splunk> 4 rookies

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> a CISCO company

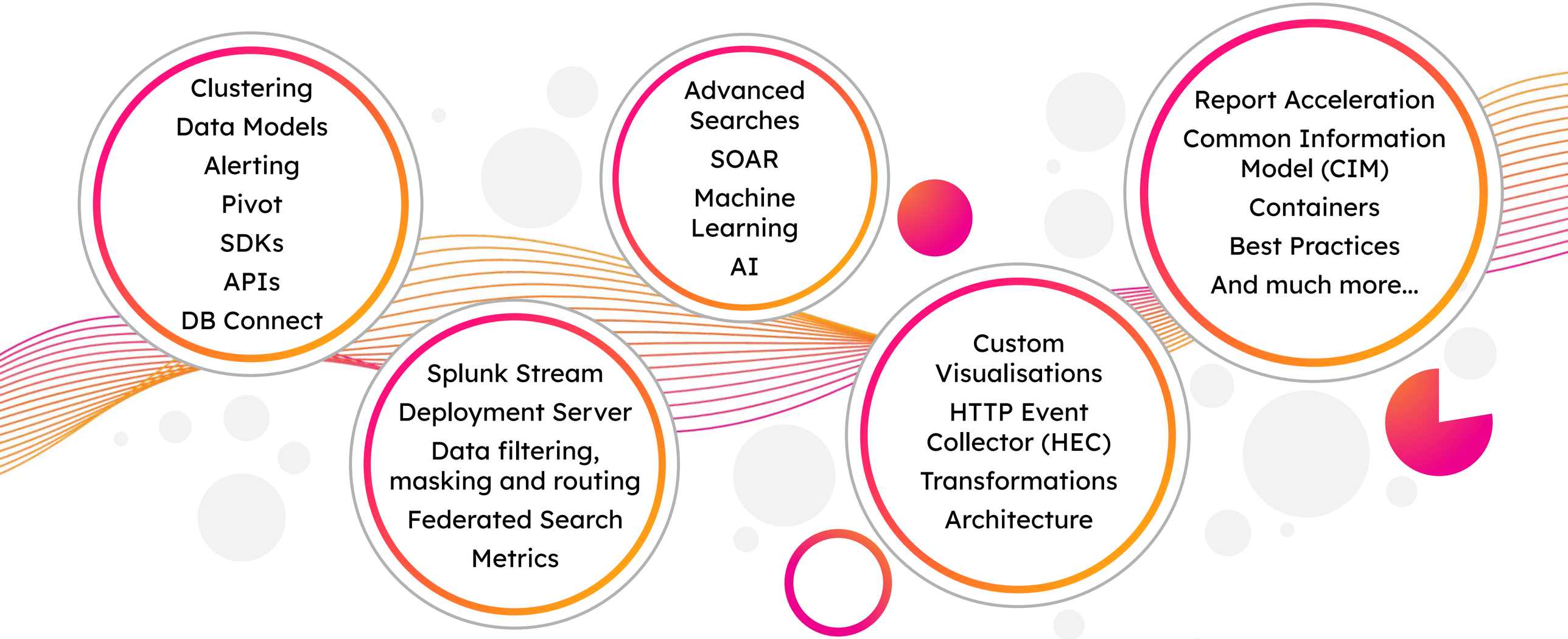
Please introduce yourself!

- 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

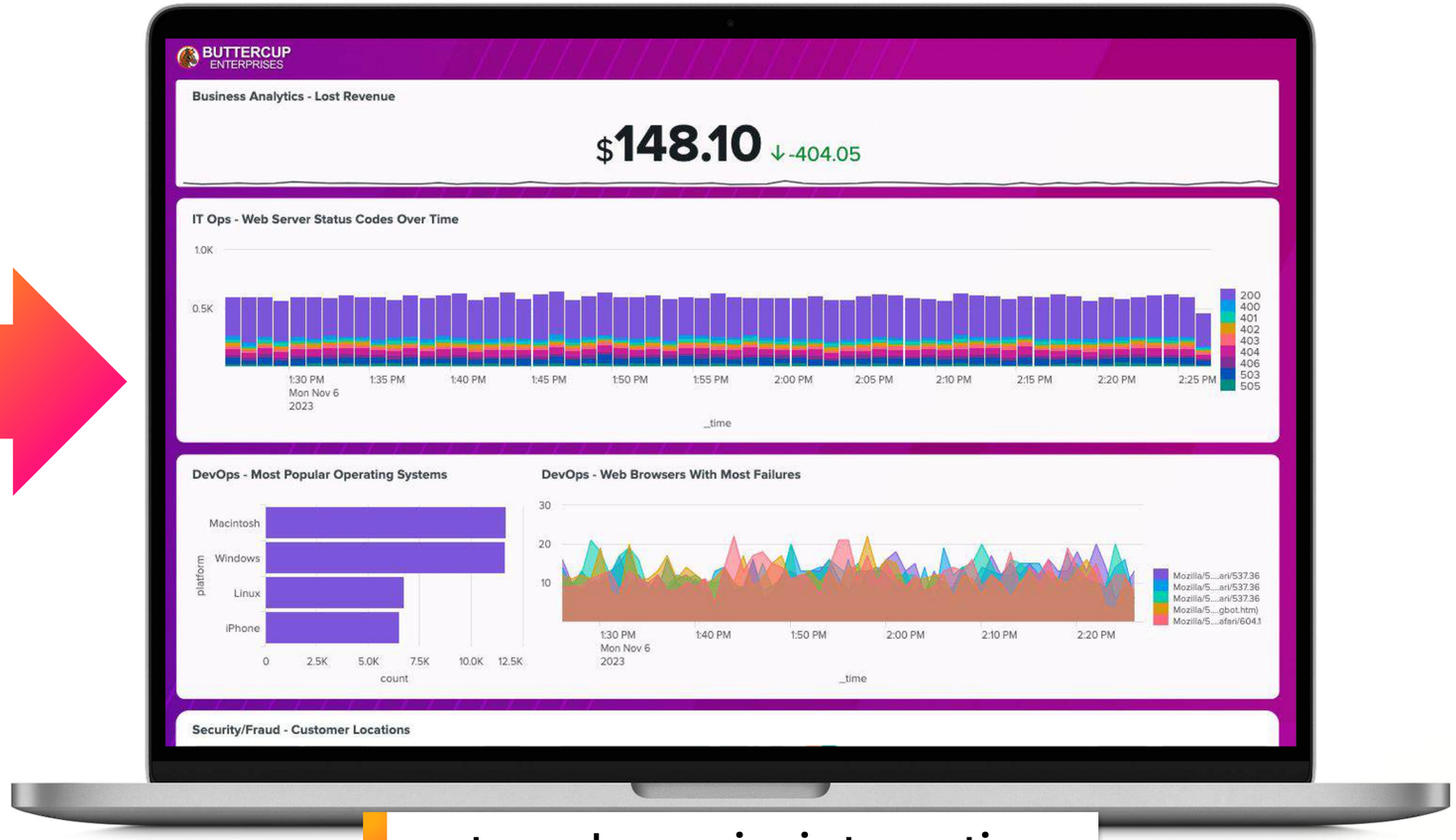
There’s a Lot More to Splunk



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

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.

Network

Architects

Engineers

Operations

SREs

Audit

Developers

IT

Security

How do you prepare for and recover from unexpected disruptions?

Build digital resilience with Splunk.

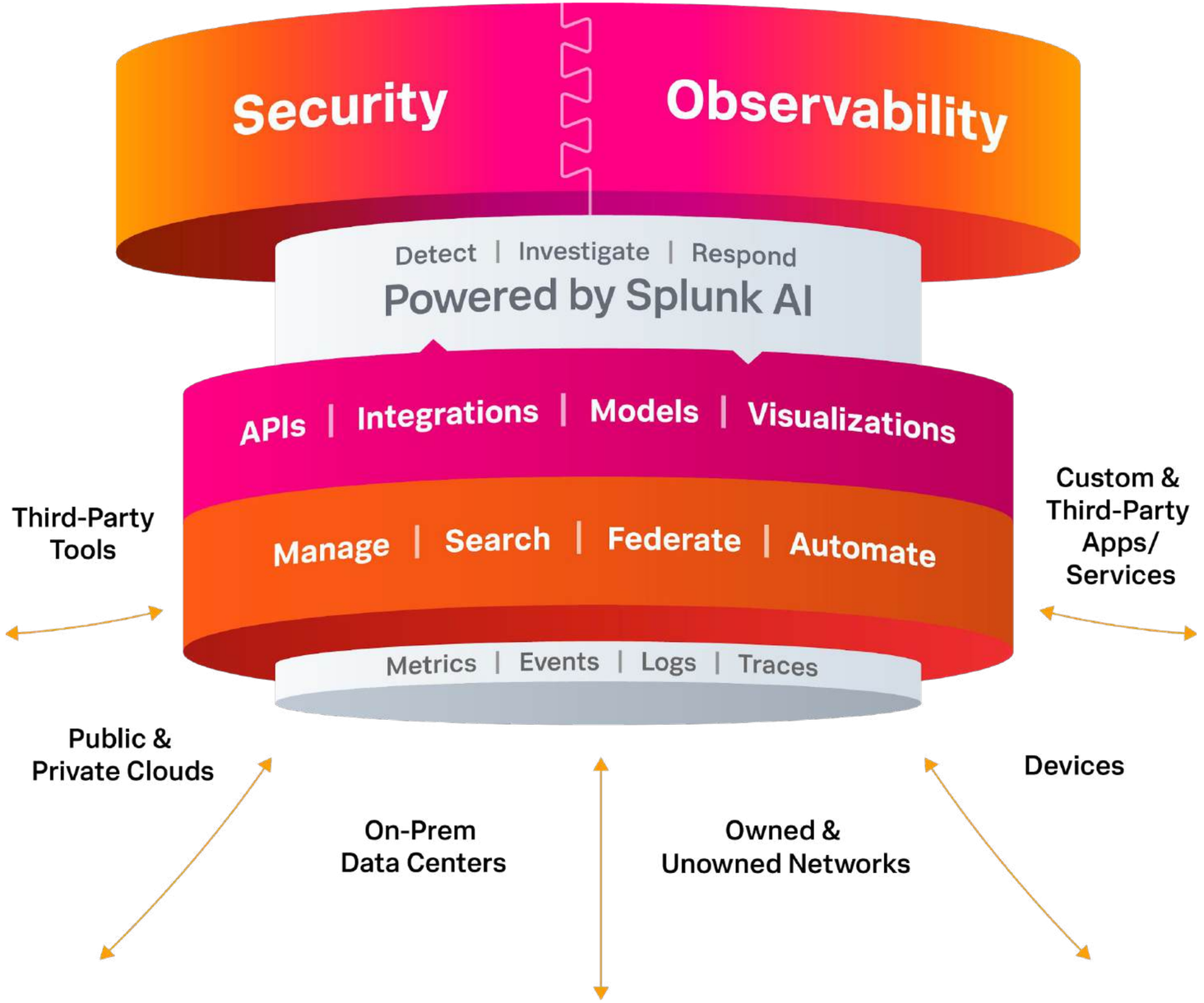
Splunk brings SecOps, ITOps and engineering together to…

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+ aws

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

splunk>cloud™

- **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**

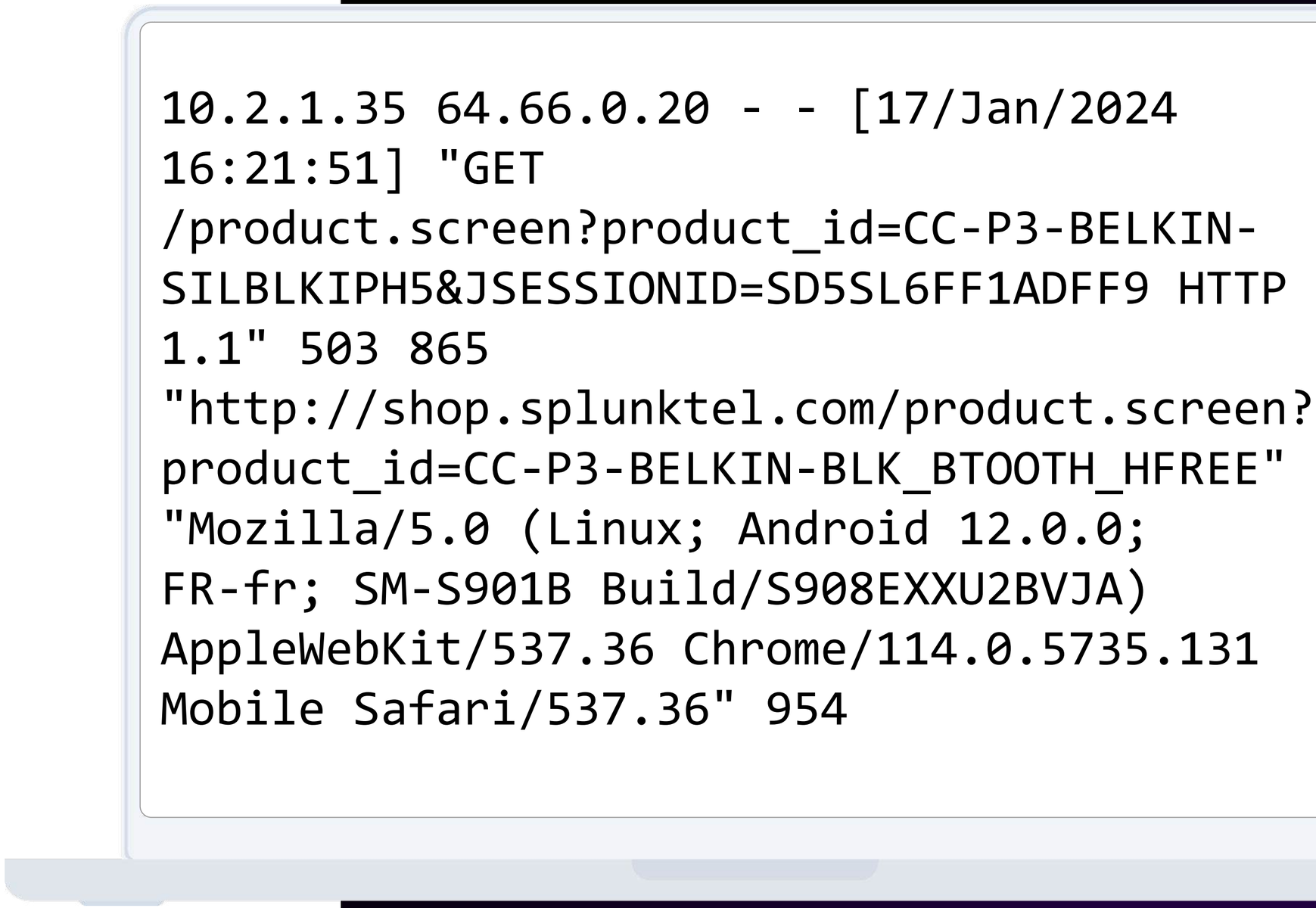
Flexible options for data collection and forwarding

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

What is a Splunk Universal Forwarder?

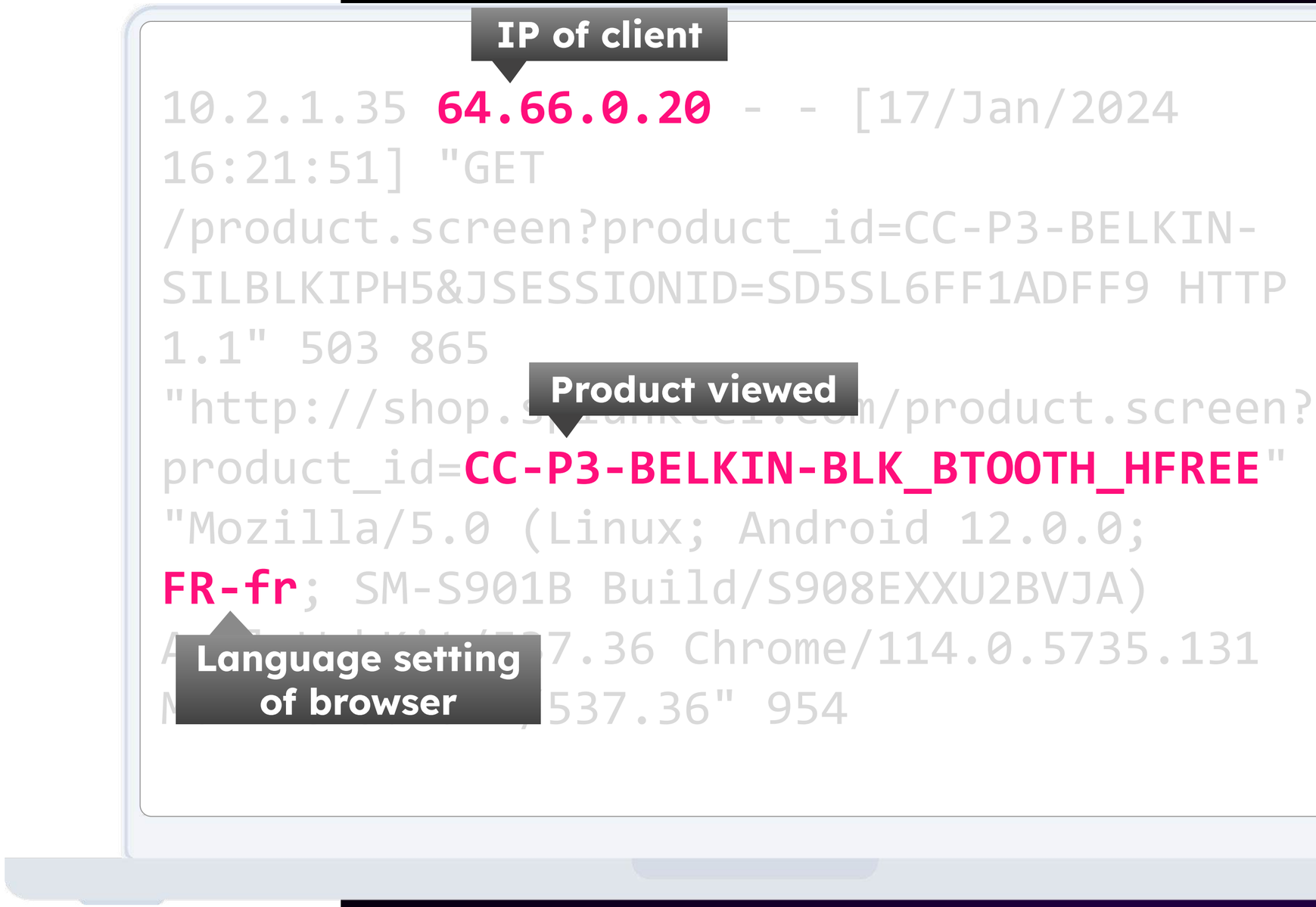
- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
  - Buffering / guaranteed delivery
  - Encryption
  - Compression
  - Load balancing
  - And more!
- Very small footprint
- Just forwards data – no parsing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

Machine data is valuable not complex!



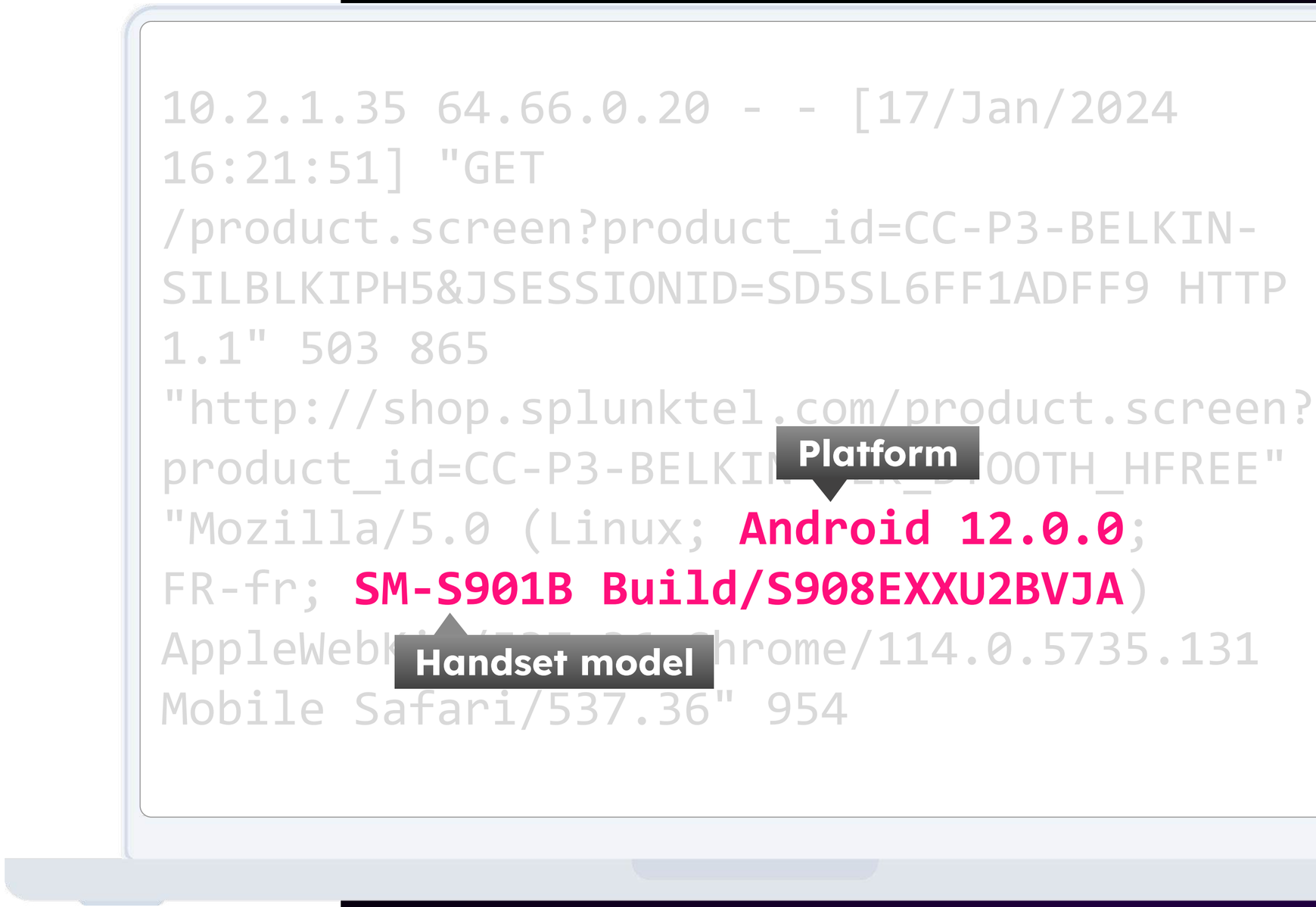
Marketing Use Case

Show the top products viewed by language



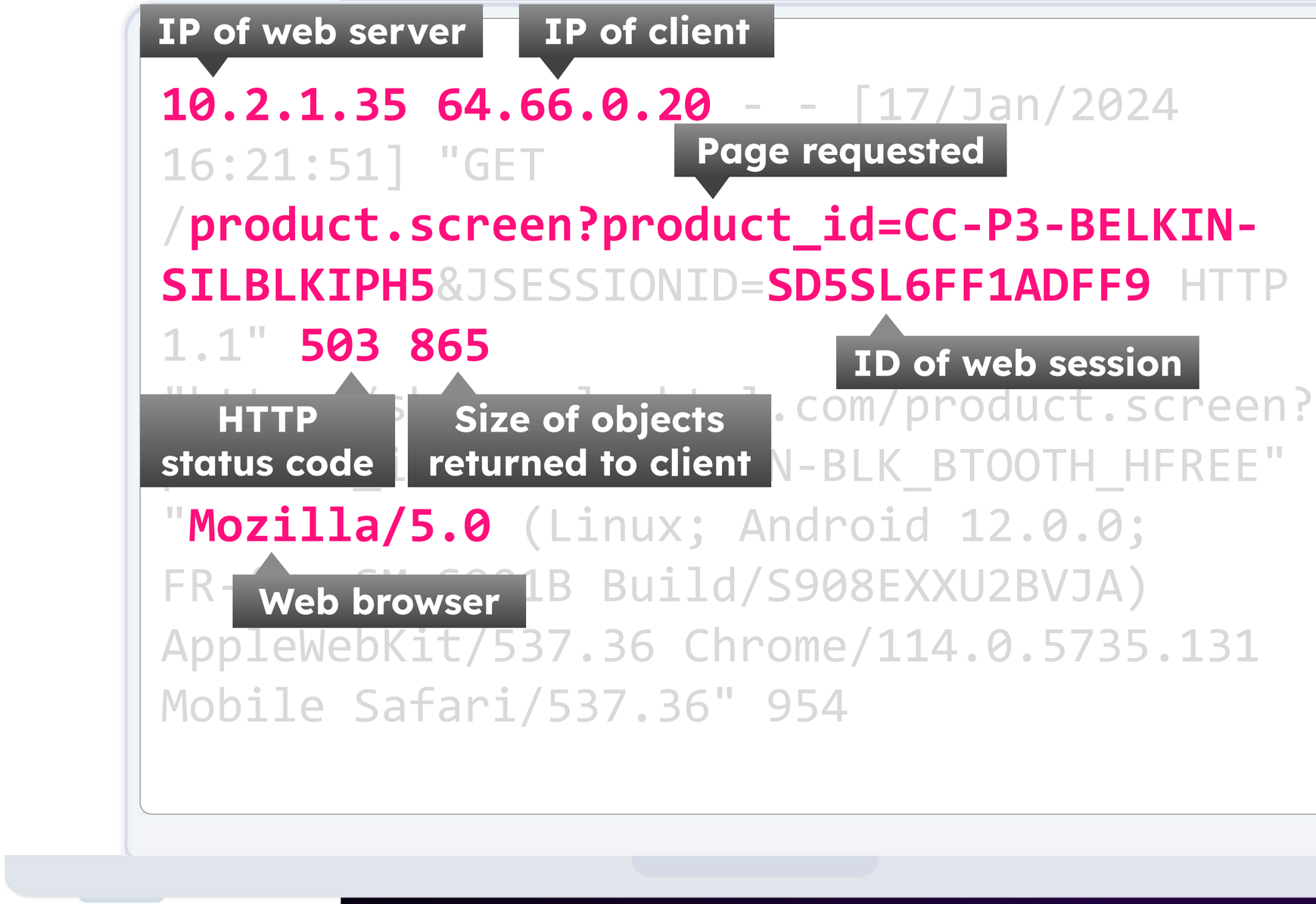
DevOps Use Case

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



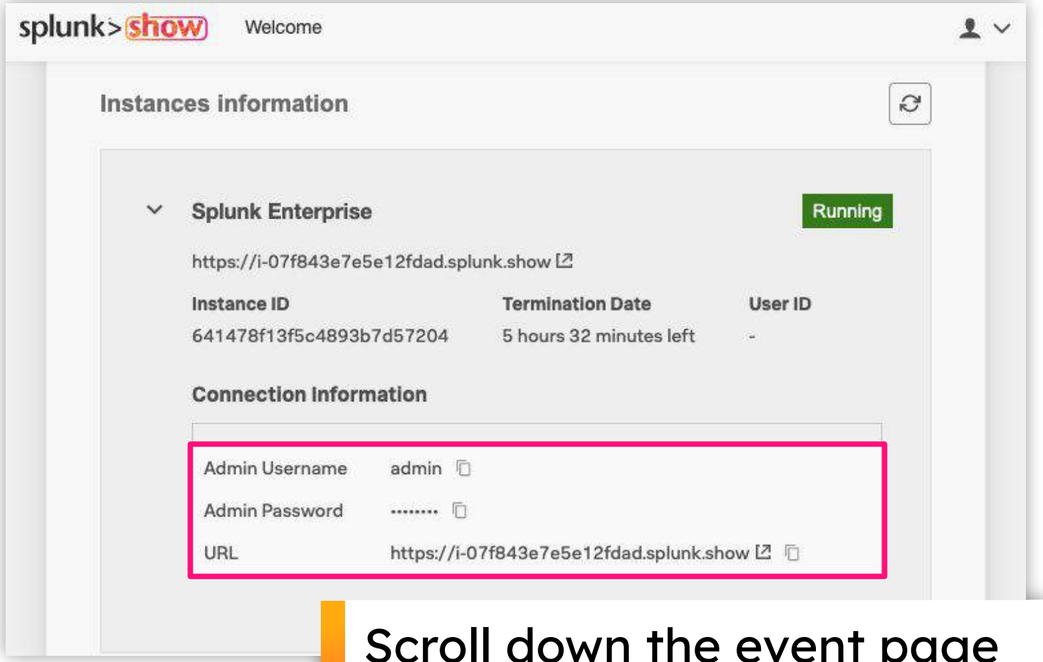
IT Ops Use Case

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



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

- 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

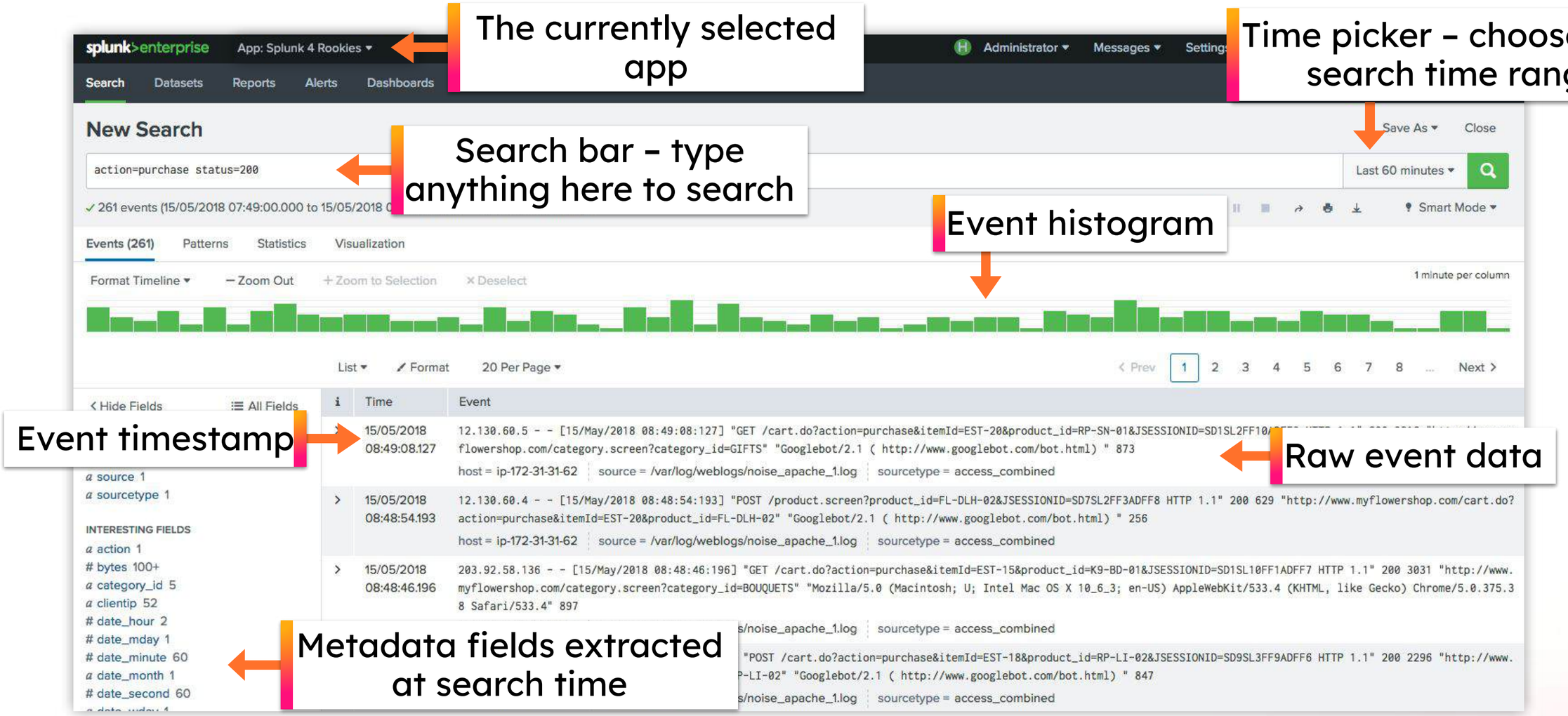
Create an App and Add Some Data

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

Reminder
Download the lab guide for step-by-step instructions!

Open your app and have a play!



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=8a9dfff3-2e4f-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/113.0.5672.92 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**

What Does the Business Want to See?

We need to create a dashboard with four views:

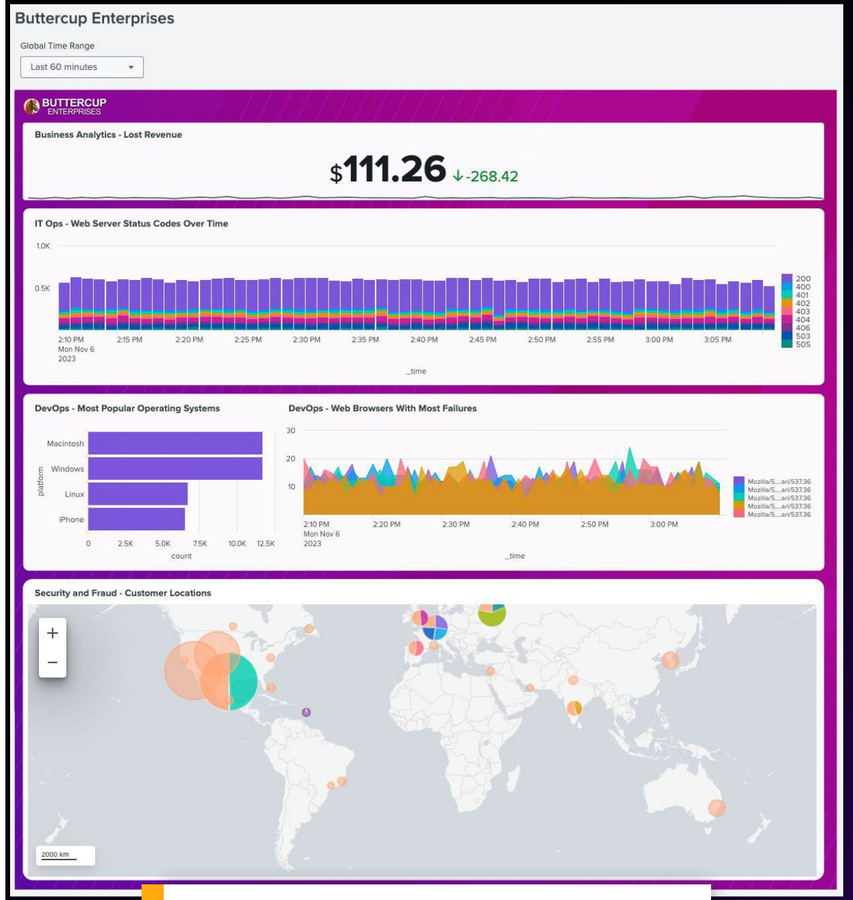
IT Operations team: Investigate successful versus unsuccessful web server requests over time

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!

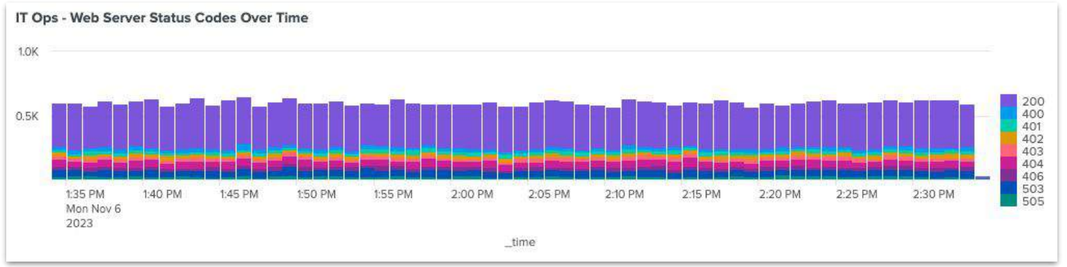
IT Operations Team

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

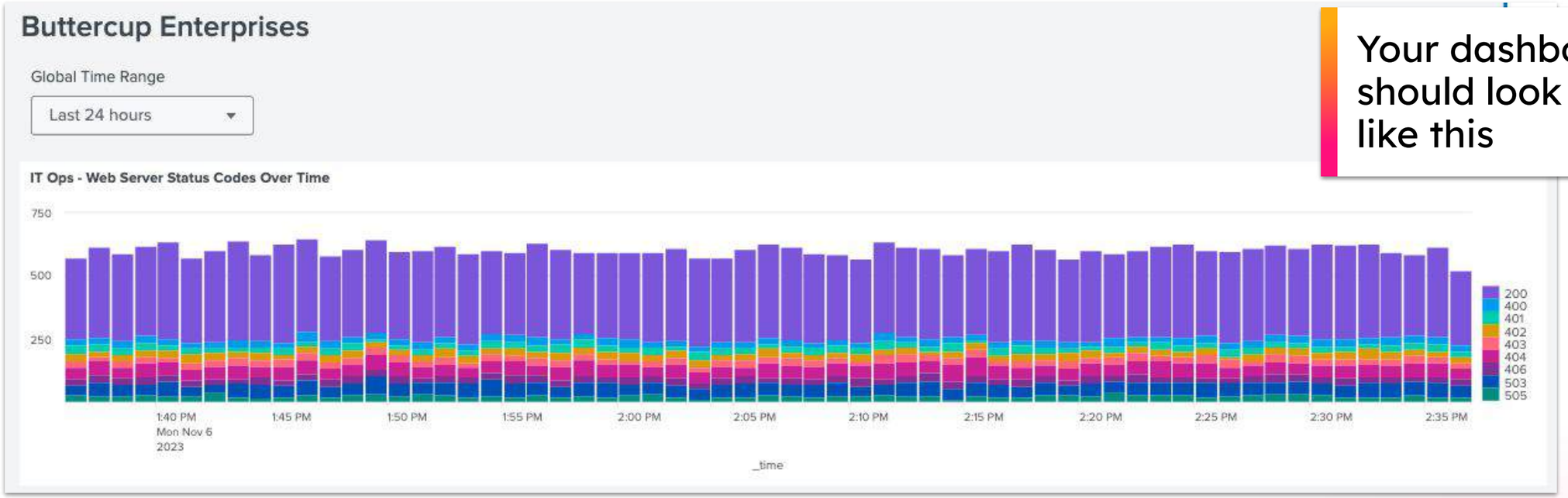
- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images**, **text boxes**, **shapes**, **lines** and **icons**, with **intact PDF export**
- **No custom code** required

IT Operations Team

Investigate successful versus unsuccessful web server requests over time

Solution:

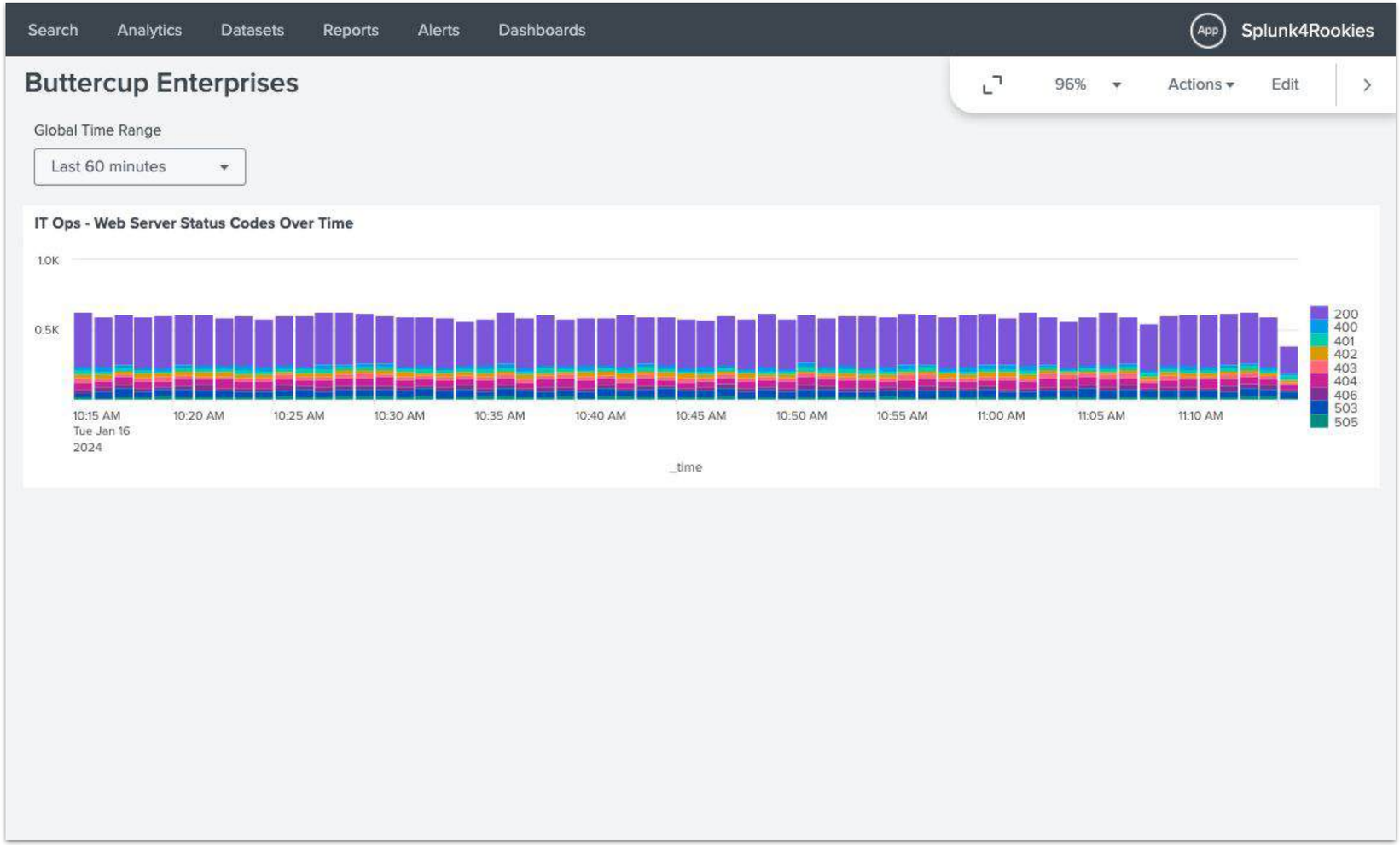
```
index=main sourcetype=access_combined | timechart count by status limit=10
```



Your dashboard panel should look something like this

Your dashboard so far...

IT Operations team ✓



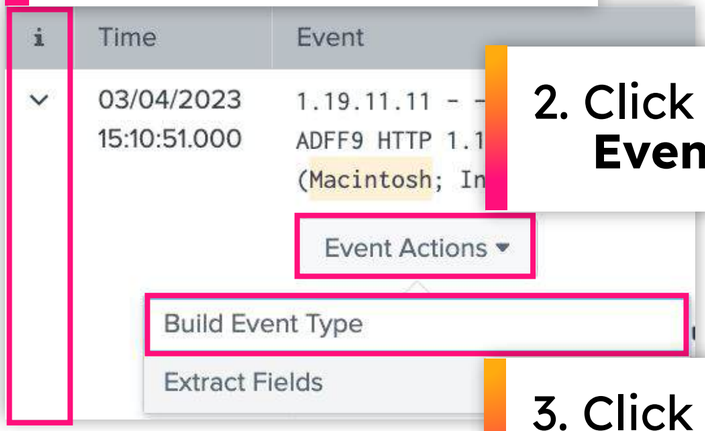
DevOps Team

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

Extracting a New Field

1. Click on the arrow to expand an event

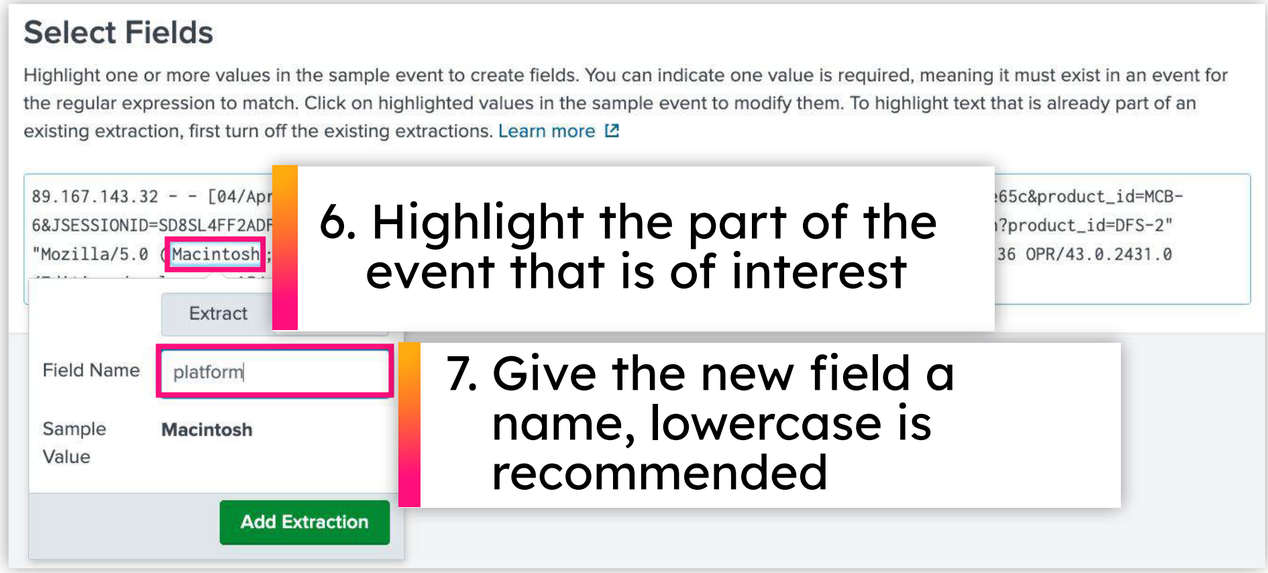


2. Click on **Event Actions**

3. Click on **Extract Fields**

4. Click on **Regular Expression**

5. Click **Next**



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

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

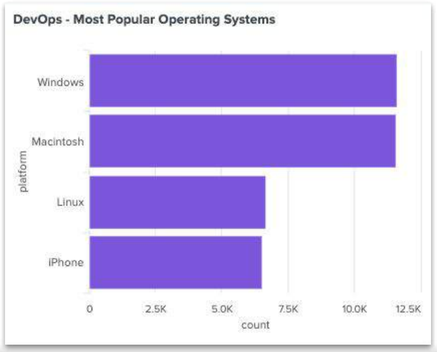
DevOps Team

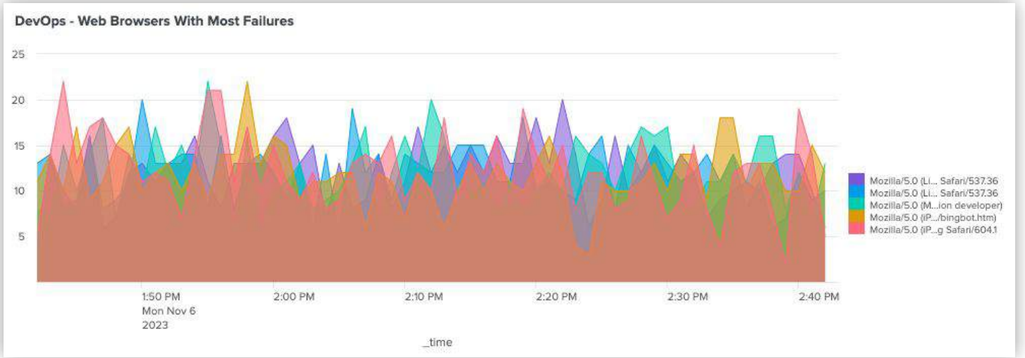
Show the most common customer operating systems and which web browsers are experiencing the most failures

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



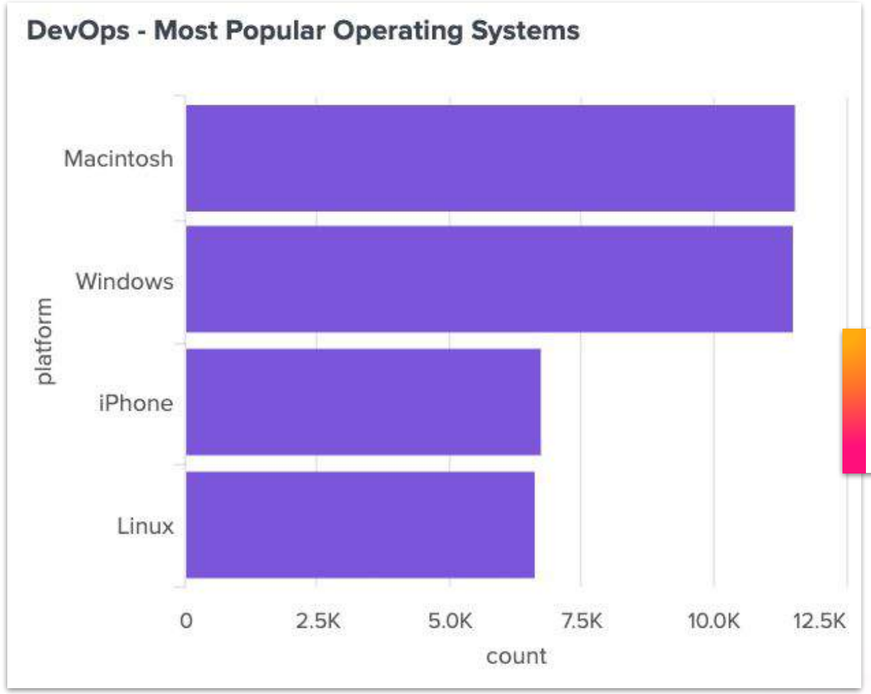


DevOps Team

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!

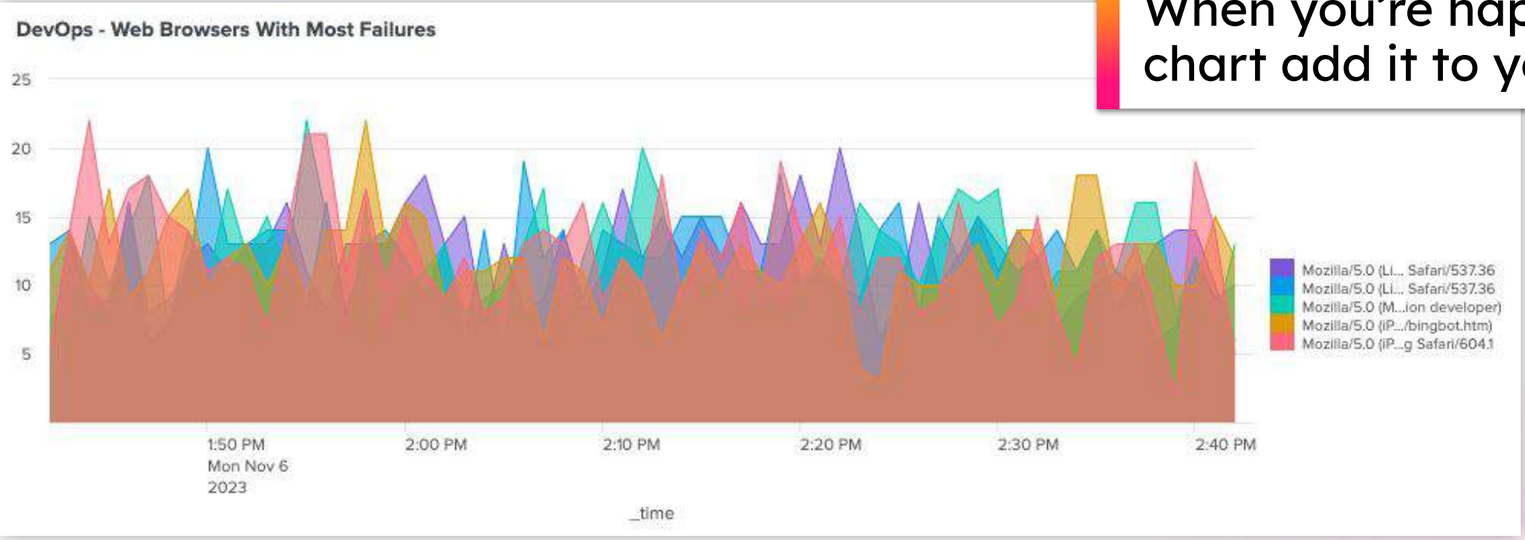
DevOps Team

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

Solution:

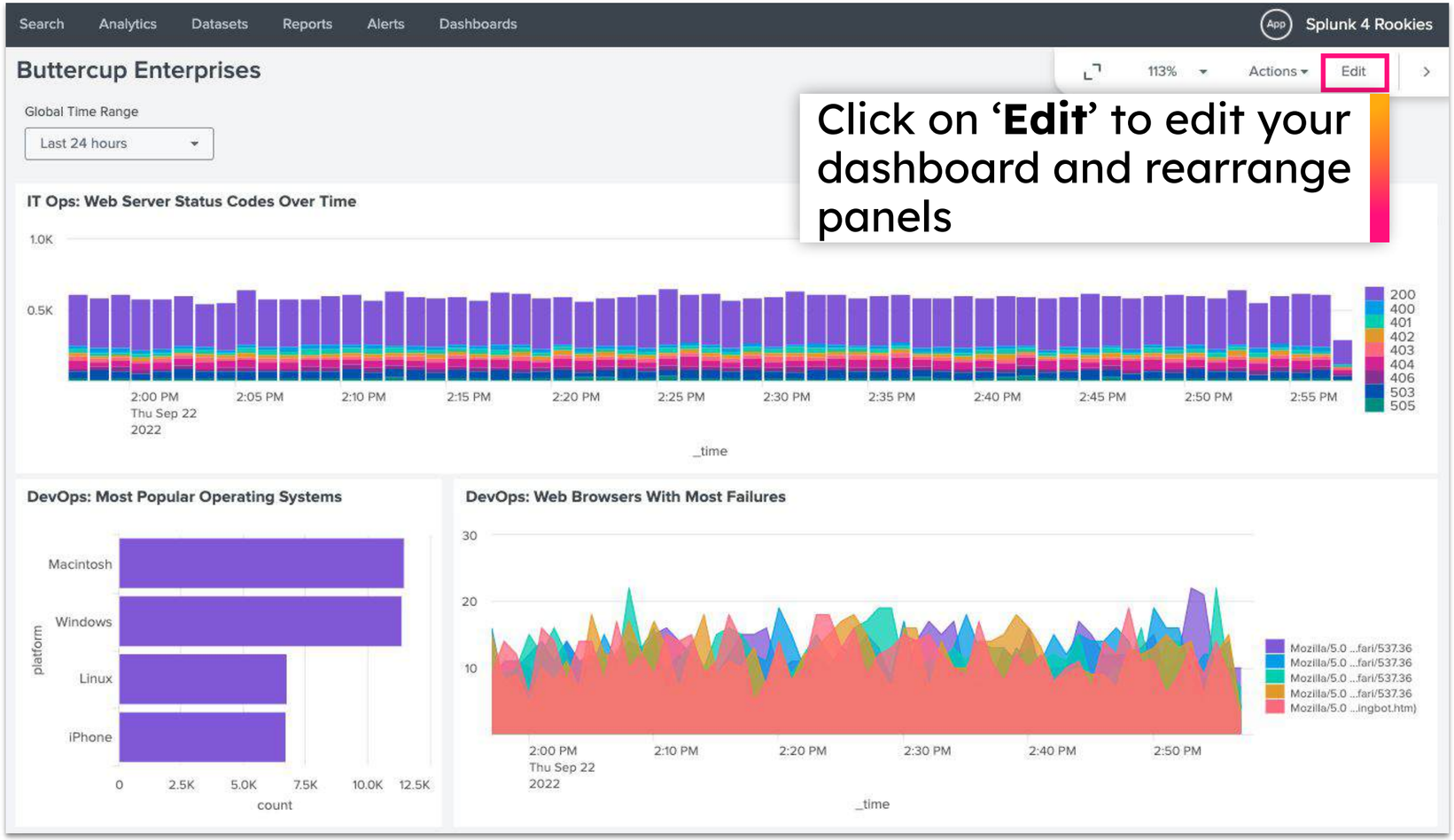
```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5 useother=f
```

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



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:

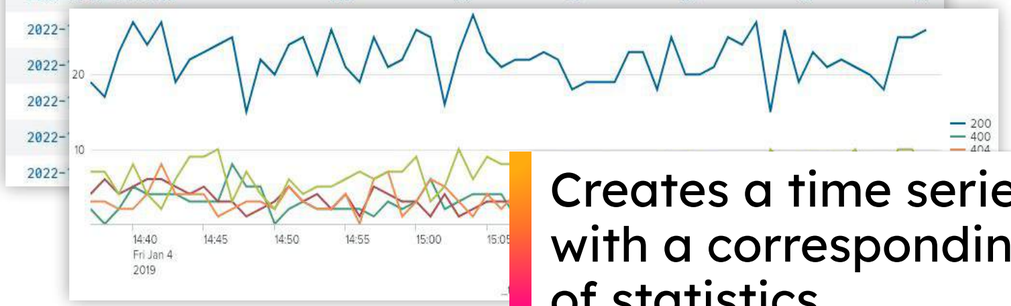
```
index=main sourcetype=access_combined
| stats distinct_count(clientip) by status
```

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
```

_time	200	400	401	402	403	404
2022-10-05 11:20:00	368	29	26	20	18	50
2022-10-05 11:21:00	374	23	19	25	33	57



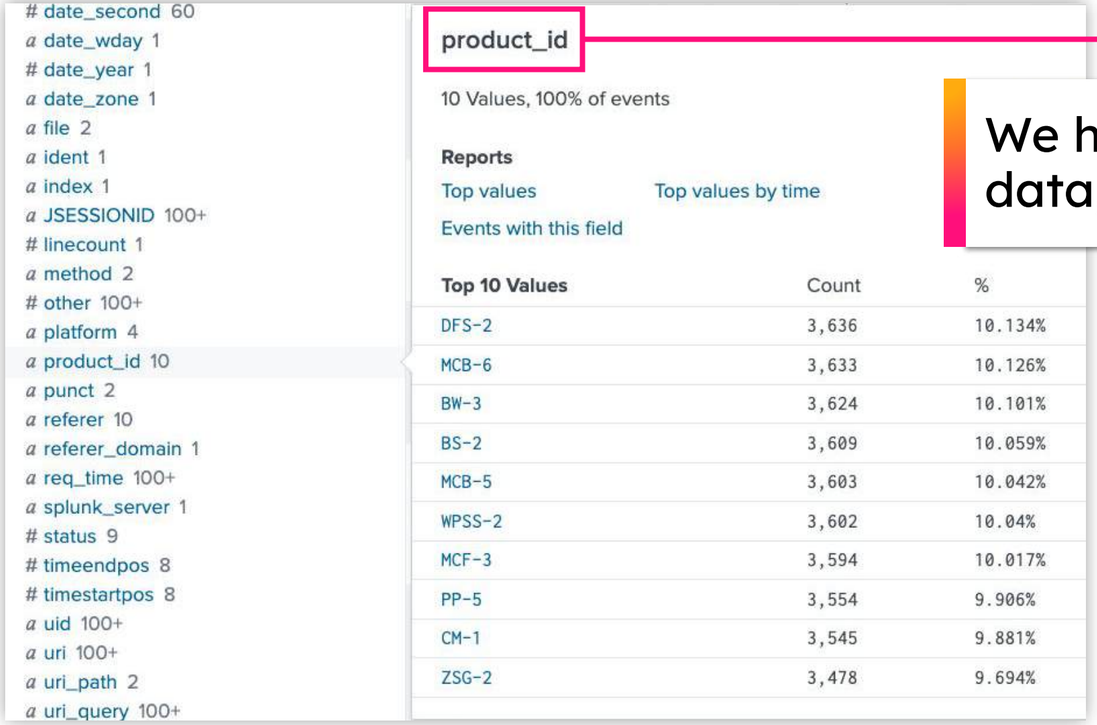
Creates a time series chart with a corresponding table of statistics

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

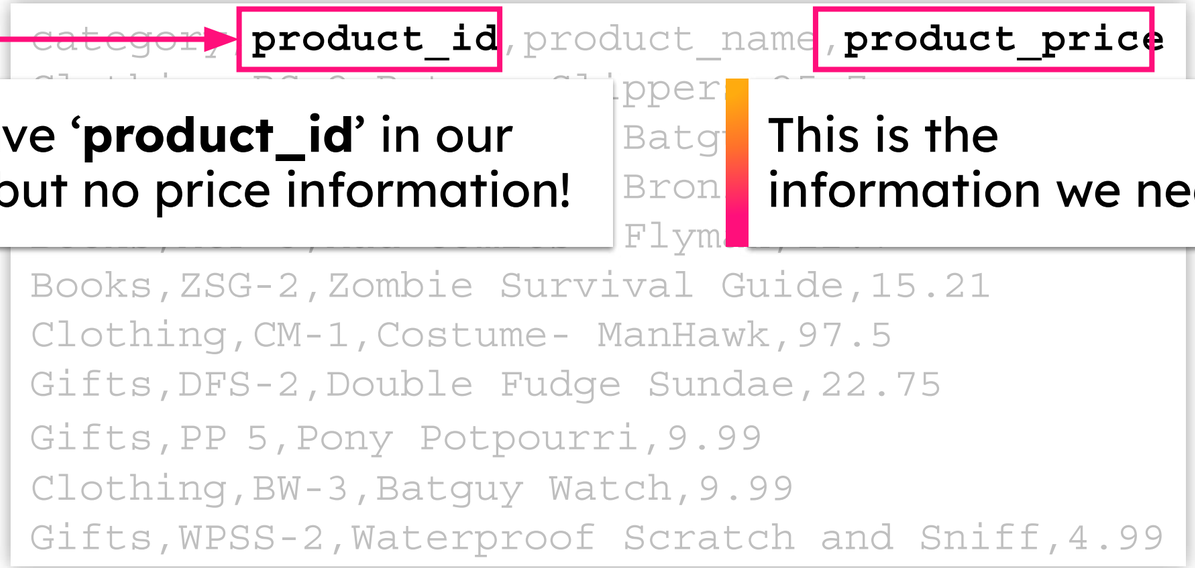
Business Analytics Team

Show lost revenue from the website

Fields extracted from events by Splunk:



External CSV file:

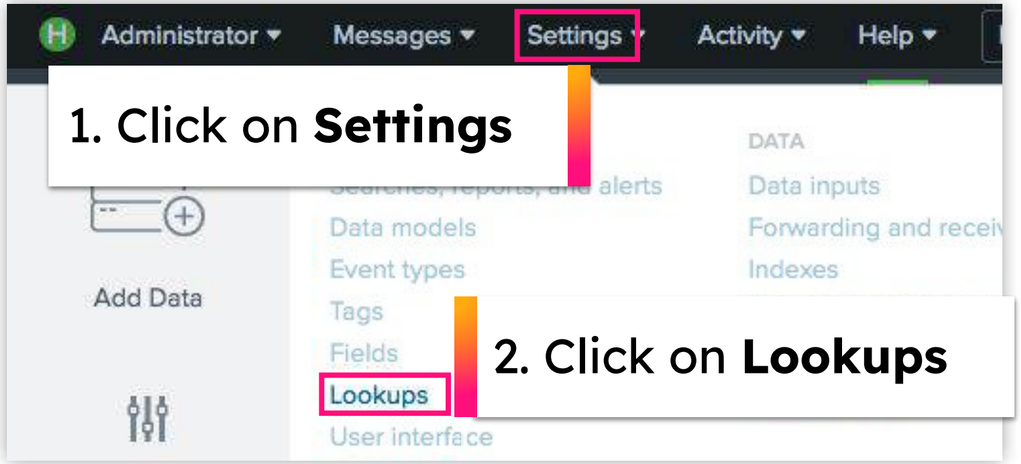


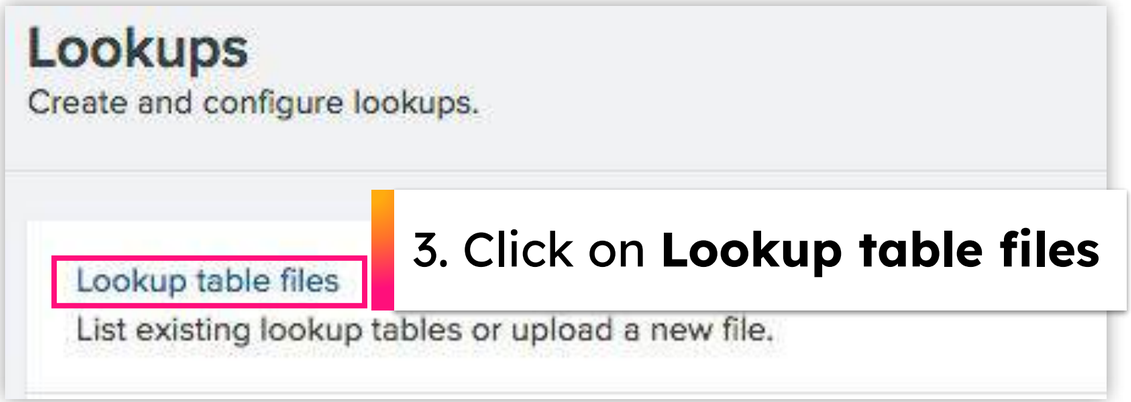
We have '**product_id**' in our data, but no price information!

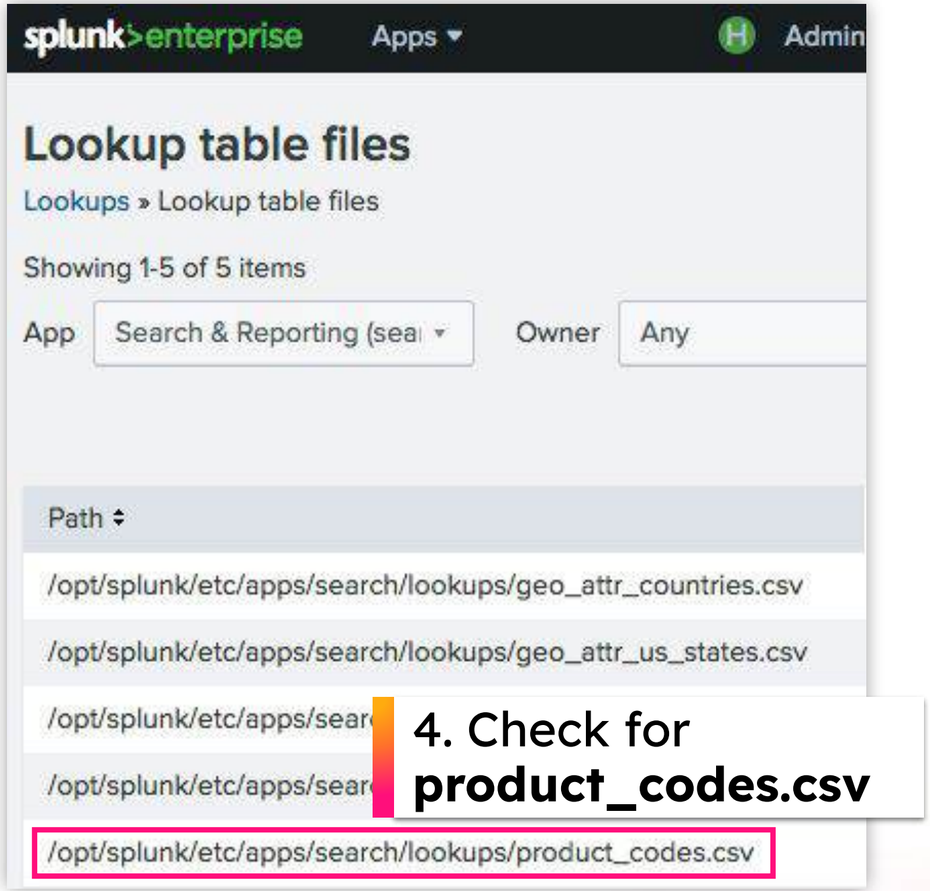
This is the information we need!

Verify That the Lookup File Exists

A lookup file has already been uploaded for you!







Enriching Data with the lookup Command

Usage:

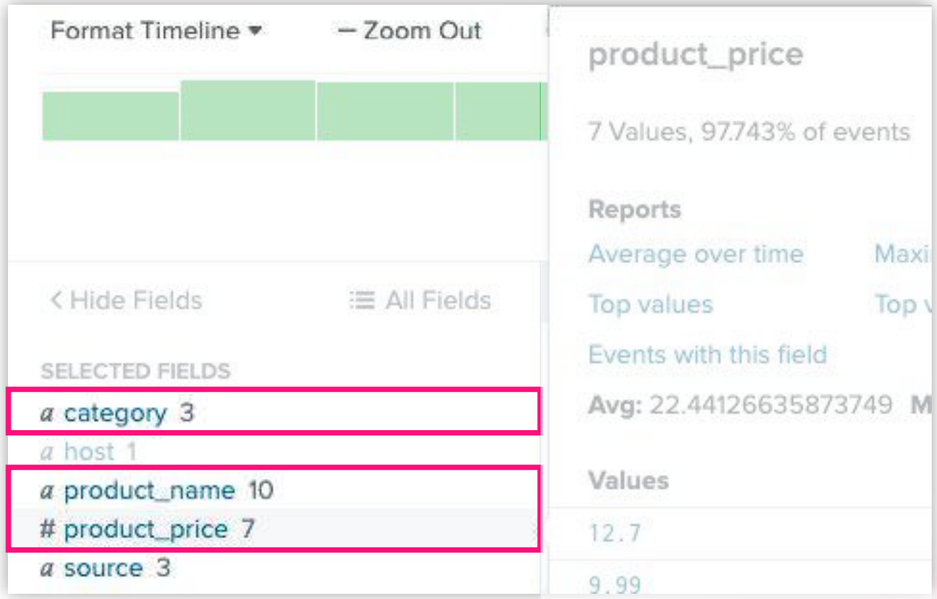
```
<your search> | lookup product_codes.csv product_id
```

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 Team

Show lost revenue from the website

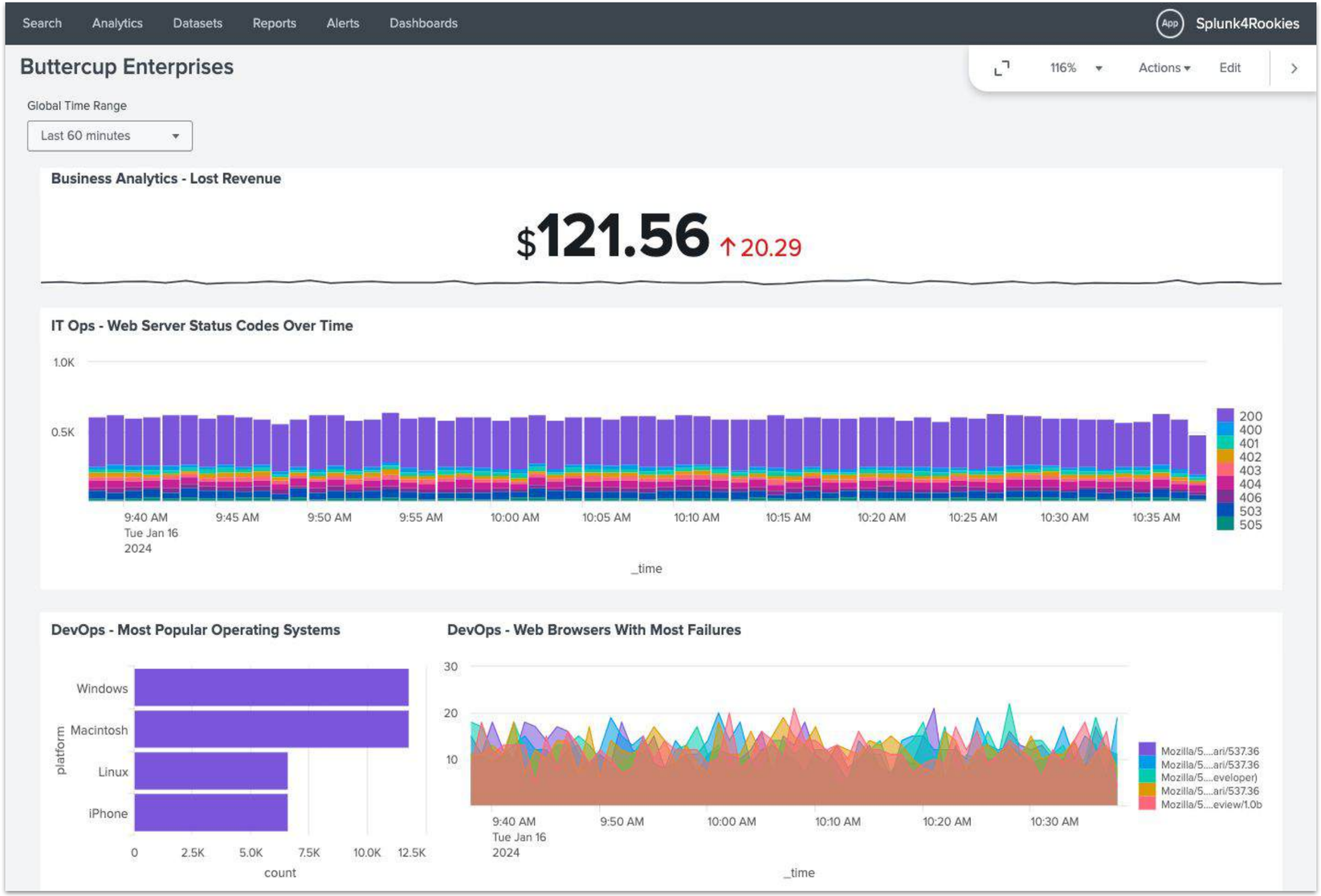
Solution:

```
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 ✓



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

Usage:

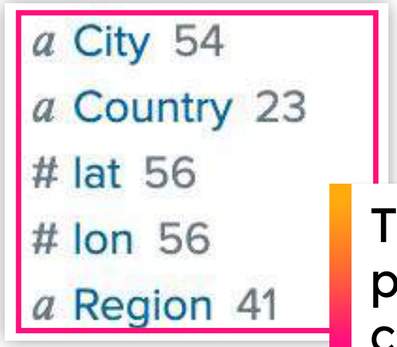
The name of a field in your data that contains IP addresses

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

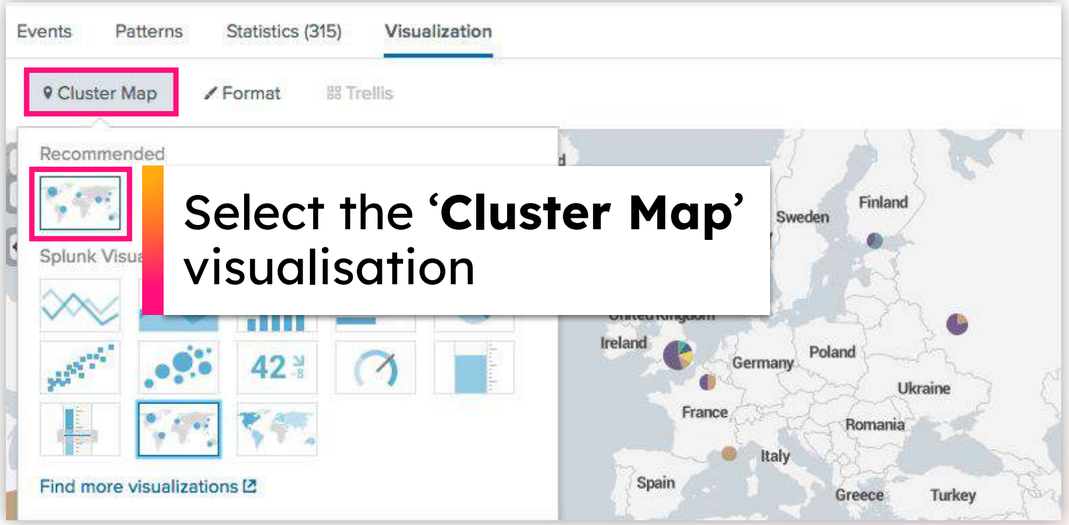
Split your results by a specific field for more detailed analysis

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

Enriches IP data on-the-fly with location data



The `iplocation` command produces additional fields containing geographic data



Select the '**Cluster Map**' visualisation

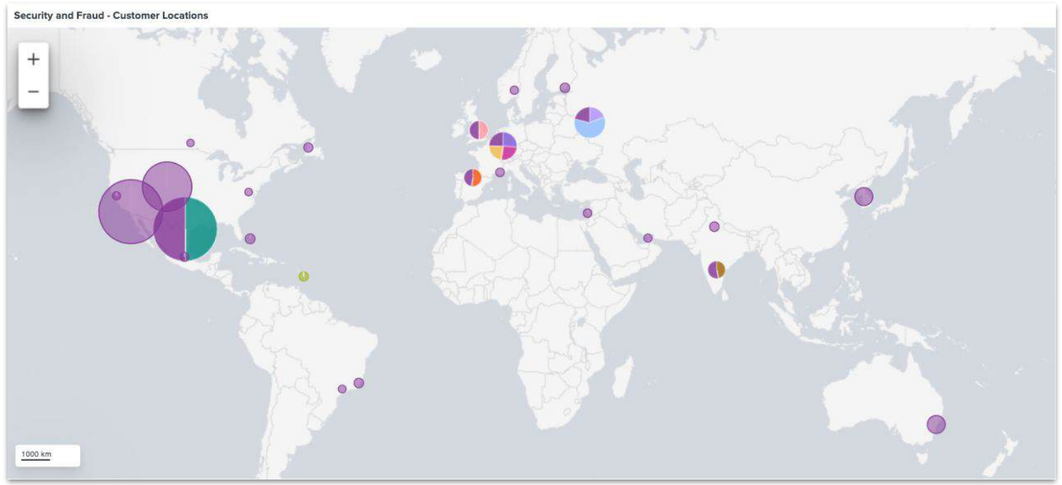
Security and Fraud Team

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

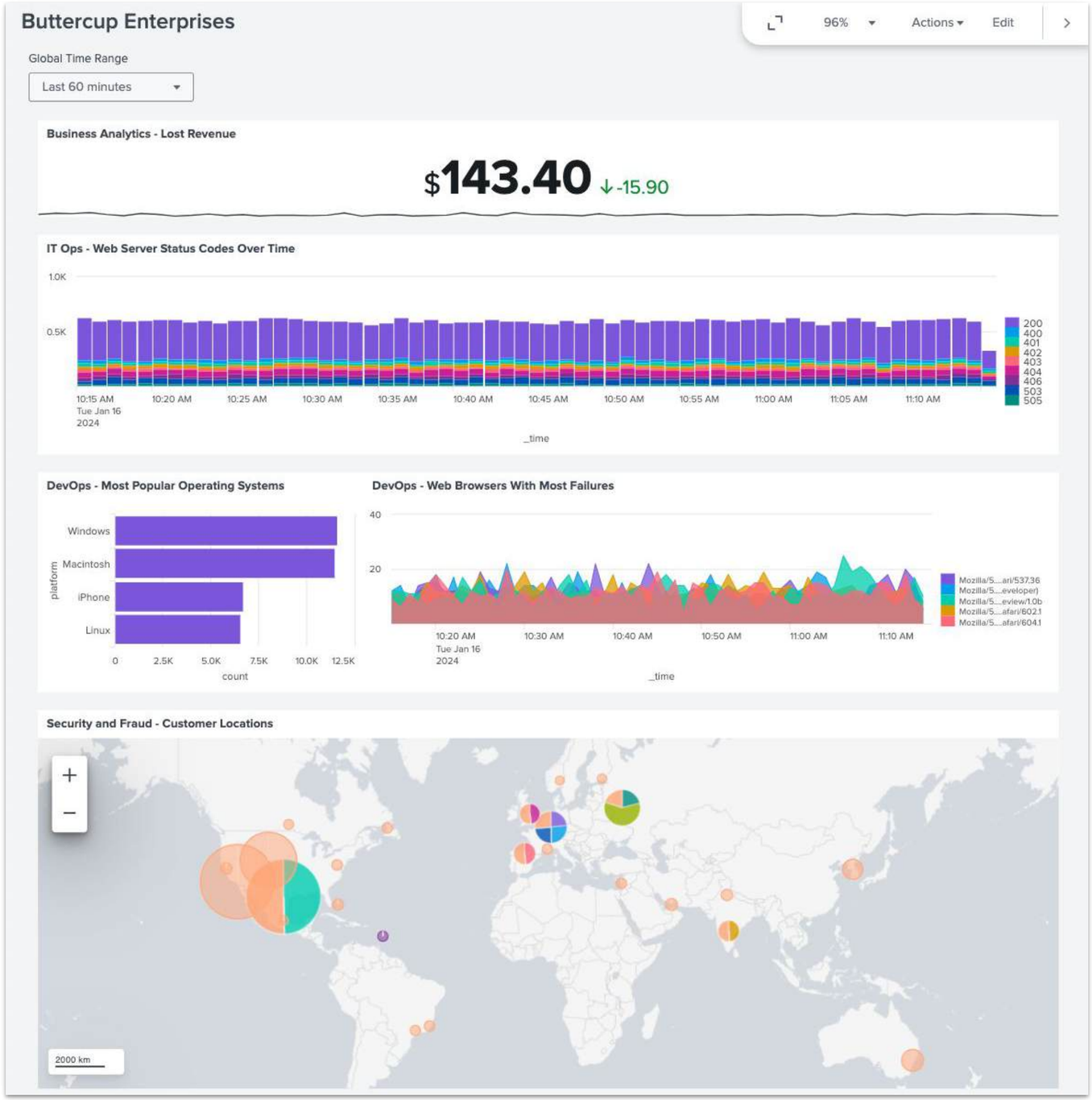
Solution:

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

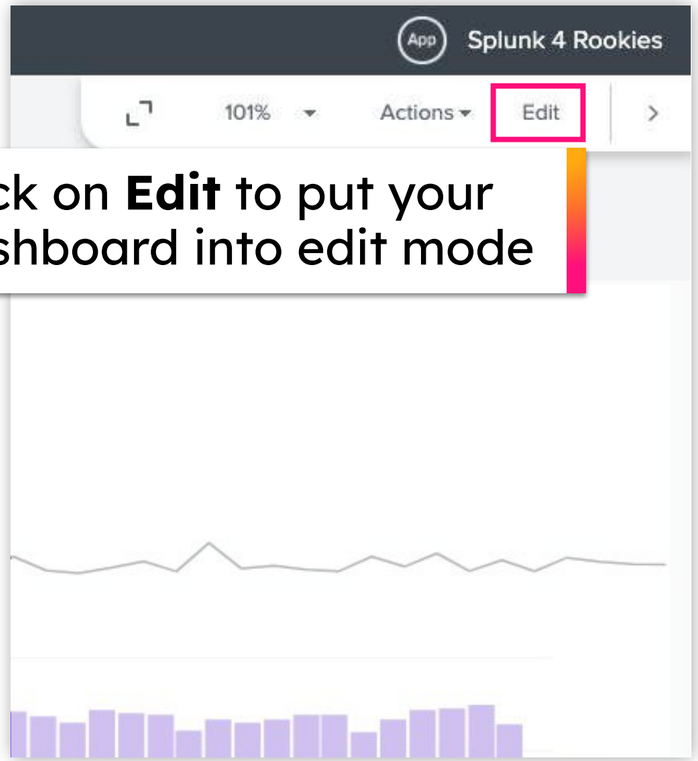
When you're happy with your chart add it to your dashboard!

Your dashboard so far...

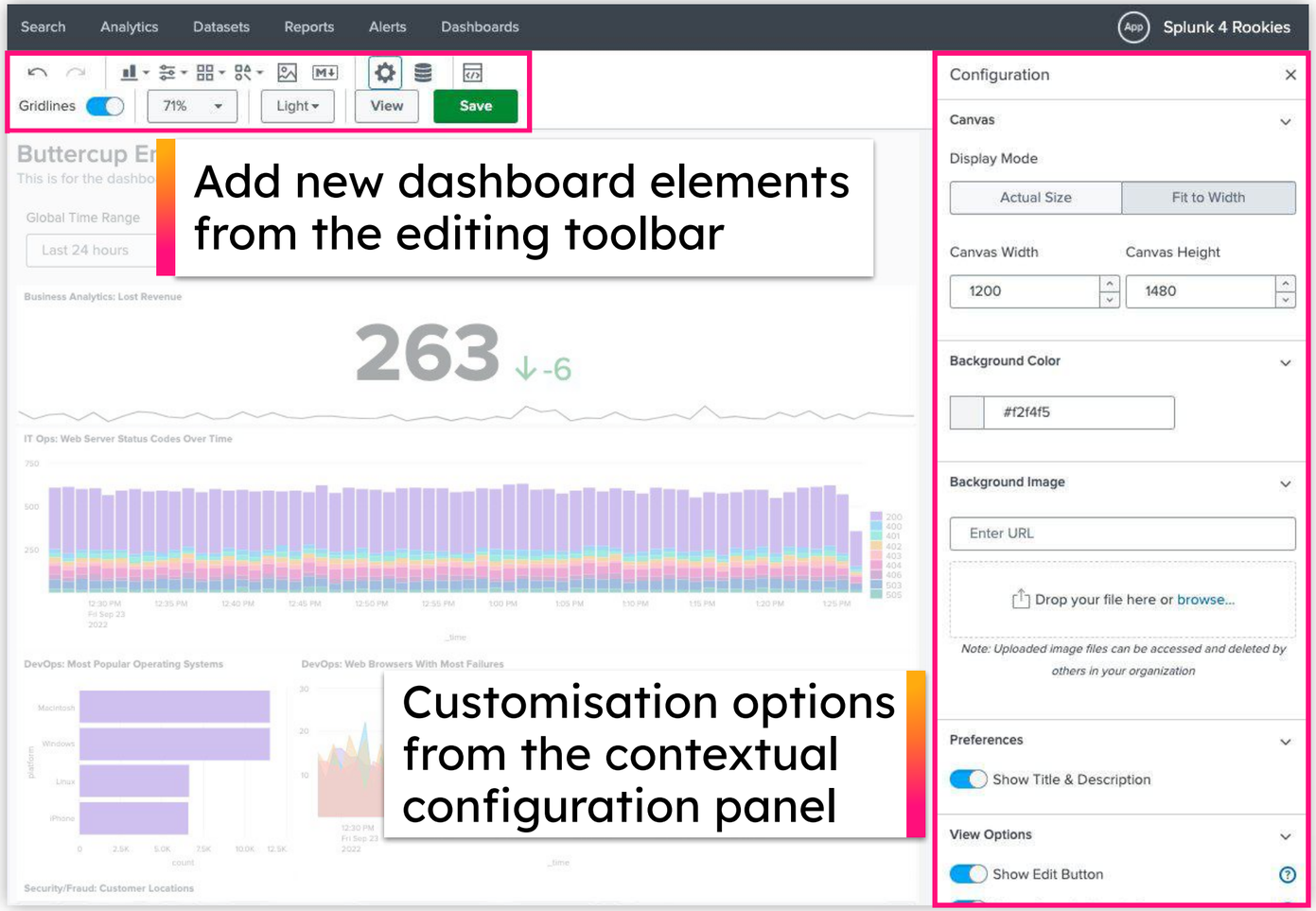
- IT Operations team ✓
- DevOps team ✓
- Business Analytics team ✓
- Security and Fraud team ✓



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

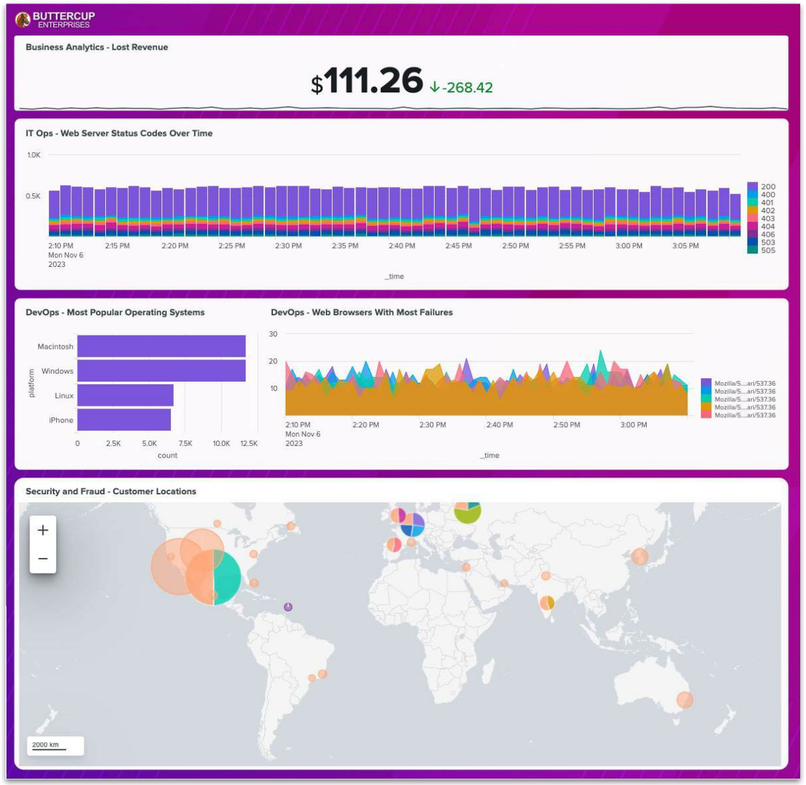
Tasks

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

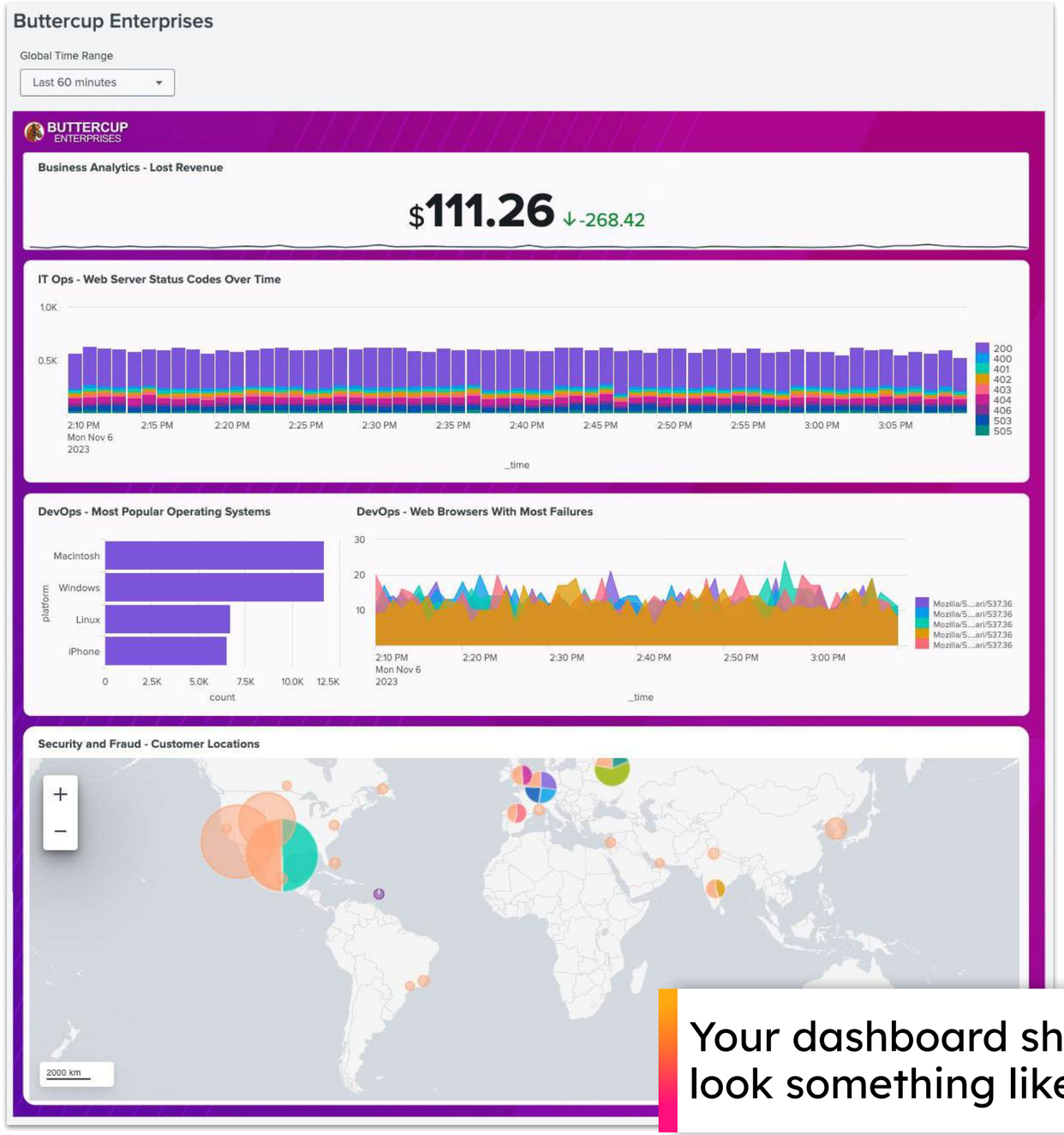
3. Link your dashboard panels to the global time picker

Goal



You've Finished the Hands-on Exercises!

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



Your dashboard should look something like this

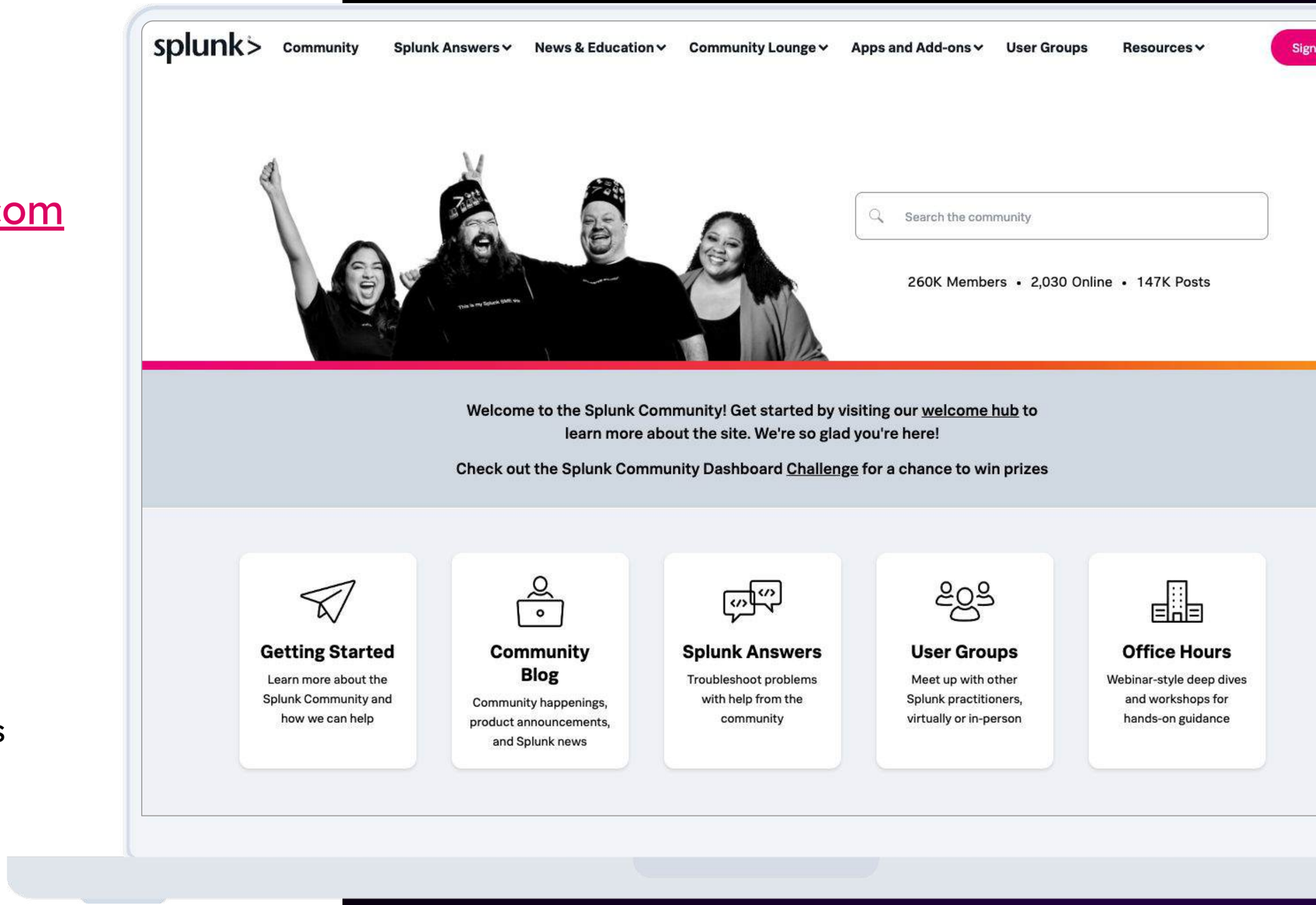
Splunk Resources

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

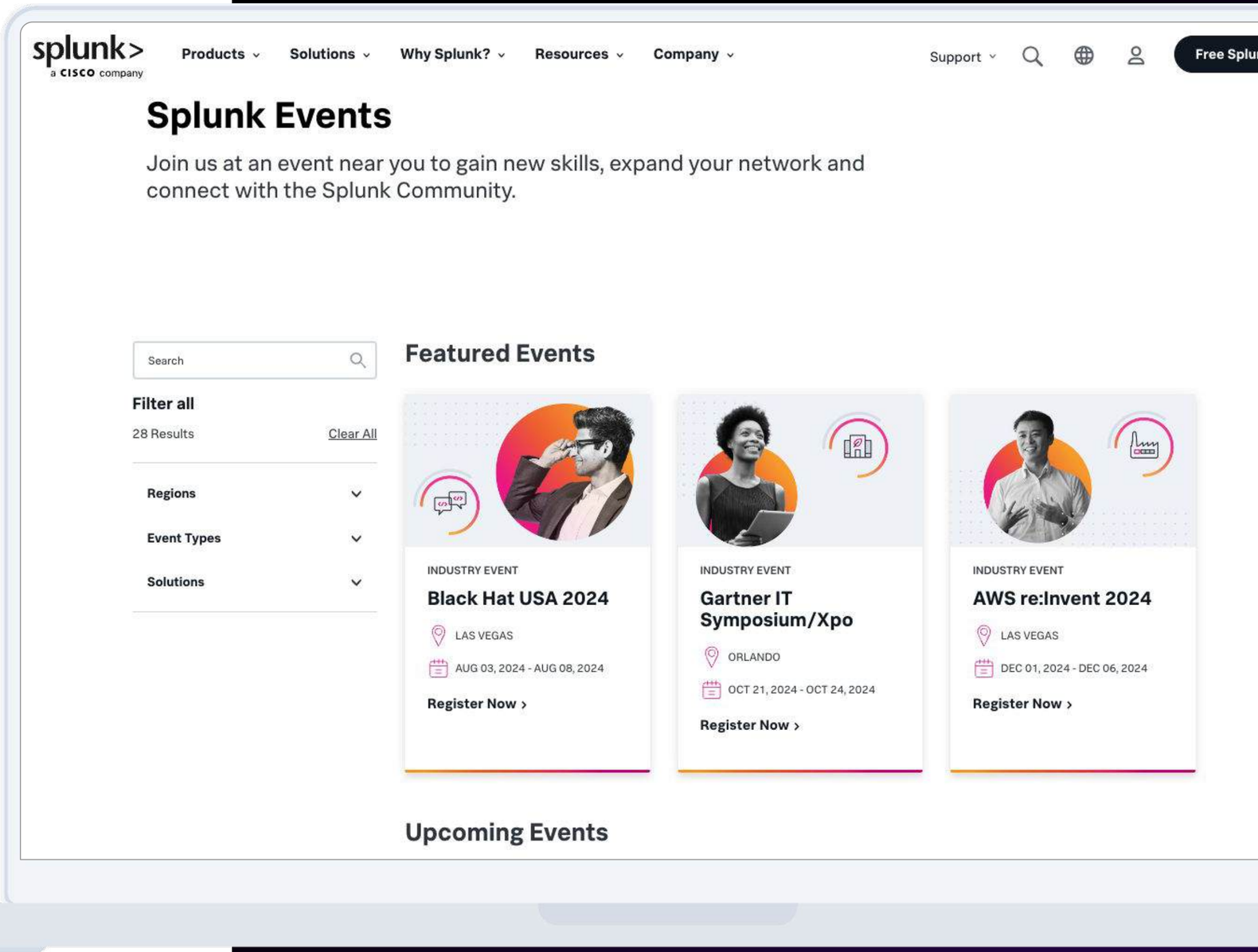
- Expand your network and connect with the global and local Splunk community

.conf25

https://conf.splunk.com

- Join us in Boston!
  8 - 11 September 2025

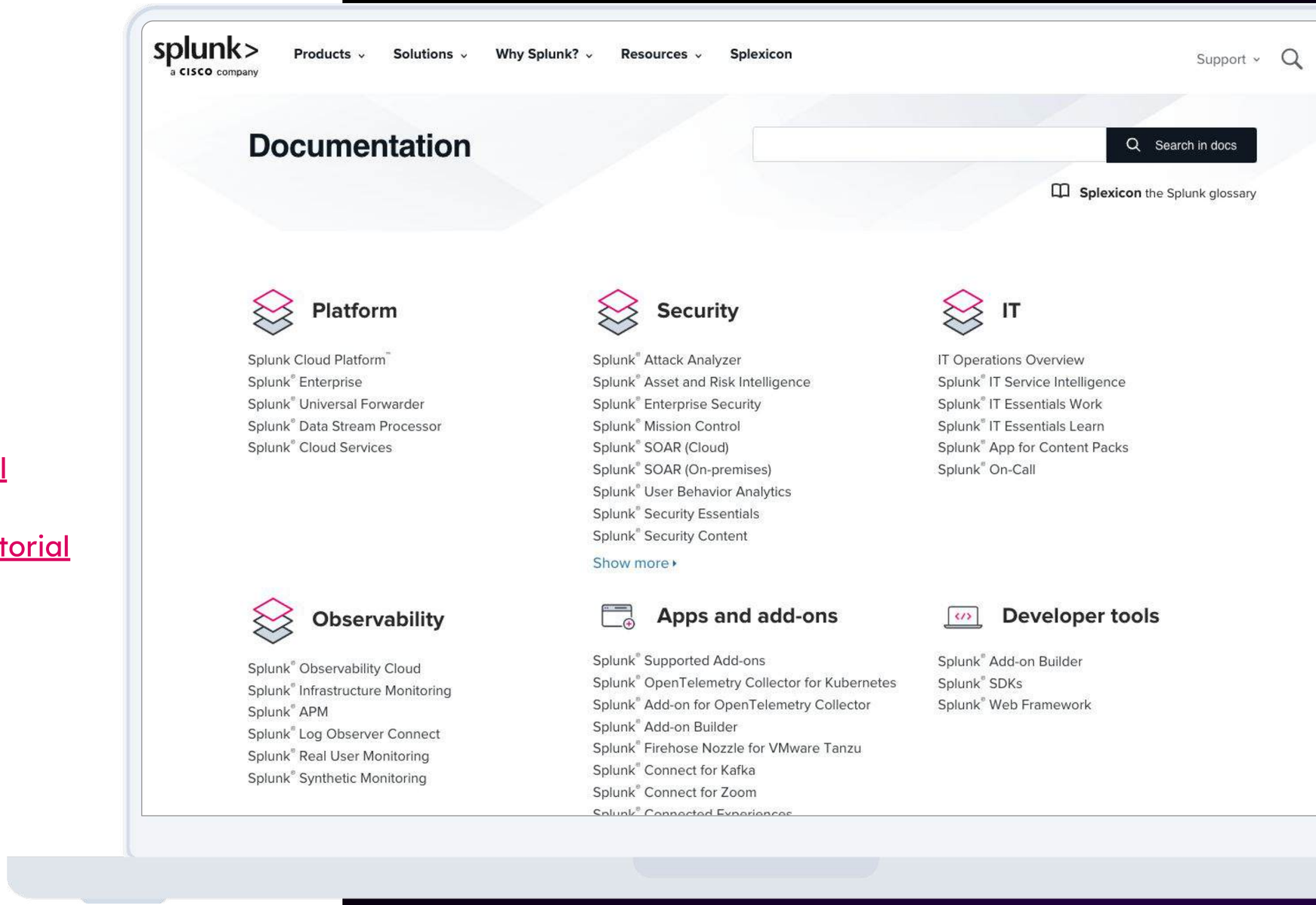
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



Documentation

https://docs.splunk.com

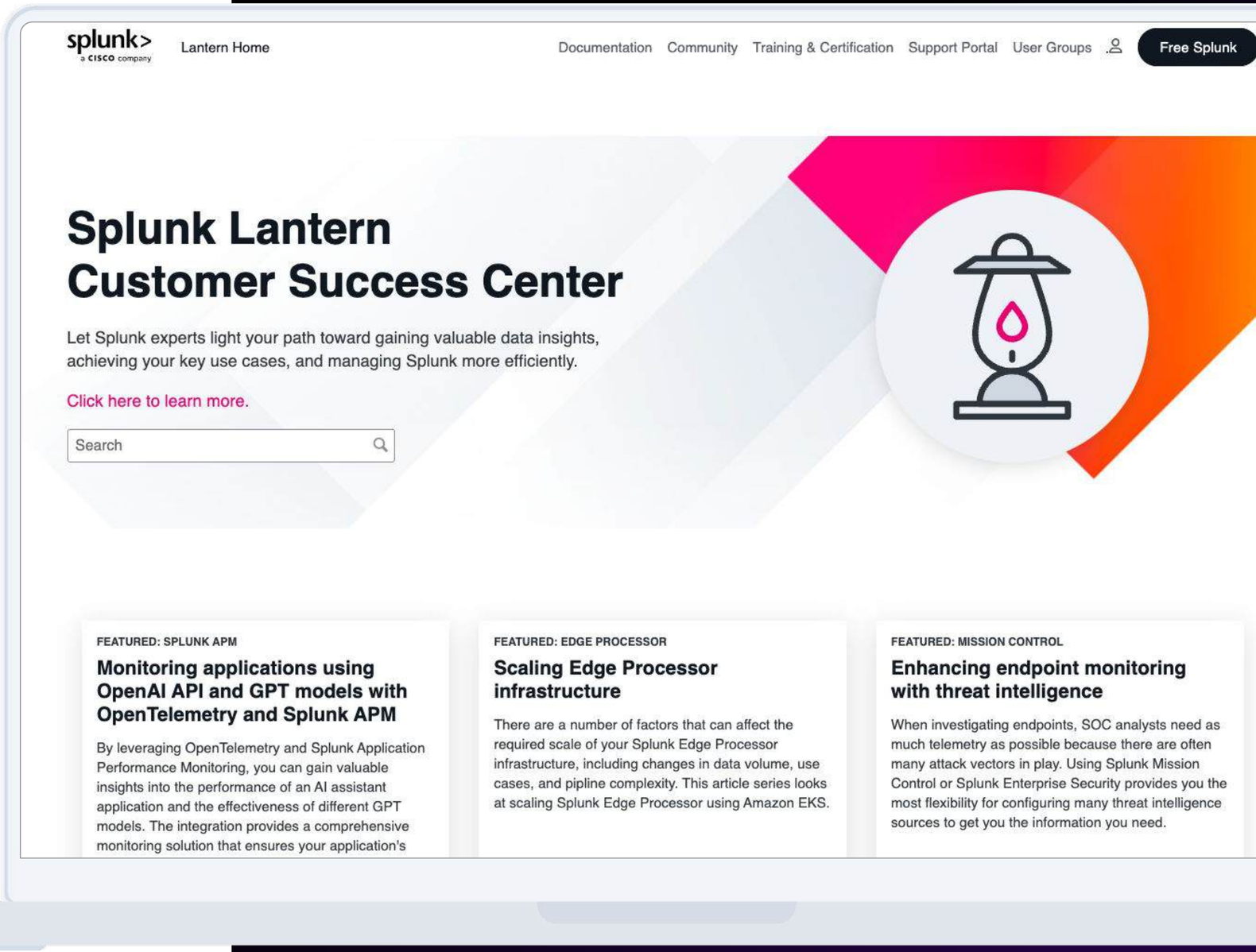
- Search reference for SPL
- Step-by-step tutorials
  Search:
  https://splk.it/SplunkSearchTutorial
  Dashboard Studio:
  https://splk.it/SplunkDashStudioTutorial
- Product references
- Procedures/guides
- And more!



Splunk Lantern

https://lantern.splunk.com

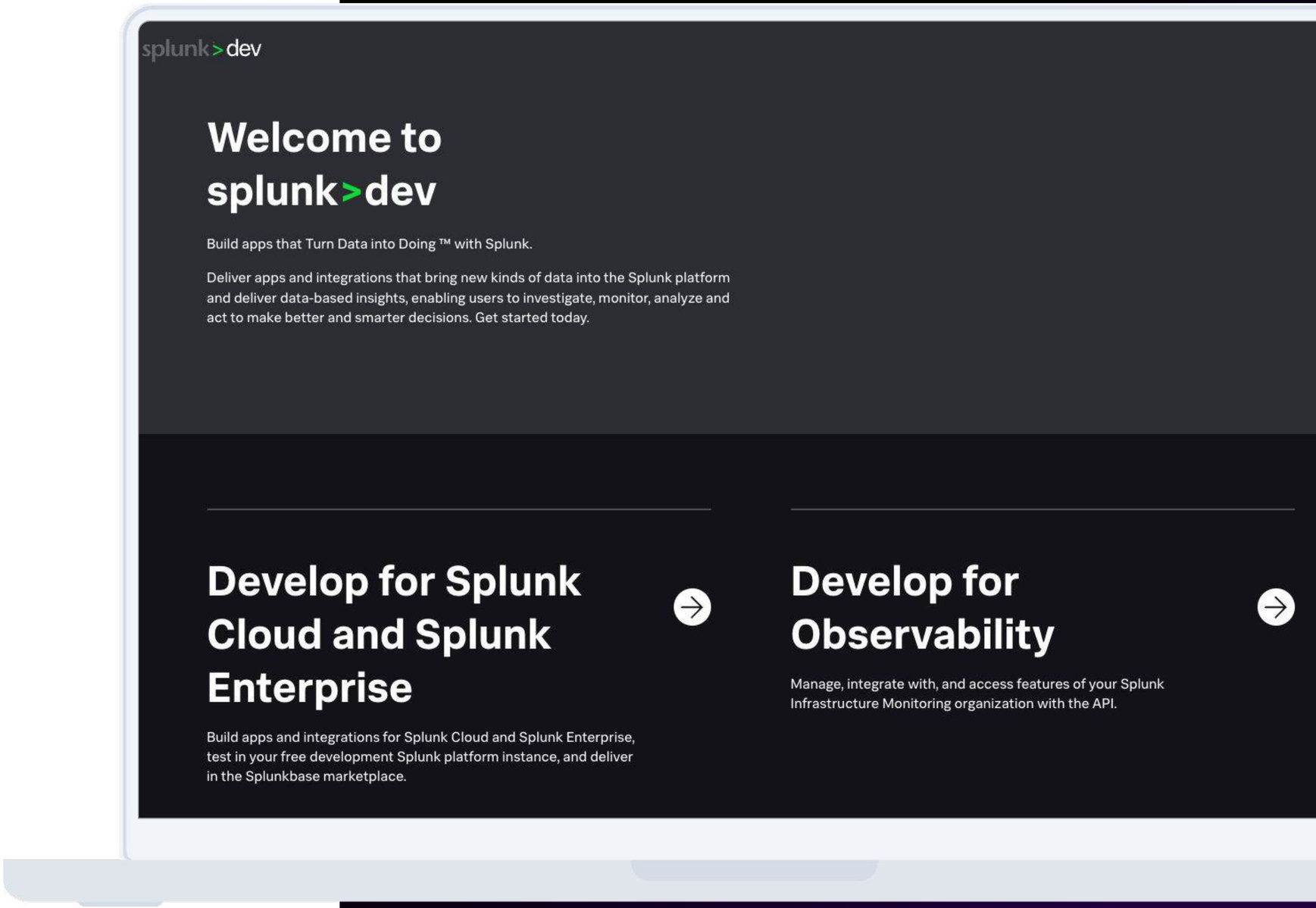
- Use case library
- Product tips
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to increase the value of Splunk across your organisation



Developer Resources

https://dev.splunk.com

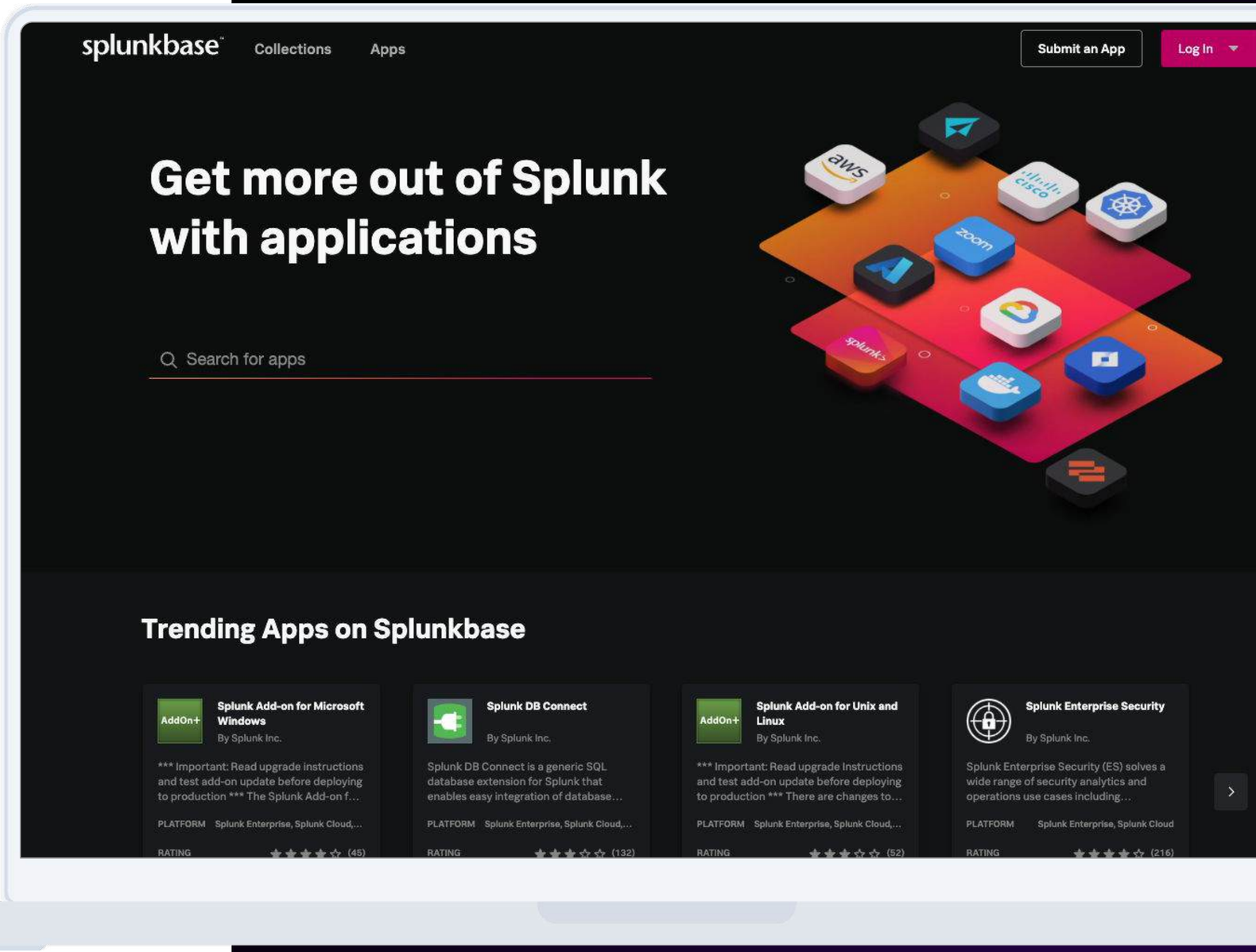
- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

https://splunkbase.splunk.com

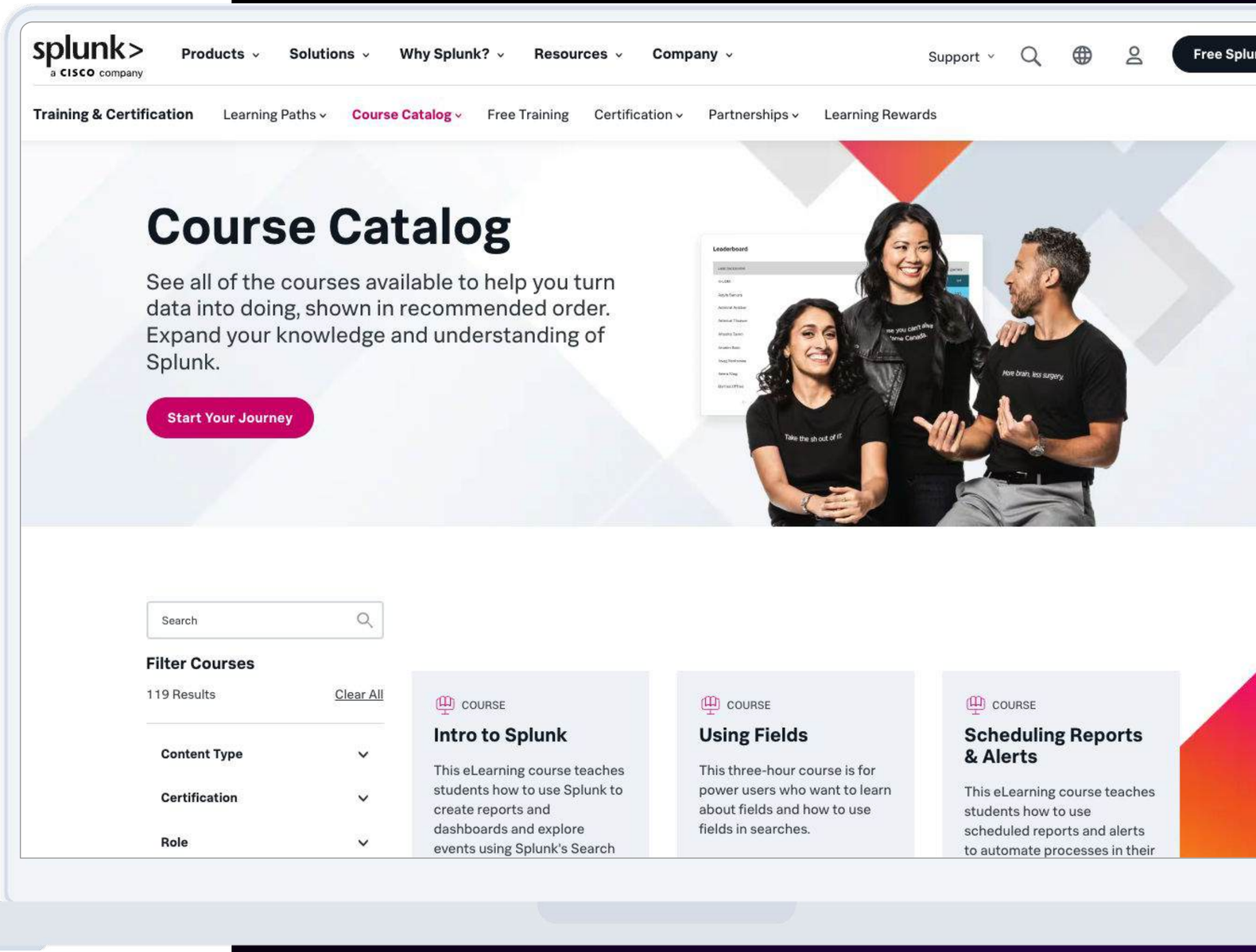
- 2200+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



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



Thank you

splunk> a CISCO company