Splunk4Rookies - Business Insights

Workshop

#Splunk4BI

splunk>

Forward-Looking Statements

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

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

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

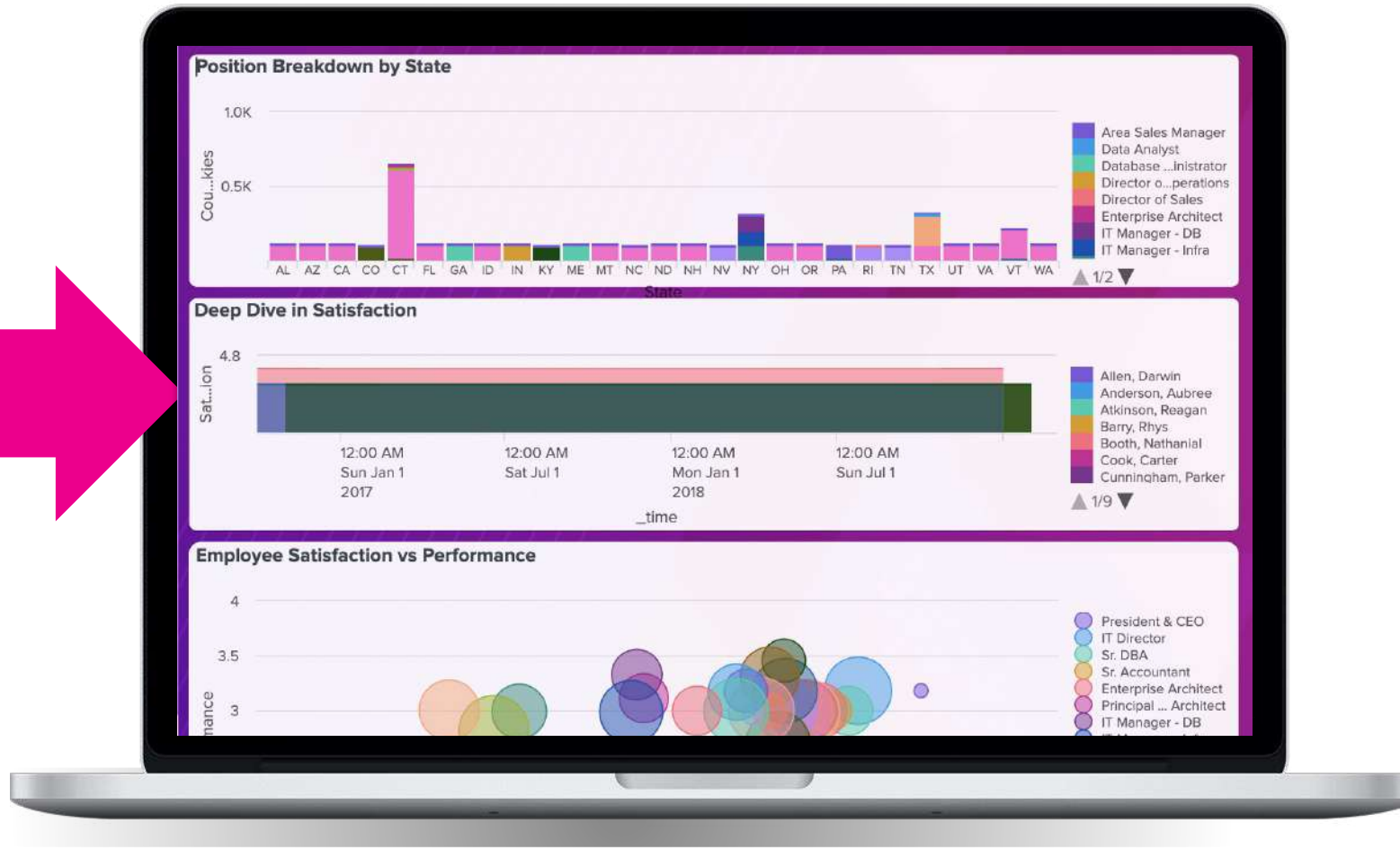
Please introduce yourself!

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

Workshop Agenda

- ✓ The value of data
- ✓ Splunk’s approach to data
- ✓ Explore table datasets
- ✓ Creating a table
- ✓ Modify existing table
- ✓ Extend Table with lookups
- ✓ Explore Pivot
- ✓ Creating a dashboard for multiple use cases
- ✓ Splunk resources

Objective for Today



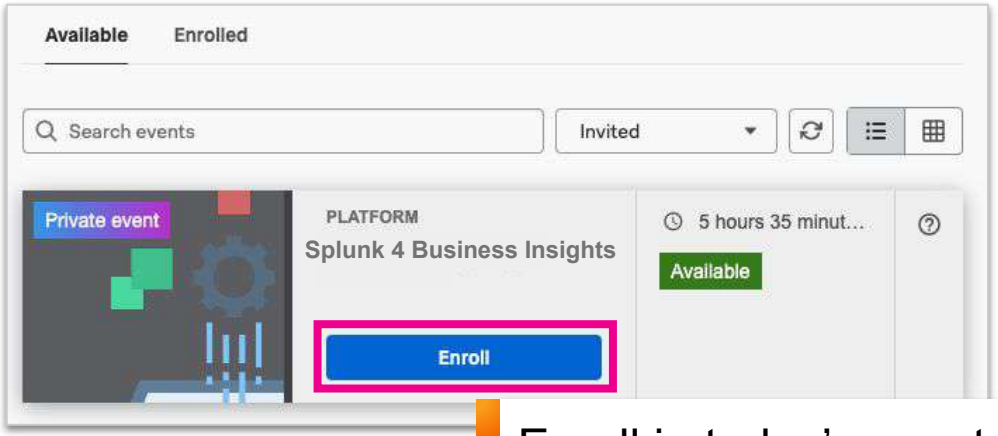
splunk>

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download a copy of today's slide deck: https://splk.it/S4RBI-Attendee

Goal



Enroll in today's event



Digital Runs the Business

Your systems need to be secure and reliable



Today, It's Hard to be Resilient

Complex Environments

Siloed tools and teams

Evolving compliance and regulations

splunk>

Service Disruptions Often Look the Same

But different internal teams struggle to see a holistic view to solve the problem

Audit

Security

IT

Operations

Legal

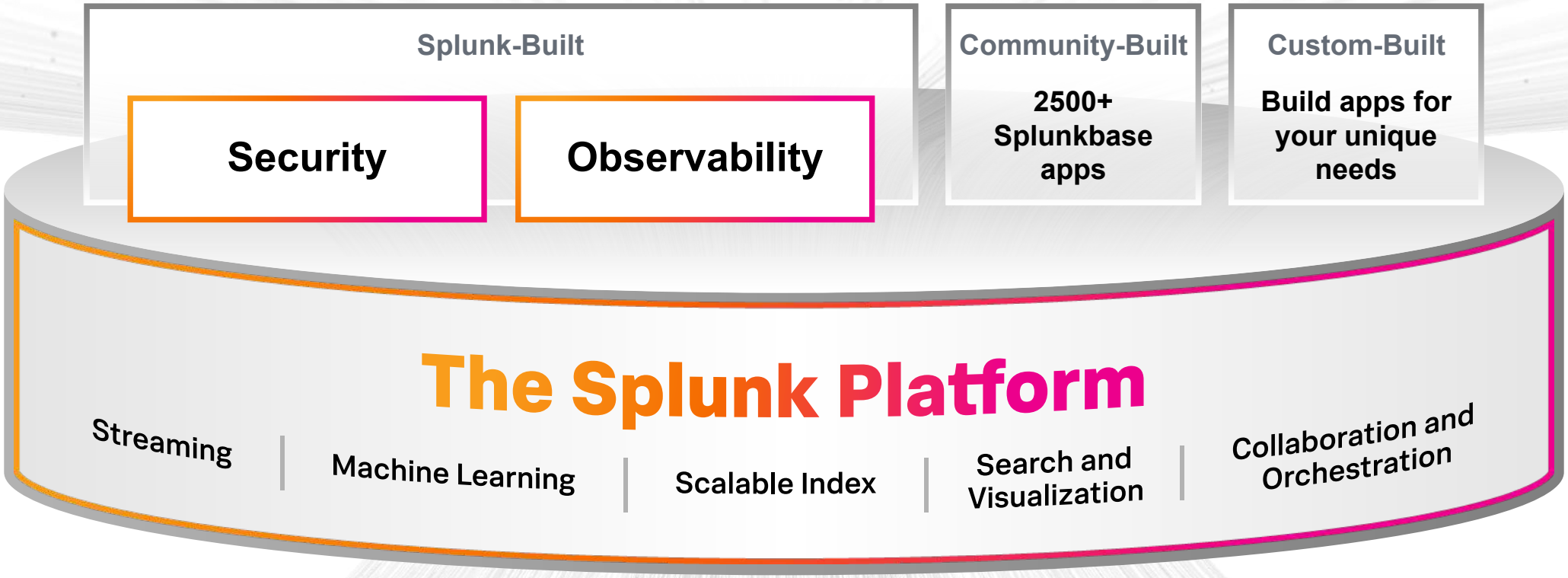
Finance

HR

Assurance

splunk>

Introducing Splunk



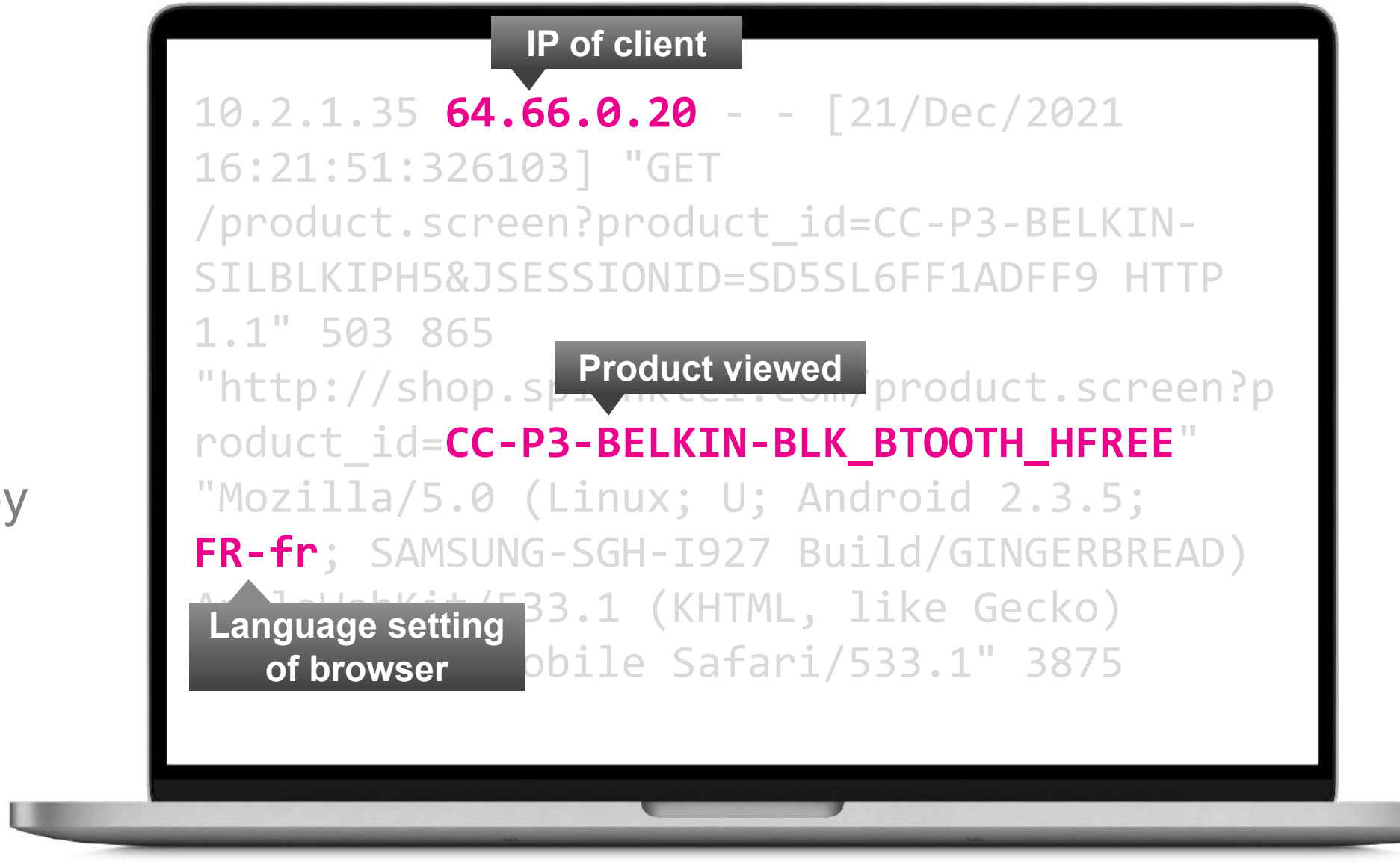
0010 01010 0101 **Events** | **Logs** | **Metrics** | **Traces**

Public Clouds · **Third-Party Tools** · **On-Prem Data Centers** · **Apps / Services** · **Edge**

Machine data is valuable not complex!

Marketing Use Case

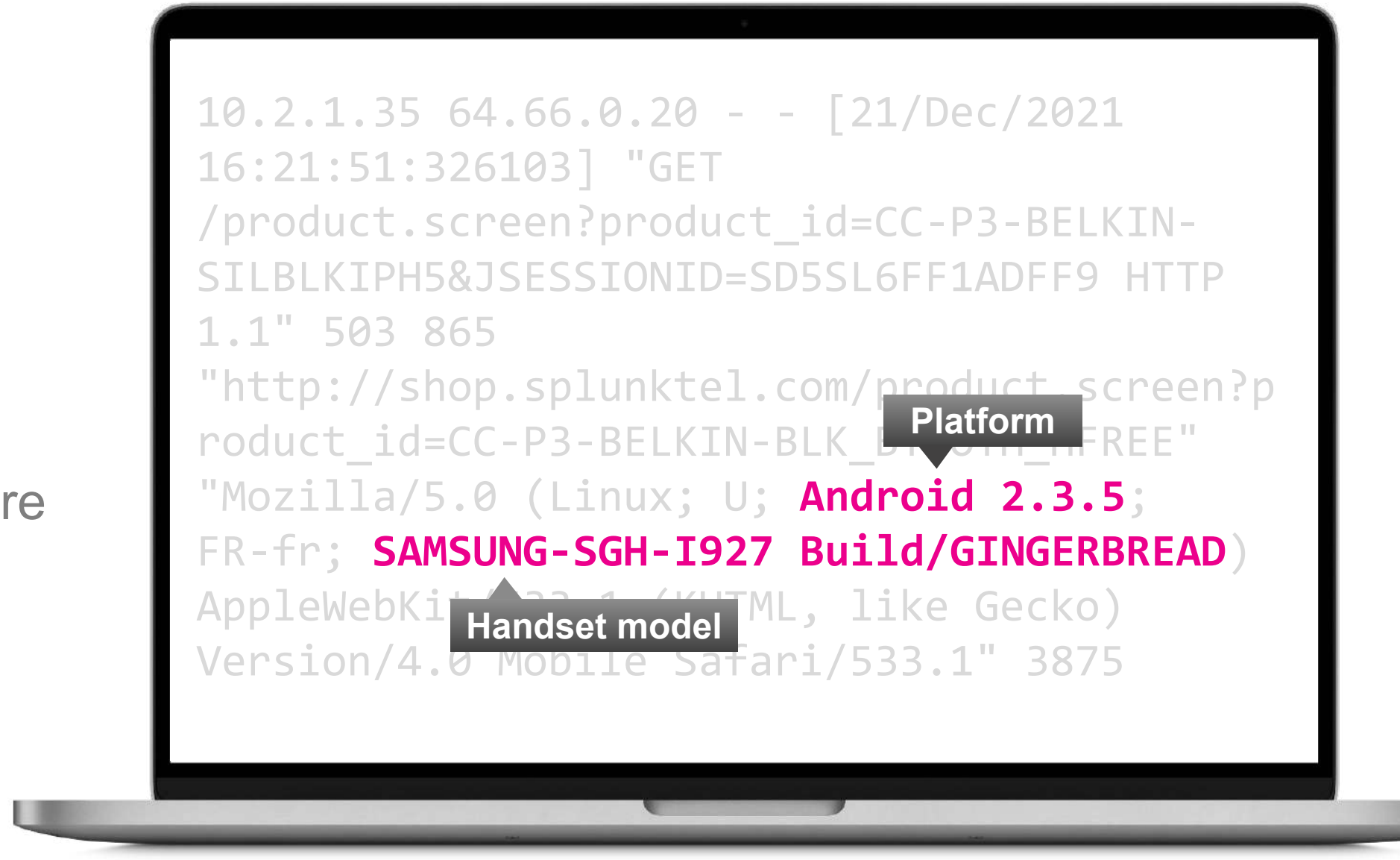
Show the top products viewed by language



splunk>

DevOps Use Case

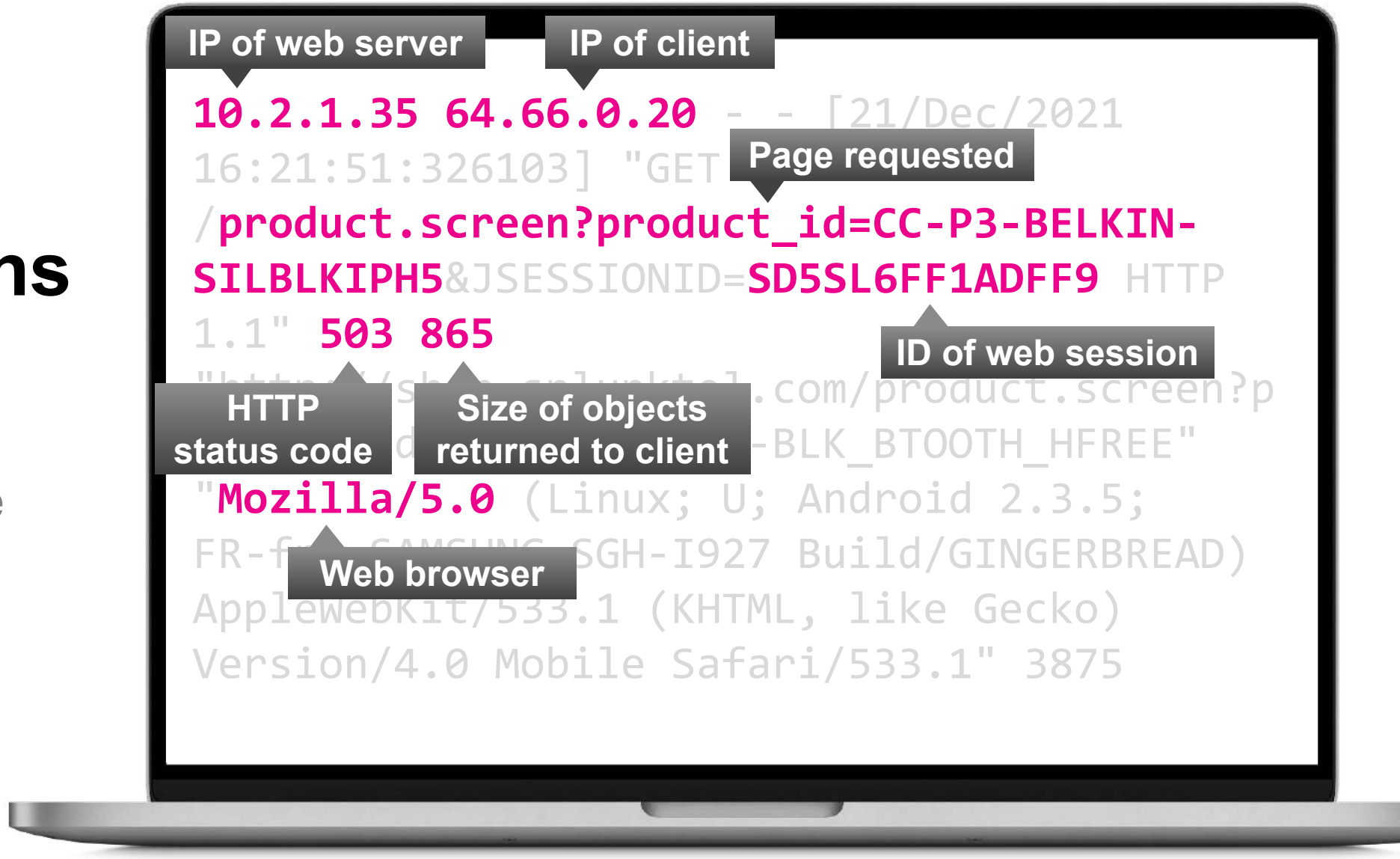
Which mobile handsets should I test the most before releasing my new app?



splunk>

IT Operations Use Case

Which web pages are generating the most errors?



splunk>

But what about all the other business functions?

Apps and Add-ons

- 2800+ free apps and add-ons available from https://splunkbase.splunk.com/
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs

Apps

Content designed to bring fast time-to-value from your data in Splunk, including pre-built dashboards, reports, alerts, visualisations and workflows

Add-ons

Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

splunk>

Today's Scenario | Buttercup Enterprises

Your Company

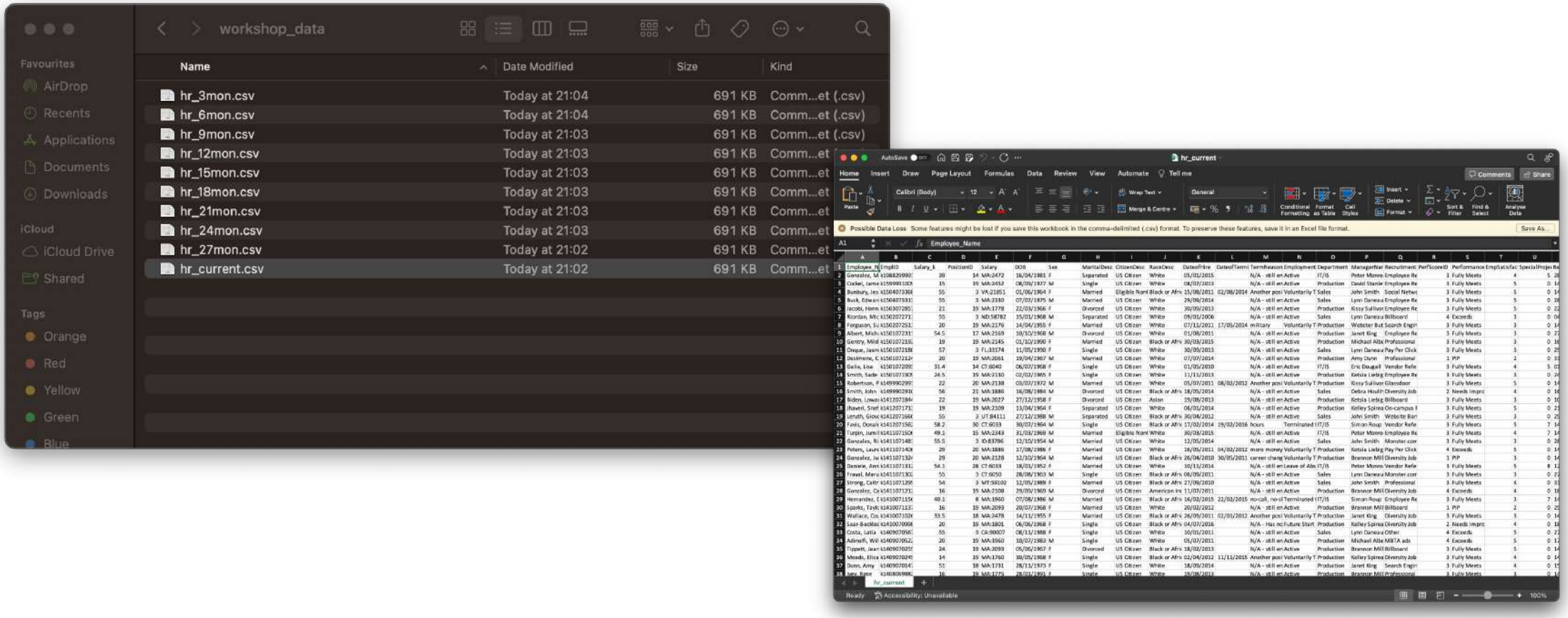
- Buttercup Enterprises is a large national online retailer operating in the US, which sells a variety of books, clothing and other gifts through its online webstore
- Buttercup Enterprises have recently invested in Splunk and now they want to start making use of it across the business

Your Role

- To provide insights to various users throughout the company
- You will be analysing:
  - **Personal Information**
  - **Employee Satisfaction**
  - **Financial Data**

Today's Data

A series of HR spreadsheets on Buttercup personnel over 2 years

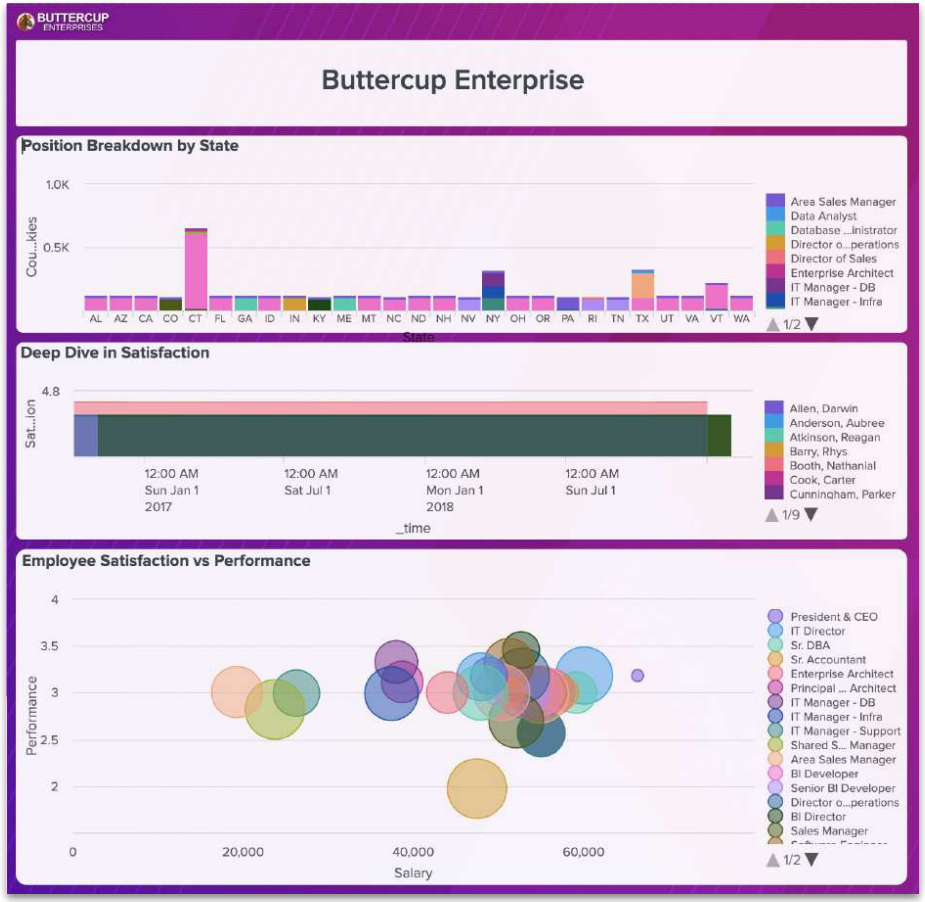


splunk>

What Does the Business Want to See?

We need to create a single dashboard with multiple insights across HR, Finance and Wellbeing:

- Understand how many employees there are per state, broken down by position/role
- Understand current employee satisfaction levels and how it impacts their performance and salary/position
- Investigate further, any groups Identified as at risk in terms of satisfaction and performance over time



splunk>

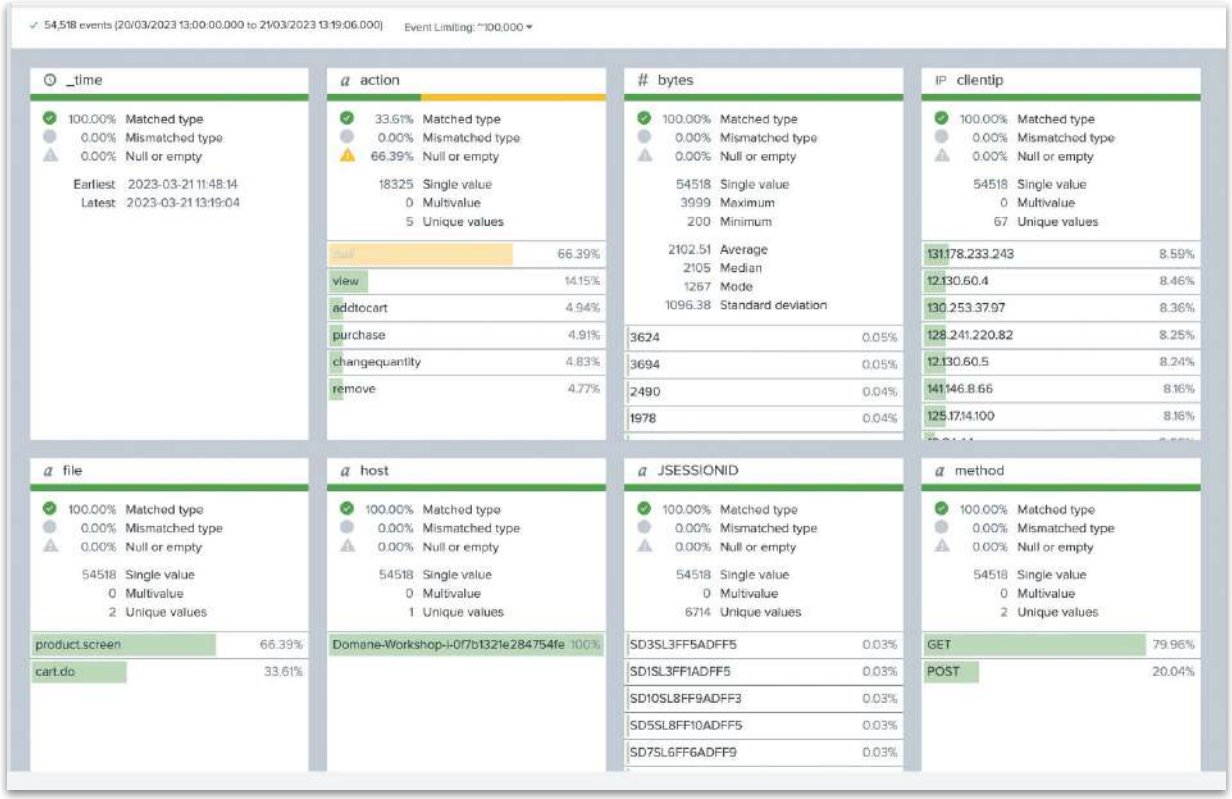
Module 1

Data preparation with Tables

splunk>

What are Datasets and Tables?

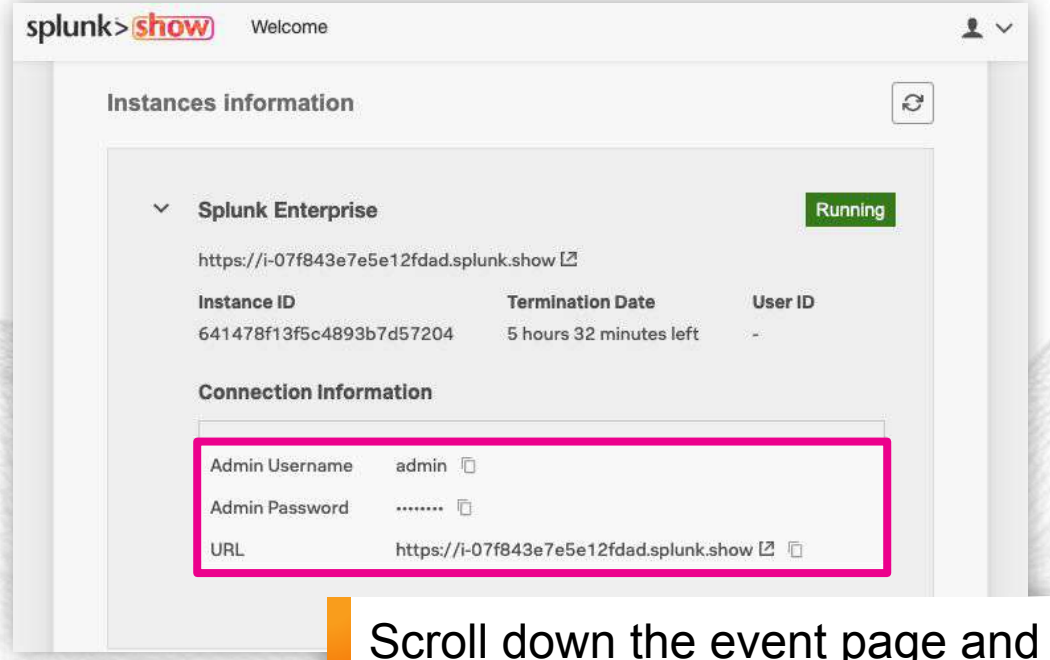
- A dataset is a structured collection of data from any source in any format presented in Splunk
- A type of **dataset** that you can create, shape, and curate for a specific purpose.
- They can be modified over time and shared with others so they can refine it further
- A powerful tool of many uses:
  - ✓ View dataset content
  - ✓ Works directly with Pivot
  - ✓ Can be extended with lookups and reports
  - ✓ Easily share datasets
  - ✓ Can be accelerated
  - ✓ And more!



splunk>

Login to Splunk

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



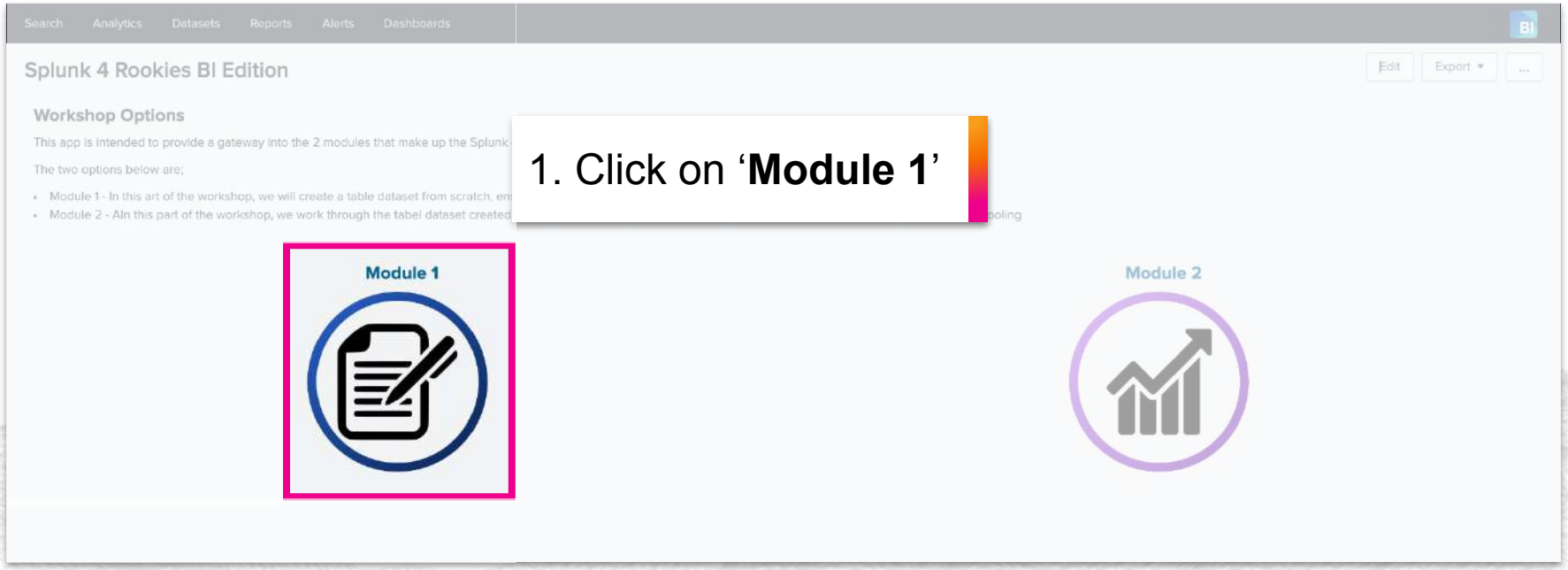
Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

Log in to your Splunk instance

Login using the credentials from Splunk Show

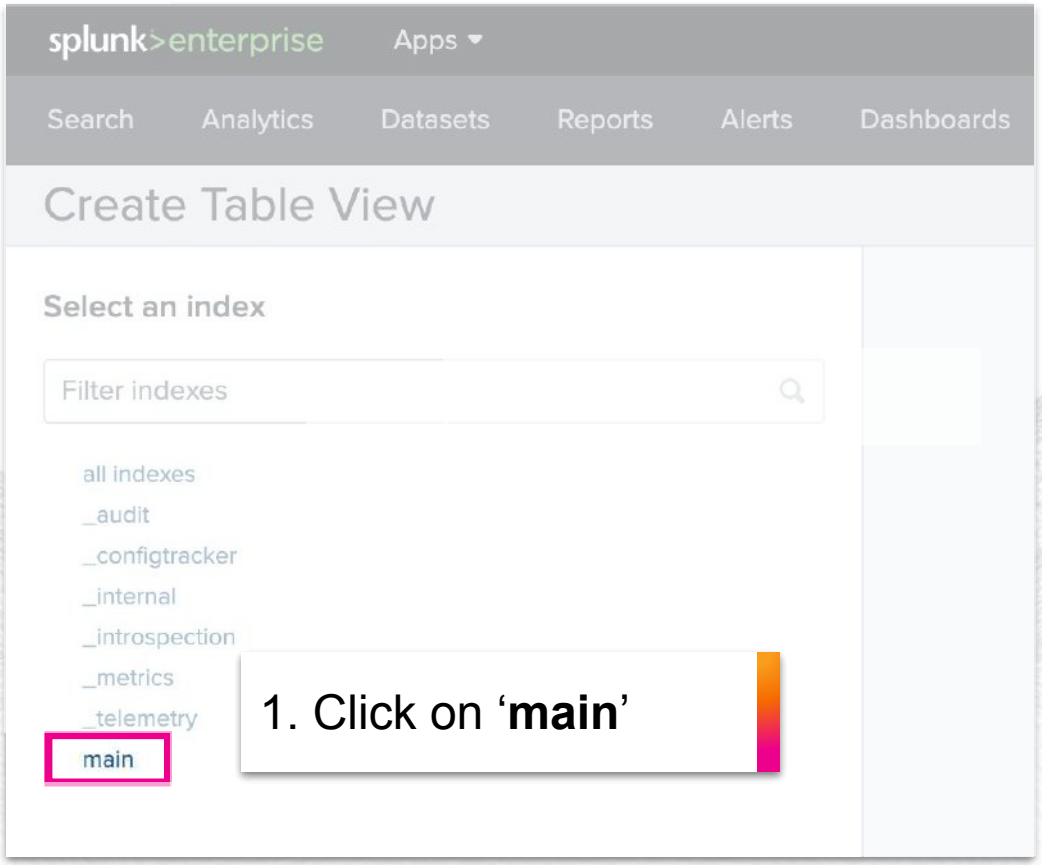
splunk>

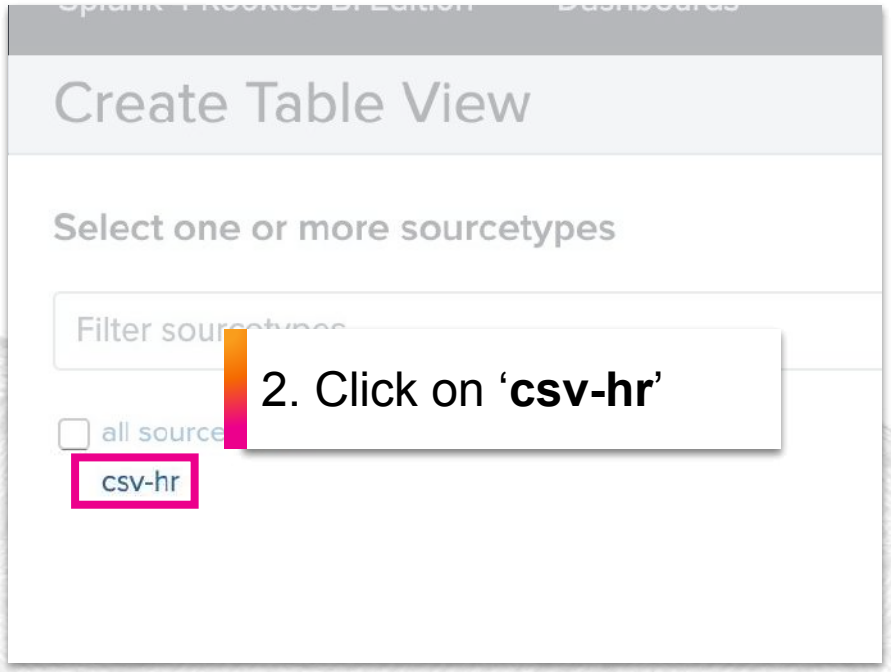
Navigate to your Module



splunk>

Selecting the data for your analysis





Select the required fields

Tasks:

1. Select the fields to be used in our analysis

- Department
- EmpID
- Employee_Name
- EmpSatisfaction
- PerformanceScore
- PerfScoreID
- PositionID
- ReviewDate
- Salary
- Salary_k

1. Select the above fields to include in our dataset

2. Click on '**Start Editing**

splunk>

Let's explore the Interface

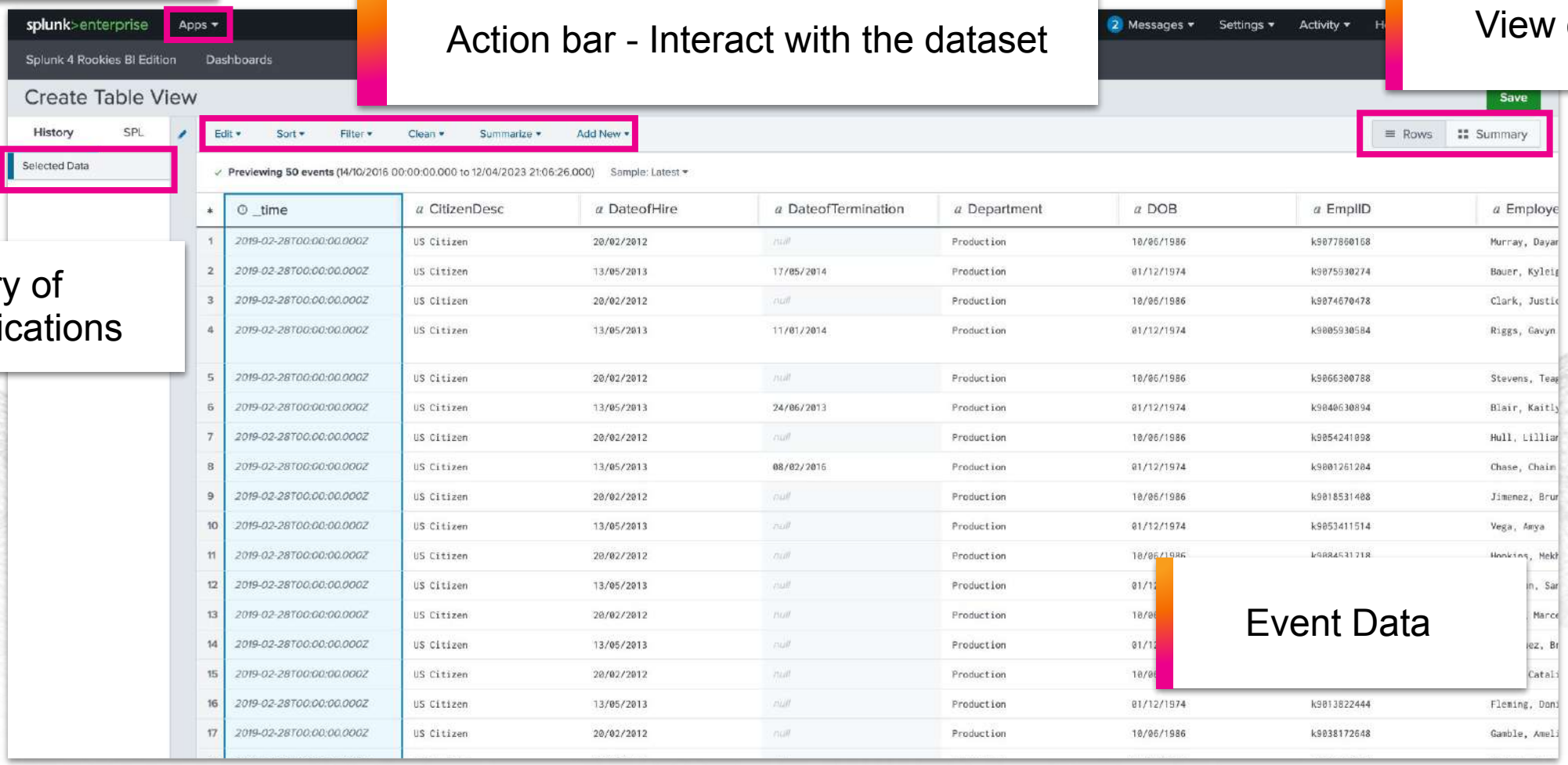
The currently selected app

Action bar - Interact with the dataset

View options

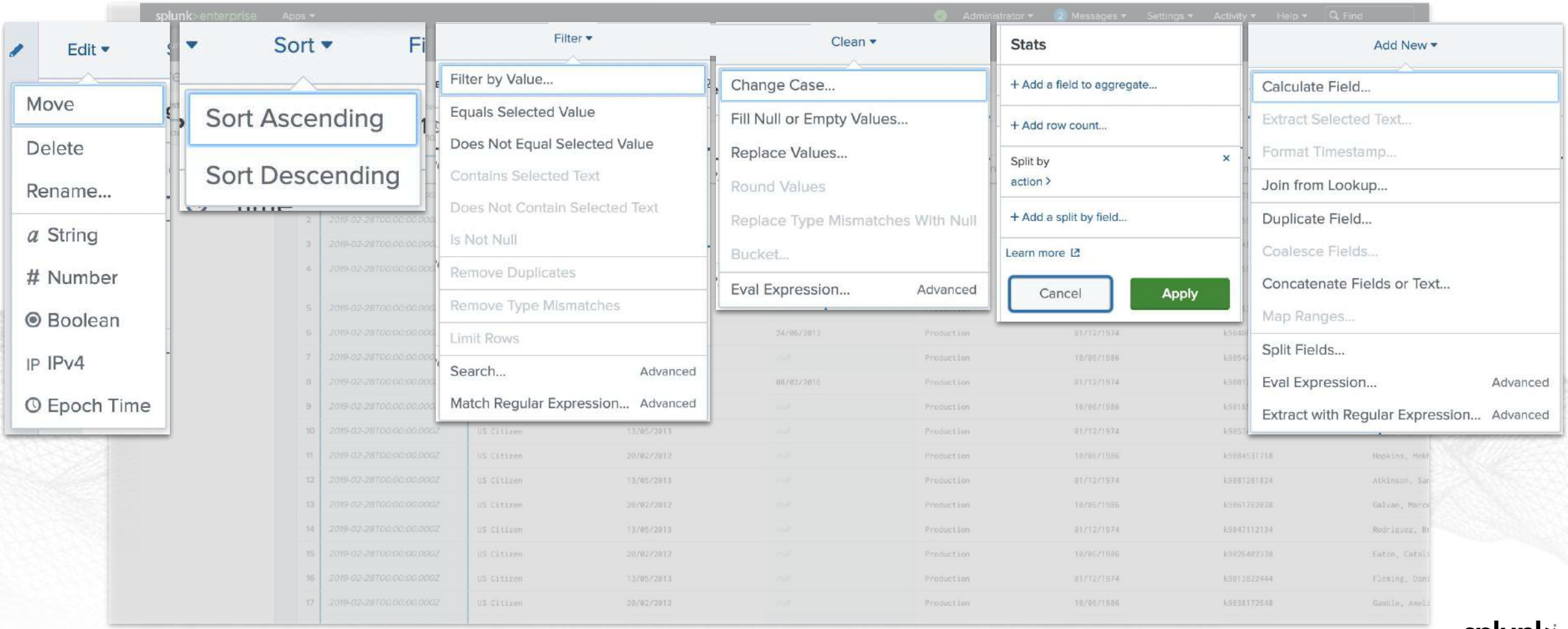
History of modifications

Event Data



splunk>

Let’s explore the Interface

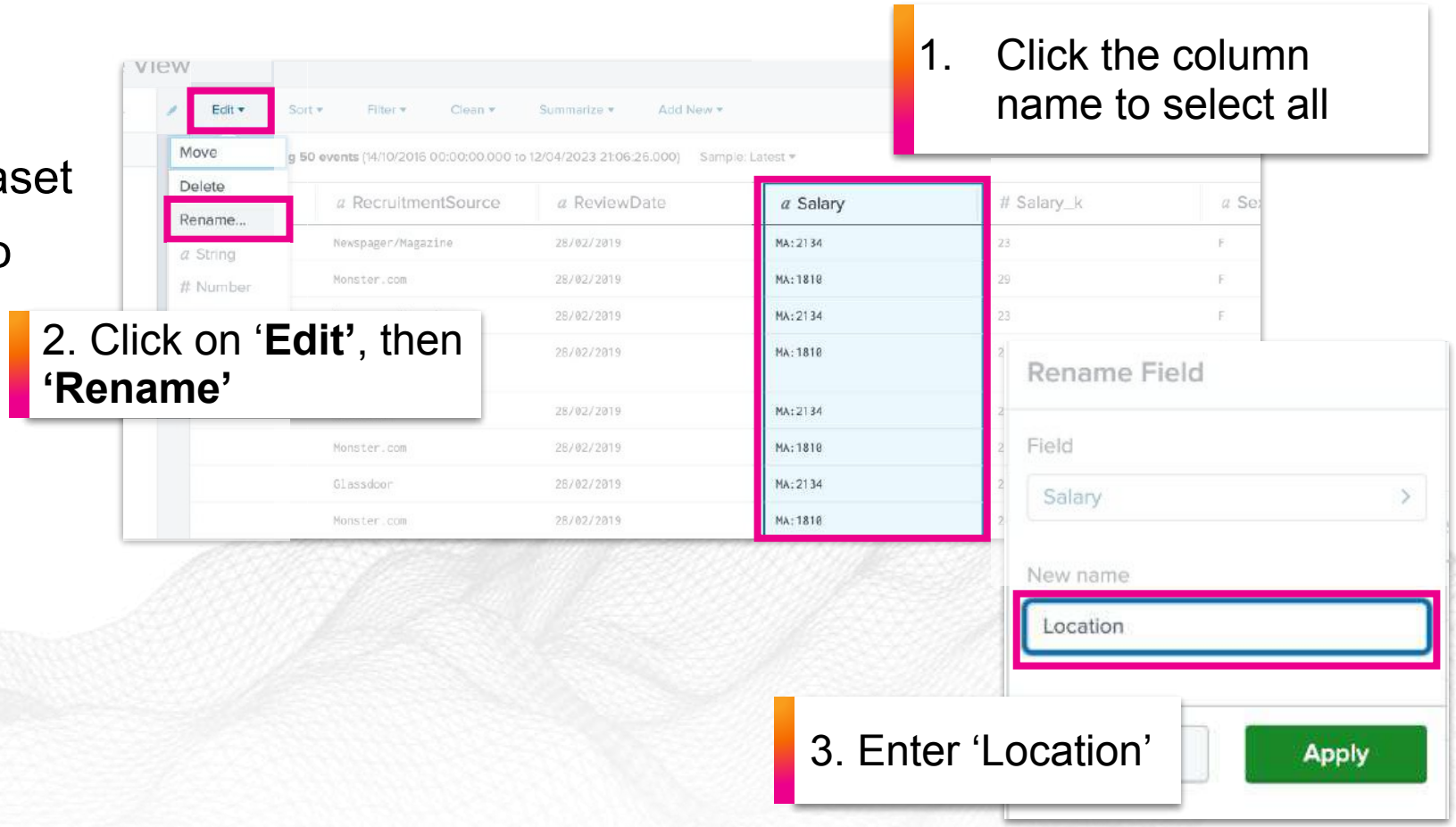


splunk>

Modify the data on the fly

Tasks:

1. Correct the error in our dataset without having to go back to source

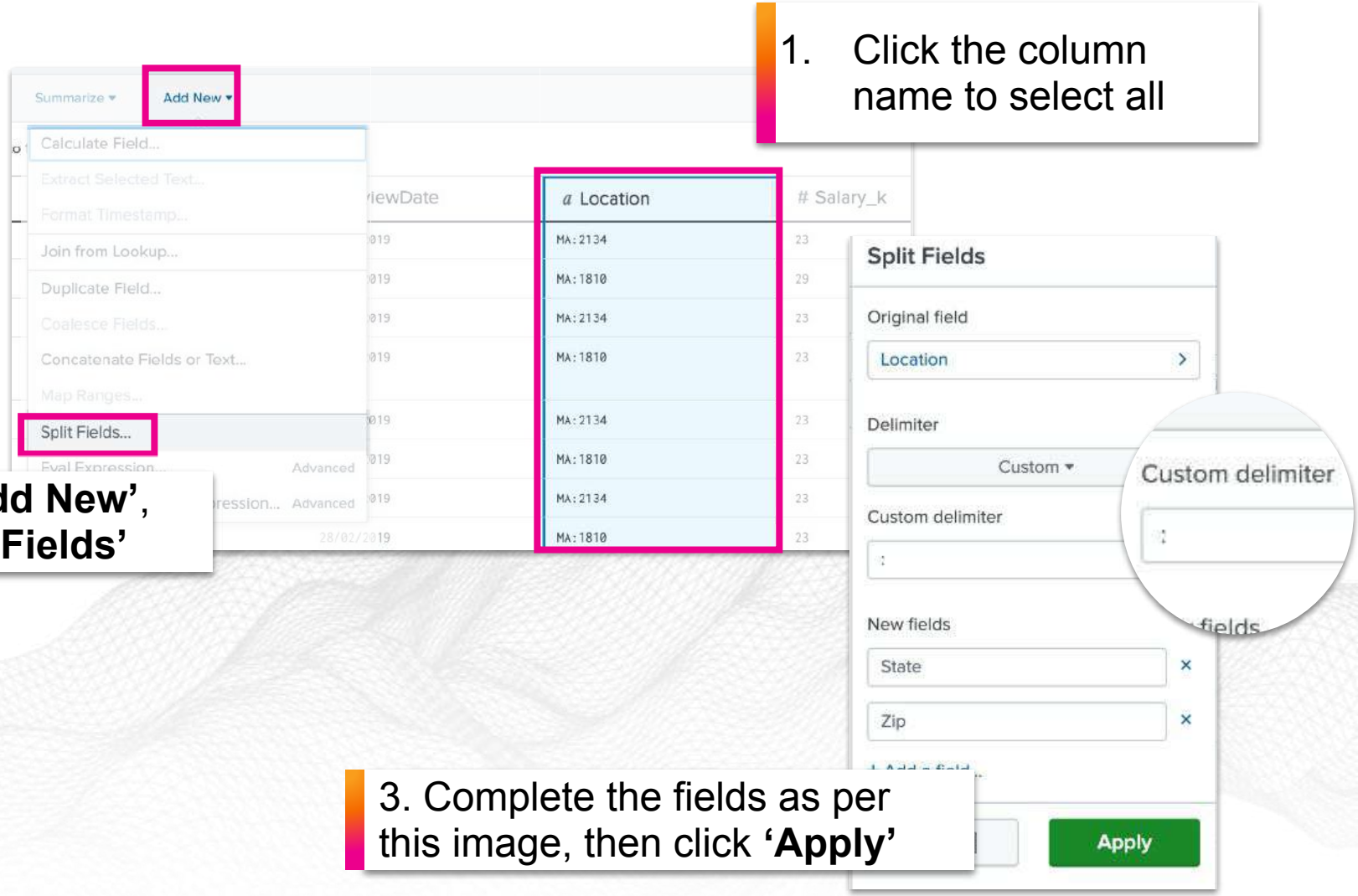


splunk>

Create a New Field

Tasks:

1. Create a new field across multiple files without modifying the original data

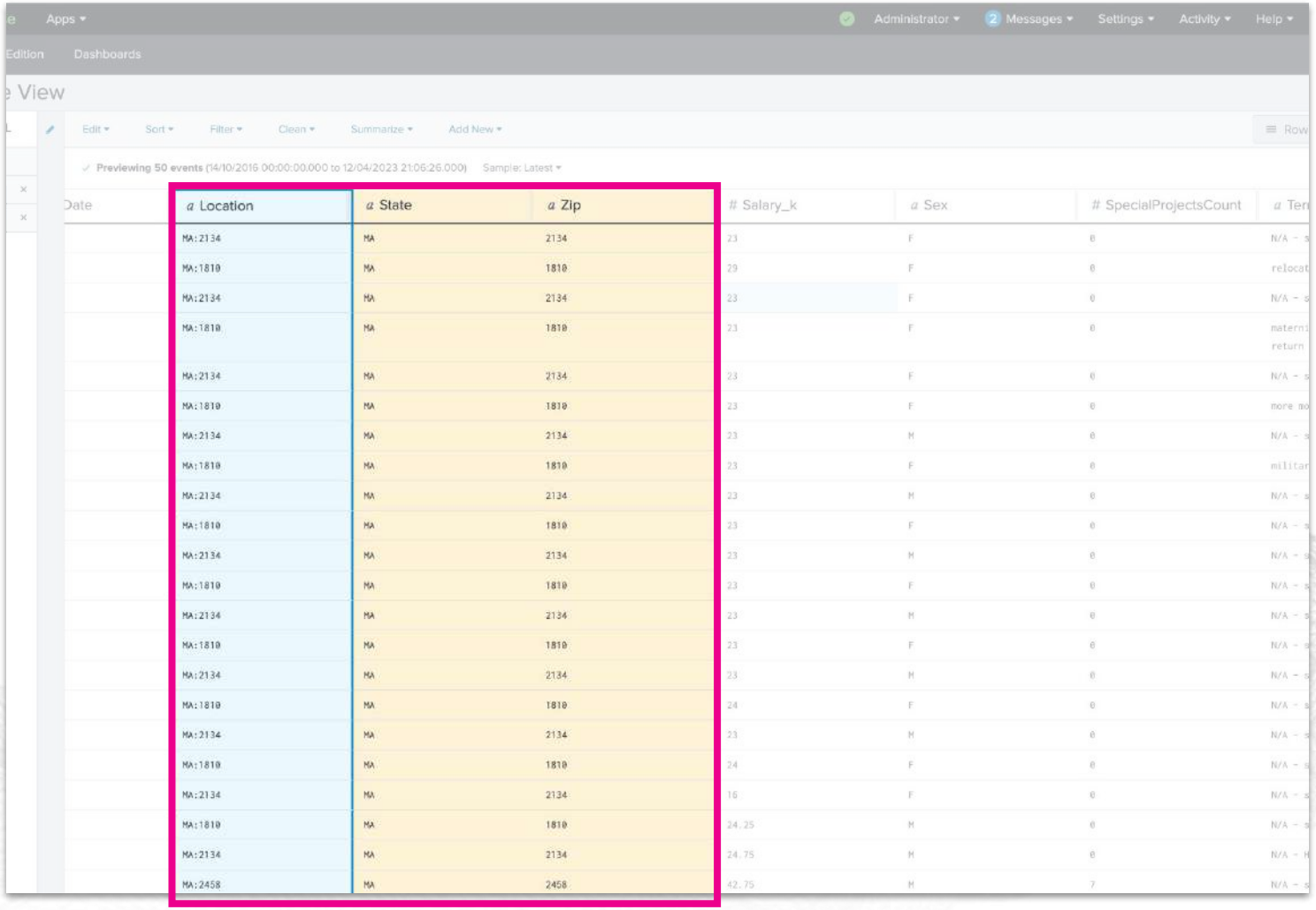


splunk>

Create a New Field

Tasks:

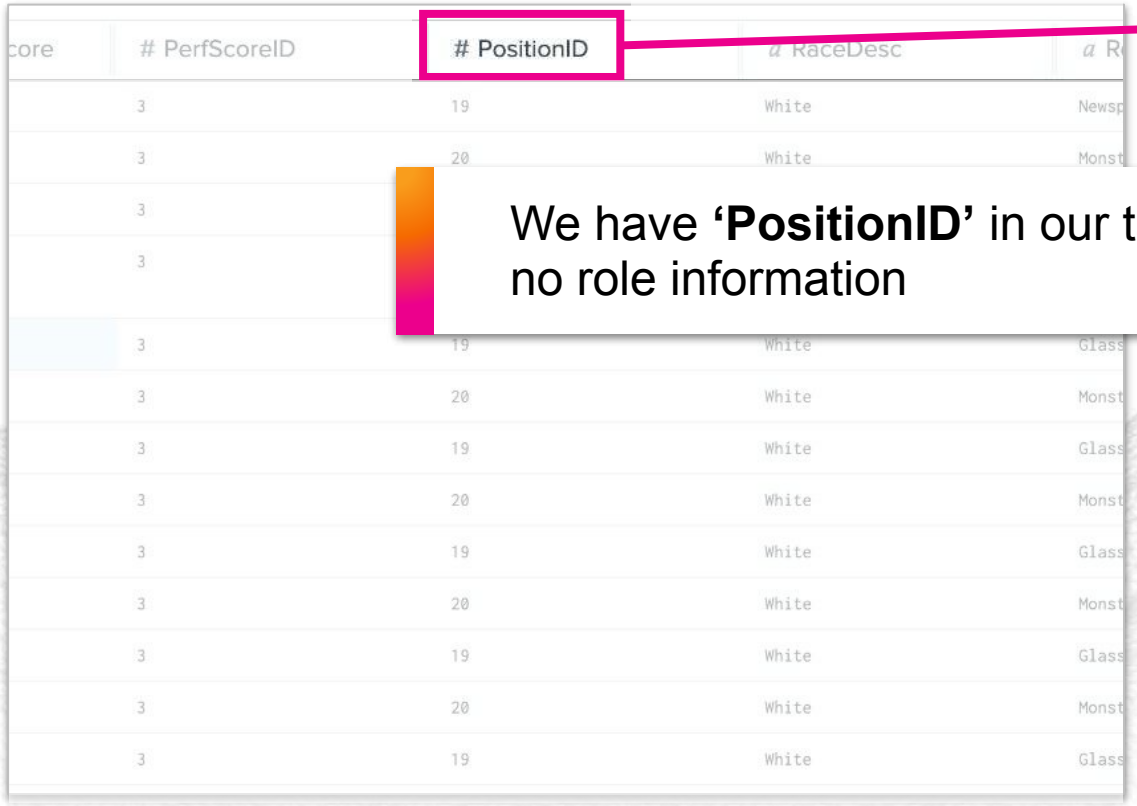
1. Explore the new fields created on the fly



splunk>

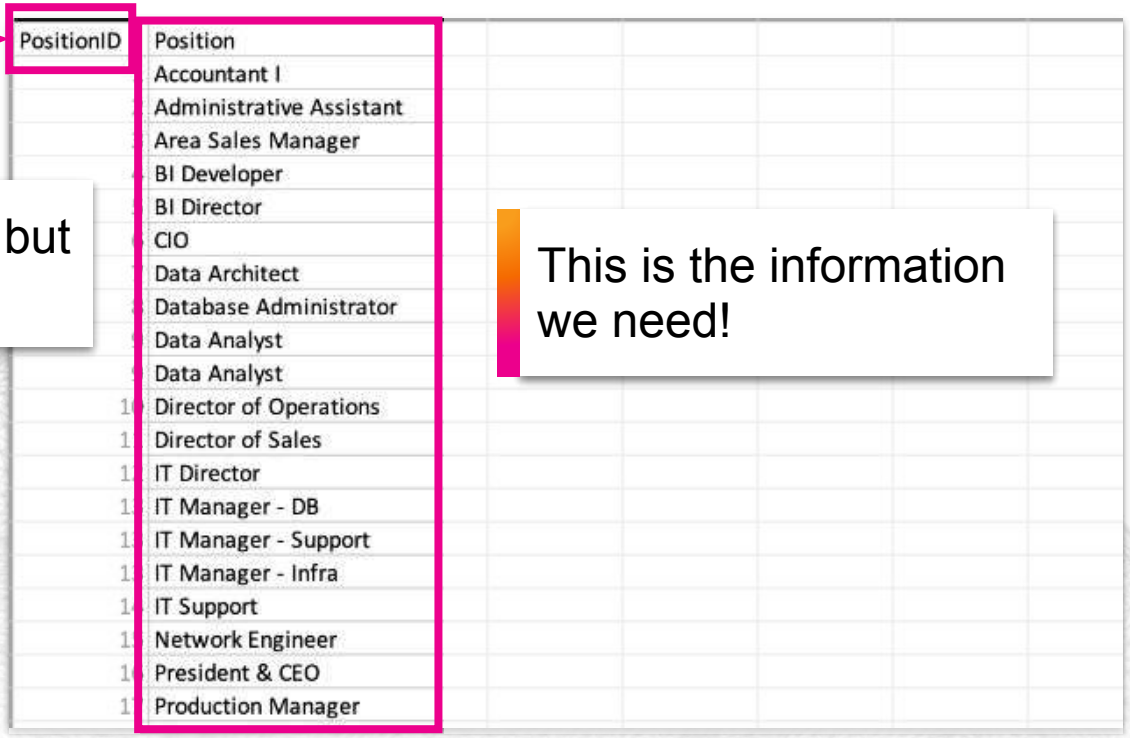
What is a Lookup?

Fields extracted from events by Splunk:



We have **'PositionID'** in our table, but no role information

External CSV file:



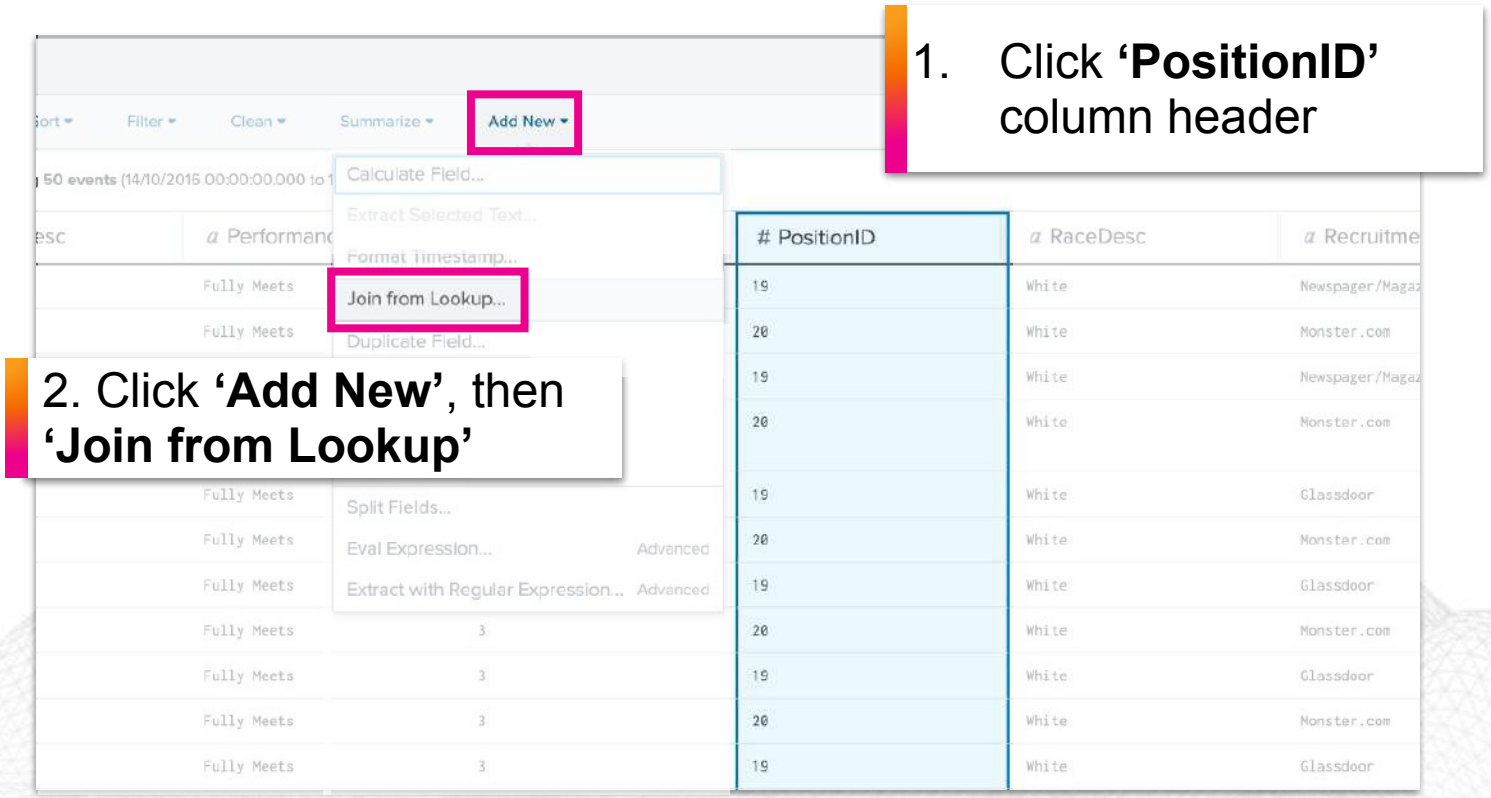
This is the information we need!

splunk>

Configuring the lookup

Tasks:

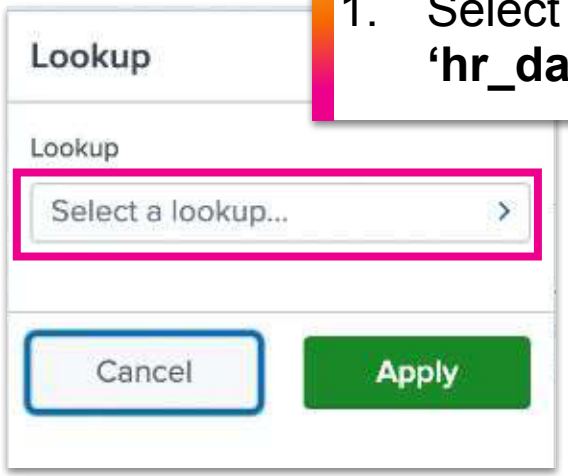
1. Extend our dataset with further metadata around what the Position number means
2. Do this by utilising a ‘lookup’



splunk>

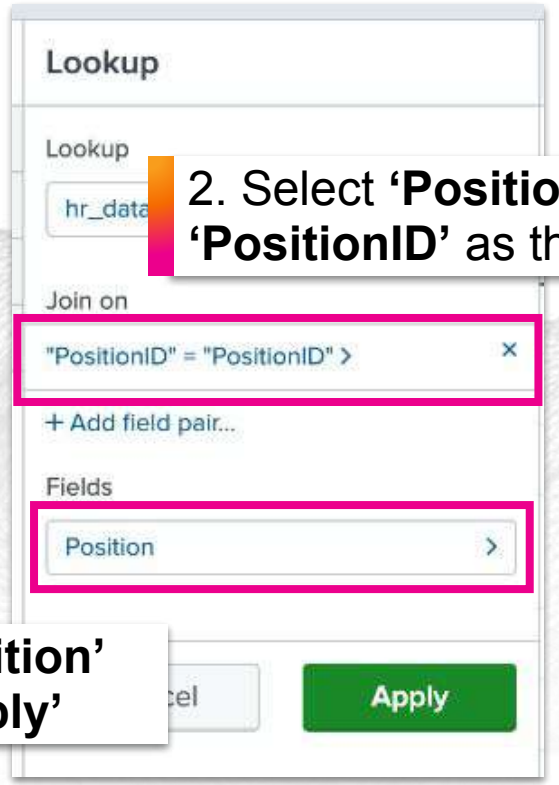
Configuring the lookup

1. Select the **'hr_data_positions_lookup'**



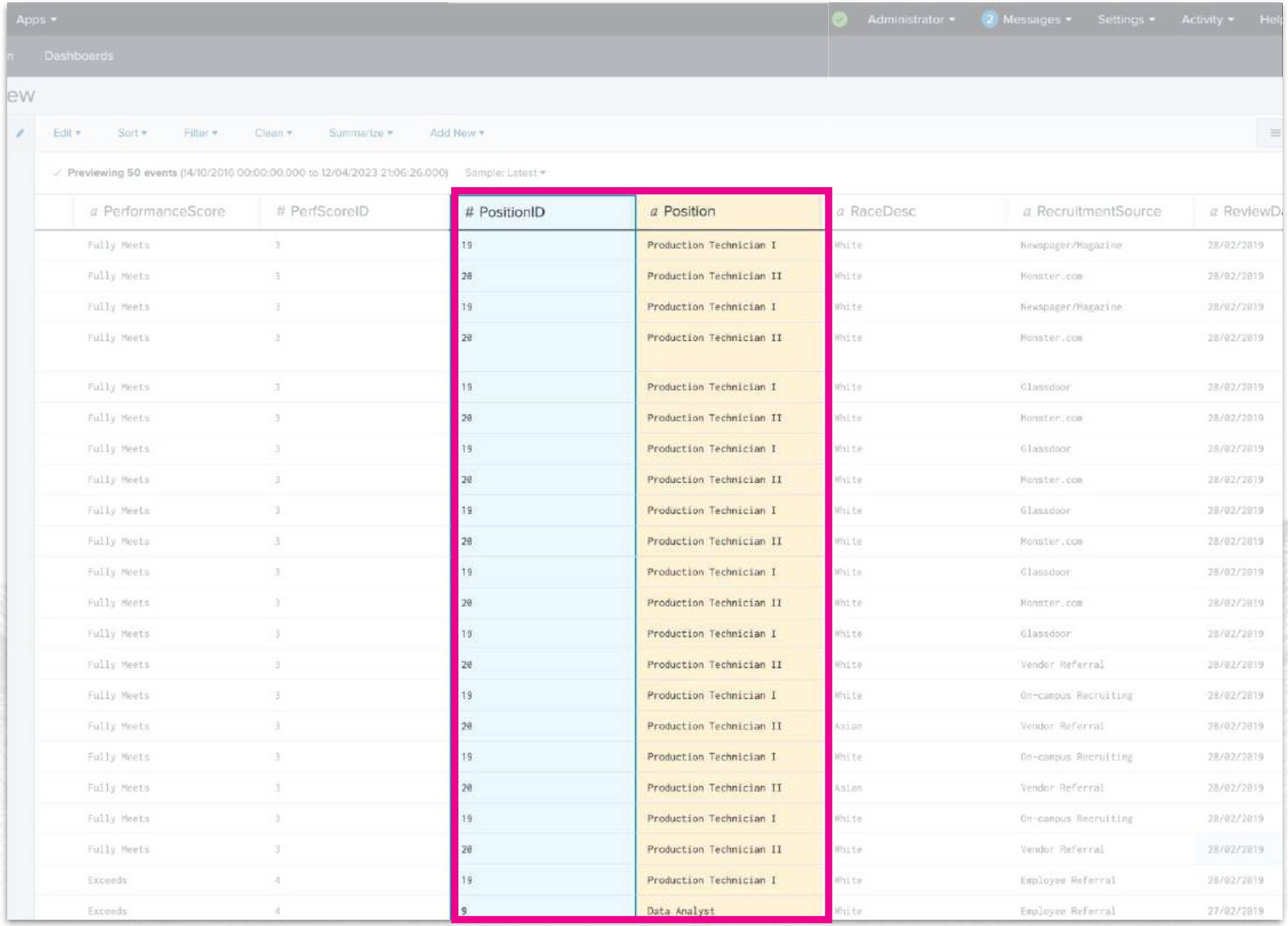
2. Select **'PositionID'** then **'PositionID'** as the join

3. Select **'Position'** then click **'Apply'**



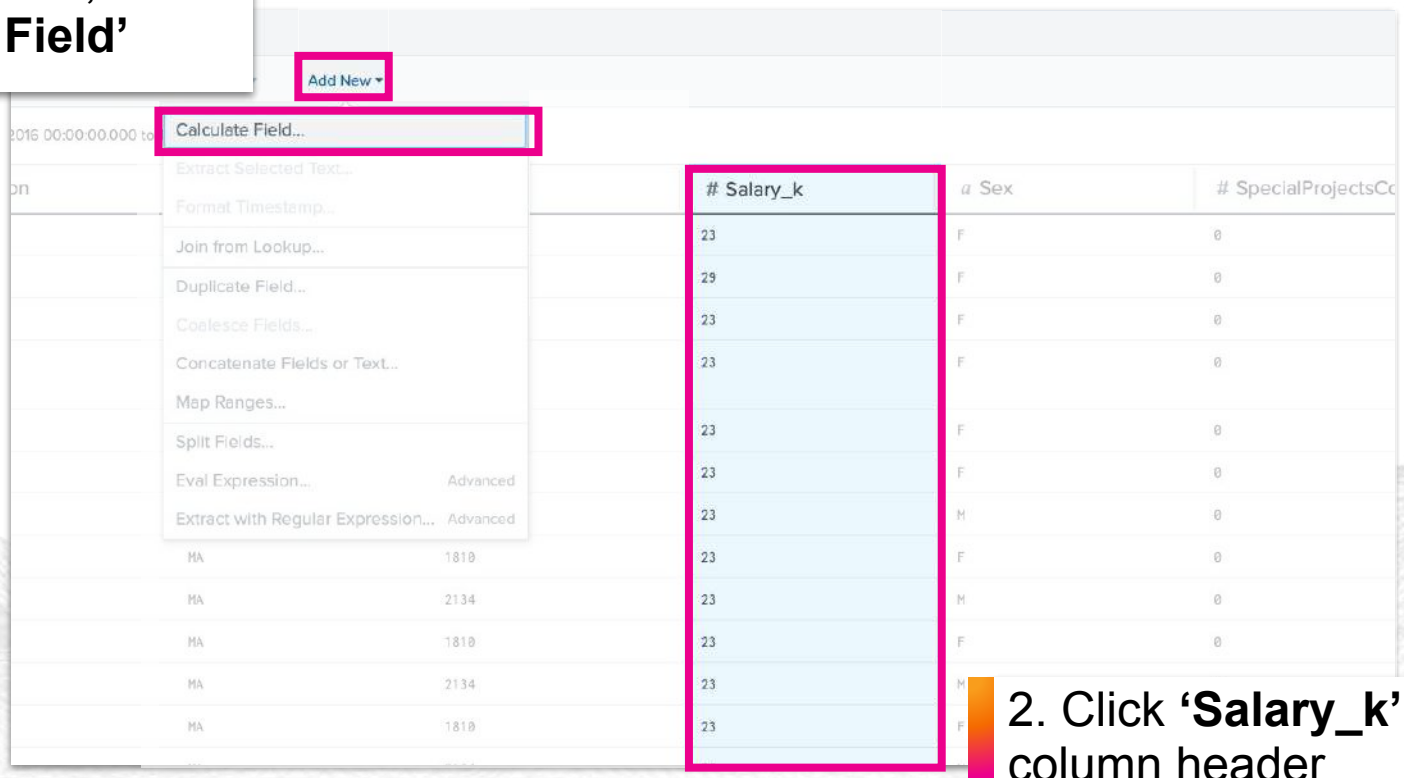
splunk>

Explore the extended fields



Calculated Field

1. Click **‘Add New’**, then **‘Calculated Field’**



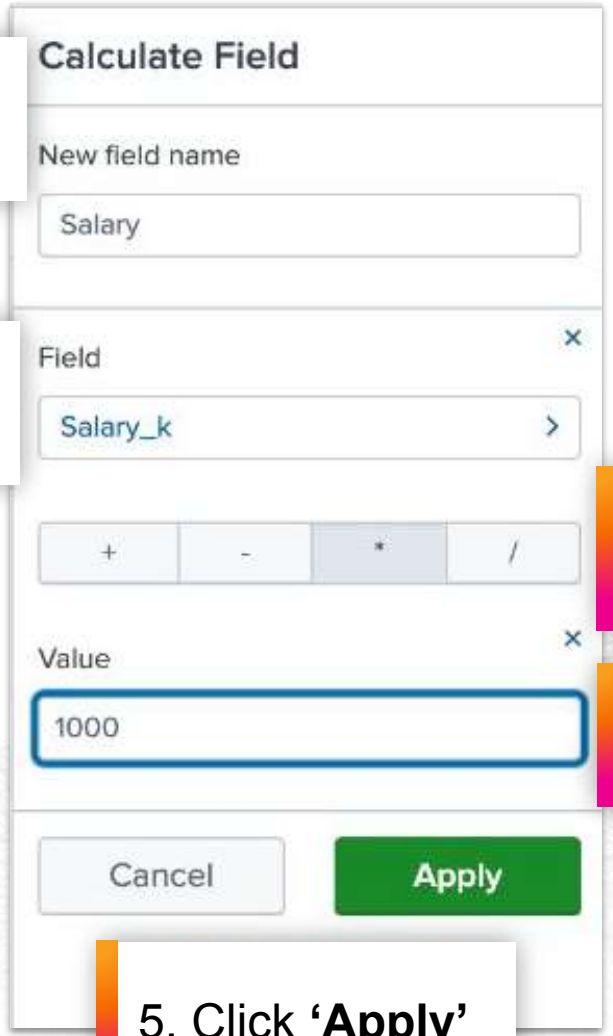
2. Click **‘Salary_k’** column header

splunk>

Calculated Field

1. Enter **'Salary'** as the field name

2. Click **'Add Numeric Field'**, then **'Salary_k'**



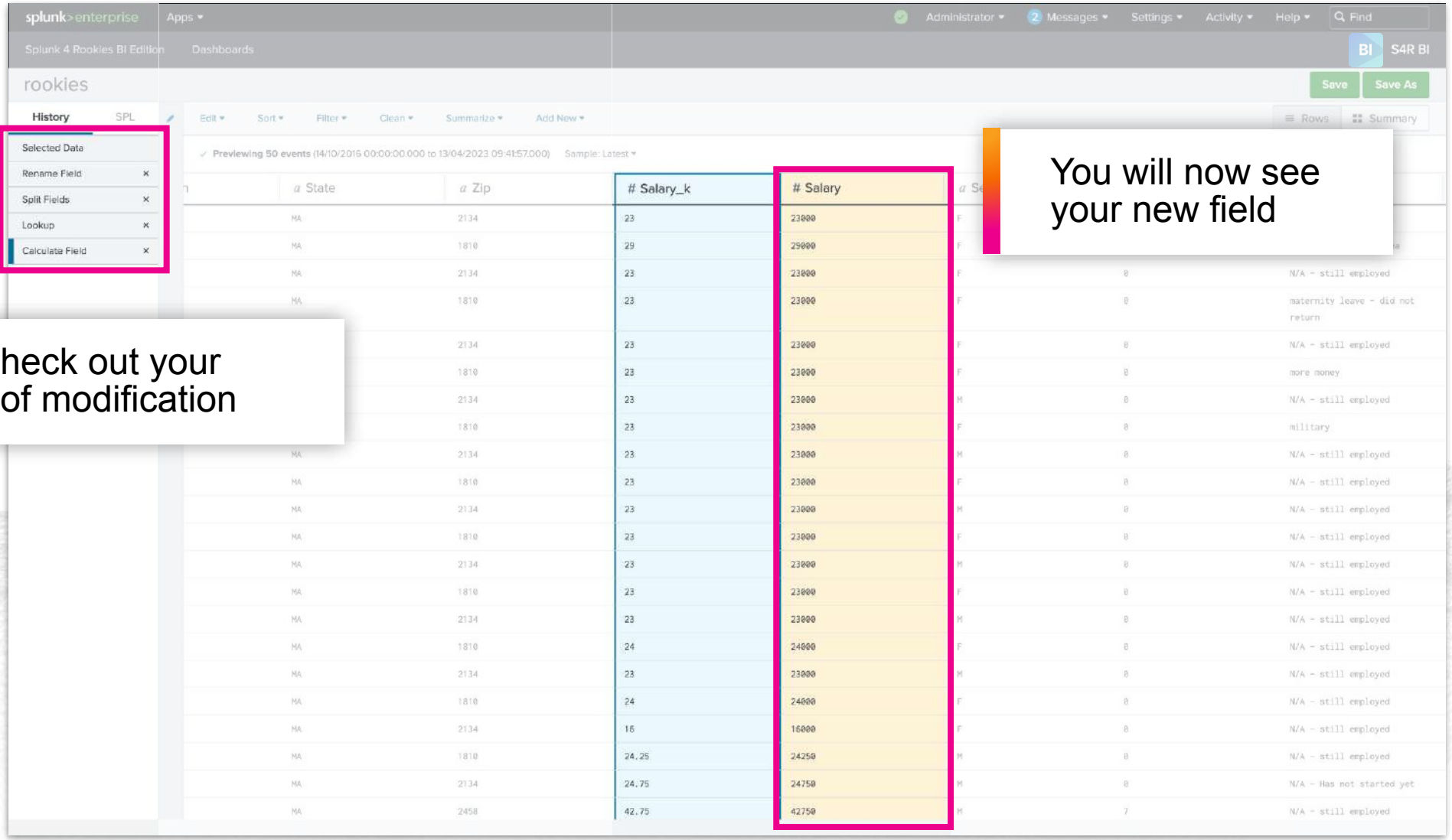
3. Select Multiply

4. Click **'Add Numeric Value'** then enter **'1000'**

5. Click **'Apply'**

splunk>

Create Calculated Field

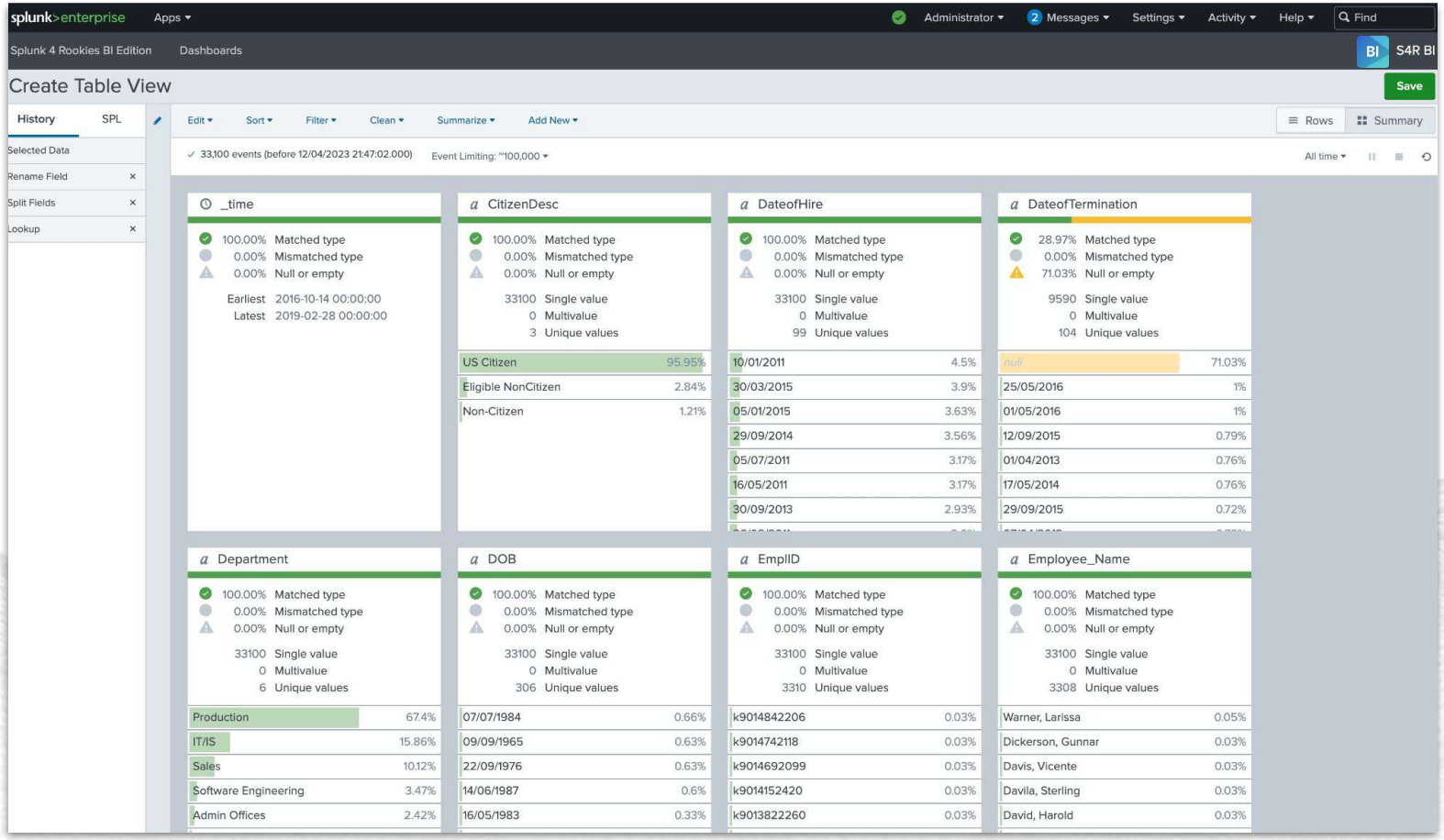


You will now see your new field

Also, Check out your history of modification

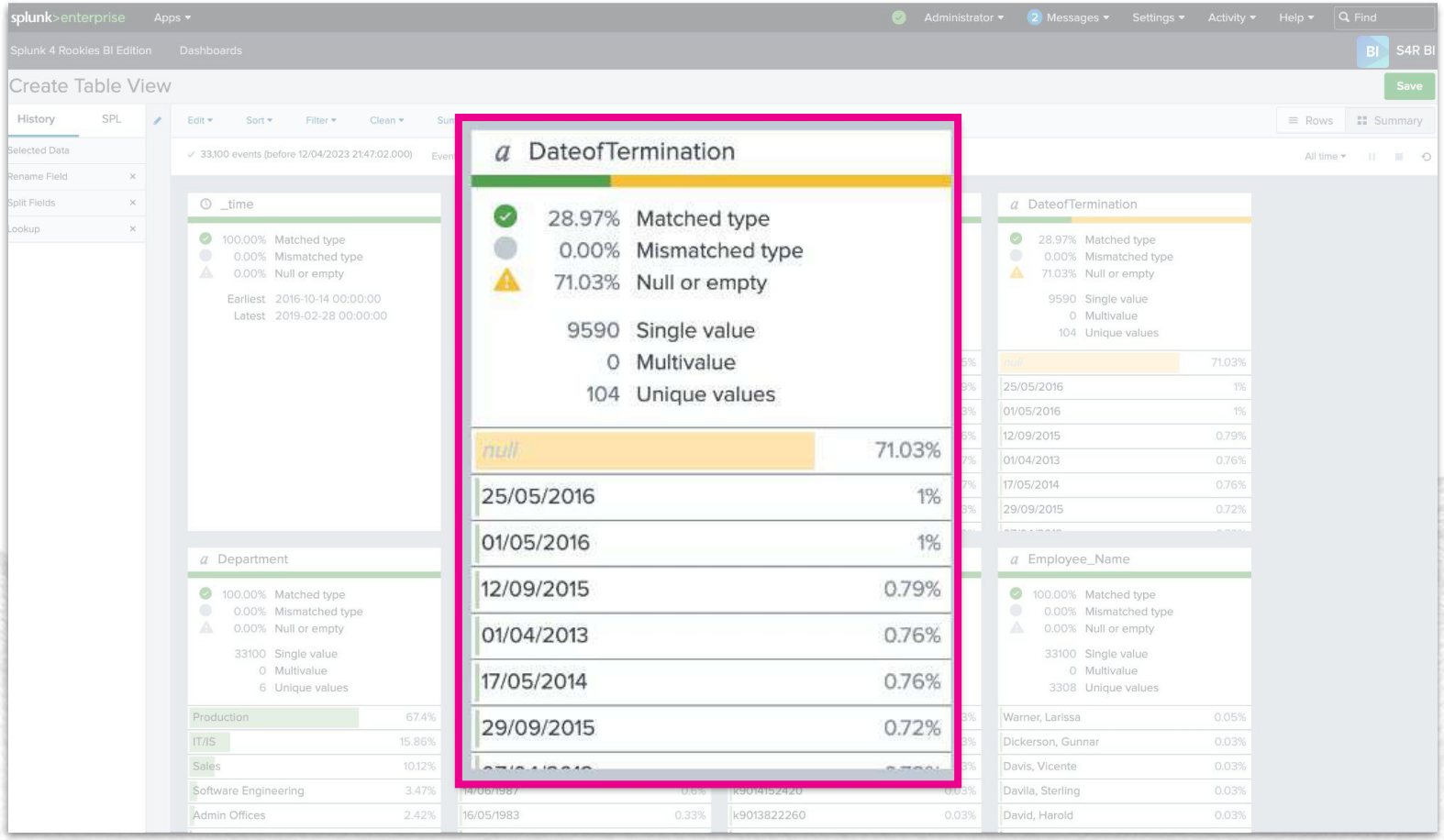
splunk>

Summary of dataset



splunk>

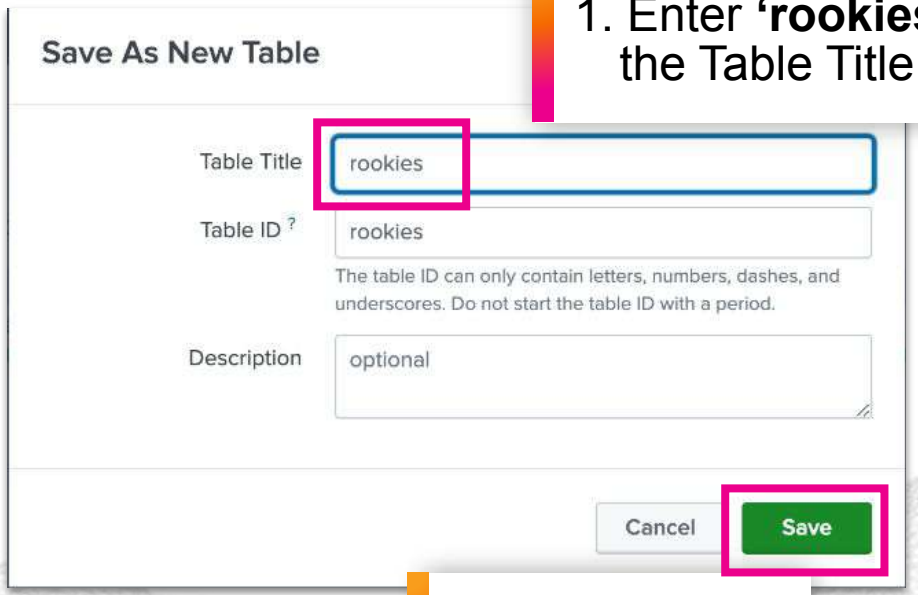
Summary of dataset



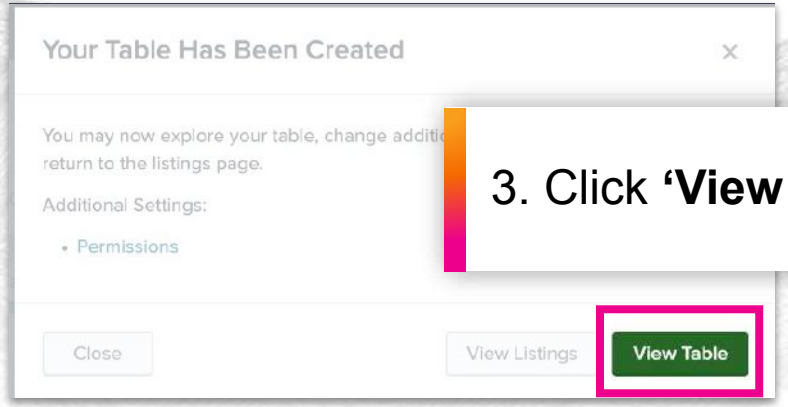
splunk>

Save the table dataset

1. Enter **'rookies'** as the Table Title



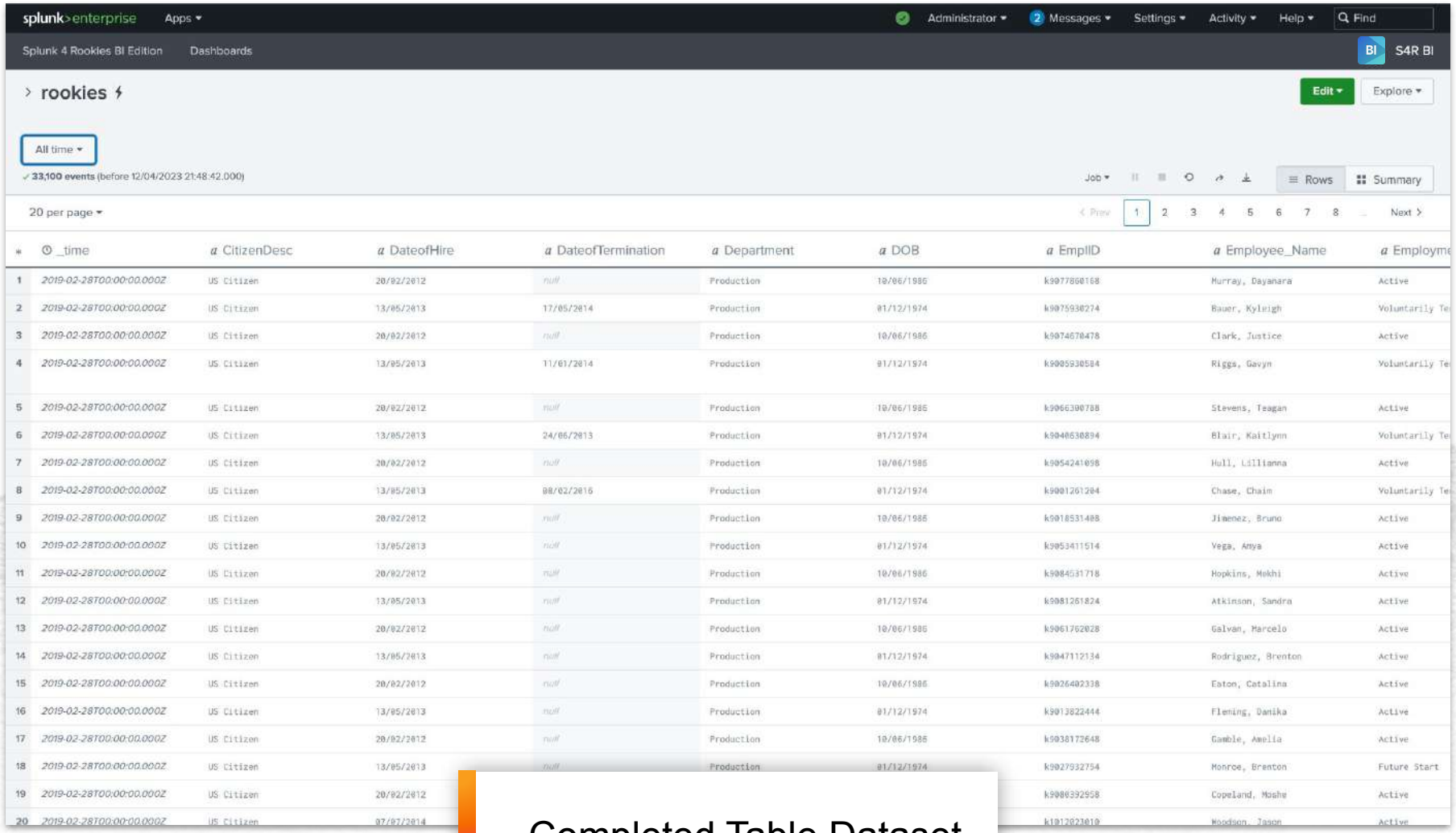
2. Click **'Save'**



3. Click **'View Table'**

splunk>

Table Dataset



Completed Table Dataset

splunk>

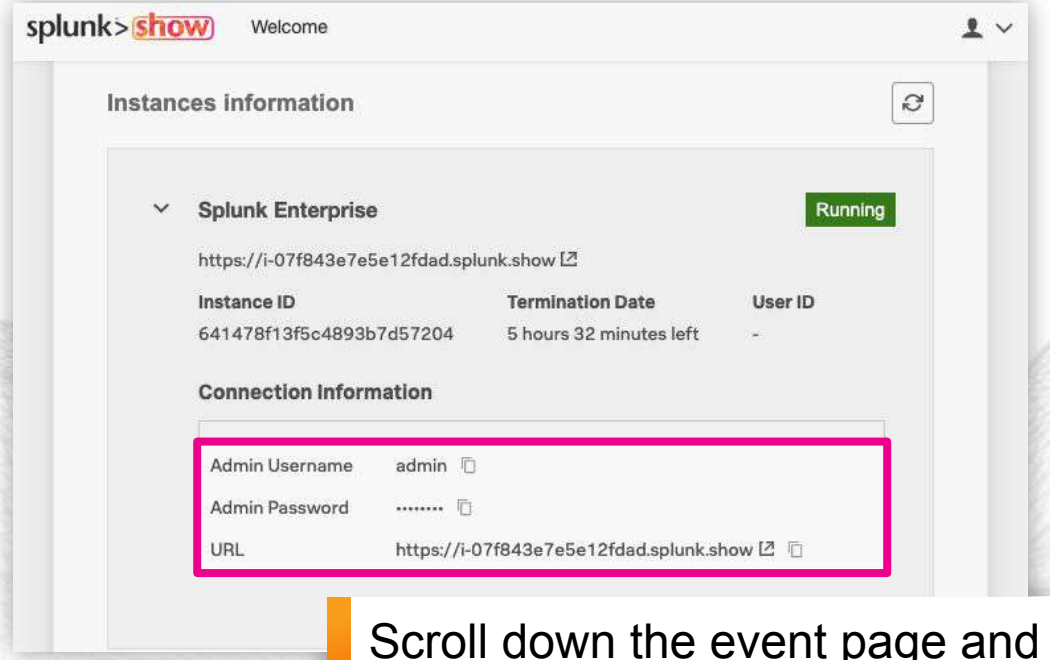
Module 2

Data visualisation with Pivot

splunk>

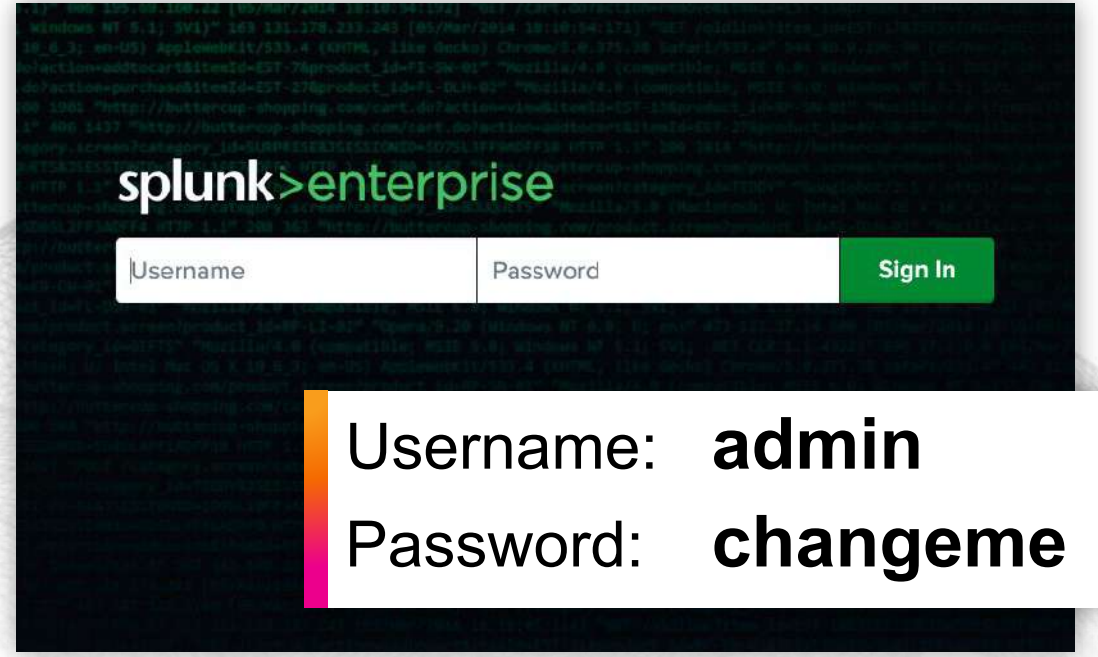
Login to Splunk

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



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

Log in to your Splunk instance

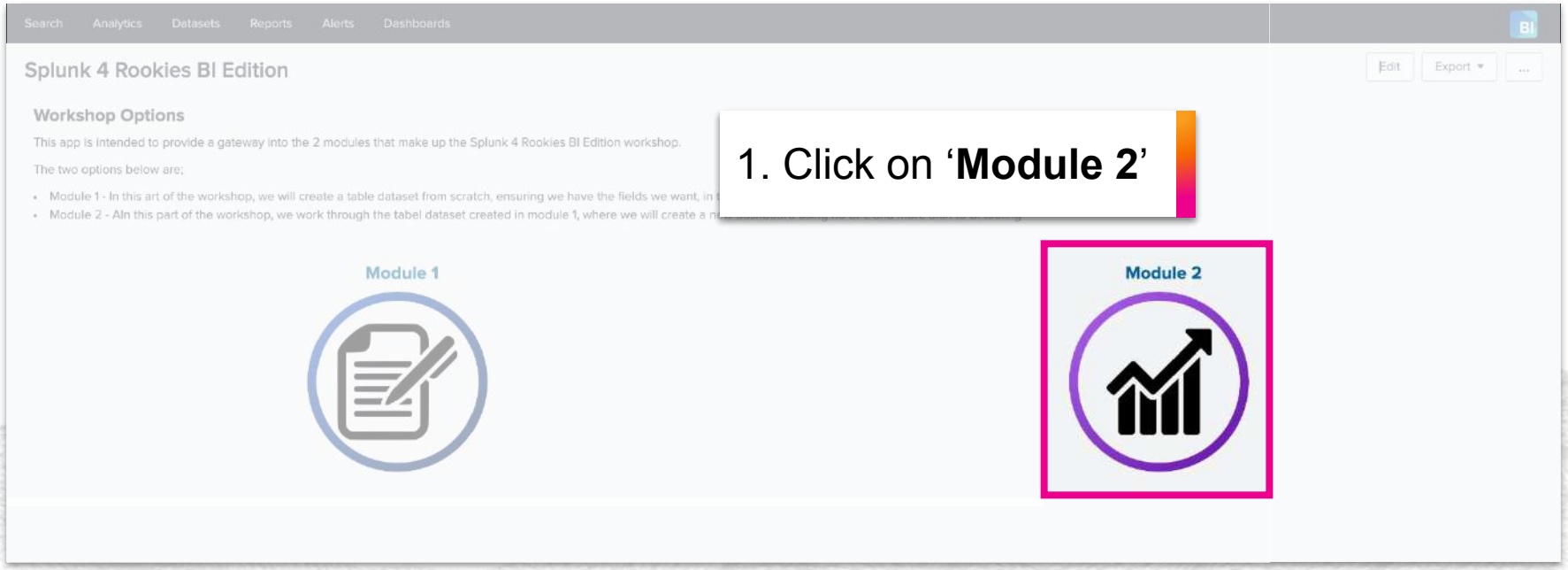


Username: **admin**

Password: **changeme**

splunk>

Navigate to your Module



splunk>

Let's Explore the UI

Visualisations

Save or modify data

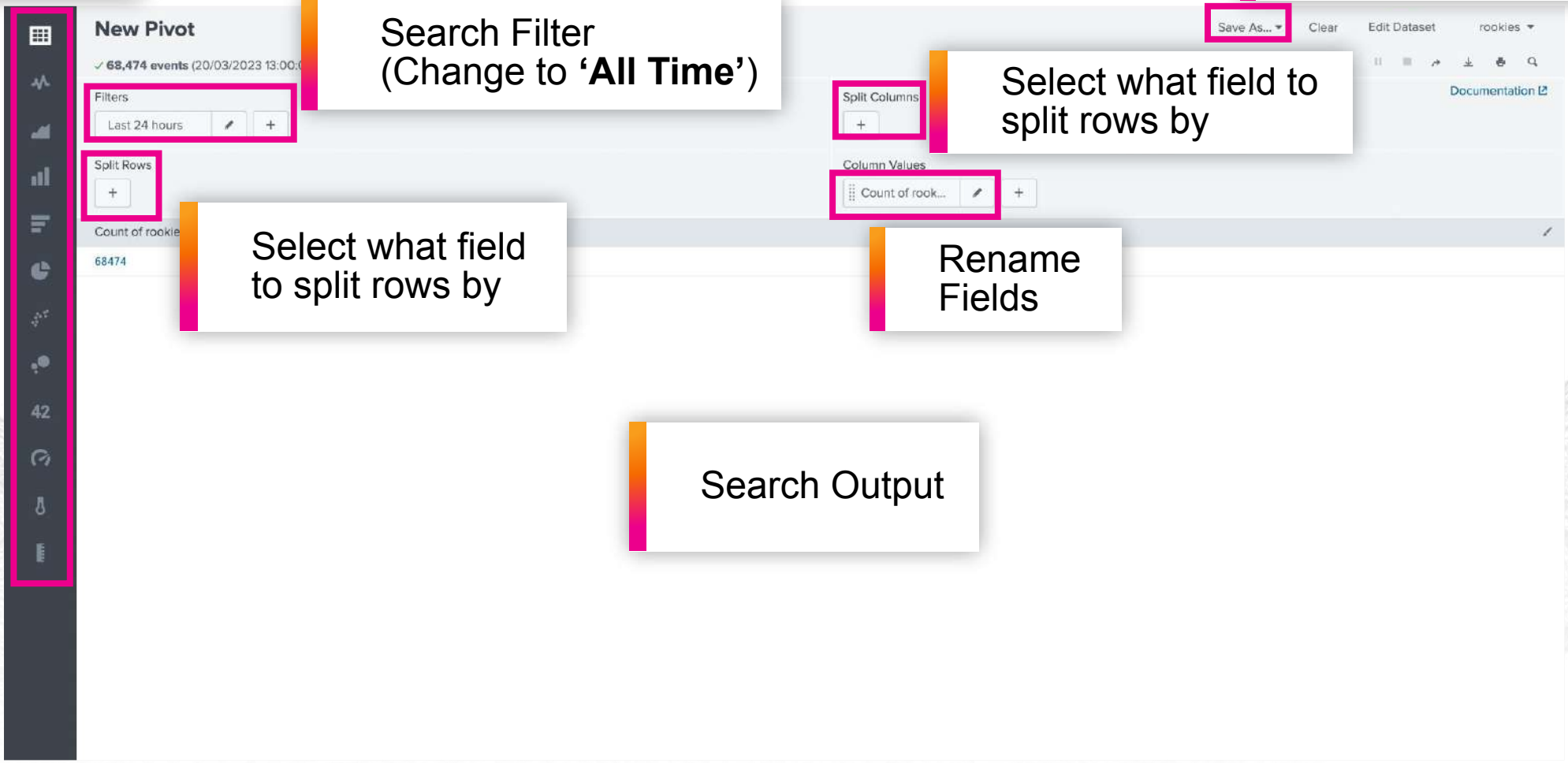
Search Filter (Change to **'All Time'**)

Select what field to split rows by

Select what field to split rows by

Rename Fields

Search Output



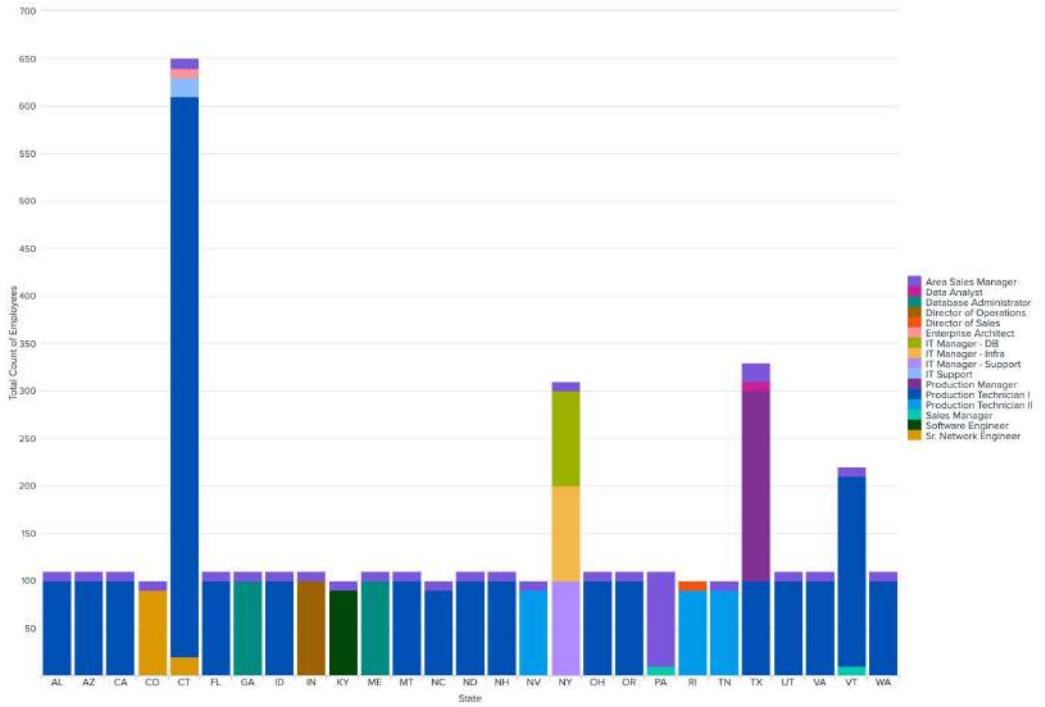
splunk>

How many employees per state by role

Tasks

1. Show how many employees there are per US state
2. Break the employee number down by Position
3. Exclude the HQ in Massachusetts
4. Show the data as a stacked column chart

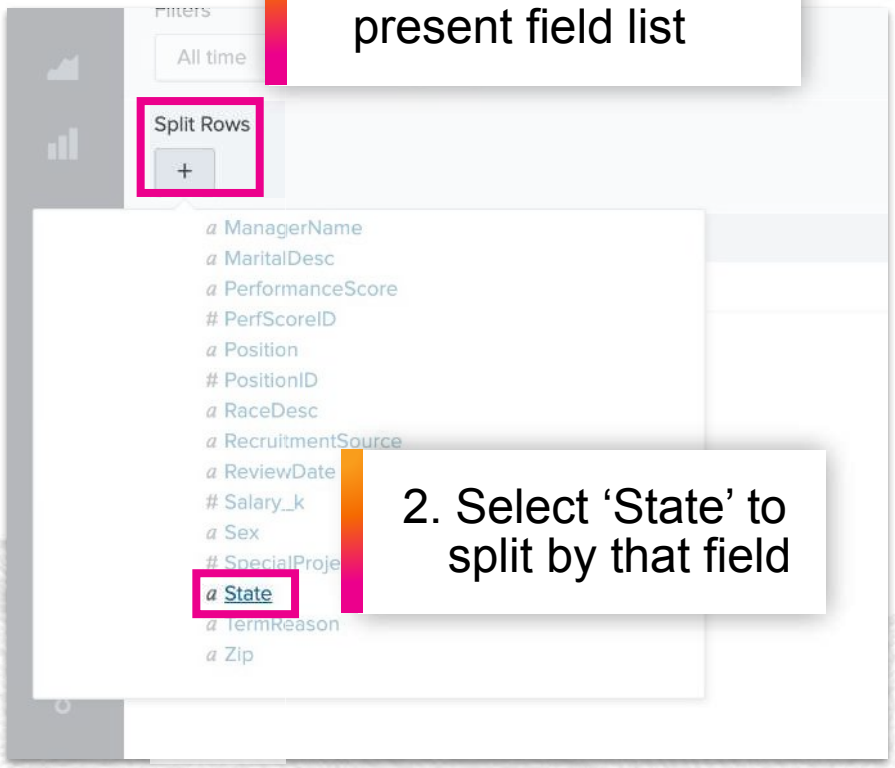
Goal



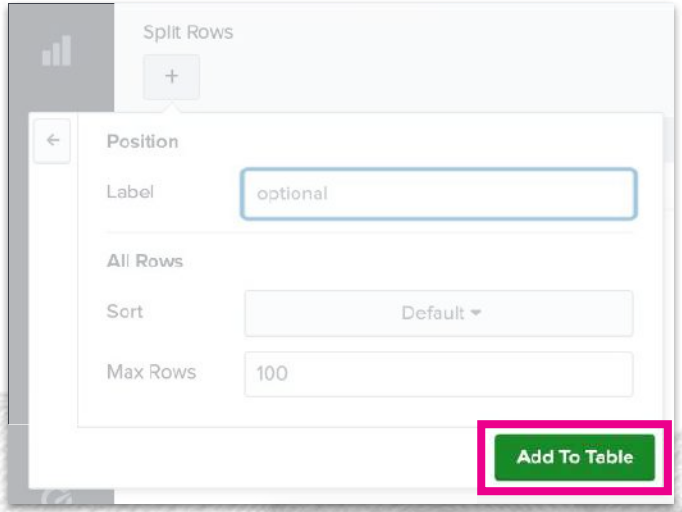
splunk>

Split by Row

1. Click the **'+'** to present field list



2. Select 'State' to split by that field



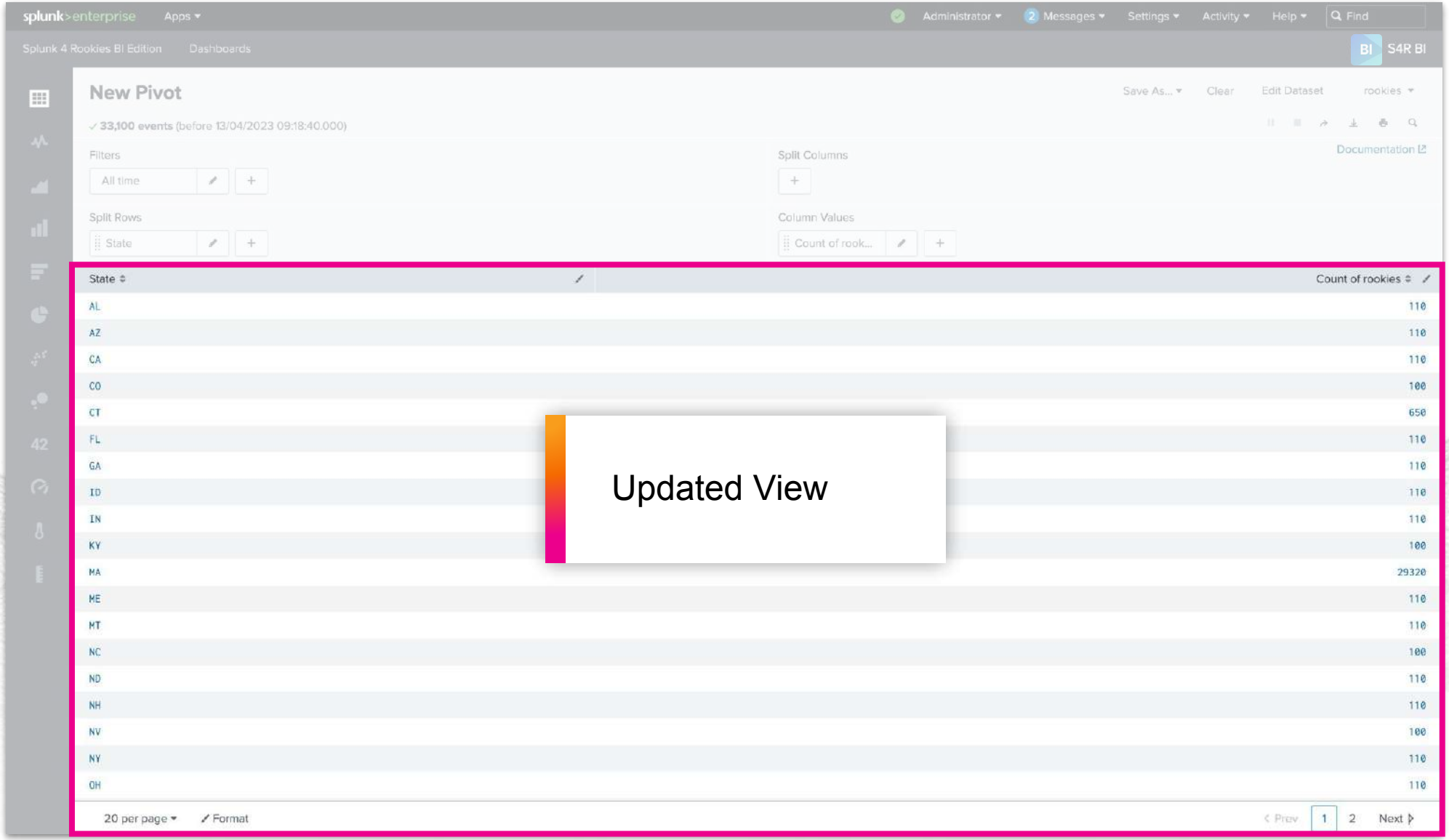
3. Click **'Add To Table'**

Tasks

1. Show how many employees there are per US state

splunk>

Live Changes

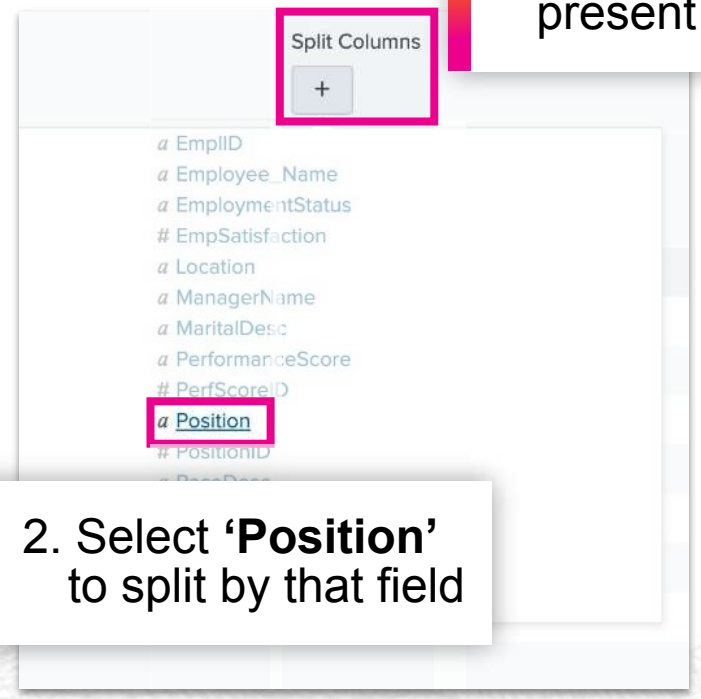


Updated View

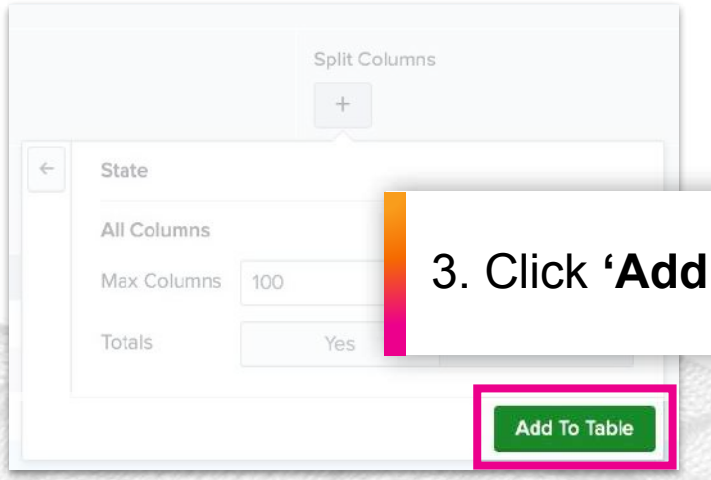
splunk>

Split by Column

1. Click the **'+'** to present column list



2. Select **'Position'** to split by that field

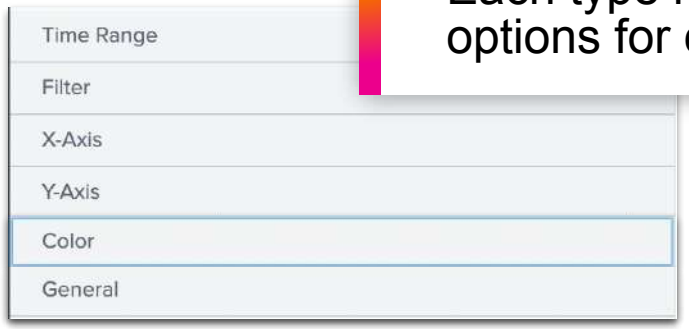


3. Click **'Add To Table'**

splunk>

Explore the Visualisations

Explore the visualisations

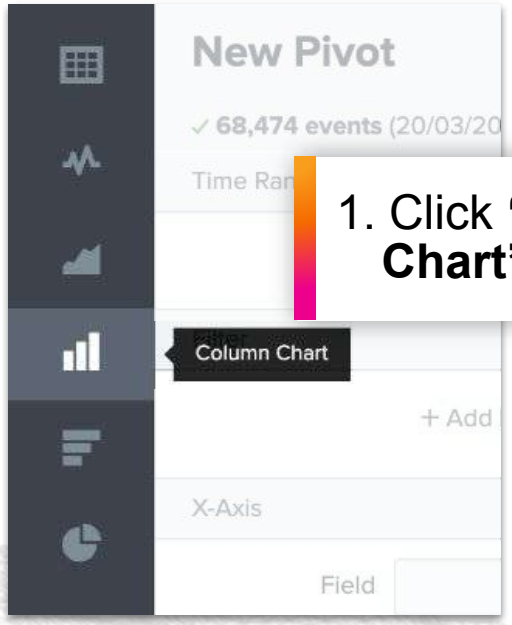


Each type has many options for customisation

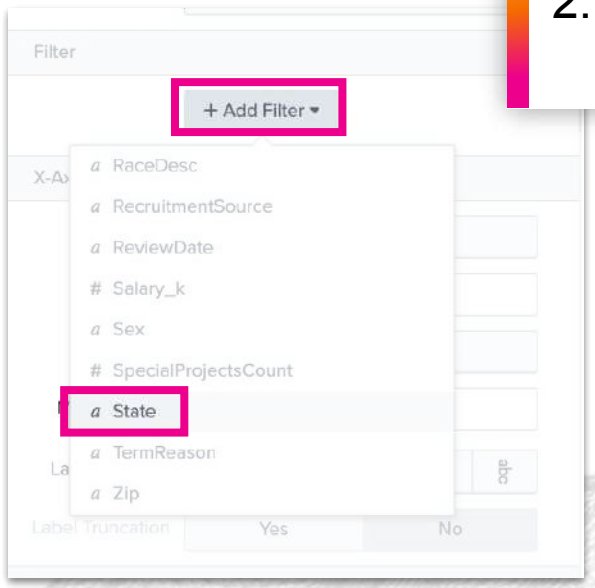
Hint

4. Show as a stacked column chart

Configure Visualisation

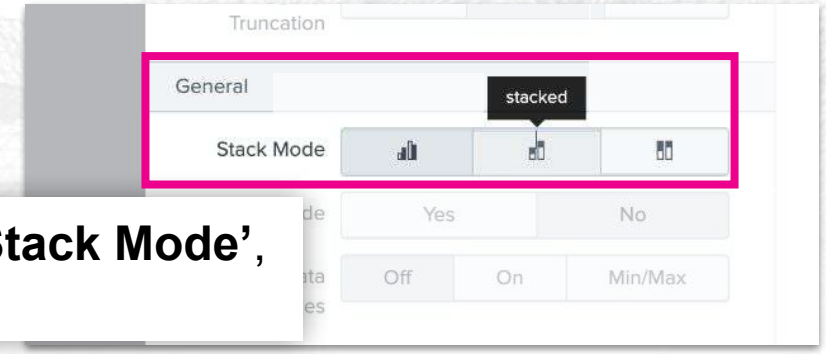


1. Click **‘Column Chart’**



2. Click **‘Add Filter’**, then select **‘State’**

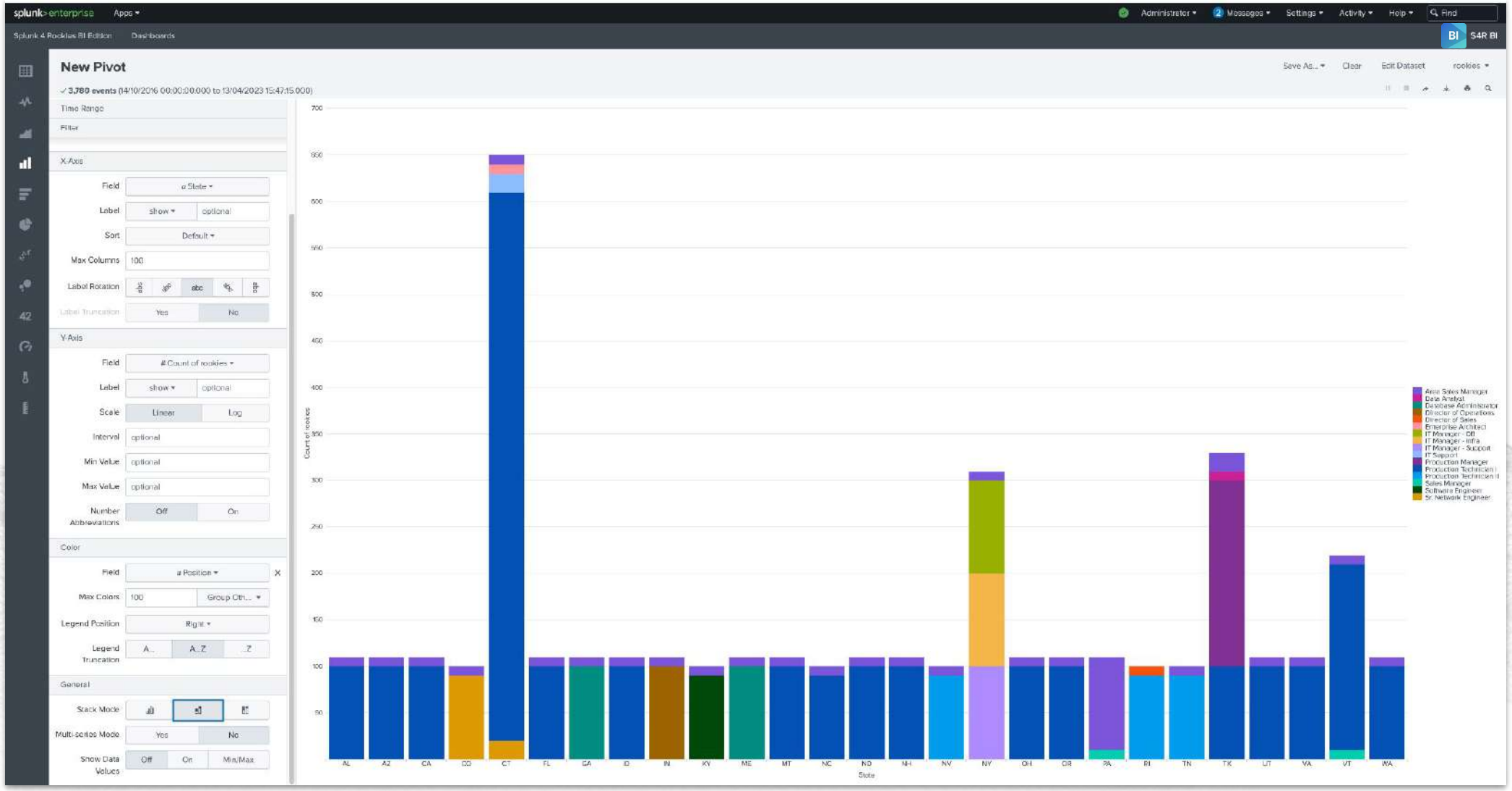
3. Change match to **‘is not’** then enter **‘MA’**



4. Under **‘General’** - **‘Stack Mode’**, Select **‘Stacked’**

splunk>

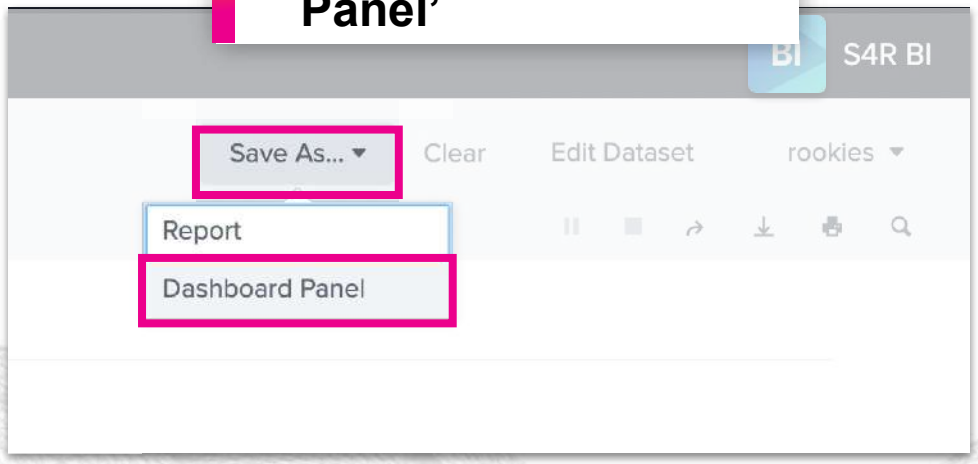
Completed Visualisation



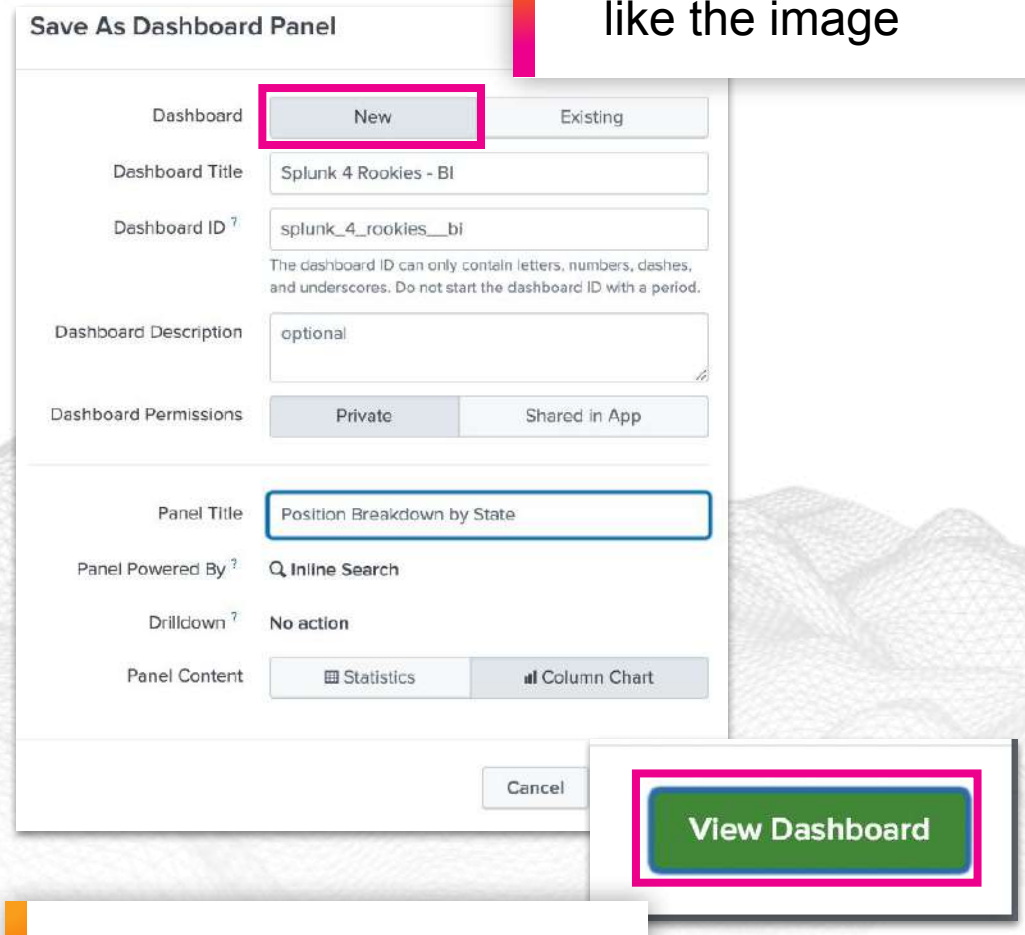
splunk>

Save Our Visualisation

1. Select **‘Save As’**, then **‘Dashboard Panel’**



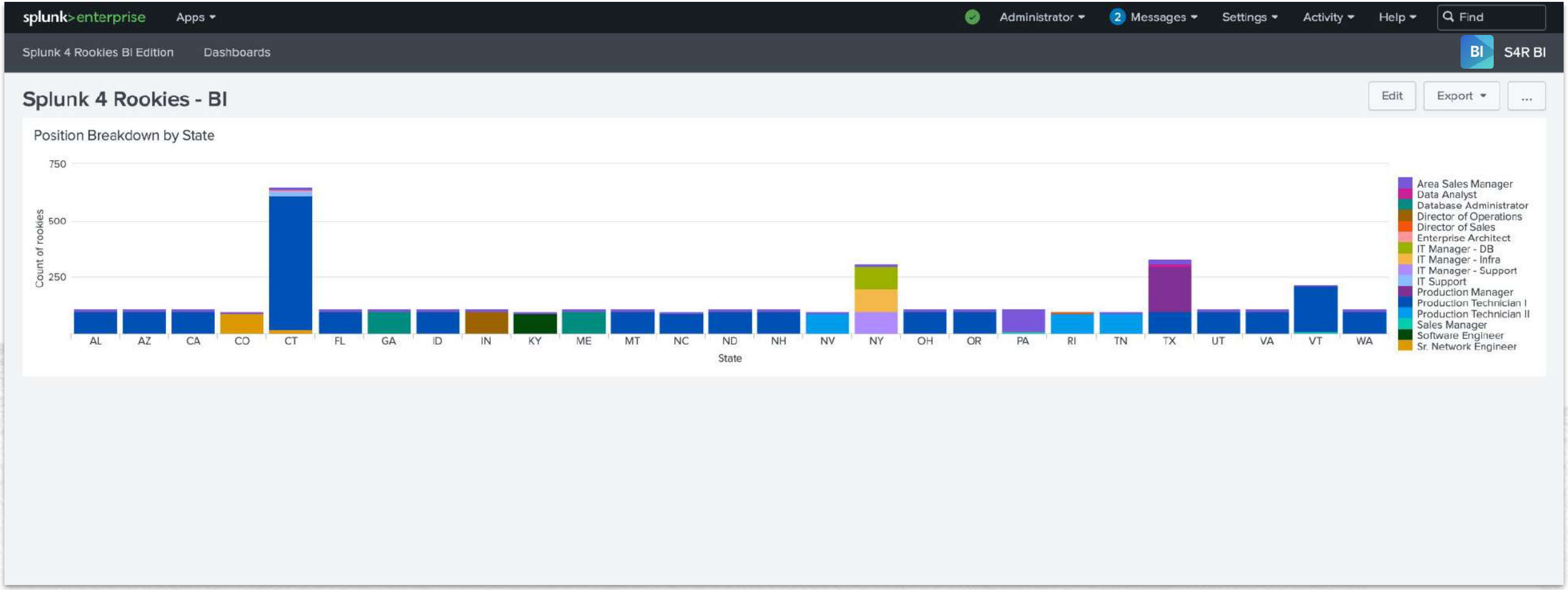
2. Complete the form like the image



3. Click **‘View Dashboard’**

splunk>

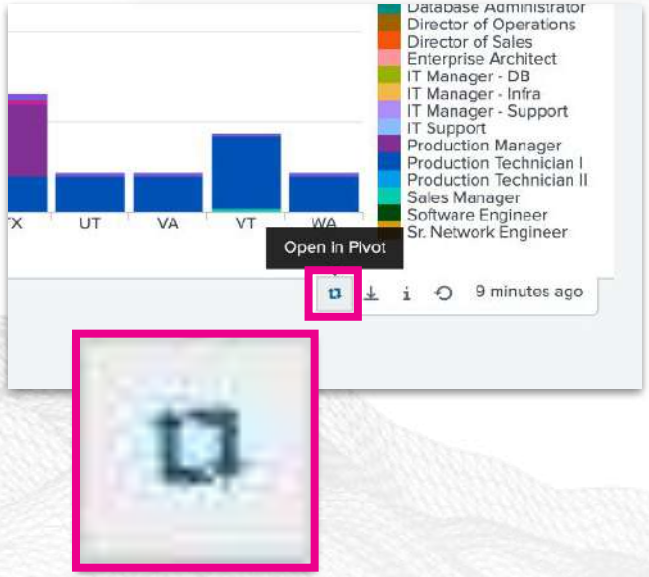
Your Dashboard So Far…

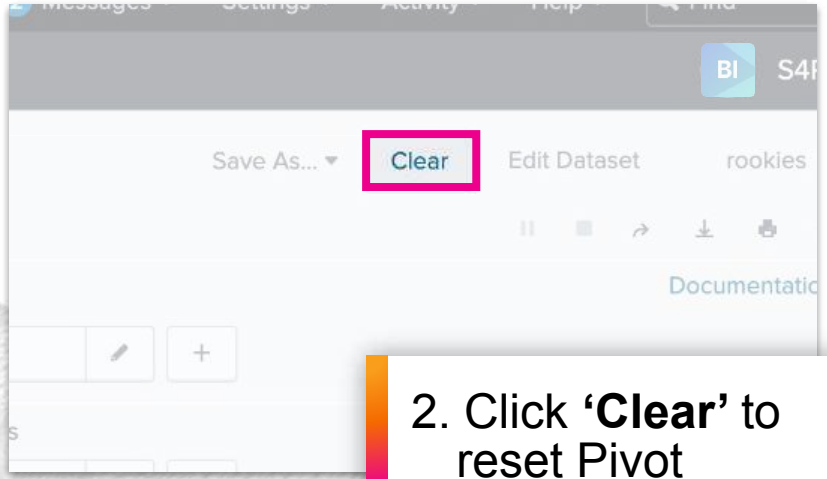


splunk>

Return to Pivot

1. Hover over the bottom right of the chart and click the Pivot icon





2. Click **'Clear'** to reset Pivot

splunk>

Employee Satisfaction

Tasks

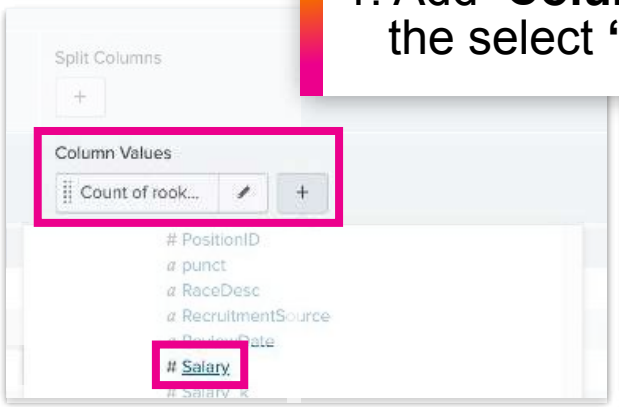
1. Display employee satisfaction
2. Compare this with the employee performance
3. Have a third dimension of Salary size
4. Display this as a Bubble chart and save it to your dashboard

Goal

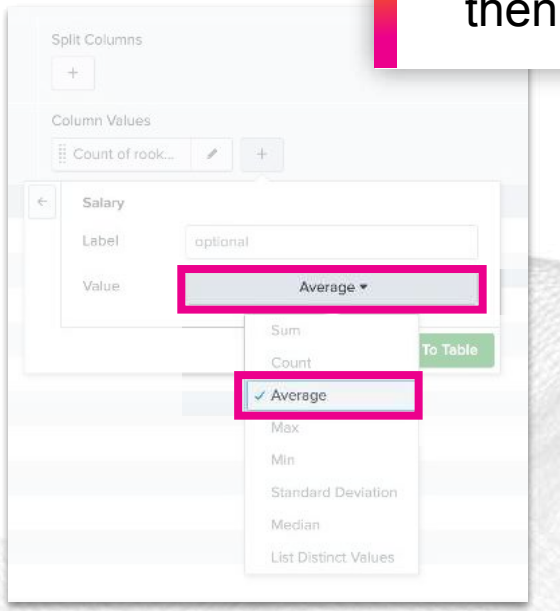
Take 10 minutes to explore the data and attempt to create the required visual

Create Visualisation

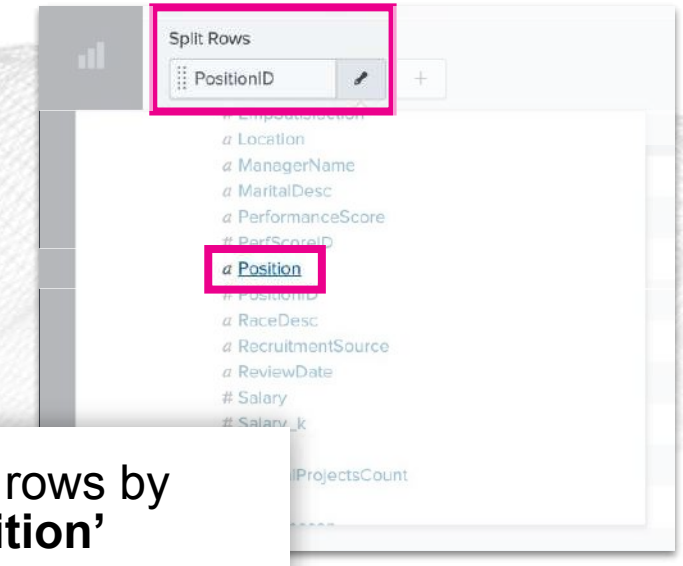
1. Add **'Column Values'**, the select **'Salary'**



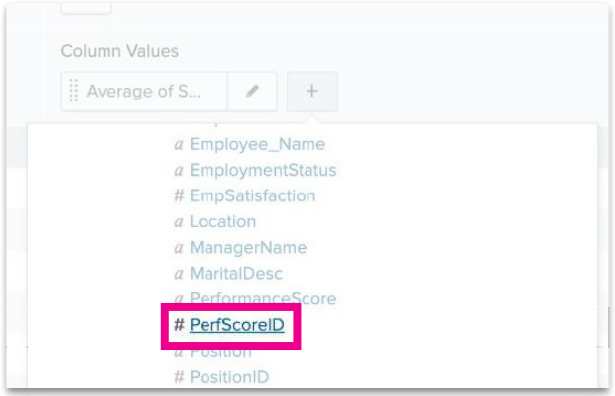
2. Select **'Average'** and then **'Add To Table'**



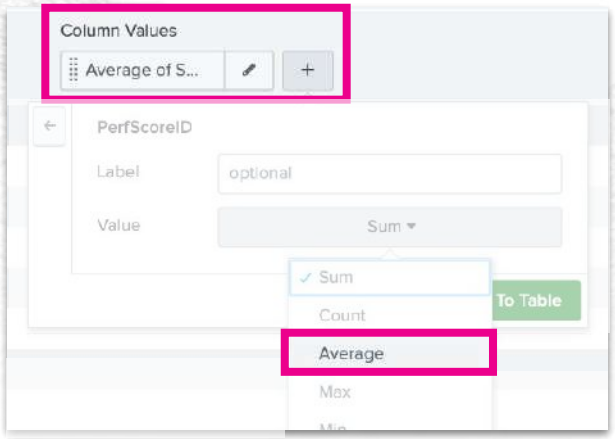
3. Split rows by **'Position'**

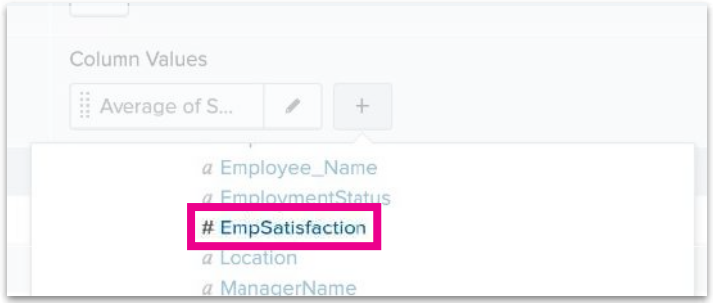


Create Visualisation

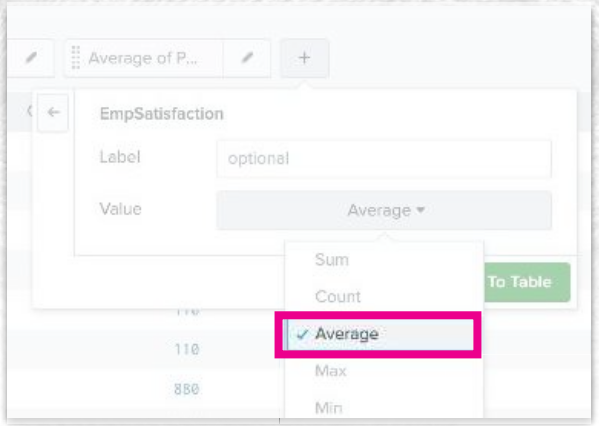


1. Add **'PerfScoreID'**, then select **'Average'**



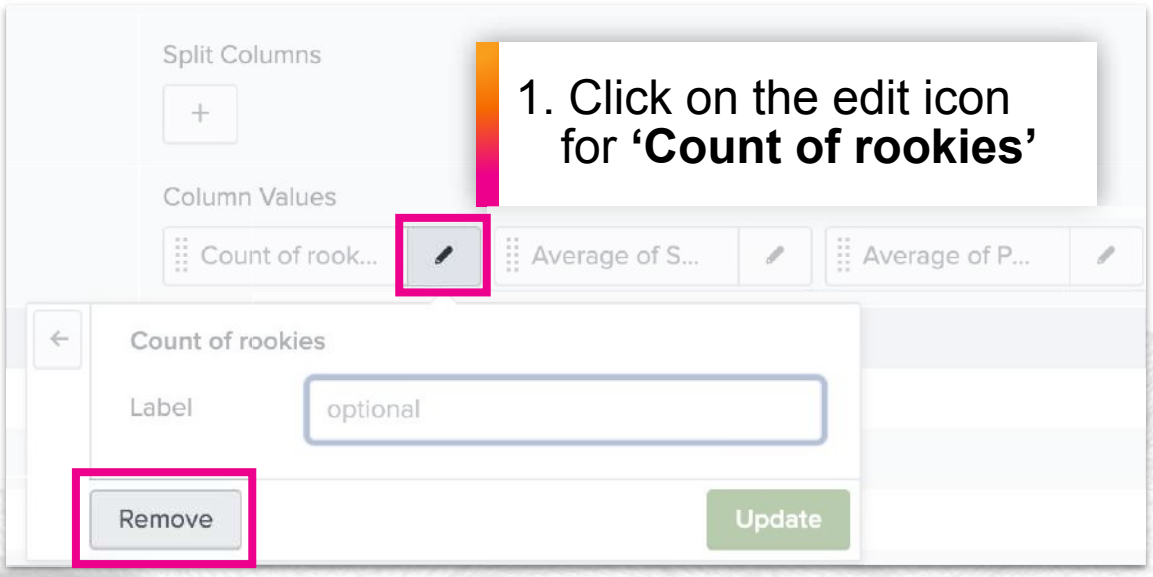


2. Add **'EmpSatisfaction'**, then **'Average'**



splunk>

Create Visualisation

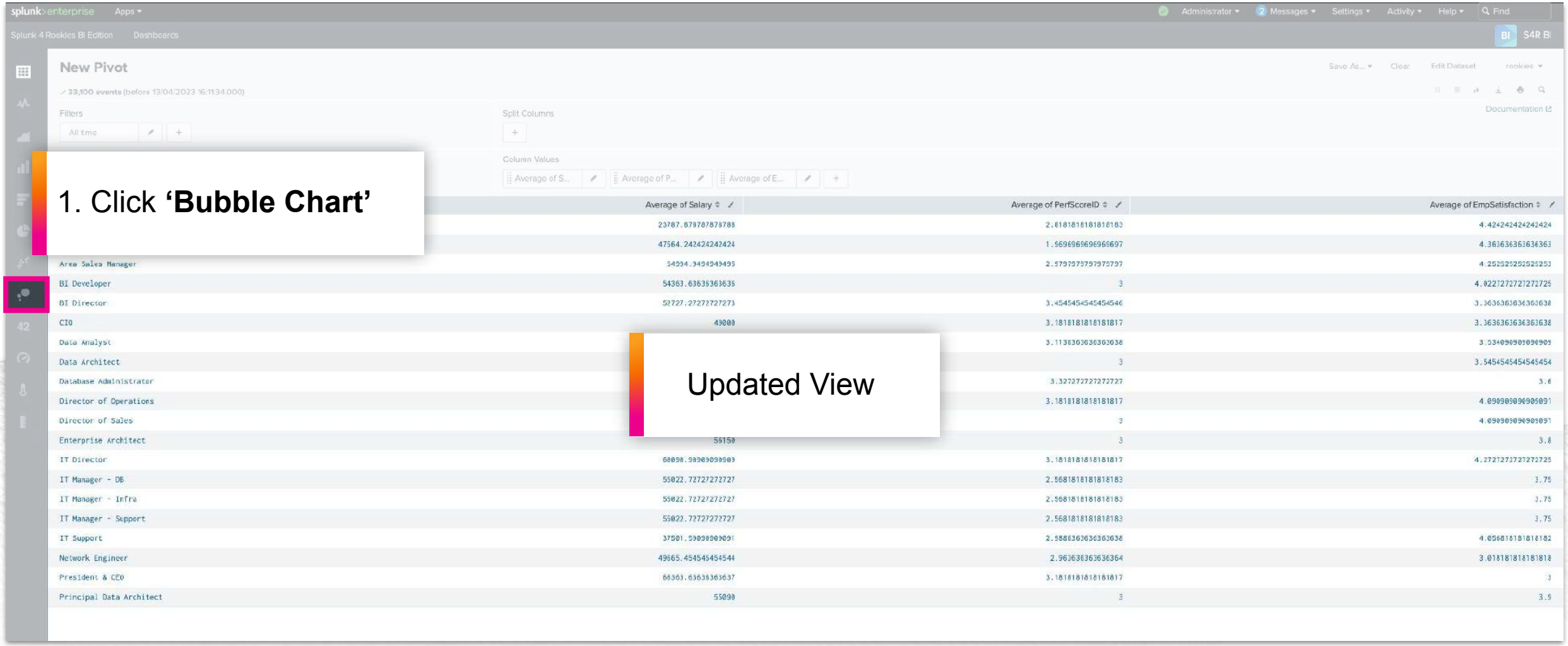


1. Click on the edit icon for **'Count of rookies'**

2. Click **'Remove'**

splunk>

Create Visualisation



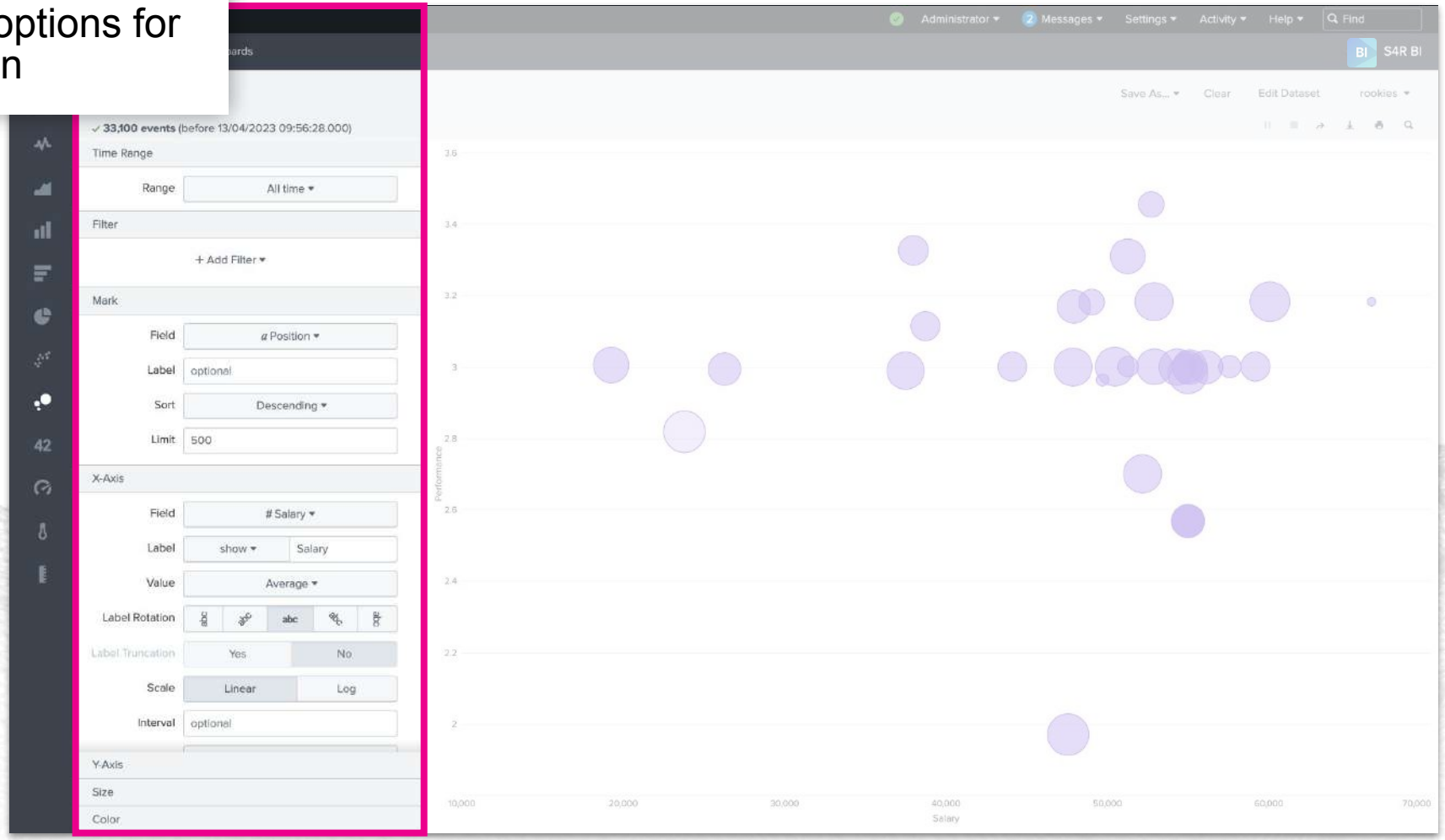
1. Click **‘Bubble Chart’**

Updated View

splunk>

Customise Visualisation

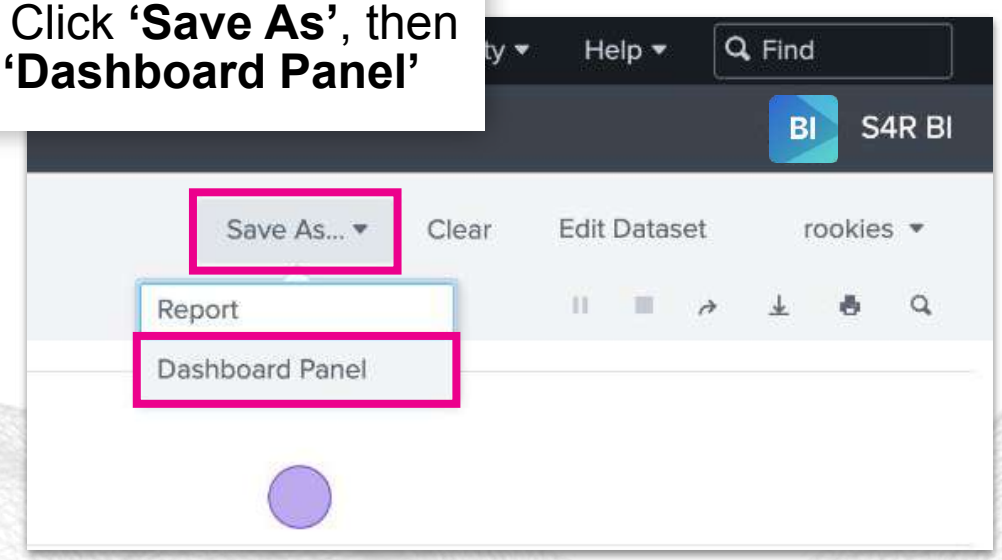
Explore the options for customisation



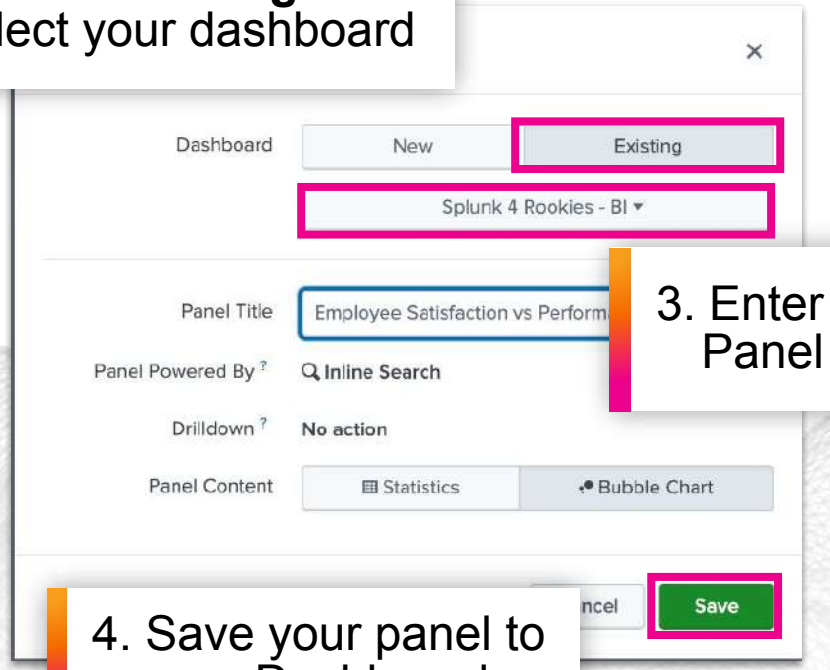
splunk>

Save Visualisation

1. Click **'Save As'**, then **'Dashboard Panel'**



2. Select **'Existing'** and select your dashboard

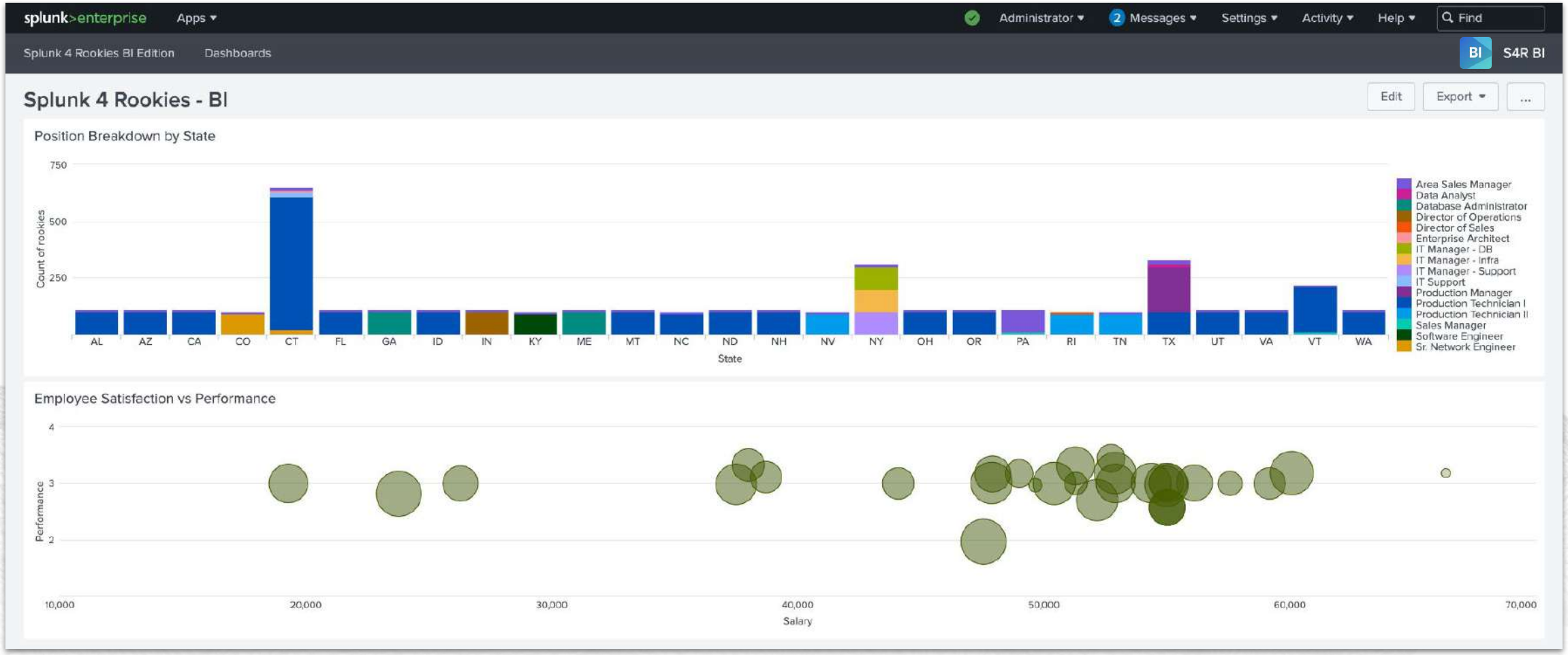


3. Enter a suitable Panel Title

4. Save your panel to **your** Dashboard

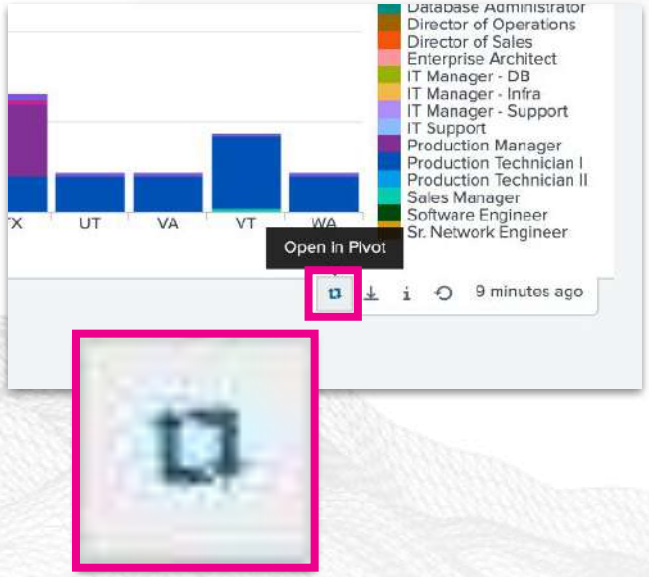
splunk>

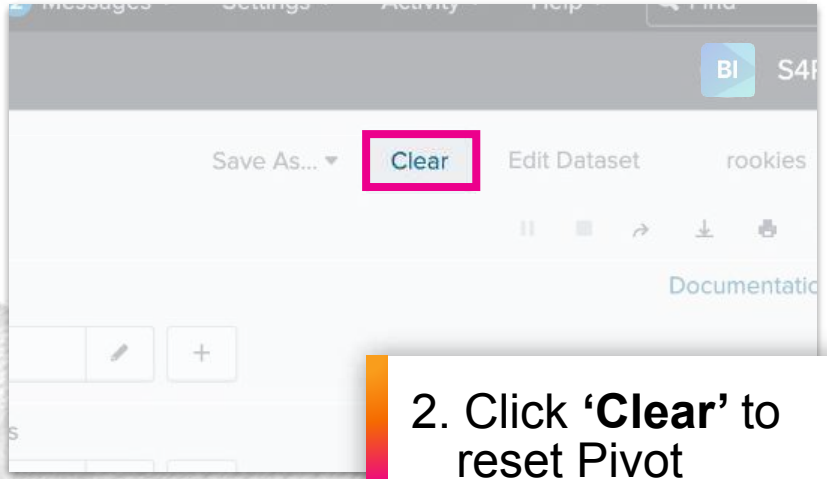
Updated Dashboard



Return to Pivot

1. Hover over the bottom right of the chart and click the Pivot icon





2. Click **'Clear'** to reset Pivot

splunk>

How many employees per state by role

Tasks

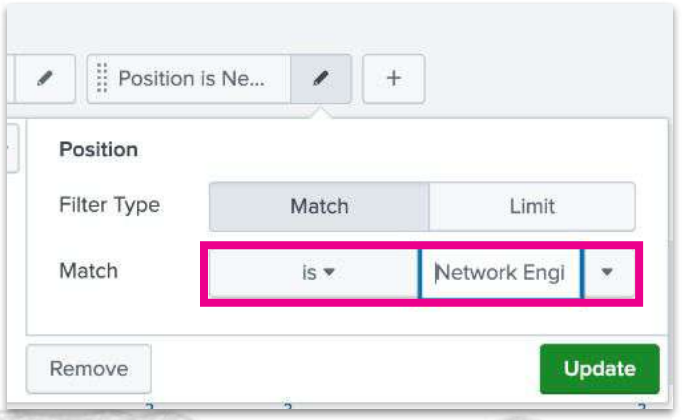
1. Deep dive into the identified groups from the previous Lab
2. Compare the employee satisfaction over time
3. Look for any outliers in the their historic data

Goal

Take 10 minutes to explore the data and attempt to create the required visual

Create Visualisation

1. Click **'Add Filter'**, then select **'Position'**

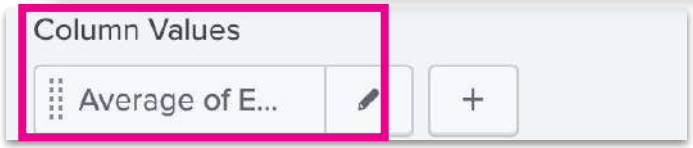


2. Select **'is'** as the match type and enter **'Network Engineer'**

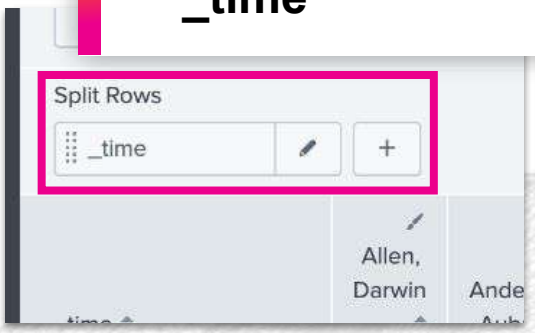
splunk>

Create Visualisation

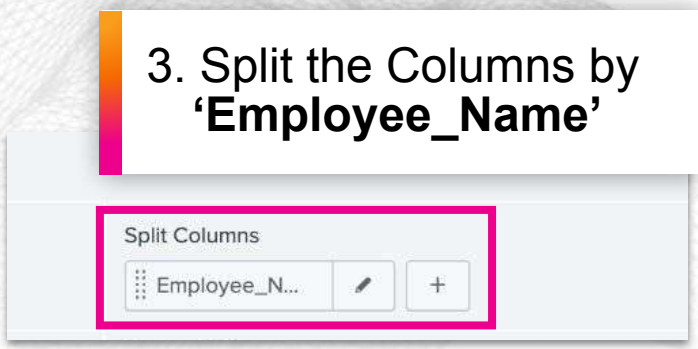
1. Add **'Column Values'** and select **'EmpSatisfaction' & 'Average'**



2. Split the Rows by **'_time'**

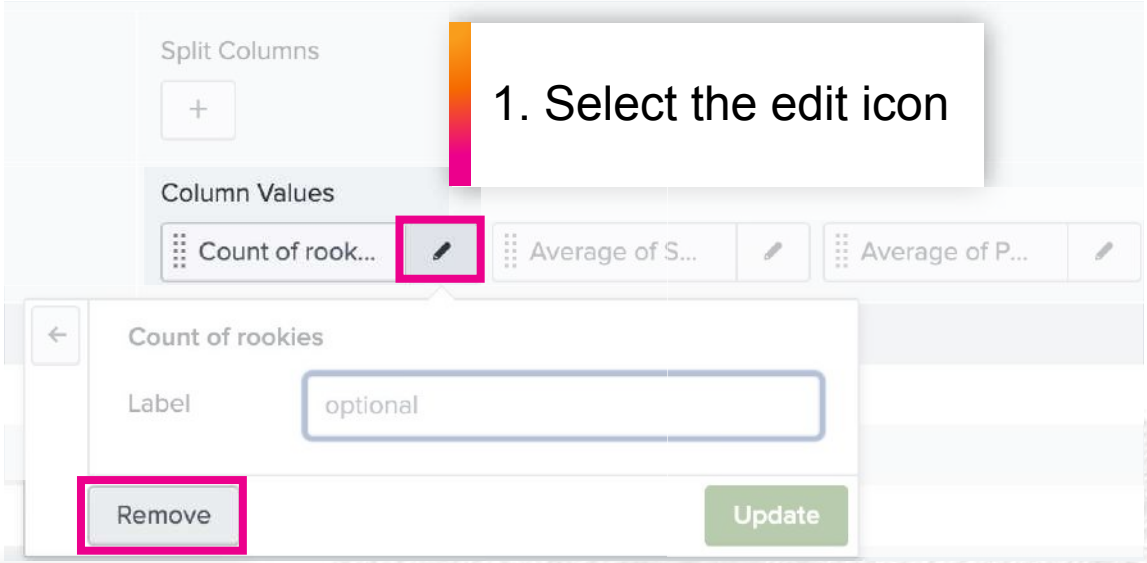


3. Split the Columns by **'Employee_Name'**



splunk>

Create Visualisation



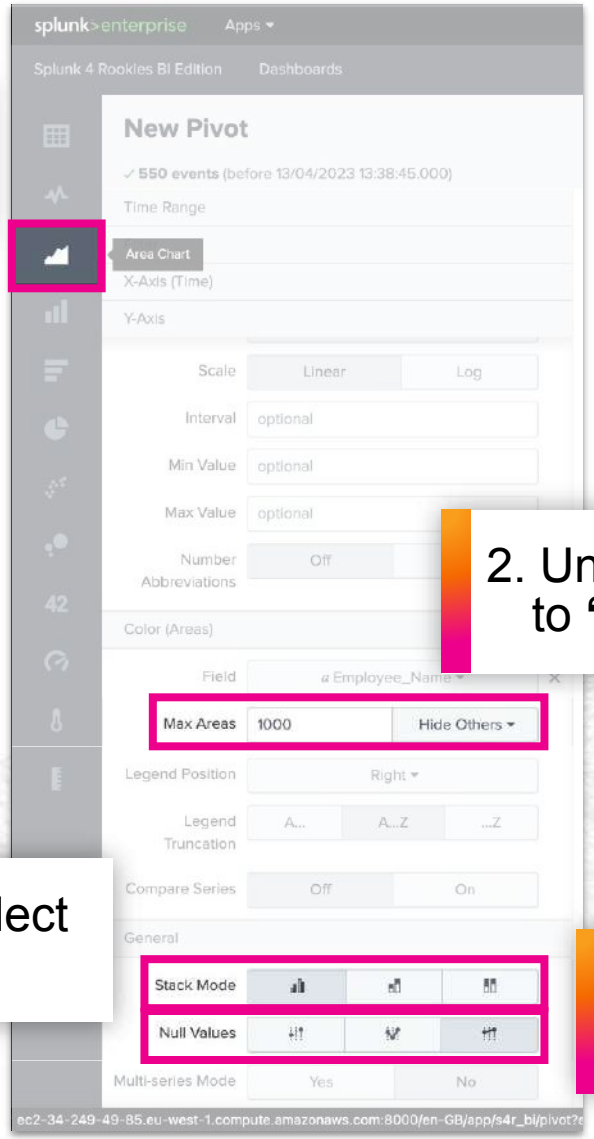
1. Select the edit icon

2. Click **'Remove'**

splunk>

Customise Visualisation

1. Select **'Area Chart'**



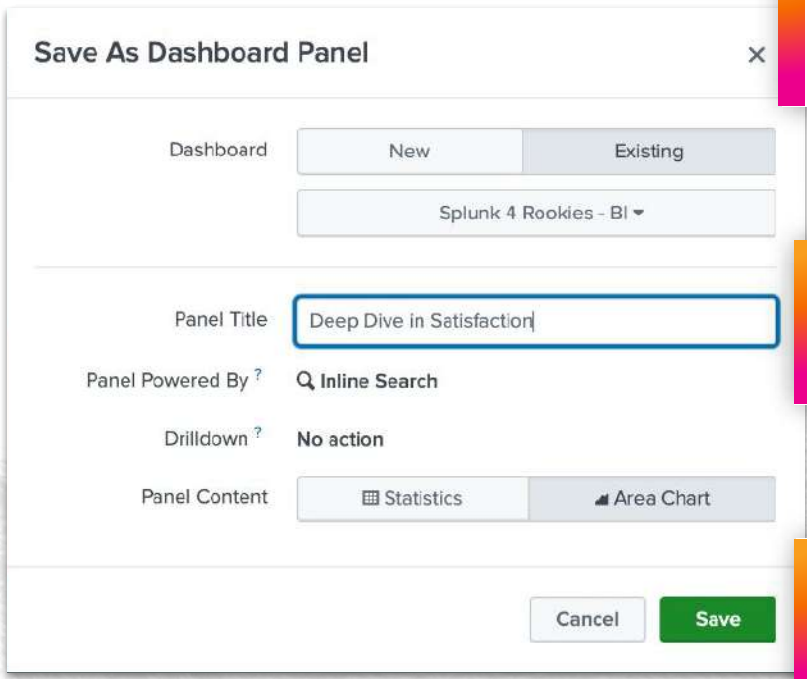
2. Under **'Color'** change **'Max Areas'** to **'Hide Others'** and enter **'1000'**

3. Under **'General'**, Select **'Not Stacked'**

4. Under **'General'**, Select **'Connect'** for null values

splunk>

Save Visualisation



1. Select ‘Existing Dashboard’

2. Enter a meaningful Panel Title

3. Click **‘Save’** and then view the Dashboard

splunk>

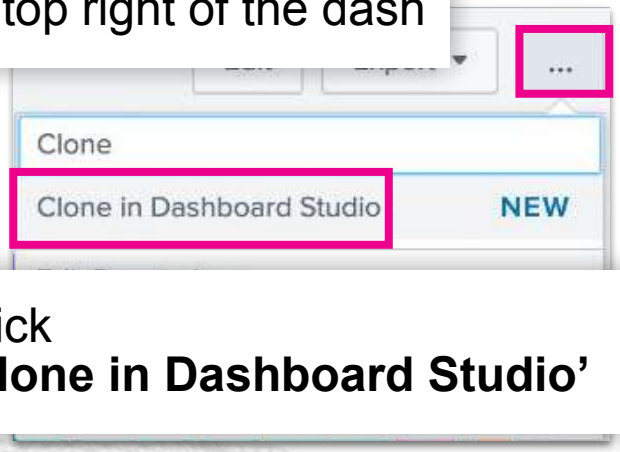
Create Powerful Story-telling Dashboards with Dashboard Studio

- Advanced visualisation tools
- Streamlined editing experience and fully customisable formats
- Flexible layouts (absolute and grid)
- Support for images, text boxes, shapes, lines and icons
- In-tact PDF export
- Support for custom SVG
- Support for dashboard level defaults

splunk>

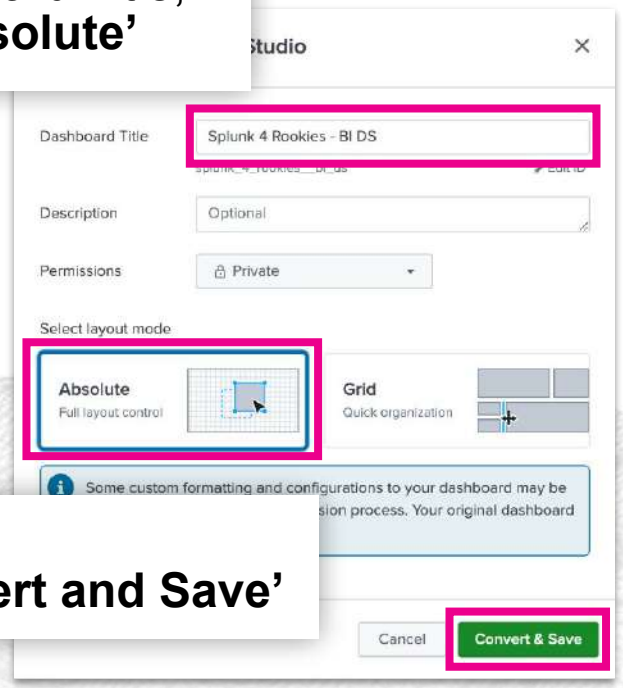
Convert to Dashboard Studio

1. Click the '**...**' on the top right of the dash



2. Click **'Clone in Dashboard Studio'**

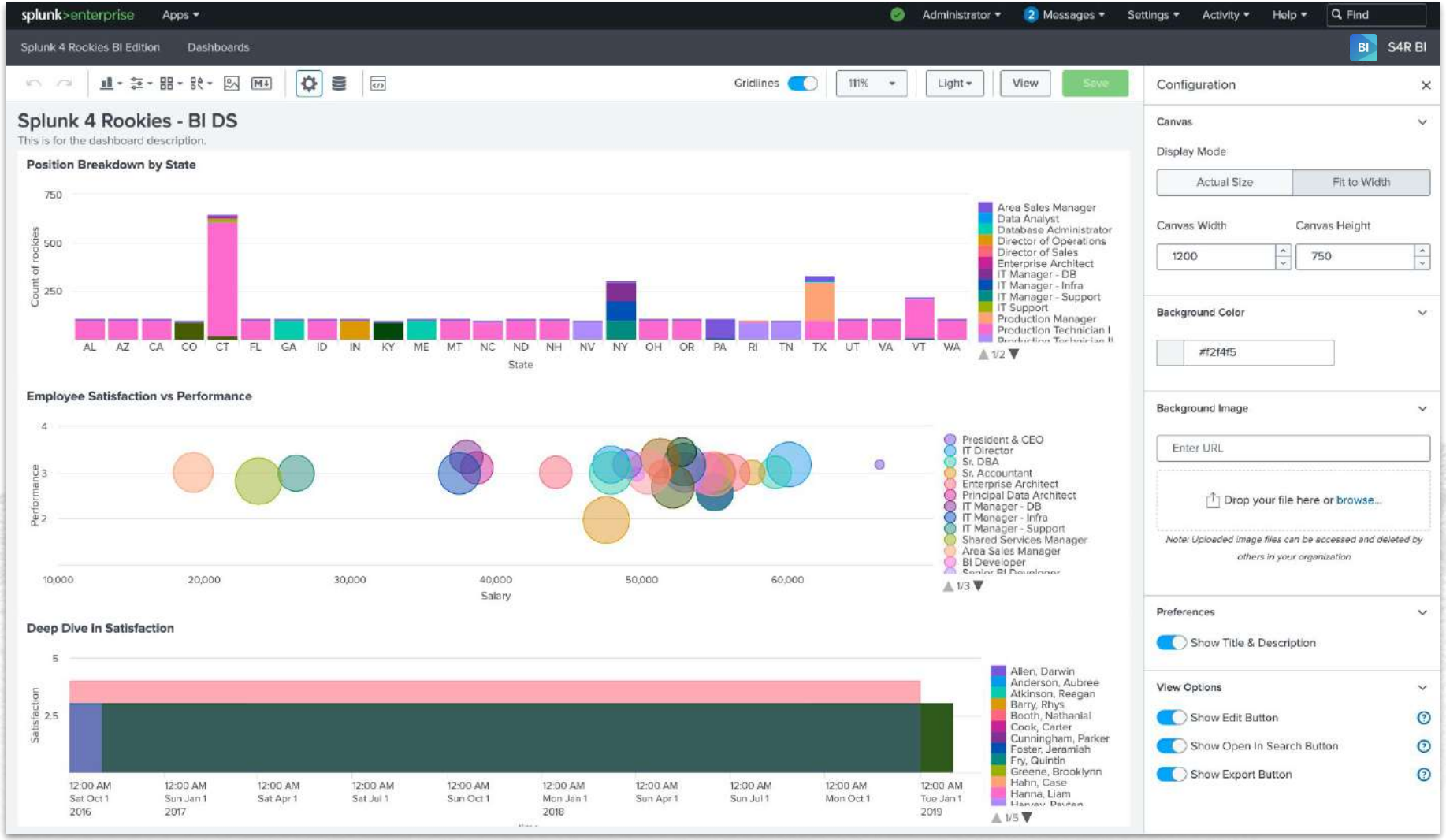
3. Enter a Dashboard Title, then select '**Absolute**'



4. Click **'Convert and Save'**

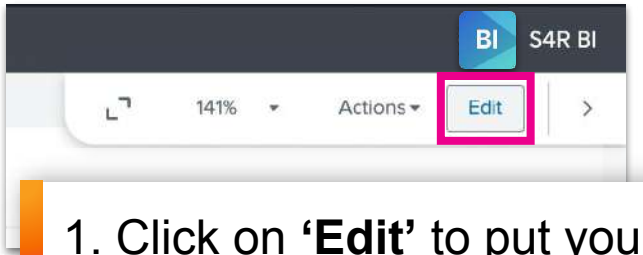
splunk>

Explore Your Dashboard

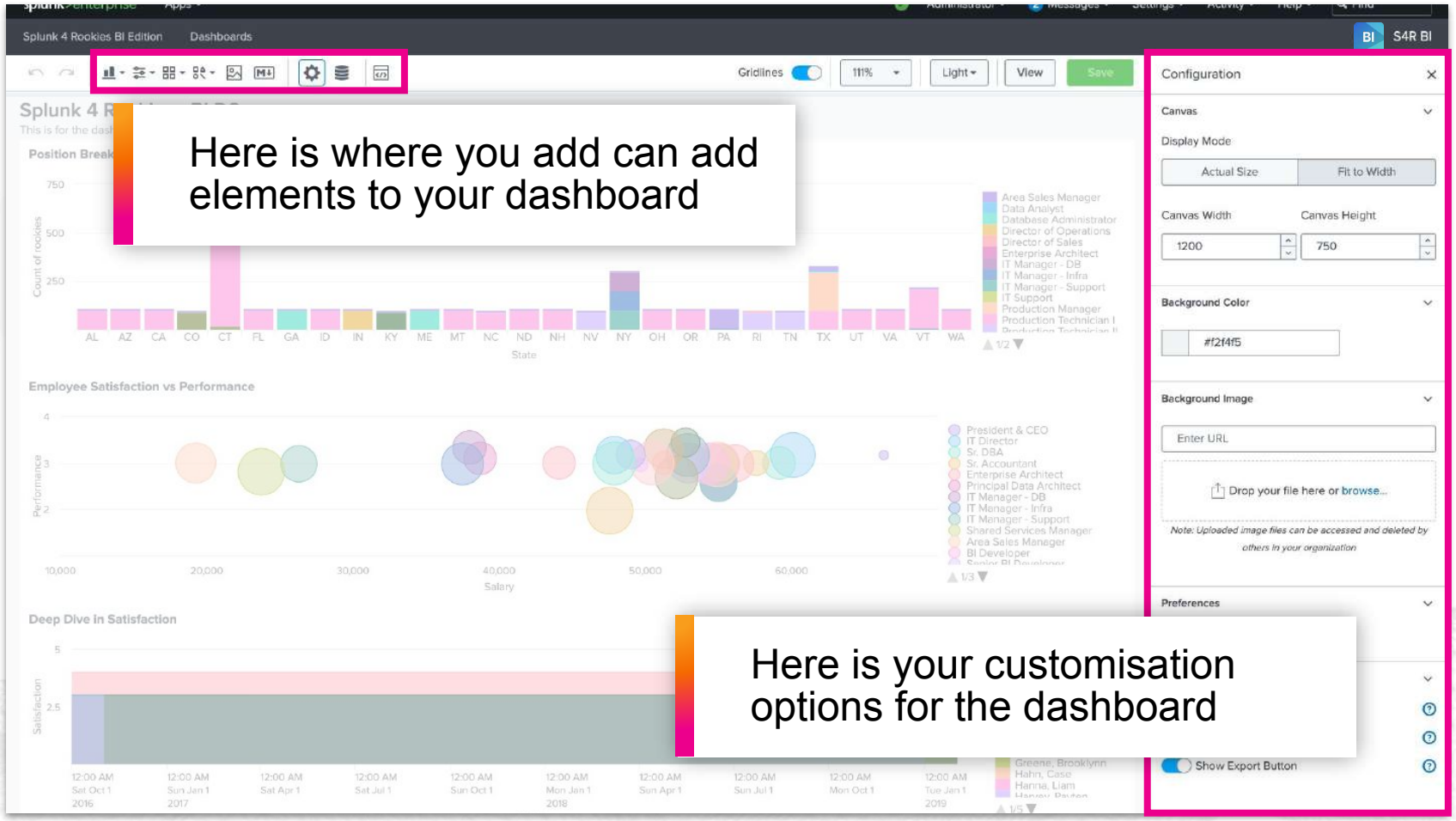


splunk>

Customise Your Dashboard



1. Click on **'Edit'** to put your dashboard into edit mode



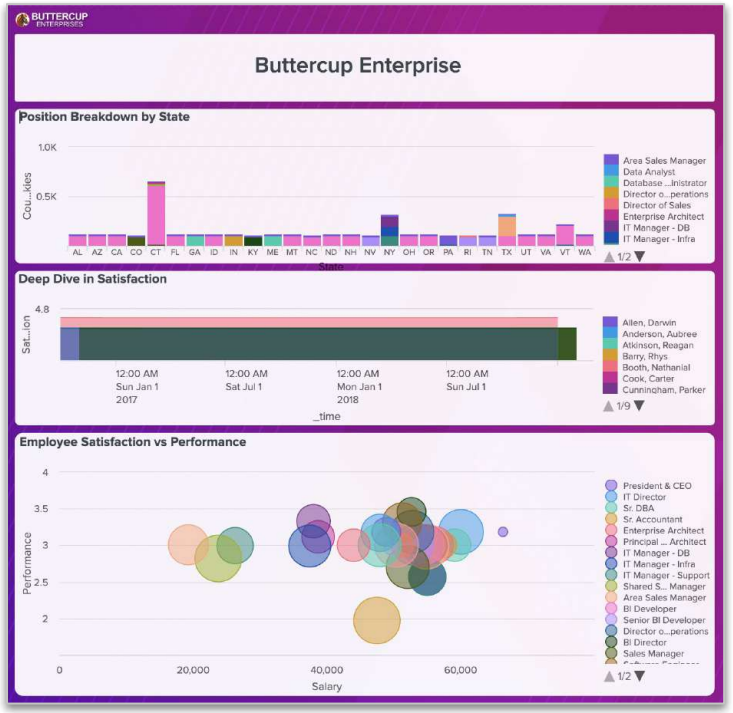
splunk>

Customise Your Dashboard!

Tasks

1. Add a custom background image provided by the Buttercup Enterprises Marketing team (https://splk.it/ButtercupBackground)
2. Resize your dashboard panels to fit within the boxes on the background image
3. Make the panels have transparent background colour

Goal

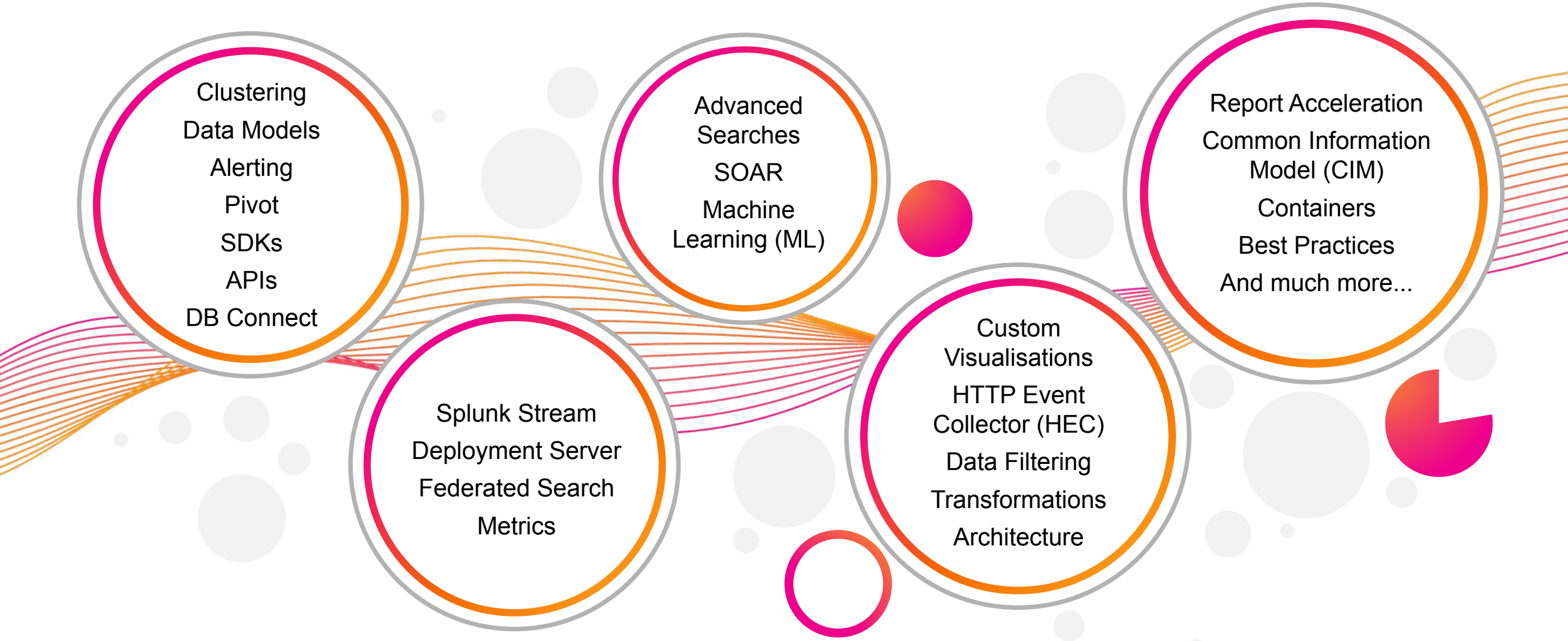


splunk>

You Finished the Hands-on Exercises!

You made it!

There's a Lot More to Splunk



Visit https://splunk.com/training to learn more!

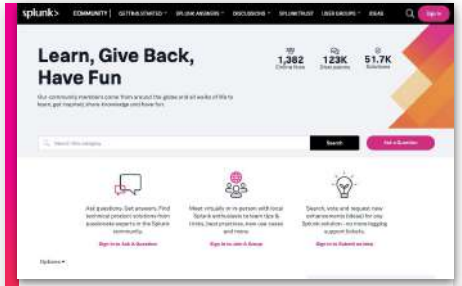
splunk>

Splunk Resources

Where to go after today's workshop

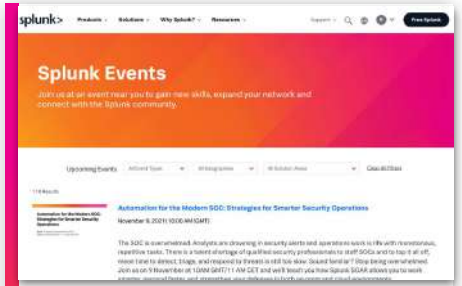
splunk>

Our World-Class Community is Here to Help



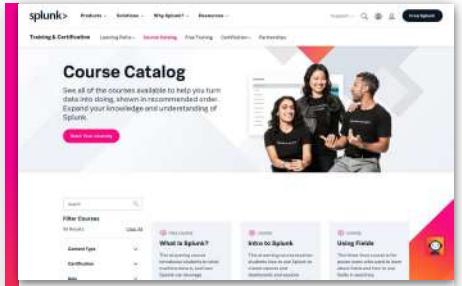
Splunk Community

230K members globally that have answered 125K+ product questions with 150+ user groups worldwide



Splunk Events

The one stop place for all Splunk events, from .conf to local hands on sessions. You can get locations, dates and times

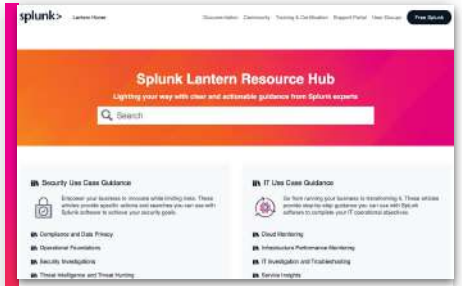


Customer Success and Education

The customer success organization are there to support your journey and success. They can also advise on training both through training.splunk.com but also local workshops

Splunkbase

Explore 2500+ applications and add-ons that simplify getting data in, visualizations, reports and more!



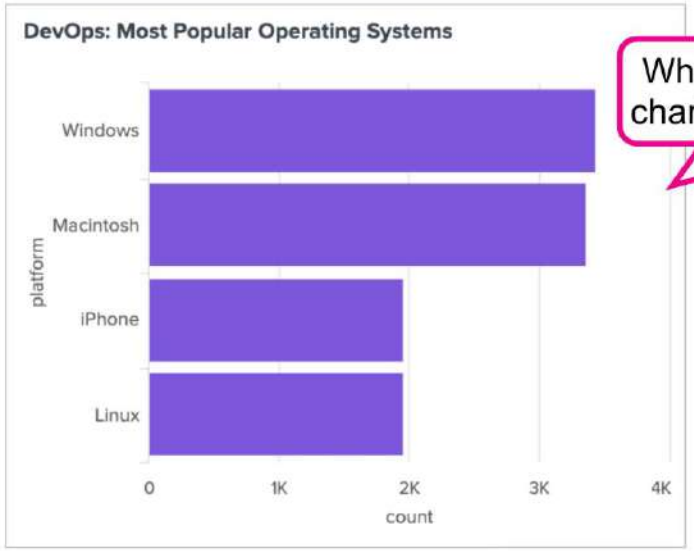
Splunk Lantern

Think of Lantern as your helper. The site provides not just advise on topics like deployments and use cases. It also provides links to applications, visuals, white papers and more

Splunk 4 Rookies - SPL Flavour

Solution:

```
> sourcetype=access_combined | top limit=20 platform showperc=f
```



When you're happy with your chart add it to your dashboard!

splunk>

Thank You!