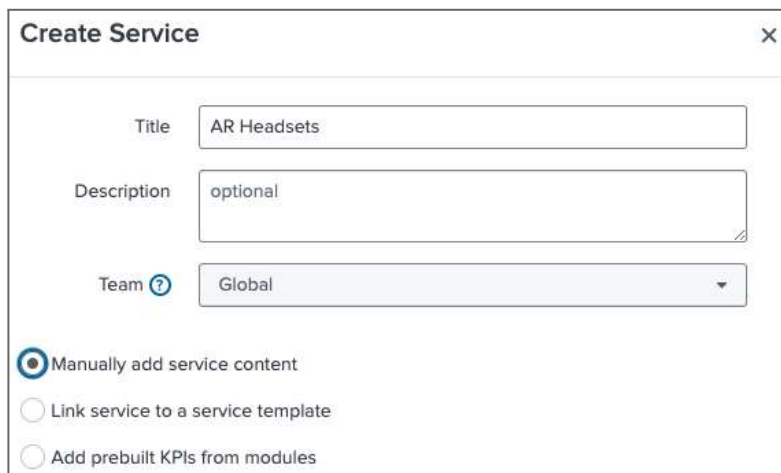
Before we start adding some KPIs for the service, we will quickly walk through the process of adding a new service to an existing service tree. Currently, for the **IIoT monitoring** service, we have 3 sub-services; **Drones**, **Turbines** and **Sensors**. We are going to add 1 more, namely **AR Headsets**.

Add a new service by selecting the **Configuration** tab from the main menu and then **Services** from drop-down.

Create a new service via the green button and drop-down



Name the service as appropriate, using the “manually add service content” option:



The 'Create Service' dialog box contains the following fields and options:

- Title:** AR Headsets
- Description:** optional
- Team:** Global (dropdown menu)
- Options:**
  - ☒ Manually add service content
  - ☐ Link service to a service template
  - ☐ Add prebuilt KPIs from modules

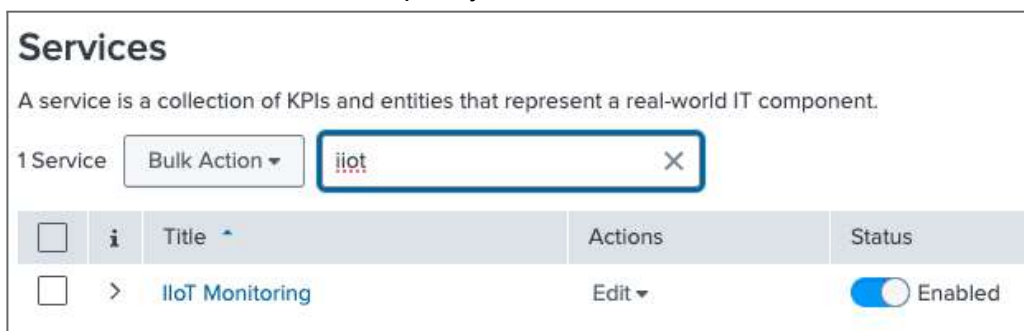
And then create via the green button



Now we have the basic service in place, we need to associate it to its parent service.

Via **Configuration > Services** in the main menu, find the **IIOT Monitoring service**.

You can use the filter to find it quickly:



The 'Services' page shows a list of services with a search filter. The filter box contains 'iiot' and is highlighted with a red rectangle. Below the filter, a table lists the services.

		Title	Actions	Status
<input type="checkbox"/>	>	IIoT Monitoring	Edit	<input checked="" type="checkbox"/> Enabled

Click on the services name (hyperlink) to edit the service, and then select the Service Dependencies tab

IIoT Monitoring

Sub-service of Splunk Widget Co.

Entities

KPIs

Service Dependencies

Settings

Predictive Analytics

Remove selected dependencies

<input type="checkbox"/>	Title	Service
<input type="checkbox"/>	ServiceHealthScore	Sensors
<input type="checkbox"/>	ServiceHealthScore	Turbines
<input type="checkbox"/>	ServiceHealthScore	Drones

Click the



button.

Filter and find the **AR Headsets** dependency, select the **ServiceHealthScore** and click

Add dependencies

ar h

1 Service

✓ AR Headset

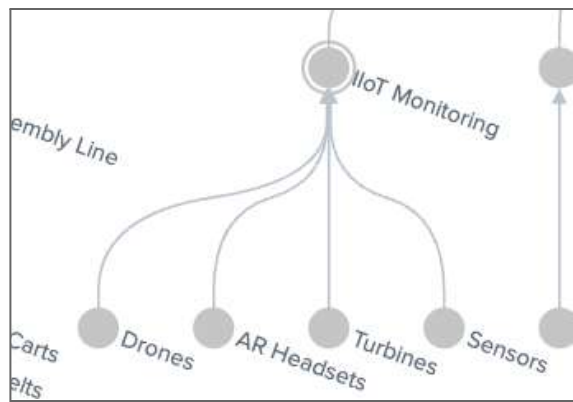
<input type="checkbox"/>	KPI Title	Service Title
<input checked="" type="checkbox"/>	ServiceHealthScore	AR Headset



when ready. And also ensure that you click



Return to the **Service Analyzer** (Default Analyzer) view to confirm your changes have taken place.



## Add some KPIs

Using what you've learnt above, edit the services in the table below, to add the following KPIs to each of these services. Use the table here for reference, detailed instructions are below the table.

Service	KPIs (Title)	Example ranges	SPL search
AR Headsets	Charge (power %)	0-100	makeresults   eval high = 99   eval low = 90   eval rand = round(((random() % high)/(high)) * (high - low) + low)
Drones	Charge (power %)	0-100	makeresults   eval high = 49   eval low = 0   eval rand = round(((random() % high)/(high)) * (high - low) + low)
Painting Robots	Vibration, PaintLevels	0-50, 0-100	makeresults   eval high = 50   eval low = 40   eval rand = round(((random() % high)/(high)) * (high - low) + low)
Liquid Washers	Temperature	0-40	makeresults   eval high = 40   eval low = 0   eval rand = round(((random() % high)/(high)) * (high - low) + low)

Start by editing each service shown in column 1 (**Configuration > Services**, filter for the service needed and select it hyperlink to edit).

For each each of the KPIs in the table, use the generic KPI option when configuring, by select **Generic KPI** from the **New** menu choice in the UI, as per:

The screenshot shows the 'AR Headsets' service configuration page. The 'KPIs' tab is active. Below the tabs, there are buttons for 'KPIs', 'Clone', and 'New'. The 'New' button is highlighted, and a dropdown menu is open, showing 'Generic KPI' as the selected option. Below the dropdown, there is a text input field containing 'Generic KPI'.

To name the KPIs, use the suggested titles in column 2 above e.g.

The screenshot shows the 'Charge (power %)' KPI configuration page. The title field is filled with 'Charge (power %)'. The page is at 'Step 1 of 7: Title and Description'.

After naming each KPI, ensure you select **Next** (not **Finish**)

The screenshot shows a green button labeled 'Next'.

For each KPI, specify the search to use as per the column 4 above, and set the **Threshold Field** to "rand" (which is the output of the SPL search) e.g:

KPI Source ? Data Model Metrics Search Ad hoc Search Base Search

Search ?   
 | eval high = 99  
 | eval low = 90  
 | eval rand = round((((random() % high)/(high)) \* (high - low) + low))

Run Search [↗](#)

Threshold Field ?

After adding the search and threshold field, click the **Finish** button (not **Next**)

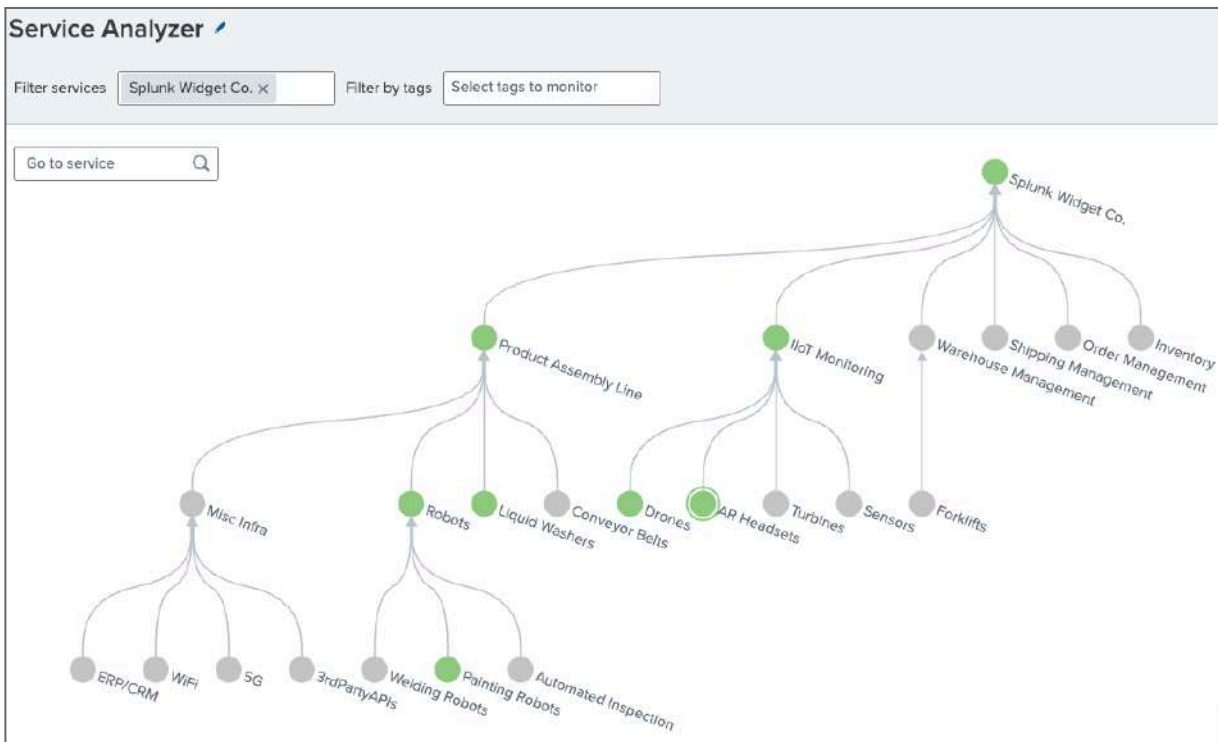
Finish

Then ensure you save the updates

Save

Repeat the above steps for KPI creation for **Drones**, **Painting Robots** and **Liquid Washers**.

When you have created all 5 KPIs, check your updates are taking effect in the **Service Analyzer**:



**Q: We only made changes to 4 services, yet we are now seeing updates (green status) to 8 services. Why?**

**Q: Ignoring the services with no configuration (in greg), everything else is green (no red or amber). Why would that be?**

## Setting Thresholds

Seeing as one of our KPIs relates to how much battery charge is available, let's put some thresholds in place to warn us when recharging might need to be considered, plus a threshold for critically low charge.

Note that for the **Drones** service, we added a KPI of **Charge**, which will be a random value between 0 and 49, every 5 minutes, as can be seen by the SPL we used:

```
| makeresults | eval high = 49 | eval low = 0 | eval rand = round(((random() % high)/(high)) * (high - low) + low)
```

This would be a good example to set thresholds to alert when charge is reduced to less than 50%. Anything above 50% should be considered normal or healthy.

Navigate back to the service configuration for **Drones** and switch to the **KPIs** tab. Expand the Search and Calculate section for the **Charge** KPI, using the arrow icon, to verify the search used to evaluate the KPI.



Now expand the **Thresholding** section by selecting the arrow icon:





### Aggregate Threshold Values

Critical ▾

0

×

Medium ▾

20

×

Normal ▾

50

×

+ Add Threshold

Base Severity

Normal ▾

View data from

last 60 minutes ▾

⚙️

When you've mirrored the settings above, ensure that you save your progress

Save

As we are updating KPI values every 5 mins, it may take a while for effects to filter through to the service analyzer.

When the **Charge** KPI value updates, does the KPI for it change colour as expected?

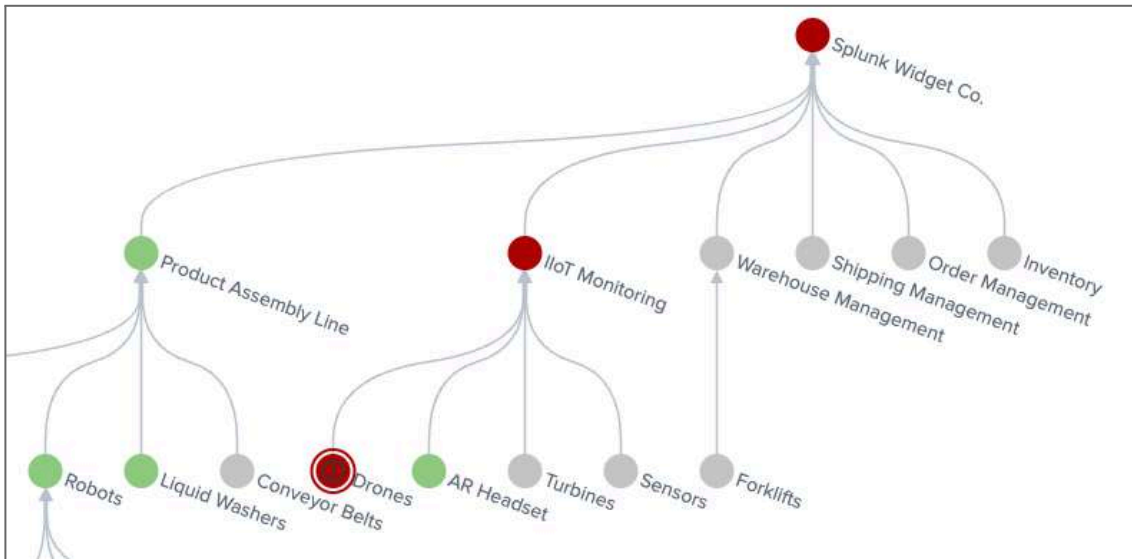
Before we made the changes, a value of 20 would show as Normal (green):



With the thresholds now in place, we see the desired results:



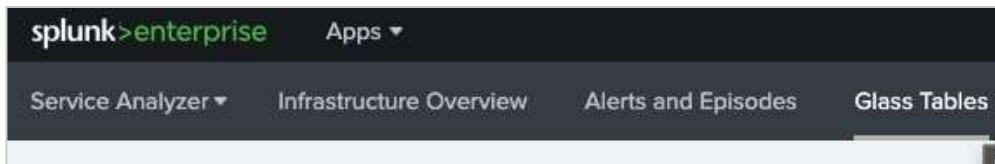
You should also notice that other services are affected by this KPI threshold breach. Why is that?



## Build custom Glass Tables: Business Services Overview

Now that we have some KPIs to work with, we can start to explore how we could make use of these in a dashboard view. For this part of the lab, we will build 2 example views. One that is high-level and that might appeal to management, in terms of generic health of operations, and then a second view that has more technical detail, to represent specific areas of technology health.

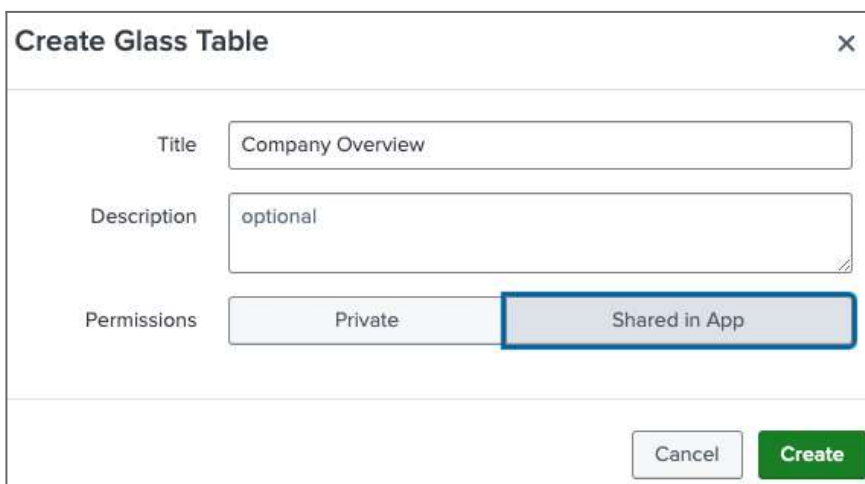
Navigate to the **Glass Table** UI via the main menu



Create a new Glass Table



We will target this GT at the business, so let's give a name that reflects the audience, such as "Company Overview" and click on the green **Create** button to finish.

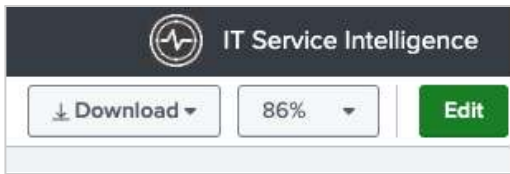
A screenshot of the 'Create Glass Table' dialog box. It has a title bar with 'Create Glass Table' and a close button. The form contains three fields: 'Title' with the value 'Company Overview', 'Description' with the value 'optional', and 'Permissions' with two radio buttons, 'Private' and 'Shared in App', where 'Shared in App' is selected. At the bottom right are 'Cancel' and 'Create' buttons.

Click on the Glass Tables title (hyperlink) to start editing it.



You will see a blank canvas for now (as we have not created anything yet).

Select the **Edit** button to continue



Note in the **Configuration** panel that there are many options we might leverage for a production-ready Glass Table, such as appropriate width/height settings, background colours and images, useful when presenting views on communal screens etc.

Download a background image from <https://splk.it/Manu-Lab-Assets>.

Choose either

- **GT-background-1.jpg** or (set Width=1400, height=930) or
- **GT-background-2.jpeg** (set Width=1400, height=790)

---

**i** Note: changes are not saved unless you select the save icon  in the Glass Table menu

---



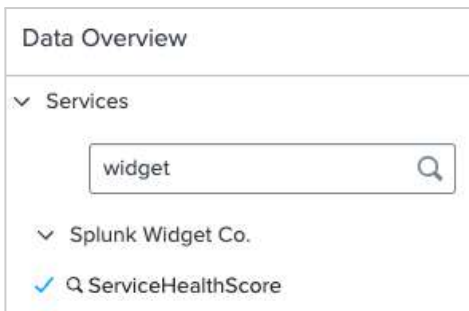
For this overview, we will add 4 health scores for:

- Splunk Widget Co.
- Product Line Assembly
- IIoT Monitoring
- Warehouse Management

Add some Service Health scores to the dashboard using the **Data Overview** icon - this provides access to both health score and KPIs



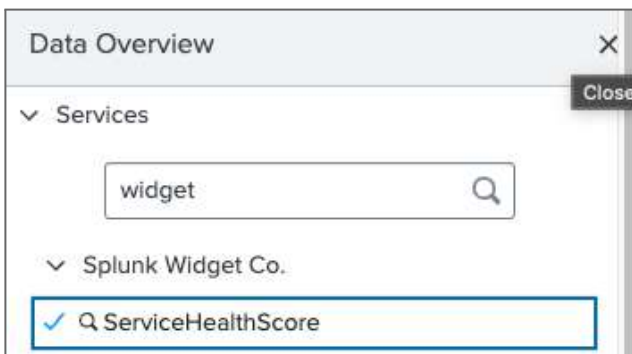
Add ServiceHealthScore for Cloud services by filtering on “widget” from the **Services** search bar in the **Data Overview** tab, and clicking on the arrow to expand the list of health scores and KPIs.



and then selecting



Close the Data Overview panel



The newly added health score will now appear on the canvas. It can be moved, resized and configured. Select it to open the Configuration tab for the health score.

In the **Visualisation Options**, give the score a name “Splunk Widget Co.” and optional description:

Configuration

Visualization Options

Visualization Type

# Single Value

Title

Splunk Widget Co.

Description

Health of all services combined

Move to the **Positions & Size** section, and use the values shown below:

Position & Size

X Position

500

Y Position

20

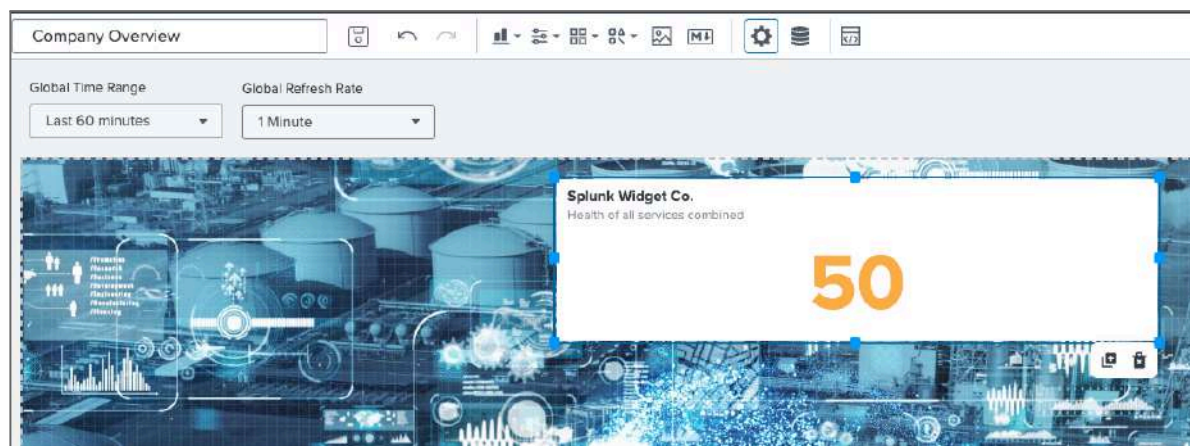
Width

560

Height

150

Your dashboard should look similar to:



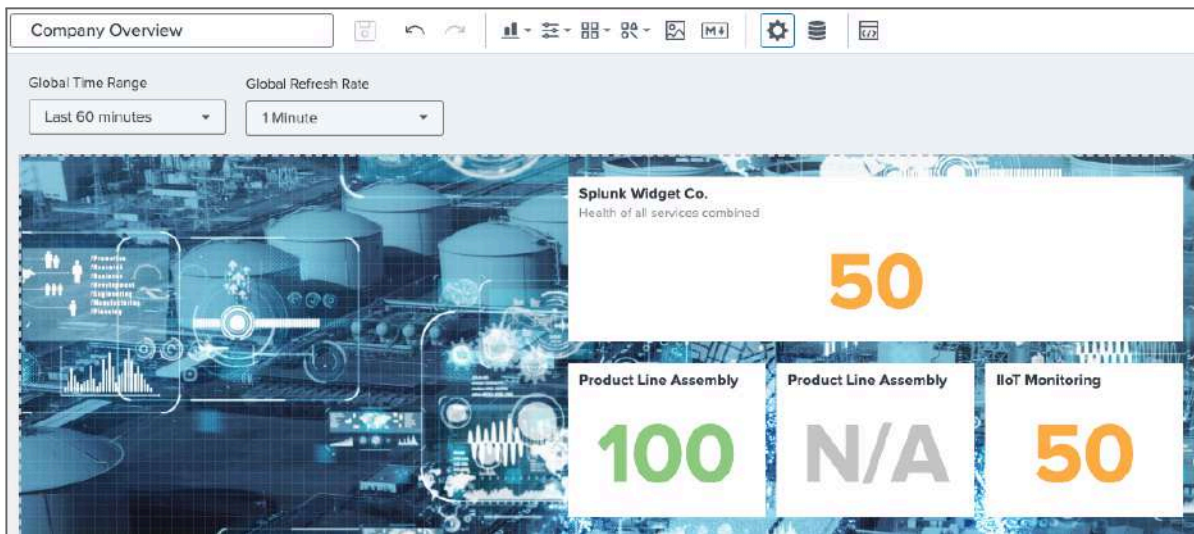



Follow the same steps as above to also add the ServiceHealthScores from

- Warehouse
- IIoT Monitoring
- Product Line Assembly

But give them a width of 180 pixels and height of 140.

So that you end up with the following:

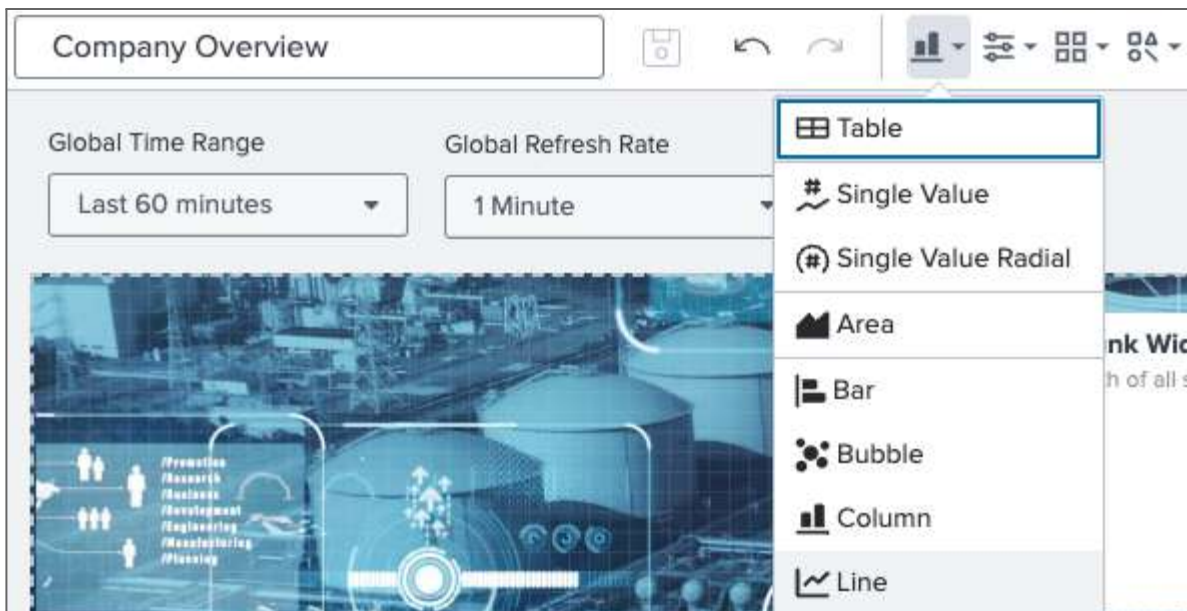


**Save** your work  and then **View** your work

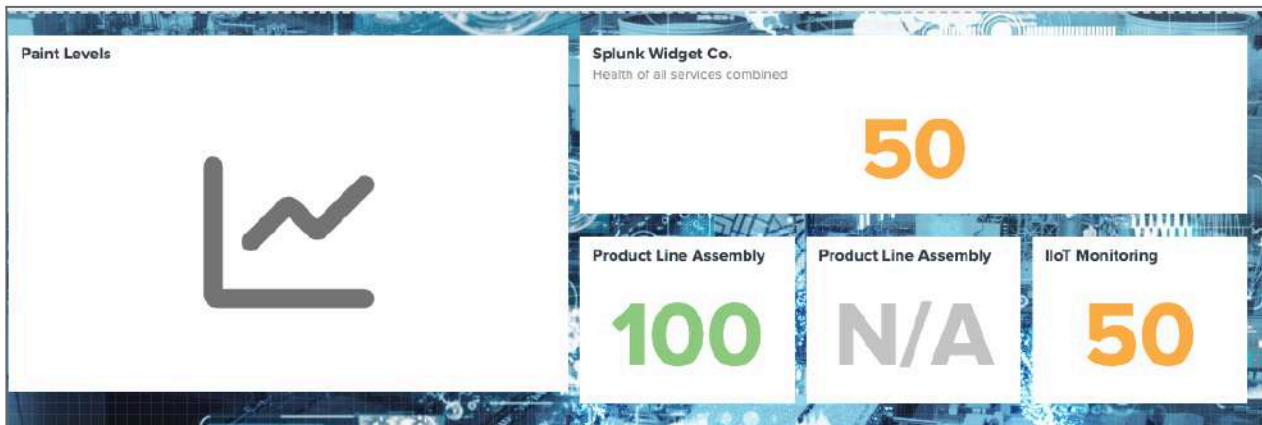


Management are happy with this view but one manager in particular would like to see the KPI for **Robot Paint Levels** displayed on here, as it is of particular importance to them. They've asked to see the performance of 5G over time, so we will add a line chart to our current view.

Select this option from the list of visualisation options



By selecting **Line**, a new image will appear which will need configuring. Move it and size it to your preference:



We now need to connect this view to a data source i.e. the KPI value for **Paint Levels**.

Perform this in the Data Configurations section for the component:



Select Data

Services

paint

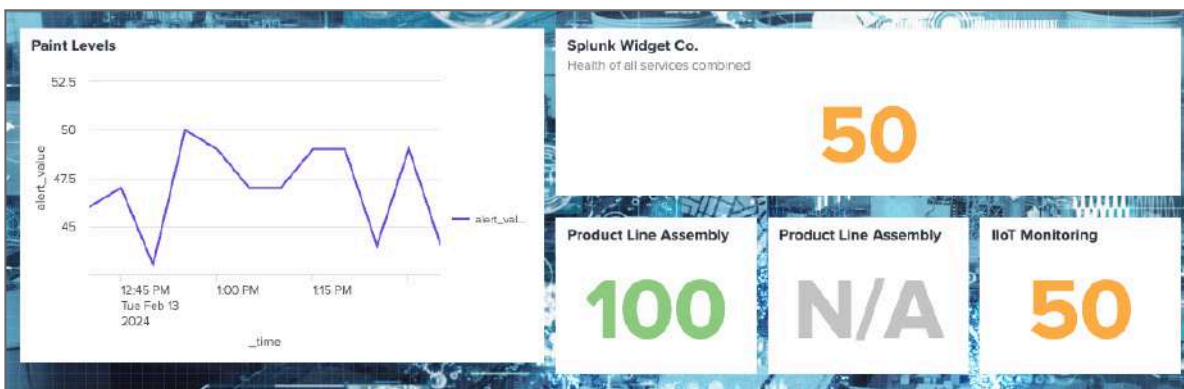
Painting Robots

ServiceHealthScore

Paint Levels

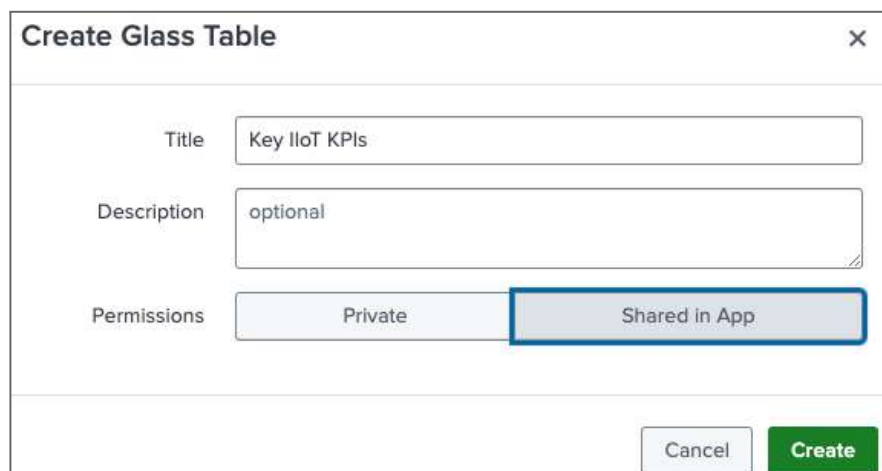
Vibration

Confirm that paint levels are now displayed also:



## Build custom Glass Tables: Infrastructure Overview

Via the **Glass Table** option in the main menu, create a new Glass Table called “Key IIOT KPIs”



The 'Create Glass Table' dialog box contains the following fields and options:

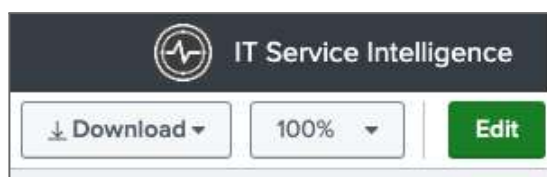
- Title:** A text input field containing 'Key IIoT KPIs'.
- Description:** A text input field containing 'optional'.
- Permissions:** Two radio button options: 'Private' and 'Shared in App'. The 'Shared in App' option is selected and highlighted with a blue border.
- Buttons:** 'Cancel' and 'Create' buttons at the bottom right.

Edit using the hyperlink option



A button with a square icon, a right-pointing chevron, and the text 'Key IIoT KPIs'.

And select Edit in the Glass Table view



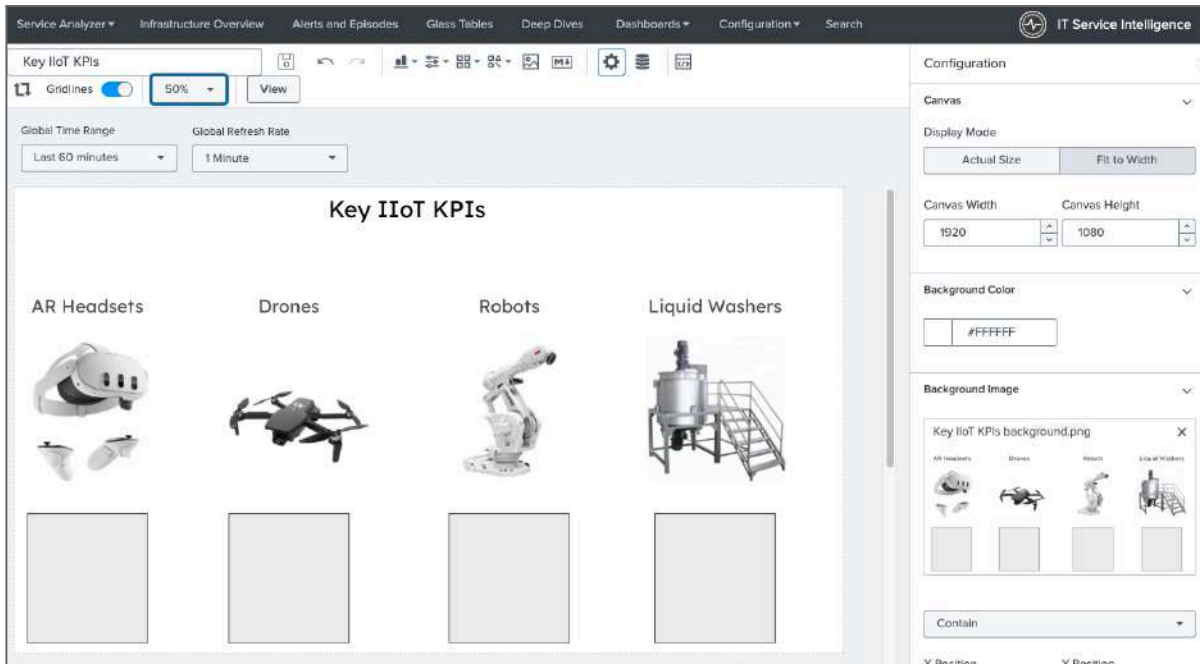
The header of the Glass Table view includes:

- IT Service Intelligence** logo and title.
- Download** button with a dropdown arrow.
- 100%** zoom level with a dropdown arrow.
- Edit** button.

For this Glass Table, we are going to add some custom images, which you can download from here: <https://splk.it/Manu-Lab-Assets>.

Download “Key IIoT KPIs background.png”

Add this as a background image to your Glass Table and set **Display Mode** to **Fit to Width**.



Add the KPIs for the following, into the grey box placeholders:

- Drones - Charge (power %)
- AR Headsets - Charge (power %)
- Painting Robots - Paint Levels
- Liquid Washers - Temperature

Use the **Data Overview** icon to make the additions



Use the search & filter view to find the 4 required KPIs e.g.

Data Overview

Services

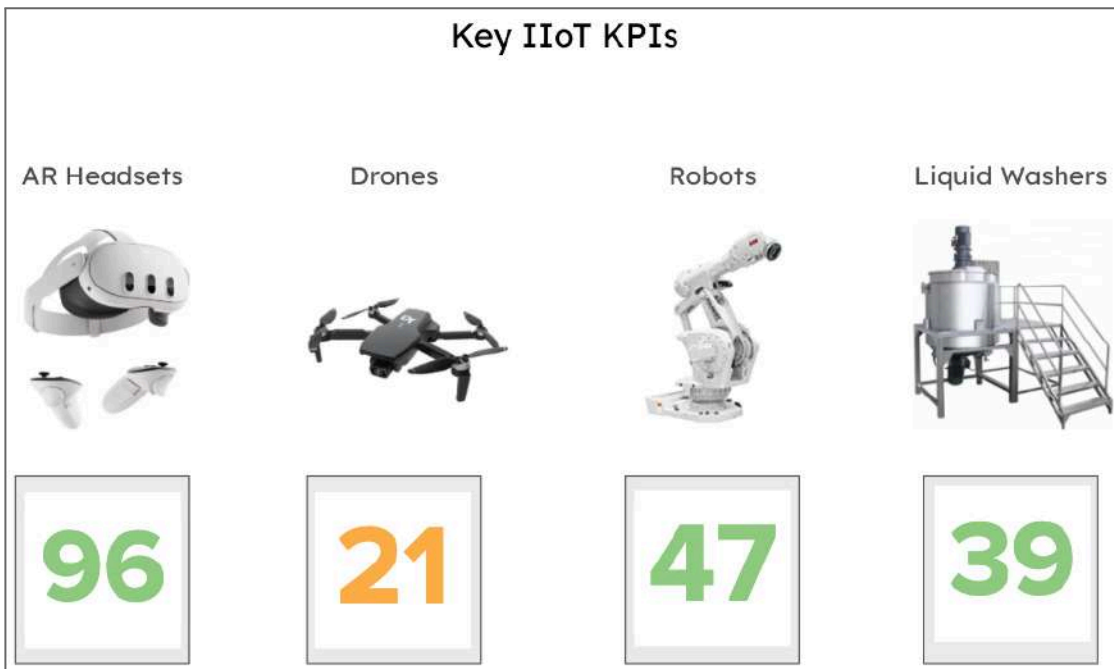
drones

Drones

ServiceHealthScore

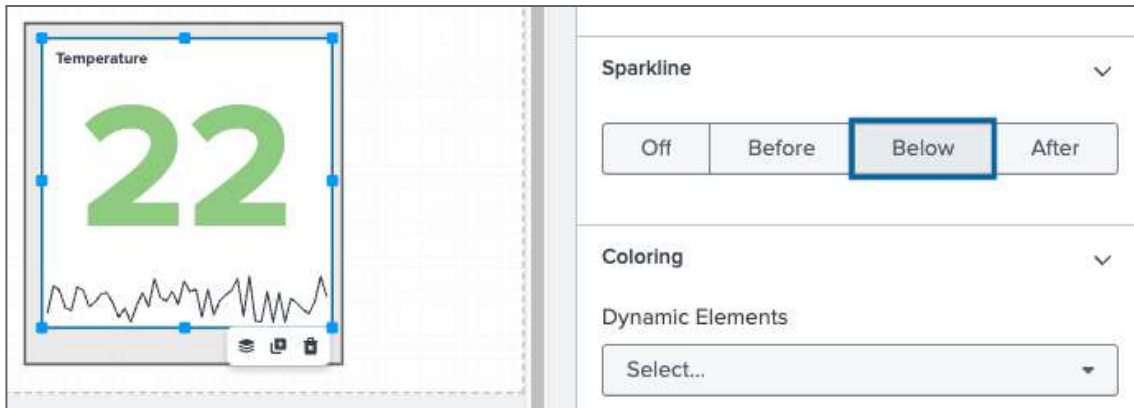
☒ Charge (power %)

You should end up with something like this:

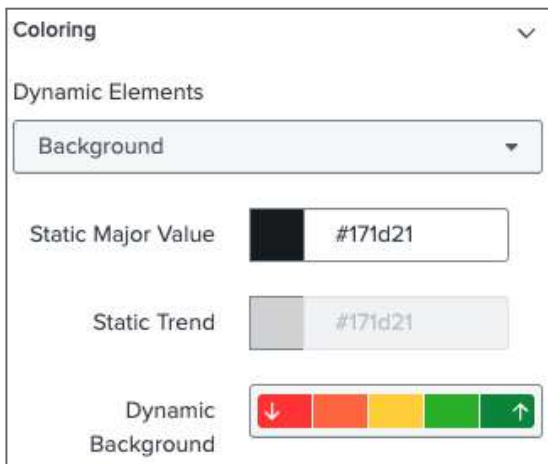


OPTIONAL: Add the KPI names to each value.

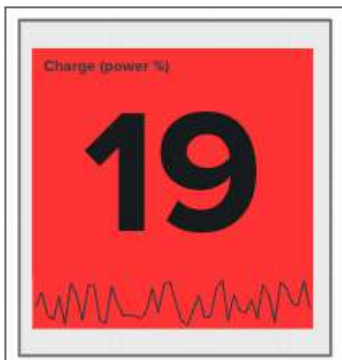
For each KPI, add a sparkline visual to show trend values over time, using the *Sparkline* settings panel in the **Configuration** panel.



Make one of the KPIs more prominent by editing the colour settings in the **Coloring** panel of **Configuration**.



To produce:



**Save** your work.

## Connecting Glass Tables

Return to the first Glass Table created; “Company Overview”.

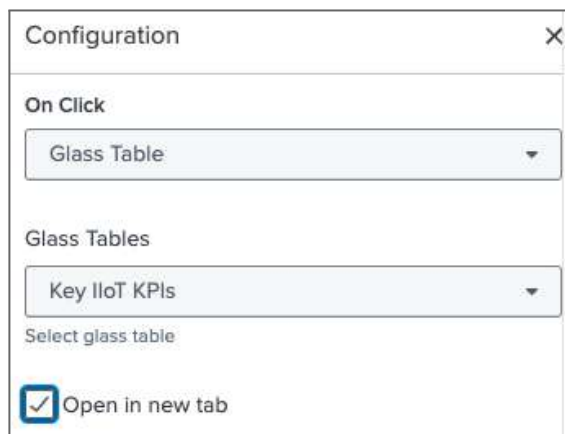
Ensure you are in edit mode and then select the **Paint Levels** KPIs component.

Locate the **Drilldown Settings** section and select **+ Add Interaction**



From the menu, select **Glass Table**, as we are going to link it to our KPI Glass Table, but note the various different options available.

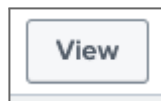
Use the options as shown below:



And ensure you select the **Apply** button



Now test the link capability by viewing the **Company Overview** glass table



Click on the line chart to drilldown





Finally, see if you can connect a KPI to a **Service Analyzer**. You may need to create a new **Service Analyzer** view first, in order for it to be available as a drilldown option.

Hint 1:

The 'Create Service Analyzer' dialog box is shown. It has a title bar with a close button (X). The form contains three fields: 'Title' with the value 'Splunk Widget Co.', 'Description' with the value 'optional', and 'Permissions' with two radio buttons: 'Private' and 'Shared in App'. The 'Shared in App' radio button is selected. At the bottom right, there are 'Cancel' and 'Create' buttons.

Field	Value
Title	Splunk Widget Co.
Description	optional
Permissions	Shared in App

Hint 2:

Configuration

×

On Click

Service Analyzer

Service Analyzers

Splunk Widget Co.

Select saved service analyzer

☒ Open in new tab

## Exercise 9 - Build Your Own Service

### Description

Now that you have learned some of the key features within ITSI, try and build a service view that aligns to your role, team or department.

Start by picking a key service - something that Line of Business cares about, and has a relatively complex IT stack supporting it.

Focus on something that provides maximum business value. Then identify 4 or 5 key technology components that underpin that service.

Finally, for each technical component, how would you determine if it was performing well or not? I.e. what are they KPIs you'd be interested in?

See how far you can get in building that out in the remaining lab time - and ask for help!

Good luck.

## Answers: Exercise 5

**Q1: Using the “interesting fields” list in the UI, can you determine how many wind turbines there are?**

A: 4

**Q2: On what date did a turbine report being offline? Which turbine?**

A: Dec 28th. WT01

**Q3: Which wind turbine produced the greatest speed? What was the speed and when did it happen?**

A: WT02. 35.4mph. Dec 2nd

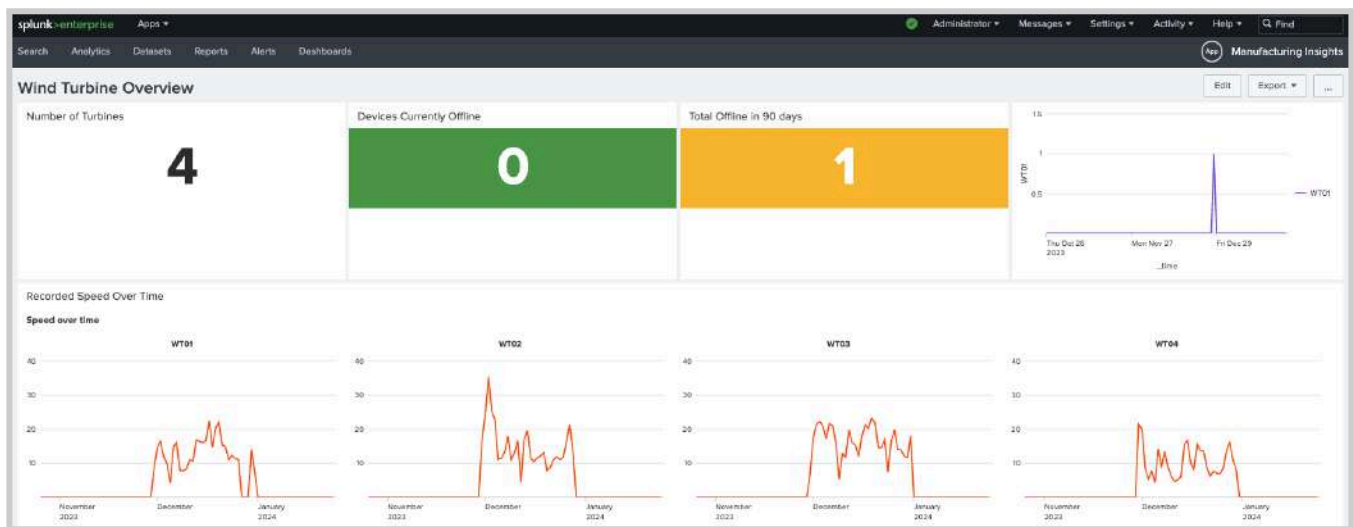
**Q4: What was significant about the speed of WT01 on Dec 27th/28th? How does it relate to the view of offline devices over time?**

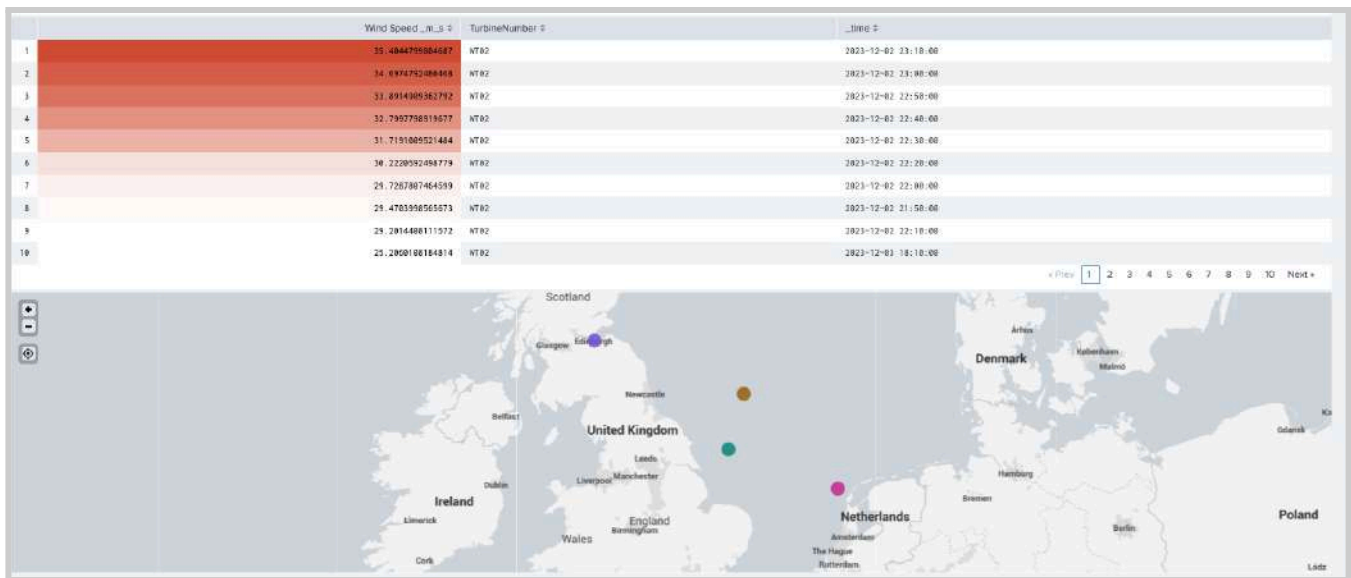
A: It reported a speed of zero. The same time as “offline” device was reported.

**Q5: What Countries are the turbines located in or near?**

A: Scotland (Edinburgh), English Coast/North Sea, Netherlands

## Final Dashboard





## Answers: Exercise 7

### Glass Tables

**Q1: Service Health - which of the 4 services has the lowest/worst health score?**

A: Confirmation / 24

**Q2: KPIs - how many Fraud alerts have occurred in the last hour?**

A:45

**Q3: What's the main reason that Confirmation has a low score?**

A: 101 Failures

**Q4: What technical components are involved in this degradation?**

A: Arcot 3DS + CCM

### Service Analyzer

**Q5: There are actually a number of services impacting Card Payments - name 2 of them. HINT: focus on the root cause.**

A: Fraud, Social Sentiment and Customer Communication Management.

**Q6: How many are there and what are their severities?**

A:4. Severities will change over time - it's a live view

## Deep Dive

**Q7: Which KPIs look particularly problematic?**

A: Response Rate (but there may be others)

**Q8: How many events have there been in the last 2 hours?**

A: Depends on demo data and time range selected

**Q9: How many are there now?**

A: less than there were in the previous view!

## Service Creation

**Q10: Are your new KPIs appearing and do they have values?**

A: Yes, you should have some values (after 5 mins at most)

**Q11: What else do you notice about the service tree?**

A: The new services are not connected to any other service