Splunk4Rookies

#Splunk4Rookies

Forward-Looking Statements

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

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

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

splunk>

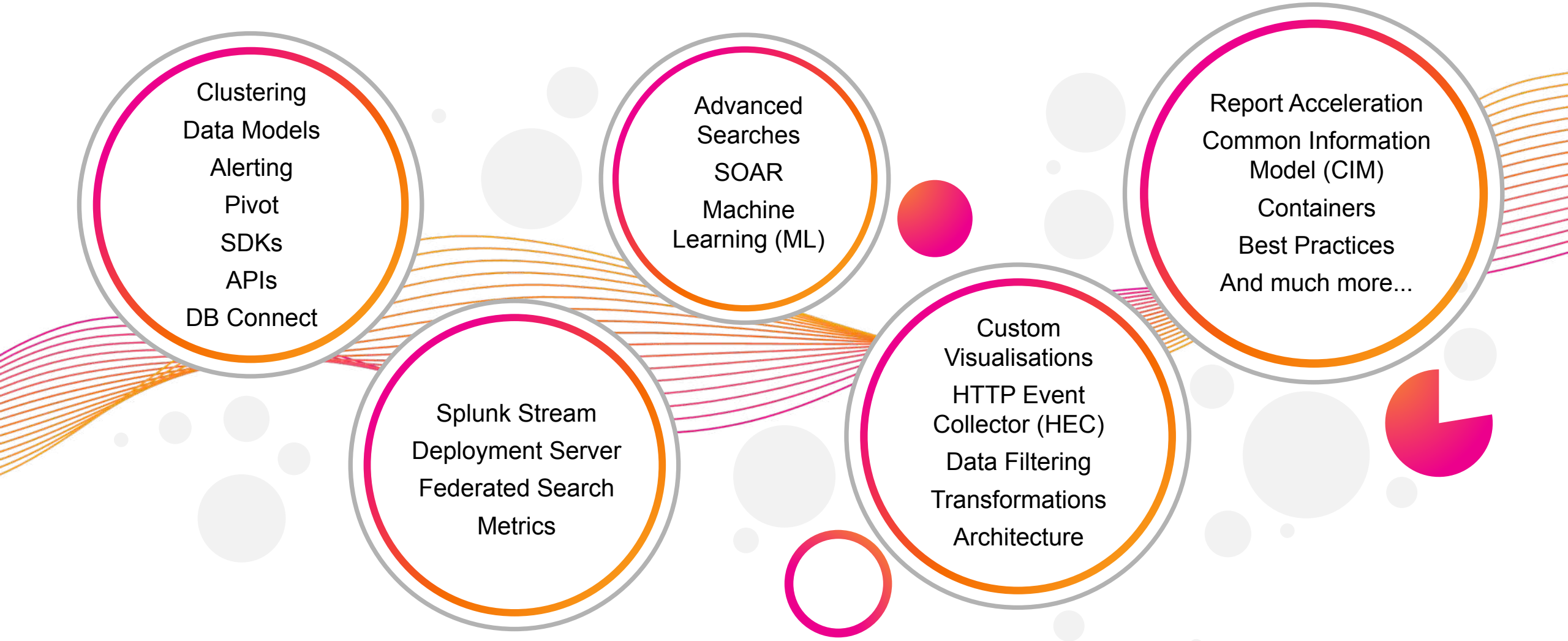
Please introduce yourself!

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

Workshop Agenda

- The value of data
- Splunk’s approach to data
- 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!

splunk>

Objective for Today

splunk>

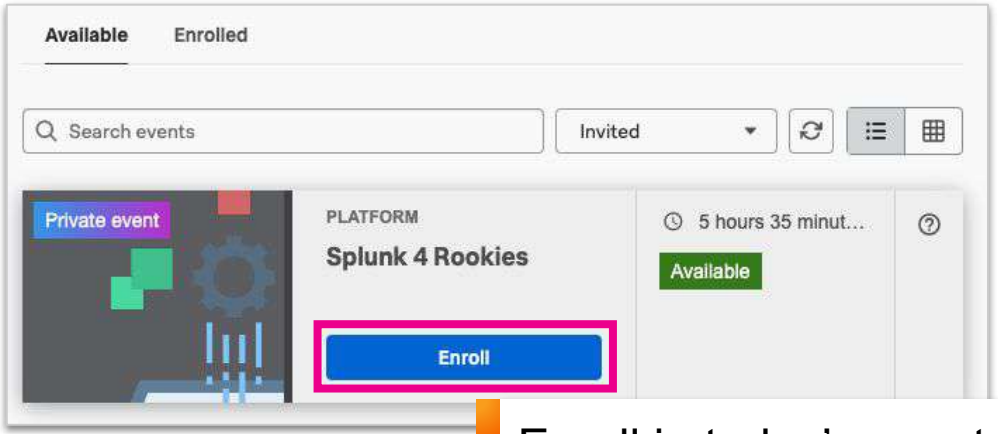
Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>
3. Download 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

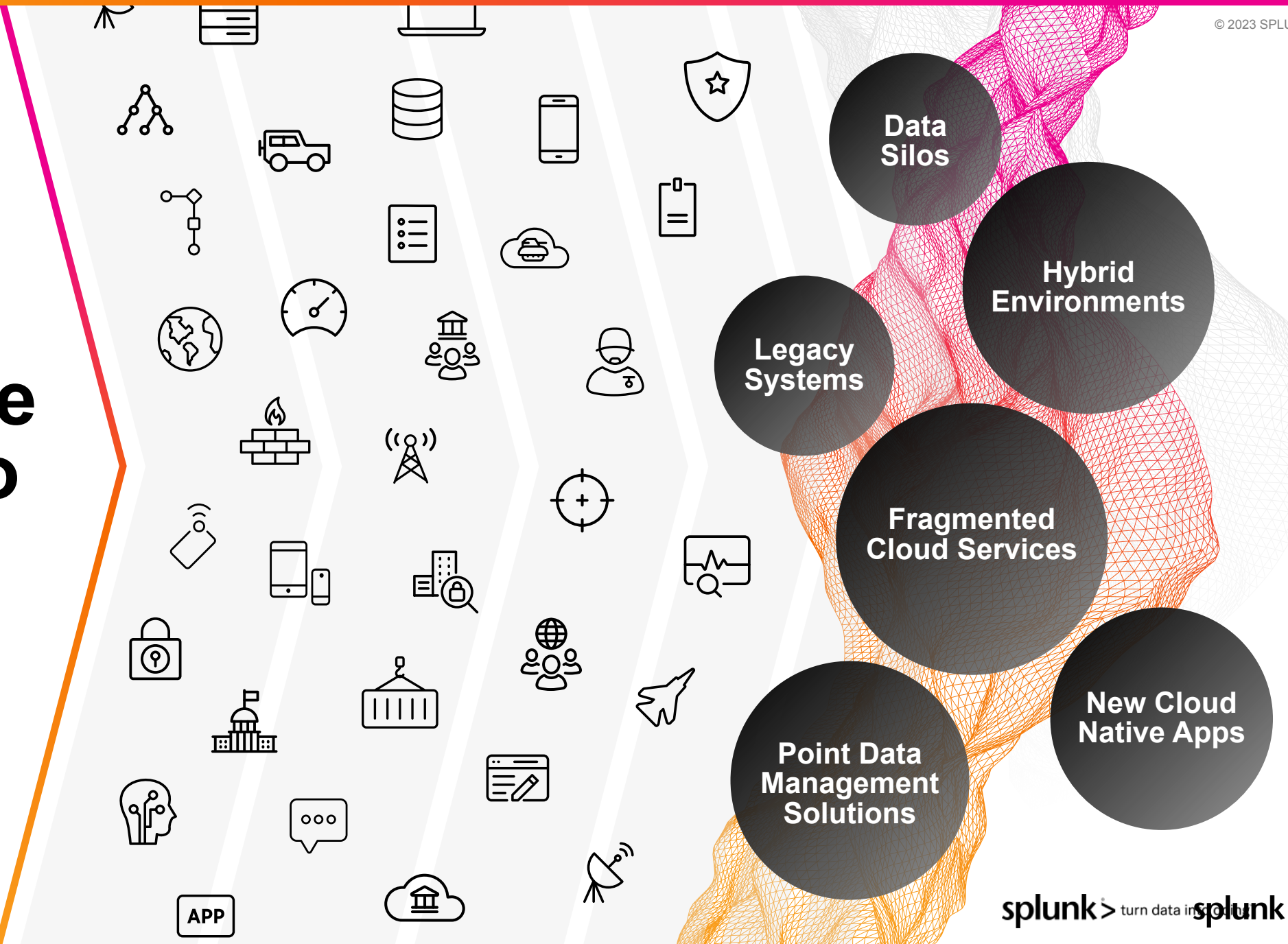
splunk>

Data is your Competitive Advantage

Data isn't just a record.
Data makes things happen.
Splunk makes it possible.

splunk> turn data into doing

Turning Real-time Data Into Action is Hard



The Power of Splunk

Delivering Unified Security and Observability

See

End-to-end visibility

No sampling or blind spots

Act

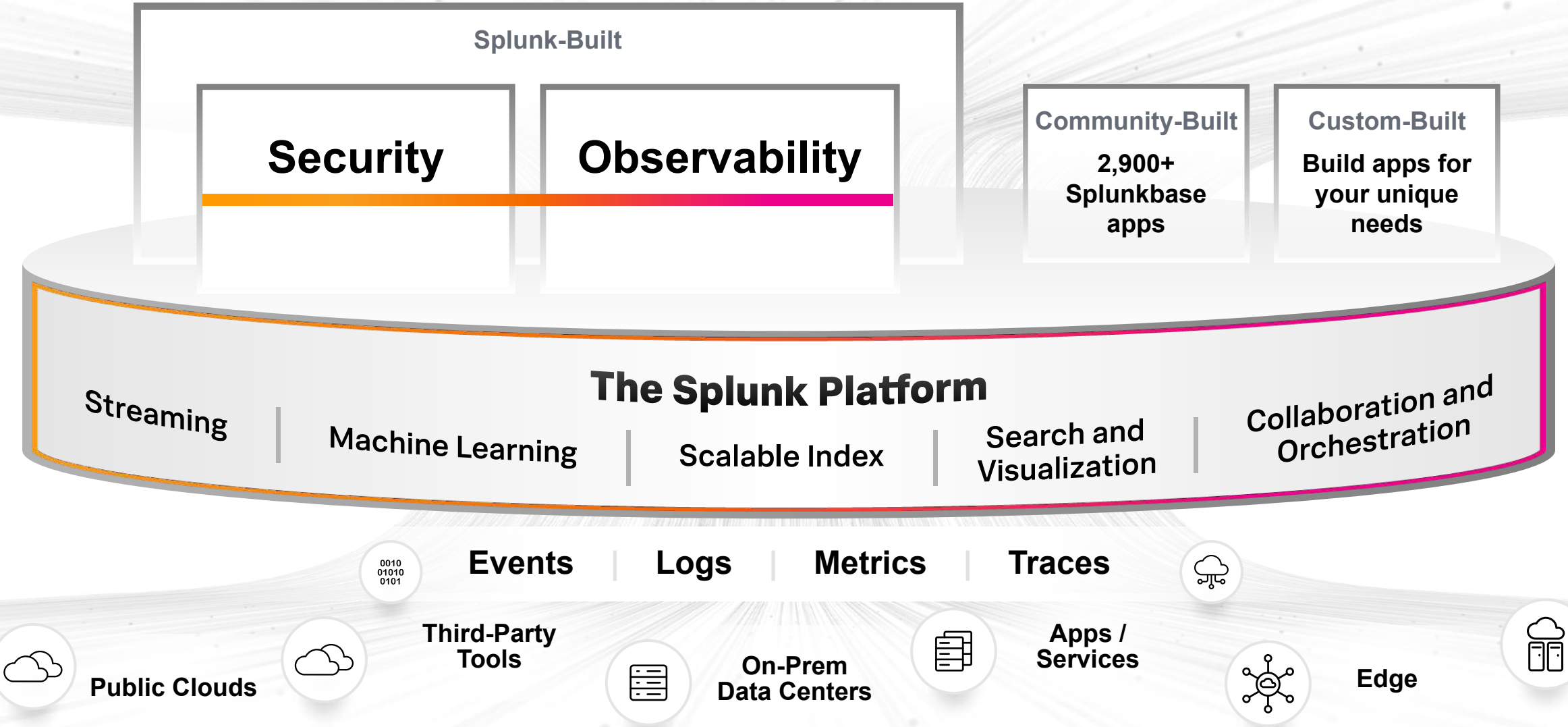
Investigate across massive data sets and take **action** fast

Extend

Extend the **platform** to use data to solve problems across the business

splunk>

The Unified Security and Observability Platform



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 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

splunk>

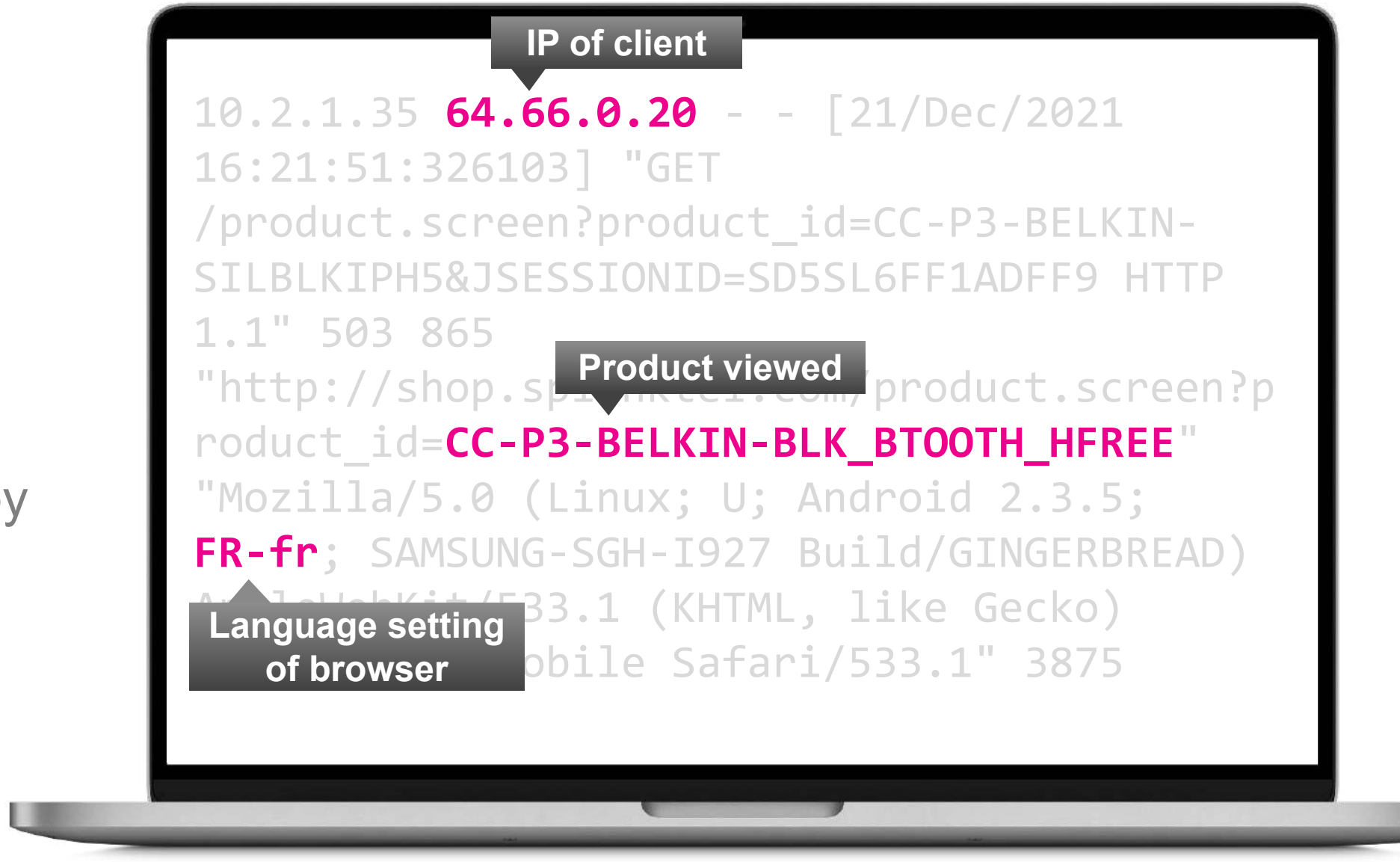
What is a Splunk Universal Forwarder?

- 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

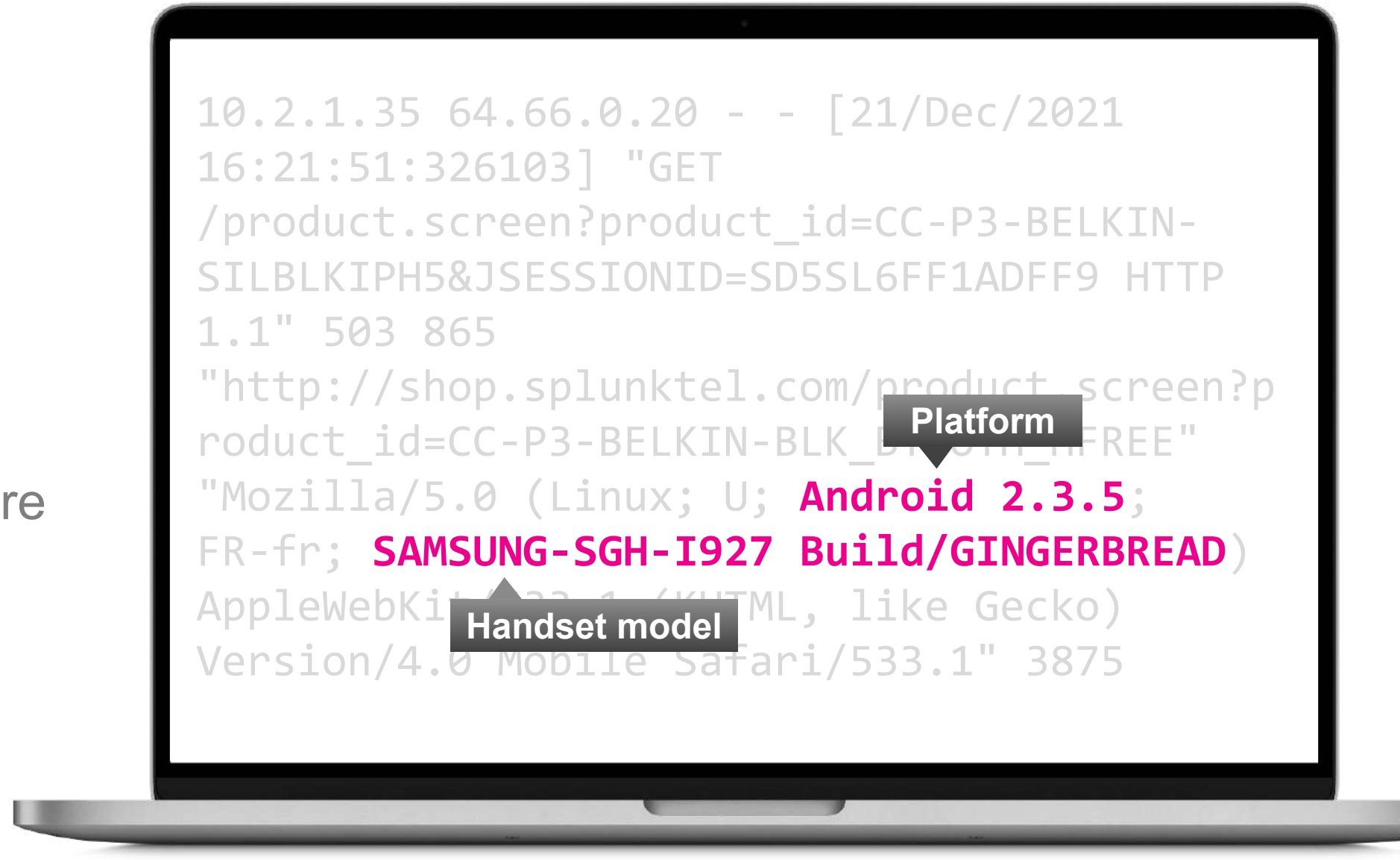
Show the top products viewed by language



splunk>

DevOps Use Case

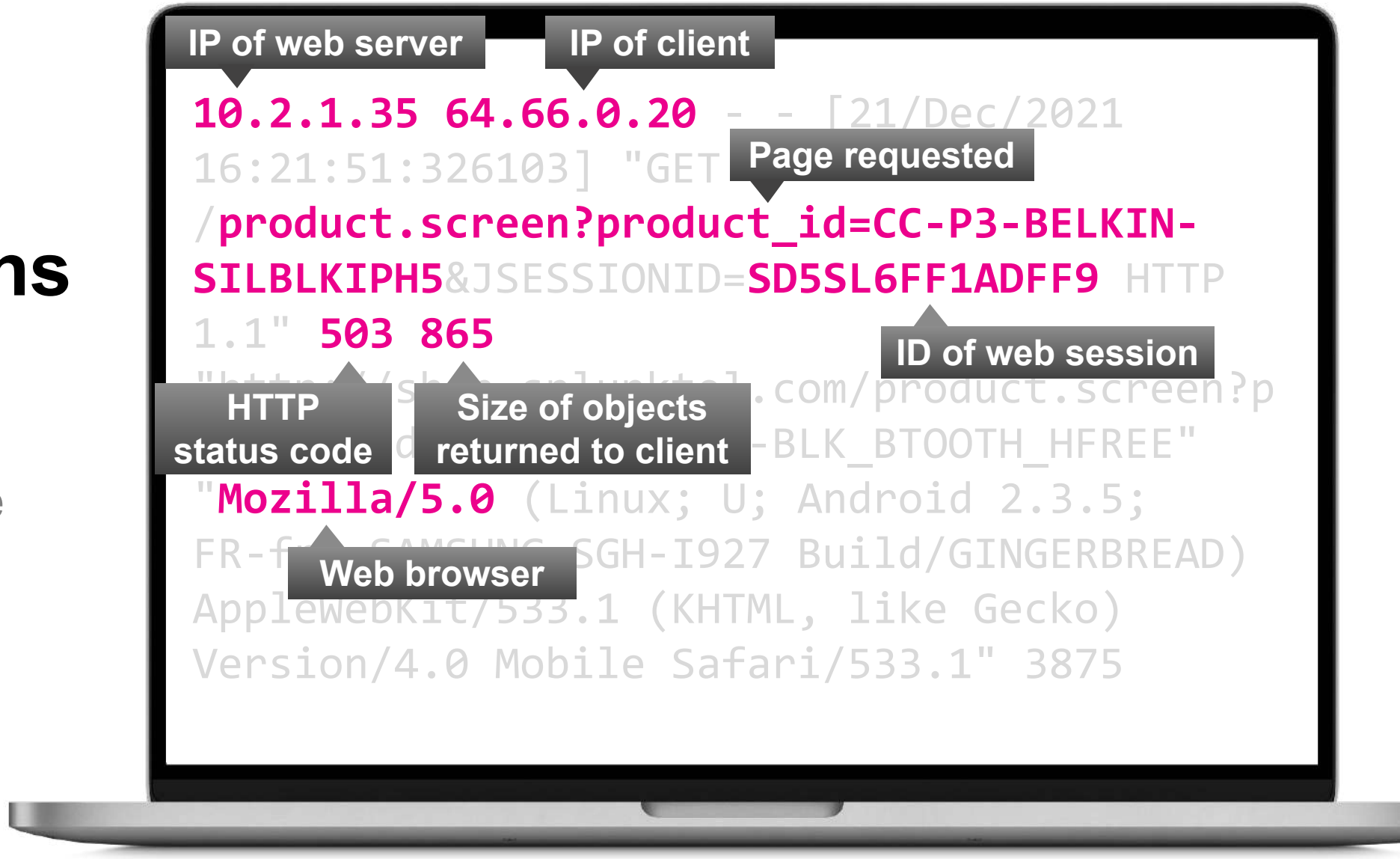
Which mobile handsets should I test the most before releasing my new app?



splunk>

IT Operations Use Case

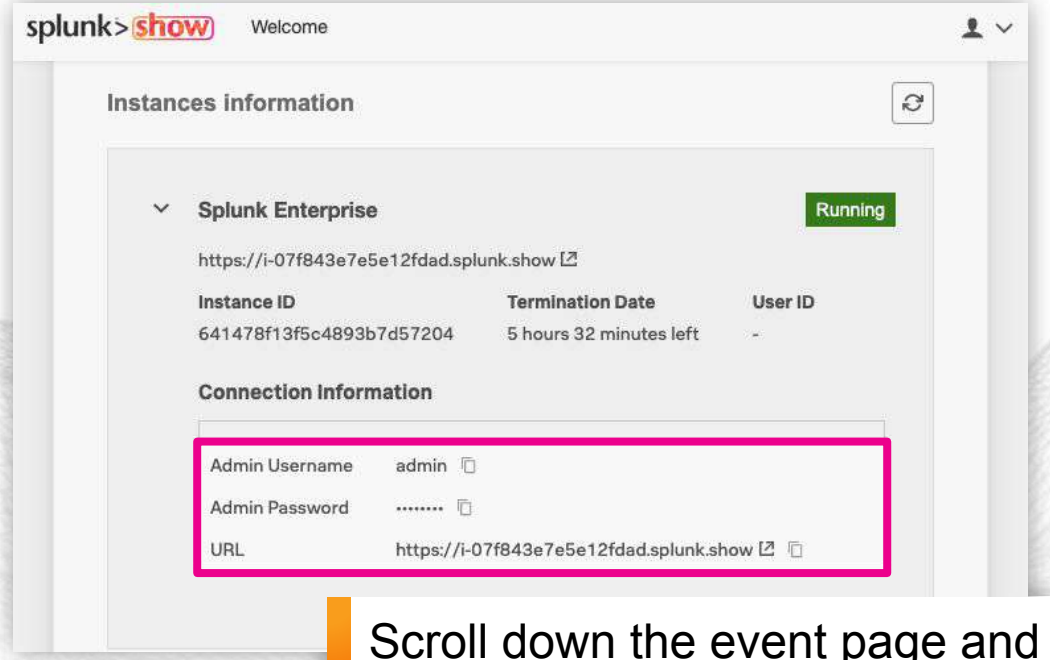
Which web pages are generating the most errors?



splunk>

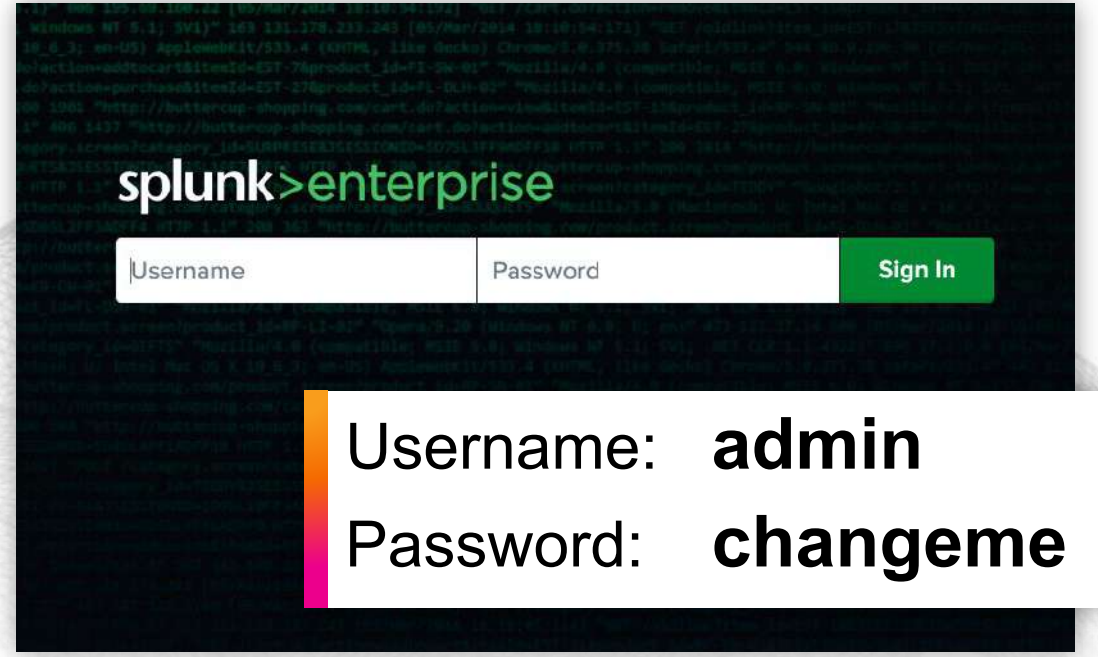
Login to Splunk

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



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

Log in to your Splunk instance



Username: **admin**

Password: **changeme**

splunk>

Apps and Add-ons

- 2900+ free apps and add-ons available from https://splunkbase.splunk.com/
- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs

Apps

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

Add-ons

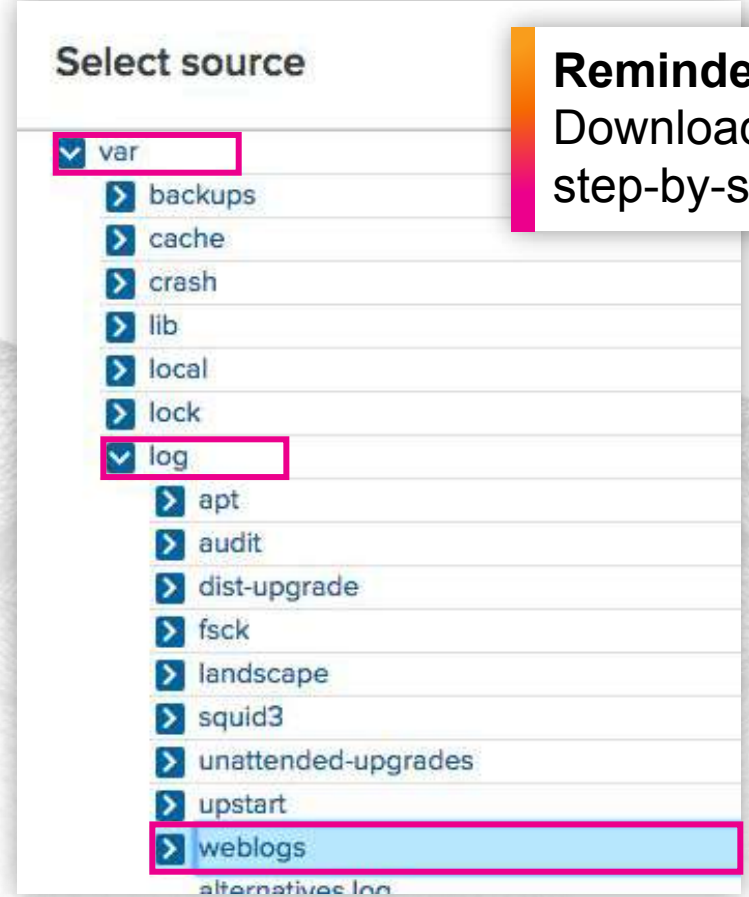
Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

splunk>

Create an App and Add Some Data

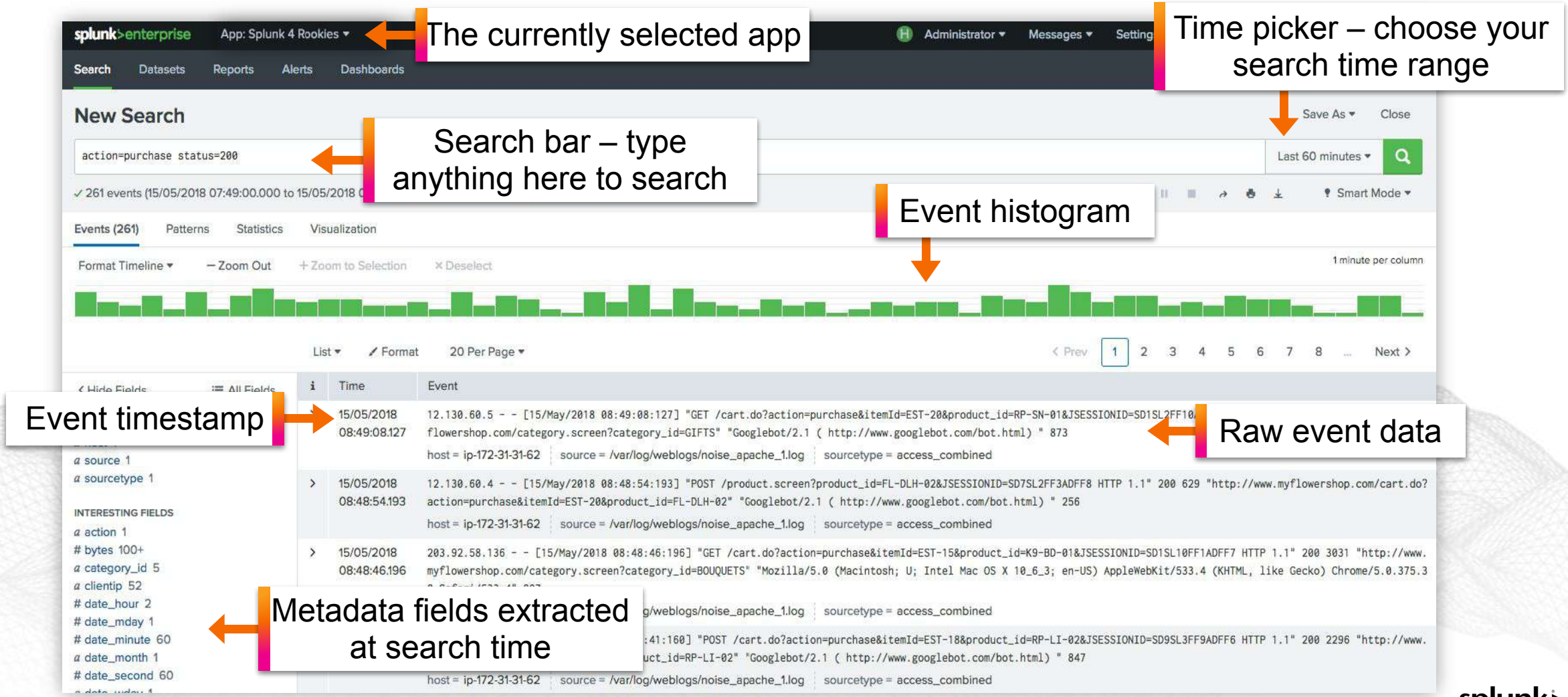
Tasks

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!



splunk>

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

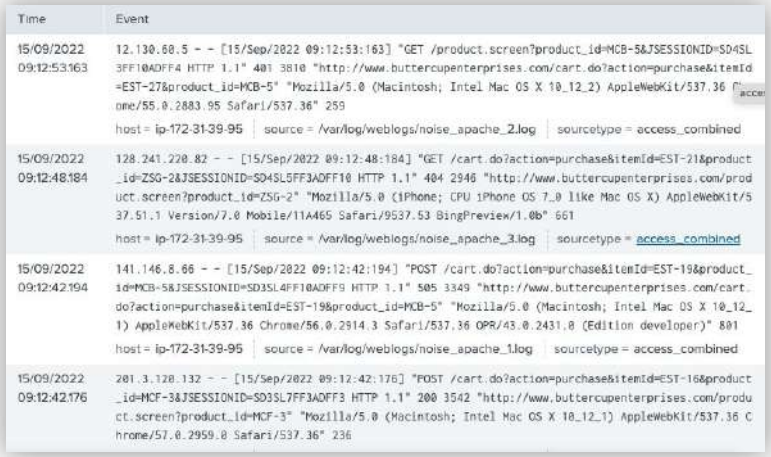
Commands

```
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"`



Time	Event
15/09/2022 09:12:53.163	12.130.60.5 - - [15/Sep/2022 09:12:53:163] "GET /product.screen?product_id=MCB-5&JSESSIONID=SD4SL3FF10ADFF4 HTTP 1.1" 401 3810 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-27&product_id=MCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 [...] one/55.0.2883.95 Safari/537.36" 259 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_2.log sourcetype = access_combined
15/09/2022 09:12:48.184	128.241.220.82 - - [15/Sep/2022 09:12:48:184] "GET /cart.do?action=purchase&itemId=EST-21&product_id=ZSG-2&JSESSIONID=SD4SL5FF3ADFF10 HTTP 1.1" 404 2946 "http://www.buttercupenterprises.com/product.screen?product_id=ZSG-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X) AppleWebKit/537.51.1 Version/7.0 Mobile/11A465 Safari/9537.53 BingPreview/1.0b" 661 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_3.log sourcetype = access_combined
15/09/2022 09:12:42.194	141.146.8.66 - - [15/Sep/2022 09:12:42:194] "POST /cart.do?action=purchase&itemId=EST-19&product_id=MCB-5&JSESSIONID=SD3SL4FF10ADFF9 HTTP 1.1" 505 3349 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-19&product_id=MCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/56.0.2814.3 Safari/537.36 OPR/43.0.2431.0 (Edition developer)" 801 host = ip-172-31-39-95 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/09/2022 09:12:42.176	201.3.128.132 - - [15/Sep/2022 09:12:42:176] "POST /cart.do?action=purchase&itemId=EST-16&product_id=MCF-3&JSESSIONID=SD3SL7FF3ADFF3 HTTP 1.1" 200 3542 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/57.0.2959.0 Safari/537.36" 236

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 | Buttercup Enterprises

Your Company

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

Your Role

- 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/Fraud**

What Does the Business Want to See?

We Need to Create a Dashboard With Four Views

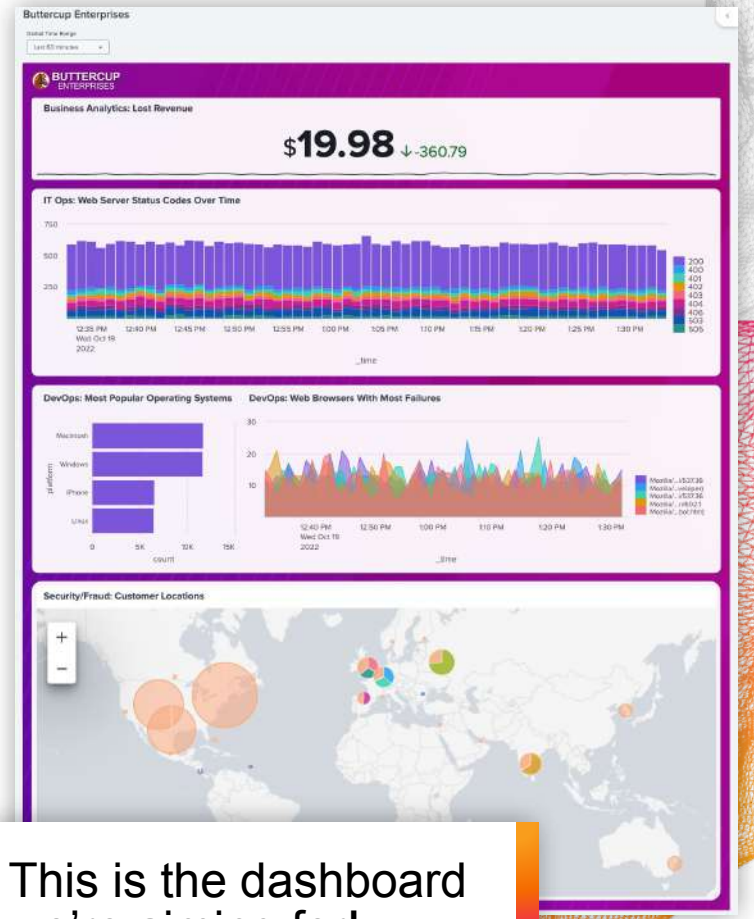
IT Operations team: Investigate successful vs unsuccessful web server requests over time

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/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!

splunk>

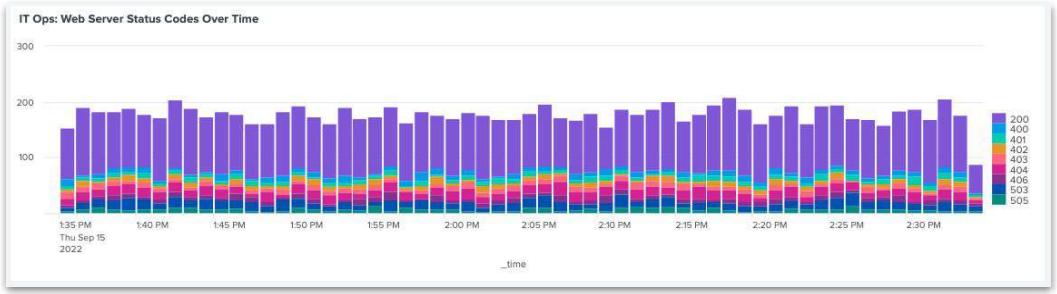
IT Operations Team

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>

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

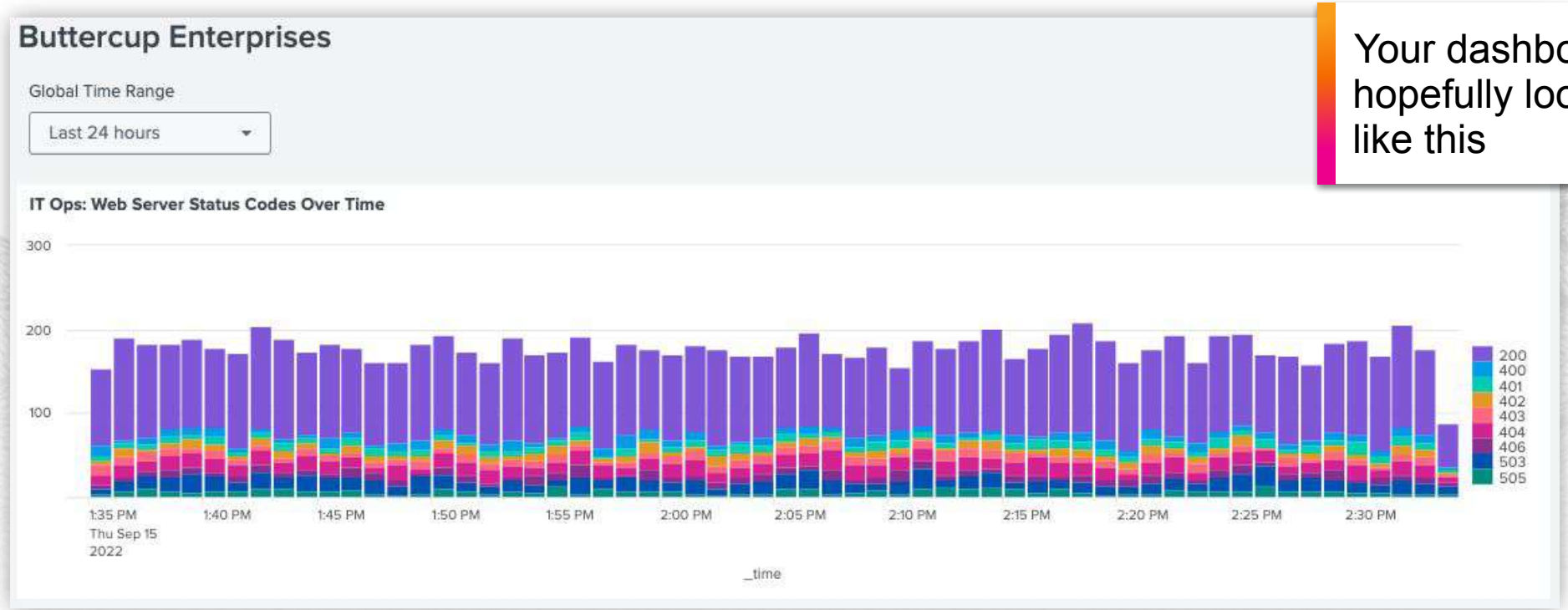
- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images**, **text boxes**, **shapes**, **lines** and **icons**, with **intact PDF export**
- **No custom code** required

splunk>

Your Dashboard So Far

Solution

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



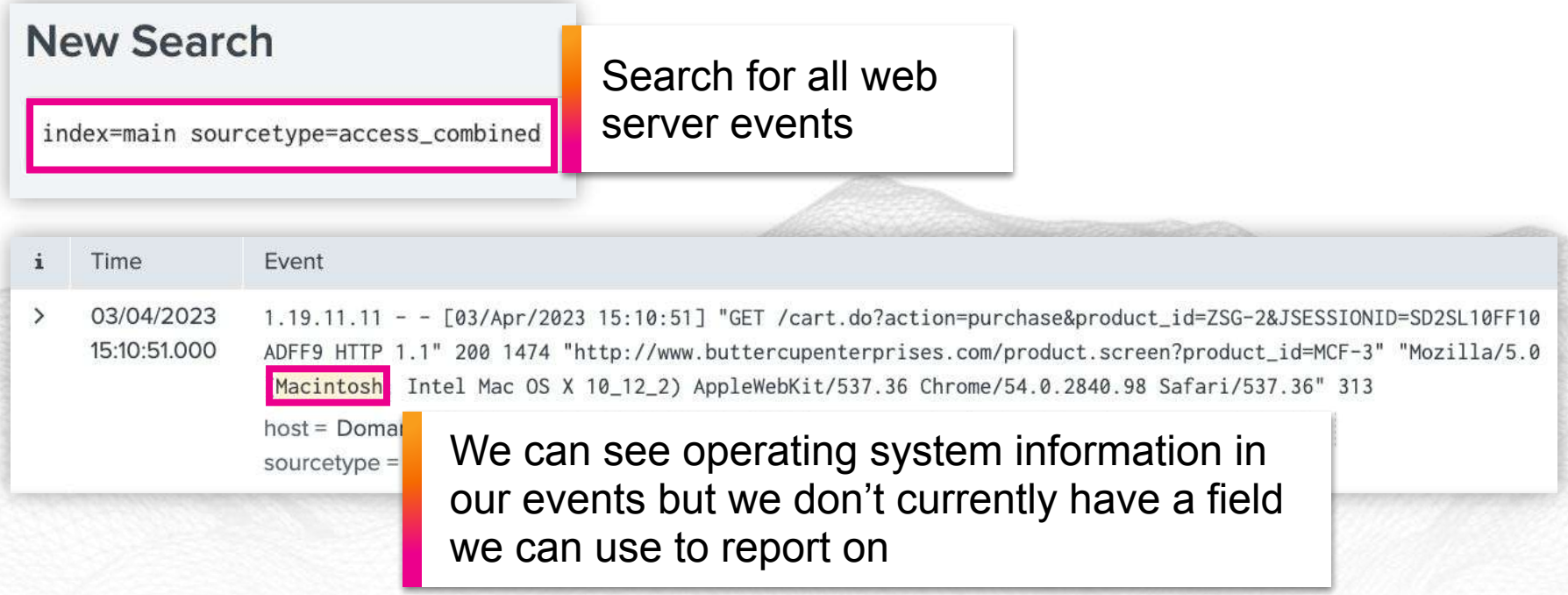
Your dashboard should hopefully look something like this

splunk>

DevOps Team

Show the Most Common Customer Operating Systems and Which Web Browsers are Experiencing the Most Failures

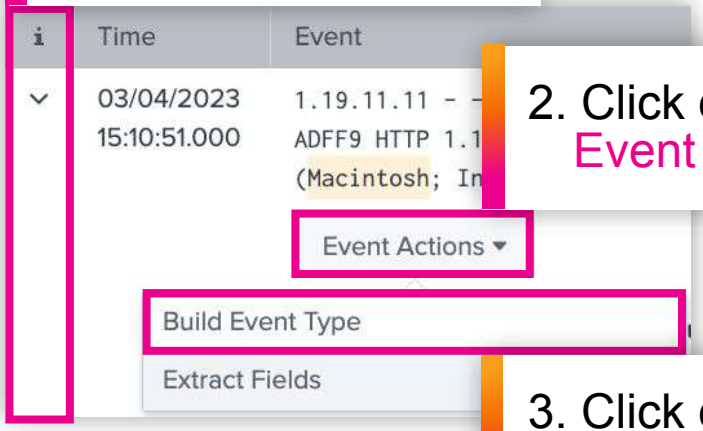
Step 1: Show the most common customer operating systems



splunk>

Extracting a New Field

1. Click on the arrow to expand an event

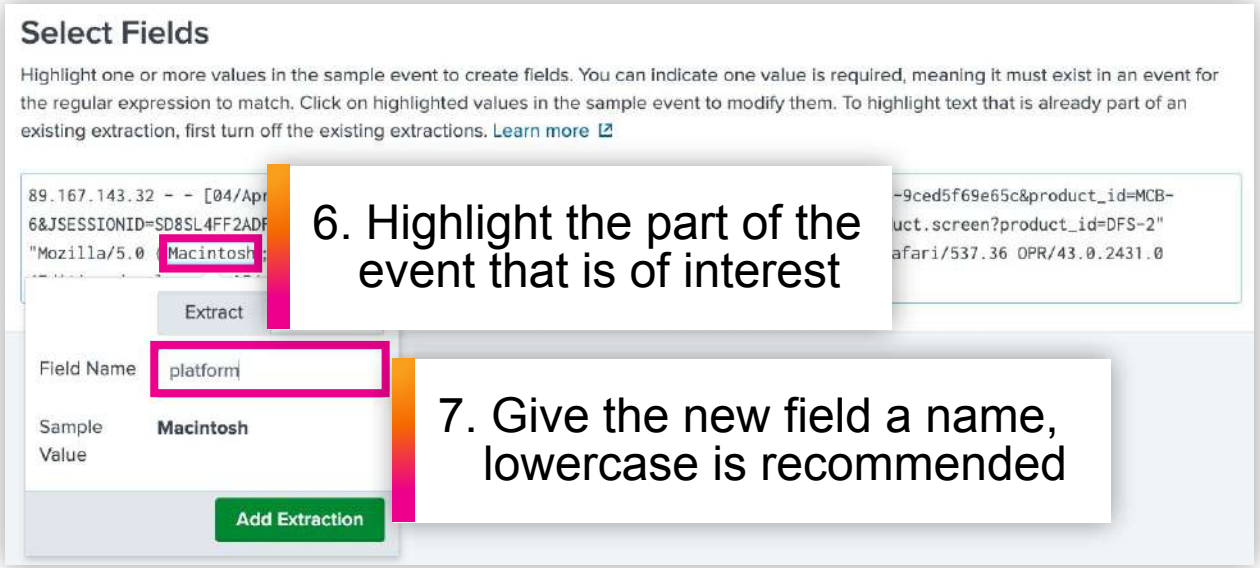


2. Click on Event Actions

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

splunk>

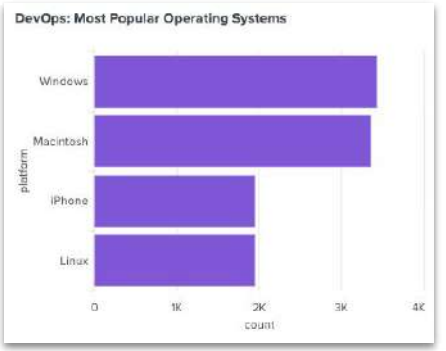
DevOps Team

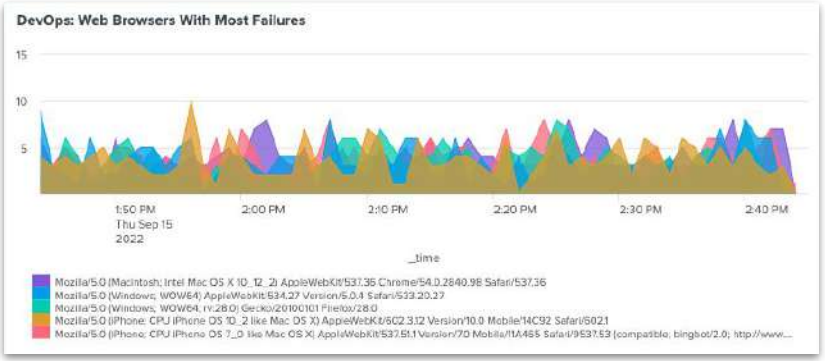
Show the most common customer operating systems and which web browsers are experiencing the most failures

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



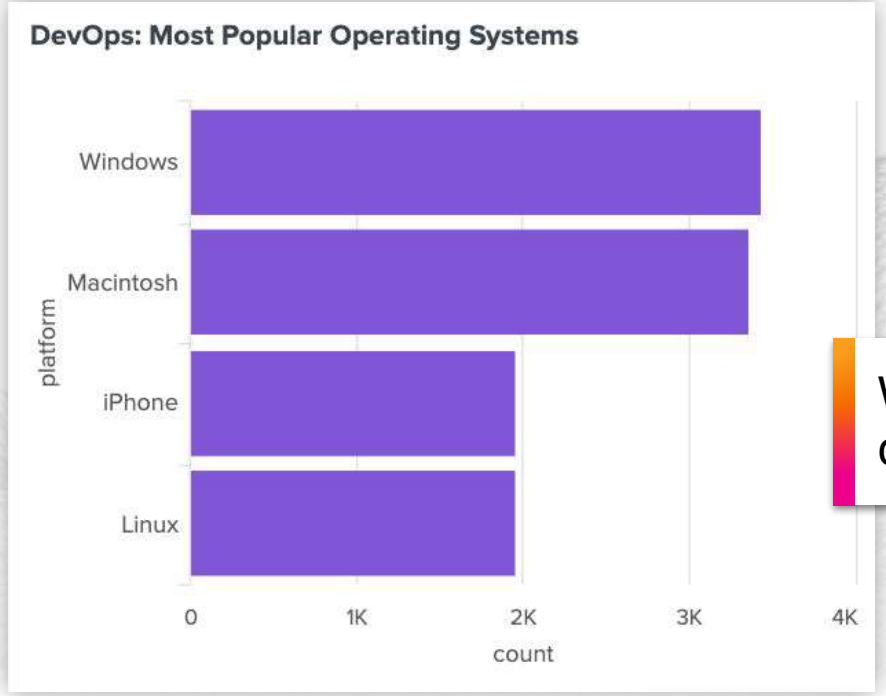


DevOps Team

Show The Most Common Customer Operating Systems

Solution

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



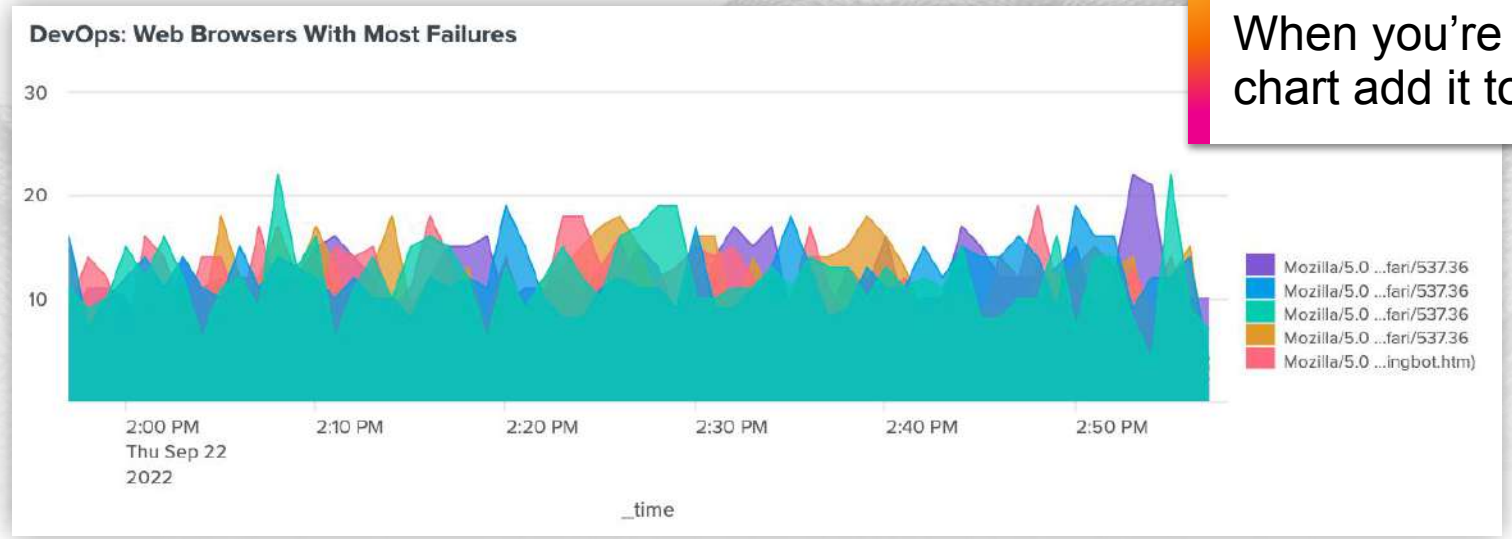
When you're happy with your chart add it to your dashboard!

DevOps Team

Create A Graph Showing the Top 5 Web Browsers That Are Experiencing the Most Failures Over Time

Solution

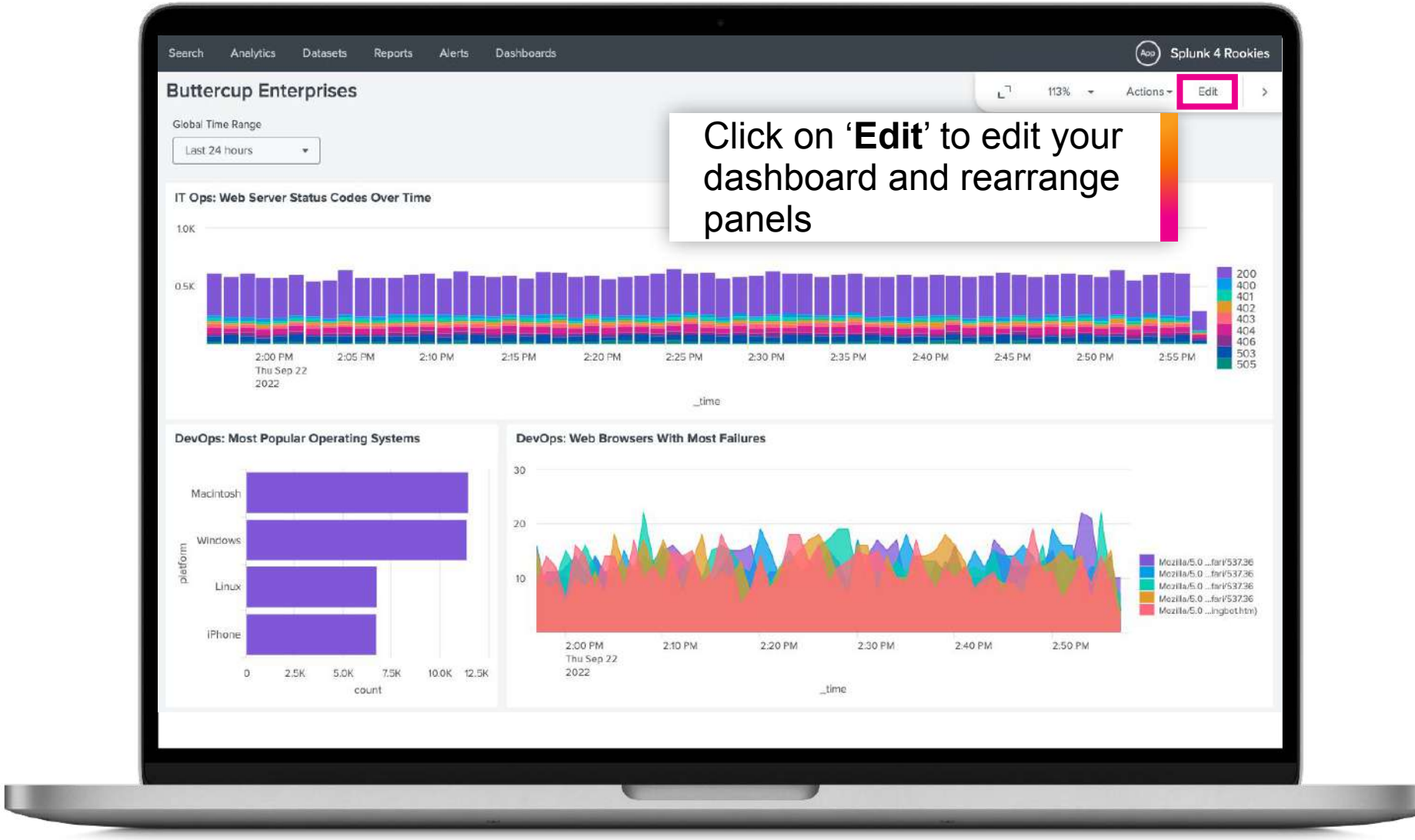
```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5 useother=f
```



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

splunk>

Your Dashboard so far…



Click on '**Edit**' to edit your dashboard and rearrange panels

Working with statistics? Use `stats` and `timechart`

Usage

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

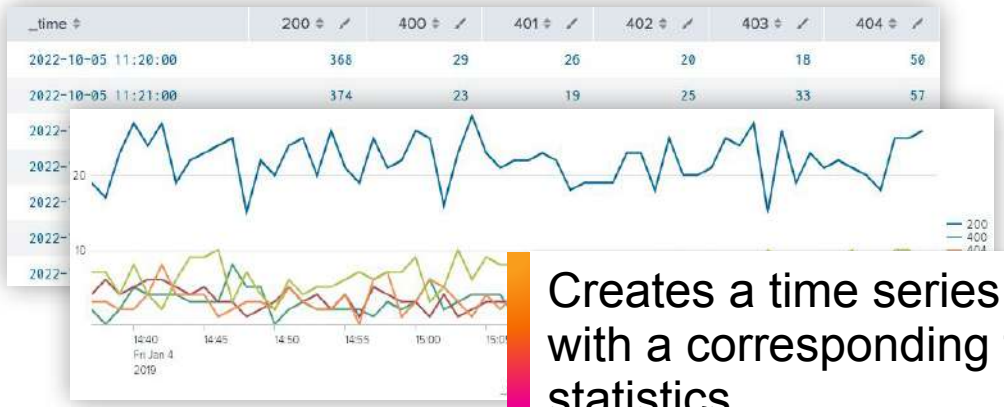
Examples

```
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

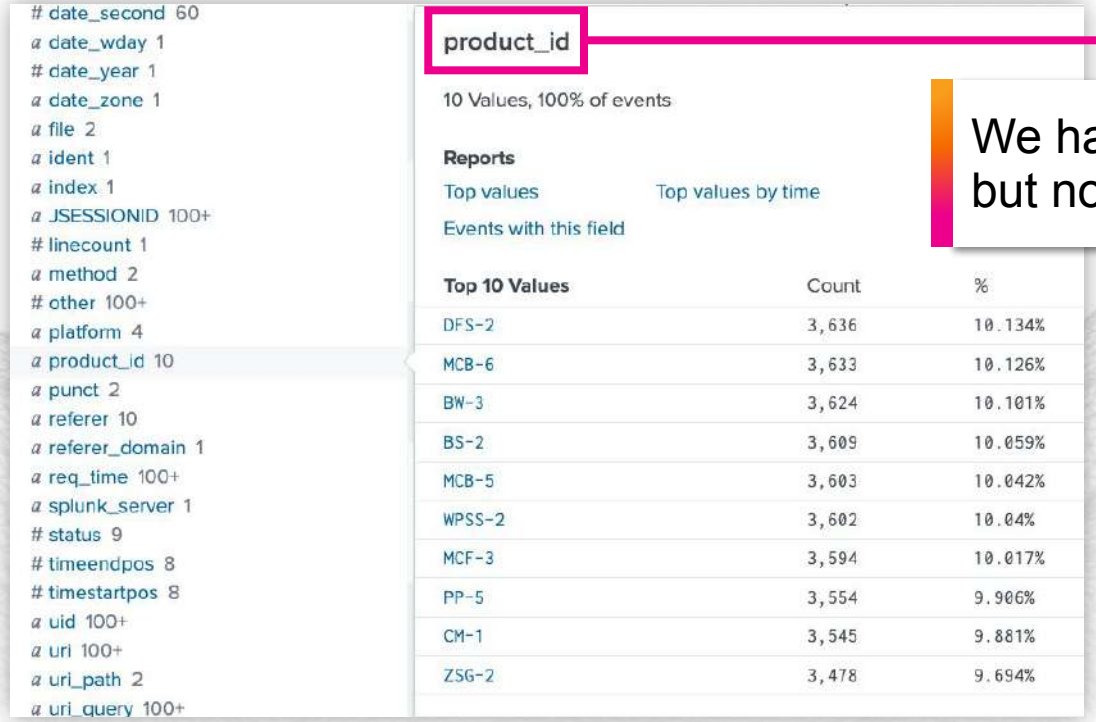
Want to know more? Check out:
Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef

splunk>

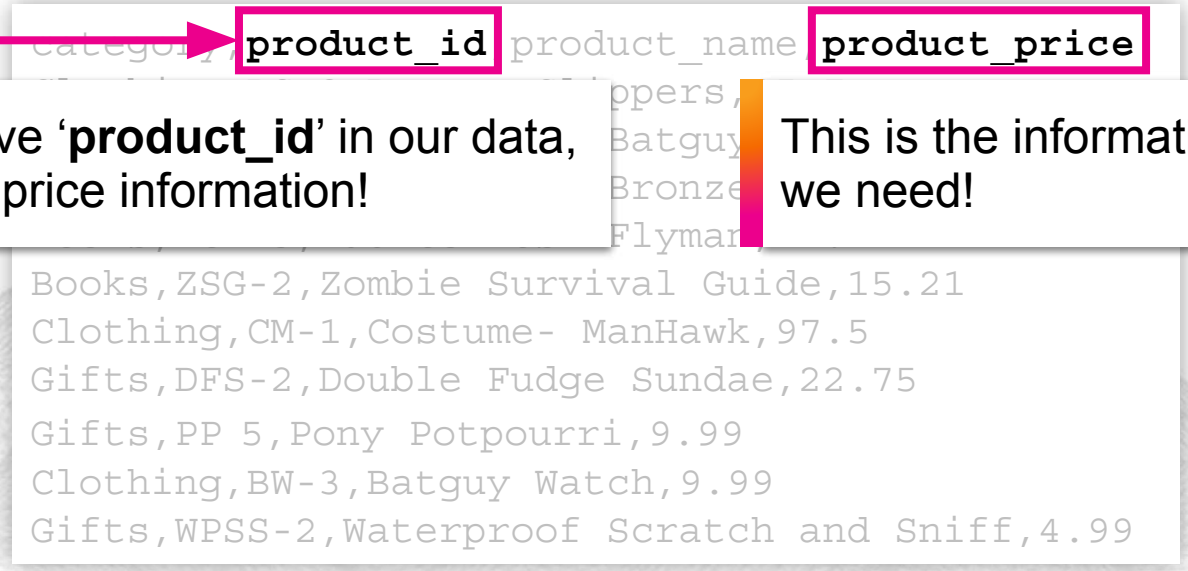
Business Analytics Team

Show Lost Revenue from the Website

Fields extracted from events by Splunk:



External CSV file:

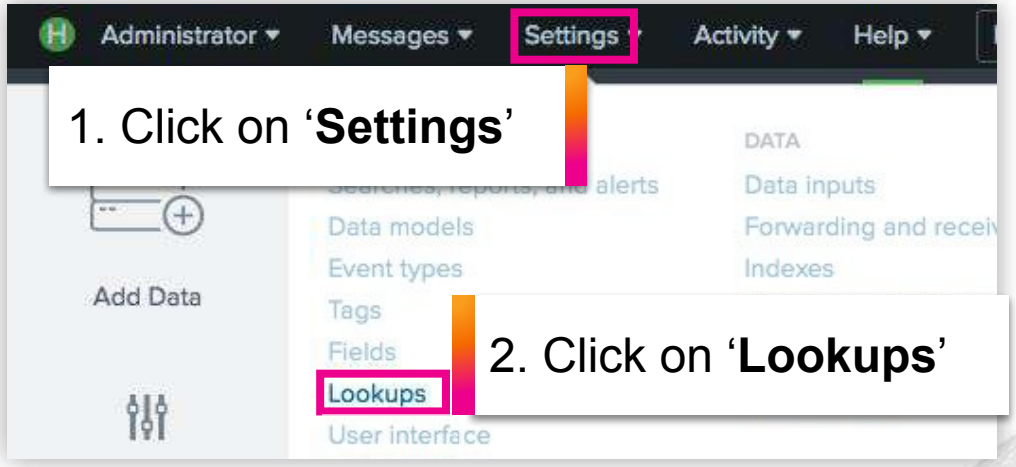


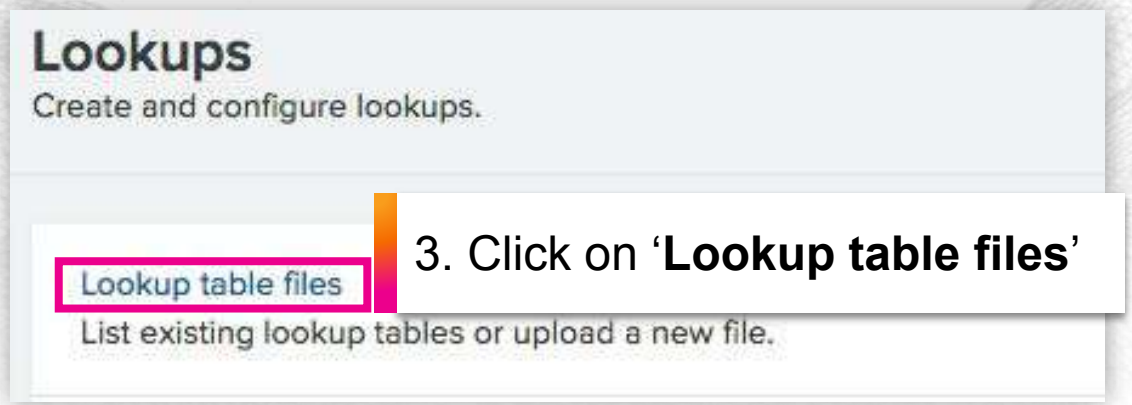
We have '**product_id**' in our data, but no price information!

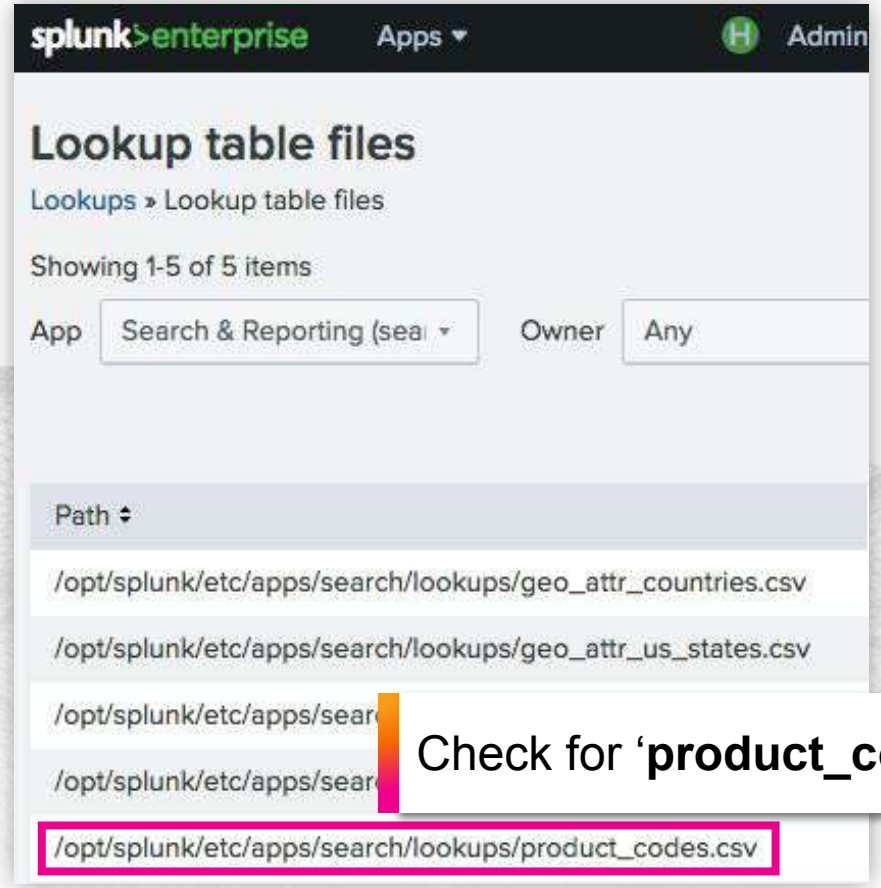
This is the information we need!

Verify That the Lookup File Exists

A lookup file has already been uploaded for you!







splunk>

Enriching Data with the `lookup` Command

Usage

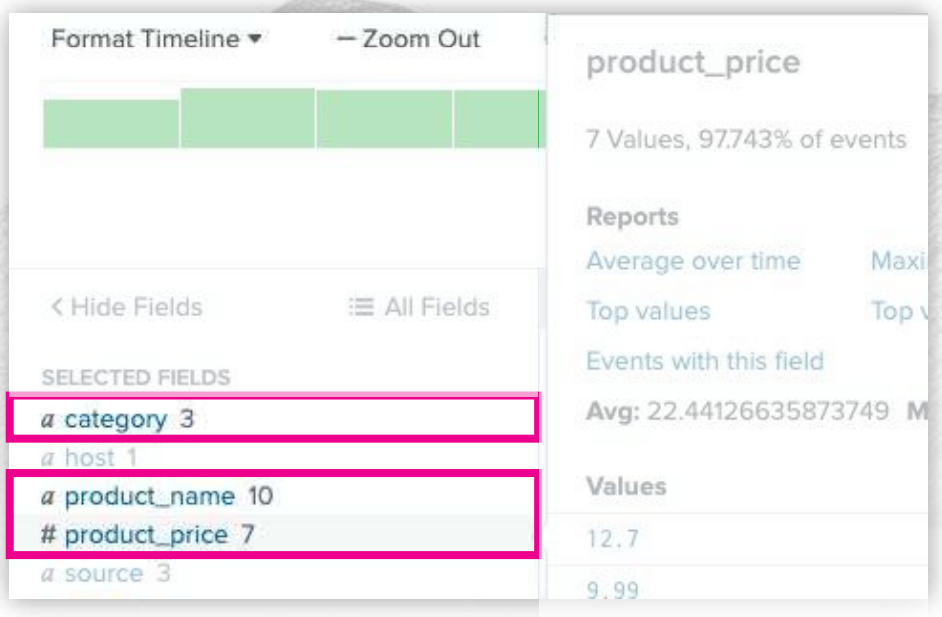
```
<your search> | lookup product_codes.csv product_id
```

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



splunk>

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!

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

splunk>

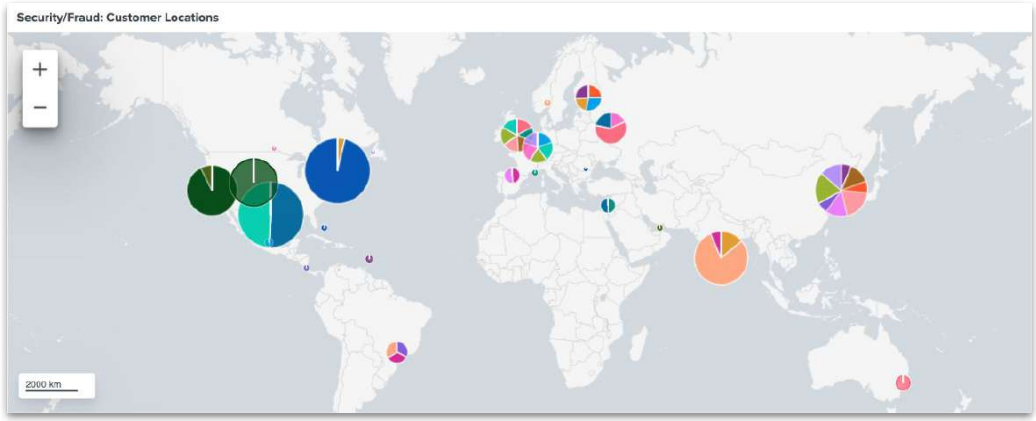
Security and Fraud Teams

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

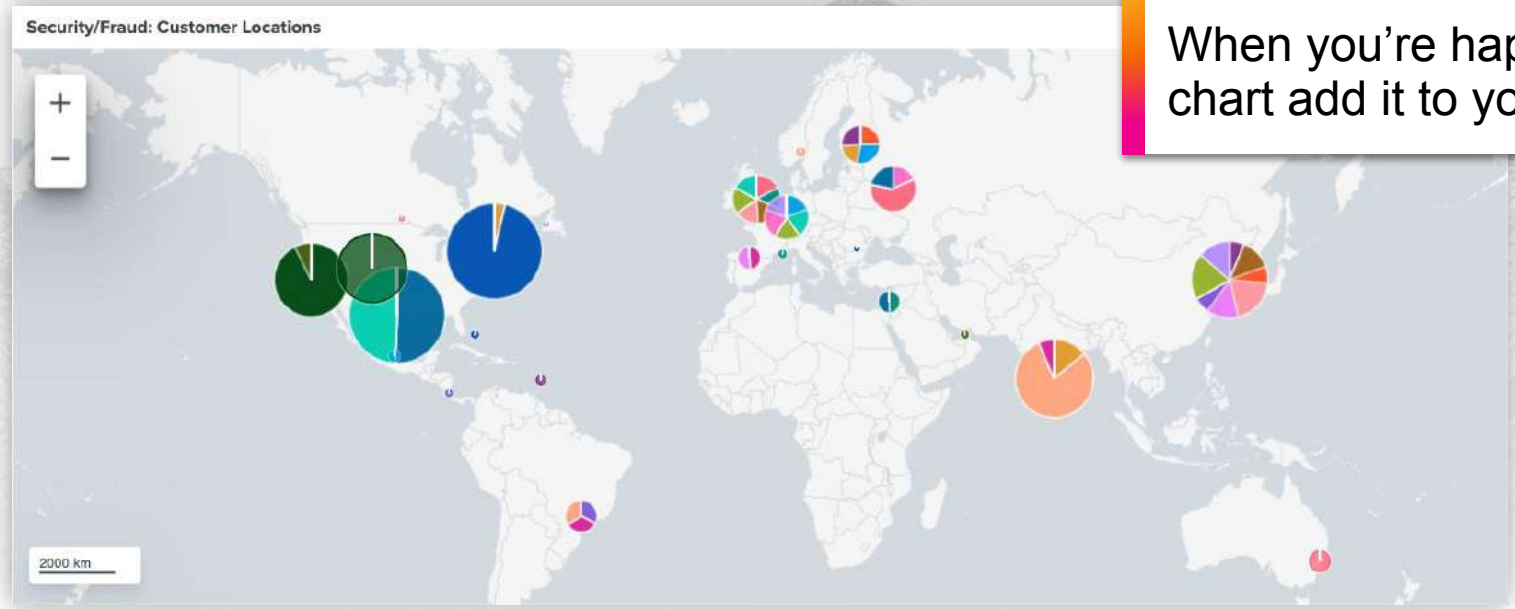


Security and Fraud Teams

Show Website Activity by Geographic Location

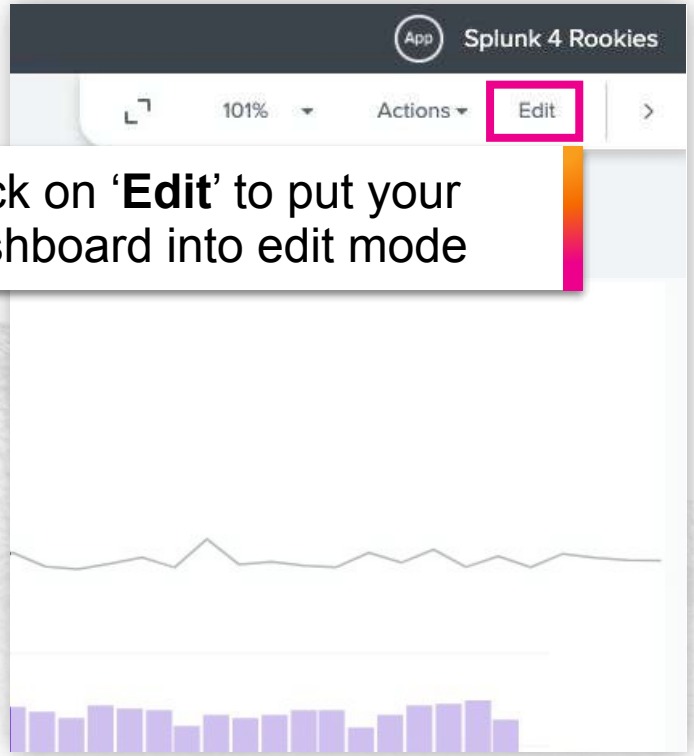
Solution

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

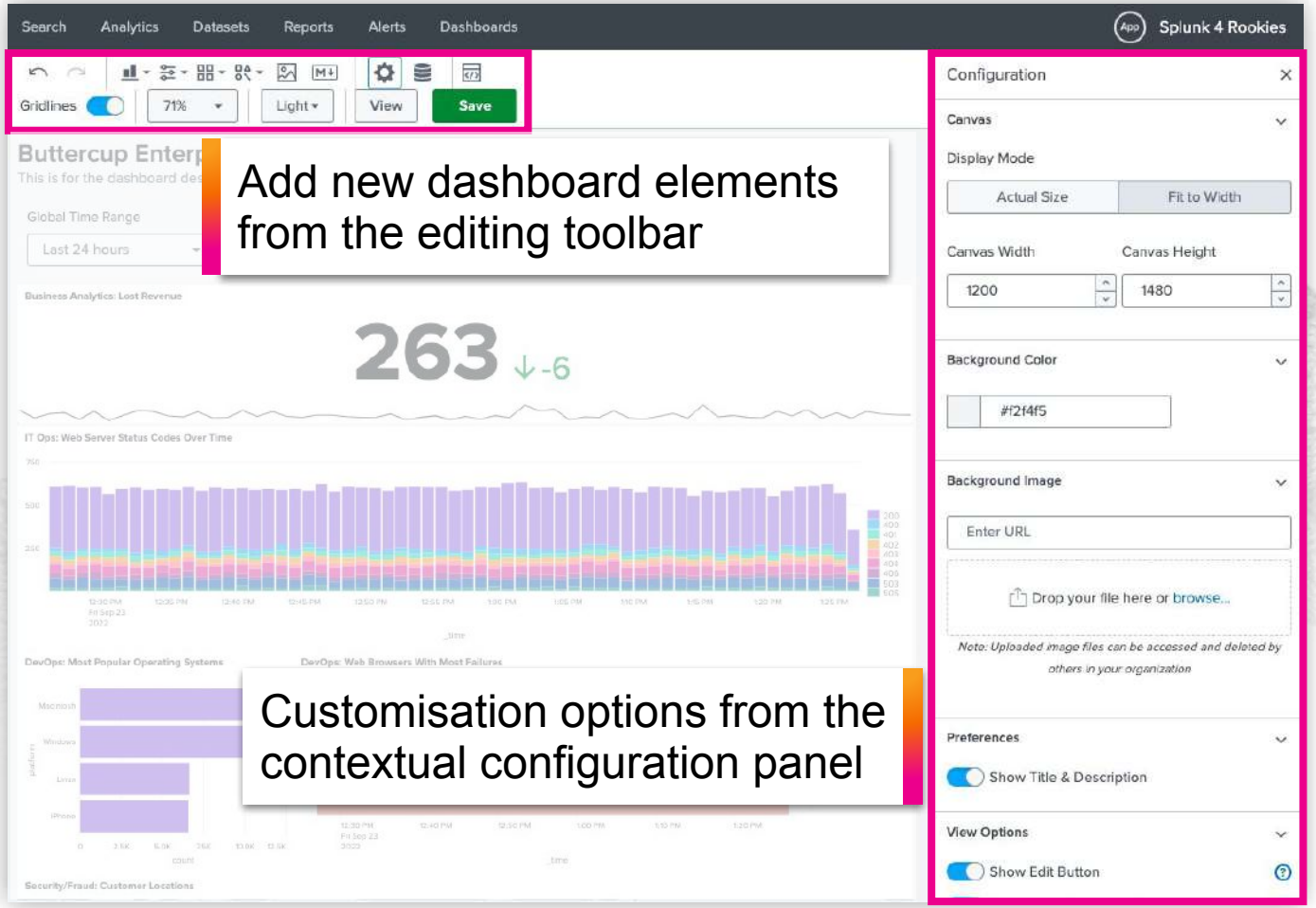


When you're happy with your chart add it to your dashboard!

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

splunk>

Customise Your Dashboard

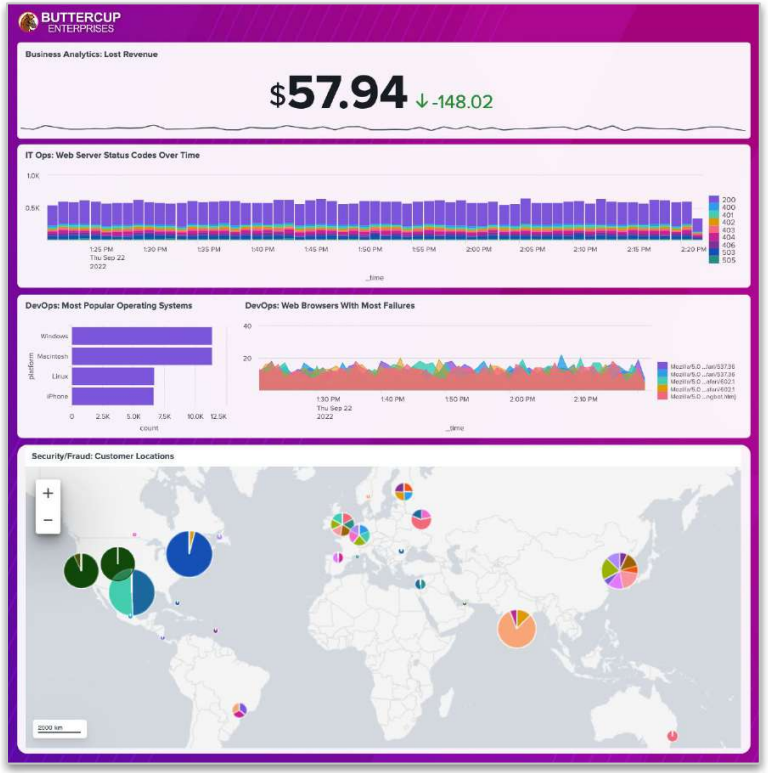
Tasks

1. Add a custom background image provided by the Buttercup Enterprises Marketing team (https://splk.it/ButtercupBackground)

2. Resize your dashboard panels to fit within the boxes on the background image

3. Link your dashboard panels to the global time picker

Goal

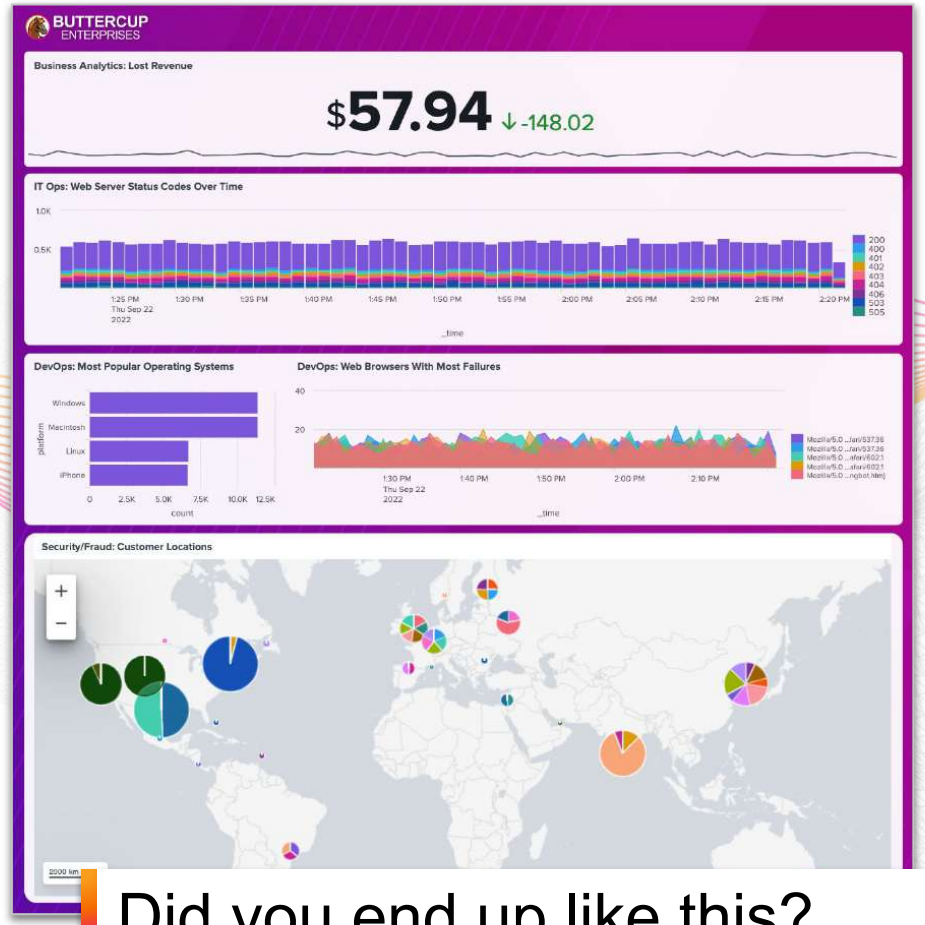


splunk>

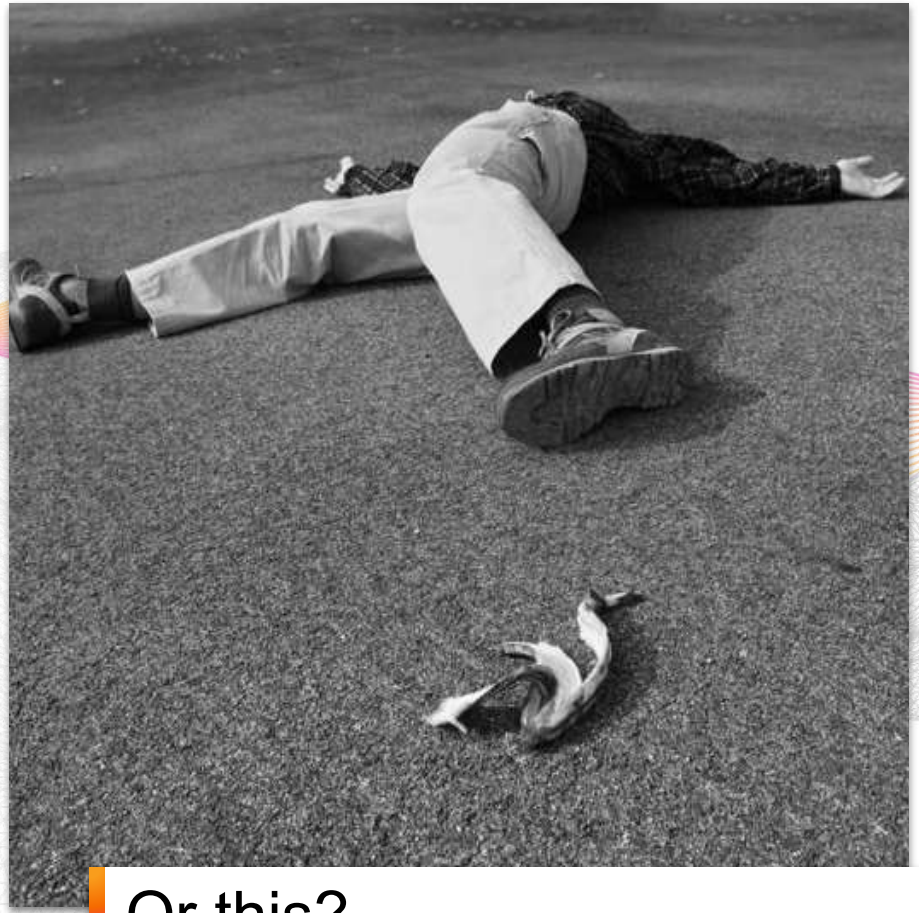
You Finished the Hands-on Exercises!

You made it!

How Did You Do?



Did you end up like this?...



Or this?

splunk>

Splunk Resources

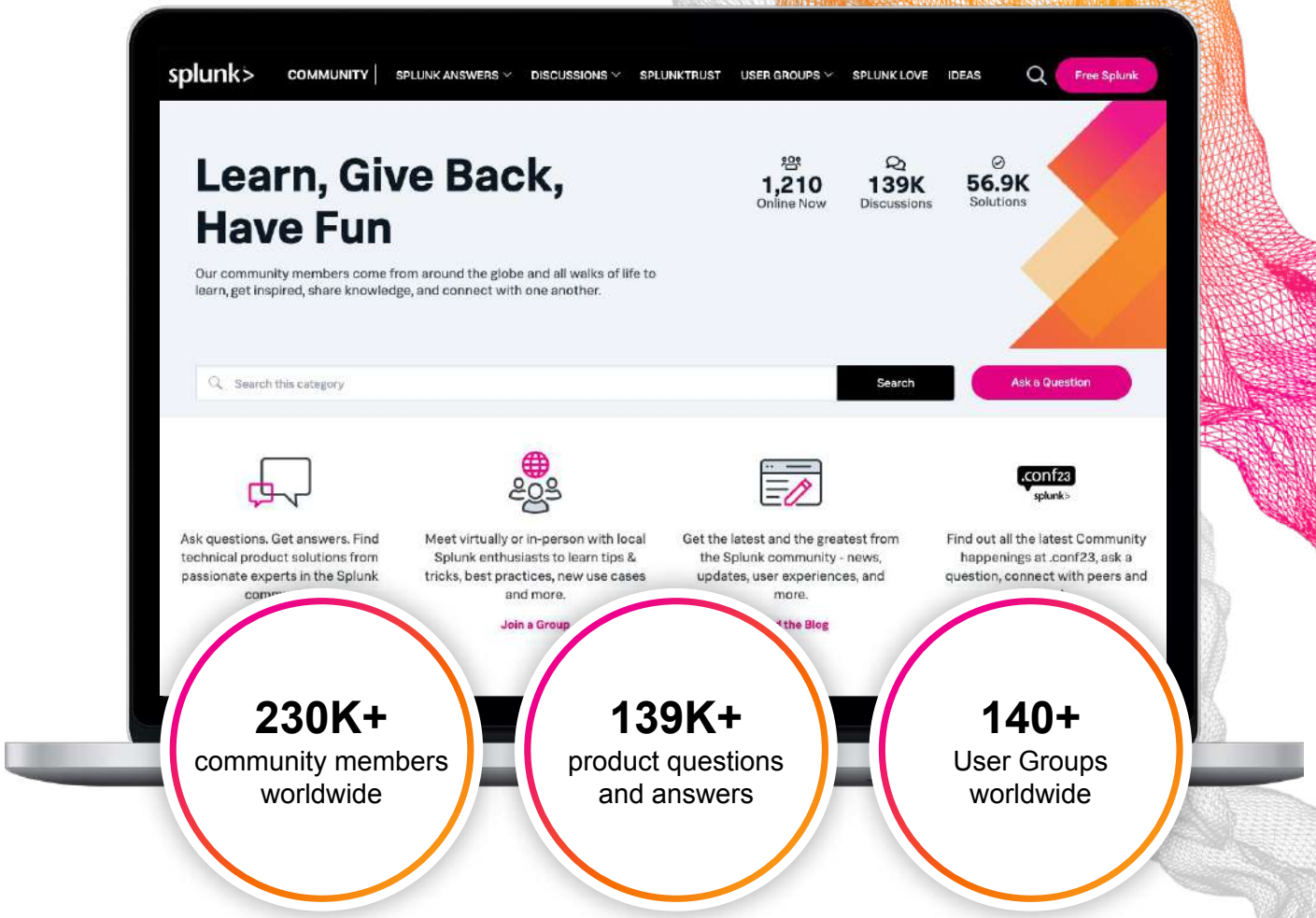
Where to go after today's workshop

splunk>

Splunk Community

https://community.splunk.com

- A free way to connect, learn, have fun, and find success with Splunk
- Ask questions, get answers, and find solutions from passionate experts in the community
- Meet in-person or virtually with like-minded enthusiasts, in your area or by interest
- Search for, vote on, or submit your own ideas for new enhancements for any product or solution



splunk>

Splunk Events

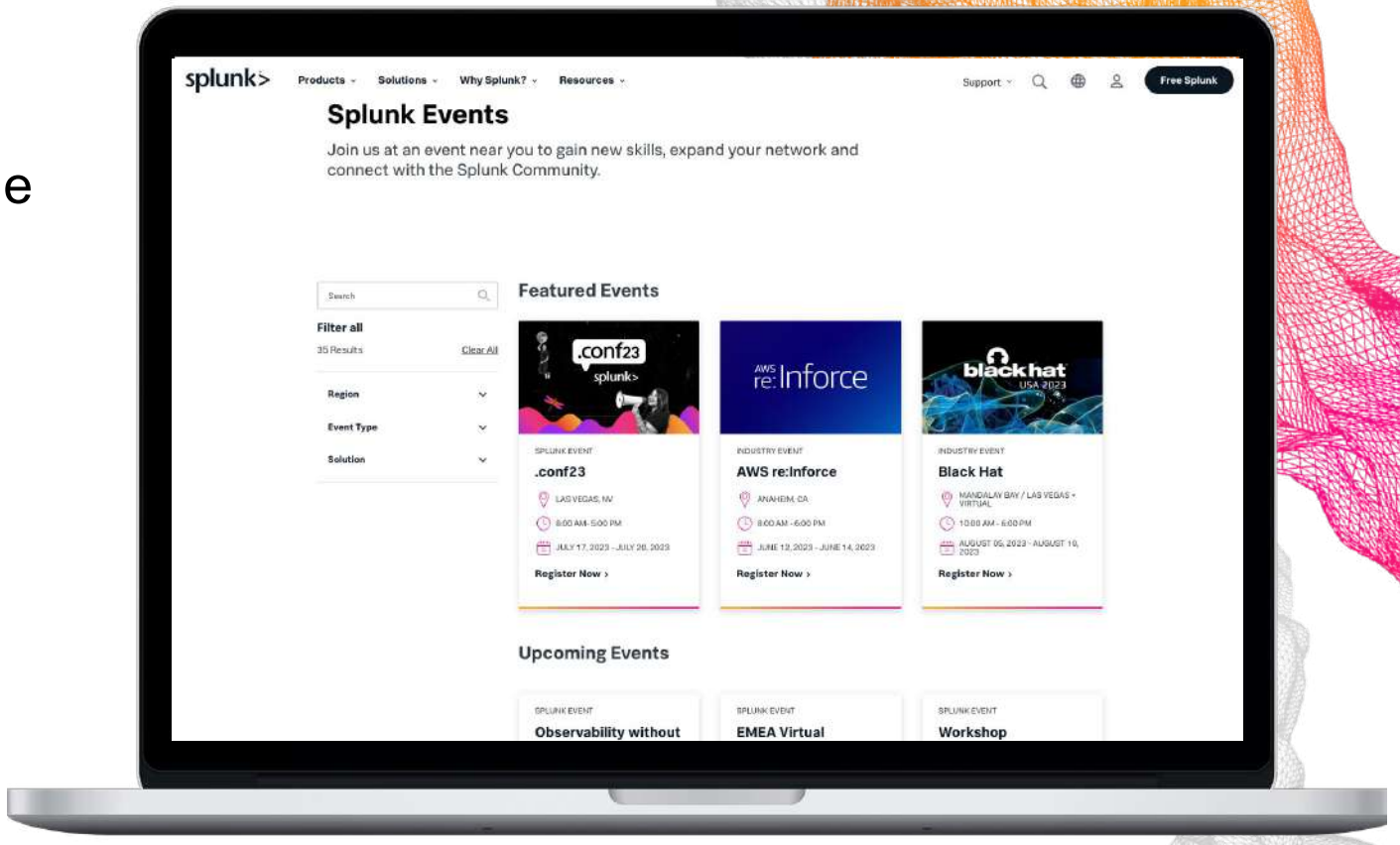
https://events.splunk.com

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

.conf

https://conf.splunk.com

- Join us at .conf23!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!

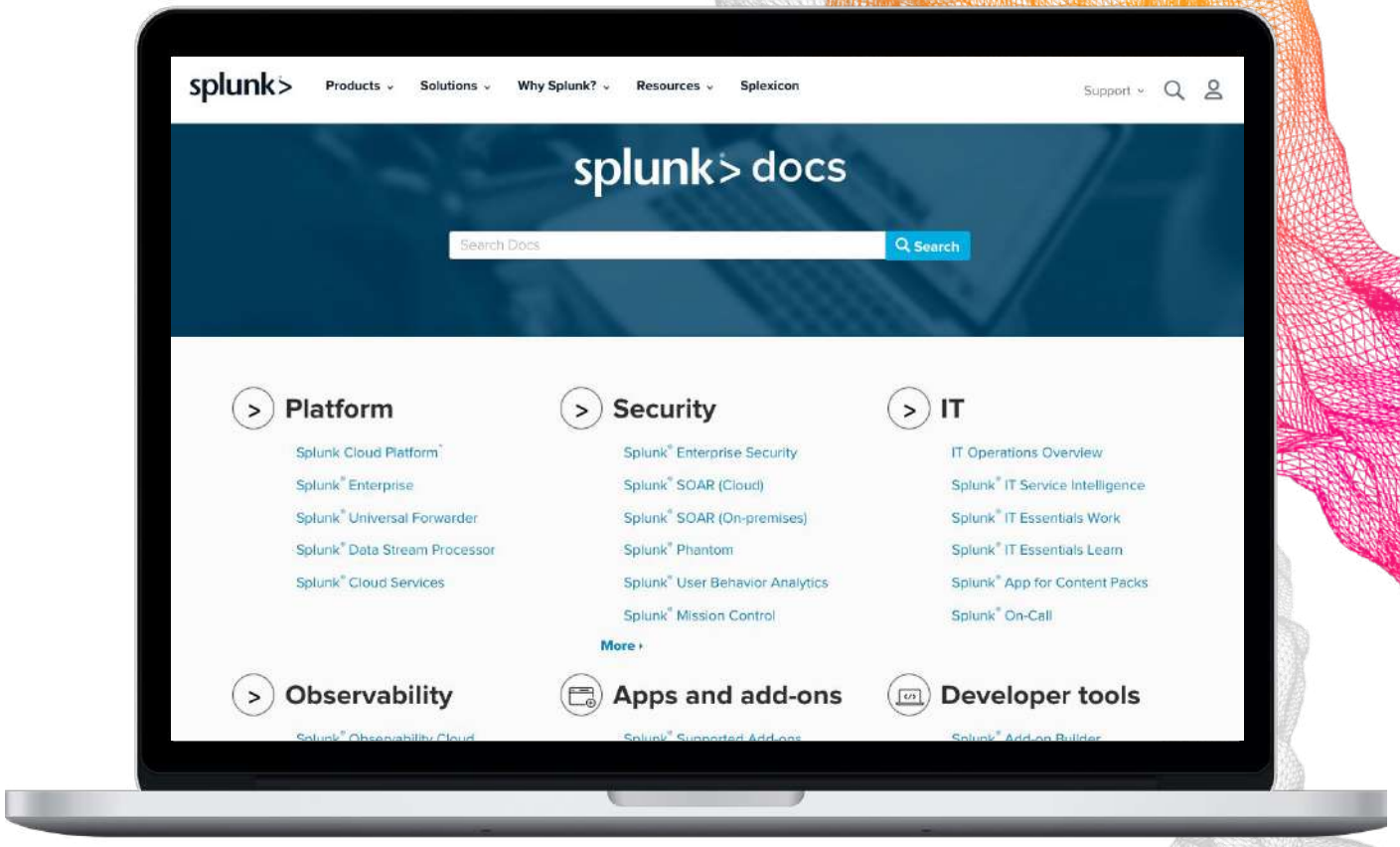


splunk>

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!

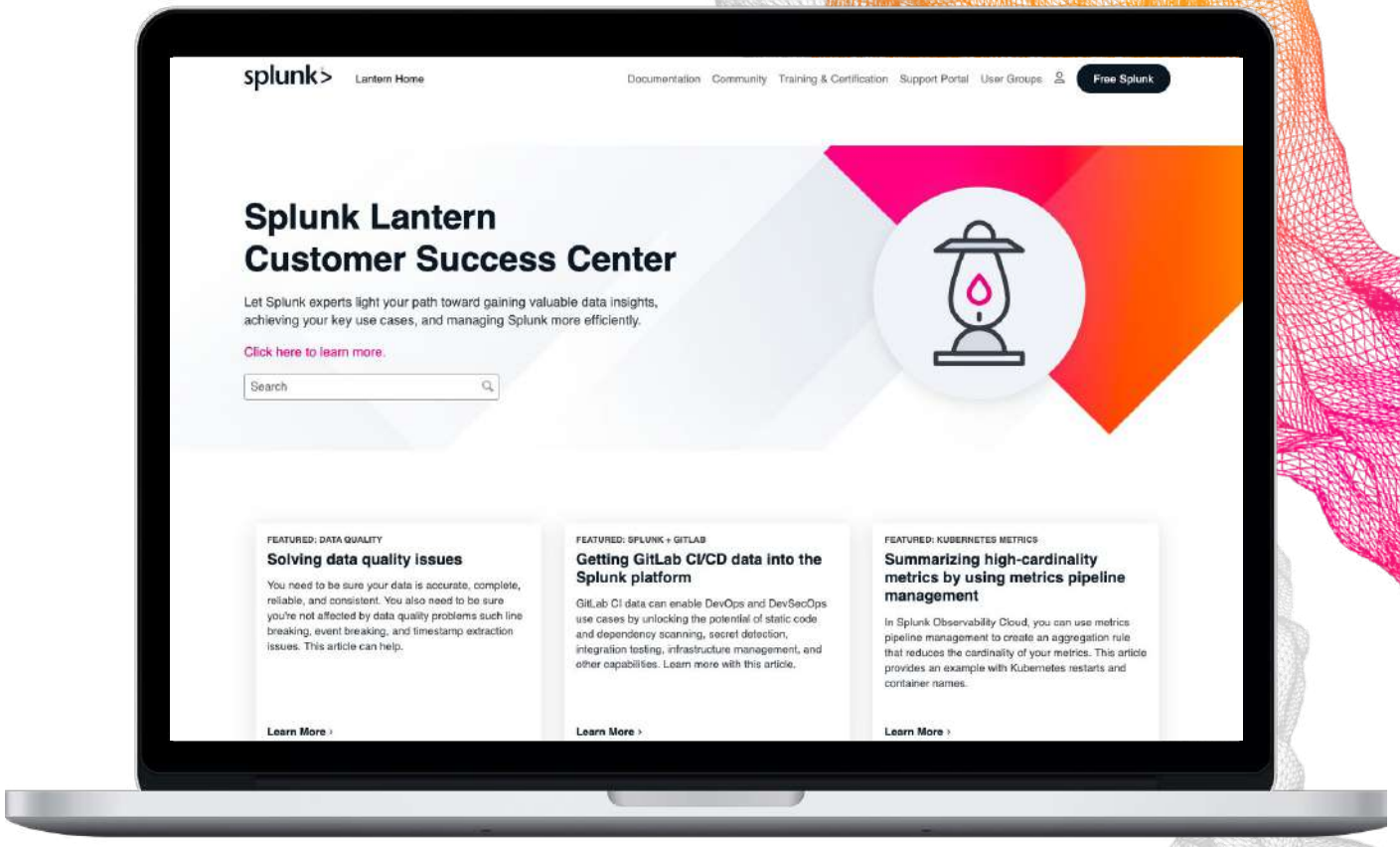


splunk>

Splunk Lantern

https://lantern.splunk.com

- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation

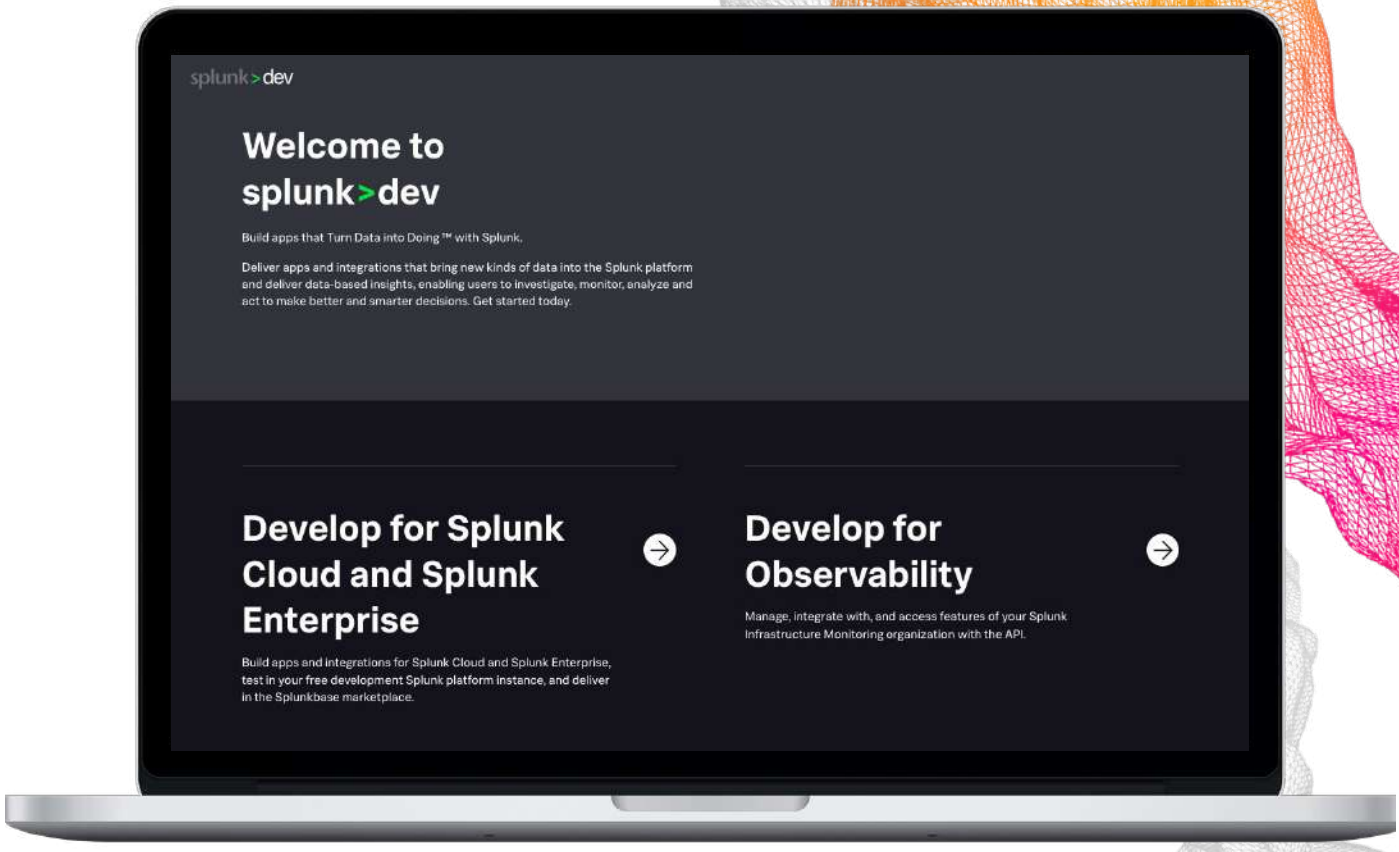


splunk>

Developer Resources

https://dev.splunk.com

- Developer Guide
- API Reference
- Tutorials
- Downloads
  APIs, libraries, tools
- Code examples
- Free Developer licence
- Splunk Cloud Developer Edition
  Test your apps for Splunk Cloud readiness

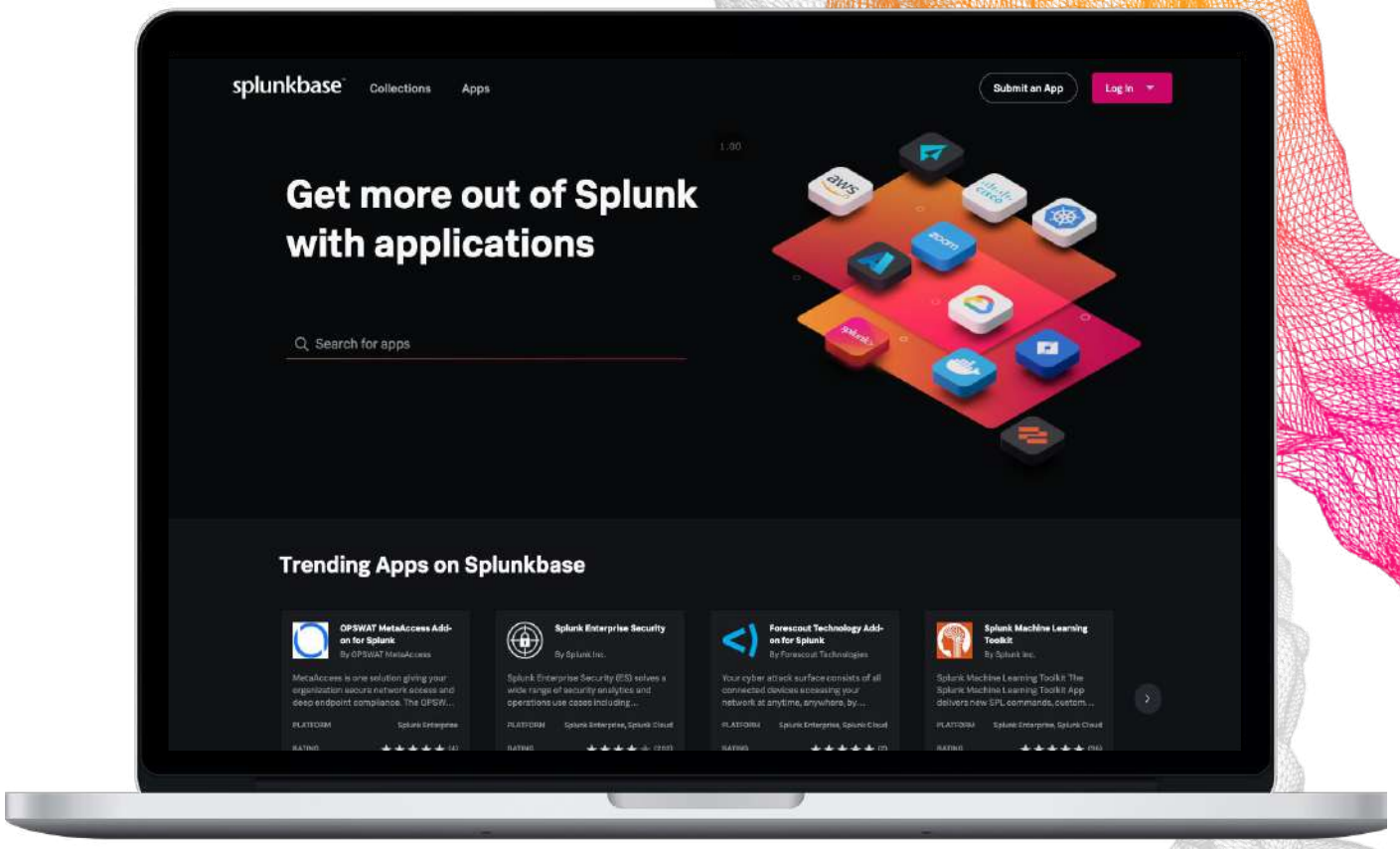


splunk>

Splunk Apps & Add-ons

https://splunkbase.splunk.com/

- 2900+ 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

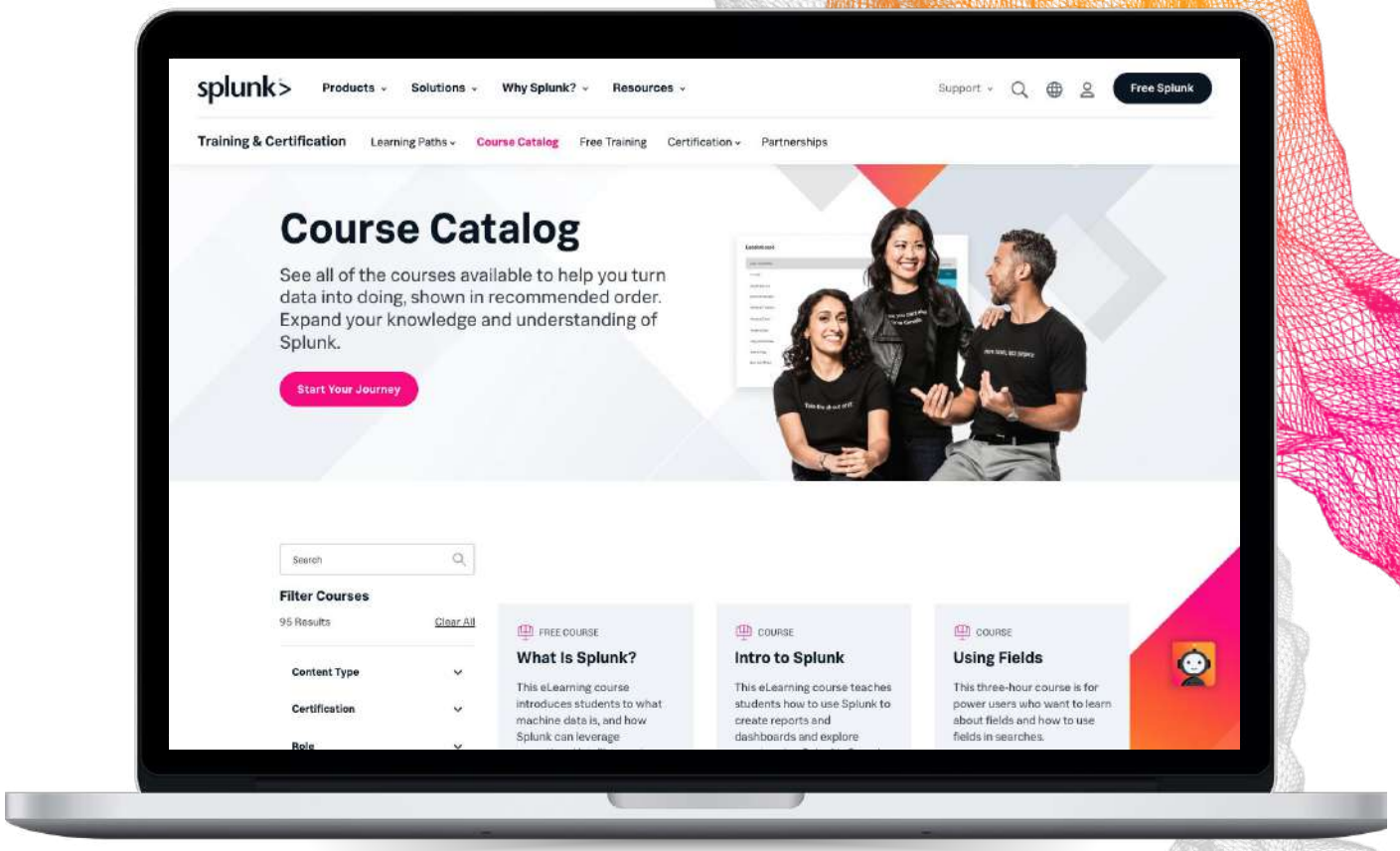
https://splunk.com/training

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!
Free single-subject eLearning courses to kick start your Splunk learning



splunk>

Thank You!