

splunk®> 4rookies

Hands-On Workshop



splunk®>
a CISCO company

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as "expects," "anticipates," "targets," "goals," "projects," "intends," "plans," "believes," "momentum," "seeks," "estimates," "continues," "endeavors," "strives," "may," variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. 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. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in 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 report on Form 10-Q filed with the SEC on November 28, 2023. 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 Cisco or Splunk, on Cisco or Splunk's website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or 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 or be relied upon in making a purchasing decision. We undertake no commitment, promise or 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. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

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

© 2025 Splunk LLC. All rights reserved.

Please introduce yourself!

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



Workshop Agenda

- 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

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

Custom Visualisations
HTTP Event Collector (HEC)
Transformations
Architecture

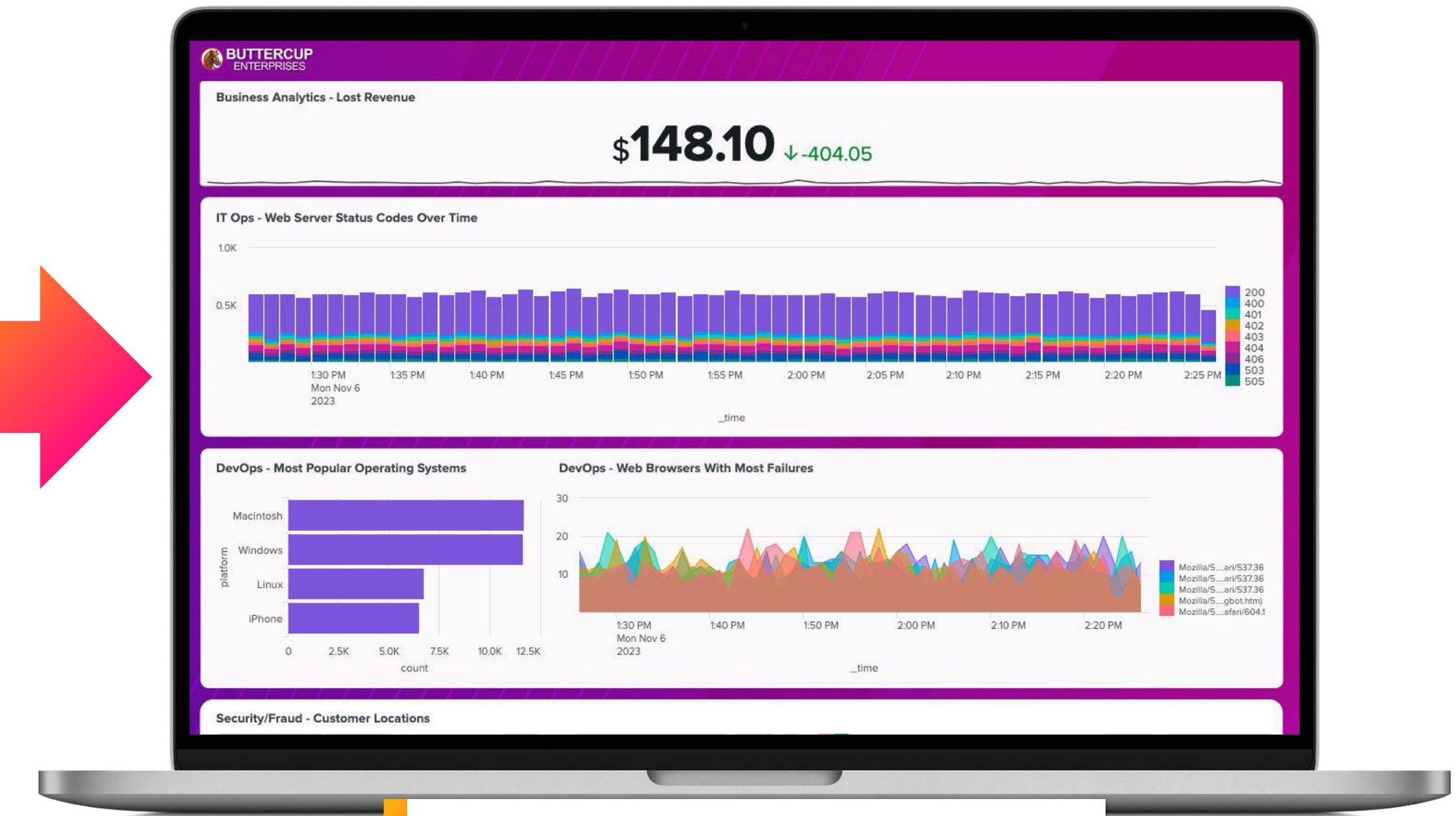
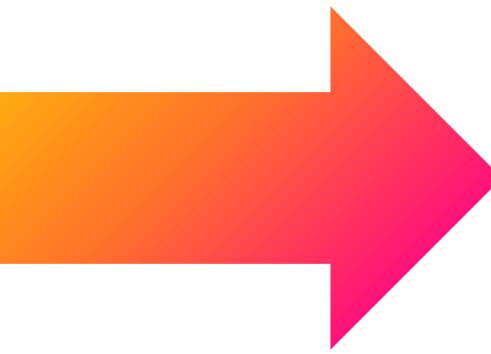
Report Acceleration
Common Information Model (CIM)
Containers
Best Practices
And much more...

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

The screenshot shows a workshop event card for 'Splunk4Rookies'. The card includes the event name, a 'Platform' section, and an 'AVAILABLE' status indicator. To the right of the card is a call-to-action button labeled 'Enroll event' with a blue gradient background and white text. A small orange and pink gradient bar is positioned to the left of the 'Enroll in today's event' text.

Enroll in today's event



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.¹



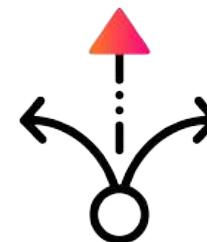
Cyber risk is business risk

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



Resilience is regulated

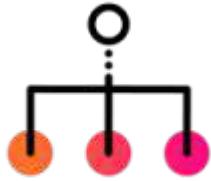
Governments have enacted stiff penalties for non-compliance.



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.



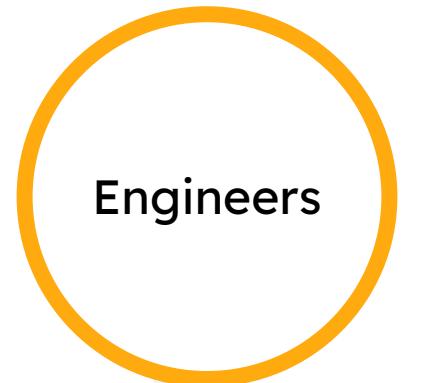
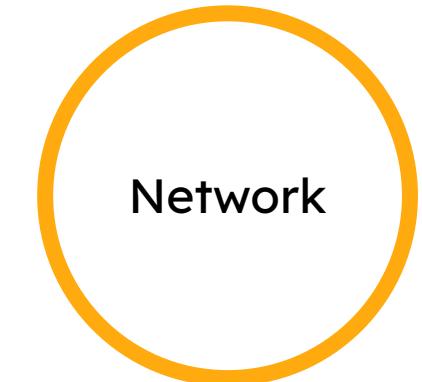
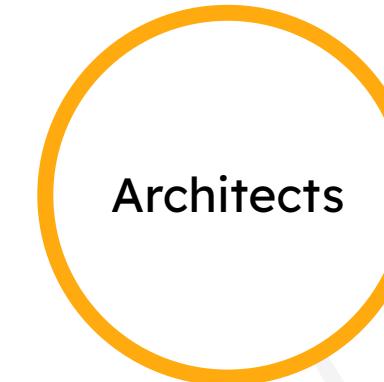
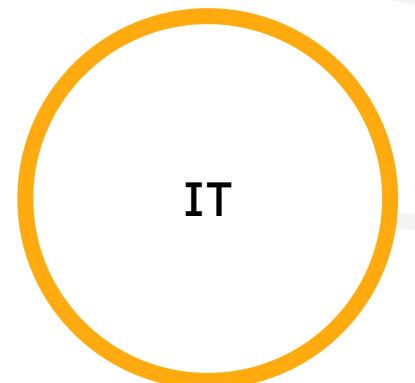
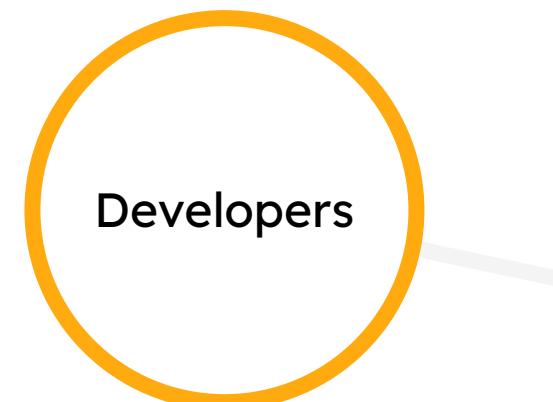
Regulations require real-time risk assessments.

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

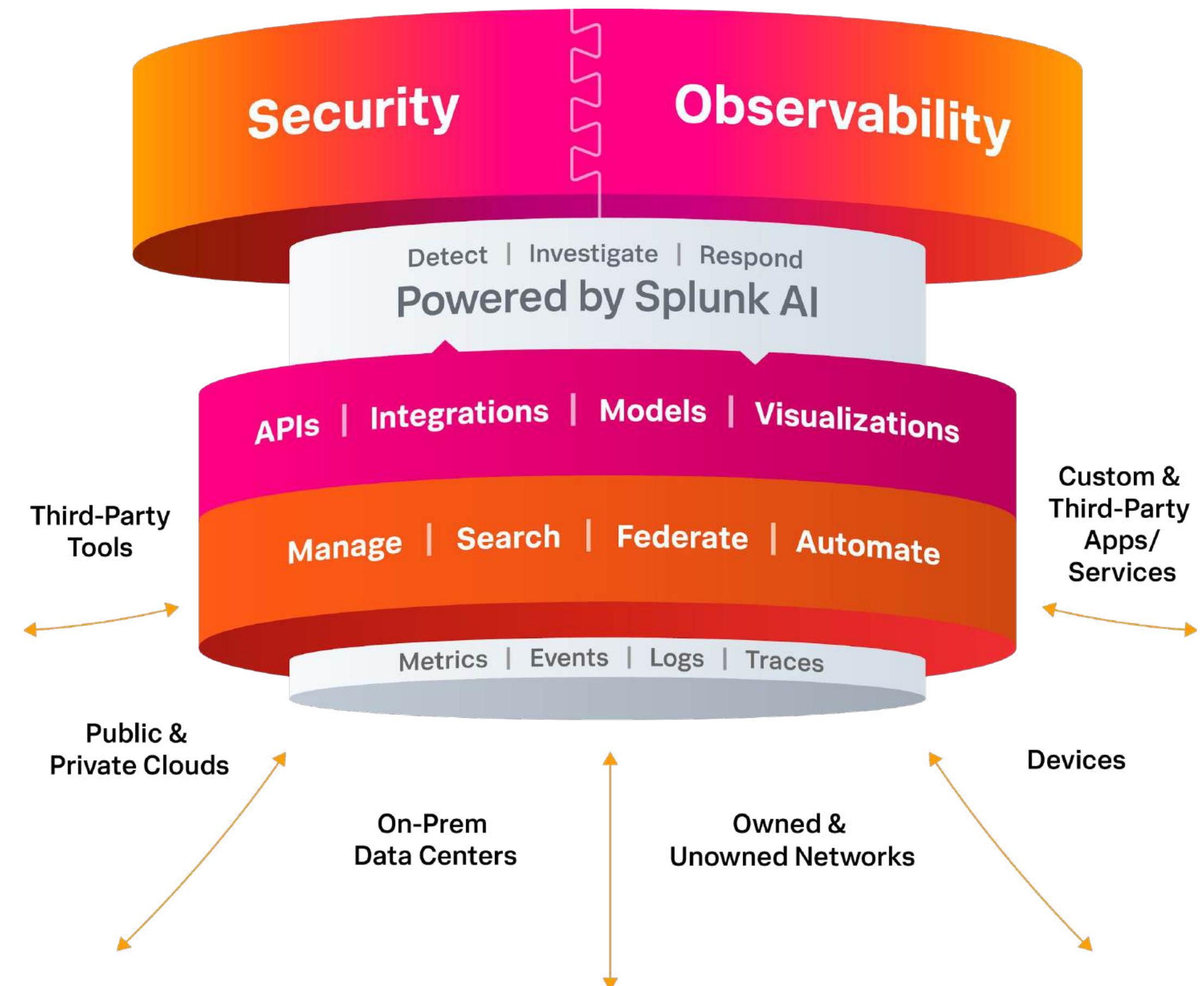


Remediate
faster



Adapt quickly

The Unified Security and Observability Platform.



What differentiates Splunk:

End-to-end **visibility and insights** into the business risk and impact of issues across your entire **hybrid** digital footprint

Only recognized leader in both **Security** and **Observability**

Ability to flexibly manage, federate, and reuse data at **enterprise scale** and apply AI no matter where you store your data

A unified platform that empowers teams to collaborate and find the root cause of problems across security and observability

Deploy Splunk in the cloud, or in your data centers.



15+



7

Google Cloud

4

Microsoft
Azure

Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

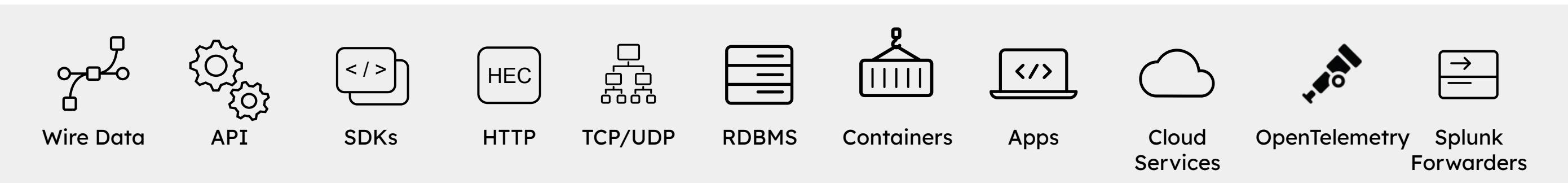
3 Simple Steps:

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



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

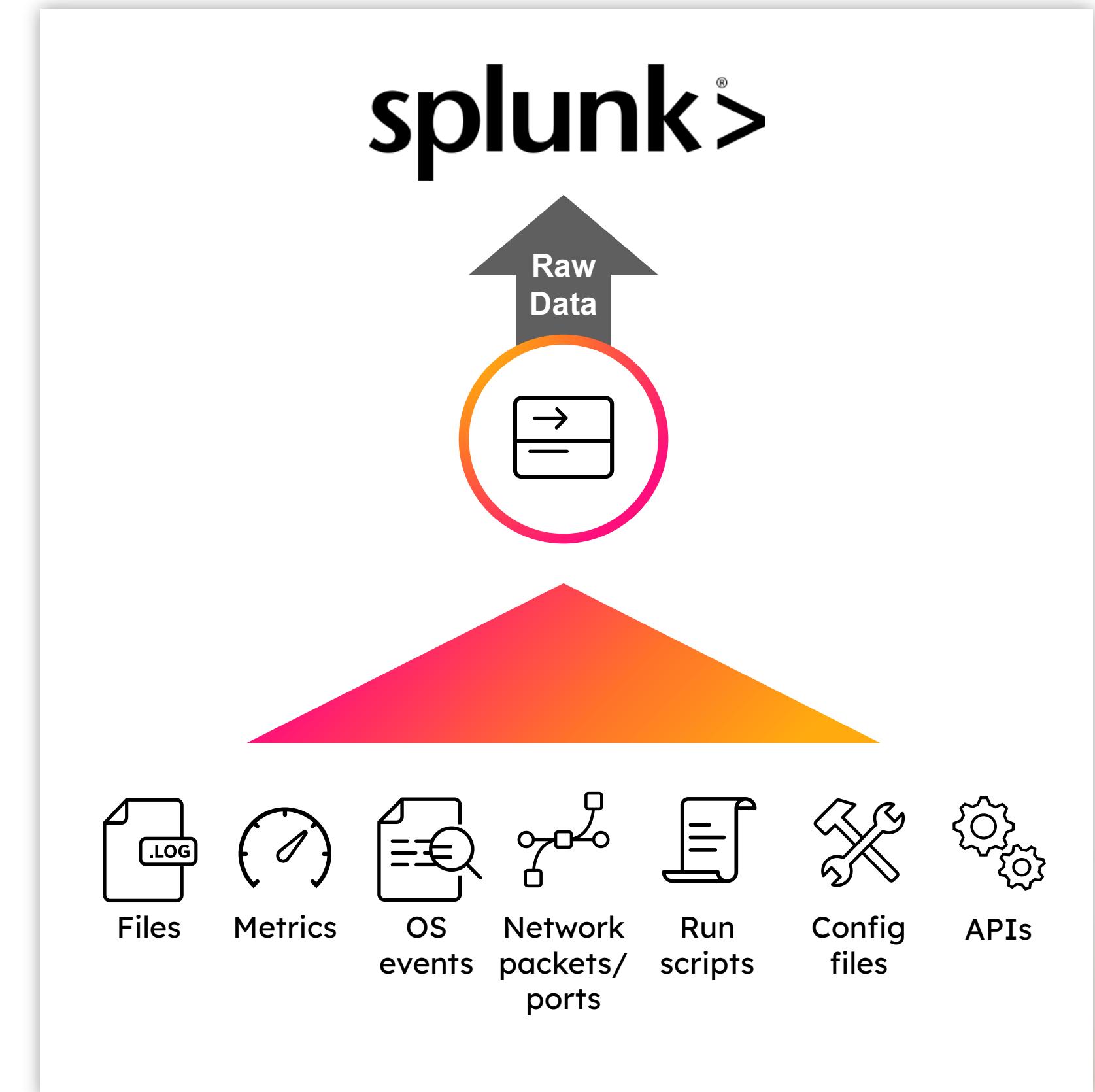
Flexible options for data collection and forwarding



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!

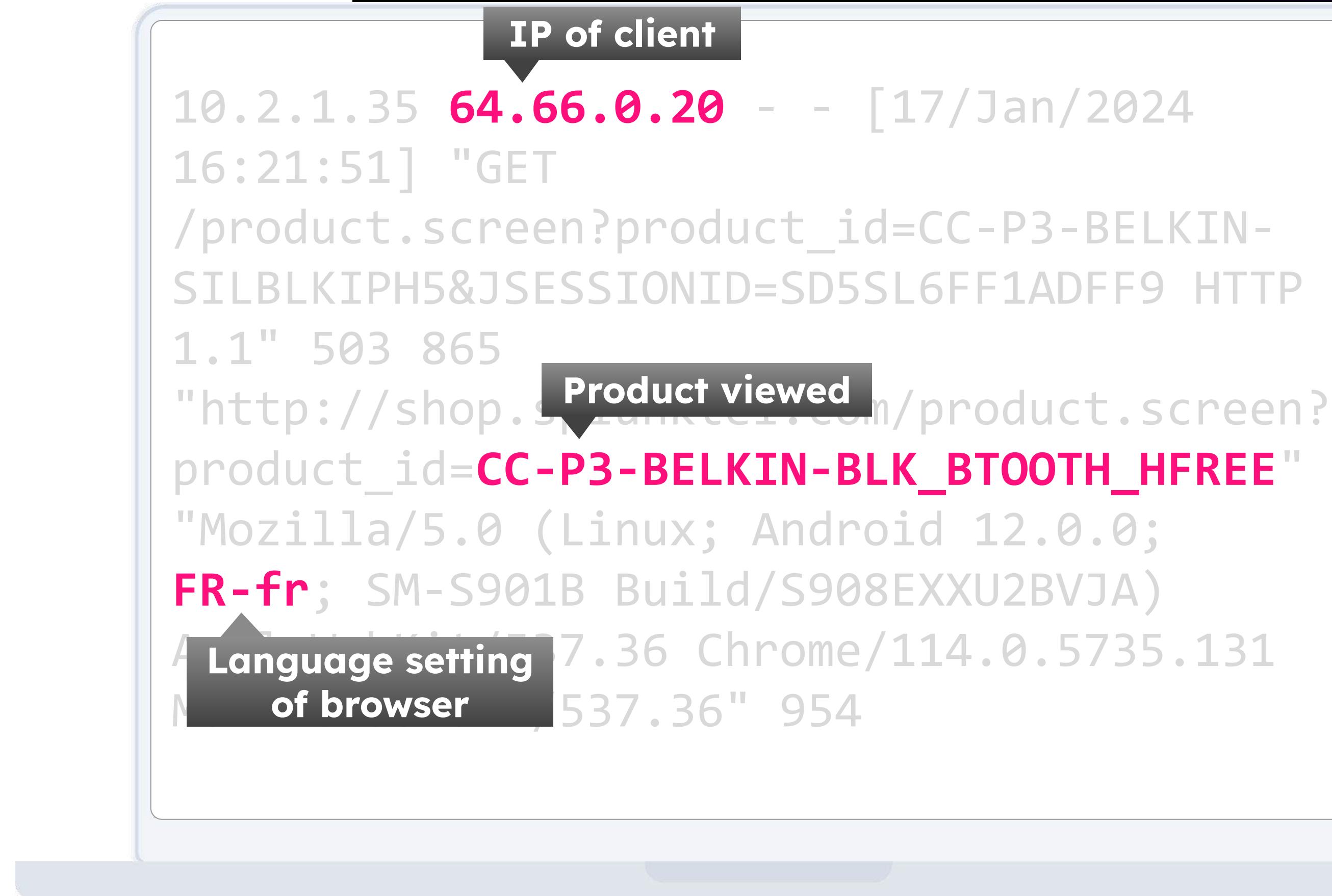


Machine data is valuable not complex!

```
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



DevOps Use Case

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

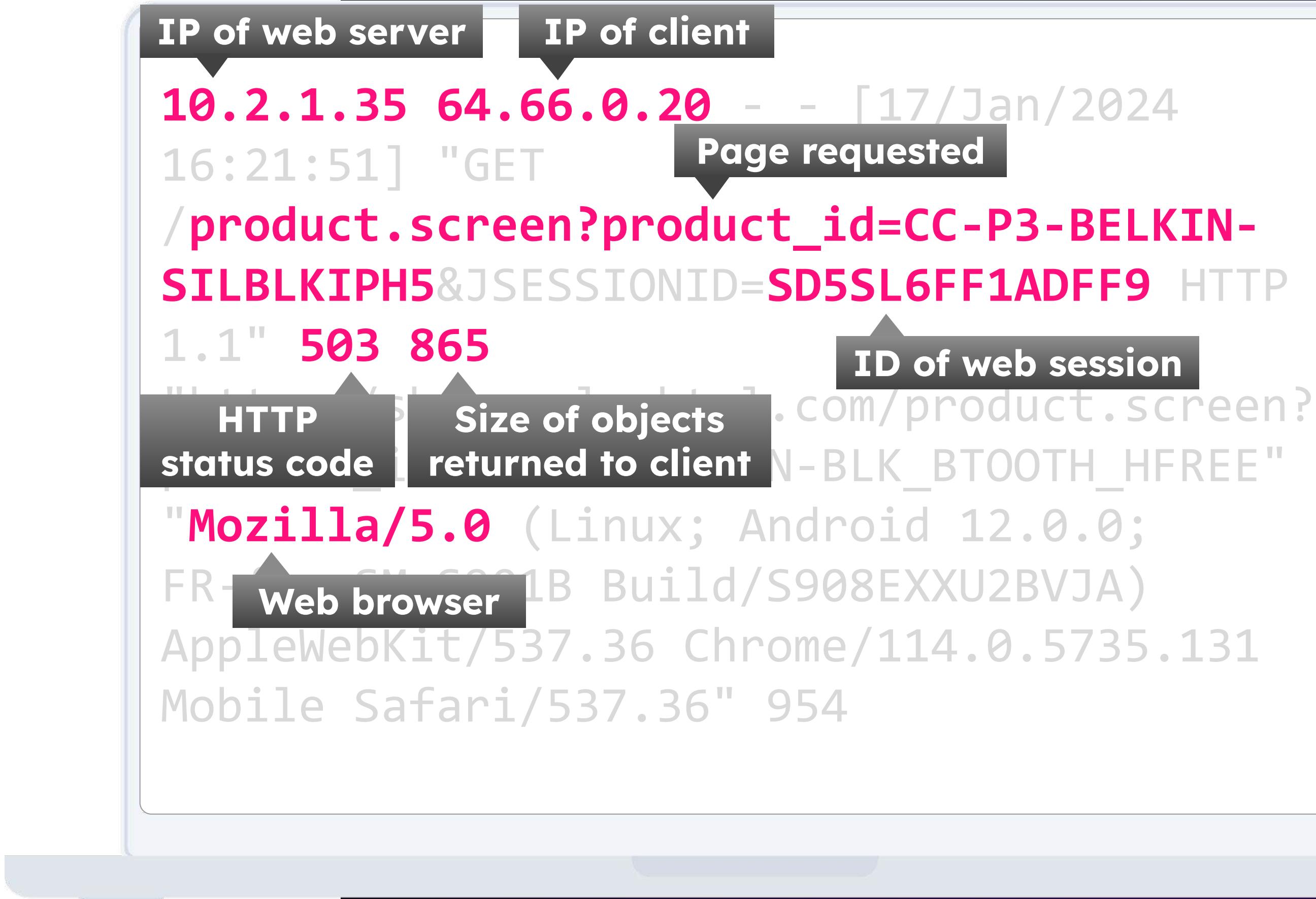
```
10.2.1.35 64.66.0.20 - - [17/Jan/2024  
16:21:51] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?  
product_id=CC-P3-BELKIN-SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9"  
Mozilla/5.0 (Linux; Android 12.0.0;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

Platform

Handset model

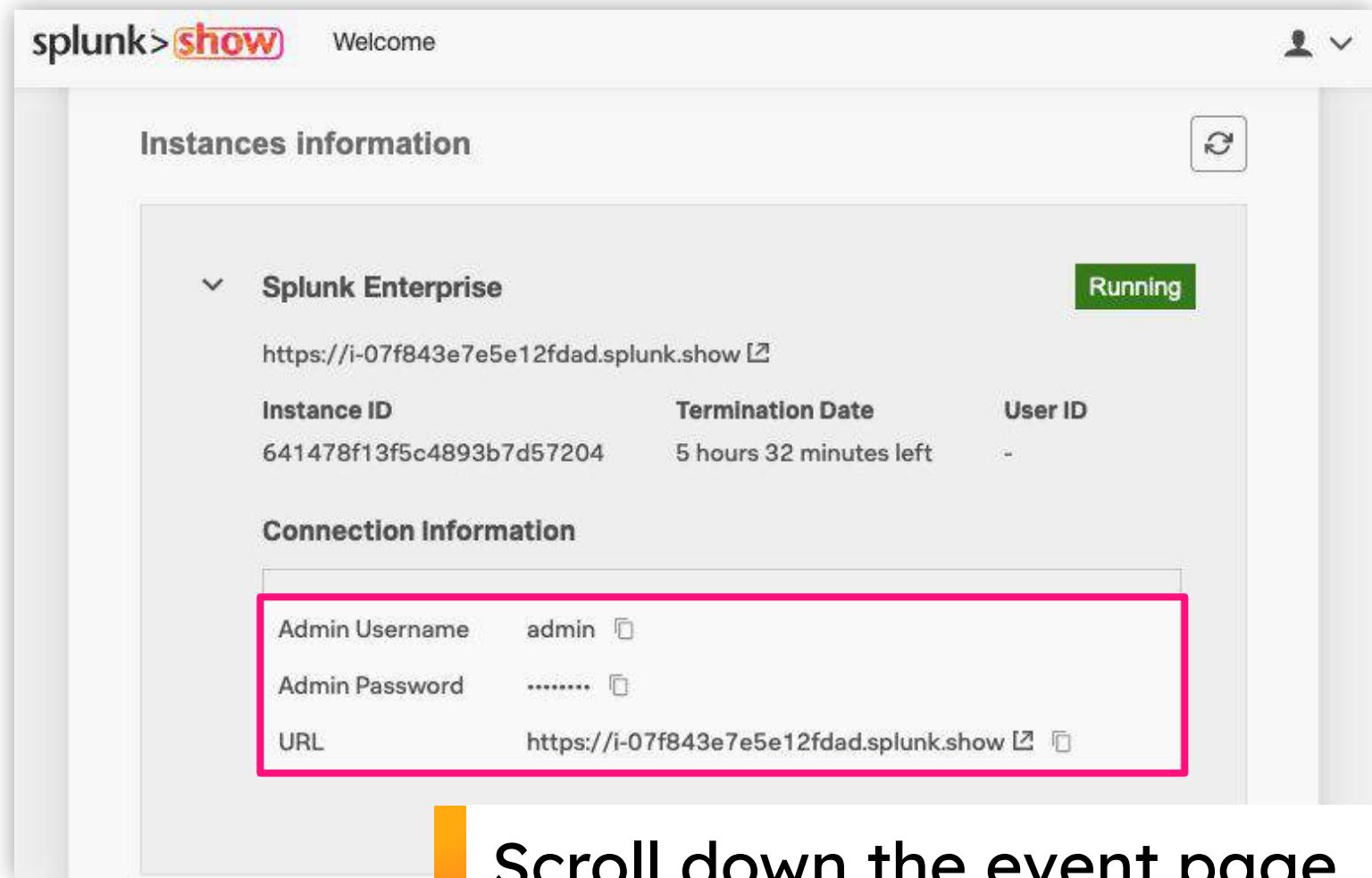
IT Ops Use Case

Which web pages
are generating the
most errors?



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 following details:

- Instances information:** Splunk Enterprise (Running)
- Instance ID:** 641478f13f5c4893b7d57204
- Termination Date:** 5 hours 32 minutes left
- Connection Information:**
 - Admin Username: admin
 - Admin Password: (redacted)
 - URL: https://i-07f843e7e5e12fdad.splunk.show

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 enterprise login page with the following fields:

- Username: [redacted]
- Password: [redacted]
- Sign In button

Login using the credentials
from Splunk Show

Apps and Add-ons

- 2200+ 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

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

Open your app and have a play!

The currently selected app

Search bar - type anything here to search

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time

This image shows a screenshot of the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'App: Splunk 4 Rookies'. Below it is a 'New Search' bar containing the query 'action=purchase status=200', which has found 261 events from May 15, 2018, between 07:49:00.000 and 15:05:2018 07:49:00.000. The main area shows an 'Events (261)' tab selected, followed by 'Patterns', 'Statistics', and 'Visualization'. A histogram titled 'Event histogram' displays event counts over time, with a note indicating '1 minute per column'. Below the histogram is a table of raw event data. The table includes columns for 'Time' (e.g., 15/05/2018 08:49:08.127) and 'Event' (e.g., 12.130.60.5 -- [15/May/2018 08:49:08:127] "GET /cart.do?..."). To the left of the table, a sidebar lists 'INTERESTING FIELDS' such as 'action', 'bytes', 'category_id', 'clientip', 'date_hour', etc. Orange arrows and callout boxes point to various UI elements with descriptive text.

Time	Event
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/... flowershop.com/category.screen?category_id=GIFTS" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 873 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
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 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
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 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined

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

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

Commands

Pipe character: Output
of left is input to right

e.g. index=main action=purchase

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/A546BXU1AWB7) 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=SD1SL6FF5ADFFC 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=CM-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/113.0.672.92 Safari/537.36" 977 host = Domane-Demo- source = /var/log/weblogs/noise_apache.log17 sourcetype = access_combined

Functions

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

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

| rename count as "number of events"

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



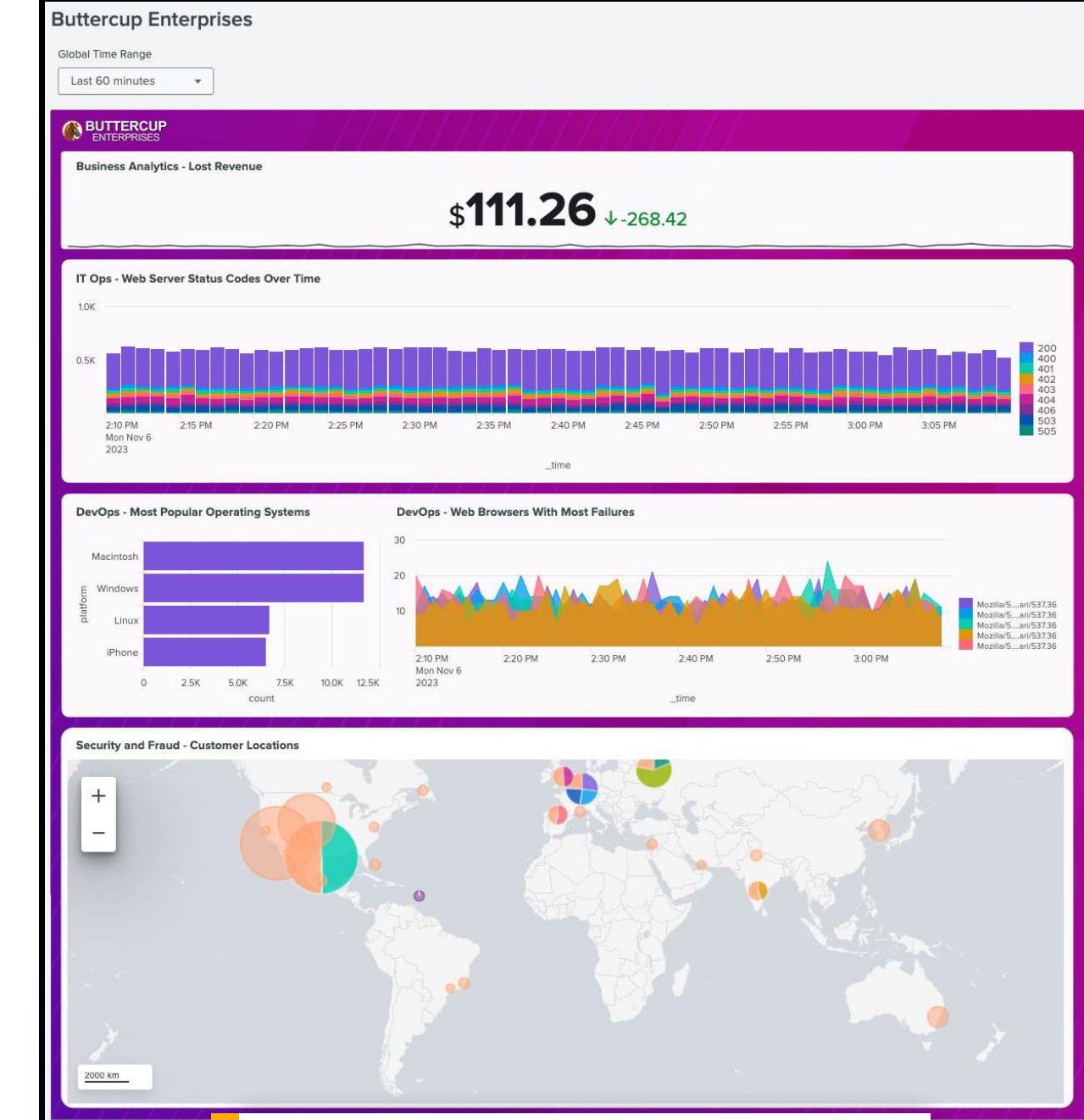
Business Analytics team: Show lost revenue from the Buttercup Enterprises website



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!



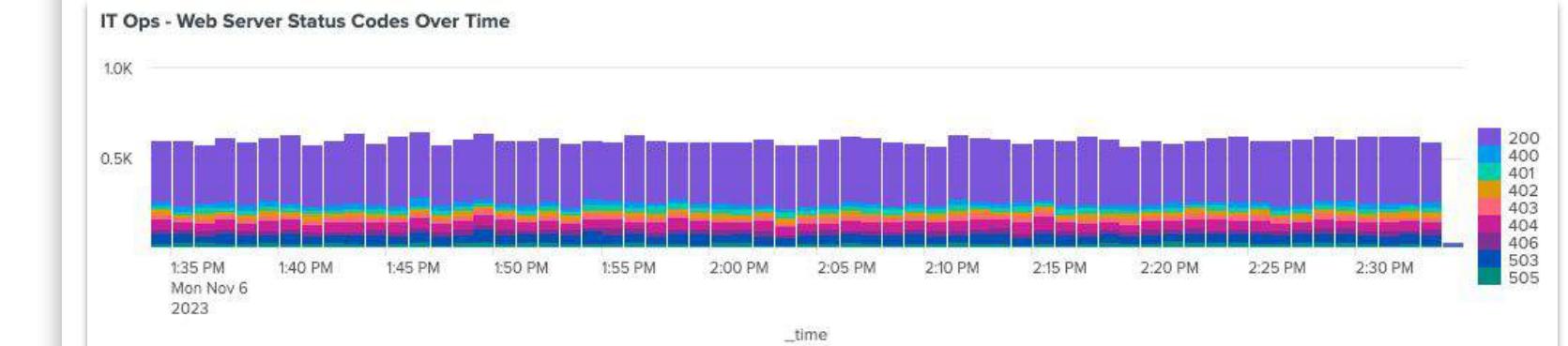
IT Operations Team

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**

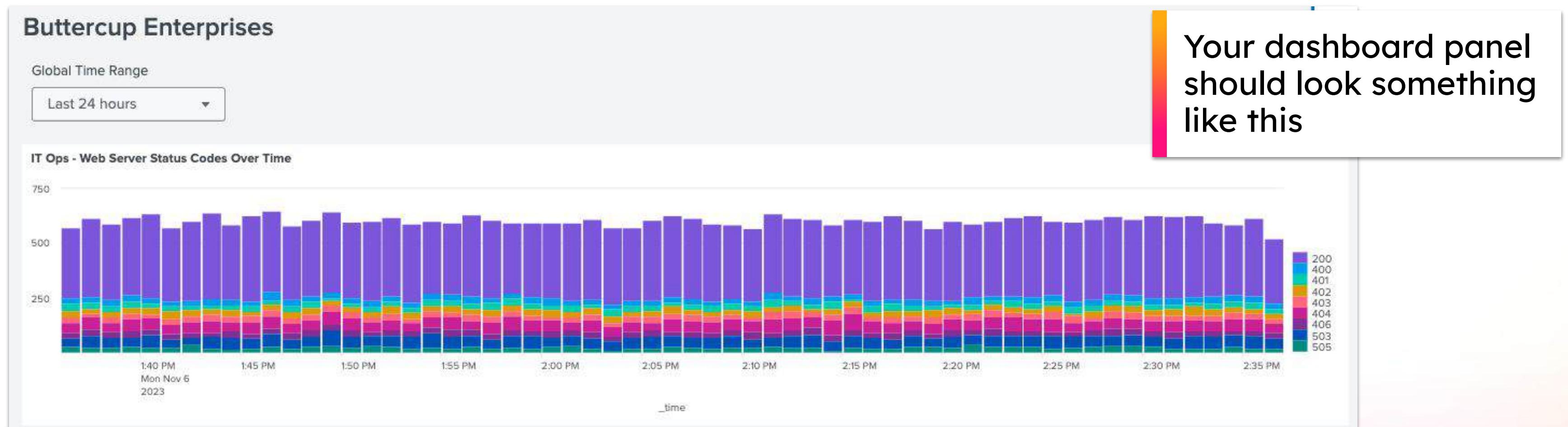


IT Operations Team

Investigate successful versus unsuccessful web server requests over time

Solution:

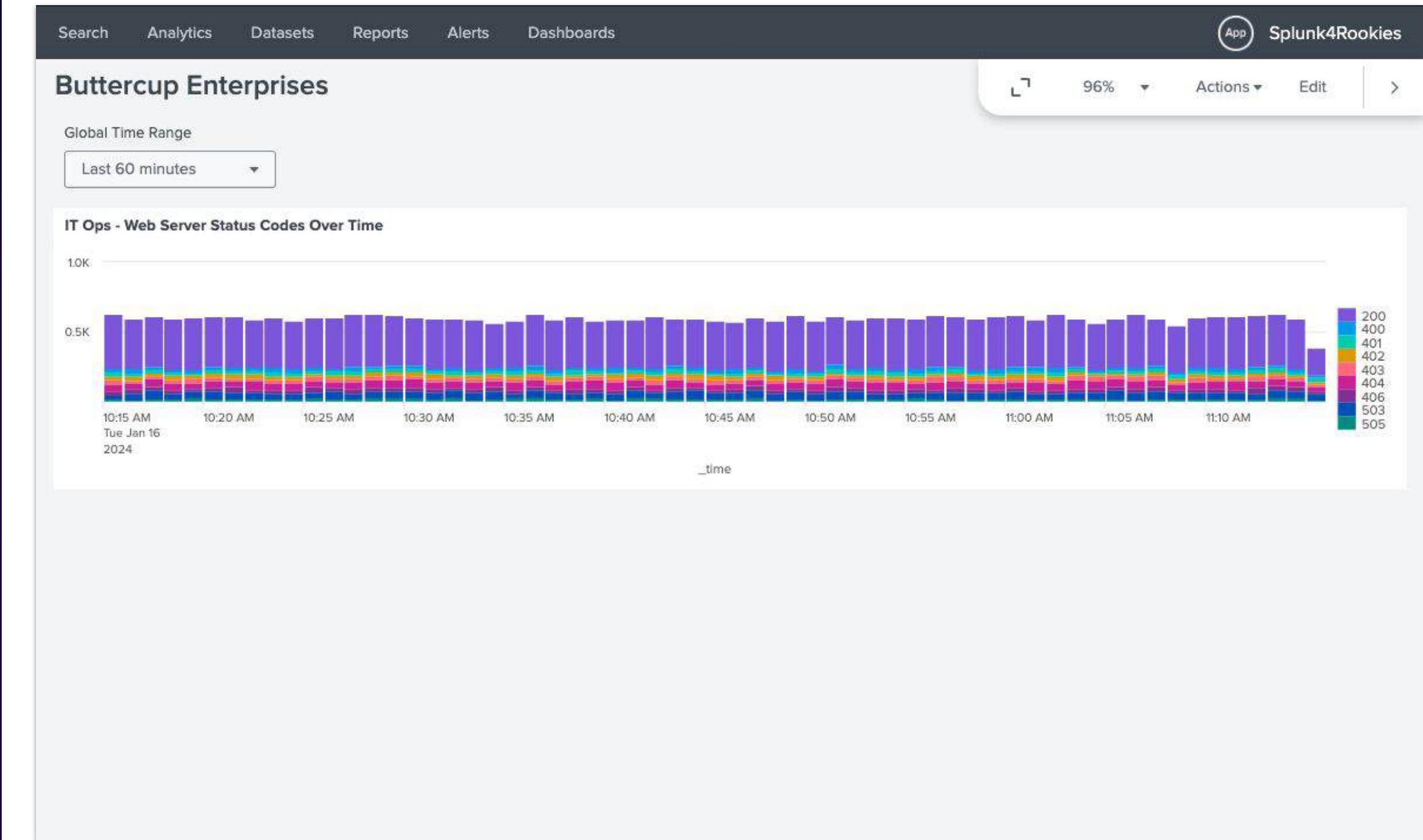
```
index=main sourcetype=access_combined | timechart count by status limit=10
```



Your dashboard 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

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

A screenshot of the Splunk interface showing a table with two columns: 'Time' and 'Event'. An event row is expanded, showing the timestamp '03/04/2023 15:10:51.000' and the event content '1.19.11.11 - - [04/Apr/2023:15:10:51:000] "ADFF9 HTTP/1.1 (Macintosh; In...'. Below the table is a button labeled 'Event Actions ▾' which is highlighted with a red box.

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/2023:15:10:51:000] "Mozilla/5.0 (Macintosh; In...
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



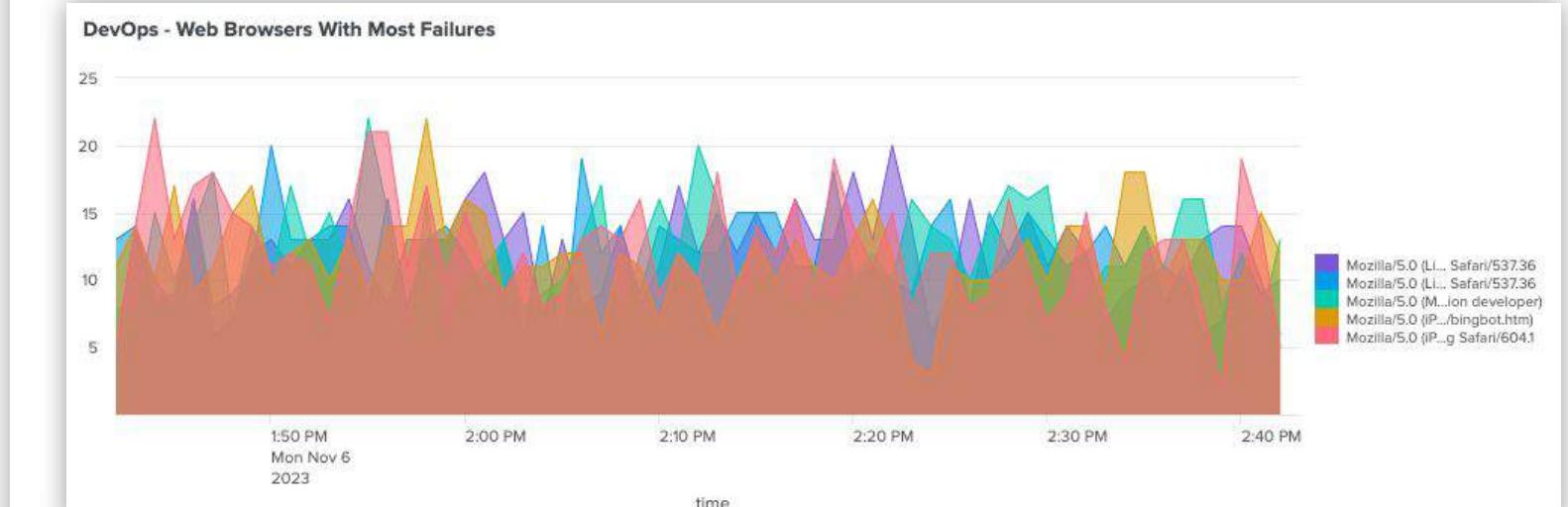
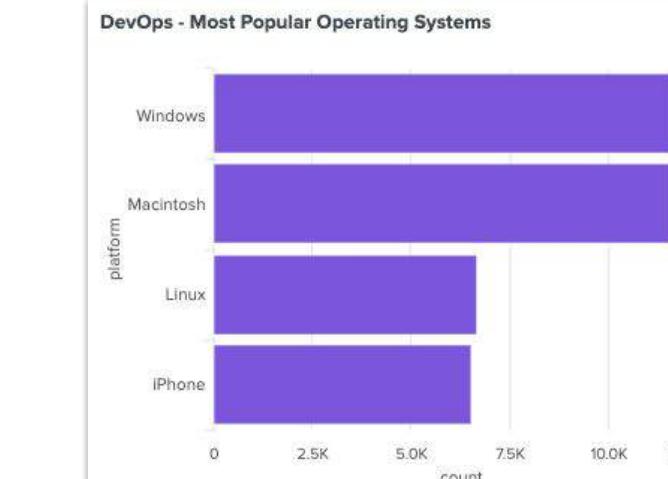
DevOps Team

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





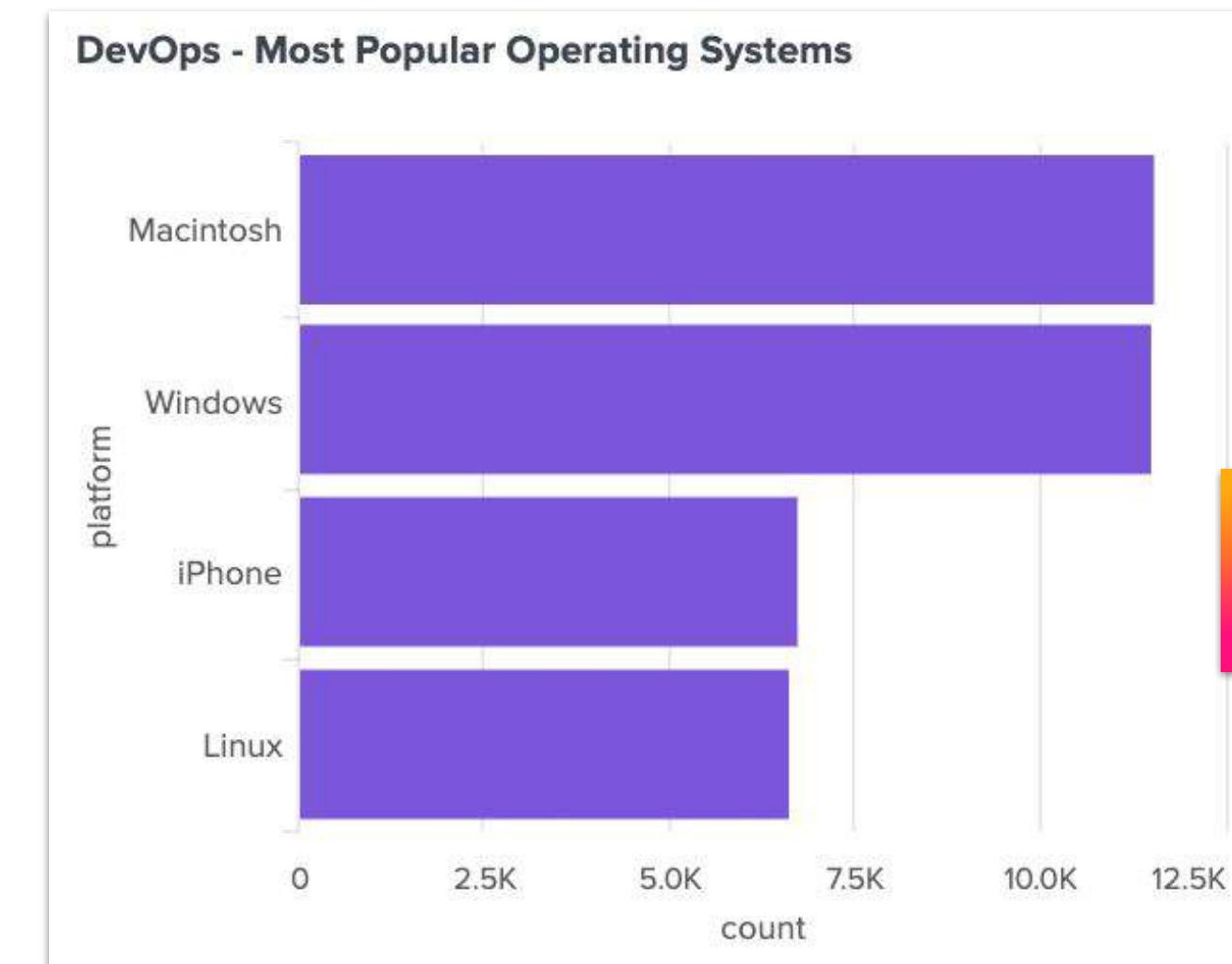
LAB EXERCISE 4

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!



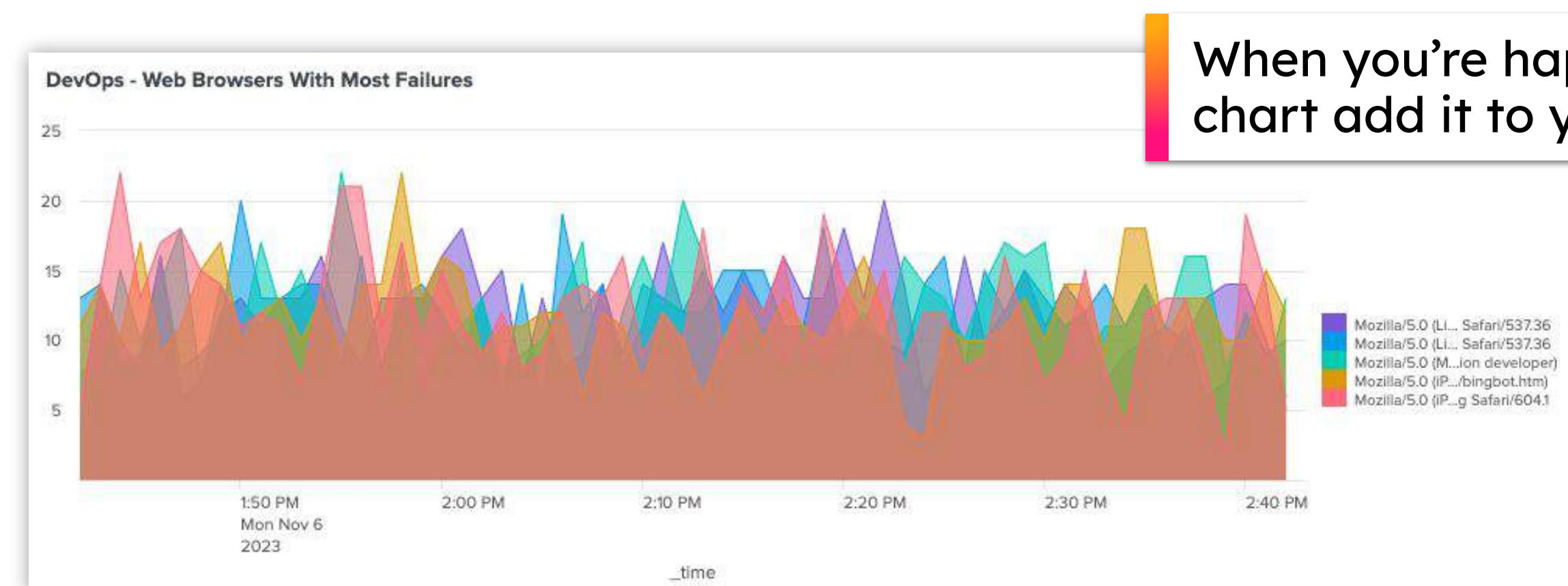
LAB EXERCISE 4

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
```



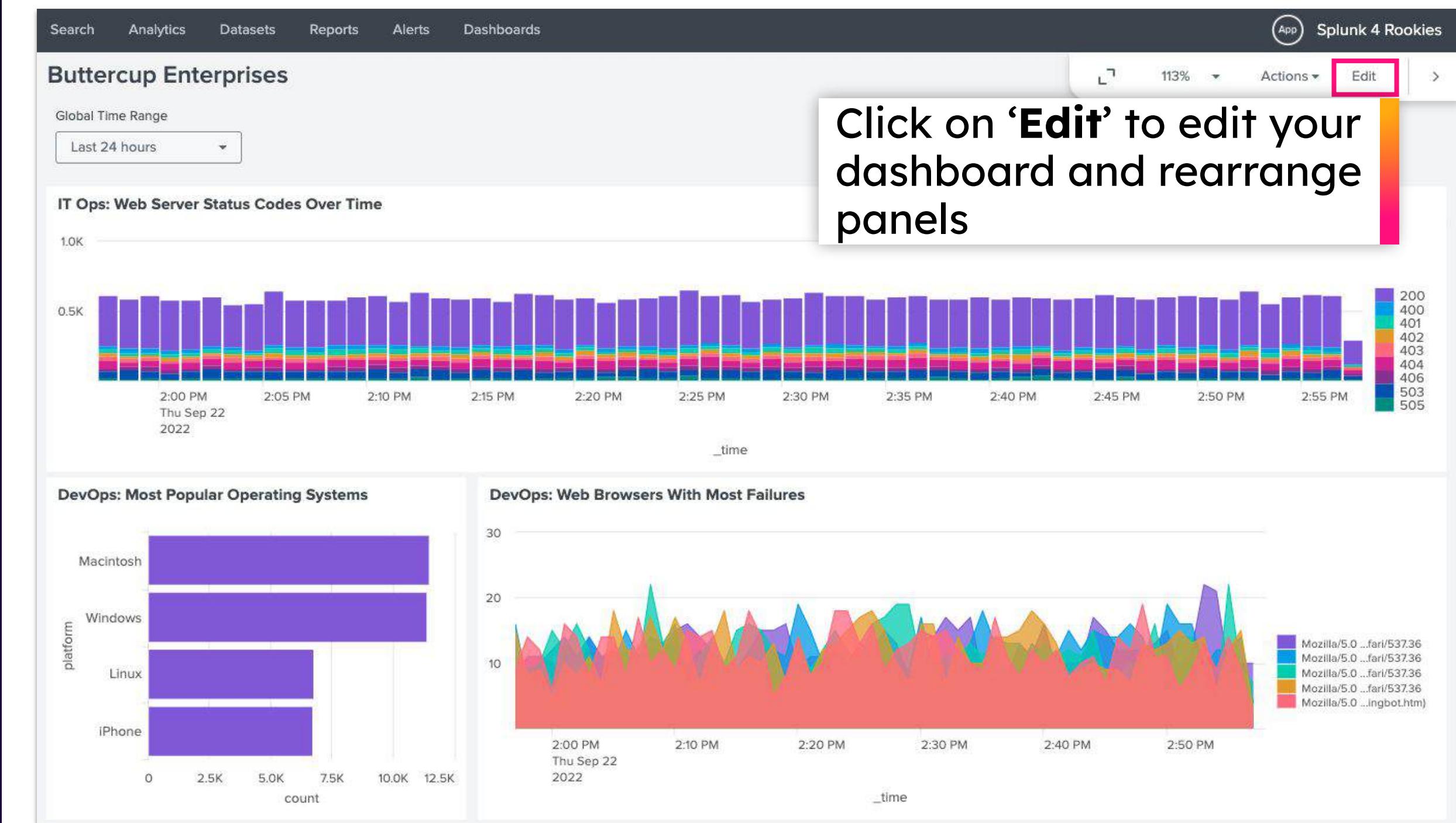
Your dashboard so far...



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>
```

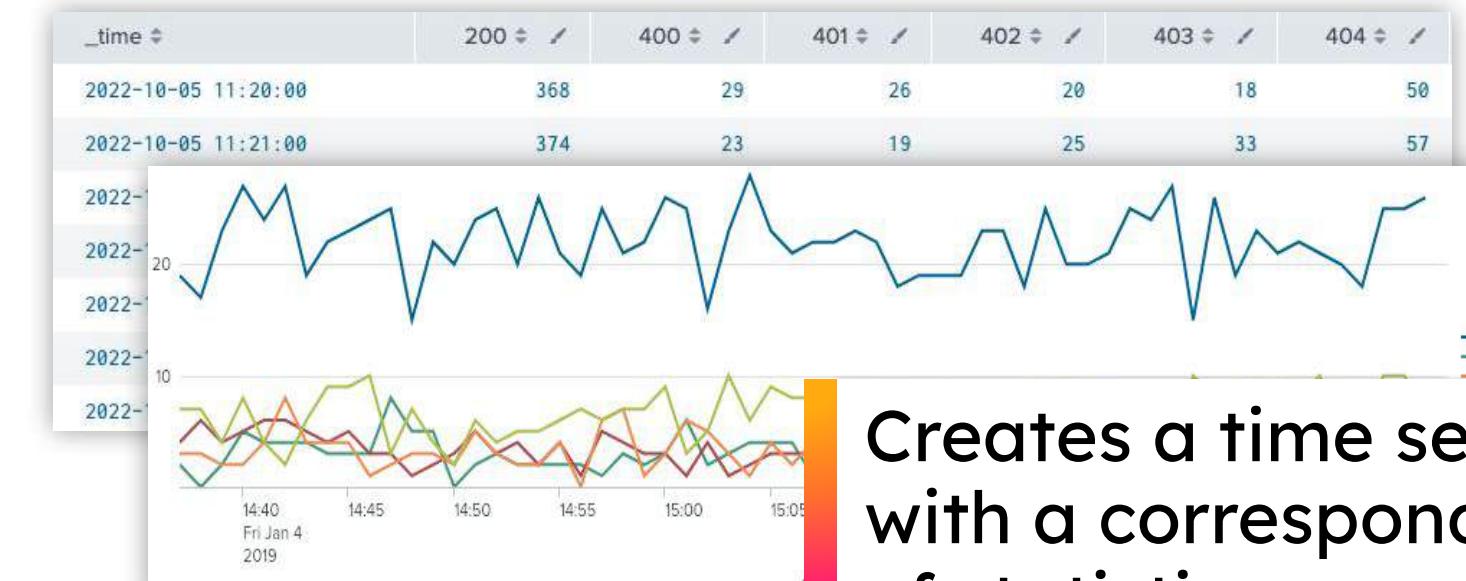
Examples:

```
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
timestamppos 8
a uid 100+
a uri 100+
a uri_path 2
a uri_query 100+

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

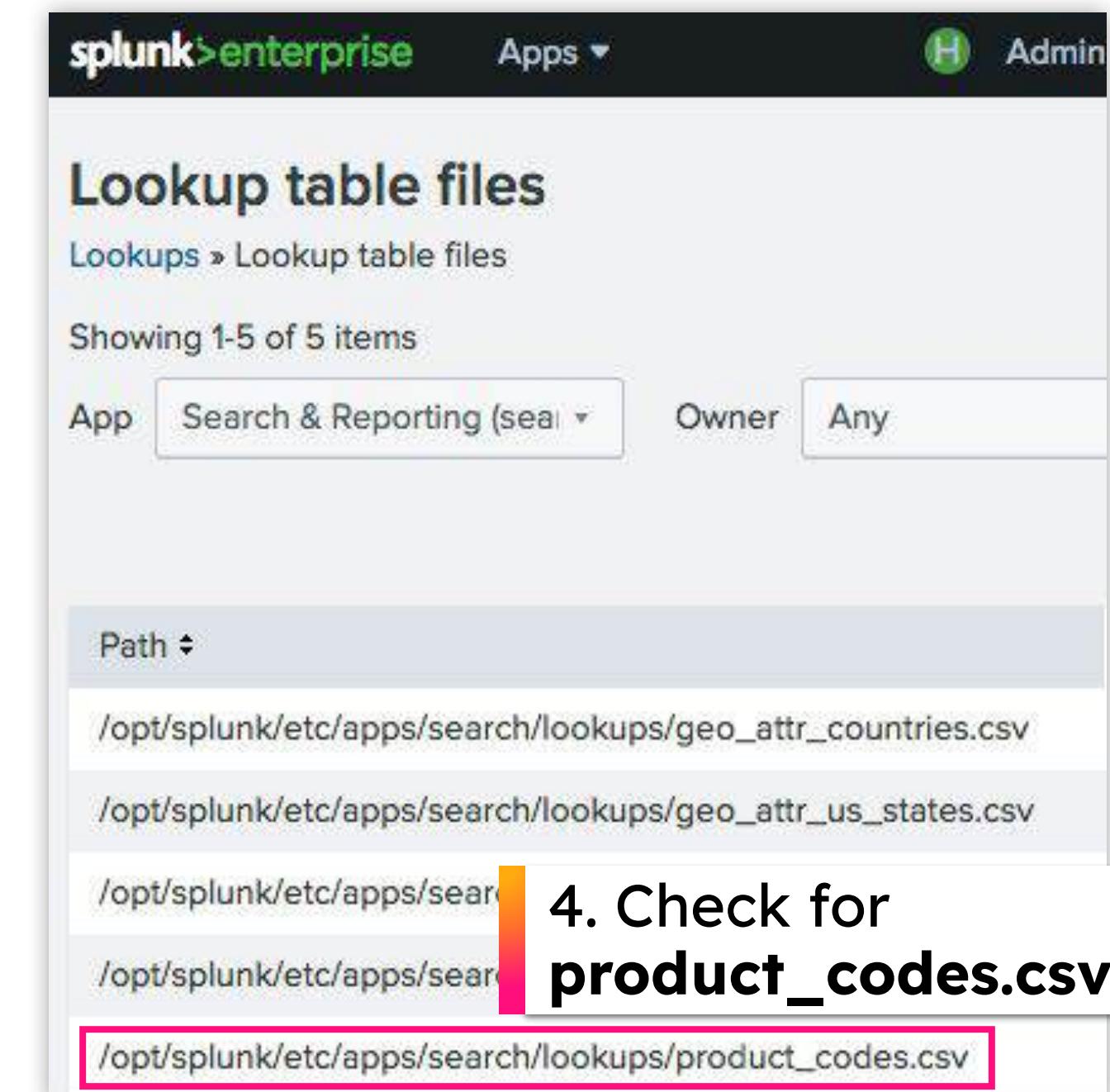
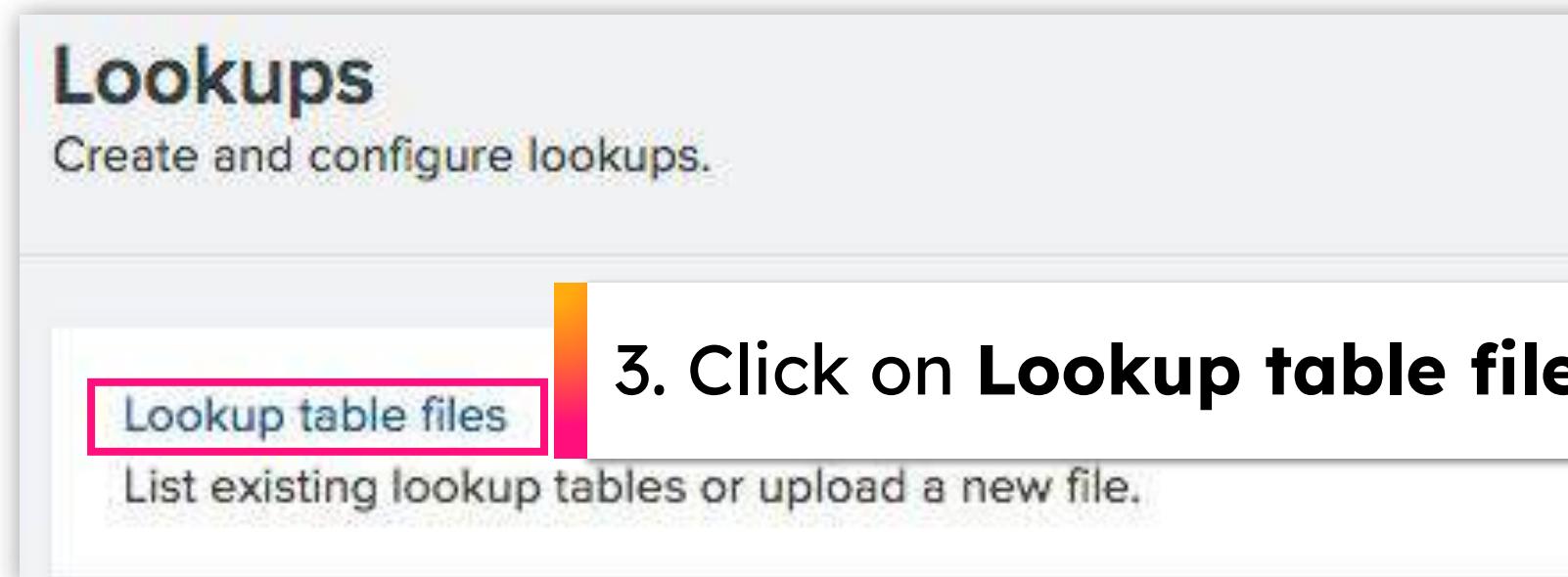
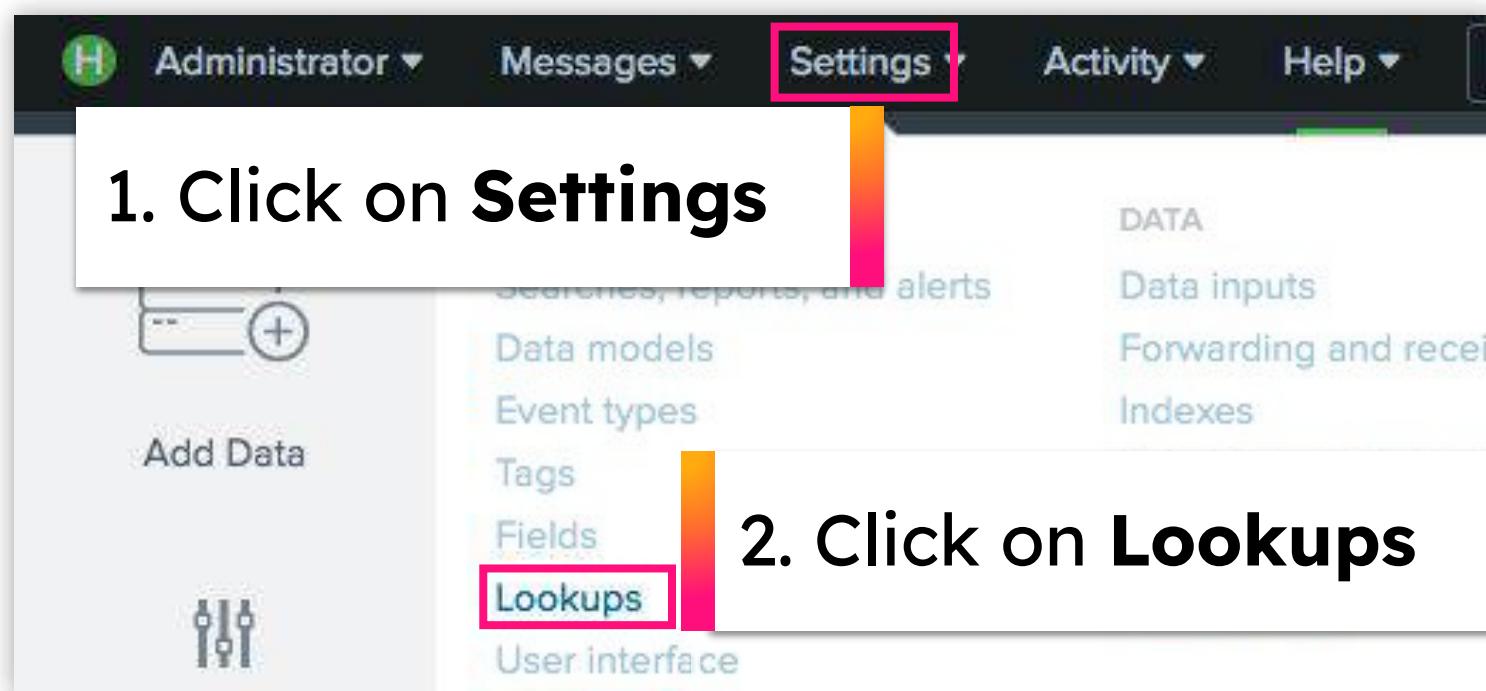
We have '**product_id**' in our data, but no price information!

This is the information we need!

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

Verify That the Lookup File Exists

A lookup file has already been uploaded for you!



Enriching Data with the `lookup` Command

Usage:

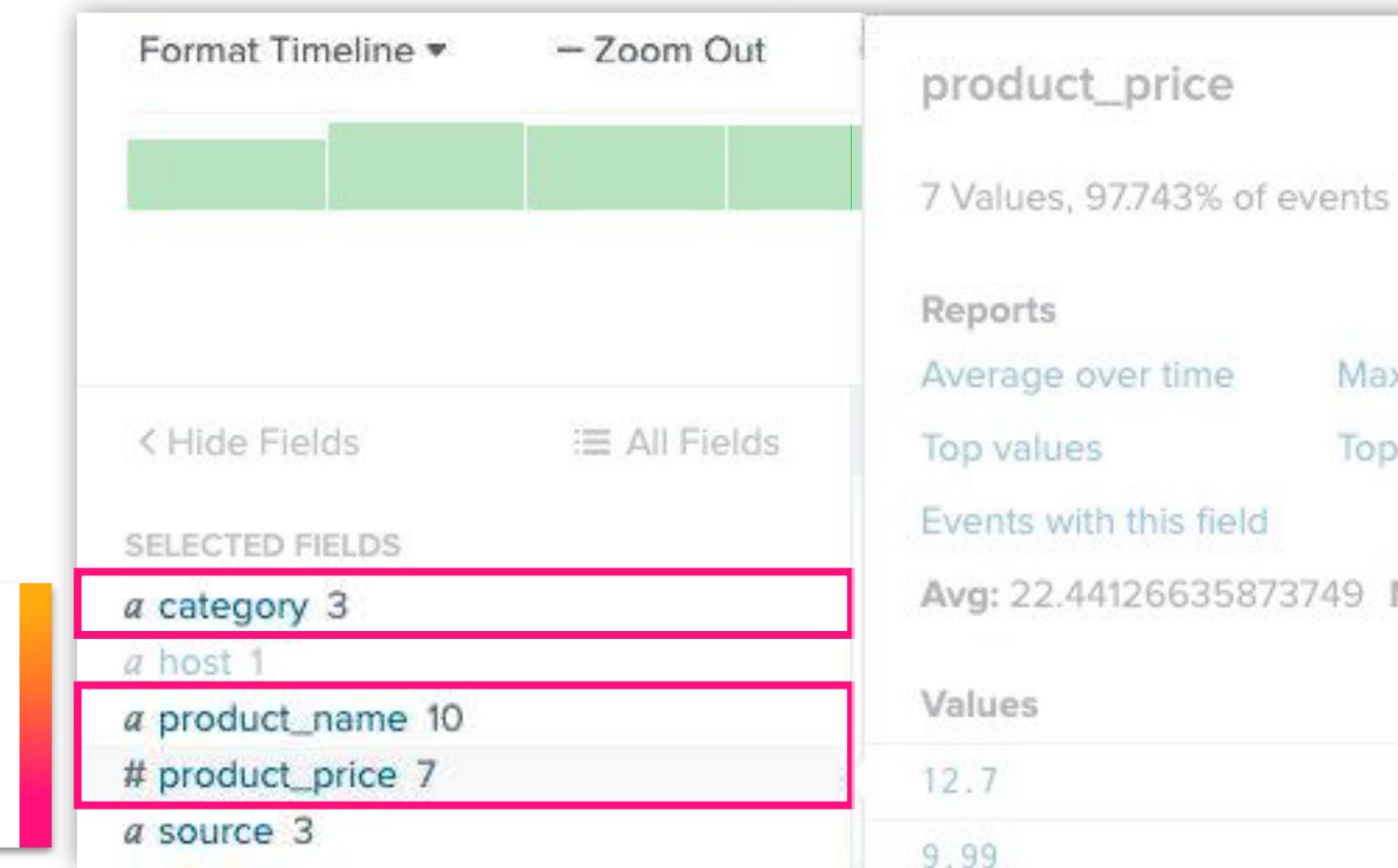
```
<your search> | lookup product_codes.csv product_id
```

**Splunk command
to enrich data
on-the-fly**

**The name of the
lookup file
uploaded to Splunk**

**The field to join on - ‘product_id’
is the field that exists in both the
Splunk data and the lookup file**

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





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





LAB EXERCISE 5

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)
```



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

Your dashboard so far...



IT Operations team



DevOps team



Business Analytics team



The dashboard is titled "Buttercup Enterprises" and includes the following sections:

- Business Analytics - Lost Revenue:** Displays a large value of "\$121.56" with a red arrow indicating an increase of "↑20.29".
- IT Ops - Web Server Status Codes Over Time:** A stacked bar chart showing status codes over time from 9:40 AM to 10:35 AM on Tuesday, January 16, 2024. The y-axis ranges from 0.5K to 1.0K. A legend on the right lists status codes: 200, 400, 401, 402, 403, 404, 406, 503, and 505.
- DevOps - Most Popular Operating Systems:** A horizontal bar chart showing the count of events for different platforms: Windows, Macintosh, Linux, and iPhone. The x-axis ranges from 0 to 12.5K.
- DevOps - Web Browsers With Most Failures:** A line chart showing the count of failures for various web browsers over time from 9:40 AM to 10:35 AM on Tuesday, January 16, 2024. The y-axis ranges from 0 to 30. A legend on the right lists browser versions: Mozilla/5....ari/537.36, Mozilla/5....ari/537.36, Mozilla/5....eveloper), Mozilla/5....ari/537.36, Mozilla/5....ari/537.36, and Mozilla/5....eview/1.0b.

Obtaining Location Information with the `iplocation` and `geostats` Commands

Usage:

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

Generates the ‘tiles’ that will be rendered on the map when visualised

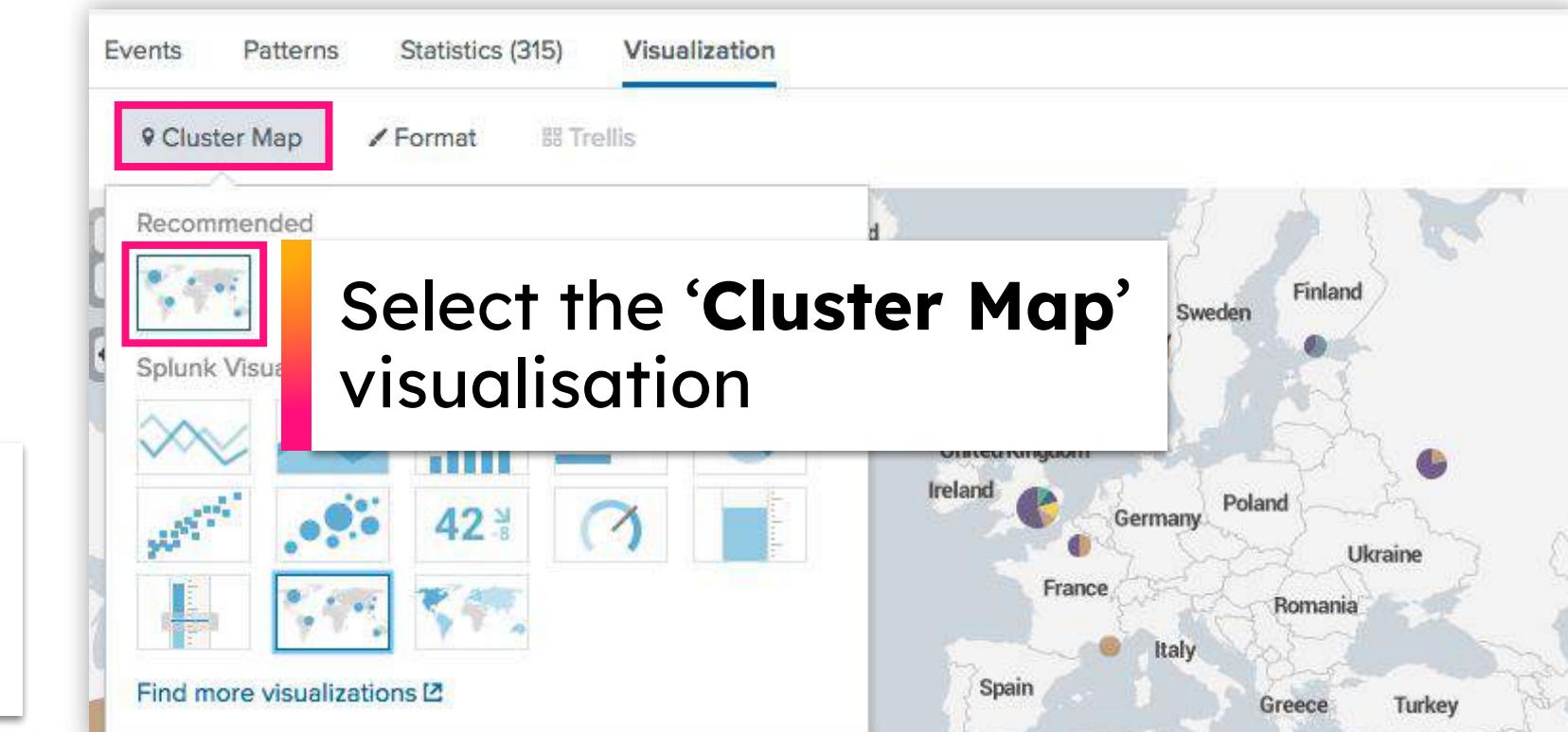
Split your results by a specific field for more detailed analysis

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

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





LAB EXERCISE 6

Security and Fraud Team

Show website activity by geographic location

Solution:

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



Your dashboard so far...



IT Operations team ✓



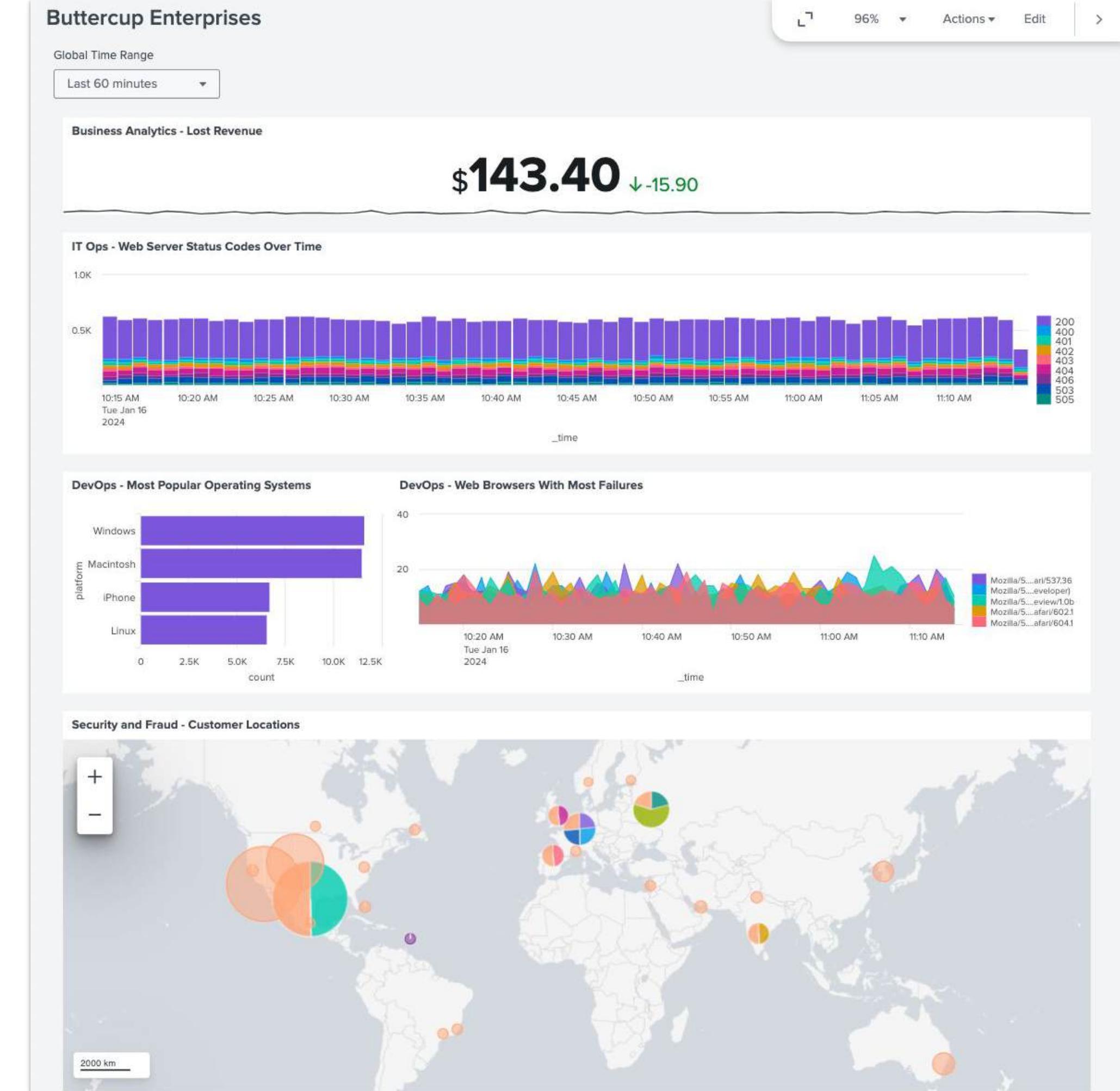
DevOps team ✓



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

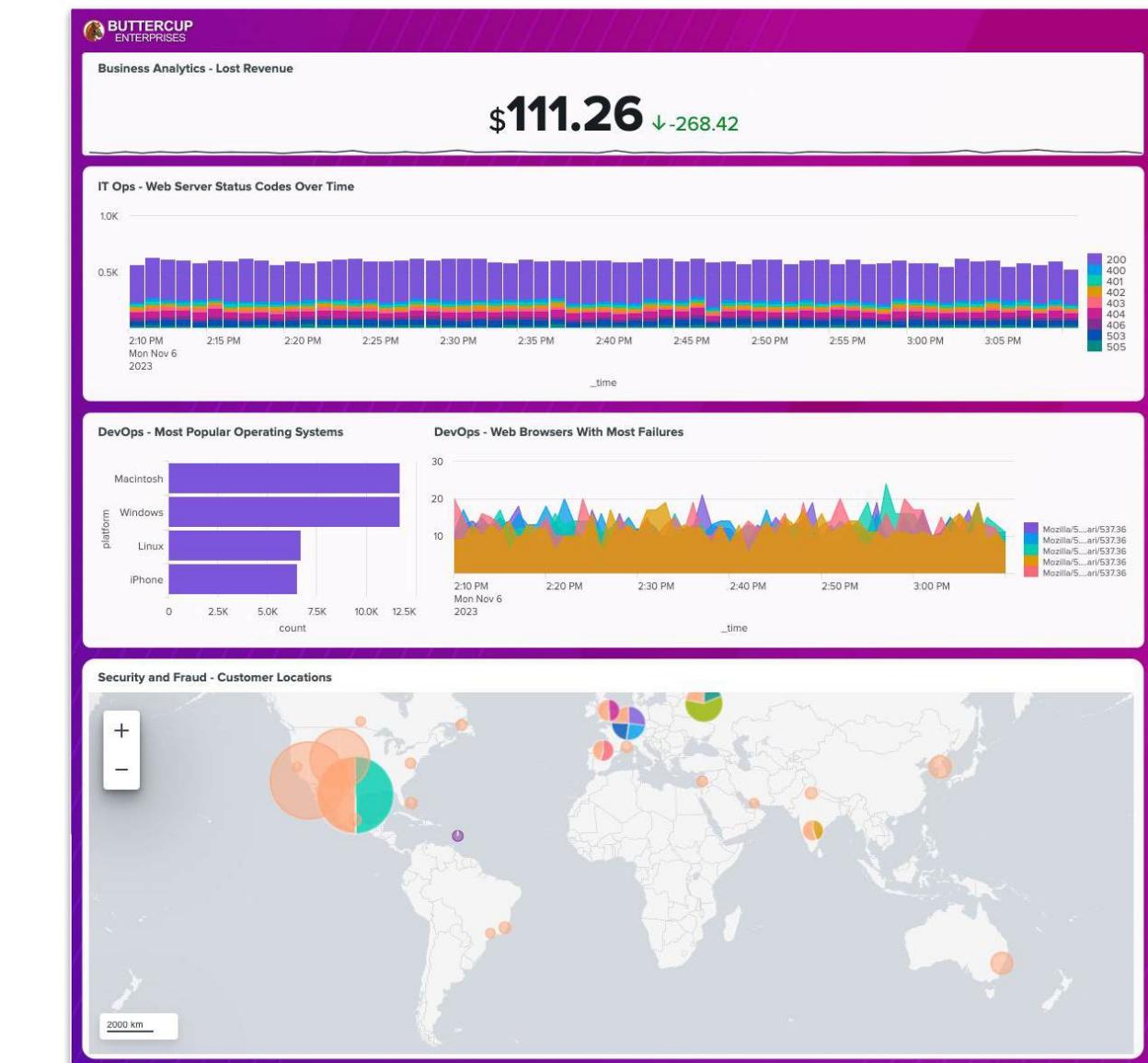


Customise Your Dashboard

Tasks

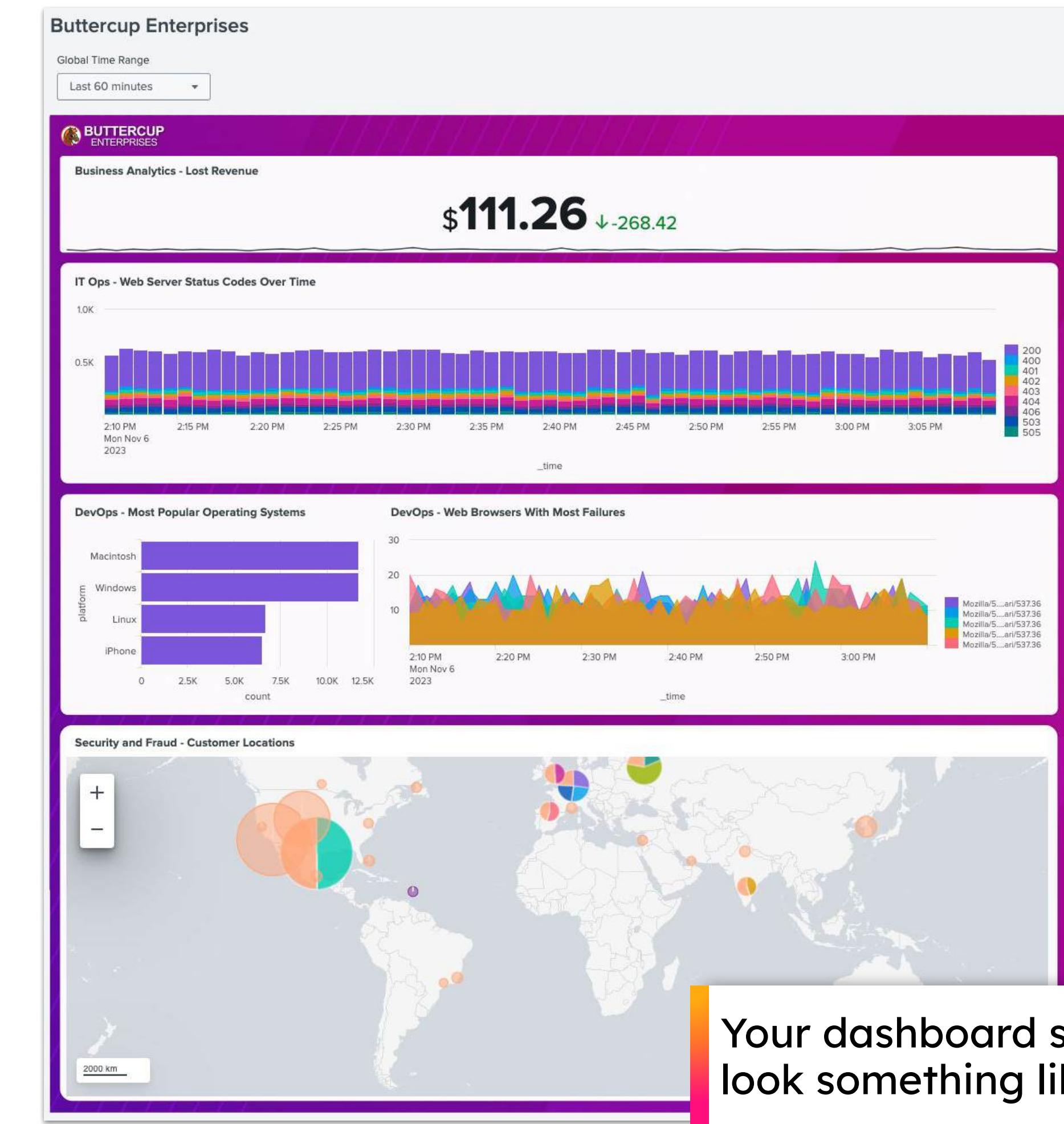
1. Add a custom background image provided by the Buttercup Enterprises Marketing team (<https://splk.it/ButtercupBackground>)
2. Resize your dashboard panels to fit within the boxes on the background image
3. Link your dashboard panels to the global time picker

Goal



You've Finished the Hands-on Exercises!

-  IT Operations team ✓
-  DevOps team ✓
-  Business Analytics team ✓
-  Security and Fraud team ✓
-  Dashboard with custom background ✓



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

The screenshot shows the homepage of the Splunk Community website. At the top, there's a navigation bar with links for Community, Splunk Answers, News & Education, Community Lounge, Apps and Add-ons, User Groups, and Resources. A "Sign In" button is also visible. Below the navigation is a large banner featuring four diverse individuals cheering. To the right of the banner is a search bar with the placeholder "Search the community". Below the banner, it says "260K Members • 2,030 Online • 147K Posts". The main content area has a grey header with the text "Welcome to the Splunk Community! Get started by visiting our [welcome hub](#) to learn more about the site. We're so glad you're here!" and "Check out the Splunk Community Dashboard [Challenge](#) for a chance to win prizes". Below this, there are five cards with icons and titles: "Getting Started" (paper airplane icon), "Community Blog" (person icon), "Splunk Answers" (speech bubbles icon), "User Groups" (people icon), and "Office Hours" (building icon). Each card also has a brief description.

Welcome to the Splunk Community! Get started by visiting our [welcome hub](#) to learn more about the site. We're so glad you're here!

Check out the Splunk Community Dashboard [Challenge](#) for a chance to win prizes

Getting Started
Learn more about the Splunk Community and how we can help

Community Blog
Community happenings, product announcements, and Splunk news

Splunk Answers
Troubleshoot problems with help from the community

User Groups
Meet up with other Splunk practitioners, virtually or in-person

Office Hours
Webinar-style deep dives and workshops for hands-on guidance

Splunk Events

<https://splunk.com/events>

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



<https://conf.splunk.com>

- Join us in Boston!
8 - 11 September 2025
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!

The screenshot shows the Splunk Events page. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Company, Support, a search icon, a globe icon, a user icon, and a "Free Splunk" button. The main heading is "Splunk Events". Below it, a sub-headline says "Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community." A search bar and a "Filter all" section with dropdown menus for Regions, Event Types, and Solutions are on the left. The right side is divided into two sections: "Featured Events" and "Upcoming Events". The "Featured Events" section displays three cards for "Black Hat USA 2024", "Gartner IT Symposium/Xpo", and "AWS re:Invent 2024", each with a photo of a speaker and details about the event location and dates. The "Upcoming Events" section is partially visible at the bottom.

Featured Events

- INDUSTRY EVENT**
Black Hat USA 2024
LAS VEGAS
AUG 03, 2024 - AUG 08, 2024
[Register Now >](#)
- INDUSTRY EVENT**
Gartner IT Symposium/Xpo
ORLANDO
OCT 21, 2024 - OCT 24, 2024
[Register Now >](#)
- INDUSTRY EVENT**
AWS re:Invent 2024
LAS VEGAS
DEC 01, 2024 - DEC 06, 2024
[Register Now >](#)

Upcoming Events

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!



Products

Solutions

Why Splunk?

Resources

Splexicon

Support



Documentation

Search in docs

Splexicon the Splunk glossary



Platform

Splunk Cloud Platform™
Splunk® Enterprise
Splunk® Universal Forwarder
Splunk® Data Stream Processor
Splunk® Cloud Services



Security

Splunk® Attack Analyzer
Splunk® Asset and Risk Intelligence
Splunk® Enterprise Security
Splunk® Mission Control
Splunk® SOAR (Cloud)
Splunk® SOAR (On-premises)
Splunk® User Behavior Analytics
Splunk® Security Essentials
Splunk® Security Content
[Show more ▾](#)



IT

IT Operations Overview
Splunk® IT Service Intelligence
Splunk® IT Essentials Work
Splunk® IT Essentials Learn
Splunk® App for Content Packs
Splunk® On-Call



Observability

Splunk® Observability Cloud
Splunk® Infrastructure Monitoring
Splunk® APM
Splunk® Log Observer Connect
Splunk® Real User Monitoring
Splunk® Synthetic Monitoring



Apps and add-ons

Splunk® Supported Add-ons
Splunk® OpenTelemetry Collector for Kubernetes
Splunk® Add-on for OpenTelemetry Collector
Splunk® Add-on Builder
Splunk® Firehose Nozzle for VMware Tanzu
Splunk® Connect for Kafka
Splunk® Connect for Zoom
Splunk® Connected Experiences



Developer tools

Splunk® Add-on Builder
Splunk® SDKs
Splunk® Web Framework

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

The screenshot shows the homepage of the Splunk Lantern Customer Success Center. At the top, there's a navigation bar with the Splunk logo, a CISCO company, and links to 'Lantern Home', 'Documentation', 'Community', 'Training & Certification', 'Support Portal', 'User Groups', and a user profile icon. A 'Free Splunk' button is also present. The main title 'Splunk Lantern Customer Success Center' is prominently displayed in large, bold, black font. Below it, a sub-headline reads: 'Let Splunk experts light your path toward gaining valuable data insights, achieving your key use cases, and managing Splunk more efficiently.' A pink link 'Click here to learn more.' is provided. A search bar with a magnifying glass icon is located below the headline. To the right, there's a large graphic featuring a lantern icon inside a circle, set against a background of overlapping colored bands (pink, red, orange). Three article cards are visible at the bottom:

- FEATURED: SPLUNK APM**
Monitoring applications using OpenAI API and GPT models with OpenTelemetry and Splunk APM
By leveraging OpenTelemetry and Splunk Application Performance Monitoring, you can gain valuable insights into the performance of an AI assistant application and the effectiveness of different GPT models. The integration provides a comprehensive monitoring solution that ensures your application's
- FEATURED: EDGE PROCESSOR**
Scaling Edge Processor infrastructure
There are a number of factors that can affect the required scale of your Splunk Edge Processor infrastructure, including changes in data volume, use cases, and pipeline complexity. This article series looks at scaling Splunk Edge Processor using Amazon EKS.
- FEATURED: MISSION CONTROL**
Enhancing endpoint monitoring with threat intelligence
When investigating endpoints, SOC analysts need as much telemetry as possible because there are often many attack vectors in play. Using Splunk Mission Control or Splunk Enterprise Security provides you the most flexibility for configuring many threat intelligence sources to get you the information you need.

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>

- 2200+ 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!

splunkbase* Collections Apps

Submit an App Log In ▾

Get more out of Splunk with applications

Search for apps



Trending Apps on Splunkbase

 Splunk Add-on for Microsoft Windows By Splunk Inc. <small>*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on f...</small> PLATFORM Splunk Enterprise, Splunk Cloud,... RATING ★★★★☆ (45)	 Splunk DB Connect By Splunk Inc. <small>Splunk DB Connect is a generic SQL database extension for Splunk that enables easy integration of database...</small> PLATFORM Splunk Enterprise, Splunk Cloud,... RATING ★★★★☆ (132)	 Splunk Add-on for Unix and Linux By Splunk Inc. <small>*** Important: Read upgrade Instructions and test add-on update before deploying to production *** There are changes to...</small> PLATFORM Splunk Enterprise, Splunk Cloud,... RATING ★★★★☆ (52)	 Splunk Enterprise Security By Splunk Inc. <small>Splunk Enterprise Security (ES) solves a wide range of security analytics and operations use cases including...</small> PLATFORM Splunk Enterprise, Splunk Cloud RATING ★★★★★ (216)
---	--	---	---

Training & Certification

<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

The screenshot shows the Splunk Course Catalog page. At the top, there's a navigation bar with links for Products, Solutions, Why Splunk?, Resources, Company, Support, a search icon, a globe icon, a user icon, and a "Free Splunk" button. Below the navigation is a secondary navigation bar with links for Training & Certification, Learning Paths, Course Catalog (which is highlighted in pink), Free Training, Certification, Partnerships, and Learning Rewards. The main content area features a large heading "Course Catalog" and a sub-headline: "See all of the courses available to help you turn data into doing, shown in recommended order. Expand your knowledge and understanding of Splunk." Below this is a "Start Your Journey" button. To the right, there's a photo of three people (two women and one man) smiling and interacting. A "Leaderboard" sidebar is visible on the far left. The main content area displays three course cards: "Intro to Splunk", "Using Fields", and "Scheduling Reports & Alerts". Each card includes a course icon, the title, a brief description, and a "COURSE" label.

Course Catalog

See all of the courses available to help you turn data into doing, shown in recommended order. Expand your knowledge and understanding of Splunk.

Start Your Journey

Search

Filter Courses

119 Results [Clear All](#)

Content Type

Certification

Role

Course

Intro to Splunk

This eLearning course teaches students how to use Splunk to create reports and dashboards and explore events using Splunk's Search

Course

Using Fields

This three-hour course is for power users who want to learn about fields and how to use fields in searches.

Course

Scheduling Reports & Alerts

This eLearning course teaches students how to use scheduled reports and alerts to automate processes in their

Thank you

