

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.

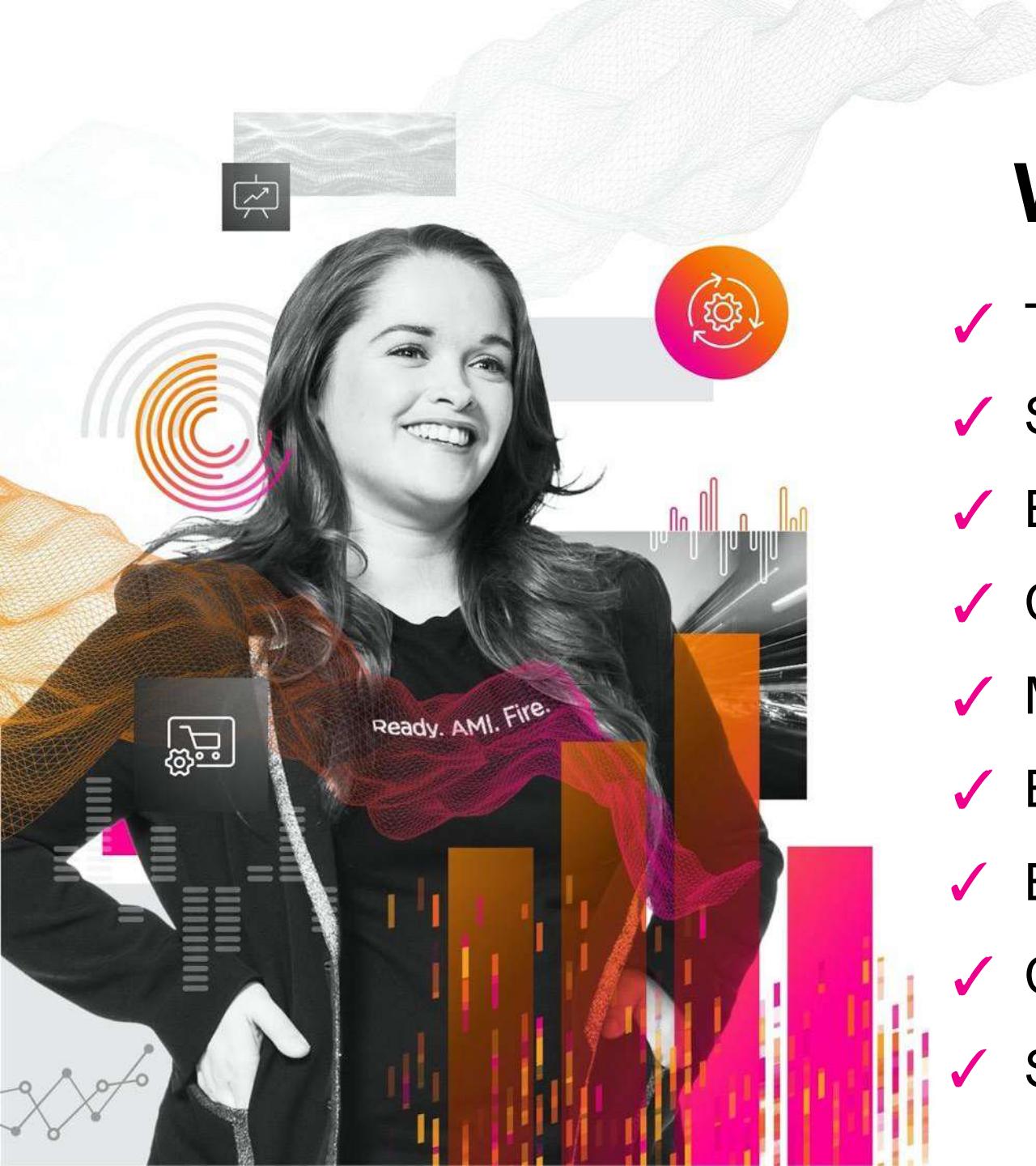
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features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

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

Please introduce yourself!

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





Workshop Agenda

- ✓ 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



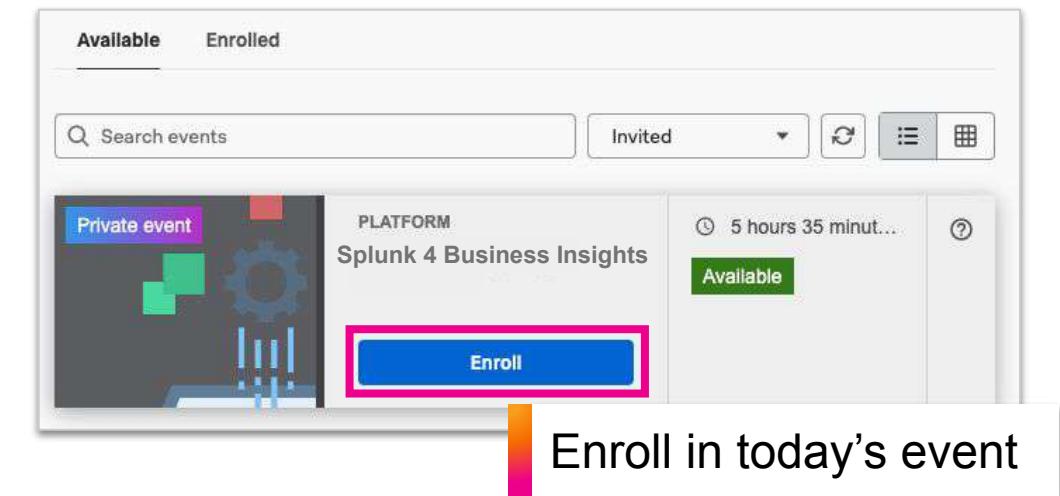


Enroll in Today's Workshop

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



The screenshot shows a web-based event management interface. At the top, there are tabs for 'Available' and 'Enrolled', with 'Available' being the active tab. Below the tabs is a search bar labeled 'Search events' and a dropdown menu set to 'Invited'. To the right of the search bar are several icons: a magnifying glass, a refresh symbol, and three small squares. The main area displays a list of events. The first event in the list is titled 'Private event' and features a dark background with a green gear icon. To the right of the title, it says 'PLATFORM Splunk 4 Business Insights', '5 hours 35 minut...', and 'Available'. A large blue button with the word 'Enroll' is centered below the event details. A callout bubble with a pink-to-yellow gradient points to this 'Enroll' button with the text 'Enroll in today's event'.

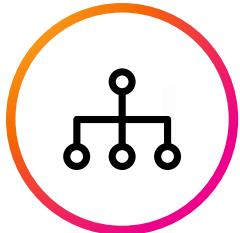


Digital Runs the Business

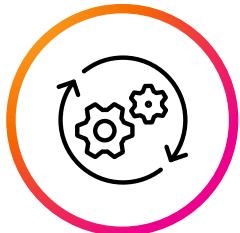
Your systems need to be secure and reliable



Today, It's Hard to be Resilient



Complex
Environments



Siloed tools
and teams



Evolving compliance
and regulations

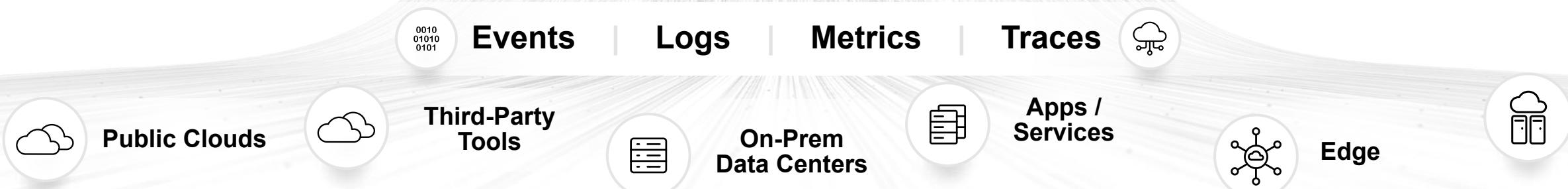
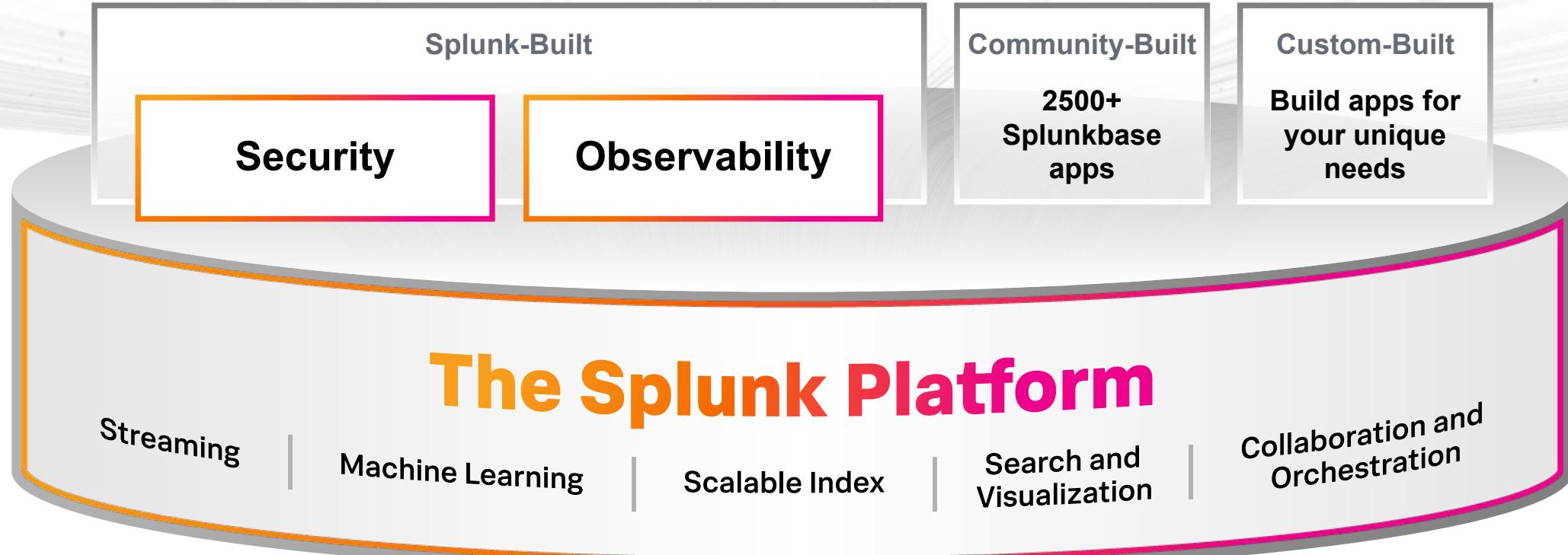


Service Disruptions Often Look the Same

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



Introducing Splunk

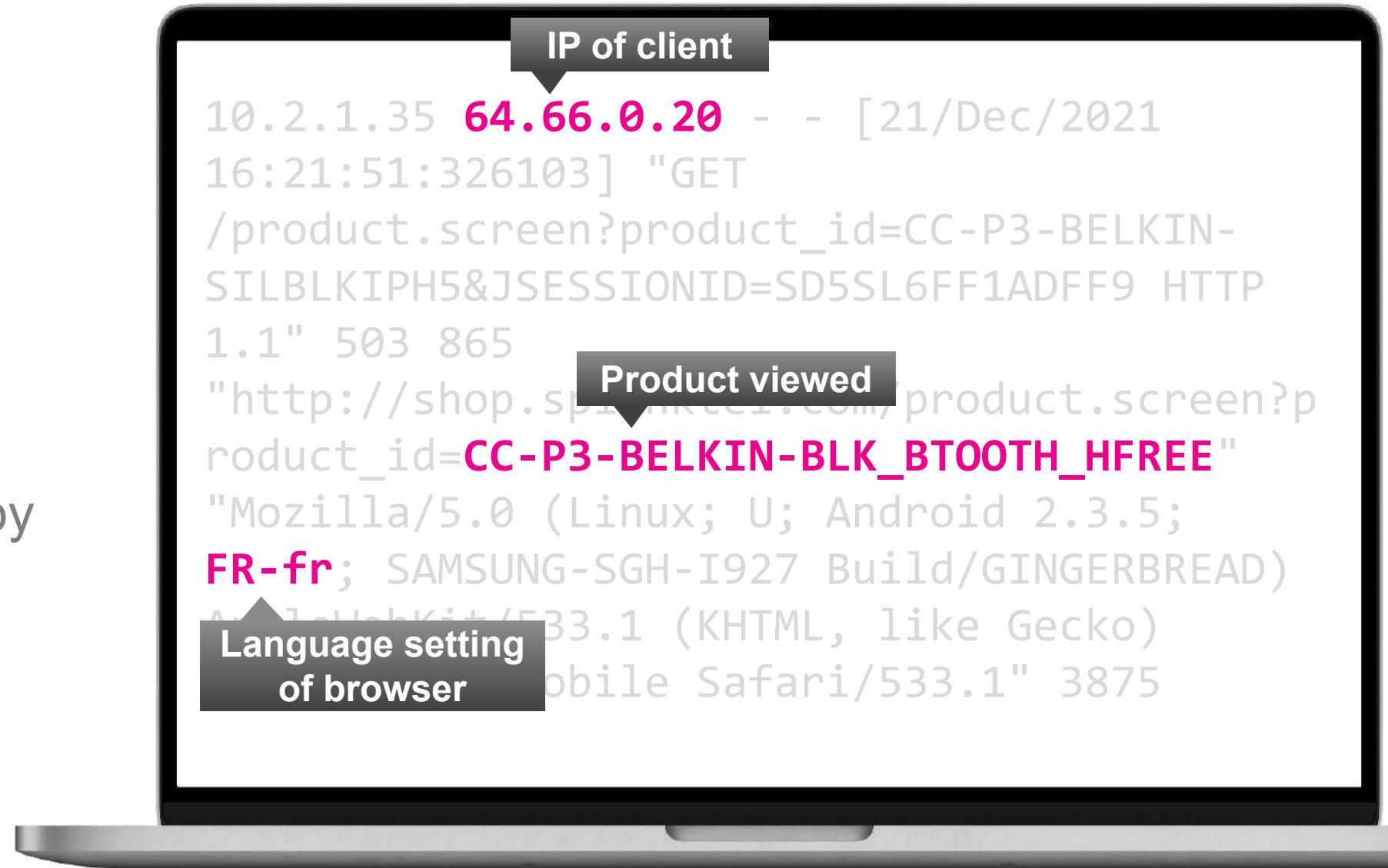


**Machine data
is valuable
not complex!**

```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BT0OTH_HFREE"  
"Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

Marketing Use Case

Show the top products viewed by language



DevOps Use Case

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

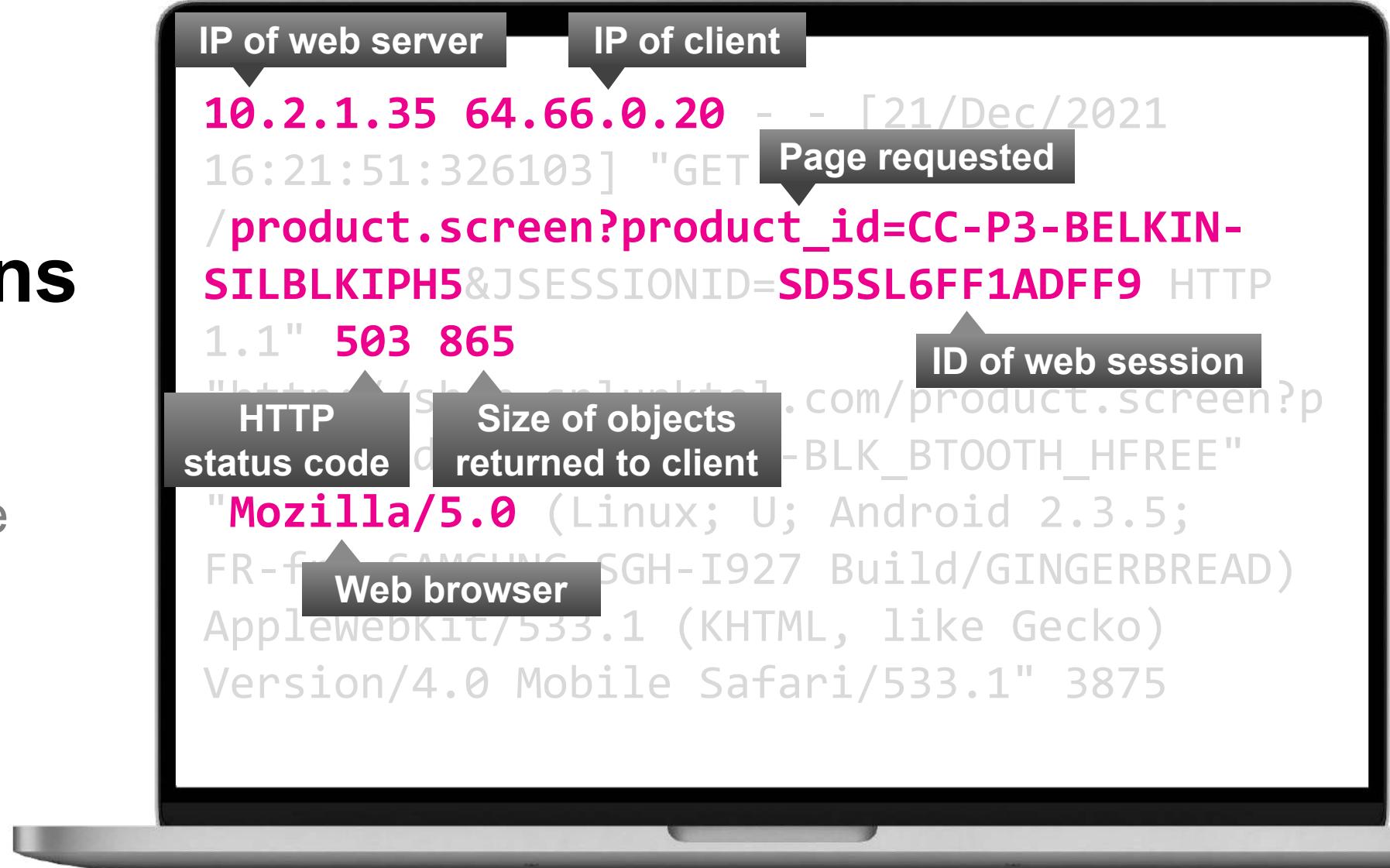
```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BRIGHT_FREE"  
Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

Platform

Handset model

IT Operations Use Case

Which web pages
are generating the
most errors?



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**



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

The screenshot shows a Mac desktop interface with a file browser window titled "workshop_data" and an open Microsoft Excel spreadsheet titled "hr_current".

File Browser (Left):

- Favourites: AirDrop, Recents, Applications, Documents, Downloads, iCloud, iCloud Drive, Shared.
- Tags: Orange, Red, Yellow, Green, Blue.

Excel Spreadsheet (Right):

File: hr_current

Sheet: hr_current

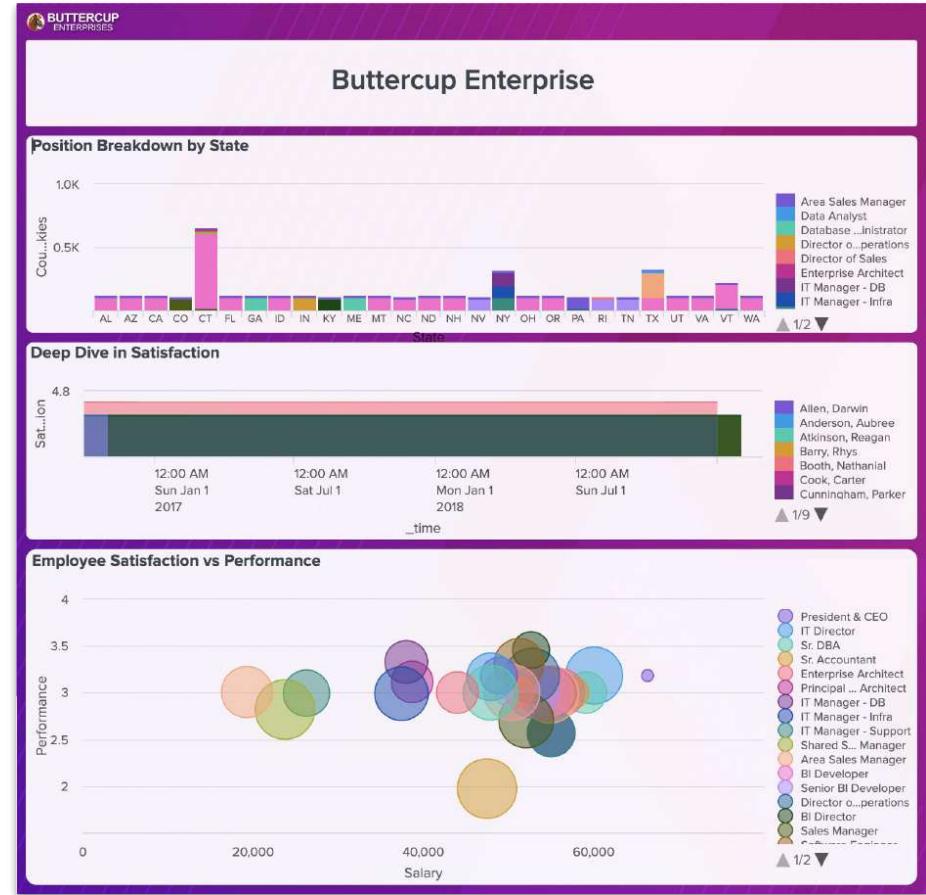
Cells A1 to U38:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U		
Employee_ID	Name	Age	Salary_k	Position	Salary	DateB	Dept	Gender	MaritalStatus	CitizenUS	Resident	DateHired	DeptEntered	TermExceeded	EmploymentType	Department	Manager	Recruitment	PerfScored	Performance	EmpStatus	SpecialProject
1	Gonzalez, Maria	45	50.2	Analyst	50200	08/04/1981	F	Female	Separated	US Citizen	White	05/01/2015	N/A - still in Active	IT/IS	Peter Monroe	Employee Re	3 Fully Meets	4	5	26		
2	Gonzalez, Maria	45	50.2	Analyst	50200	08/04/1981	F	Female	Separated	US Citizen	White	08/07/2013	N/A - still in Active	Production	David Stanek	Employee Re	3 Fully Meets	5	0	14		
3	Carter, Jamie	45	50.2	Analyst	50200	08/04/1981	F	Female	Single	US Citizen	White	08/07/2013	N/A - still in Active	Production	John Smith	Social Netw	3 Fully Meets	5	0	14		
4	Brown, Robert	45	50.2	Analyst	50200	08/04/1981	M	Male	Married	US Citizen	Black or Afric	05/01/2011	02/08/2014	Another pos Voluntarily T/Sales	David Stanek	Employee Re	3 Fully Meets	5	0	14		
5	Smith, John	45	50.2	Analyst	50200	08/04/1981	M	Male	Married	US Citizen	White	05/01/2015	N/A - still in Active	Production	Lynn Denaeza	Billboard	3 Fully Meets	5	0	14		
6	Isaac, Henry	45	50.2	Analyst	50200	08/04/1981	M	Male	Divorced	US Citizen	White	06/09/2013	N/A - still in Active	Production	Karen Sullivan	Employee Re	3 Fully Meets	5	0	14		
7	Kordan, Merv	45	50.2	Analyst	50200	08/04/1981	M	Male	Separated	US Citizen	White	05/01/2006	N/A - still in Active	Sales	Lynn Denaeza	Billboard	4 Exceeds	3	0	04		
8	Ferguson, Sue	45	50.2	Analyst	50200	08/04/1981	F	Female	Married	US Citizen	White	07/11/2001	17/05/2014	military	Voluntarily T Production	Webster Bill Search Engin	3 Fully Meets	3	0	14		
9	Albert, Michael	45	50.2	Analyst	50200	08/04/1981	M	Male	Divorced	US Citizen	White	01/08/2015	N/A - still in Active	Production	Janet King	Employee Re	3 Fully Meets	3	0	27		
10	Gentry, Mindy	45	50.2	Analyst	50200	08/04/1981	F	Female	Married	US Citizen	Black or Afric	08/03/2004	N/A - still in Active	Production	Michael Atley	Professional	3 Fully Meets	3	0	16		
11	Wade, Karen	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	White	01/08/2015	N/A - still in Active	Production	John Smith	Social Netw	3 Fully Meets	5	0	14		
12	Diamond, Karen	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	White	07/07/2014	N/A - still in Active	Production	David Stanek	Employee Re	3 Fully Meets	5	0	14		
13	Diamond, Karen	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	White	07/07/2014	N/A - still in Active	Production	Eric Douglas	Vendor Re	3 Fully Meets	4	0	04		
14	Giles, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Single	US Citizen	White	01/05/2019	N/A - still in Active	Production	Karen Sullivan	Employee Re	3 Fully Meets	3	0	24		
15	Smith, Steve	45	50.2	Analyst	50200	08/04/1981	M	Male	Single	US Citizen	White	11/12/2013	N/A - still in Active	Production	Rossy Sullivan	Classroo	3 Fully Meets	5	0	14		
16	Roberts, Robert	45	50.2	Analyst	50200	08/04/1981	M	Male	Married	US Citizen	White	05/07/2011	08/01/2013	Another pos Voluntarily T Production	John Smith	Website Bar	2 Fully Meets	4	0	14		
17	Albert, Michael	45	50.2	Analyst	50200	08/04/1981	M	Male	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Sales	John Smith	Website Bar	2 Fully Meets	3	0	14		
18	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
19	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
20	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
21	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
22	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
23	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
24	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
25	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
26	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
27	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
28	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
29	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
30	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
31	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
32	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
33	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
34	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
35	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
36	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
37	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
38	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
39	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
40	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
41	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
42	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
43	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
44	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
45	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
46	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
47	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
48	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
49	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
50	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
51	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
52	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
53	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
54	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
55	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
56	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
57	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
58	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets	3	0	14		
59	Robertson, Linda	45	50.2	Analyst	50200	08/04/1981	F	Female	Divorced	US Citizen	Black or Afric	16/08/2013	N/A - still in Active	Production	Rebecca Lee	Blind	2 Fully Meets					

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





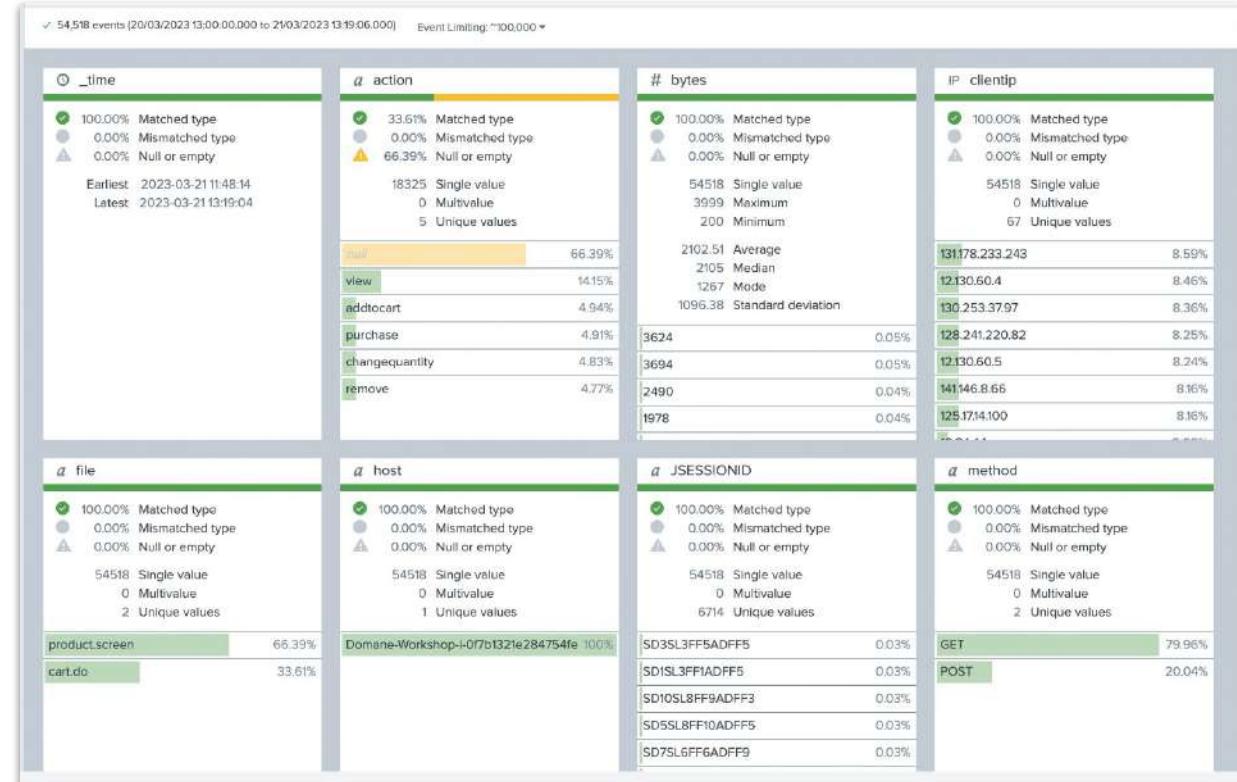
Module 1

Data preparation with
Tables

splunk>

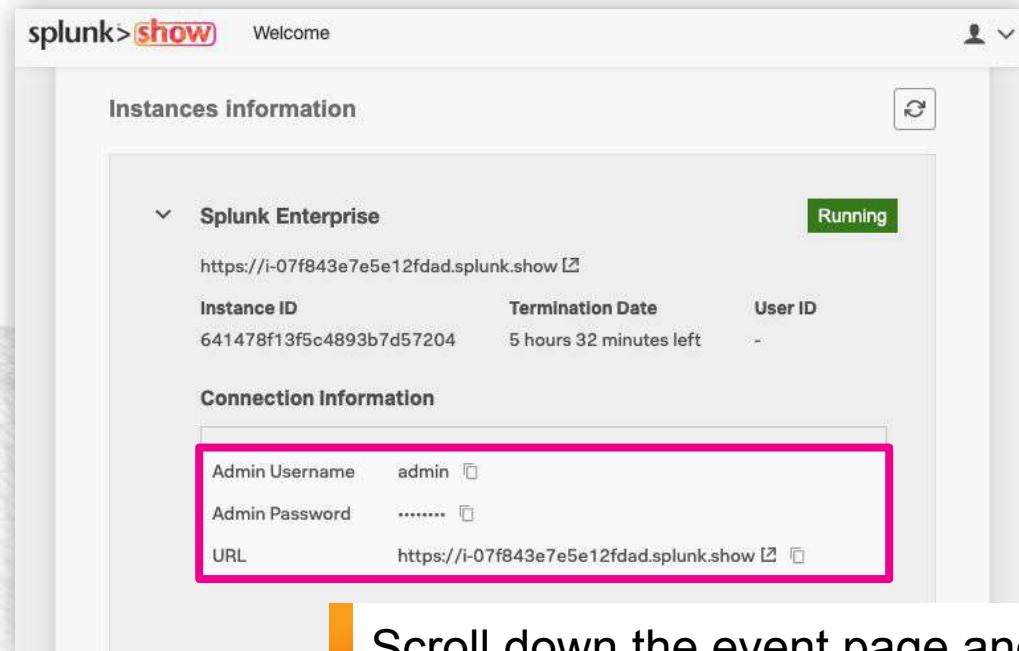
What are Datasets and Tables?

- > 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!



Login to Splunk

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



The screenshot shows the Splunk Show event page with the title "splunk>show". Under "Instances information", there is a section for "Splunk Enterprise" which is "Running". It displays the URL <https://i-07f843e7e5e12fdad.splunk.show>, Instance ID 641478f13f5c4893b7d57204, Termination Date 5 hours 32 minutes left, and User ID -. Below this, under "Connection Information", are fields for Admin Username (admin), Admin Password (redacted), and URL <https://i-07f843e7e5e12fdad.splunk.show>. The URL field is highlighted with a pink border.

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

Log in to your Splunk instance



The screenshot shows the Splunk instance login screen with the title "splunk>enterprise". It features a "Username" field, a "Password" field, and a "Sign In" button. The background is filled with log entries from the Splunk instance.

Login using the credentials
from Splunk Show



Navigate to your Module

The screenshot shows a web-based application interface for 'Splunk 4 Rookies BI Edition'. At the top, there is a navigation bar with links for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header, there are buttons for 'Edit', 'Export', and three dots. Below the header, the title 'Splunk 4 Rookies BI Edition' is displayed, followed by a section titled 'Workshop Options'. This section contains a brief description and two options:

- Module 1 - In this part of the workshop, we will create a table dataset from scratch, etc.
- Module 2 - In this part of the workshop, we work through the table dataset created

Two circular icons represent the modules: 'Module 1' on the left with a blue border and a notepad icon, and 'Module 2' on the right with a purple border and a bar chart icon. A callout box with a pink border and white background points to the 'Module 1' icon, containing the instruction '1. Click on 'Module 1''. The background of the page features a faint, abstract wavy pattern.



Selecting the data for your analysis

1. Click on 'main'

2. Click on 'csv-hr'

Select the required fields

Tasks:

1. Select the fields to be used in our analysis

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

1. Select the above fields to include in our dataset

Select existing fields

Filter existing fields Search icon

+ Add a missing existing field

all fields
 `_time`
 > `_raw`
 `a CitizenDesc`
 # `date_mday`
 `a date_month`
 `a date_wday`
 # `date_year`
 `a zone`

 `a EmplID`
 `a Employee_Na`
 `a EmploymentSta`
 `# EmpSatisfactor`
 `a host`
 `a index`
 # `linecount`
 `a ManagerName`
 `a MaritalDesc`
 `a PerformanceScore`
 # `PerfScoreID`
 # `PositionID`

2. Click on 'Start Editing'

Start Editing

Let's explore the Interface

The currently selected app

Action bar - Interact with the dataset

#	○ _time	α CitizenDesc	α DateofHire	α DateofTermination	α Department	α DOB	α EmpID	α Employee
1	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9077860158	Murray, Dayan
2	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	17/05/2014	Production	01/12/1974	k9075930274	Bauer, Kyleigh
3	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9074670478	Clark, Justice
4	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	11/01/2014	Production	01/12/1974	k9005930584	Riggs, Gavyn
5	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9066300788	Stevens, Team
6	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	24/06/2013	Production	01/12/1974	k9040630894	Blair, Kaitlyn
7	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9054241098	Hull, Lillian
8	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	08/02/2016	Production	01/12/1974	k9001261284	Chase, Chain
9	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9018531408	Jimenez, Bruna
10	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9053411514	Vega, Amya
11	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9084531718	Hawkins, Mekhi
12	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9084531718	In, Sarah
13	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9084531718	Marcos, Br
14	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9084531718	Catalina
15	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9013822444	Fleming, Daniel
16	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9038172648	Gamble, Ameli
17	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9038172648	Gamble, Ameli

View options

History of modifications

Event Data

Let's explore the Interface

The screenshot illustrates the Splunk interface with several open toolbars and a data table:

- Left Panel:** Shows a sidebar with navigation links: Edit, Move, Delete, Rename..., and categories for String, Number, Boolean, IPv4, and Epoch Time.
- Top Bar:** Includes the Splunk logo, user status (Administrator), and navigation links: Messages, Settings, Activity, Help, and a search bar labeled "Find".
- Open Toolbars:**
 - Sort:** Displays options for Sort Ascending and Sort Descending.
 - Filter:** Displays options for Filter by Value, Change Case, Fill Null or Empty Values, Replace Values, Round Values, Replace Type Mismatches With Null, Bucket, Eval Expression (with Advanced button), and Learn more.
 - Stats:** Displays options for Add a field to aggregate, Add row count, Split by (with action dropdown), Add a split by field, and Learn more.
 - Add New:** Displays options for Calculate Field, Extract Selected Text, Format Timestamp, Join from Lookup, Duplicate Field, Coalesce Fields, Concatenate Fields or Text, Map Ranges, Split Fields, Eval Expression (with Advanced button), and Extract with Regular Expression (with Advanced button).
- Data Table:** A table with columns: ID, Name, Citizenship, Birth Date, and Action. The table shows 17 rows of data, with the last few rows partially cut off.

ID	Name	Citizenship	Birth Date	Action
1	John Doe	US Citizen	24/06/2013	Production
2	Jane Smith	US Citizen	28/02/2012	Production
3	David Johnson	US Citizen	08/02/2016	Production
4	Sarah Williams	US Citizen	28/02/2012	Production
5	Michael Brown	US Citizen	13/05/2013	Production
6	Alexander Green	US Citizen	28/02/2012	Production
7	Emily Davis	US Citizen	28/02/2012	Production
8	Christopher White	US Citizen	13/05/2013	Production
9	Olivia Parker	US Citizen	28/02/2012	Production
10	Noah King	US Citizen	28/02/2012	Production
11	Leah Clark	US Citizen	28/02/2012	Production
12	Wyatt Hayes	US Citizen	13/05/2013	Production
13	Zoe Martinez	US Citizen	28/02/2012	Production
14	Lucas Wilson	US Citizen	13/05/2013	Production
15	Madison Parker	US Citizen	28/02/2012	Production
16	Wyatt Hayes	US Citizen	13/05/2013	Production
17	Zoe Martinez	US Citizen	28/02/2012	Production



Modify the data on the fly

Tasks:

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

The screenshot shows the Splunk Data View interface with a 'Rename Field' dialog open. The main view displays a table with columns: 'RecruitmentSource', 'ReviewDate', and 'Salary'. The 'Salary' column contains values like 'MA:2134' and 'MA:1810'. A context menu is open over the 'Salary' column, with the 'Edit' option highlighted. A callout bubble points to the 'Edit' option with the text '2. Click on 'Edit', then 'Rename''. The 'Rename Field' dialog has 'Field' set to 'Salary' and 'New name' set to 'Location'. A callout bubble points to the 'New name' input field with the text '3. Enter 'Location''. A large pink rectangle highlights the 'Salary' column in the main view and the 'New name' input field in the dialog.

1. Click the column name to select all

2. Click on 'Edit', then 'Rename'

3. Enter 'Location'

Create a New Field

Tasks:

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

The screenshot shows the Splunk interface for creating a new field. On the left, a context menu is open under 'Add New' with 'Split Fields...' highlighted. On the right, the 'Split Fields' configuration dialog is displayed, showing the 'Original field' set to 'Location' and the 'Custom delimiter' set to ':'. The 'New fields' section contains 'State' and 'Zip' fields. A green 'Apply' button is at the bottom right of the dialog.

1. Click the column name to select all

2. Click 'Add New', then 'Split Fields'

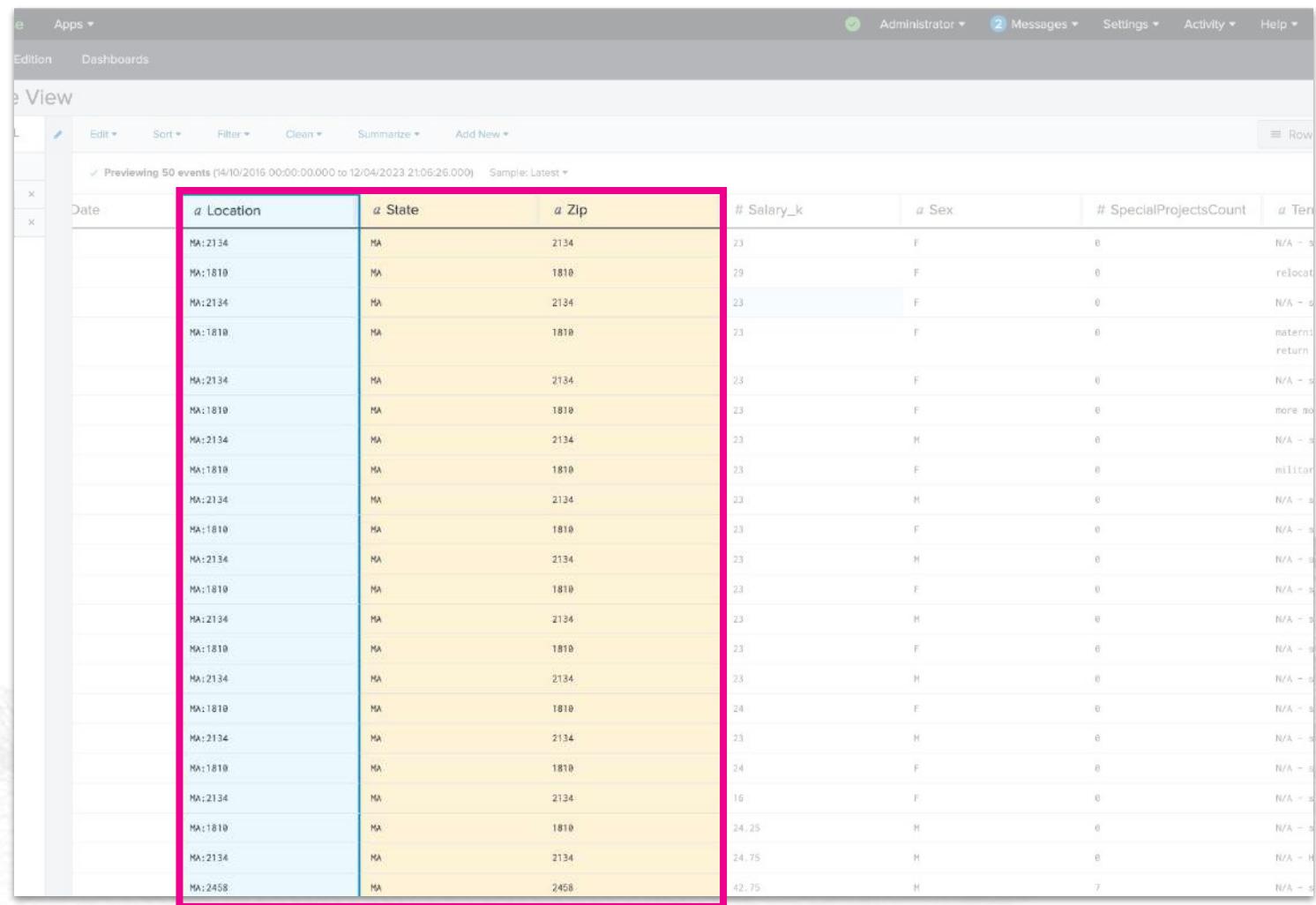
3. Complete the fields as per this image, then click 'Apply'

#	Location	# Salary_K
1	MA:2134	23
2	MA:1810	29
3	MA:2134	23
4	MA:1810	23
5	MA:2134	23
6	MA:1810	23
7	MA:2134	23
8	MA:1810	23

Create a New Field

Tasks:

1. Explore the new fields created on the fly



The screenshot shows a Splunk Data View window. At the top, there are navigation tabs for 'Edition' and 'Dashboards'. Below that is a toolbar with 'Edit', 'Sort', 'Filter', 'Clean', 'Summarize', and 'Add New' buttons. The main area is titled 'View' and shows a preview of 50 events from 10/2016 to 04/2023. The table has the following columns: Date, a Location, a State, a Zip, # Salary_k, a Sex, # SpecialProjectsCount, and a TerminationDate. The first three columns ('Date', 'a Location', and 'a State') are highlighted with a red border. The data in the table consists of many rows of event details, such as dates like '2016-10-10T00:00:00.000Z' and locations like 'MA:2134'.

Date	a Location	a State	a Zip	# Salary_k	a Sex	# SpecialProjectsCount	a TerminationDate
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	29	F	0	relocat
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	materni
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	more bo
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	militar
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	23	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	24	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	23	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	24	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	16	F	0	N/A - s
2016-10-10T00:00:00.000Z	MA:1810	MA	1810	24.25	H	0	N/A - s
2016-10-10T00:00:00.000Z	MA:2134	MA	2134	24.75	H	0	N/A - H
2016-10-10T00:00:00.000Z	MA:2458	MA	2458	42.75	H	7	N/A - s



What is a Lookup?

Fields extracted from events by Splunk:

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

External CSV file:

PositionID	Position
1	Accountant I
1	Administrative Assistant
1	Area Sales Manager
1	BI Developer
1	BI Director
1	CIO
1	Data Architect
1	Database Administrator
1	Data Analyst
1	Data Analyst
1	Director of Operations
1	Director of Sales
1	IT Director
1	IT Manager - DB
1	IT Manager - Support
1	IT Manager - Infra
1	IT Support
1	Network Engineer
1	President & CEO
1	Production Manager

This is the information we need!

Configuring the lookup

Tasks:

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

The screenshot shows the Splunk Data Model Editor interface. On the left, there is a search bar with '50 events (14/10/2016 00:00:00.000 to 14/10/2016 00:00:00.000)' and a dropdown menu with options like 'Sort', 'Filter', 'Clean', 'Summarize', and 'Add New'. The 'Add New' option is highlighted with a pink box. Below the search bar is a context menu with items: 'Calculate Field...', 'Extract Selected Text...', 'Format Timestamp...', 'Join from Lookup...', and 'Duplicate Field...'. The 'Join from Lookup...' option is also highlighted with a pink box. To the right of the interface is a table titled '# PositionID' with columns 'RaceDesc' and 'Recruitme'. The table contains 15 rows of data, showing various combinations of PositionID (19 or 20), RaceDesc (White, Glassdoor, or Monster.com), and Recruitment source (Newspaper/Magazine, Monster.com, Glassdoor). A large callout box with a pink-to-yellow gradient at the top contains the instructions: '1. Click 'PositionID' column header' and '2. Click 'Add New', then 'Join from Lookup''.

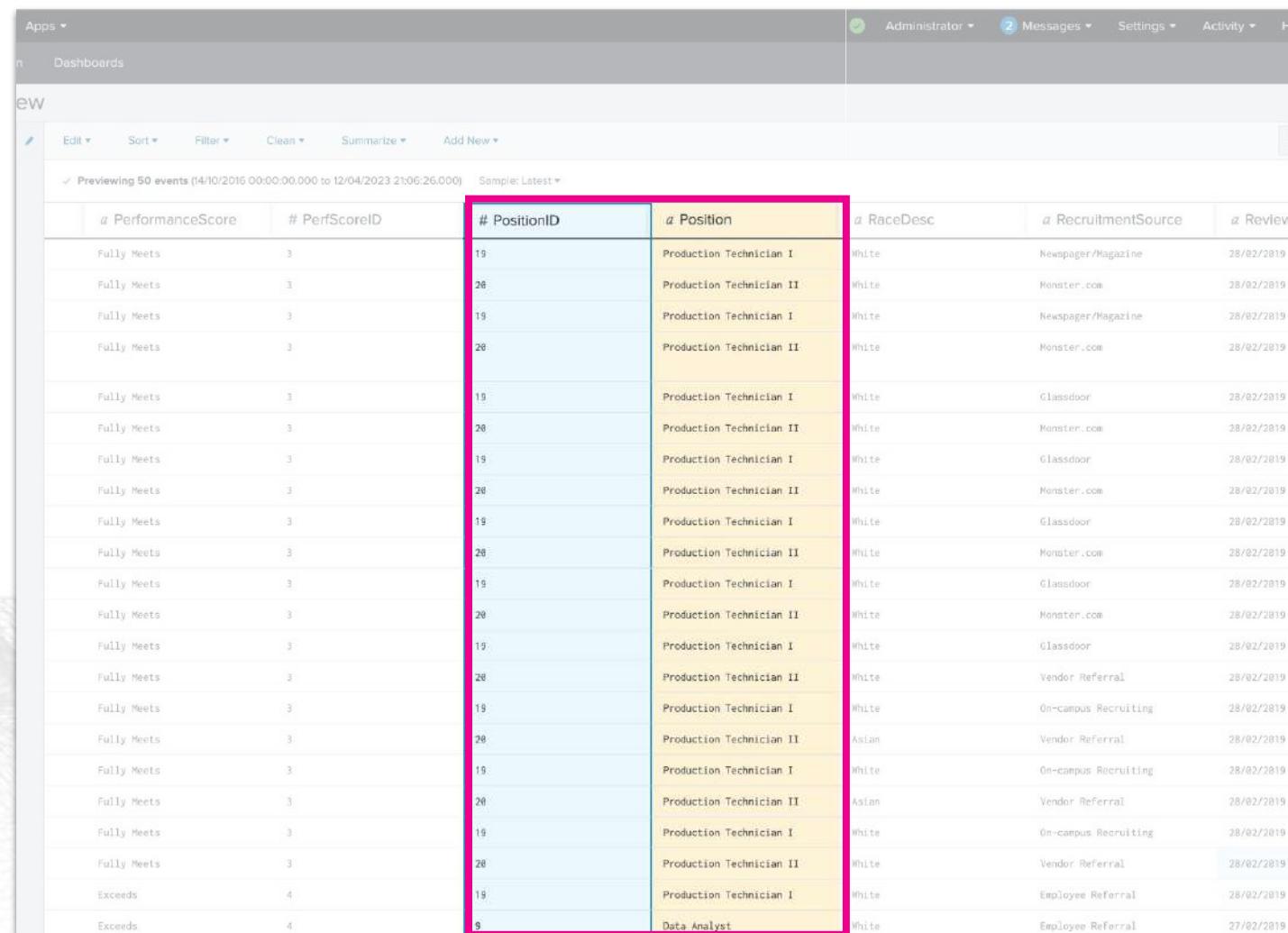
# PositionID	RaceDesc	Recruitme
19	White	Newspaper/Magaz
20	White	Monster.com
19	White	Newspaper/Magaz
20	White	Monster.com
19	White	Glassdoor
20	White	Monster.com
19	White	Glassdoor
20	White	Monster.com
19	White	Glassdoor
20	White	Monster.com
19	White	Glassdoor
20	White	Monster.com
19	White	Glassdoor

Configuring the lookup

The screenshot shows the Splunk interface for configuring a lookup. It consists of three main panels:

- Step 1:** A modal window titled "Lookup" with a sub-section "Select a lookup...". A pink box highlights this section. The text "1. Select the 'hr_data_positions_lookup'" is overlaid on the top right of the modal.
- Step 2:** A larger window titled "Lookup" showing the configuration for the selected lookup. It includes a "Join on" section with the condition "`"PositionID" = "PositionID"`" and a "Fields" section containing the field "Position". A pink box highlights the "Join on" section. The text "2. Select 'PositionID' then 'PositionID' as the join" is overlaid on the top right of this window.
- Step 3:** A smaller window titled "Lookup" showing the final configuration. It contains the same "Join on" and "Fields" sections as the previous window, along with "Cancel" and "Apply" buttons. A pink box highlights the "Fields" section. The text "3. Select 'Position' then click 'Apply'" is overlaid on the bottom right of this window.

Explore the extended fields



#	PerformanceScore	#	PerfScoreID	#	PositionID	#	Position	#	RaceDesc	#	RecruitmentSource	#	ReviewDate
	Fully Meets		3		19		Production Technician I		White		Newspaper/Magazine		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Monster.com		28/02/2019
	Fully Meets		3		19		Production Technician I		White		Newspaper/Magazine		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Monster.com		28/02/2019
	Fully Meets		3		19		Production Technician I		White		Glassdoor		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Monster.com		28/02/2019
	Fully Meets		3		19		Production Technician I		White		Glassdoor		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Monster.com		28/02/2019
	Fully Meets		3		19		Production Technician I		White		Glassdoor		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Monster.com		28/02/2019
	Fully Meets		3		19		Production Technician I		White		Glassdoor		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Vendor Referral		28/02/2019
	Fully Meets		3		19		Production Technician I		White		On-campus Recruiting		28/02/2019
	Fully Meets		3		28		Production Technician II		Asian		Vendor Referral		28/02/2019
	Fully Meets		3		19		Production Technician I		White		On-campus Recruiting		28/02/2019
	Fully Meets		3		28		Production Technician II		Asian		Vendor Referral		28/02/2019
	Fully Meets		3		19		Production Technician I		White		On-campus Recruiting		28/02/2019
	Fully Meets		3		28		Production Technician II		White		Vendor Referral		28/02/2019
	Exceeds		4		19		Production Technician I		White		Employee Referral		28/02/2019
	Exceeds		4		9		Data Analyst		White		Employee Referral		27/02/2019



Calculated Field

1. Click 'Add New', then 'Calculated Field'

The screenshot shows a Splunk search interface. A context menu is open over a table, with the 'Add New' option highlighted and a dropdown menu showing 'Calculate Field...' selected. The table has columns: #, Salary_k, Sex, and # SpecialProjectsCo. The 'Salary_k' column is highlighted with a red box. The data in the table is as follows:

#	Salary_k	Sex	# SpecialProjectsCo
23		F	0
29		F	0
23		M	0
23		M	0
23		F	0
23		M	0
23		F	0

2. Click 'Salary_k' column header

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**'

The screenshot shows the 'Calculate Field' dialog box. The 'New field name' field is populated with 'Salary'. In the 'Field' section, 'Salary_k' is listed. Below the field list is a row of arithmetic operators: +, -, *, and /. Underneath the operators is a 'Value' input field containing '1000', which is highlighted with a blue border. At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

Create Calculated Field

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

- Top Bar:** Splunk > enterprise, Apps, Splunk 4 Rookies BI Edition, Dashboards, Administrator, Messages, Settings, Activity, Help, Find.
- Left Sidebar:** rookies, History, SPL, Selected Data (highlighted with a red box), Rename Field, Split Fields, Lookup, Calculate Field.
- Central Area:** Previewing 50 events (14/10/2016 00:00:00.000 to 13/04/2023 09:41:57.000) Sample: Latest. The table includes columns: State, Zip, # Salary_k, and # Salary. A color scale legend is present.
- Right Side Callout:** You will now see your new field.
- Bottom Left Overlay:** check out your of modification.

You will now see
your new field

Also, Check out your history of modification

Summary of dataset

Create Table View

History SPL

Selected Data Rename Field Split Fields Lookup

33,100 events (before 12/04/2023 21:47:02.000) Event Limiting: ~100,000

All time Rows Summary

_time

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

Earliest: 2016-10-14 00:00:00 Latest: 2019-02-28 00:00:00

CitizenDesc

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	95.95%
0 Multivalue	2.84%
3 Unique values	1.21%

DateofHire

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	4.5%
0 Multivalue	3.63%
99 Unique values	3.17%

DateofTermination

- 28.97% Matched type
- 0.00% Mismatched type
- 71.03% Null or empty

9590 Single value	71.03%
0 Multivalue	1%
104 Unique values	1%

Department

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	67.4%
0 Multivalue	15.86%
6 Unique values	10.12%

DOB

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	0.66%
0 Multivalue	0.63%
306 Unique values	0.33%

EmplID

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	0.03%
0 Multivalue	0.03%
3310 Unique values	0.03%

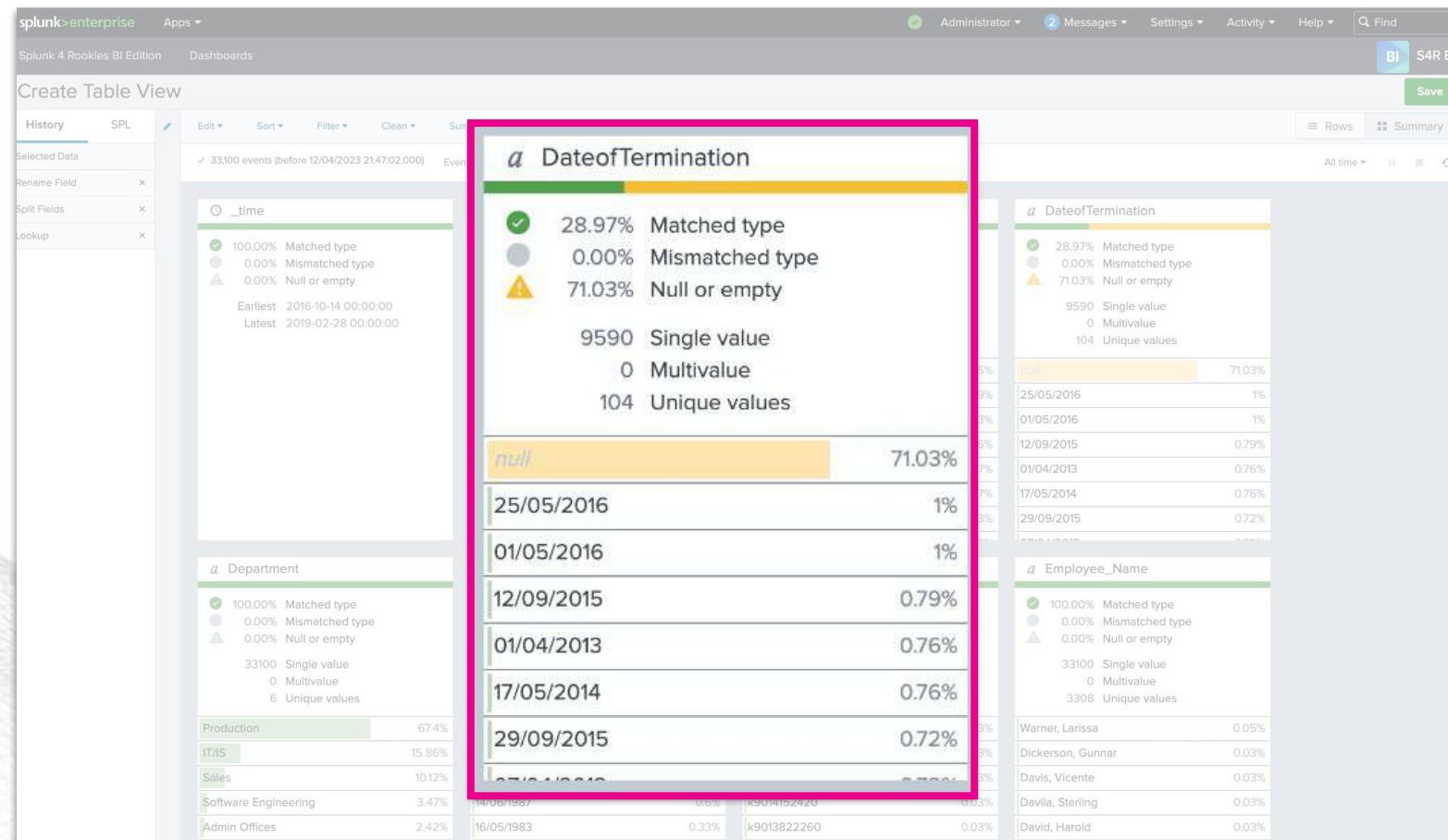
Employee_Name

- 100.00% Matched type
- 0.00% Mismatched type
- 0.00% Null or empty

33100 Single value	0.05%
0 Multivalue	0.03%
3308 Unique values	0.03%

Save

Summary of dataset



Save the table dataset

1. Enter 'rookies' as the Table Title

Table Title: rookies

Table ID ?: rookies

Description: optional

Cancel Save

Your Table Has Been Created

You may now explore your table, change additional settings, or return to the listings page.

Additional Settings:

- Permissions

Close View Listings View Table

2. Click 'Save'

3. Click 'View Table'

Table Dataset

splunk>enterprise Apps ▾

Splunk 4 Rookies BI Edition Dashboards **BI S4R BI**

> rookies ↻ **Edit** **Explore**

All time ▾ **33,100 events (before 12/04/2023 21:48:42.000)**

20 per page ▾ **1** 2 3 4 5 6 7 8 ... Next >

#	⌚ _time	¤ CitizenDesc	¤ DateofHire	¤ DateofTermination	¤ Department	¤ DOB	¤ EmpID	¤ Employee_Name	¤ Employment_Status
1	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9977860168	Murray, Dayanara	Active
2	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	17/05/2014	Production	01/12/1974	k9975930274	Bauer, Kylieigh	Voluntarily Terminated
3	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9974670478	Clark, Justice	Active
4	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	11/01/2014	Production	01/12/1974	k9905930504	Riggs, Gavyn	Voluntarily Terminated
5	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9966300788	Stevens, Teagan	Active
6	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	24/06/2013	Production	01/12/1974	k9946530894	Blair, Kaitlynn	Voluntarily Terminated
7	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9954241098	Hull, Lillianna	Active
8	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	08/02/2016	Production	01/12/1974	k9901261204	Chase, Chaim	Voluntarily Terminated
9	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9918531488	Jimenez, Bruno	Active
10	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9953411514	Vega, Anya	Active
11	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9905317118	Hopkins, Melchi	Active
12	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9981261824	Atkinson, Sandra	Active
13	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9961762028	Galvan, Marcelo	Active
14	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9947112134	Rodriguez, Brenton	Active
15	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9926402338	Eaton, Catalina	Active
16	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9913822444	Fleming, Damika	Active
17	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012	null	Production	10/06/1986	k9938172648	Gamble, Amelia	Active
18	2019-02-28T00:00:00.000Z	US Citizen	13/05/2013	null	Production	01/12/1974	k9927932754	Monroe, Brenton	Future Start
19	2019-02-28T00:00:00.000Z	US Citizen	20/02/2012				k9900392958	Copeland, Moshe	Active
20	2019-02-28T00:00:00.000Z	US Citizen	07/07/2014				k1012021010	Woodson, Jaqen	Active

Completed Table Dataset





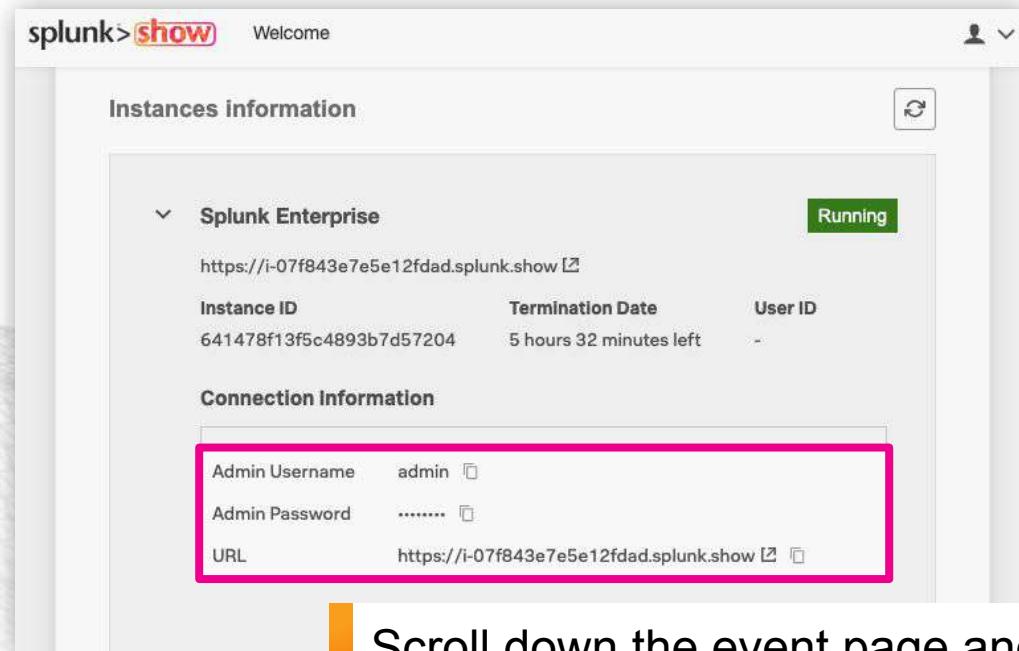
Module 2

Data visualisation with Pivot

splunk>

Login to Splunk

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



The screenshot shows the Splunk Show event page. In the 'Instances information' section, there is a collapsed 'Splunk Enterprise' item. Underneath it, the URL <https://i-07f843e7e5e12fdad.splunk.show> is listed. Below this, 'Connection Information' is expanded, showing fields for 'Admin Username' (admin), 'Admin Password' (redacted), and 'URL' (<https://i-07f843e7e5e12fdad.splunk.show>). A pink box highlights the 'Admin Username' and 'URL' fields.

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**



Navigate to your Module

Search Analytics Datasets Reports Alerts Dashboards

Splunk 4 Rookies BI Edition

Workshop Options

This app is intended to provide a gateway into the 2 modules that make up the Splunk 4 Rookies BI Edition workshop.

The two options below are:

- Module 1 - In this part of the workshop, we will create a table dataset from scratch, ensuring we have the fields we want, in the right order.
- Module 2 - In this part of the workshop, we work through the table dataset created in module 1, where we will create a new dashboard.

1. Click on 'Module 2'

Module 1

Module 2

Edit Export ...

Let's Explore the UI

Visualisations

The screenshot shows the Splunk user interface with several UI elements highlighted by pink boxes:

- Visualisations**: A sidebar on the left containing a list of visualization icons.
- New Pivot**: A search bar at the top with the text "68,474 events (20/03/2023 13:00:00)".
- Filters**: A section with a dropdown menu set to "Last 24 hours".
- Split Rows**: A button to add a new row splitting condition.
- Count of rookie**: A metric value of 68474.
- Search Filter (Change to 'All Time')**: A callout pointing to the search bar.
- Select what field to split rows by**: A callout pointing to the "Split Rows" button.
- Search Output**: A large central area showing search results.
- Select what field to split rows by**: A callout pointing to the "Split Columns" button.
- Column Values**: A dropdown menu with "Count of rookie..." selected.
- Save As...**: A button in the top right corner.
- Clear**: A button in the top right corner.
- Edit Dataset**: A button in the top right corner.
- rookies**: A dropdown menu in the top right corner.
- Documentation**: A link in the top right corner.
- Save or modify data**: A callout pointing to the top right corner.
- Rename Fields**: A callout pointing to the "Column Values" dropdown.

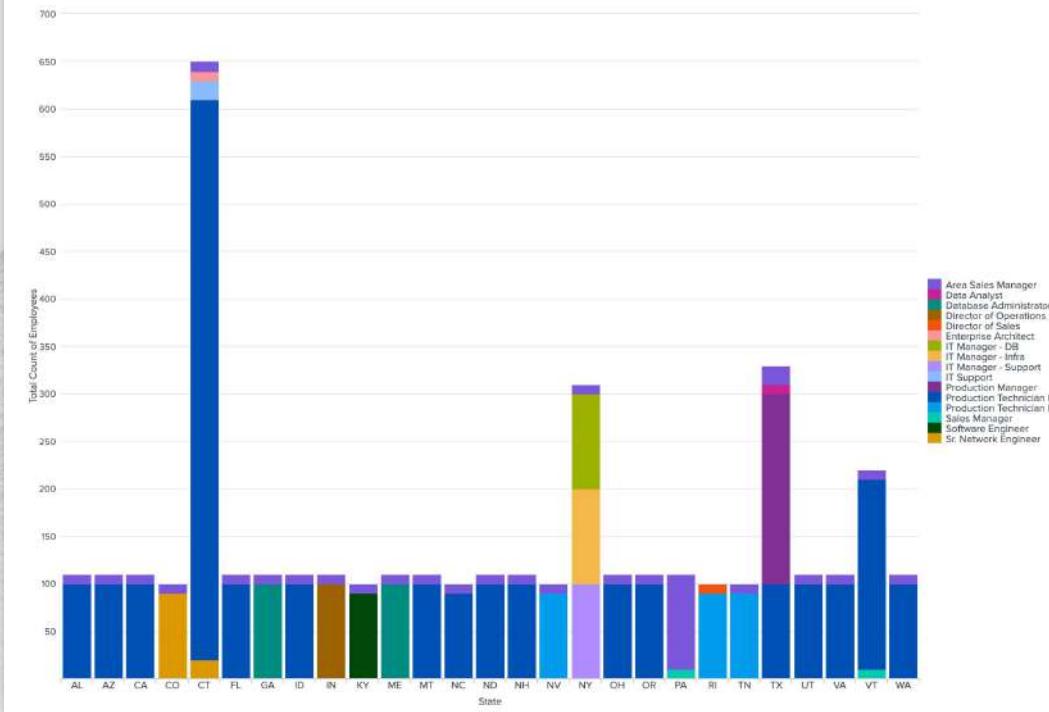


How many employees per state by role

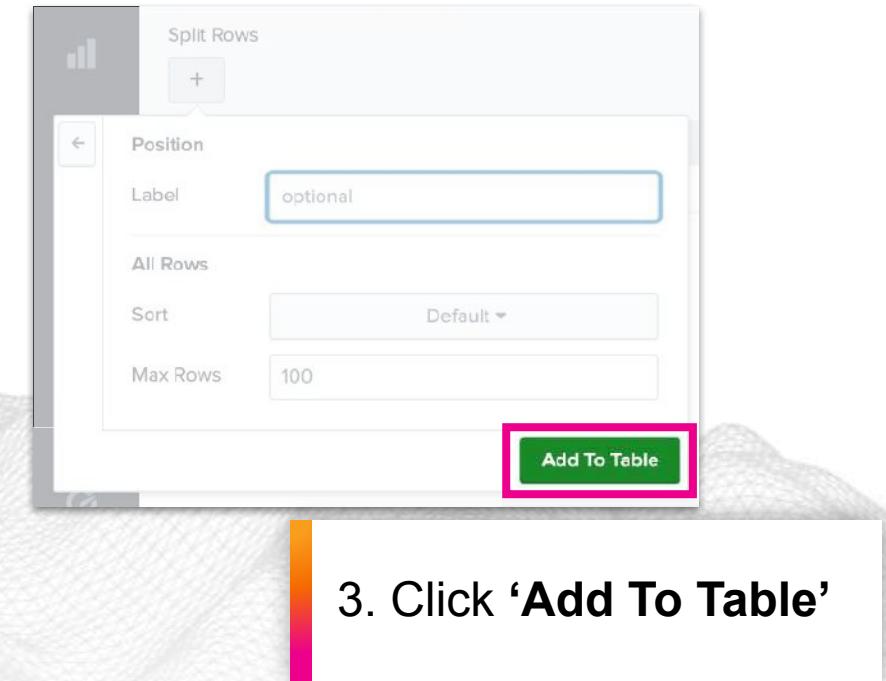
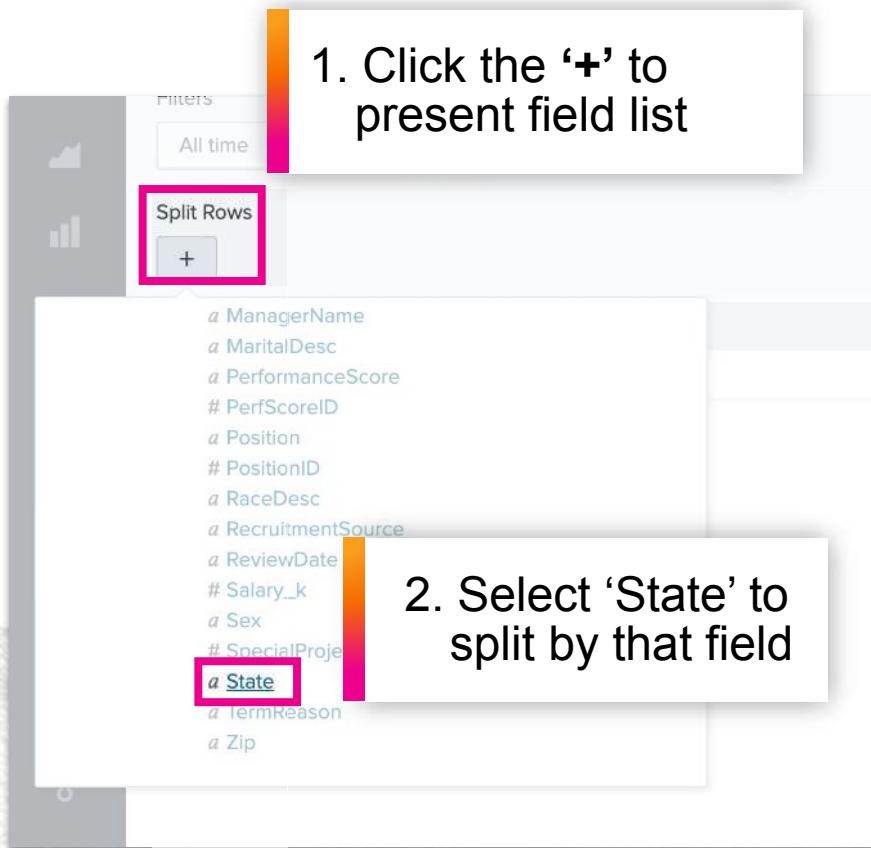
Tasks

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



Split by Row



Tasks

1. Show how many employees there are per US state

Live Changes

splunk>enterprise Apps ▾

Splunk 4 Rookies BI Edition Dashboards BI S4R BI

New Pivot ✓ 33,100 events (before 13/04/2023 09:18:40.000)

Filters All time +

Split Rows State +

Split Columns +

Column Values Count of rookies +

Documentation ↗

State : Count of rookies :

State	Count of rookies
AL	110
AZ	110
CA	110
CO	100
CT	650
FL	110
GA	110
ID	110
IN	110
KY	100
MA	29320
ME	110
MT	110
NC	100
ND	110
NH	110
NV	100
NY	110
OH	110

Updated View

20 per page ▾ ✓ Format < Prev 1 2 Next >

splunk>

Split by Column

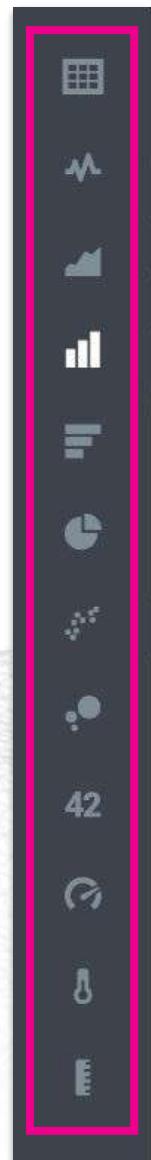
The screenshot shows the Splunk interface with three main components:

- Left Panel:** A list of fields: a EmpID, a Employee_Name, a EmploymentStatus, # EmpSatisfaction, a Location, a ManagerName, a MaritalDesc, a PerformanceScore, # PerfScoreID, a Position, # PositionID, and a PosDate. A red box highlights the '+ Split Columns' button.
- Middle Panel:** A large, semi-transparent watermark of a mountain range is visible across the center.
- Right Panel:** A configuration window titled 'Split Columns'. It includes:
 - A back arrow icon.
 - A 'State' section with a 'Split Columns' button.
 - A 'Max Columns' input field set to '100'.
 - A 'Totals' section with a 'Yes' checkbox.
 - A green 'Add To Table' button highlighted with a red box.

Annotations:

- 1. Click the ‘+’ to present column list**: Points to the '+ Split Columns' button in the left panel.
- 2. Select ‘Position’ to split by that field**: Points to the 'Position' field in the list of fields.
- 3. Click ‘Add To Table’**: Points to the 'Add To Table' button in the right panel.

Explore the Visualisations



Explore the visualisations

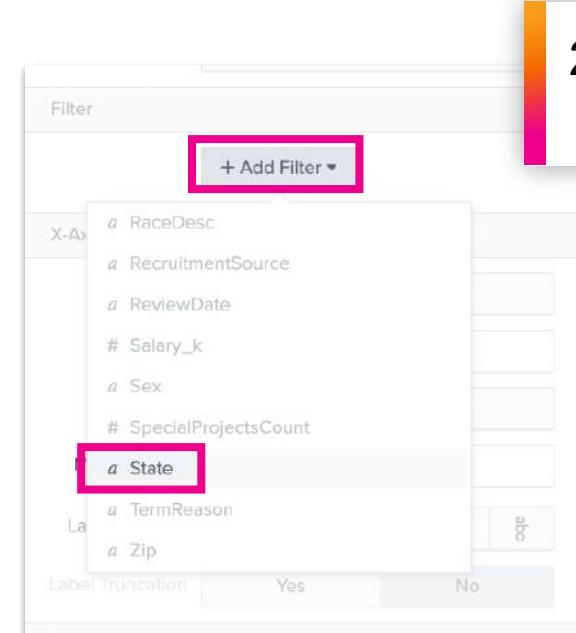
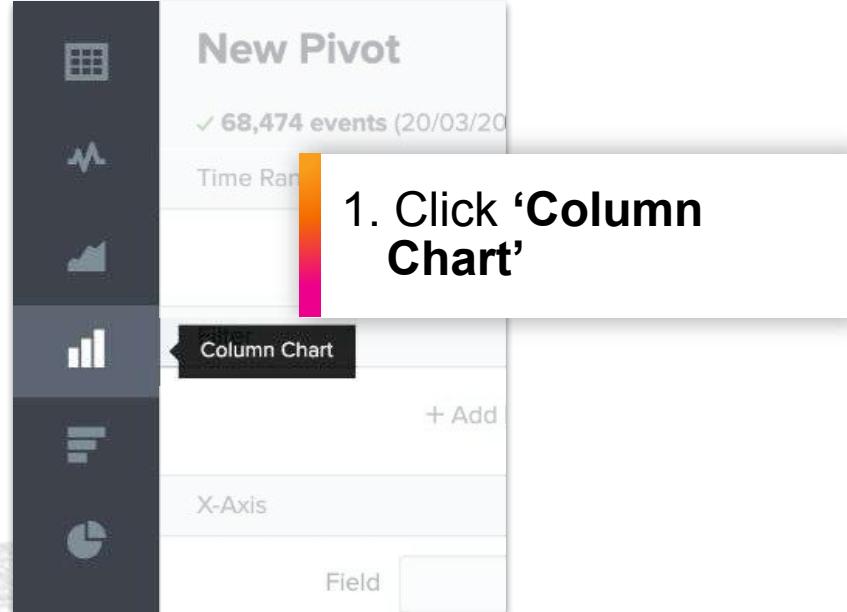


Each type has many options for customisation

Hint

4. Show as a stacked column chart

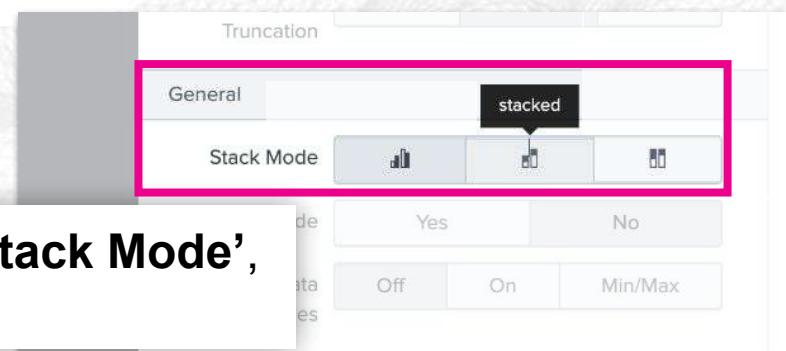
Configure Visualisation



2. Click 'Add Filter', then select 'State'

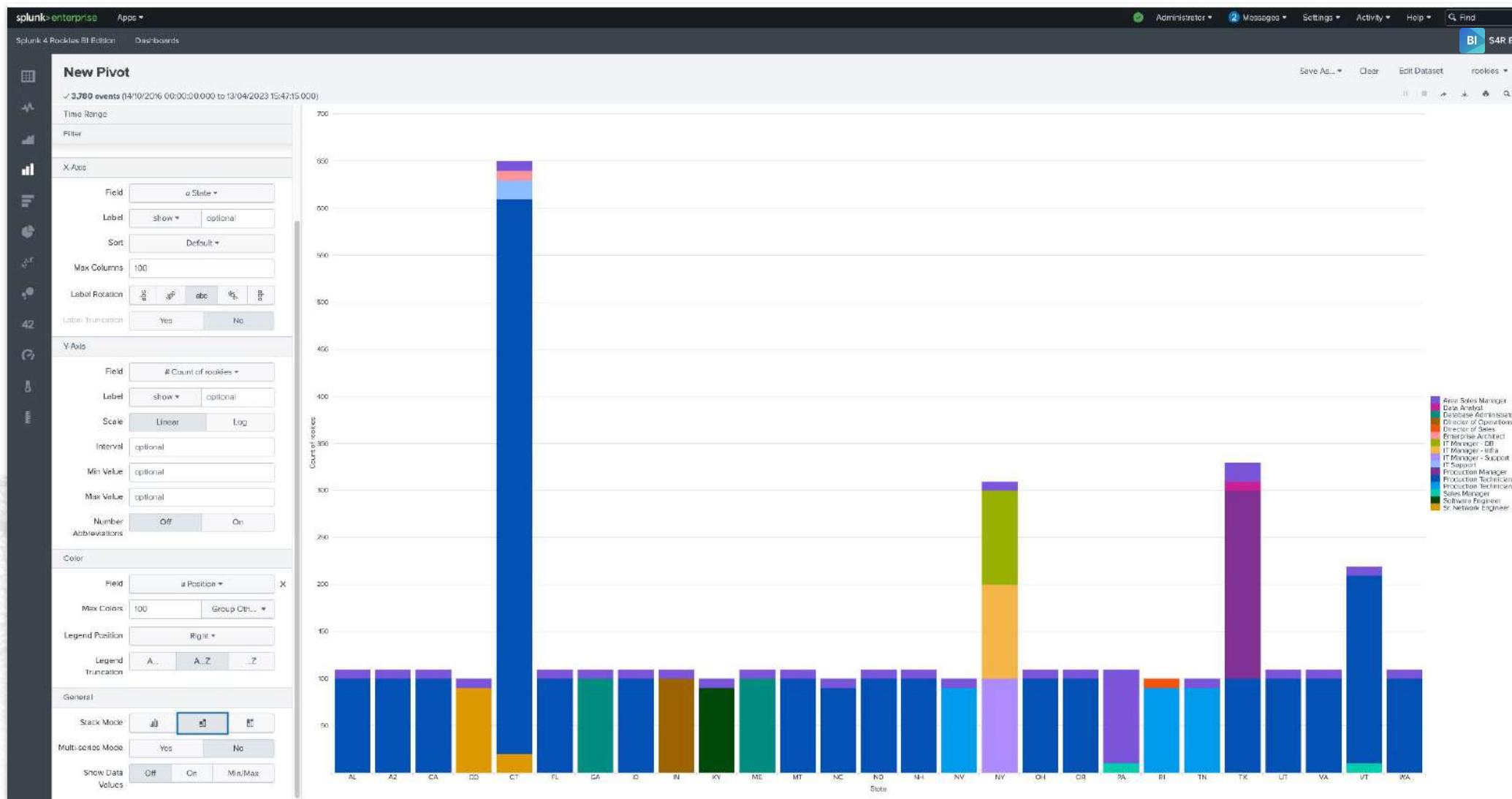


3. Change match to 'is not' then enter 'MA'

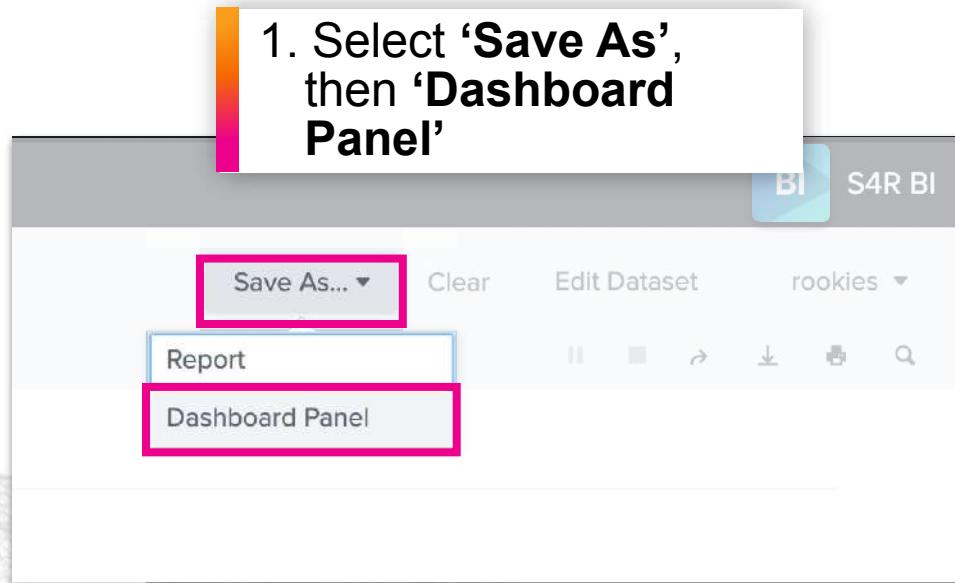


4. Under 'General' - 'Stack Mode', Select 'Stacked'

Completed Visualisation



Save Our Visualisation



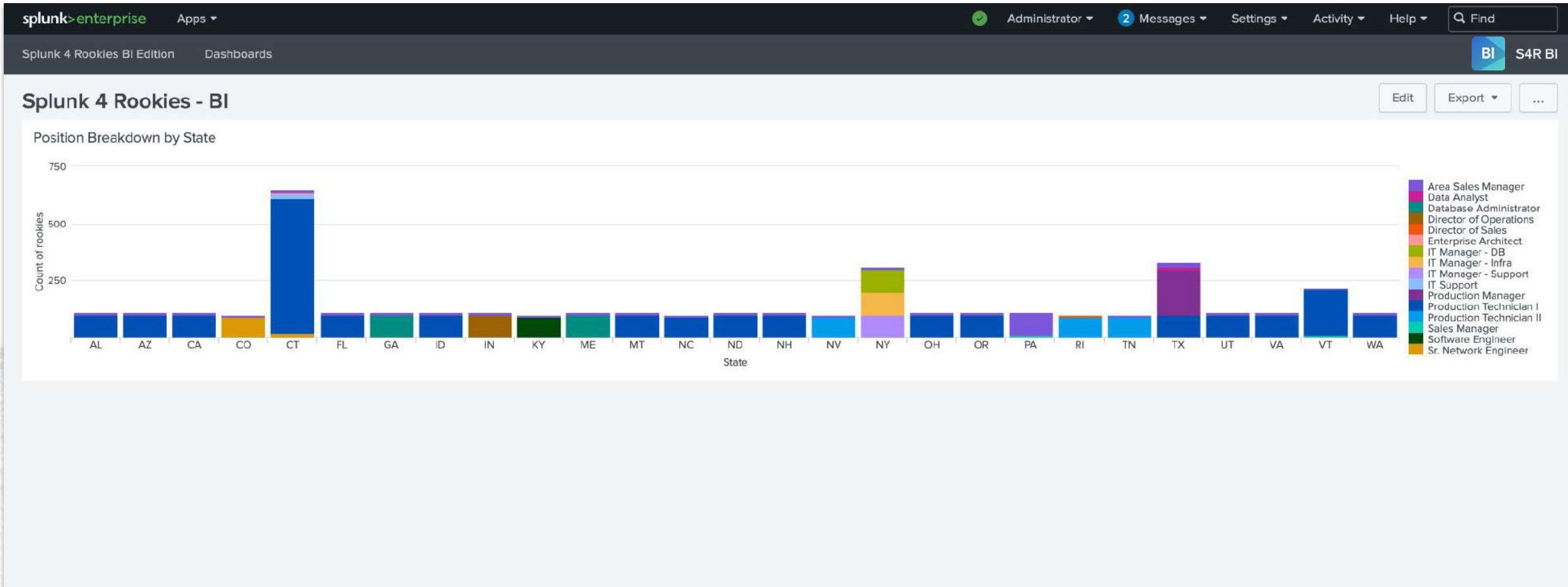
1. Select 'Save As',
then 'Dashboard
Panel'

The screenshot shows the 'Save As Dashboard Panel' dialog box. It has two tabs: 'New' (selected) and 'Existing'. The 'Dashboard Title' field contains 'Splunk 4 Rookies - BI'. The 'Dashboard ID' field contains 'splunk_4__rookies__bi' with a note below stating: 'The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.' The 'Dashboard Description' field is set to 'optional'. Under 'Dashboard Permissions', 'Private' is selected. The 'Panel Title' field contains 'Position Breakdown by State'. The 'Panel Powered By' field has 'Q Inline Search' selected. The 'Drilldown' field is set to 'No action'. Under 'Panel Content', 'Statistics' is selected. At the bottom right is a green button labeled 'View Dashboard'.

2. Complete the form
like the image

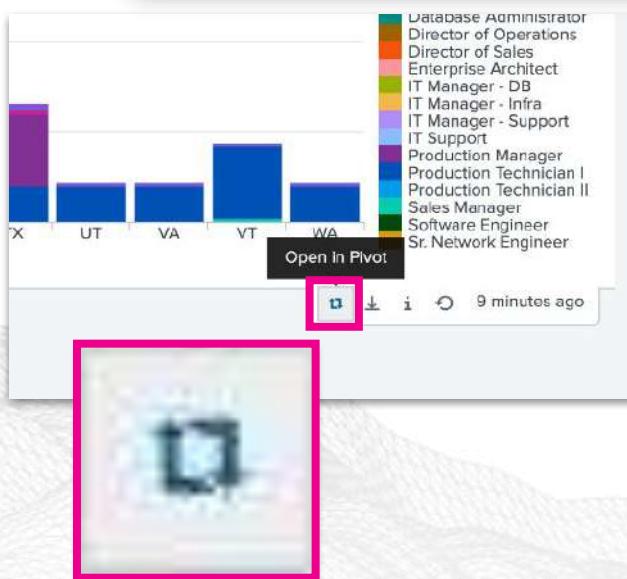
3. Click 'View Dashboard'

Your Dashboard So Far...

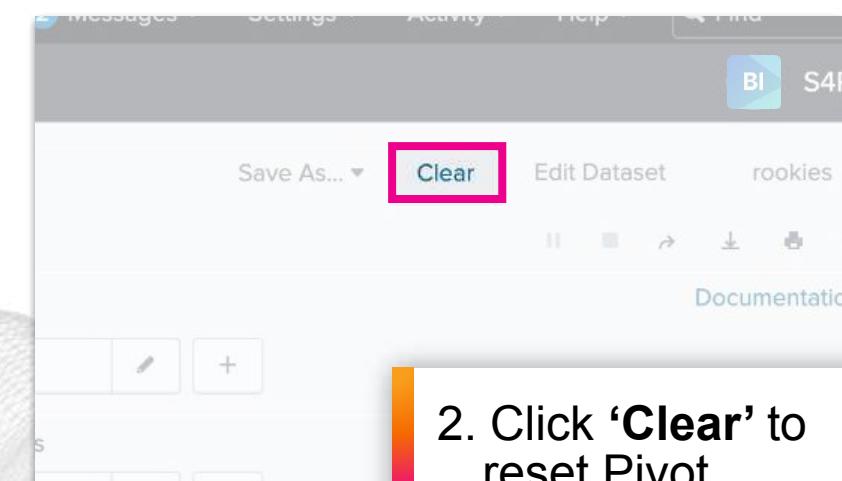


Return to Pivot

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



2. Click 'Clear' to reset Pivot





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

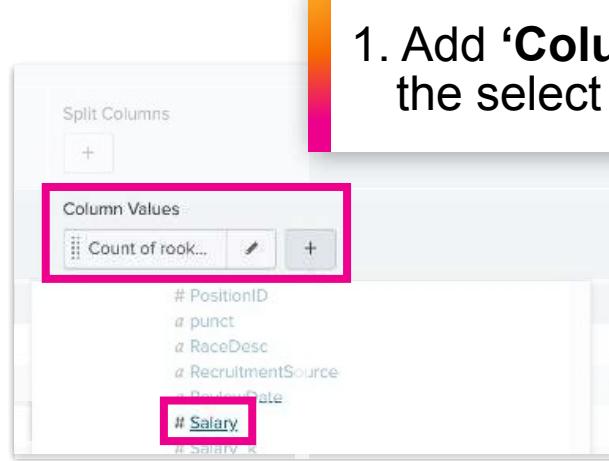
Goal



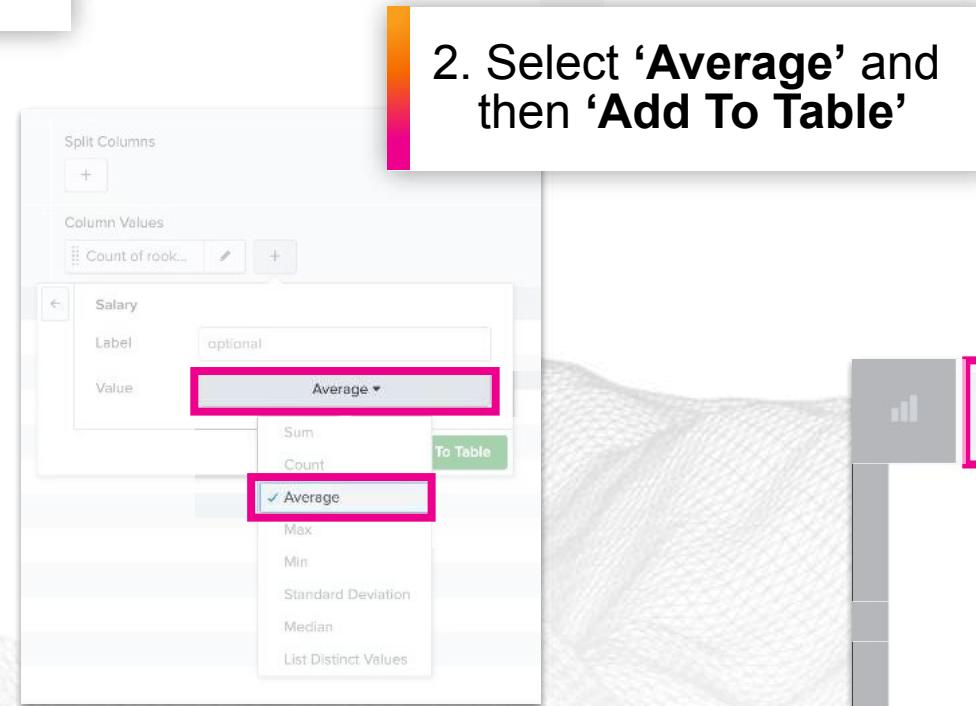
Take 10 minutes to explore the data and attempt to create the required visual

Create Visualisation

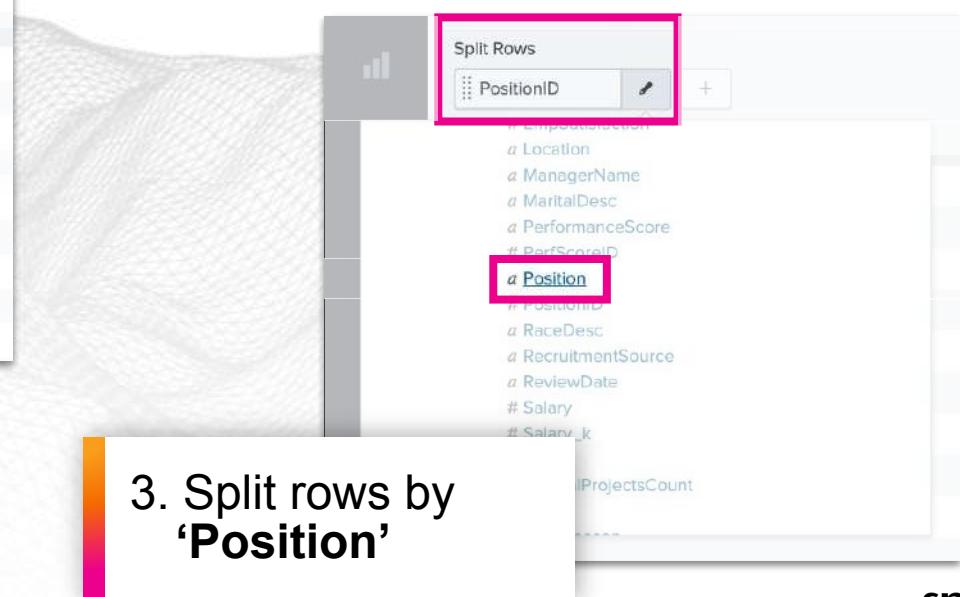
1. Add 'Column Values',
the select 'Salary'



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



3. Split rows by
'Position'



Create Visualisation

A screenshot of a software interface titled "Column Values". It shows a list of fields: "Average of S...", "Employee_Name", "EmploymentStatus", "# EmpSatisfaction", "Location", "ManagerName", "MaritalDesc", "PerformanceScore", and "# PerfScoreID". The "# PerfScoreID" field is highlighted with a red box.

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

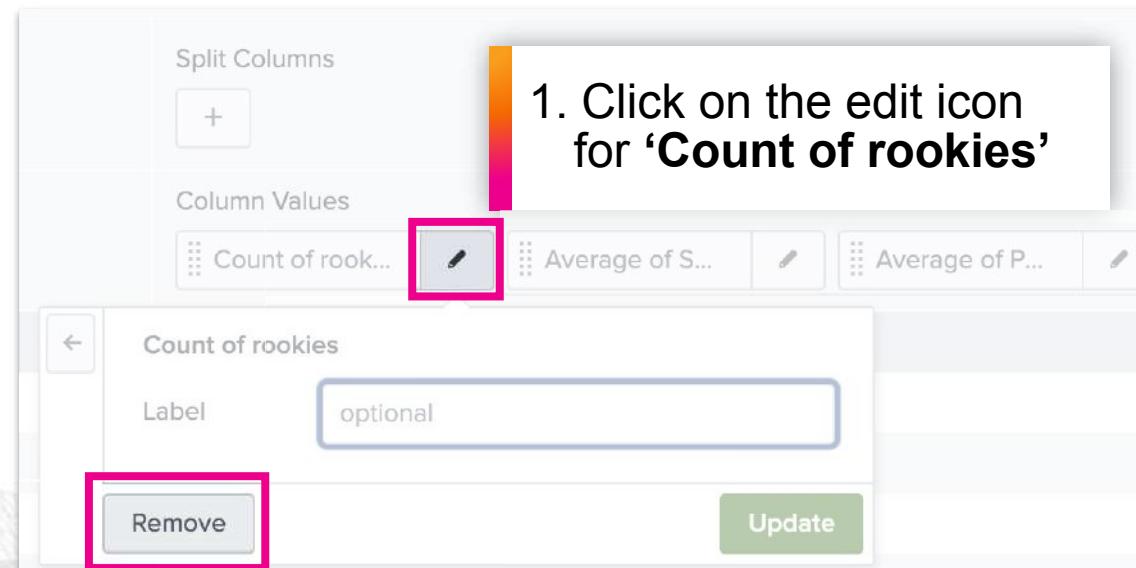
A screenshot of a software interface titled "Column Values". It shows a list of fields: "Average of S...", "Employee_Name", "EmploymentStatus", "# EmpSatisfaction", "Location", "ManagerName", and "# PerfScoreID". The "# PerfScoreID" field is highlighted with a red box. Below, there is a configuration panel for "PerfScoreID" with "Label" set to "optional" and "Value" set to "Sum". Under "Value", there are options: "Sum" (selected), "Count", "To Table", and "Average". The "Average" option is highlighted with a red box.

A screenshot of a software interface titled "Column Values". It shows a list of fields: "Average of S...", "Employee_Name", "EmploymentStatus", "# EmpSatisfaction", "Location", and "ManagerName". The "# EmpSatisfaction" field is highlighted with a red box.

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

A screenshot of a software interface titled "Column Values". It shows a list of fields: "Average of S...", "Employee_Name", "EmploymentStatus", "# EmpSatisfaction", "Location", and "ManagerName". The "# EmpSatisfaction" field is highlighted with a red box. Below, there is a configuration panel for "EmpSatisfaction" with "Label" set to "optional" and "Value" set to "Average". Under "Value", there are options: "Sum", "Count", "To Table", "Average" (selected), "Max", and "Min". The "Average" option is highlighted with a red box.

Create Visualisation



2. Click 'Remove'

Create Visualisation

New Pivot

33,100 events (before 13/04/2023 16:13:40.000)

Filters: All time

Column Values: Average of Salary, Average of PerfScoreID, Average of EmpSatisfaction

Split Columns: +

Documentation: S4R BI

Save As... Clear Edit Dataset cookies

1. Click 'Bubble Chart'

Area Sales Manager
BI Developer
BI Director
CIO
Data Analyst
Data Architect
Database Administrator
Director of Operations
Director of Sales
Enterprise Architect
IT Director
IT Manager - DB
IT Manager - Infra
IT Manager - Support
IT Support
Network Engineer
President & CEO
Principal Data Architect

Average of Salary: 23787.6797878788, 47564.2424242424, 54363.6363636363, 52727.2727272727, 43000, 55150, 58090.9898909090, 55022.727272727, 55022.727272727, 55022.727272727, 37501.5309090909, 49865.4545454545, 66363.6363636363, 55090

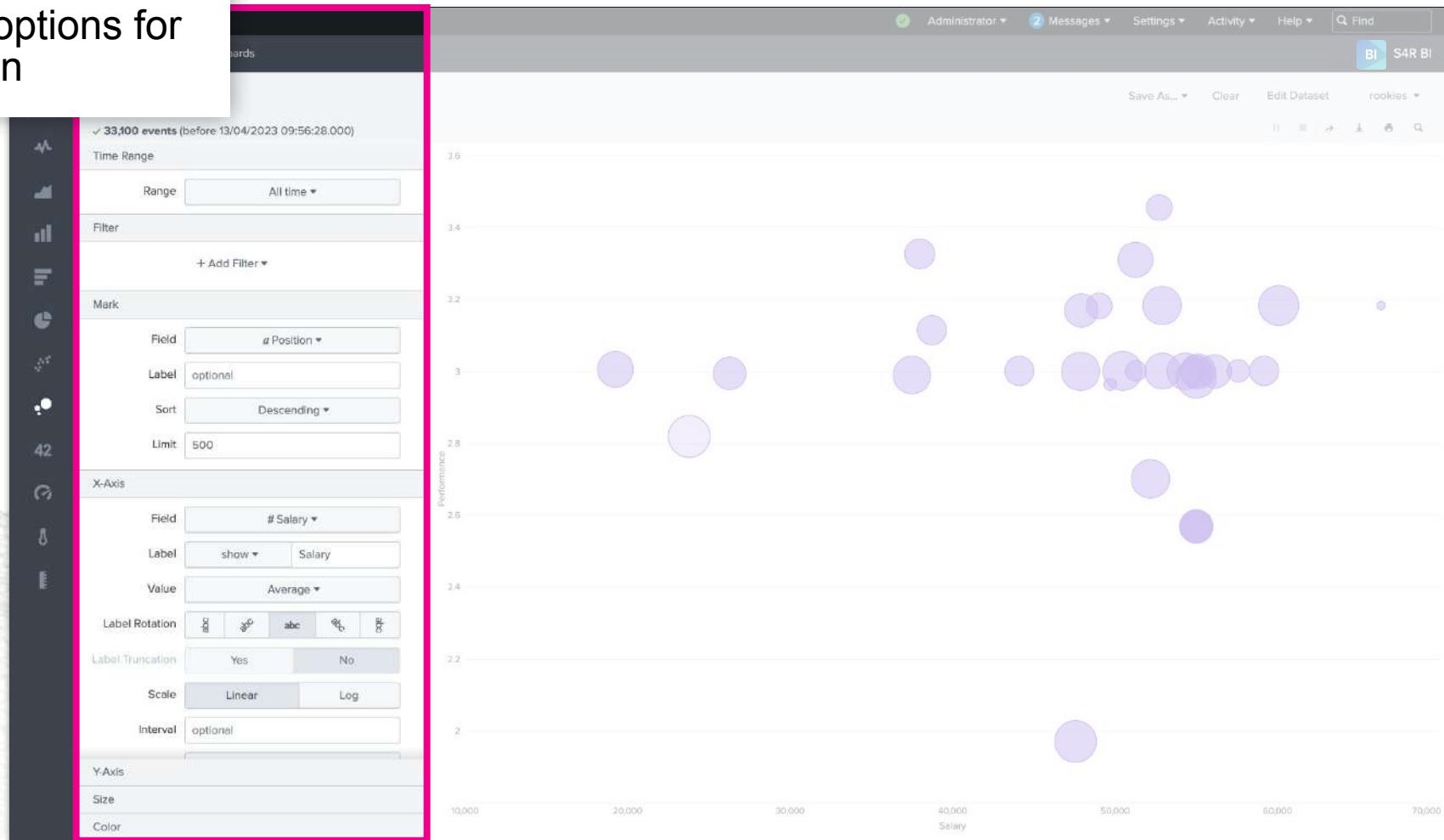
Average of PerfScoreID: 2.6181818181818183, 1.9696969696969697, 2.9797979797979797, 3, 3.4545454545454546, 3.1818181818181817, 3.1136363636363636, 3, 3.327272727272727, 3.1818181818181817, 3, 3

Average of EmpSatisfaction: 4.42424242424242, 4.3616361636163613, 4.252525252525251, 4.8227272727272725, 3.363636363636361638, 3.363636363636361638, 3.534090909090909, 3.5454545454545454, 3.6, 4.090909090909091, 4.090909090909091, 3.5454545454545454, 3.6, 4.2721272127212725, 3.75, 3.75, 3.75, 3.75, 3.0181818181818181, 3.9

Updated View

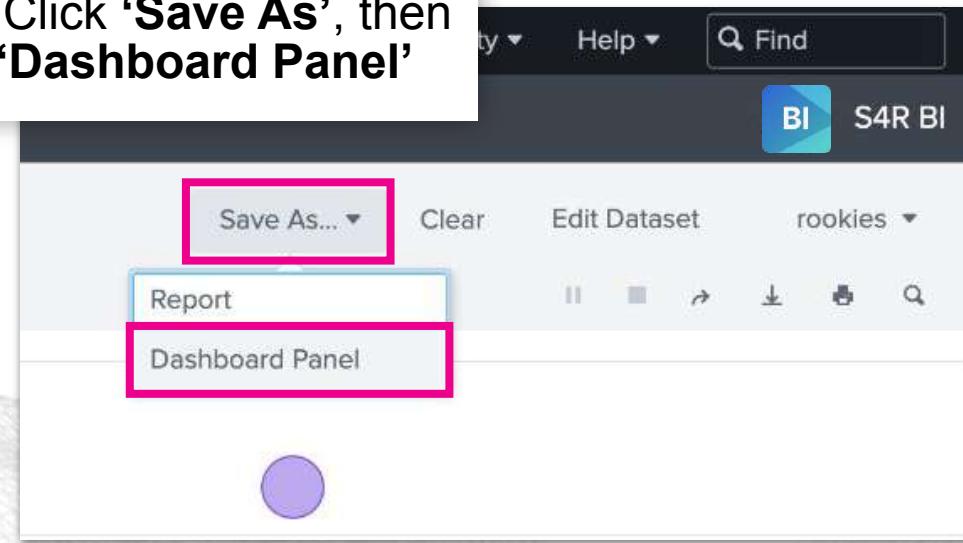
Customise Visualisation

Explore the options for customisation

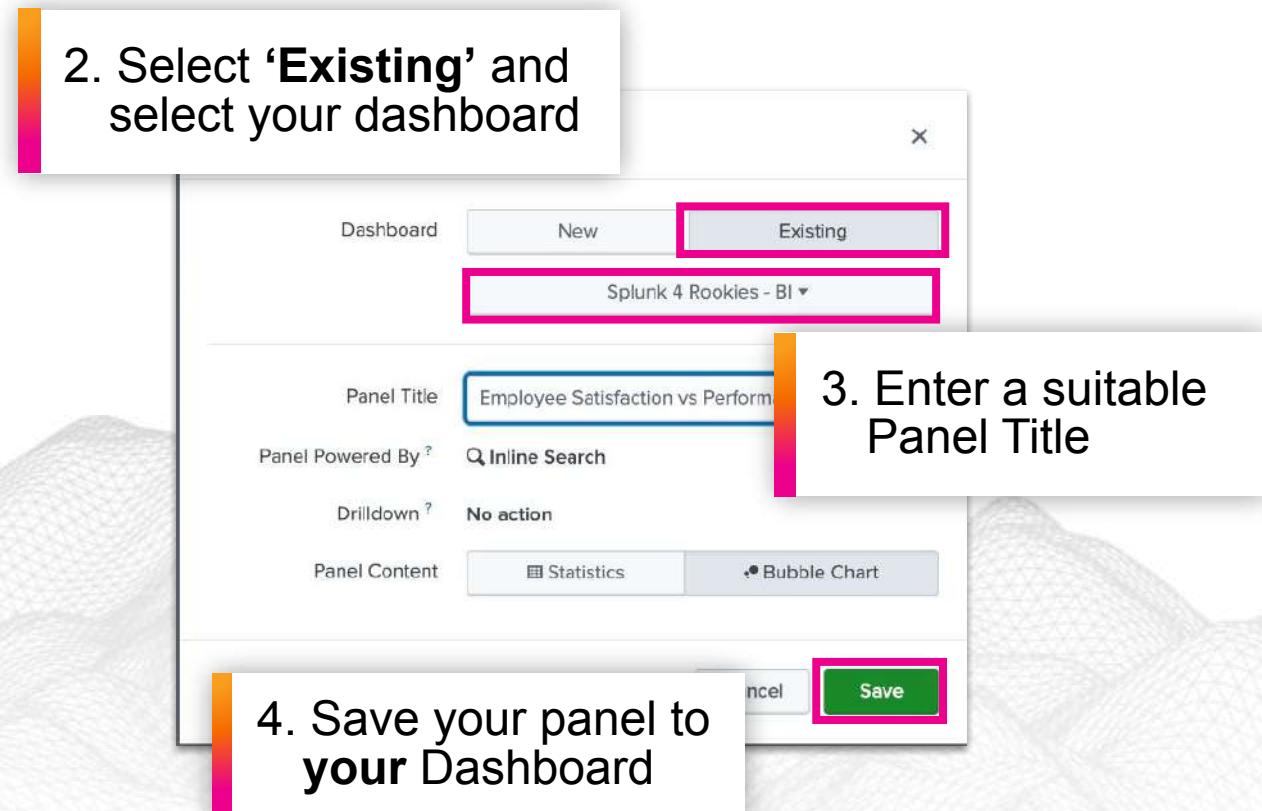


Save Visualisation

1. Click ‘Save As’, then ‘Dashboard Panel’



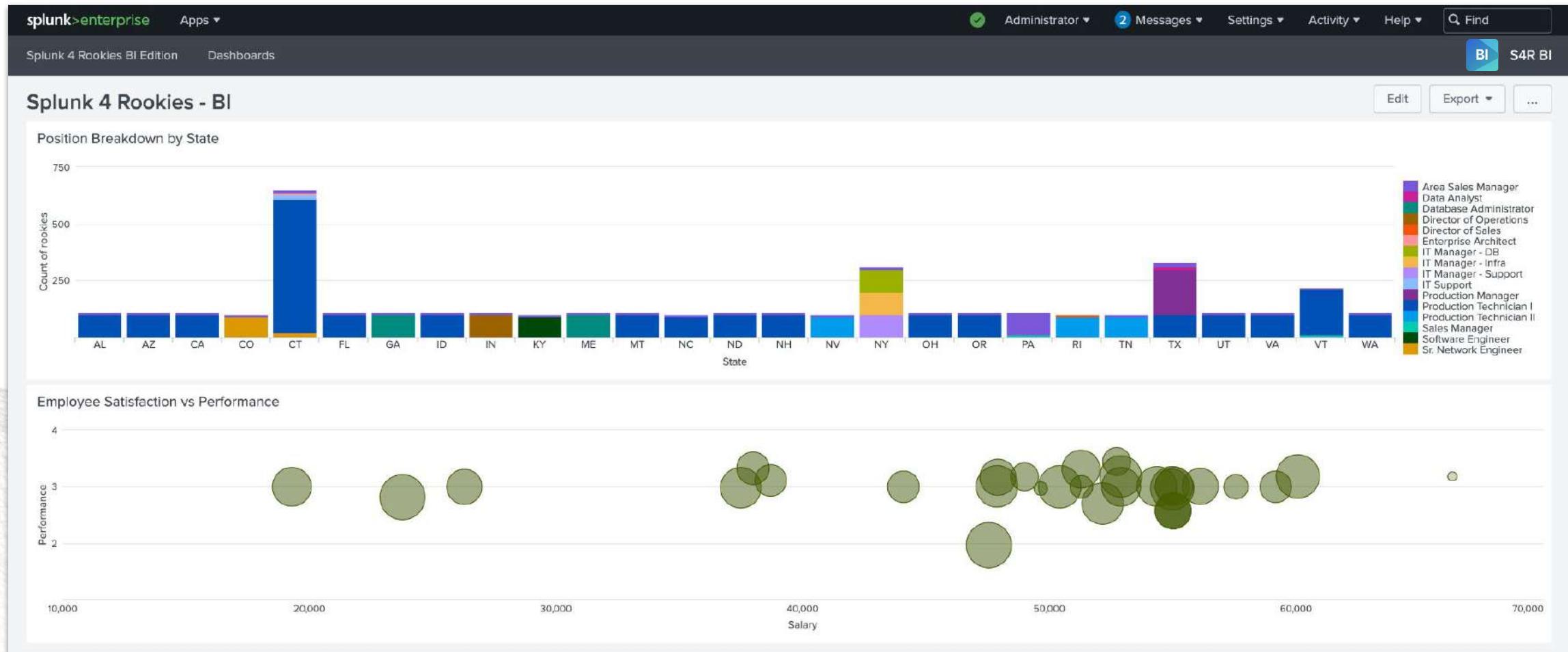
2. Select ‘Existing’ and select your dashboard



3. Enter a suitable Panel Title

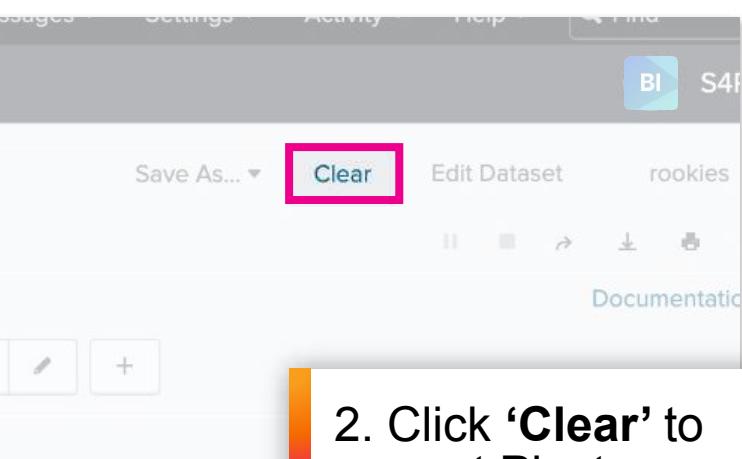
4. Save your panel to your Dashboard

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

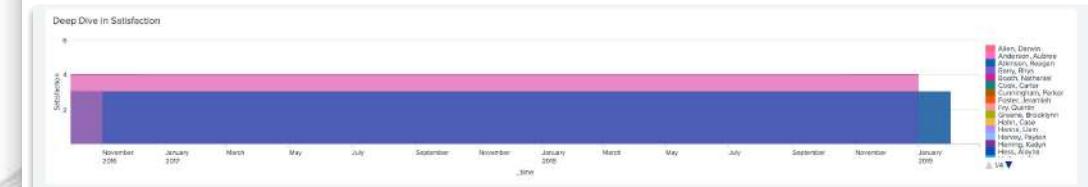


How many employees per state by role

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 their historic data

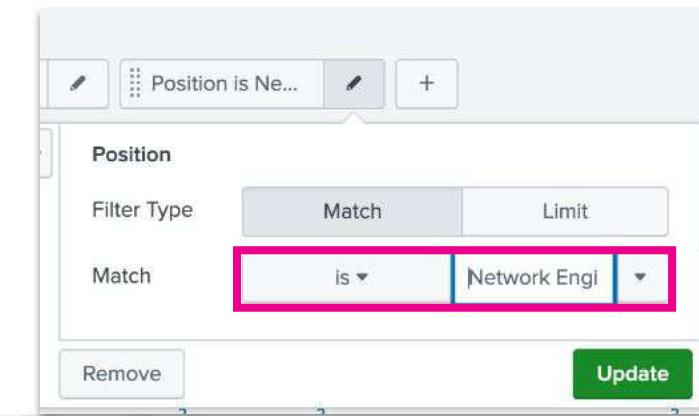
Goal



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

Create Visualisation

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



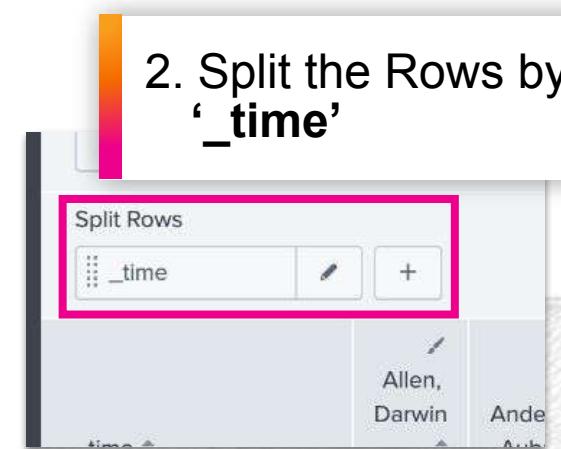
2. Select '**is**' as the match type
and enter '**Network Engineer**'

Create Visualisation

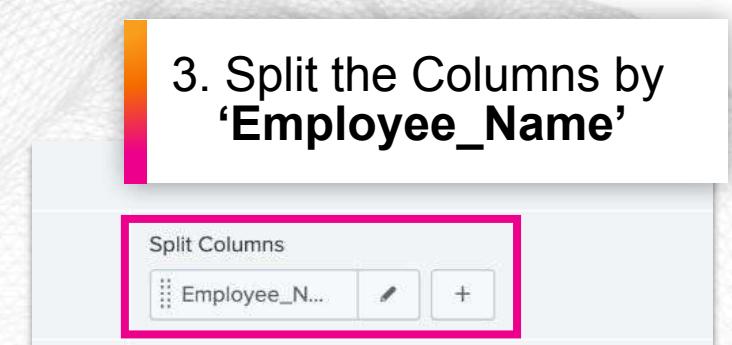
1. Add 'Column Values' and select 'EmpSatisfaction' & 'Average'



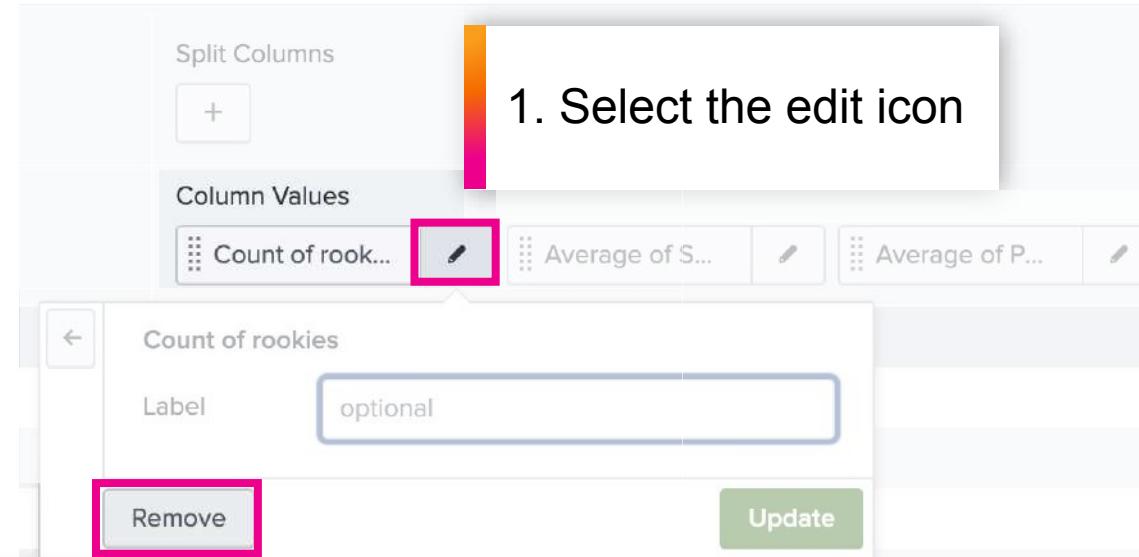
2. Split the Rows by '_time'



3. Split the Columns by 'Employee_Name'



Create Visualisation

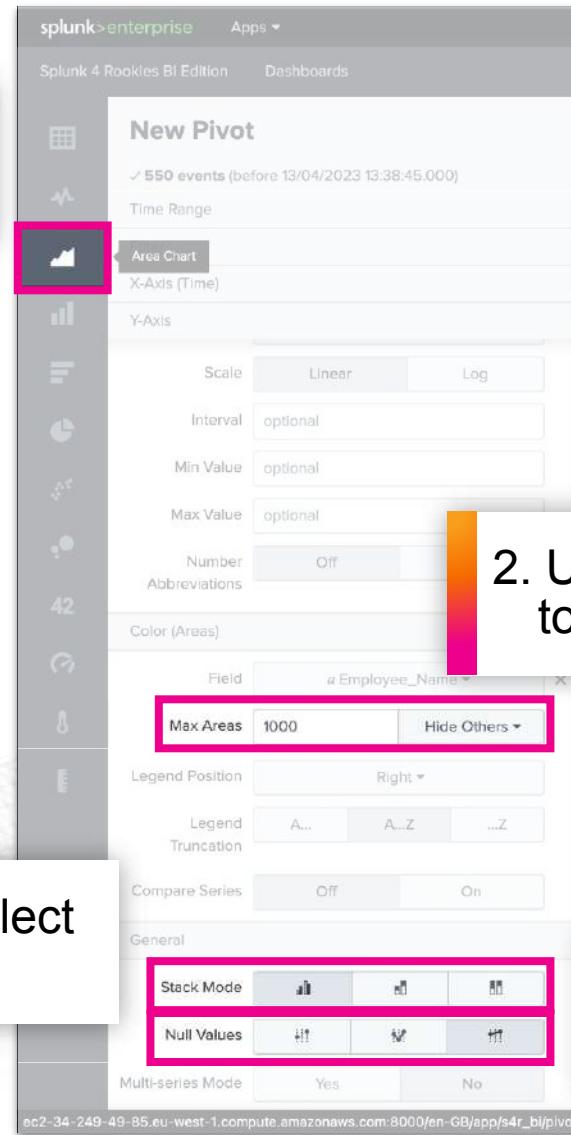


1. Select the edit icon

2. Click 'Remove'

Customise Visualisation

1. Select '**Area Chart**'

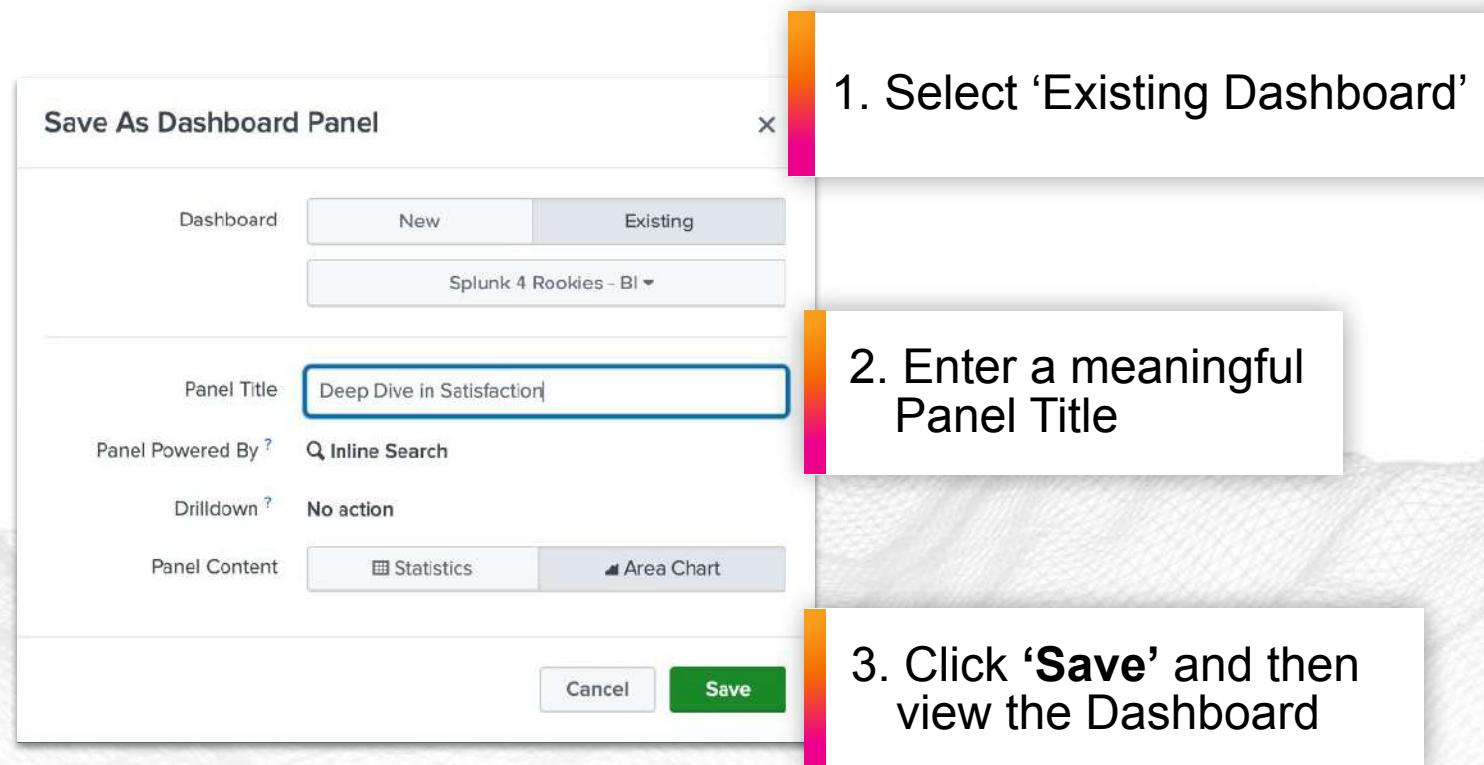


2. Under '**Color**' change '**Max Areas**' to '**Hide Others**' and enter '**1000**'

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

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

Save Visualisation



Create Powerful Story-telling Dashboards with Dashboard Studio

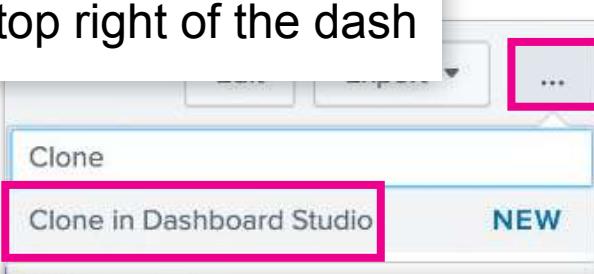
- Advanced visualisation tools
- Streamlined editing experience and fully customisable formats
- Flexible layouts (absolute and grid)
- Support for images, text boxes, shapes, lines and icons
- In-tact PDF export
- Support for custom SVG
- Support for dashboard level defaults





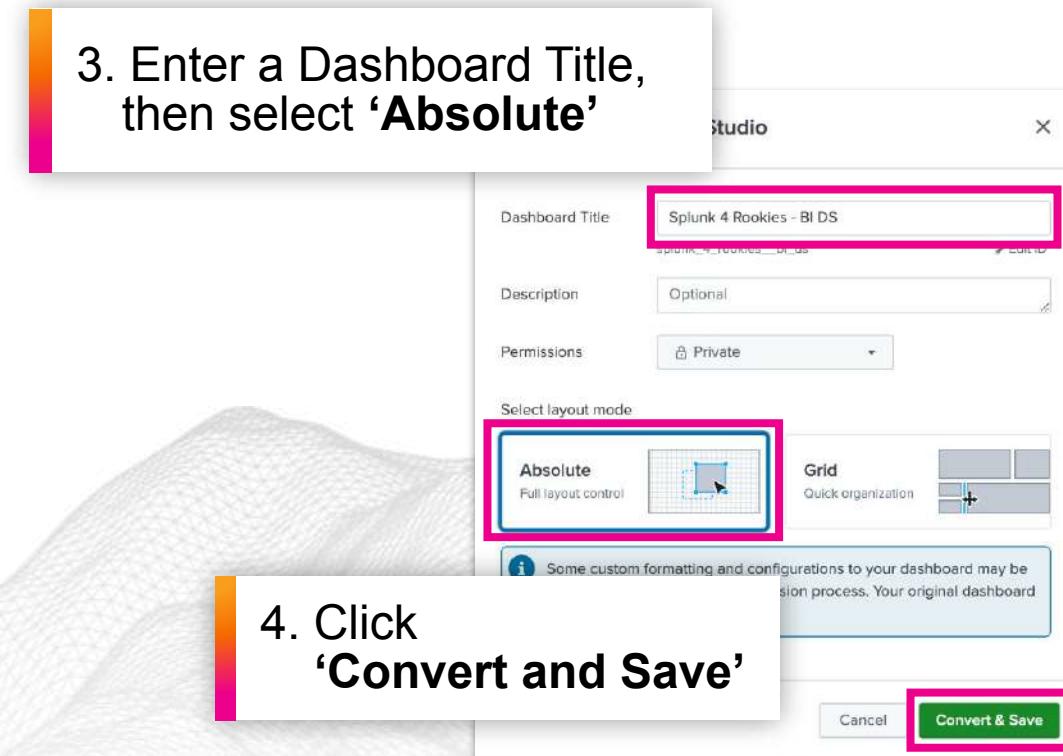
Convert to Dashboard Studio

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'

Explore Your Dashboard

Splunk 4 Rookies BI Edition Apps Dashboards

Position Breakdown by State

State	Area Sales Manager	Data Analyst	Database Administrator	Director of Operations	Director of Sales	Enterprise Architect	IT Manager - DB	IT Manager - Infra	IT Manager - Support	IT Support	Production Manager	Production Technician I	Production Technician II
AL	10	10	10	10	10	10	10	10	10	10	10	10	10
AZ	10	10	10	10	10	10	10	10	10	10	10	10	10
CA	10	10	10	10	10	10	10	10	10	10	10	10	10
CO	10	10	10	10	10	10	10	10	10	10	10	10	10
CT	10	10	10	10	10	10	10	10	10	10	10	10	10
FL	10	10	10	10	10	10	10	10	10	10	10	10	10
GA	10	10	10	10	10	10	10	10	10	10	10	10	10
ID	10	10	10	10	10	10	10	10	10	10	10	10	10
IN	10	10	10	10	10	10	10	10	10	10	10	10	10
KY	10	10	10	10	10	10	10	10	10	10	10	10	10
ME	10	10	10	10	10	10	10	10	10	10	10	10	10
MT	10	10	10	10	10	10	10	10	10	10	10	10	10
NC	10	10	10	10	10	10	10	10	10	10	10	10	10
ND	10	10	10	10	10	10	10	10	10	10	10	10	10
NH	10	10	10	10	10	10	10	10	10	10	10	10	10
NV	10	10	10	10	10	10	10	10	10	10	10	10	10
NY	10	10	10	10	10	10	10	10	10	10	10	10	10
OH	10	10	10	10	10	10	10	10	10	10	10	10	10
OR	10	10	10	10	10	10	10	10	10	10	10	10	10
PA	10	10	10	10	10	10	10	10	10	10	10	10	10
RI	10	10	10	10	10	10	10	10	10	10	10	10	10
TN	10	10	10	10	10	10	10	10	10	10	10	10	10
TX	10	10	10	10	10	10	10	10	10	10	10	10	10
UT	10	10	10	10	10	10	10	10	10	10	10	10	10
VA	10	10	10	10	10	10	10	10	10	10	10	10	10
VT	10	10	10	10	10	10	10	10	10	10	10	10	10
WA	10	10	10	10	10	10	10	10	10	10	10	10	10

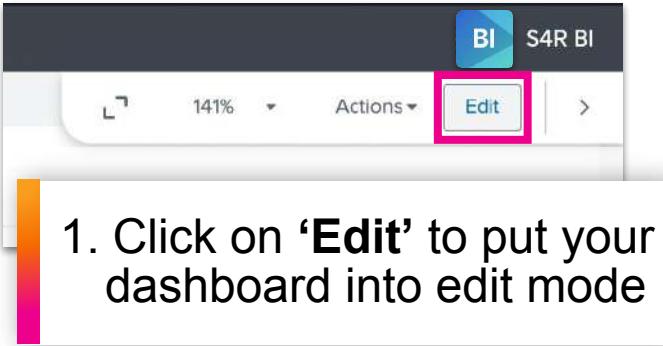
Employee Satisfaction vs Performance

Role	Approx. Salary Range	Approx. Satisfaction Range
President & CEO	50,000 - 60,000	3.5 - 3.8
IT Director	40,000 - 50,000	3.0 - 3.5
Sr. DBA	30,000 - 40,000	2.8 - 3.2
Sr. Accountant	20,000 - 30,000	2.5 - 3.0
Enterprise Architect	40,000 - 50,000	3.0 - 3.5
Principal Data Architect	40,000 - 50,000	3.0 - 3.5
IT Manager - DB	30,000 - 40,000	2.8 - 3.2
IT Manager - Infra	20,000 - 30,000	2.5 - 3.0
IT Manager - Support	10,000 - 20,000	2.5 - 3.0
Shared Services Manager	30,000 - 40,000	2.8 - 3.2
Area Sales Manager	20,000 - 30,000	2.5 - 3.0
BI Developer	10,000 - 20,000	2.5 - 3.0
Sales BI Analyst	10,000 - 20,000	2.5 - 3.0

Deep Dive In Satisfaction

Date	Role	Satisfaction Value
12:00 AM Sat Oct 1 2016	Allen, Darwin	2.5
12:00 AM Sun Jan 1 2017	Anderson, Aubree	2.5
12:00 AM Sat Apr 1 2017	Atkinson, Reagan	2.5
12:00 AM Sat Jul 1 2017	Barry, Rhys	2.5
12:00 AM Sun Oct 1 2017	Booth, Nathaniel	2.5
12:00 AM Mon Jan 1 2018	Cook, Carter	2.5
12:00 AM Sun Apr 1 2018	Cunningham, Parker	2.5
12:00 AM Sun Jul 1 2018	Foster, Jarrahil	2.5
12:00 AM Mon Oct 1 2018	Fry, Quinlan	2.5
12:00 AM Tue Jan 1 2019	Greene, Brooklyn	2.5
12:00 AM Sun Apr 1 2019	Hahn, Case	2.5
12:00 AM Mon Oct 1 2019	Hanna, Liam	2.5
12:00 AM Tue Jan 1 2020	Hanson, Dakota	2.5

Customise Your Dashboard



Here is where you add can add elements to your dashboard

Position Breakdown

State	Count
AL	~100
AZ	~100
CA	~100
CO	~100
CT	~100
FL	~100
GA	~100
ID	~100
IN	~100
KY	~100
ME	~100
MT	~100
NC	~100
ND	~100
NH	~100
NV	~100
NY	~100
OH	~100
OR	~100
PA	~100
RI	~100
TN	~100
TX	~100
UT	~100
VA	~100
VT	~100
WA	~100

Employee Satisfaction vs Performance

Salary Range	Performance Level	Count
\$10,000 - \$20,000	Low	High
\$20,000 - \$30,000	Medium	Medium
\$30,000 - \$40,000	Medium	High
\$40,000 - \$50,000	Medium	Very High
\$50,000 - \$60,000	High	Very High
\$60,000+	Very High	Medium

Deep Dive in Satisfaction

Date	Satisfaction Level
Set Oct 1 2016	Low
12:00 AM Sun Jan 1 2017	Medium
12:00 AM Sat Apr 1 2017	Medium
12:00 AM Set Jul 1 2017	Medium
12:00 AM Sun Oct 1 2017	Medium
12:00 AM Mon Jan 1 2018	Medium
12:00 AM Sun Jul 1 2018	Medium
12:00 AM Mon Oct 1 2018	Medium
12:00 AM Sun Jan 1 2019	Medium
12:00 AM Tue Jun 1 2019	Medium

Configuration

Canvas

Display Mode

Actual Size Fit to Width

Canvas Width Canvas Height

1200 750

Background Color

#f2f4f5

Background Image

Enter URL

Drop your file here or browse...

Note: Uploaded image files can be accessed and deleted by others in your organization

Preferences

Show Export Button

Here is your customisation options for the dashboard

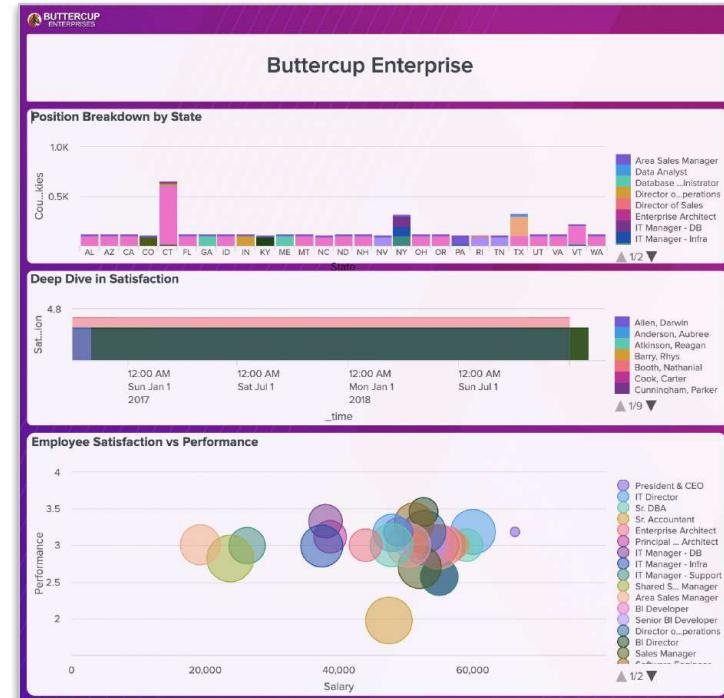


Customise Your Dashboard!

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



You Finished the Hands-on Exercises!

You made it!



There's a Lot More to Splunk

- Clustering
- Data Models
- Alerting
- Pivot
- SDKs
- APIs
- DB Connect

- Advanced Searches
- SOAR
- Machine Learning (ML)

- Splunk Stream
- Deployment Server
- Federated Search
- Metrics

- Custom Visualisations
- HTTP Event Collector (HEC)
- Data Filtering
- Transformations
- Architecture

- Report Acceleration
- Common Information Model (CIM)
- Containers
- Best Practices
- And much more...

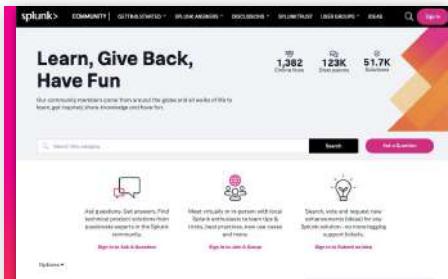


Splunk Resources

Where to go after today's workshop

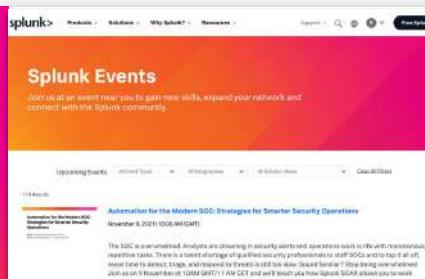
splunk>

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



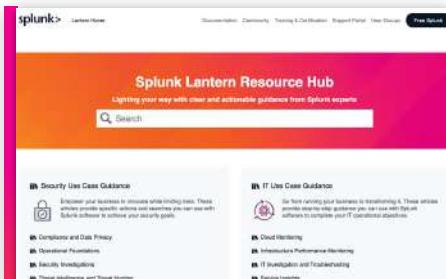
Customer Success and Education

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!



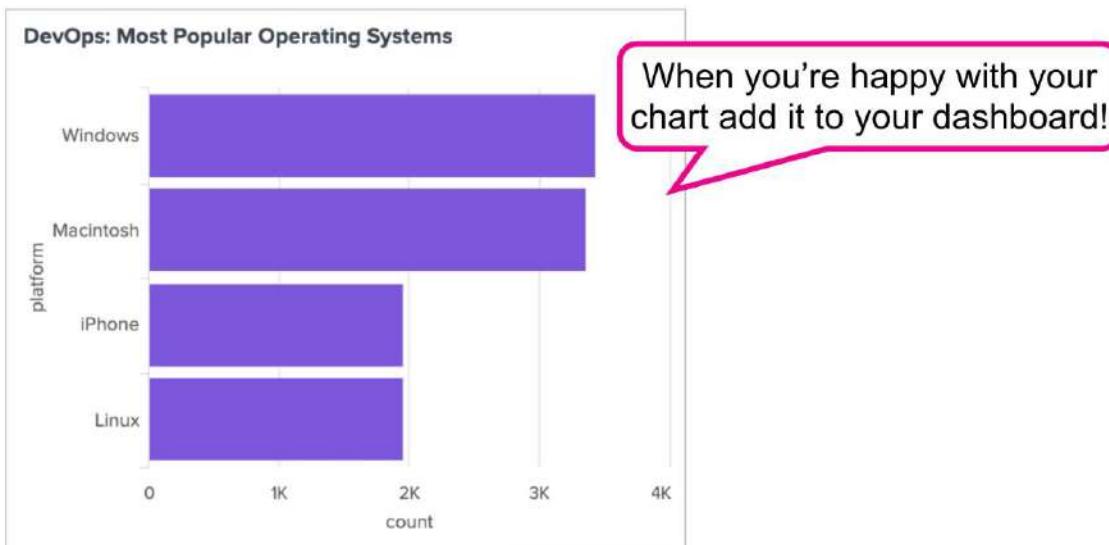
Splunk Lantern

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
```



Thank You!

