

# splunk<sup>></sup> 4rookies

Hands-On Workshop

X #Splunk4Rookies



splunk<sup>></sup>  
a CISCO company

# Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by 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.

© 2024 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

- Building digital resilience with Splunk
- Creating a Splunk app
- Adding data
- Searching and reporting
- Extracting a new field
- Using lookups
- Creating a dashboard for multiple use cases
- Splunk resources

# There's a Lot More to Splunk

Clustering  
Data Models  
Alerting  
Pivot  
SDKs  
APIs  
DB Connect

Advanced  
Searches  
SOAR  
Machine  
Learning  
AI

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

Splunk Stream  
Deployment Server  
Data filtering,  
masking and routing  
Federated Search  
Metrics

Custom  
Visualisations  
HTTP Event  
Collector (HEC)  
Transformations  
Architecture

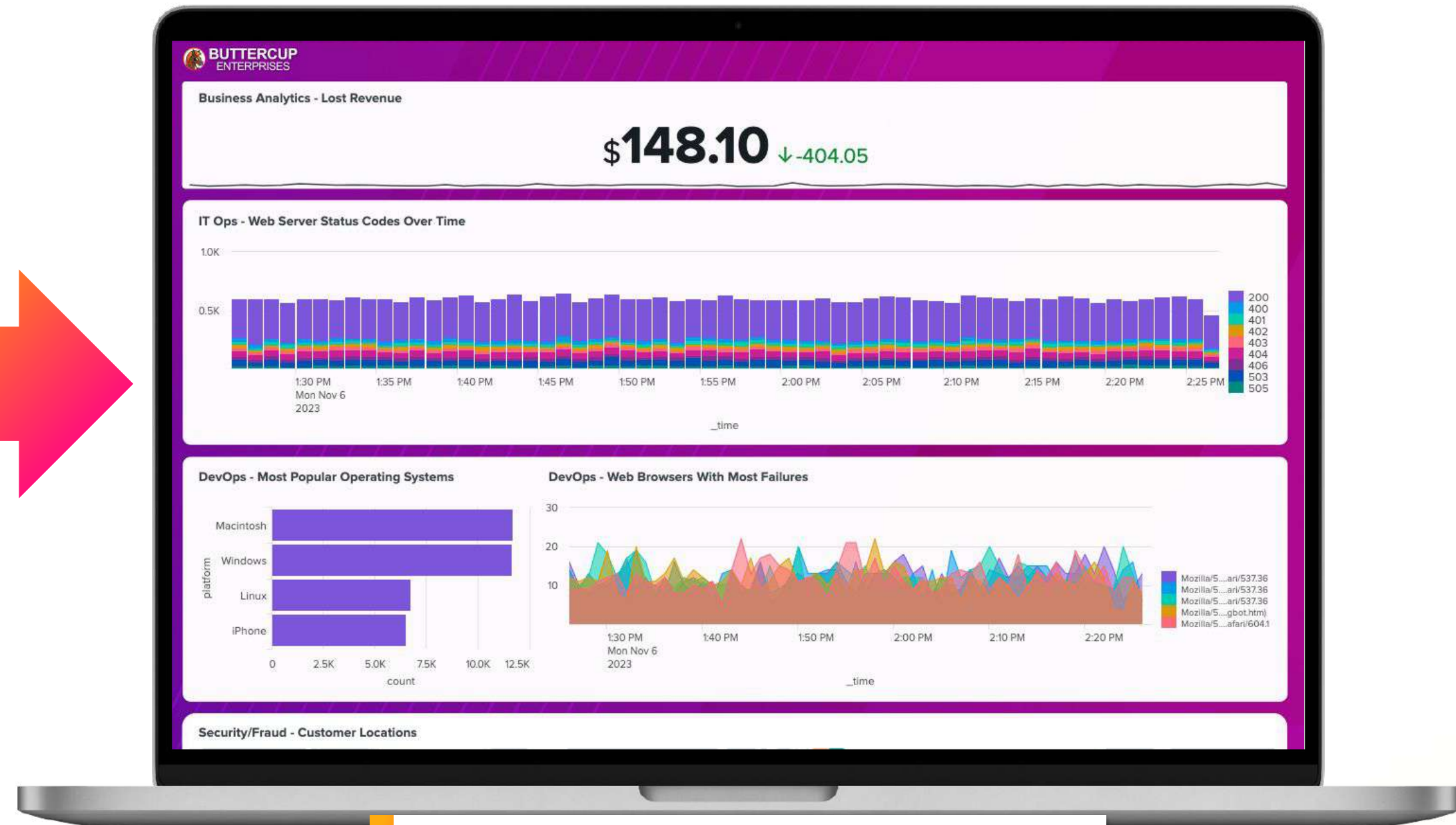
Visit <https://splunk.com/training> to learn more!



# Objective for Today



Go from messy machine data...



...to a dynamic, interactive dashboard!



# 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 the hands-on lab guide:  
<https://splk.it/S4R-Lab-Guide>  

Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:  
<https://splk.it/S4R-Attendee>

## Goal

Enroll in today's event

Home > Splunk4Rookies

Splunk4Rookies

Platform

▶ AVAILABLE



Enroll event

Request Help



**We're building  
a safer and  
more resilient  
digital world.**





# The evolving world has created new demands.



## **Downtime is detrimental**

Large companies lose \$200M/year in costs from downtime.<sup>1</sup>



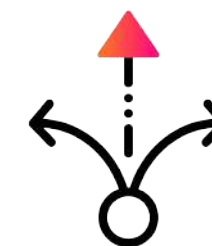
## **Cyber risk is business risk**

Cyber is now the #1 risk and a growing problem thanks to AI.<sup>2</sup>



## **Resilience is regulated**

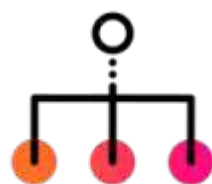
Governments have enacted stiff penalties for non-compliance.



## **Innovation velocity is essential**

Getting products to market faster is a competitive advantage.

# It's hard to be resilient.



Complex environments expand attack surface and failure points.

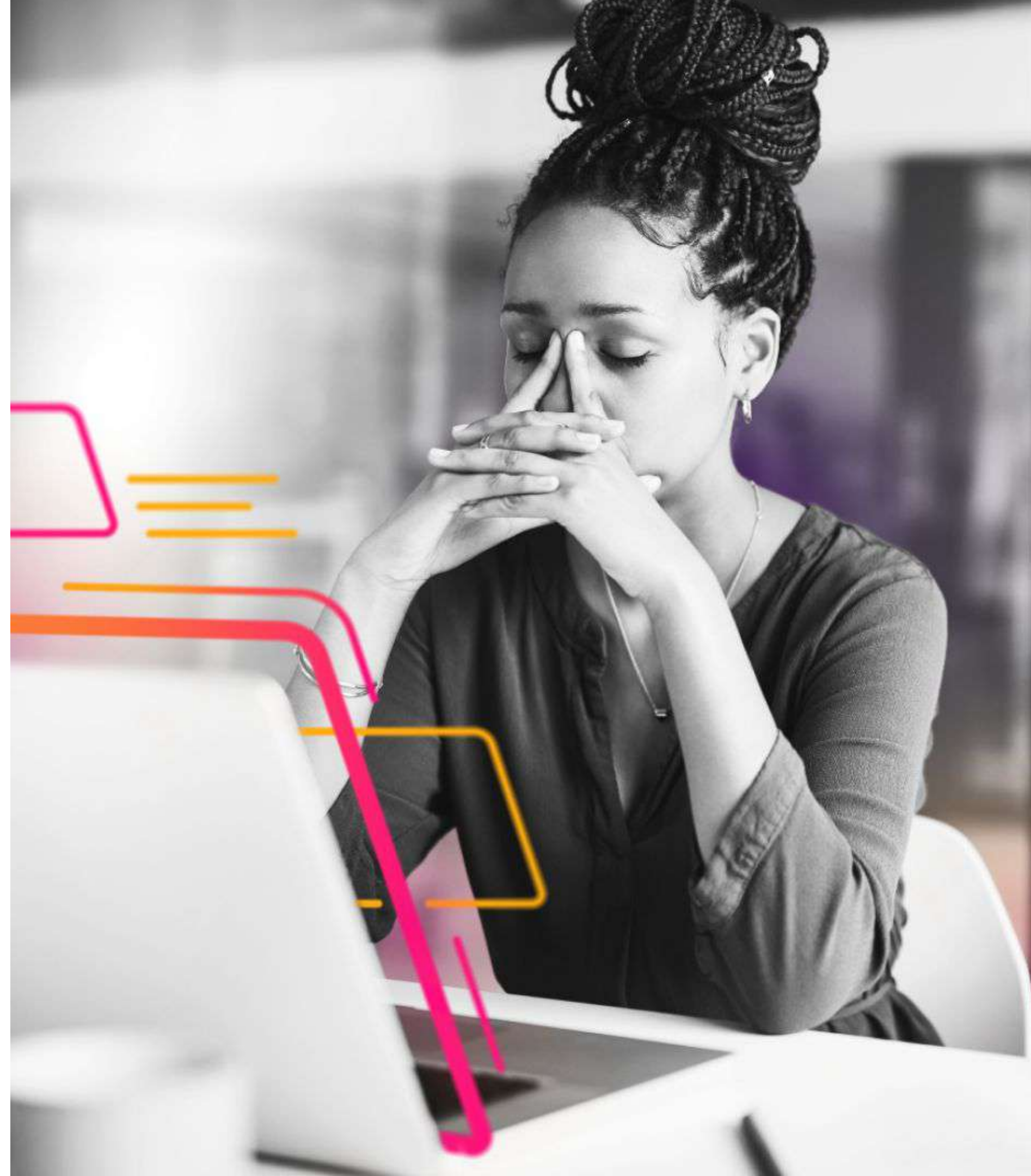


Growing data volumes sit in silos and are increasingly hard to manage.



Regulations require real-time risk assessments.

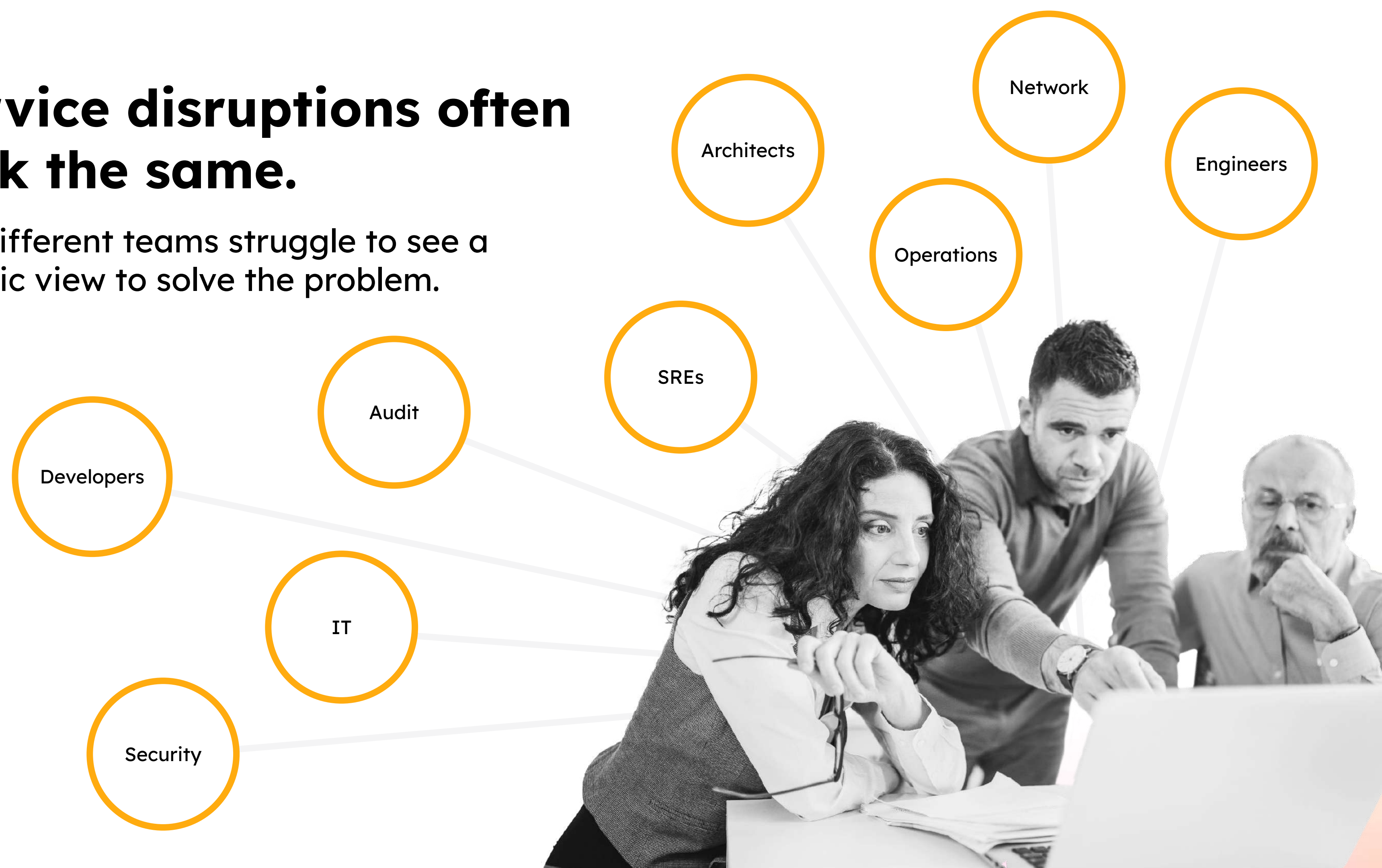
The AI era is accelerating all these challenges and creating entirely new ones.





# Service disruptions often look the same.

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



How do you prepare for and recover  
from **unexpected disruptions**?

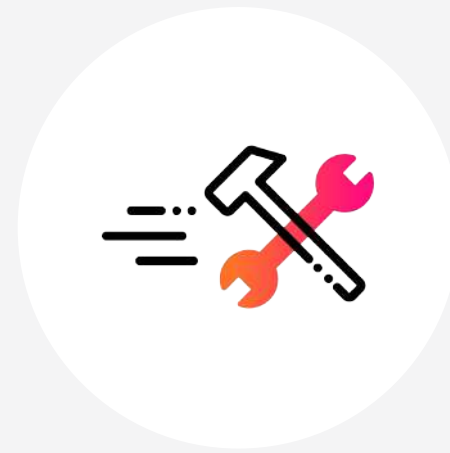


# Build digital resilience with Splunk.

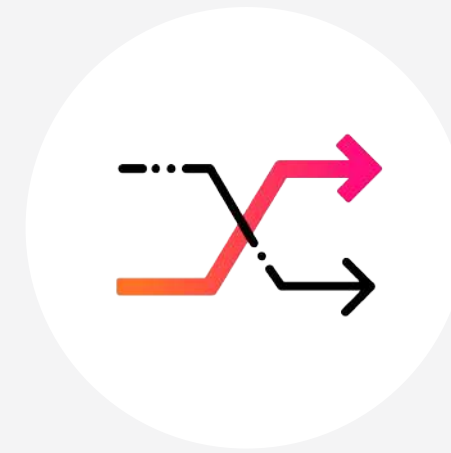
Splunk brings SecOps, ITOps and engineering together to...



Prevent major  
issues

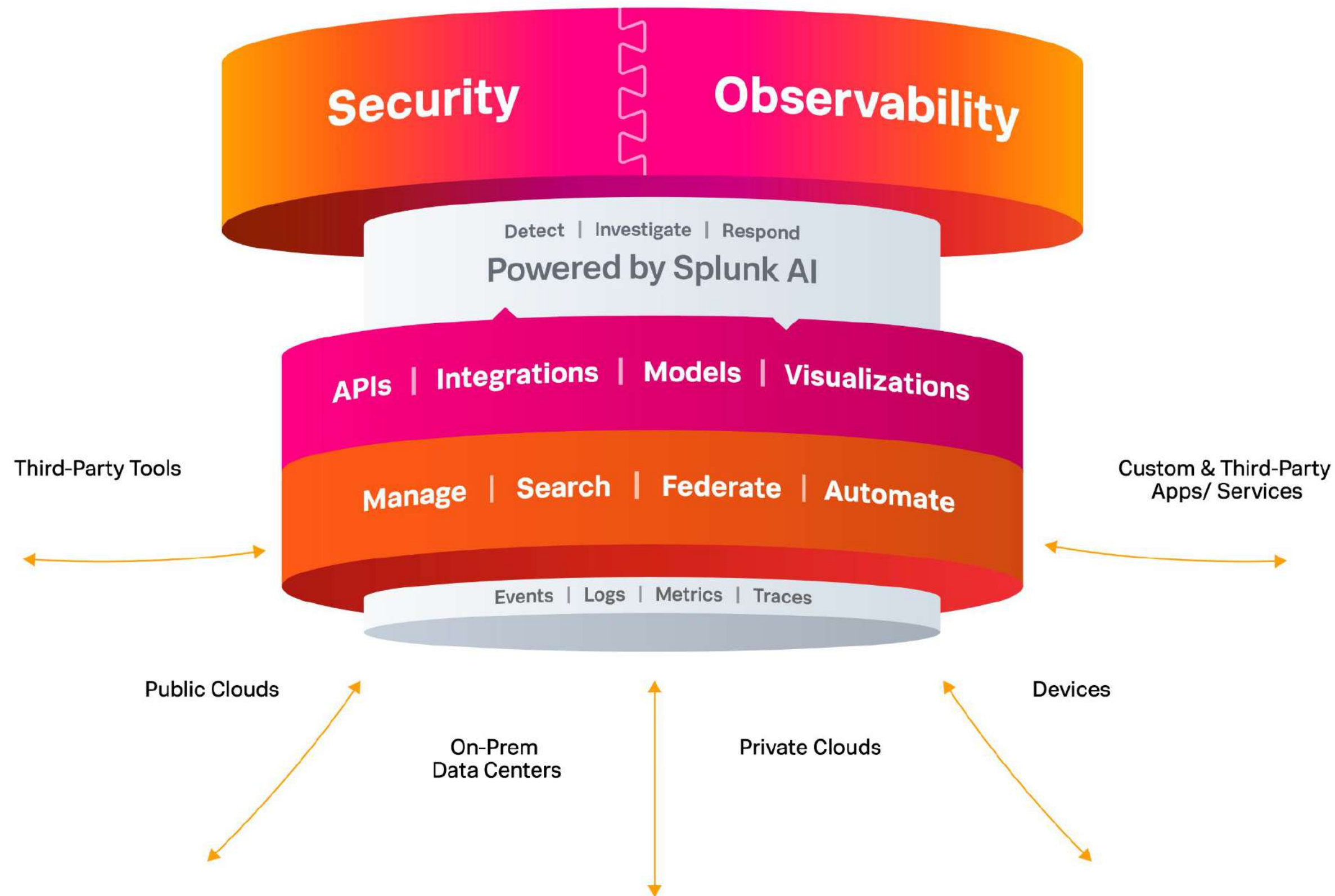


Remediate  
faster



Adapt quickly

# The Unified Security and Observability Platform





# Splunk delivers unparalleled digital resilience.

Providing **end-to-end visibility** and insights across your entire digital footprint

Powering the **SOC of the future** with unified threat detection investigation and response, enhanced with network insights

Delivering **observability for the entire enterprise** to prevent unplanned downtime across all environments

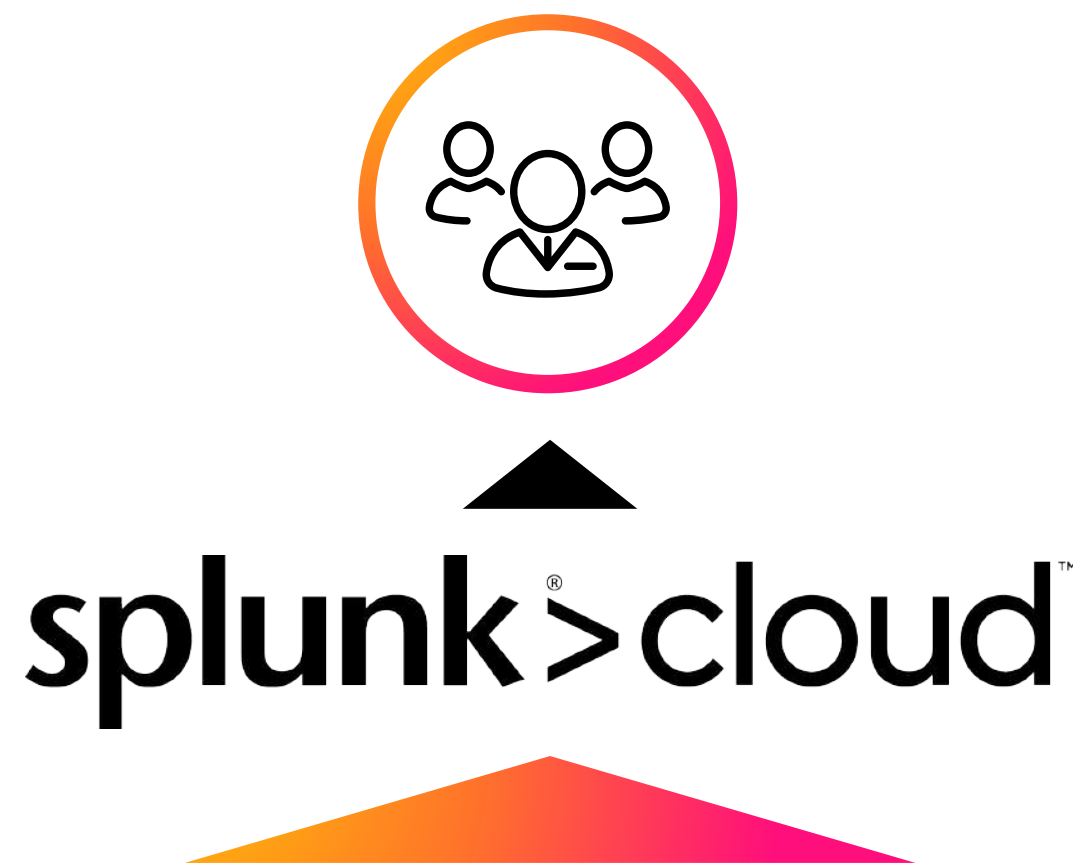
Unified by a flexible platform that provides enterprise scale data management

# Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

## 3 Simple Steps:

1. Onboard data
2. Onboard users
3. Get value from your data



- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI DSS, HIPAA, FedRAMP Moderate, DoD IL5, IRAP
- **Encryption-in-transit** - plus optional encryption-at-rest
- **Resilient infrastructure**
- **100% uptime guarantee**
- **24/7 NOC/SOC support team**

## Flexible options for data collection and forwarding



Splunk Cloud Service Description: <https://splk.it/SplunkCloudServDesc>



# What is a Splunk Universal Forwarder?

- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
  - Buffering / guaranteed delivery
  - Encryption
  - Compression
  - Load balancing
  - And more!
- Very small footprint
- Just forwards data – no parsing beforehand!



# Machine data is valuable not complex!

```
10.2.1.35 64.66.0.20 - - [17/Jan/2024  
16:21:51] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?  
product_id=CC-P3-BELKIN-BLK_BT00TH_HFREE"  
"Mozilla/5.0 (Linux; Android 12.0.0;  
FR-fr; SM-S901B Build/S908EXXU2BVJA)  
AppleWebKit/537.36 Chrome/114.0.5735.131  
Mobile Safari/537.36" 954
```

# Marketing Use Case

Show the top  
products viewed  
by language

IP of client

10.2.1.35 **64.66.0.20** - - [17/Jan/2024

16:21:51] "GET

/product.screen?product\_id=CC-P3-BELKIN-

SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP

1.1" 503 865

Product viewed

"http://shop.splunk.com/product.screen?

product\_id=**CC-P3-BELKIN-BLK\_BTTOOTH\_HFREE**"

"Mozilla/5.0 (Linux; Android 12.0.0;

**FR-fr**; SM-S901B Build/S908EXXU2BVJA)

Language setting  
of browser

Android 12.0.0 (S908EXXU2BVJA) AppleWebKit/537.36 Chrome/114.0.5735.131

Mobile Safari/537.36" 954



# DevOps Use Case

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

```
10.2.1.35 64.66.0.20 - - [17/Jan/2024
16:21:51] "GET
/product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP
1.1" 503 865
"http://shop.splunktel.com/product.screen?
product_id=CC-P3-BELKIN-SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9"
"Mozilla/5.0 (Linux; Android 12.0.0;
FR-fr; SM-S901B Build/S908EXXU2BVJA)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.131
Mobile Safari/537.36" 954
```

Platform

Handset model

# IT Ops Use Case

Which web pages  
are generating the  
most errors?

IP of web server

IP of client

10.2.1.35 64.66.0.20 - - [17/Jan/2024

16:21:51] "GET

Page requested

/product.screen?product\_id=CC-P3-BELKIN-SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP

1.1" 503 865

ID of web session

HTTP  
status code

Size of objects  
returned to client

"Mozilla/5.0 (Linux; Android 12.0.0;

Web browser

FR-1201B Build/S908EXXU2BVJA)

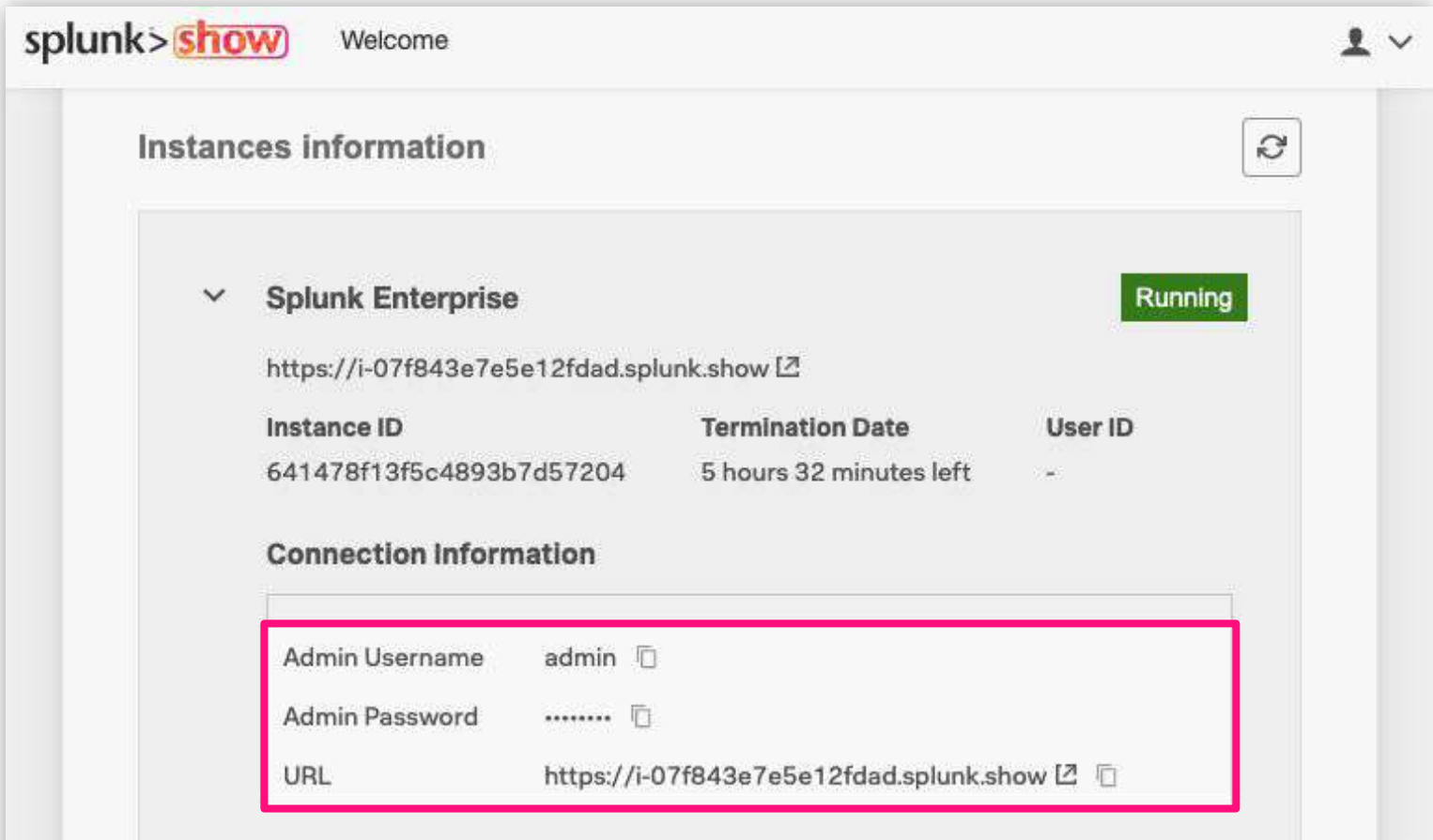
AppleWebKit/537.36 Chrome/114.0.5735.131

Mobile Safari/537.36" 954

# 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



# Apps and Add-ons

- 2100+ 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**





# Create an App and Add Some Data

## Tasks

1. Create a new app
2. Monitor a directory: `/var/log/weblogs`
3. Select a source type: `access_combined`
4. View your data in Splunk

### Select source

▼ var

- > backups
- > cache
- > crash
- > lib
- > local
- > lock
- ▼ log
  - > apt
  - > audit
  - > dist-upgrade
  - > fsck
  - > landscape
  - > squid3
  - > unattended-upgrades
  - > upstart
  - > weblogs
  - alternatives log

### Reminder

Download the [lab guide](#) for step-by-step instructions!

# Open your app and have a play!

The currently selected app

Time picker – choose your search time range

Search bar – type anything here to search

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time

The screenshot shows the Splunk web interface. At the top, the navigation bar includes 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'App: Splunk 4 Rookies' dropdown is highlighted. Below the navigation bar, the 'New Search' section contains a search bar with the query 'action=purchase status=200'. To the right of the search bar is a time picker set to 'Last 60 minutes'. Below the search bar, there is an 'Event histogram' showing a bar chart of event frequency over time. Below the histogram, a table of raw event data is displayed. The table has columns for 'Time' and 'Event'. The first three rows of data are visible. To the left of the table, a sidebar shows 'INTERESTING FIELDS' with a list of metadata fields extracted at search time, including 'source', 'sourcetype', 'action', 'bytes', 'category\_id', 'clientip', 'date\_hour', 'date\_mday', 'date\_minute', 'date\_month', 'date\_second', and 'date\_weekday'.

i	Time	Event
1	15/05/2018 08:49:08.127	12.130.60.5 - - [15/May/2018 08:49:08:127] "GET /cart.do?action=purchase&itemId=EST-20&product_id=RP-SN-01&JSESSIONID=SD1SL2FF10" 200 629 "http://www.myflowershop.com/category.screen?category_id=GIFTS" "Googlebot/2.1 ( http://www.googlebot.com/bot.html) " 873
2	15/05/2018 08:48:54.193	12.130.60.4 - - [15/May/2018 08:48:54:193] "POST /product.screen?product_id=FL-DLH-02&JSESSIONID=SD7SL2FF3ADFF8 HTTP 1.1" 200 629 "http://www.myflowershop.com/cart.do?action=purchase&itemId=EST-20&product_id=FL-DLH-02" "Googlebot/2.1 ( http://www.googlebot.com/bot.html) " 256
3	15/05/2018 08:48:46.196	203.92.58.136 - - [15/May/2018 08:48:46:196] "GET /cart.do?action=purchase&itemId=EST-15&product_id=K9-BD-01&JSESSIONID=SD1SL10FF1ADFF7 HTTP 1.1" 200 3031 "http://www.myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 897



# Start Exploring Your Data

## Example searches:

503 purchase

Find all events that contain the words “503” and “purchase”

503 pur\*

Find all events containing “503” and words beginning with “pur”

503 (purchase OR addtocart)

Boolean operators (AND/OR/NOT) – must be UPPERCASE!

status=503 action=purchase

Use *fieldname = value* to ensure accurate search results

**How would you find events with a status code of 200 that are NOT purchase events?**

status=200 NOT action=purchase

status=200 action!=purchase

# Splunk's Search Processing Language (SPL)

Search Terms

Commands

index=main action=purchase | stats count by status | rename count as "number of events"

Pipe character: Output of left is input to right

Functions

e.g. index=main action=purchase

| stats count by status | rename count as "number of events"

i	Time	Event
>	16/01/2024 11:03:08.000	27.102.0.0 - - [16/Jan/2024 11:03:08] "GET /cart.do?action=view&product_id=MCB-5&JSESSIONID=SD6SL6FF10ADFF3 HTTP 1.1" 200 3453 "http://www.buttercupenterprises.com/product.screen?product_id=DFS-2" "Mozilla/5.0 (Linux; Android 12.0.0; SM-A546B Build/A546BXXU1AWB7) AppleWebKit/537.36 Chrome/114.0.5735.61 Mobile Safari/537.36 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 388 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	131.178.233.243 - - [16/Jan/2024 11:03:08] "POST /product.screen?uid=5ac99574-edc7-417d-ad38-df91f883d280&product_id=PP-5&JSESSIONID=SD7SL3FF6ADFF8 HTTP 1.1" 200 2311 "http://www.buttercupenterprises.com/product.screen?product_id=PP-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 Chrome/107.0.5304.122 Safari/537.36" 703 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.4 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=881e7945-8fd6-4a55-94c1-880f668ea048&product_id=BW-3&JSESSIONID=SD1SL6FF5ADFF6 HTTP 1.1" 400 3158 "http://www.buttercupenterprises.com/product.screen?product_id=BS-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 Version/15.0 Mobile/19A346 Safari/602.1" 602 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.130.60.5 - - [16/Jan/2024 11:03:08] "GET /product.screen?uid=8a9dff3-2e4f-4ea6-aef6-088cdb412b8e&product_id=BW-3&JSESSIONID=SD8SL1FF4ADFF1 HTTP 1.1" 505 1310 "http://www.buttercupenterprises.com/product.screen?product_id=CH-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/113.0.5672.92 Safari/537.36" 977 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined

status	count
200	850
400	81
401	76
402	50
403	57

status	number of events
200	850
400	81
401	76
402	50
403	57

Want to know more? Check out:  
Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>  
Search manual: <https://splk.it/SplunkSearchManual>

# Today's Scenario

## 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

- You are one of the chosen few: a Splunk power user!
- Your responsibility is to provide insights to users throughout the company
- The teams you support include:
  - **IT Operations**
  - **DevOps**
  - **Business Analytics**
  - **Security and Fraud**



**BUTTERCUP**  
ENTERPRISES

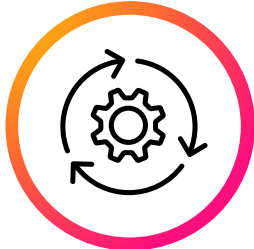


# What Does the Business Want to See?

We need to create a dashboard with four views:



**IT Operations team:** Investigate successful versus unsuccessful web server requests over time



**DevOps team:** Show the most common customer operating systems and which web browsers are experiencing the most failures



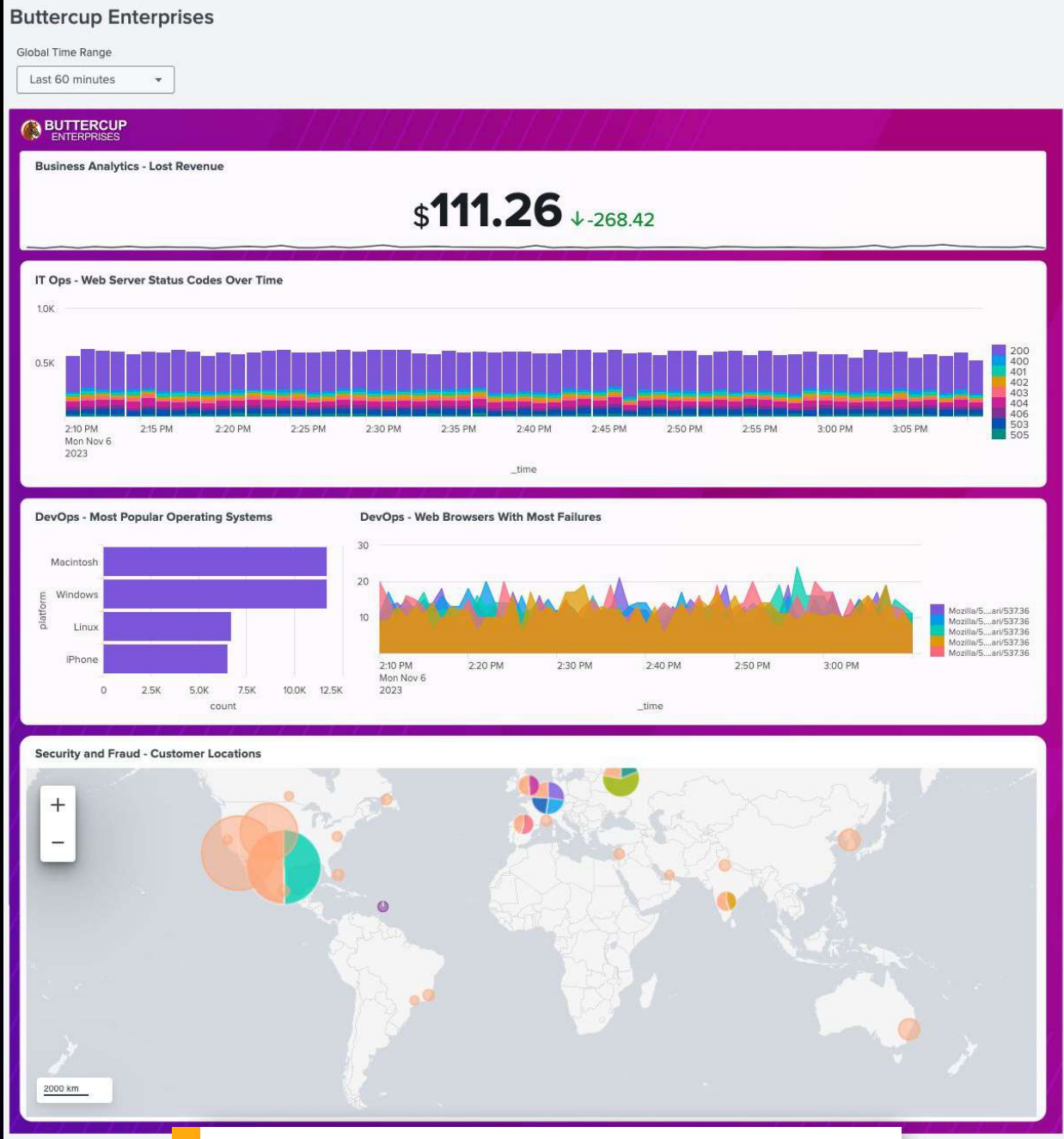
**Business Analytics team:** Show lost revenue from the Buttercup Enterprises website



**Security and Fraud team:** Show website activity by geographic location



**Buttercup Enterprises:** Add all of this to a single dashboard with a custom background image



This is the dashboard we're aiming for!



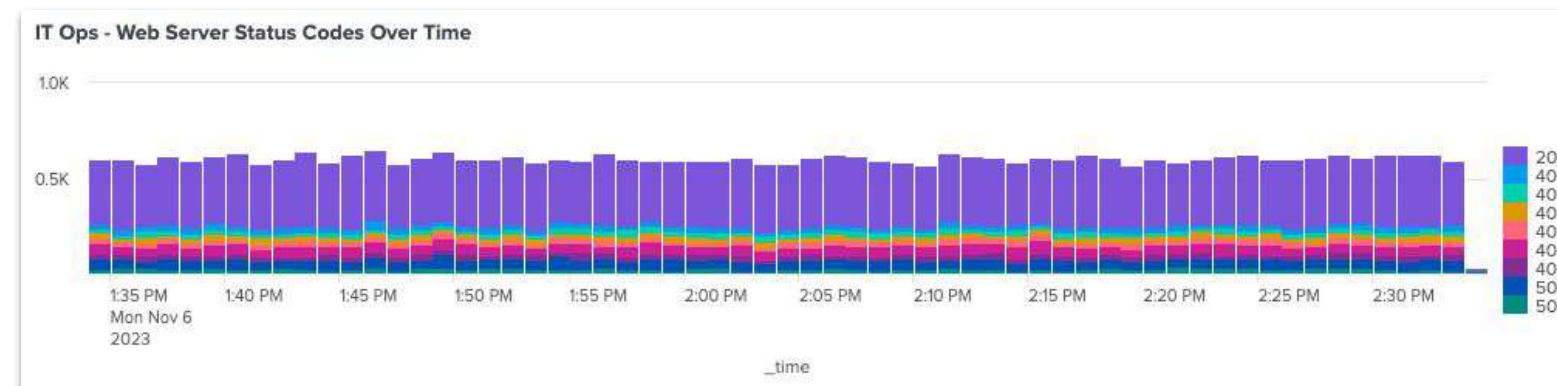
# IT Operations Team

Investigate successful versus unsuccessful web server requests over time

## Tasks

1. Show successful vs unsuccessful web server requests over time
2. Use a stacked column chart visualisation
3. Add your chart to a new dashboard
4. Choose 'Dashboard Studio' and use 'Absolute' layout mode to allow for future dashboard customisation!

## Goal



# Splunk Dashboards

## Classic Dashboards (Simple XML)



- Easy to deploy a **wide variety of visualisations**, but **hard to craft a story**
- **Flexible and extensible**, but **time consuming** to build something truly beautiful (e.g. custom JS, CSS)
- **PDF export loses look/feel** of dashboard

## Dashboard Studio



- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images, text boxes, shapes, lines and icons**, with **intact PDF export**
- **No custom code** required



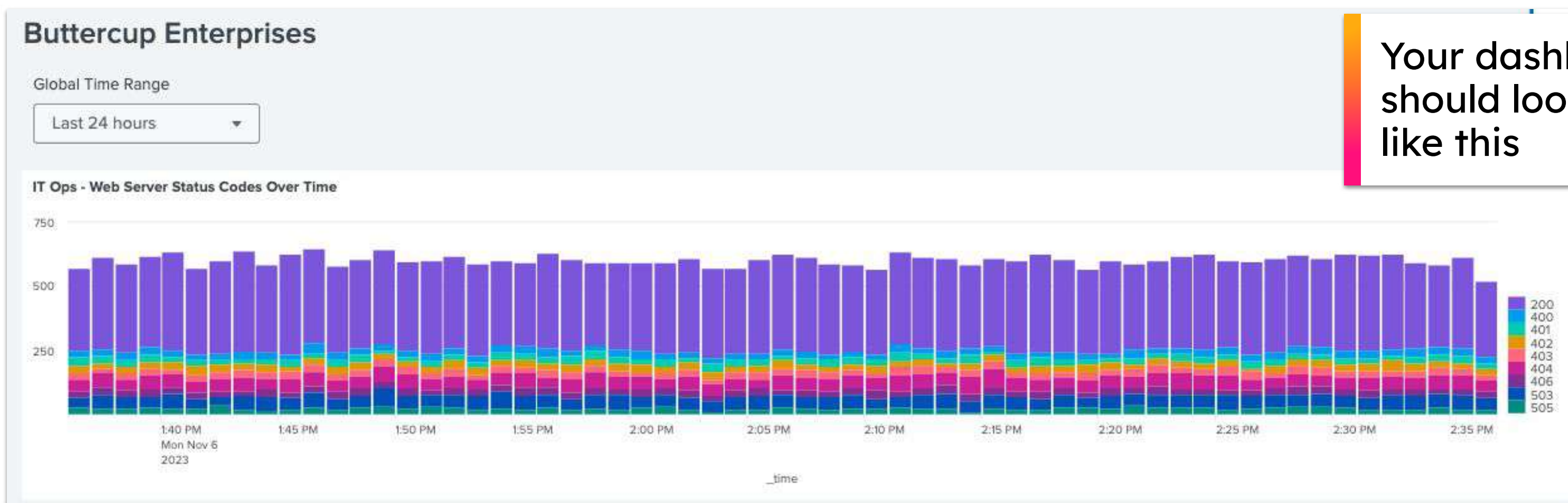


# IT Operations Team

Investigate successful versus unsuccessful web server requests over time

## Solution:

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

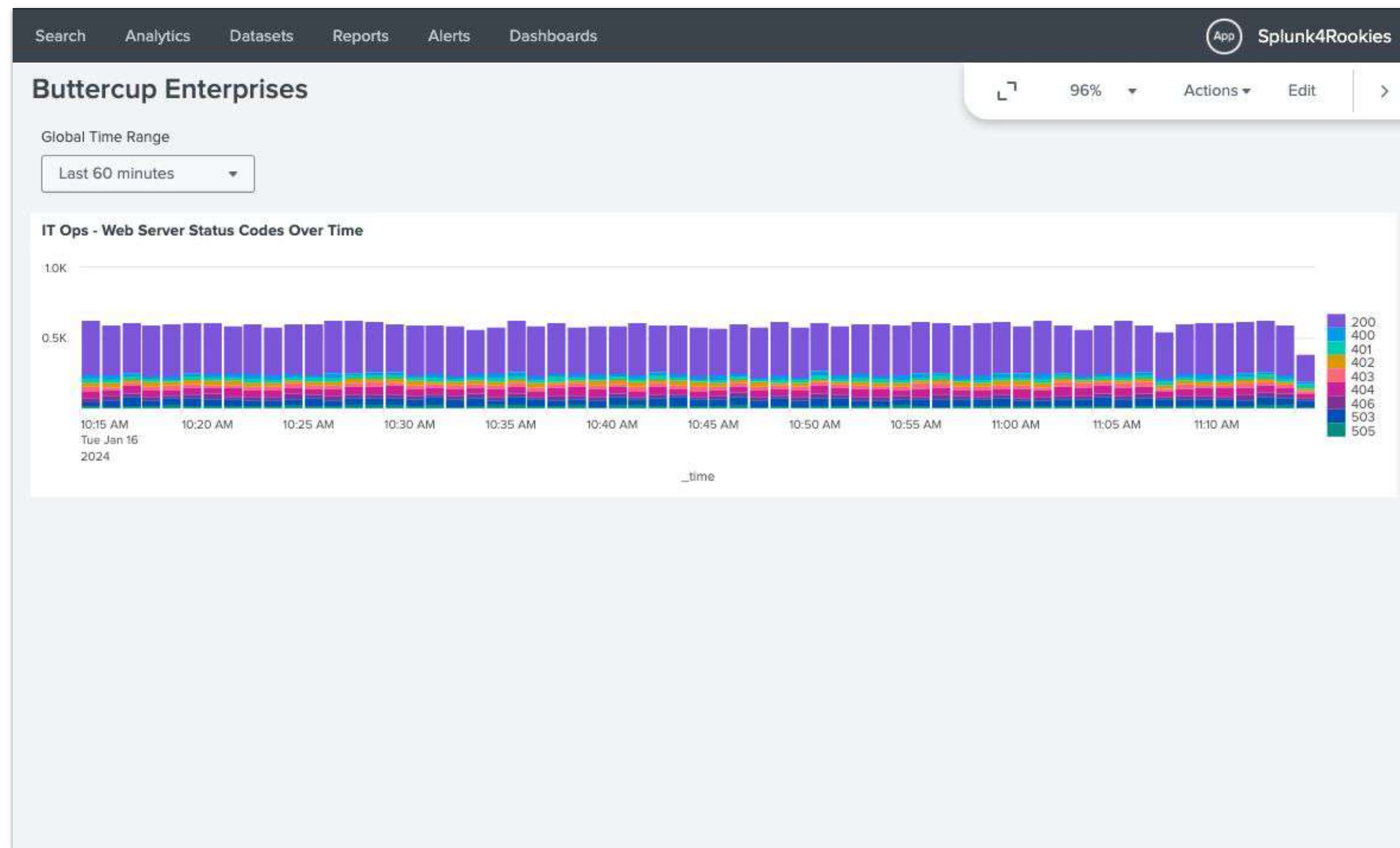


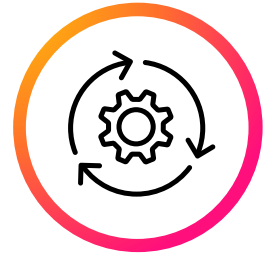
Your dashboard panel should look something like this

# Your dashboard so far...



IT Operations team





# DevOps Team

Show the most common customer operating systems and which web browsers are experiencing the most failures

## Step 1: Show the most common customer operating systems

### New Search

index=main sourcetype=access\_combined

Search for all web server events

i	Time	Event
>	03/04/2023 15:10:51.000	1.19.11.11 - - [03/Apr/2023 15:10:51] "GET /cart.do?action=purchase&product_id=ZSG-2&JSESSIONID=SD2SL10FF10ADFF9 HTTP 1.1" 200 1474 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 Chrome/54.0.2840.98 Safari/537.36" 313 host = Domain sourcetype =

We can see operating system information in our events but we don't currently have a field we can use to report on



# Extracting a New Field

1. Click on the arrow to expand an event

i	Time	Event
▼	03/04/2023 15:10:51.000	1.19.11.11 - - ADF9 HTTP 1.1 (Macintosh; In

Event Actions ▼

Build Event Type

Extract Fields

2. Click on **Event Actions**

3. Click on **Extract Fields**

(.\*?)

**Regular Expression**

Splunk Enterprise will extract fields using a Regular Expression.

4. Click on **Regular Expression**

Extract Fields

Select Method

Select Fields

Validate

Save

Next >

5. Click **Next**

## Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

89.167.143.32 - - [04/Apr  
6&JSESSIONID=SD8SL4FF2ADF  
"Mozilla/5.0 (Macintosh;

Extract

Field Name platform

Sample Value Macintosh

Add Extraction

6. Highlight the part of the event that is of interest

7. Give the new field a name, lowercase is recommended



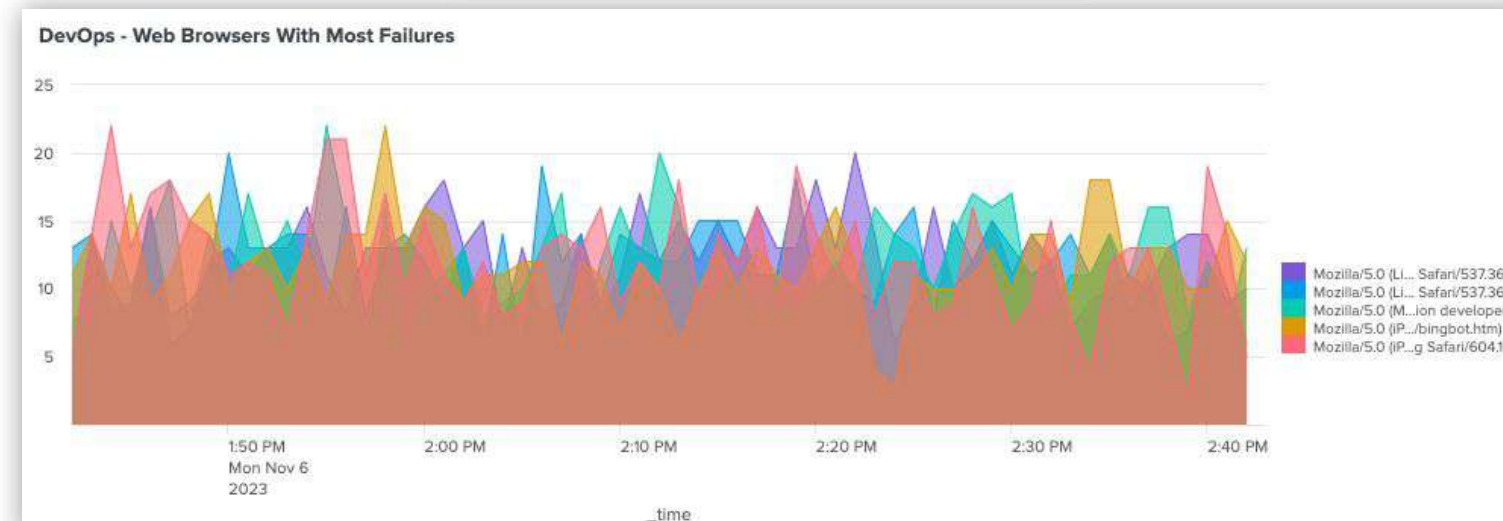
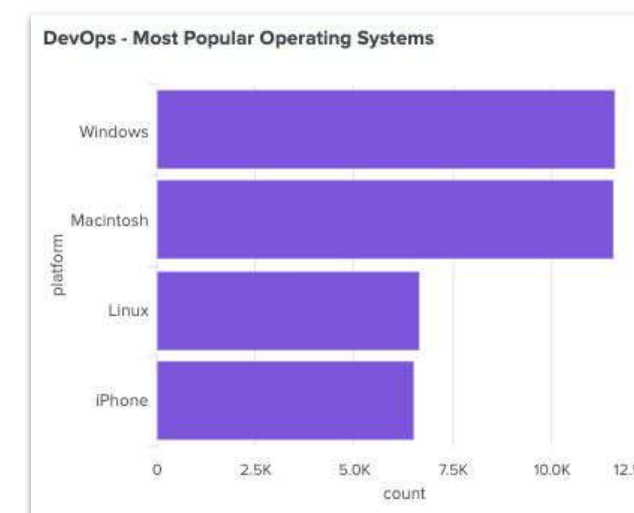
# DevOps Team

Show the most common customer operating systems and which web browsers are experiencing the most failures

## Tasks

1. Extract a new **platform** field
2. Show the top values using a bar chart visualisation
3. Create an area chart showing the top 5 web browsers that are experiencing the most failures over time
4. Add your charts to your existing dashboard

## Goal



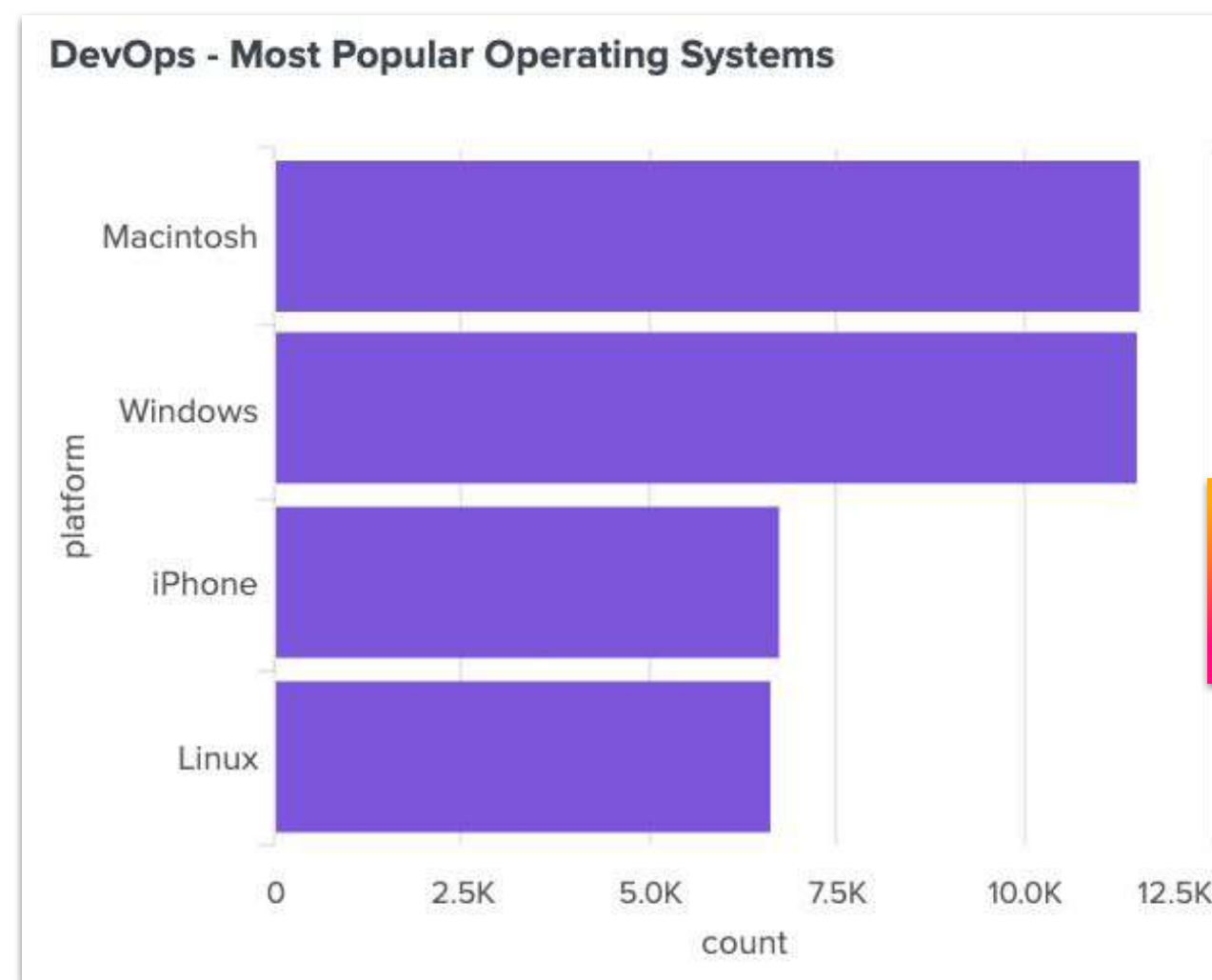


# DevOps Team

Show the most common customer operating systems

## Solution:

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



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



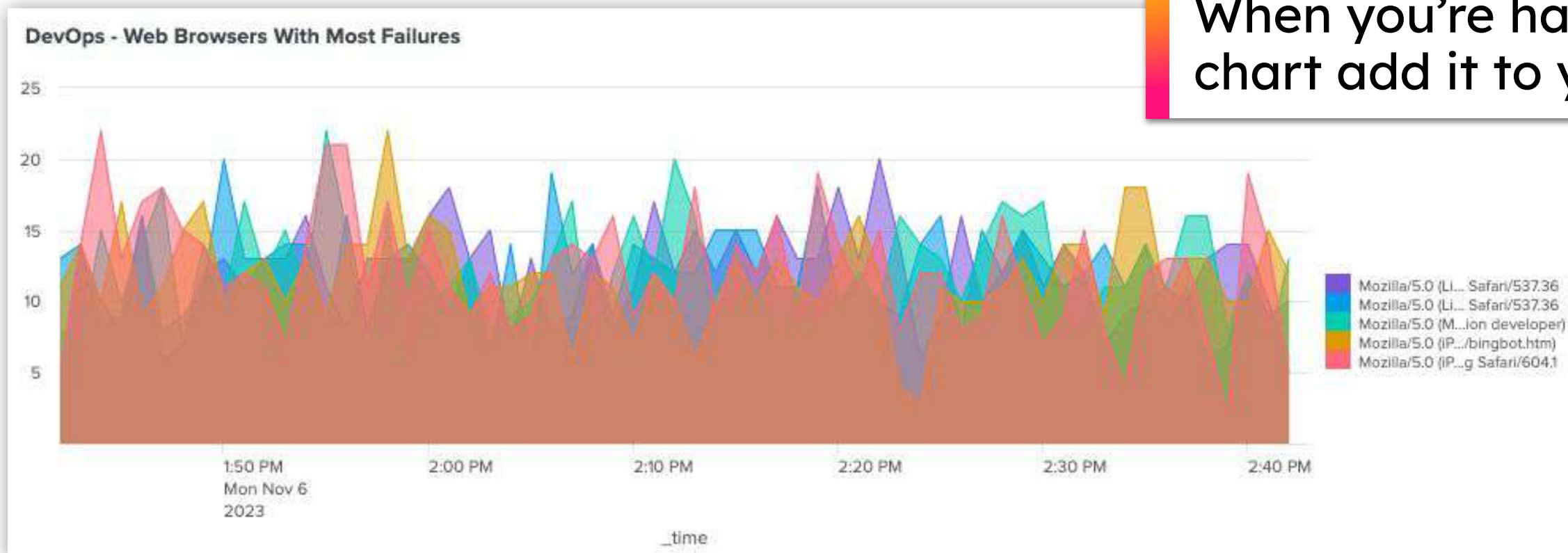


# DevOps Team

Create a graph showing the top 5 web browsers that are experiencing the most failures over time

## Solution:

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



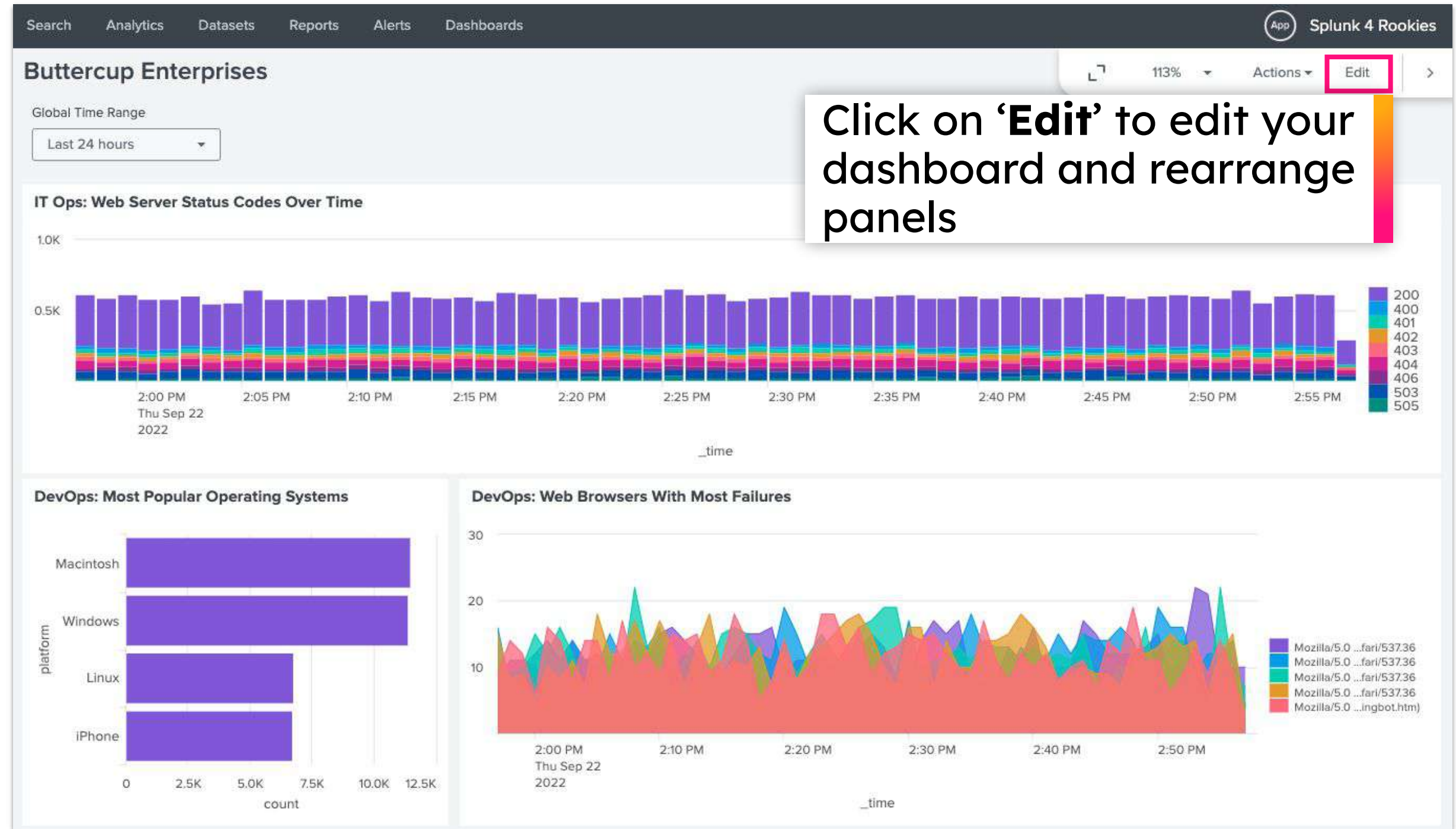
# Your dashboard so far...



IT Operations team



DevOps team



# Working with statistics? Use stats and timechart

## Usage:

```
<your search> | stats <function> <by clause>  
<your search> | timechart <function> <by clause>
```

## Examples:

```
index=main sourcetype=access_combined  
| stats distinct_count(clientip) by status
```

status	distinct_count(clientip)
200	67
400	67
401	67
402	

Calculates statistics based on fields in your events

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



Creates a time series chart with a corresponding table of statistics

Want to know more? Check out:  
Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>





# Business Analytics Team

Show lost revenue from the website

Fields extracted from events by Splunk:

# date_second 60	
a date_wday 1	
# date_year 1	
a date_zone 1	
a file 2	
a ident 1	
a index 1	
a JSESSIONID 100+	
# linecount 1	
a method 2	
# other 100+	
a platform 4	
a product_id 10	
a punct 2	
a referer 10	
a referer_domain 1	
a req_time 100+	
a splunk_server 1	
# status 9	
# timeendpos 8	
# timestartpos 8	
a uid 100+	
a uri 100+	
a uri_path 2	
a uri_query 100+	

product\_id

10 Values, 100% of events

Reports

Top values

Top values by time

Events with this field

Top 10 Values	Count	%
DFS-2	3,636	10.134%
MCB-6	3,633	10.126%
BW-3	3,624	10.101%
BS-2	3,609	10.059%
MCB-5	3,603	10.042%
WPSS-2	3,602	10.04%
MCF-3	3,594	10.017%
PP-5	3,554	9.906%
CM-1	3,545	9.881%
ZSG-2	3,478	9.694%

External CSV file:

category	product_id	product_name	product_price
Books	ZSG-2	Zombie Survival Guide	15.21
Clothing	CM-1	Costume- ManHawk	97.5
Gifts	DFS-2	Double Fudge Sundae	22.75
Gifts	PP 5	Pony Potpourri	9.99
Clothing	BW-3	Batguy Watch	9.99
Gifts	WPSS-2	Waterproof Scratch and Sniff	4.99

We have 'product\_id' in our data, but no price information!

This is the information we need!

# Verify That the Lookup File Exists

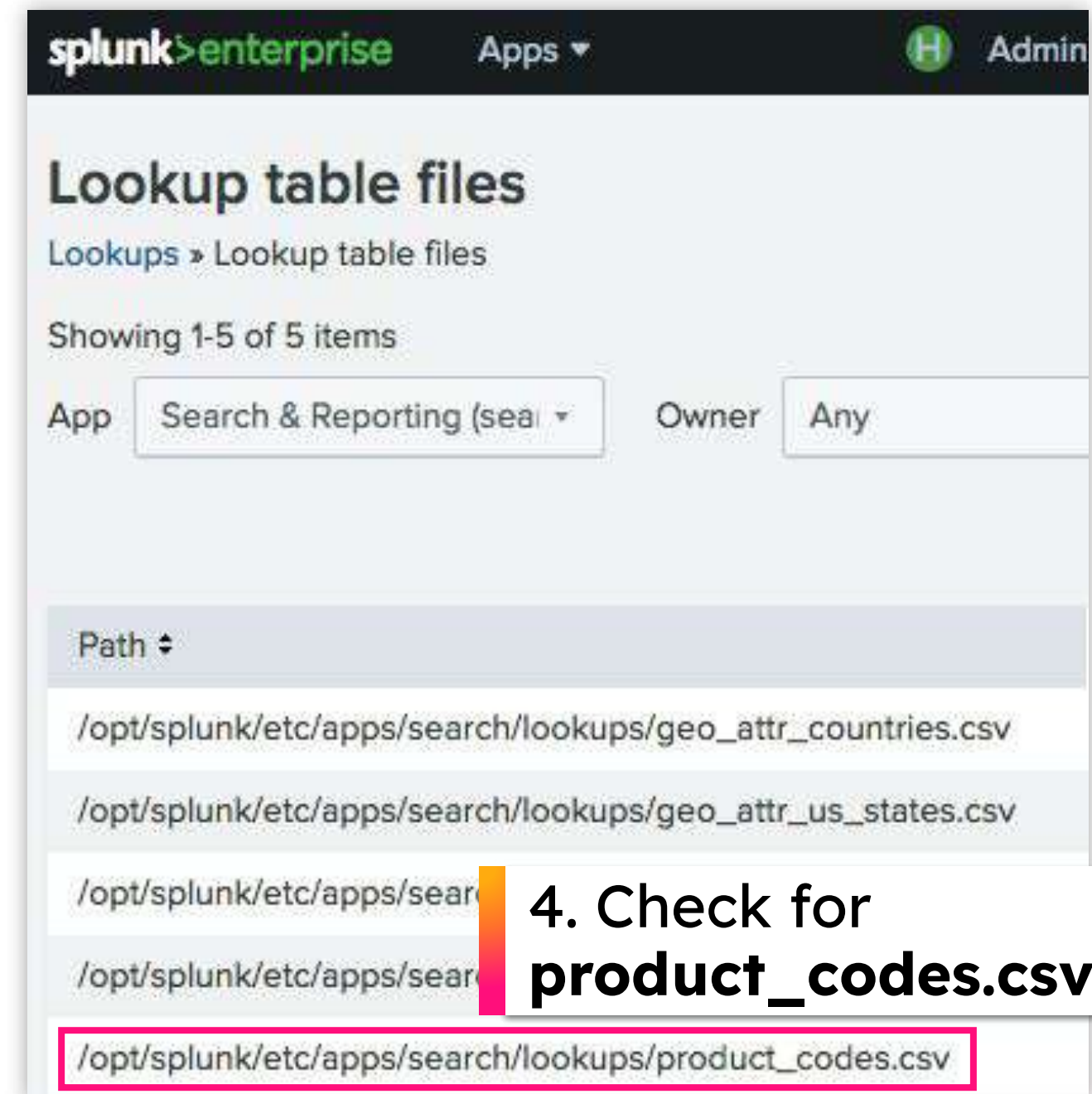
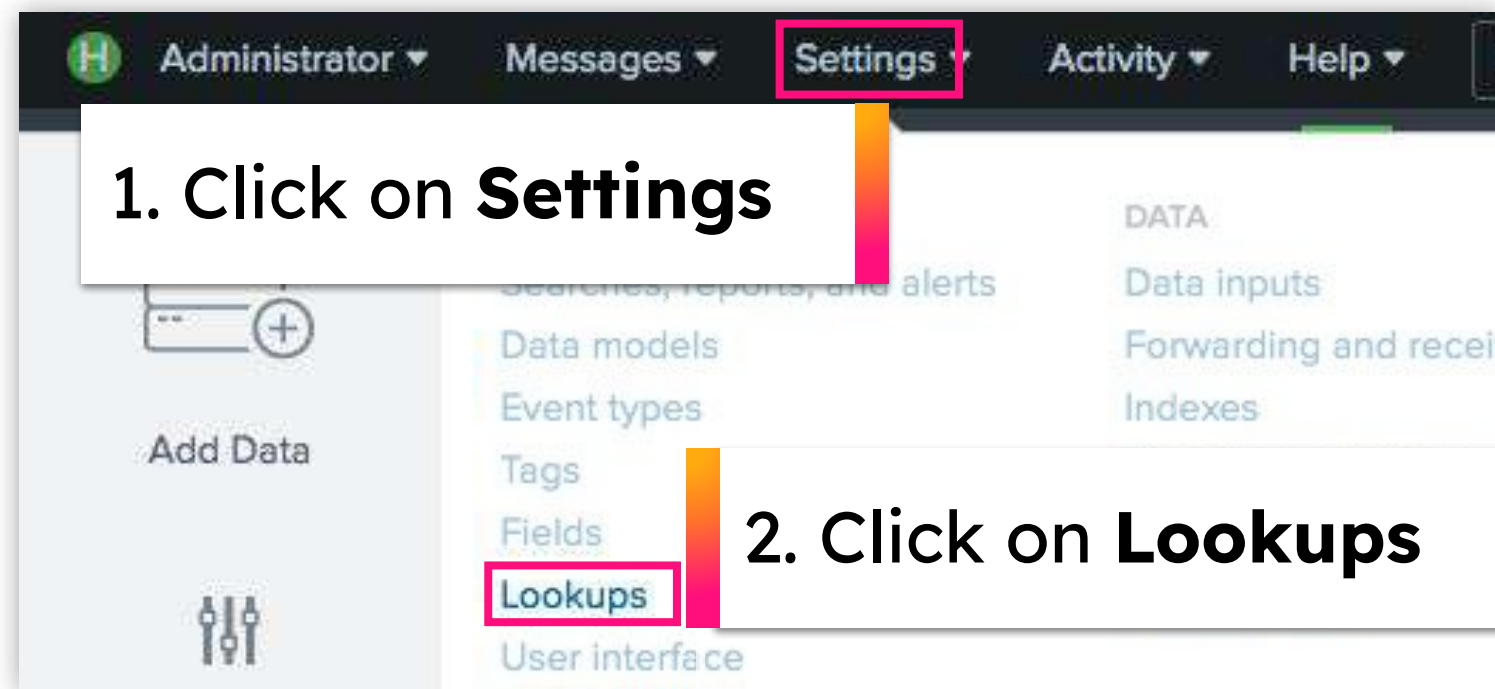
A lookup file has already been uploaded for you!

1. Click on **Settings**

2. Click on **Lookups**

3. Click on **Lookup table files**

4. Check for  
**product\_codes.csv**



# Enriching Data with the **lookup** Command

## Usage:

```
<your search> | lookup product_codes.csv product_id
```



The **lookup** command retrieves additional fields from the lookup file

The screenshot shows the Splunk interface with the following elements:

- Format Timeline** and **Zoom Out** buttons at the top.
- product\_price** field selected, showing **7 Values, 97.743% of events**.
- Reports** section with options: **Average over time**, **Top values**, **Events with this field**, and **Avg: 22.44126635873749**.
- SELECTED FIELDS** list with the following items (highlighted with red boxes):
  - `a category 3`
  - `a host 1`
  - `a product_name 10`
  - `# product_price 7` (highlighted in blue)
  - `a source 3`





# Business Analytics Team

Show lost revenue from the website

## Tasks

1. Use the `lookup` command to enrich the events with price data from our lookup file
2. Show lost website revenue using a Single Value visualisation
3. Add your visualisation to your existing dashboard

## Goal

Business Analytics - Lost Revenue

**\$35.69** ↓ -199.03





# Business Analytics Team

Show lost revenue from the website

## Solution:

```
index=main sourcetype=access_combined action=purchase status>=400  
| lookup product_codes.csv product_id  
| timechart sum(product_price)
```

Business Analytics - Lost Revenue

**\$35.69** ↓ -199.03



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

# Your dashboard so far...



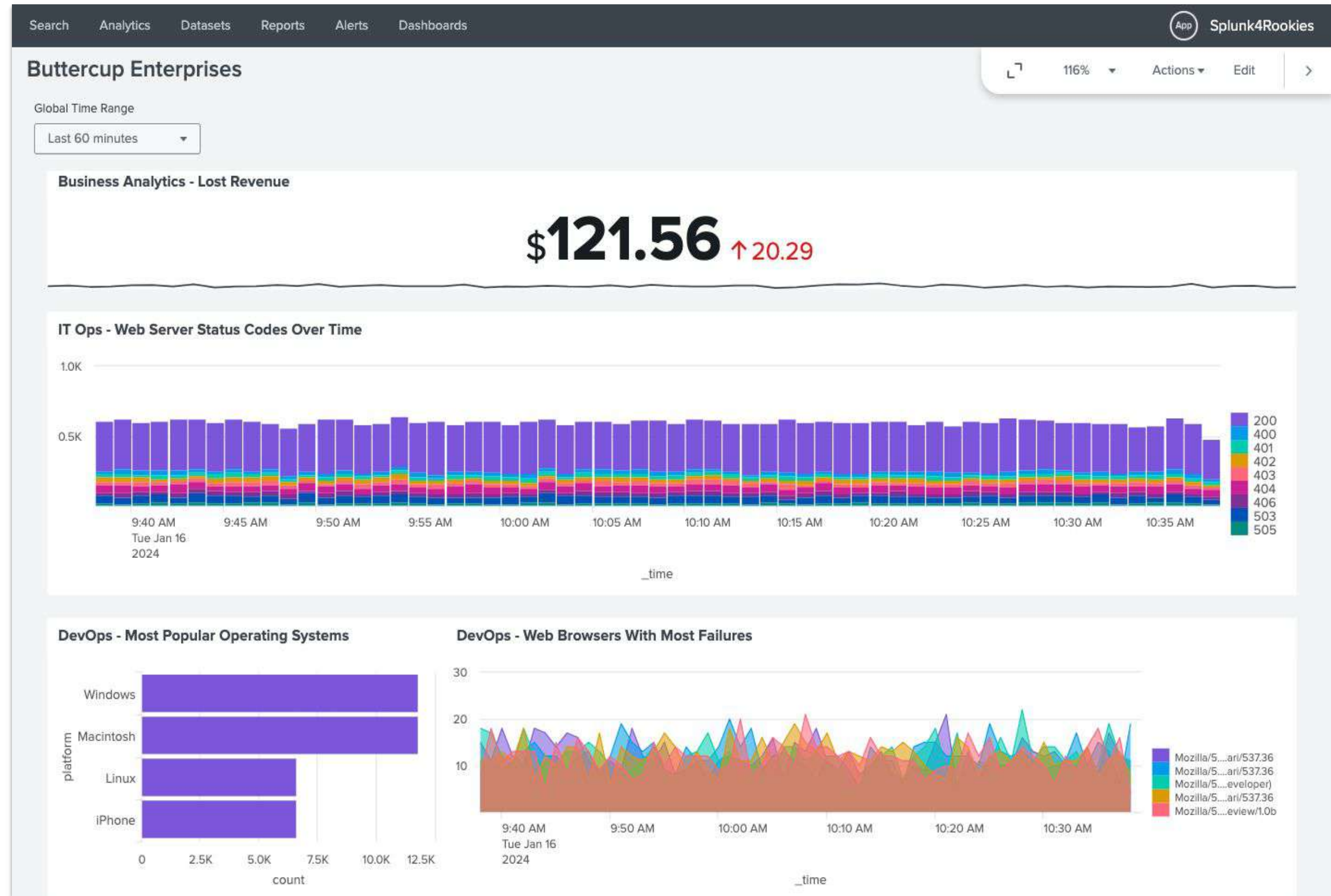
IT Operations team



DevOps team



Business Analytics team





# Obtaining Location Information with the **iplocation** and **geostats** Commands

## Usage:

```
<your search> | iplocation clientip | geostats count by <field>
```

The name of a field in your data that contains IP addresses

Generates the 'tiles' that will be rendered on the map when visualised

Split your results by a specific field for more detailed analysis

Enriches IP data on-the-fly with location data

```
a City 54  
a Country 23  
# lat 56  
# lon 56  
a Region 41
```

The **iplocation** command produces additional fields containing geographic data





# Security and Fraud Team

Show website activity by geographic location

## Tasks

1. Use the `iplocation` command to enrich the events with location data
2. Generate a world map showing the geographic location of all website activity down to the city level
3. Add your visualisation to your existing dashboard

## Goal





# Security and Fraud Team

Show website activity by geographic location

## Solution:

```
index=main sourcetype=access_combined  
| iplocation clientip | geostats count by City
```

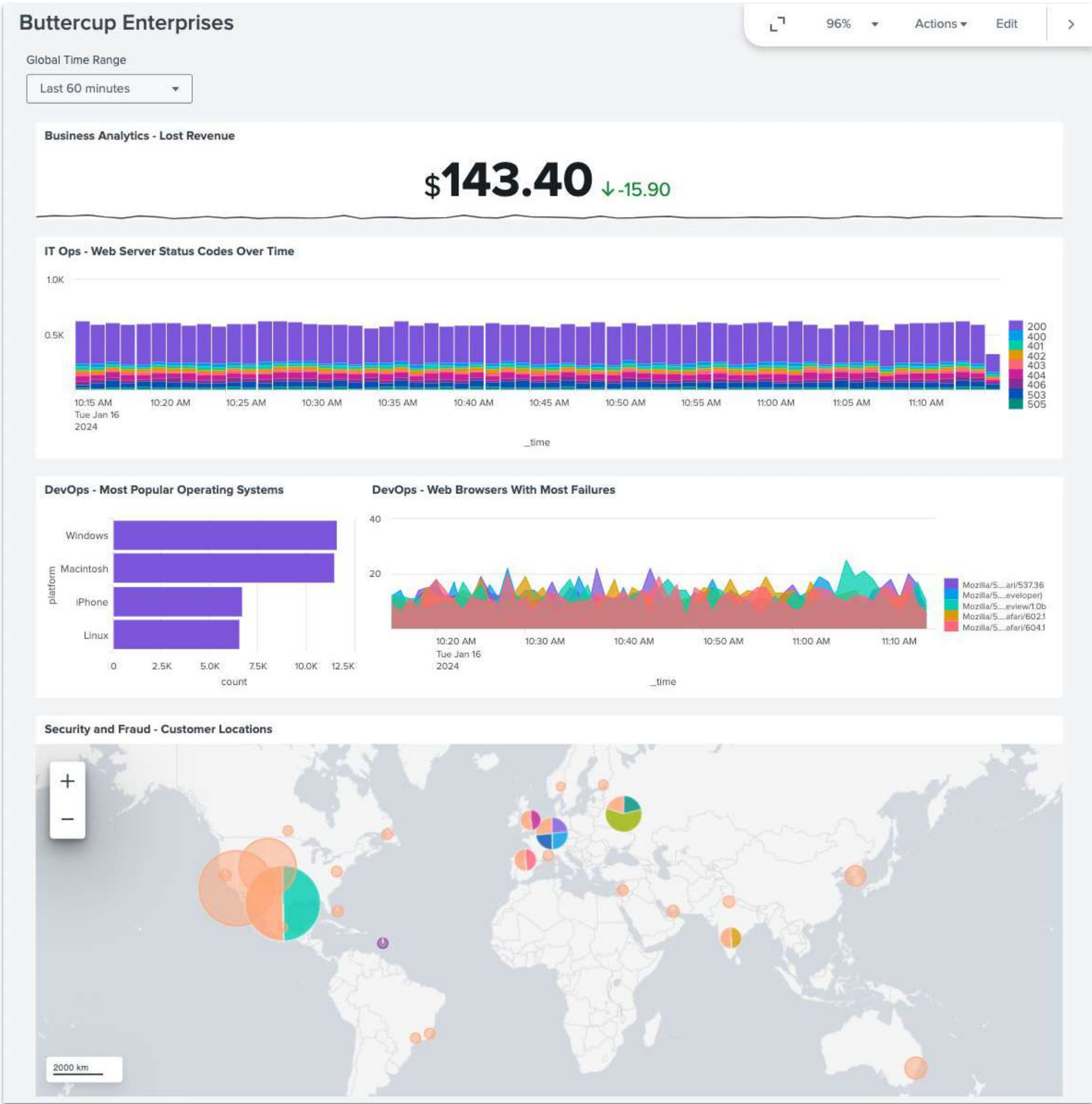


When you're happy with your chart add it to your dashboard!



# Your dashboard so far...

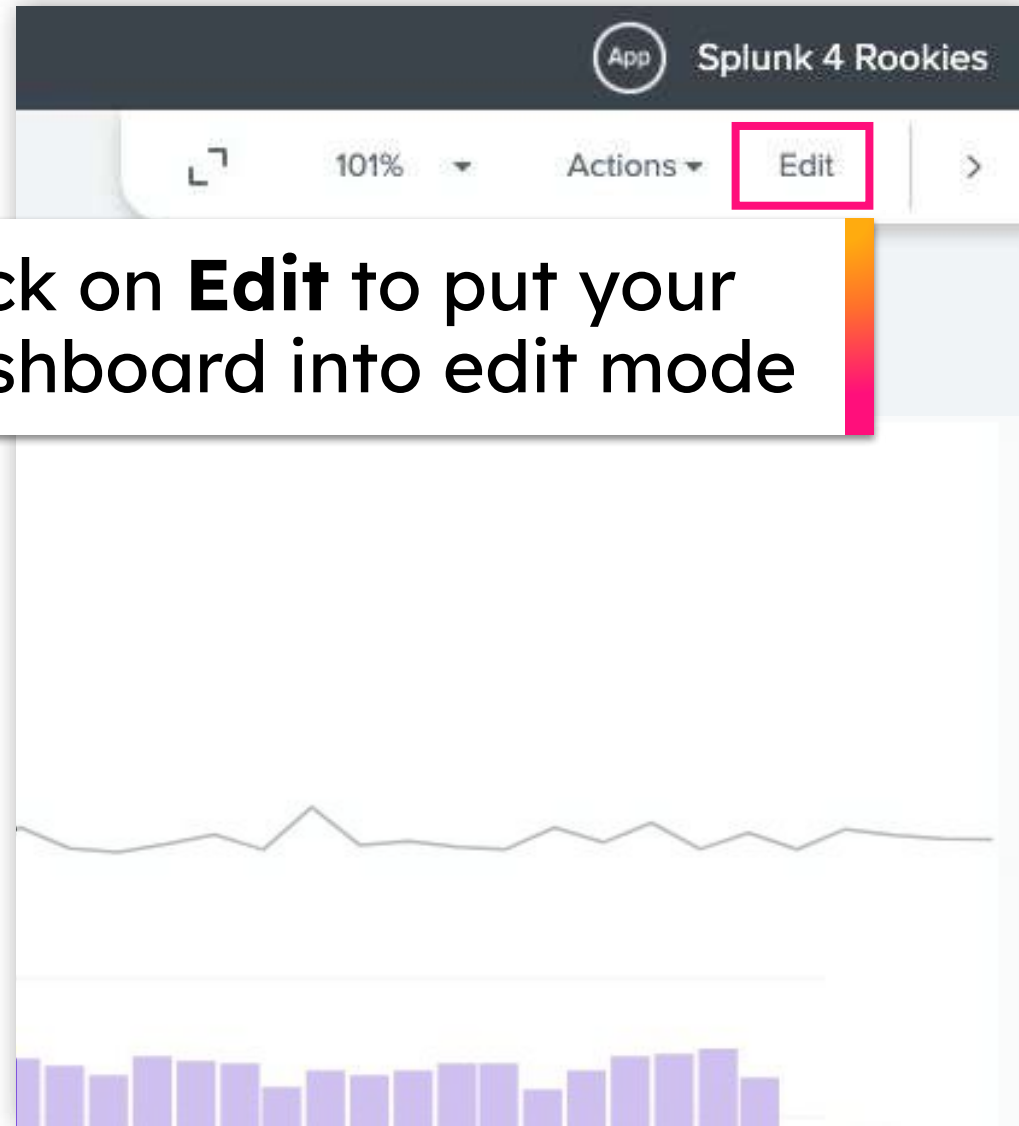
-  IT Operations team ✓
-  DevOps team ✓
-  Business Analytics team ✓
-  Security and Fraud team ✓



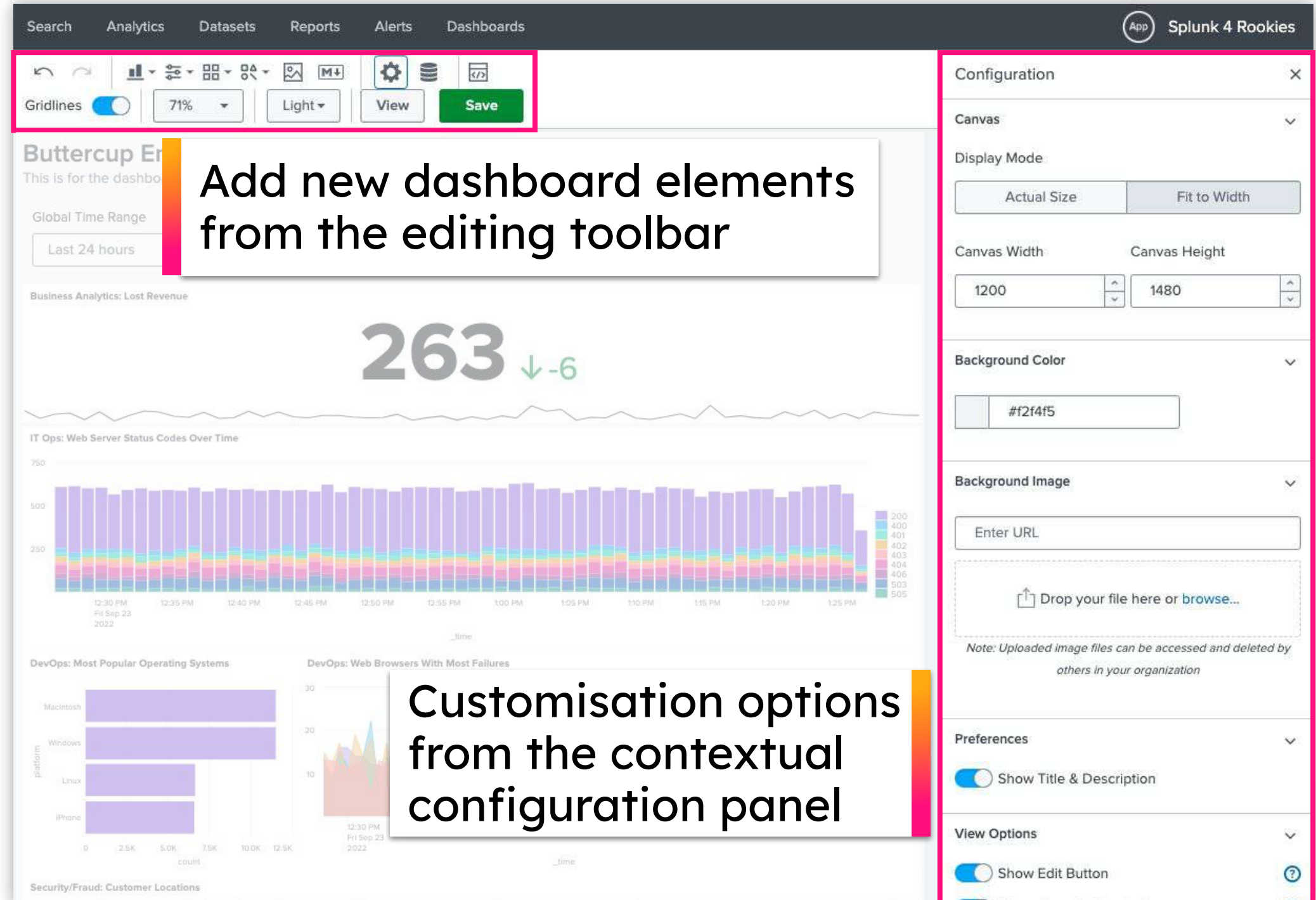


# Customise Your Dashboard

Click on **Edit** to put your dashboard into edit mode



Add new dashboard elements from the editing toolbar



Customisation options from the contextual configuration panel

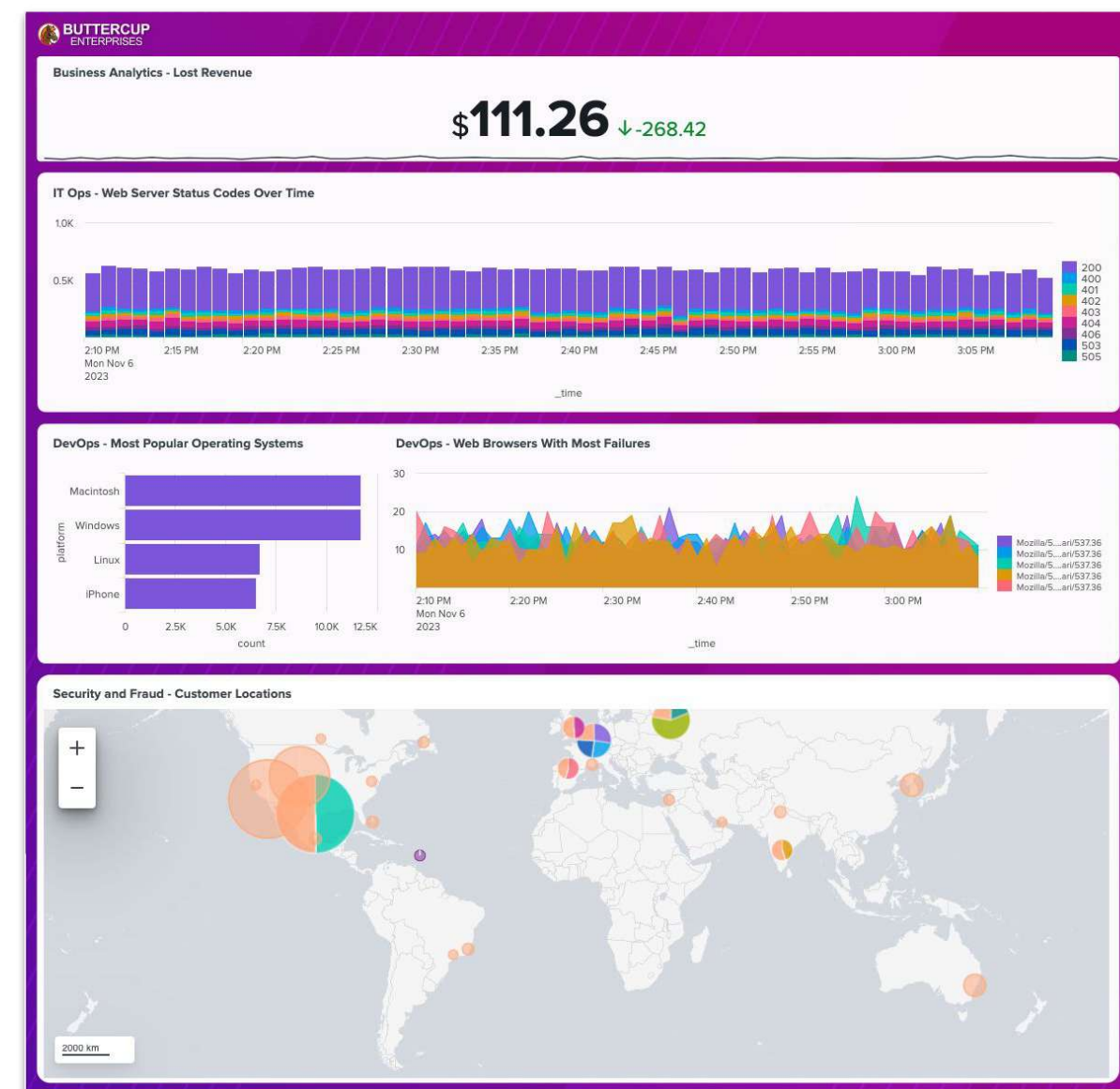


# Customise Your Dashboard

## 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. Link your dashboard panels to the global time picker

## Goal





# You've Finished the Hands-on Exercises!



IT Operations team



DevOps team



Business Analytics team



Security and Fraud team



Dashboard with custom background

## Buttercup Enterprises

Global Time Range

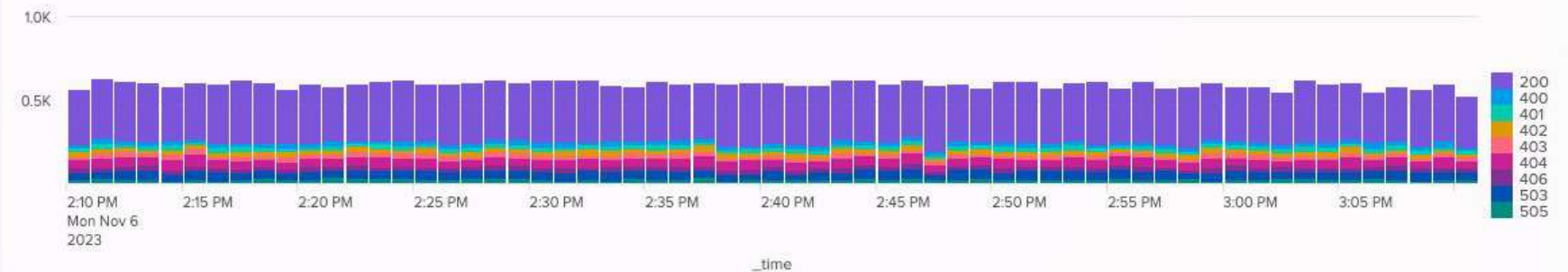
Last 60 minutes



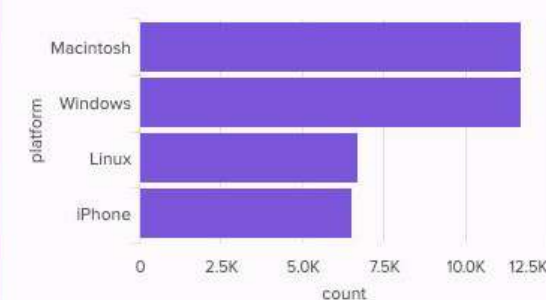
### Business Analytics - Lost Revenue

\$111.26 ↓-268.42

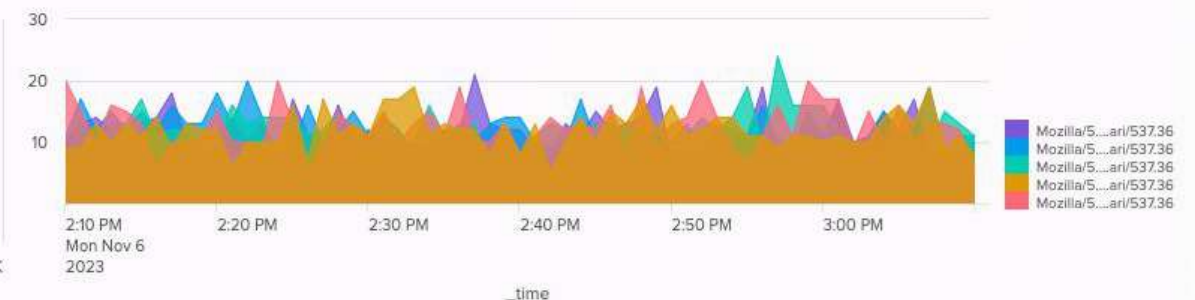
### IT Ops - Web Server Status Codes Over Time



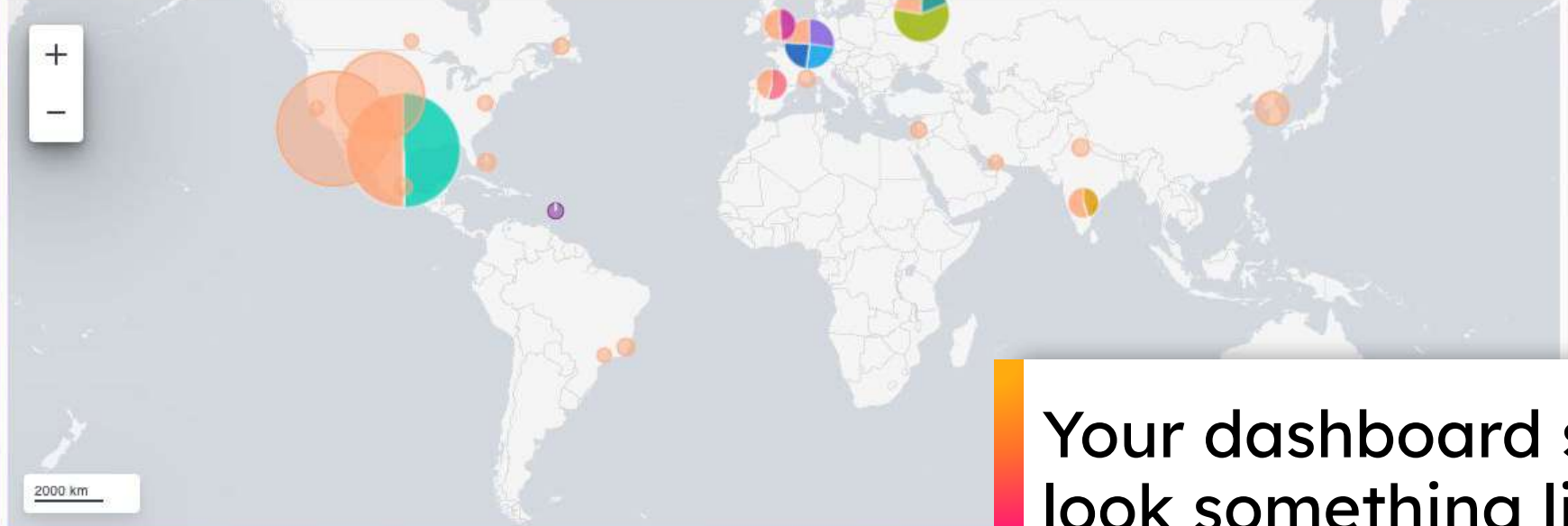
### DevOps - Most Popular Operating Systems



### DevOps - Web Browsers With Most Failures



### Security and Fraud - Customer Locations



Your dashboard should look something like this

# Splunk Resources

Where to go after today's workshop

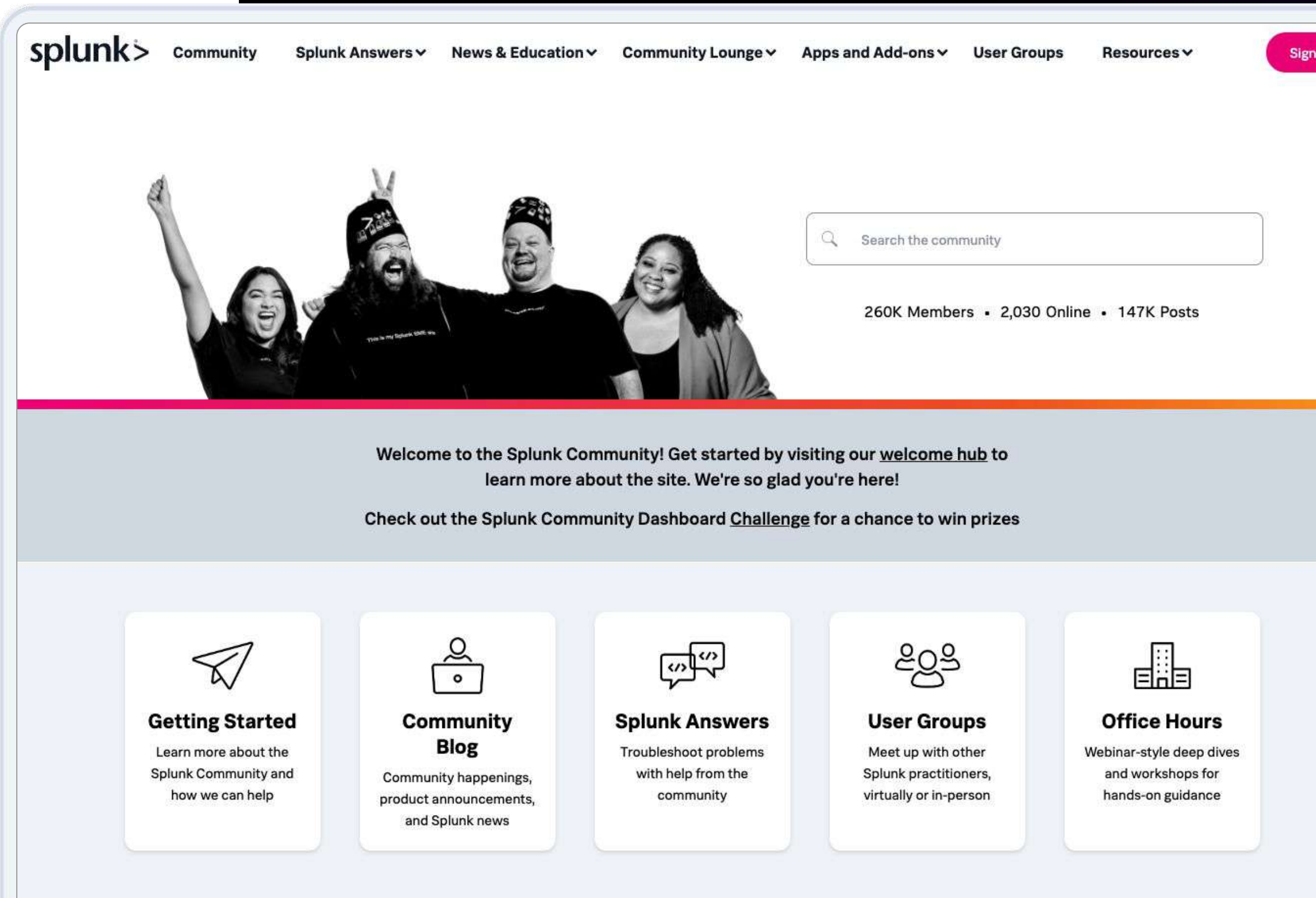




# Splunk Community

<https://community.splunk.com>

- Connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from experts
- Meet in-person or virtually with like-minded enthusiasts
- Search for, vote on, or submit ideas for product enhancements





# Splunk Events

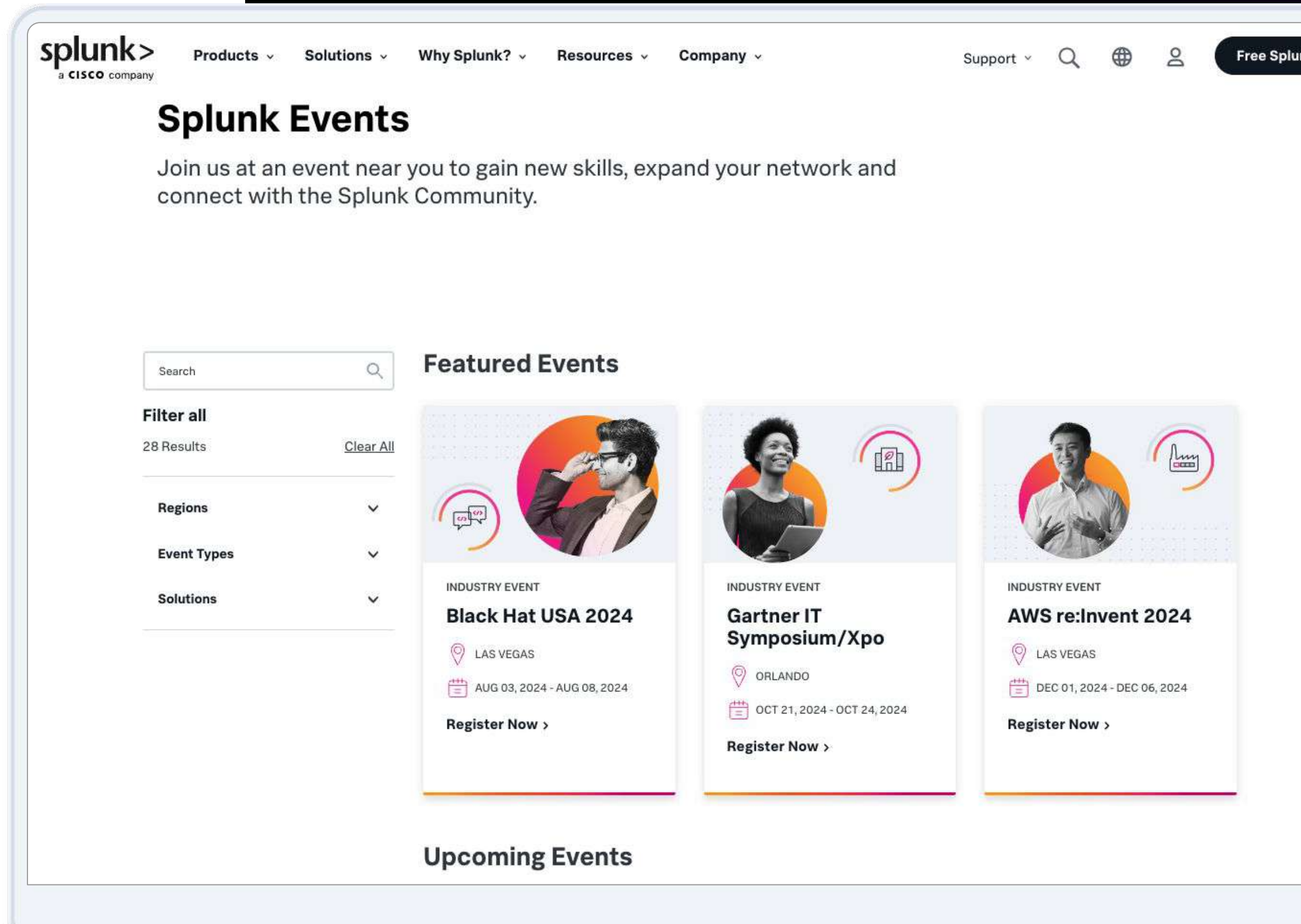
<https://splunk.com/events>

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



<https://conf.splunk.com>

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

A screenshot of the Splunk Events website. The header includes the Splunk logo (a CISCO company), navigation links for Products, Solutions, Why Splunk?, Resources, and Company, and a Support link with search, globe, and user icons. The main heading is "Splunk Events" with a subtext: "Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community." Below this is a search bar and a "Filter all" section showing 28 Results with links for Clear All, Regions, Event Types, and Solutions. The "Featured Events" section displays three event cards: "Black Hat USA 2024" (Las Vegas, Aug 03-08, 2024), "Gartner IT Symposium/Xpo" (Orlando, Oct 21-24, 2024), and "AWS re:Invent 2024" (Las Vegas, Dec 01-06, 2024). Each card includes a "Register Now >" link. The "Upcoming Events" section is partially visible at the bottom.

# Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search:

<https://splk.it/SplunkSearchTutorial>

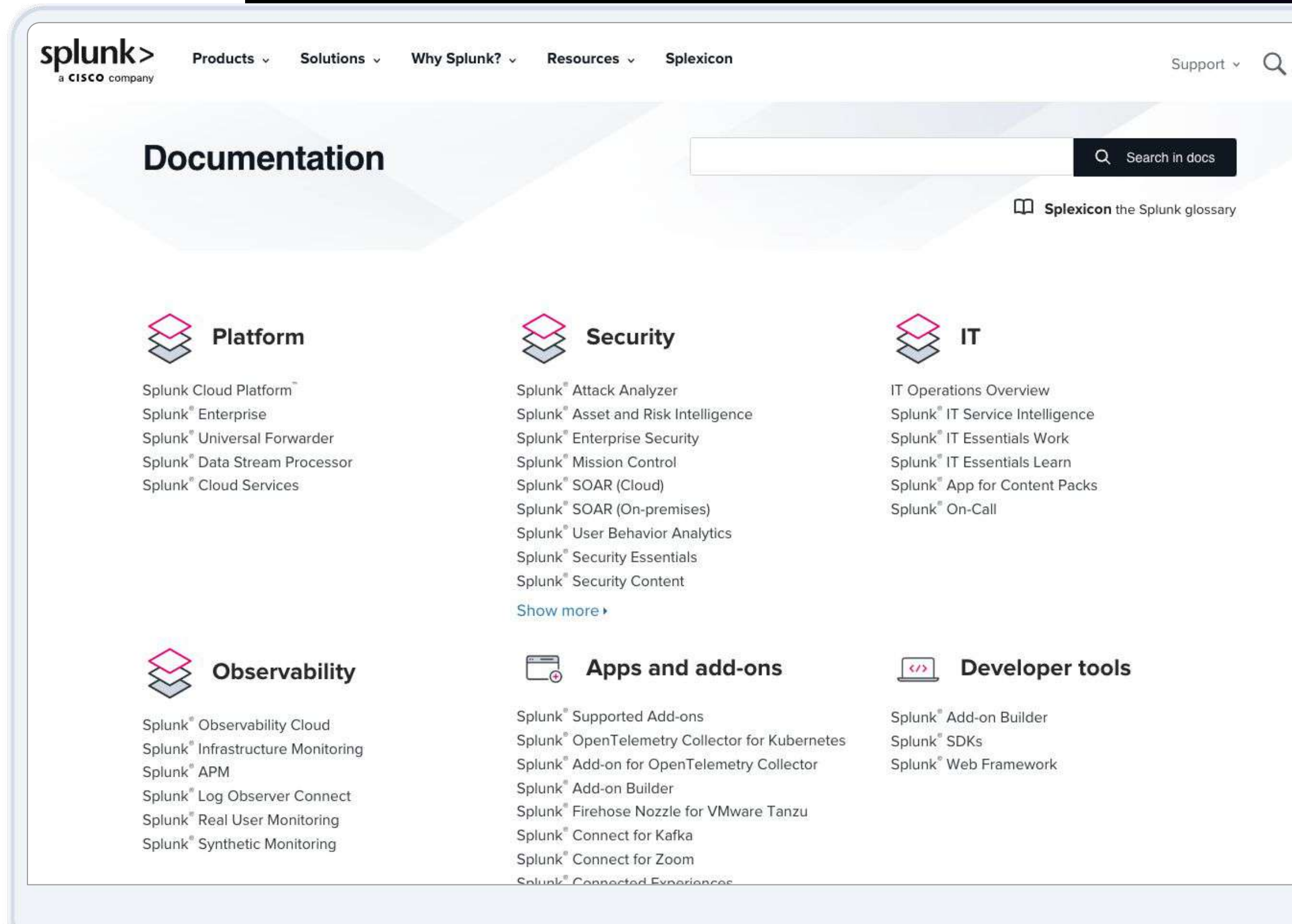
Dashboard Studio:

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

- And more!

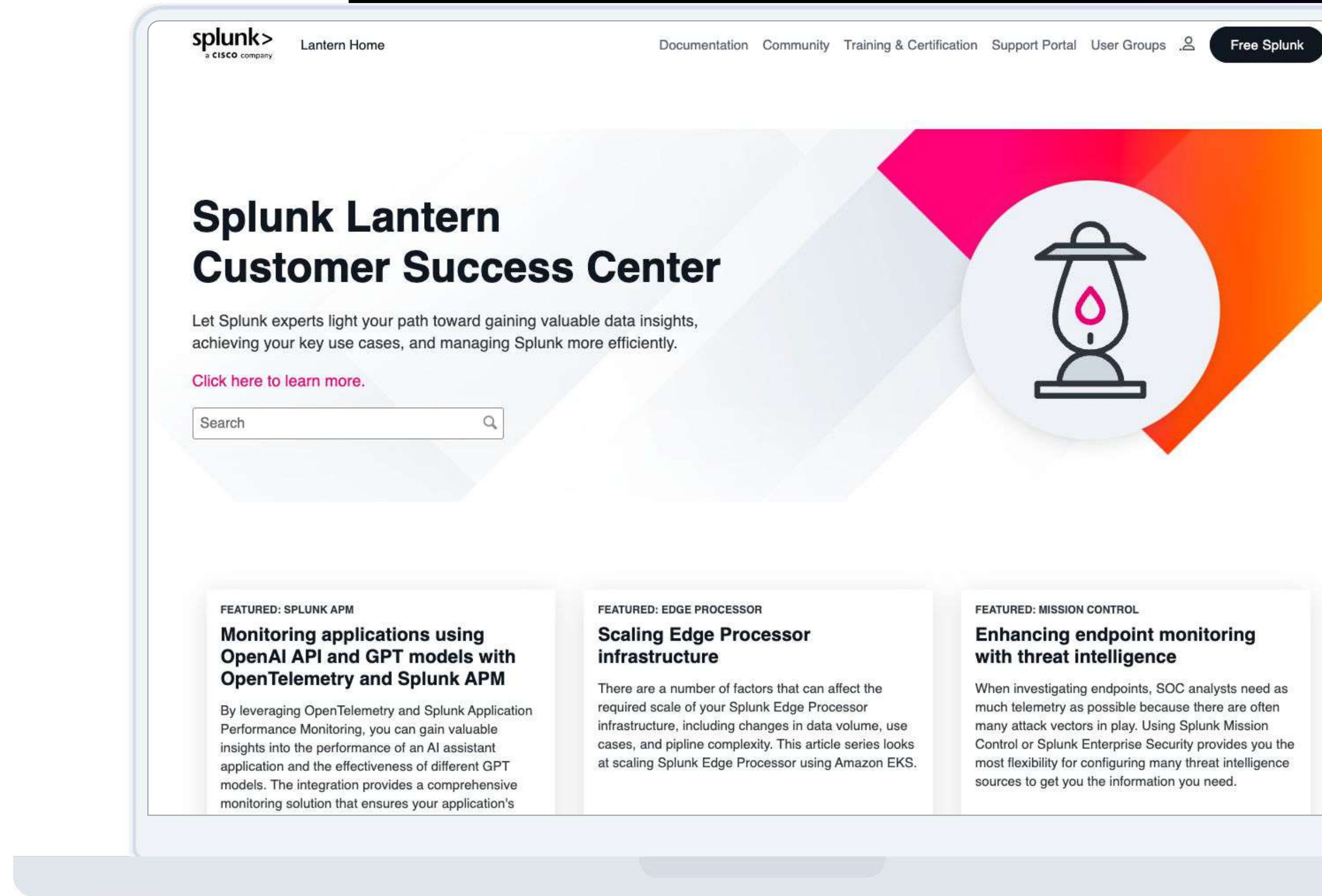




# Splunk Lantern

<https://lantern.splunk.com>

- Use case library
- Product tips
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to increase the value of Splunk across your organisation





# Developer Resources

<https://dev.splunk.com>

- Developer Guide
- API Reference
- Tutorials
- Downloads  
APIs, libraries, tools
- Code examples
- Free Developer licence

splunk>dev

## Welcome to splunk>dev

Build apps that Turn Data into Doing™ with Splunk.

Deliver apps and integrations that bring new kinds of data into the Splunk platform and deliver data-based insights, enabling users to investigate, monitor, analyze and act to make better and smarter decisions. Get started today.

## Develop for Splunk Cloud and Splunk Enterprise

Build apps and integrations for Splunk Cloud and Splunk Enterprise, test in your free development Splunk platform instance, and deliver in the Splunkbase marketplace.



## Develop for Observability

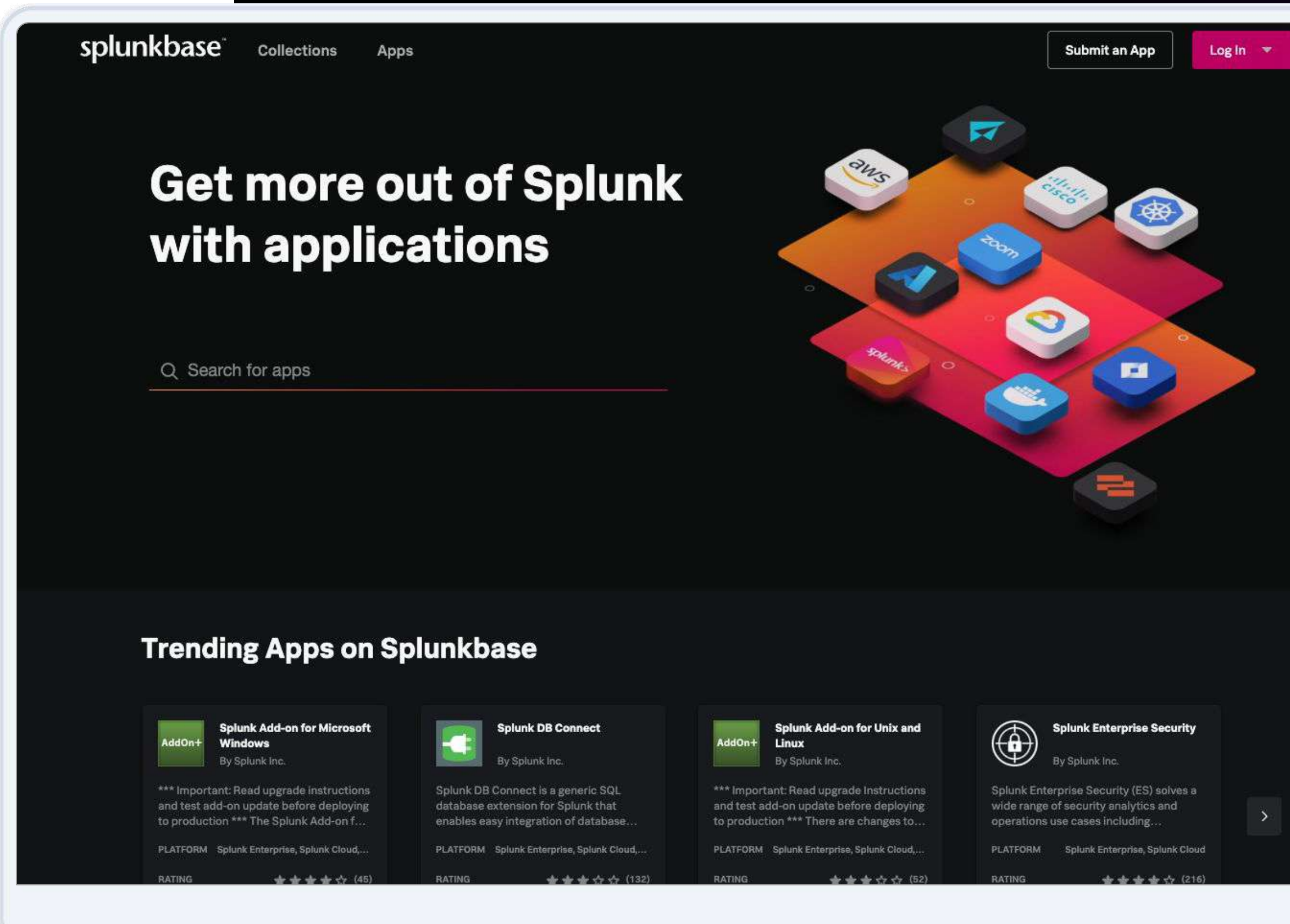
Manage, integrate with, and access features of your Splunk Infrastructure Monitoring organization with the API.



# Splunk Apps & Add-ons

<https://splunkbase.splunk.com>

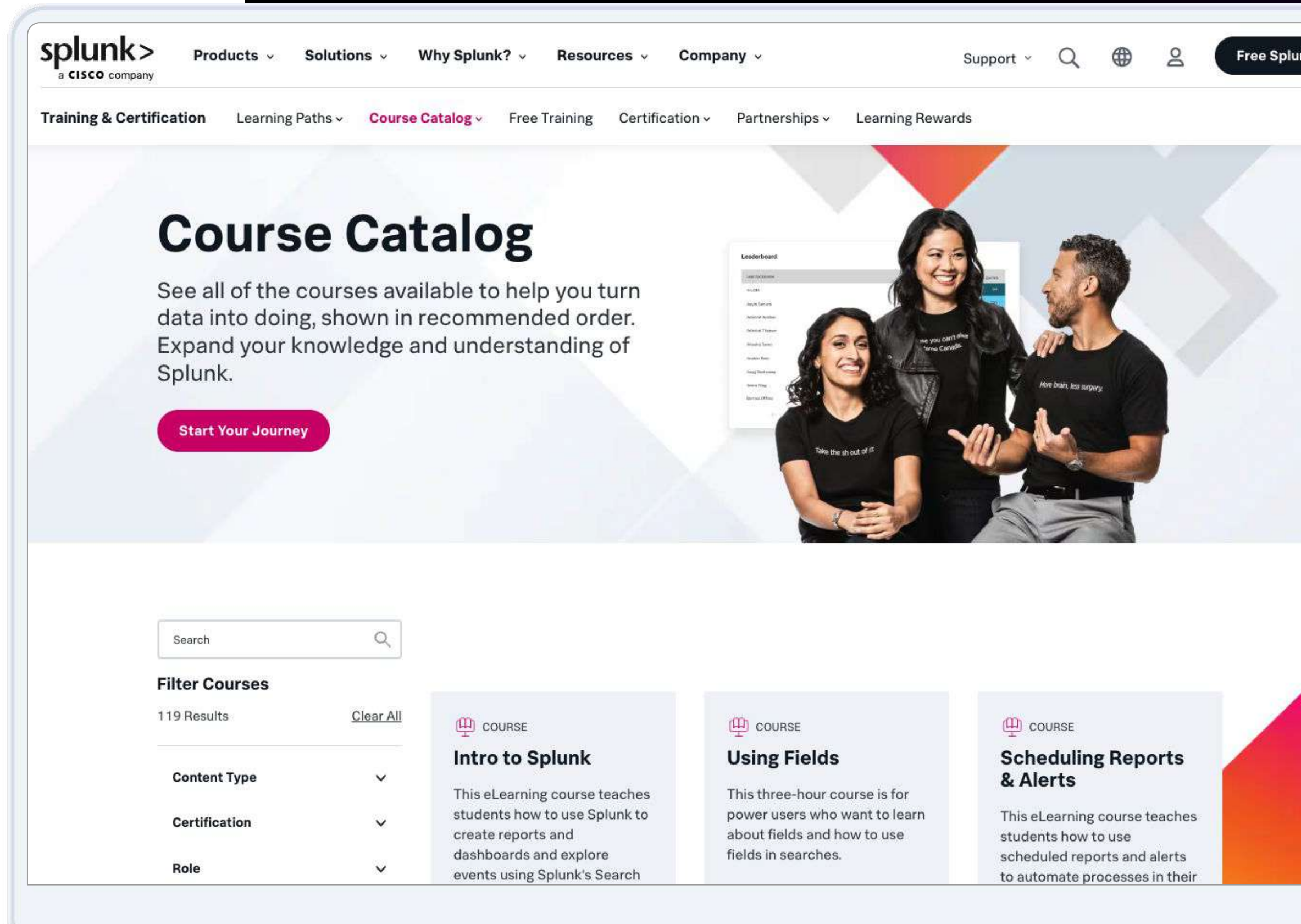
- 2100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!





<https://splunk.com/training>

- **Online education classes**  
Instructor-led and self-paced eLearning
- **Certification tracks for different roles**  
User, Power User, Admin, Architect and Developer
- **Splunk Education Rewards**  
Complete training and receive points that you can redeem for Splunk swag!
- **Free education!**  
Single-subject eLearning courses to kick start your Splunk learning





# Thank you