

splunk®> 4 rookies

Hands-On Workshop



splunk®

Forward-looking statements

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

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

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

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.
© 2024 Splunk Inc. All rights reserved.

Please introduce yourself!

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



Workshop Agenda

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

There's a Lot More to Splunk

Clustering
Data Models
Alerting
Pivot
SDKs
APIs
DB Connect

Advanced Searches
SOAR
Machine Learning
AI

Splunk Stream
Deployment Server
Federated Search
Metrics

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

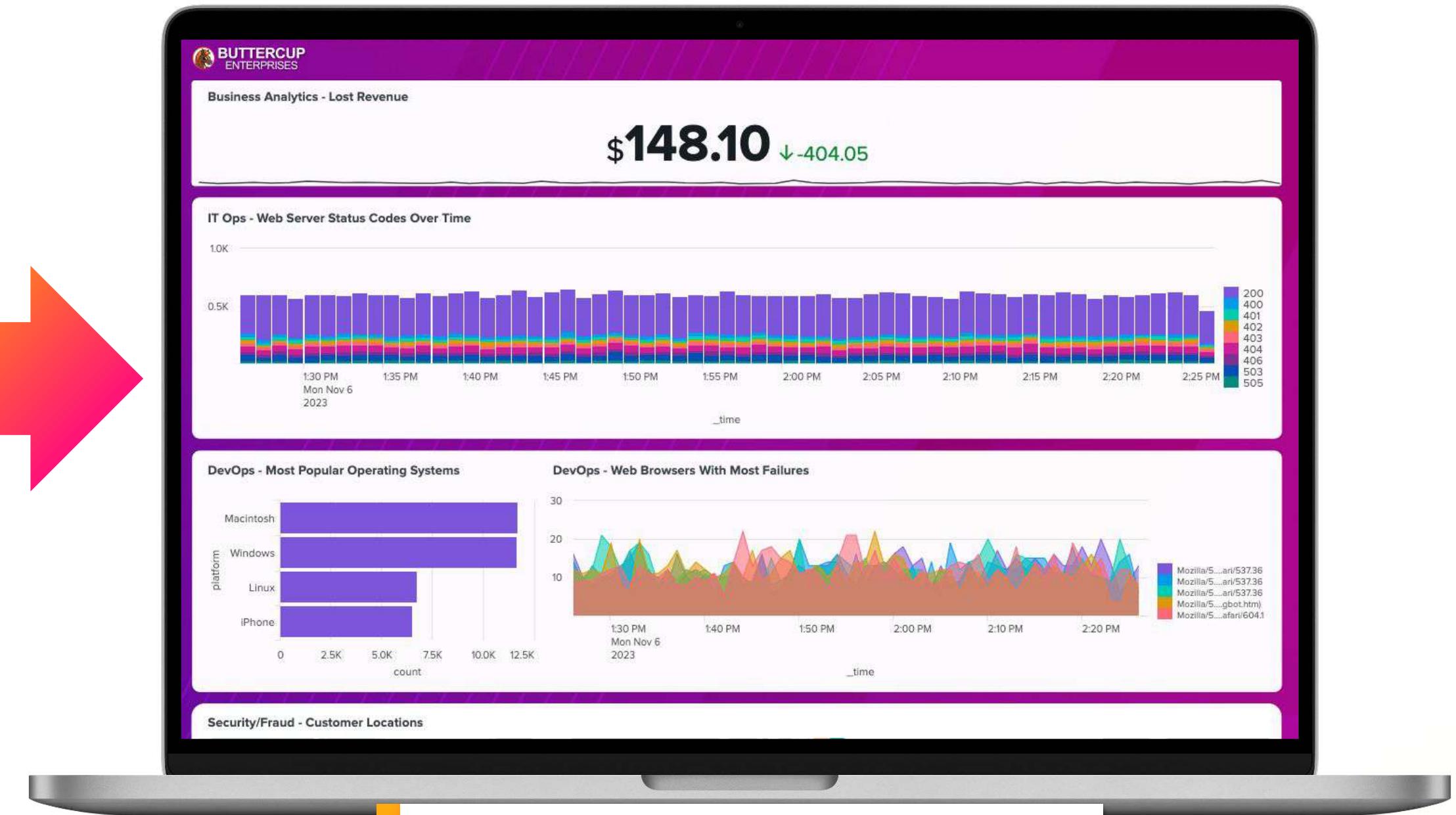
Report Acceleration
Common Information Model (CIM)
Containers
Best Practices
And much more...

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-CSX-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-CSX-Attendee>

Goal

Available Enrolled

Search events Invited

Private event

PLATFORM

01/16 (10:37) - 01/16 (18:29)
Europe/London (GMT +00:00)

Available

Enroll

Enroll in today's event



Data is your Competitive Advantage

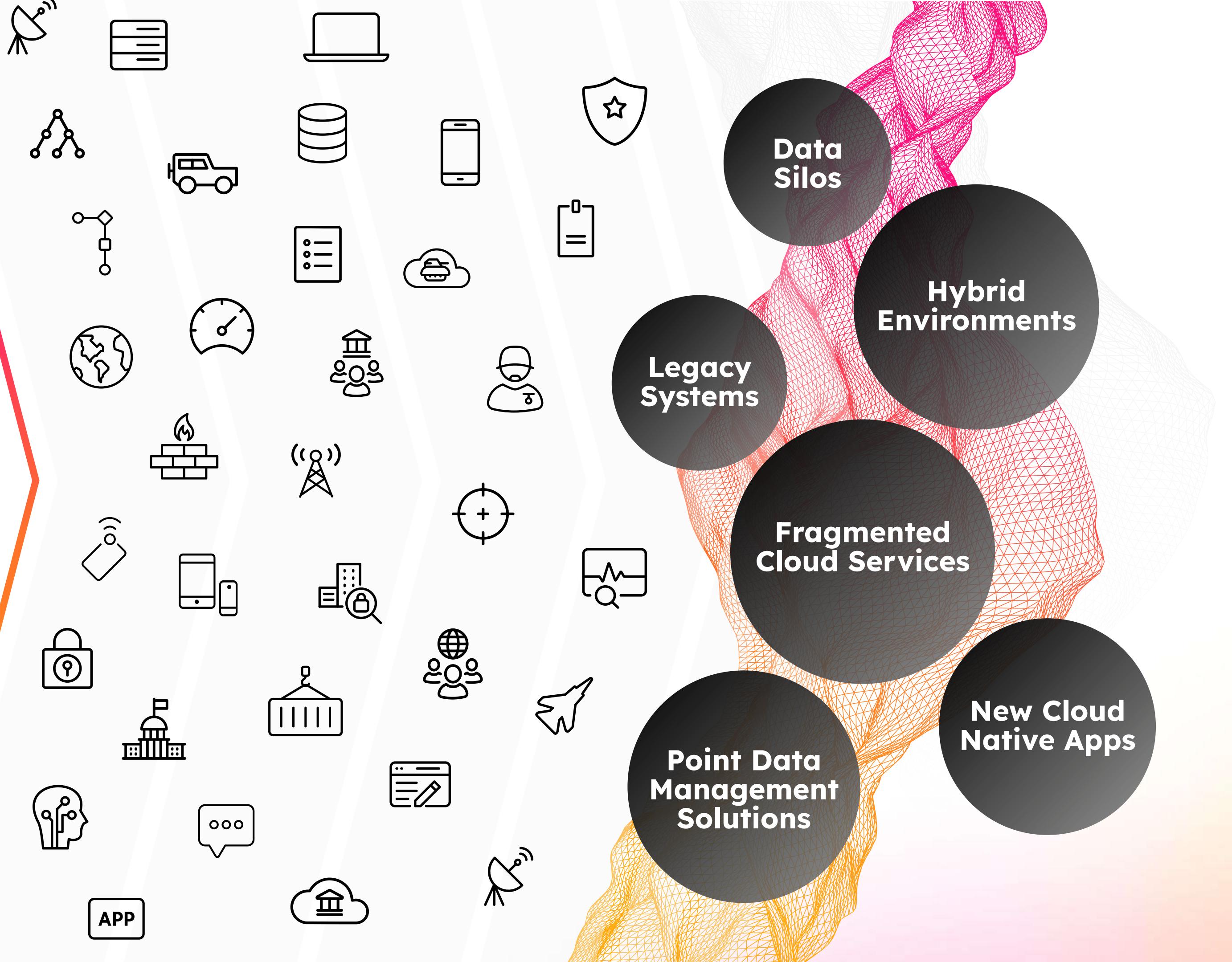
Data isn't just a record.
Data makes things happen.
Splunk makes it possible.



SPLUNK



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

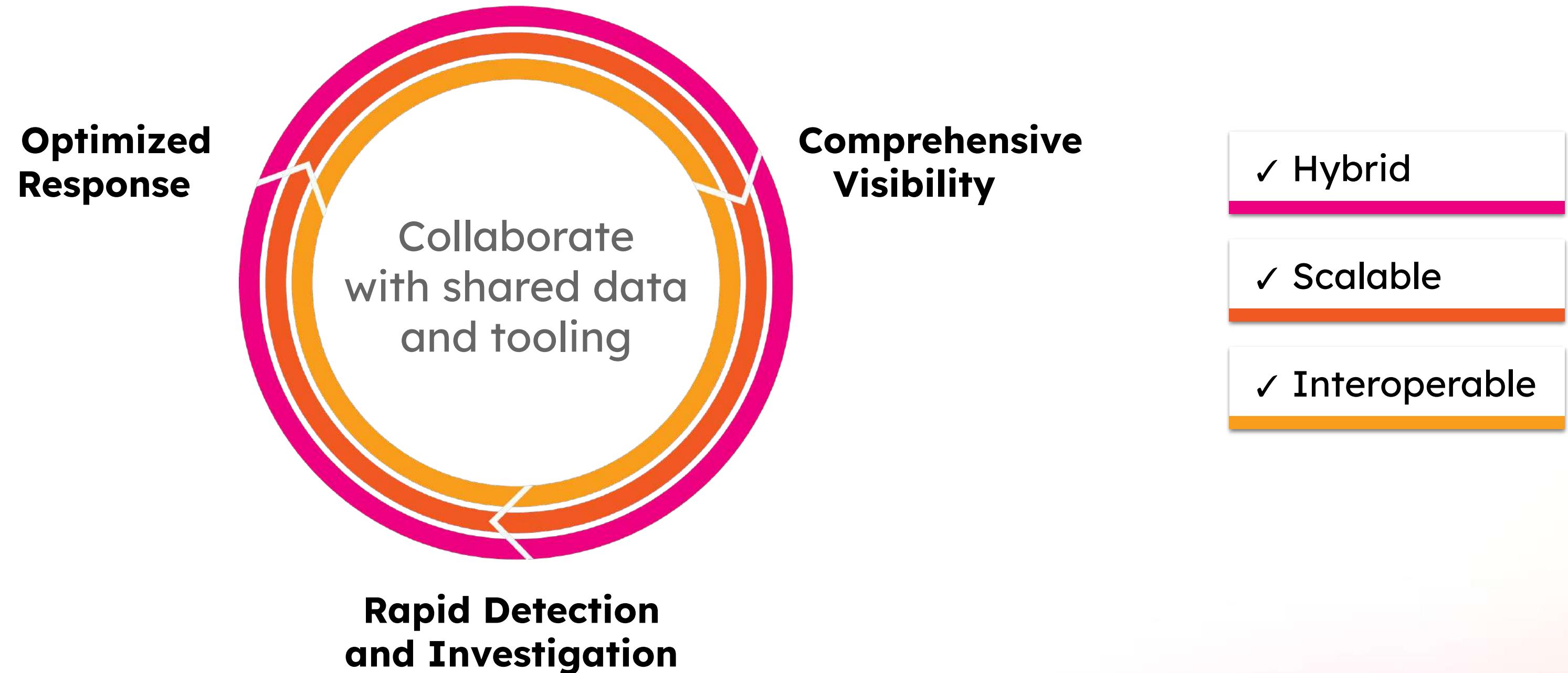
Act

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

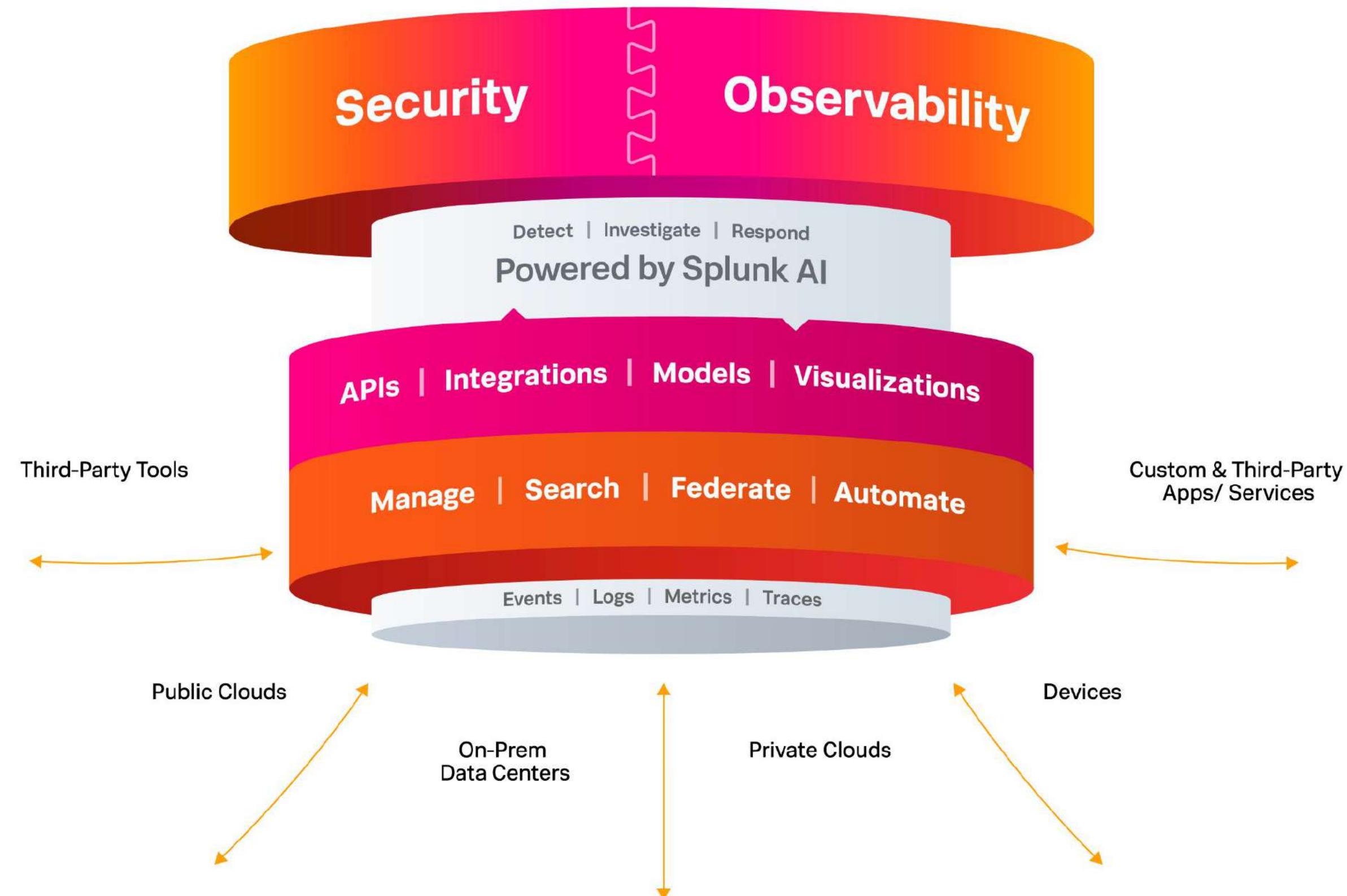
Extend

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

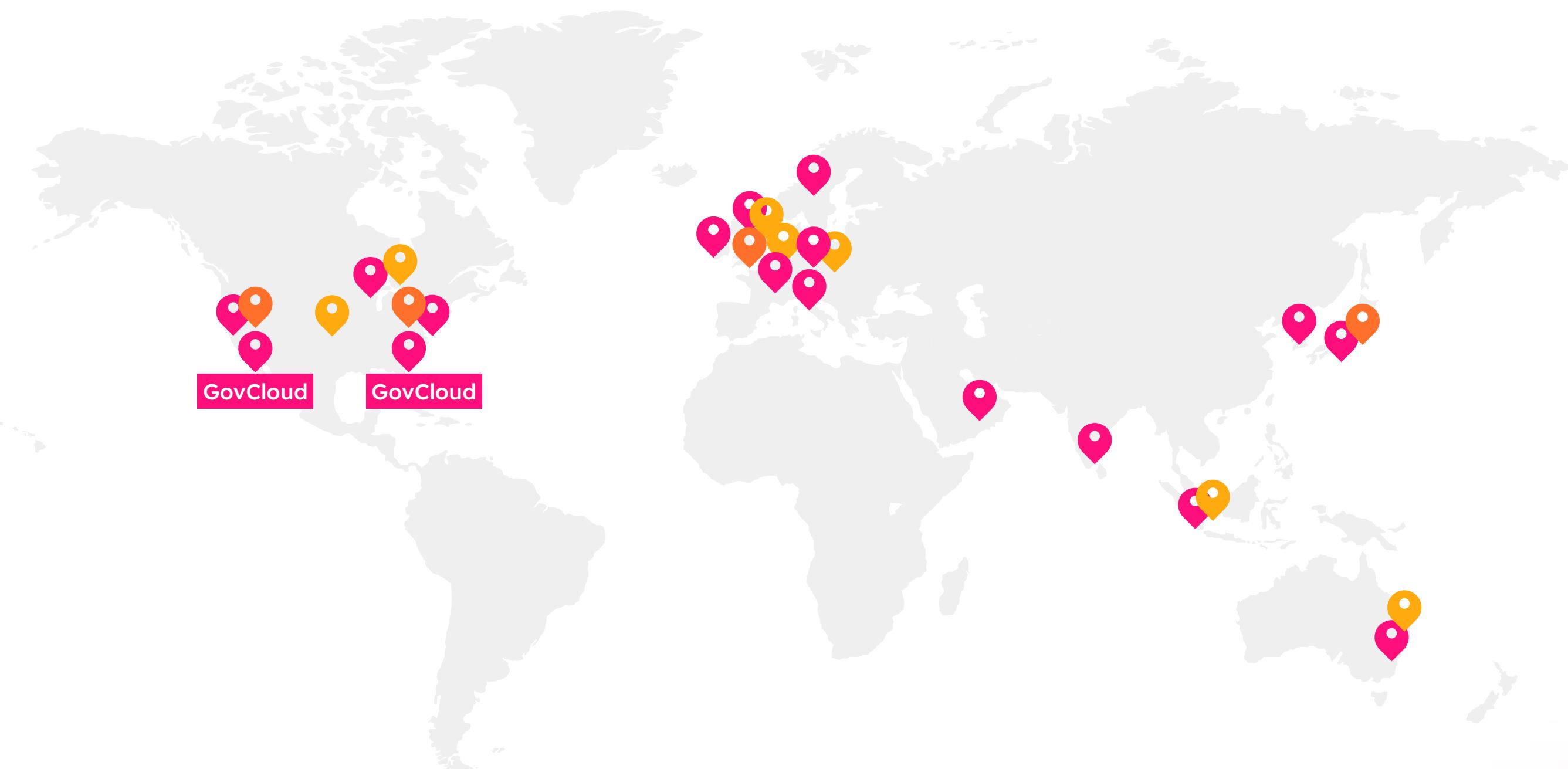
Splunk enables faster detection, investigation and response



The Unified Security and Observability Platform



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



15+



7

Google Cloud

4

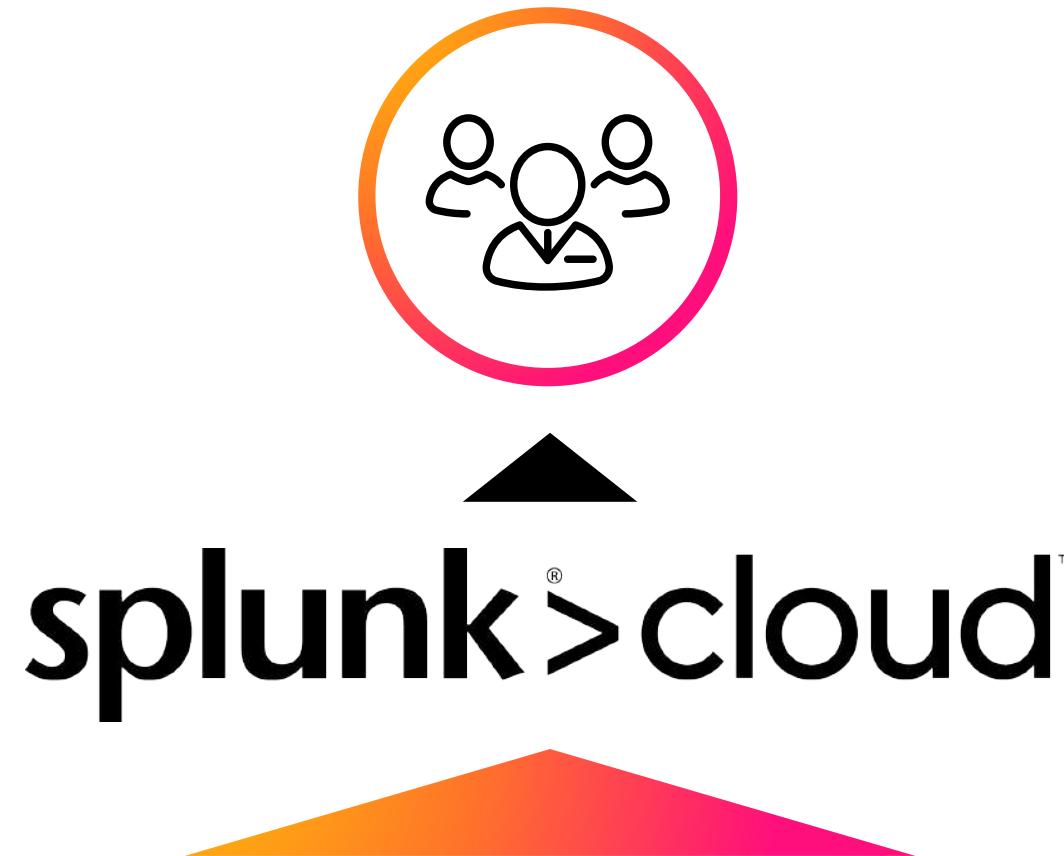
Microsoft
Azure

Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

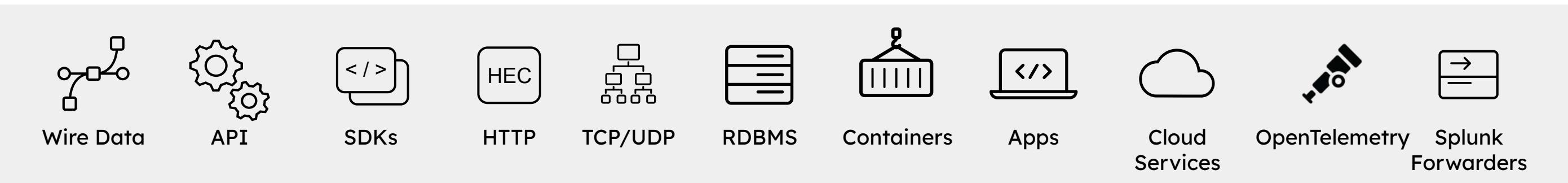
3 Simple Steps:

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**

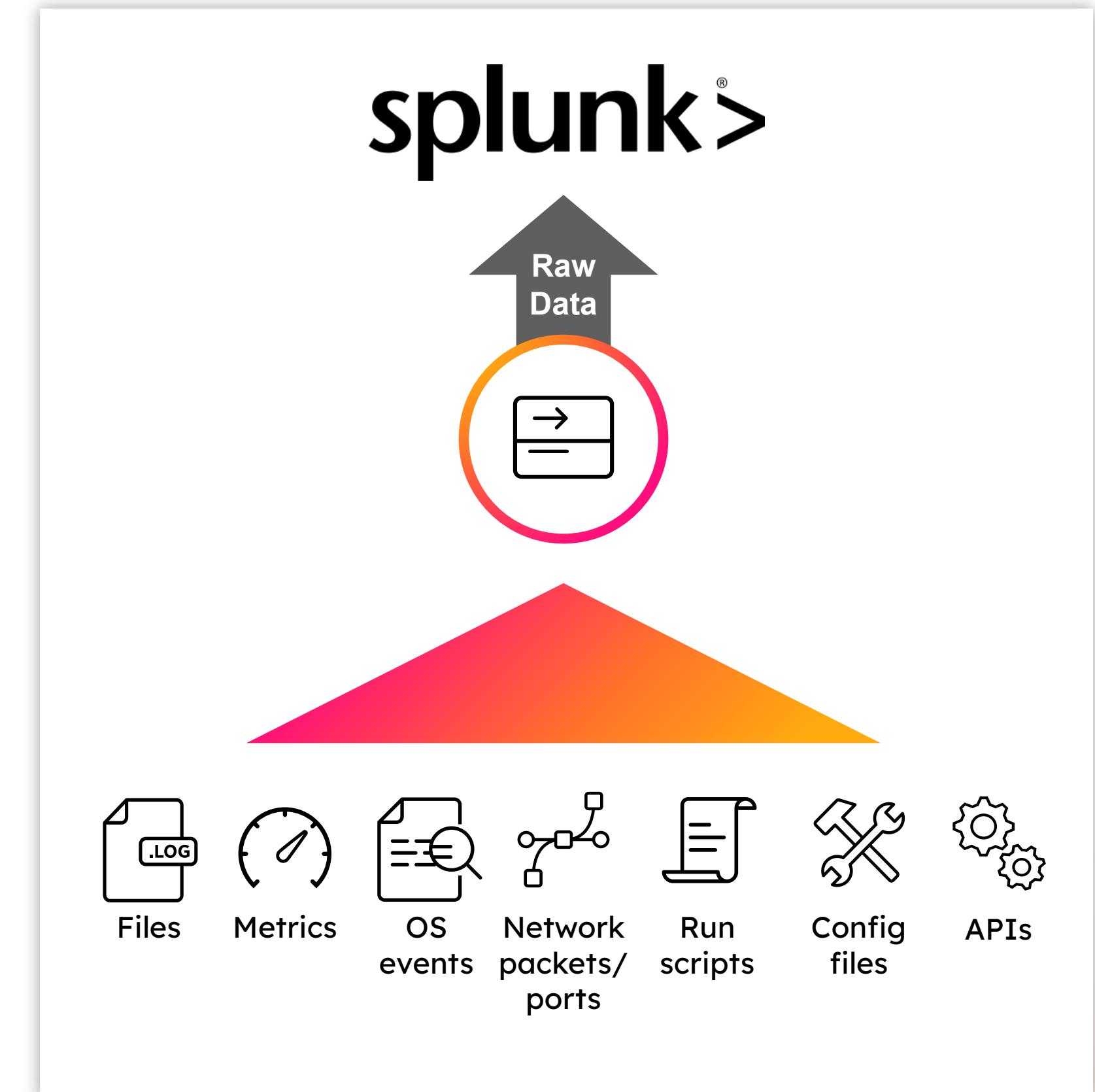
Flexible options for data collection and forwarding



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!

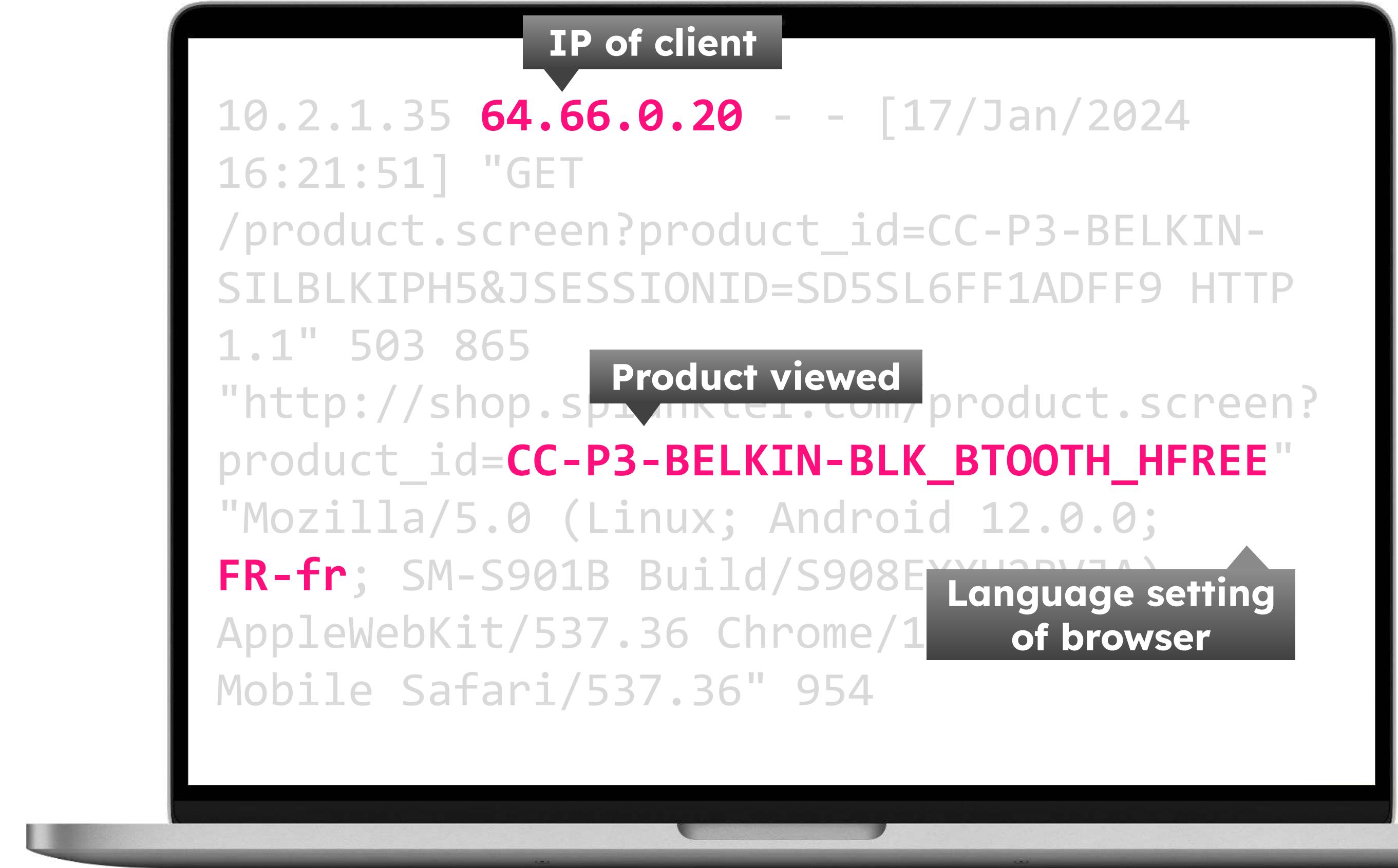


Machine data is valuable not complex!

```
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?

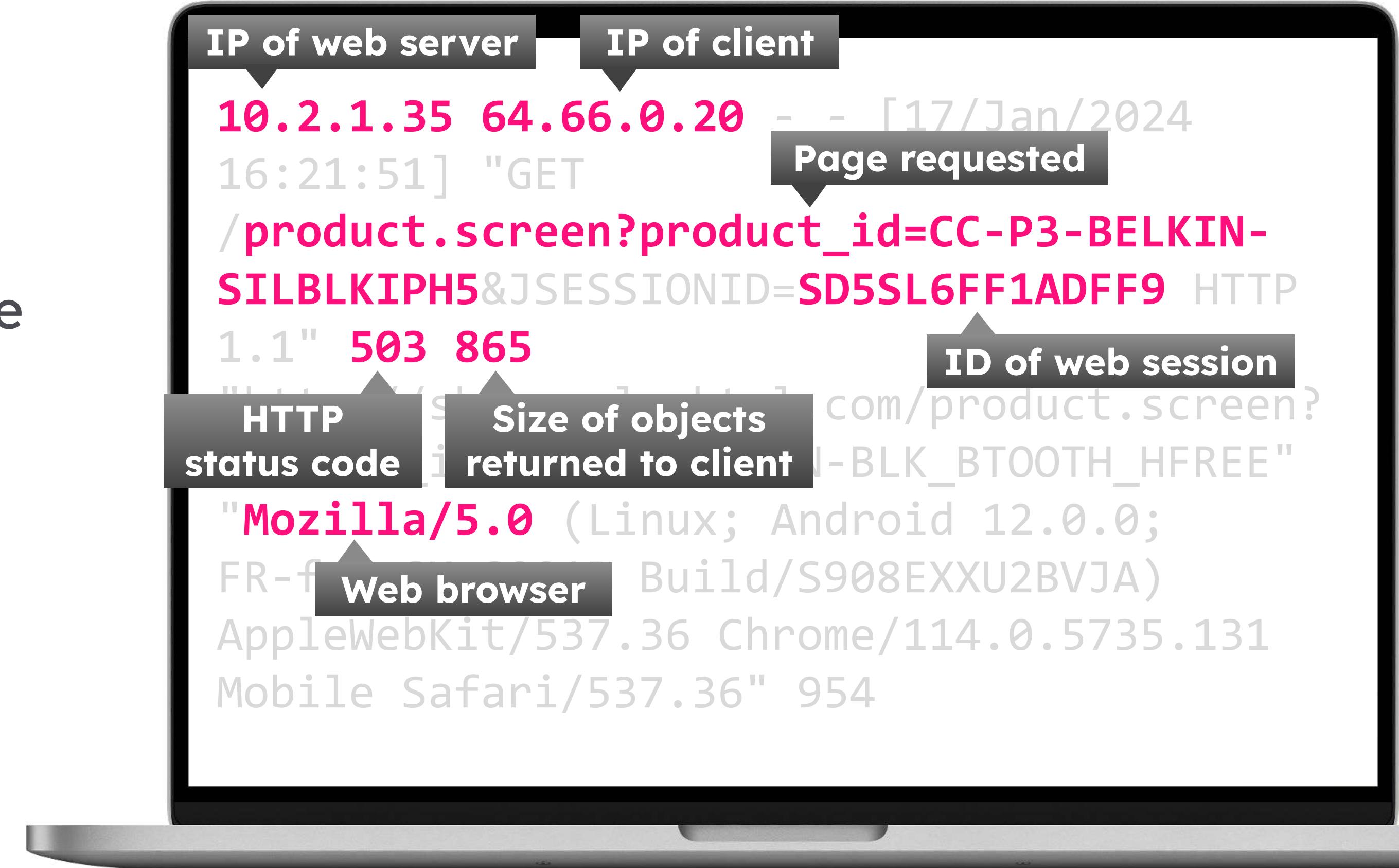
```
10.2.1.35 64.66.0.20 - - [17/Jan/2024  
16:21:51] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?  
product_id=CC-P3-BELKIN-BLUETOOTH_HFREE"  
"Mozilla/5.0 (Linux; Android 12.0.0;  
FR-fr; SM-S901B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

Platform

Handset model

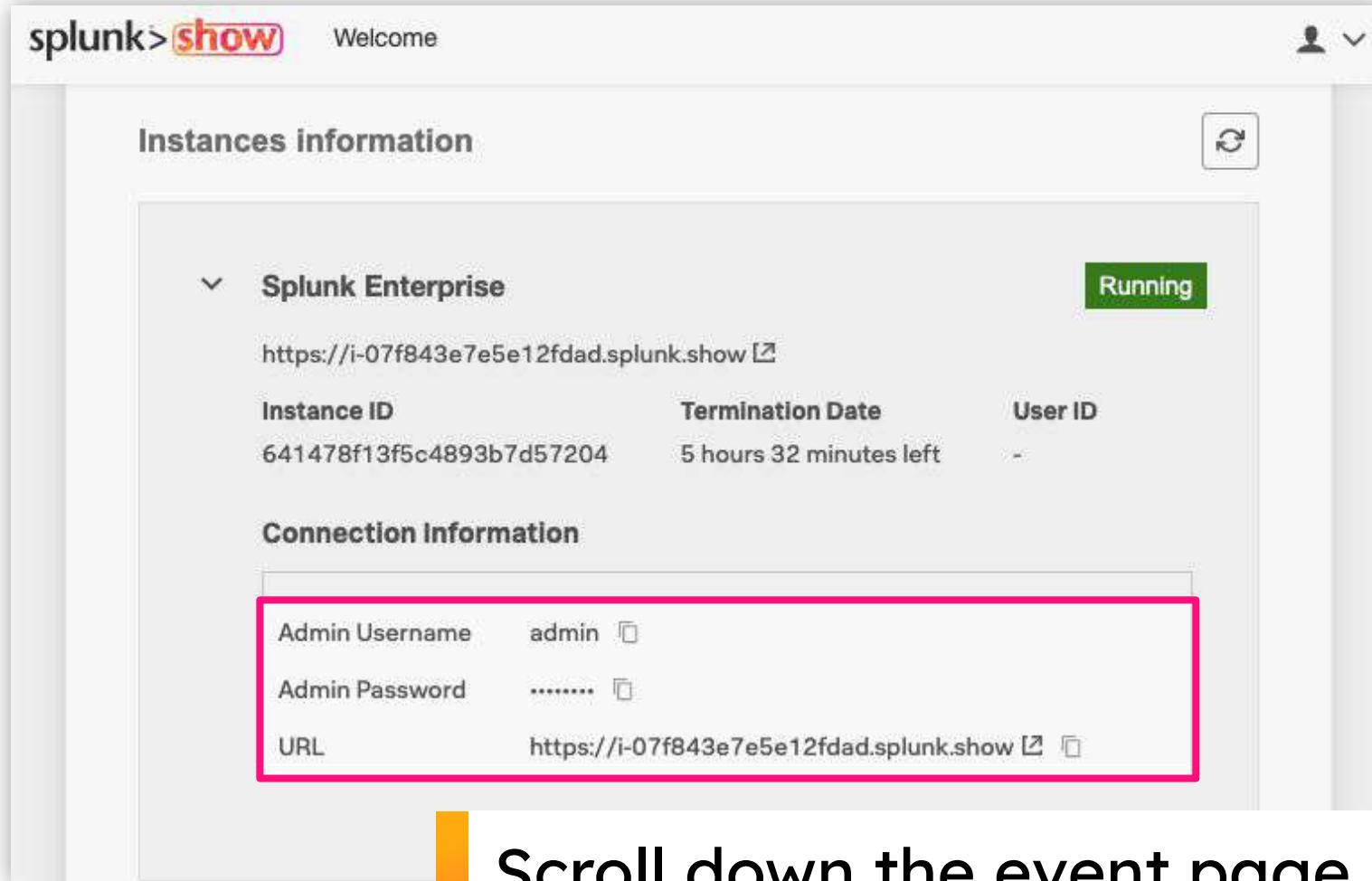
IT Ops Use Case

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
 - User ID: -
- 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 details:

- Header: splunk>enterprise
- Form fields: Username, Password, Sign In
- Background: A terminal window displaying log messages.

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 screenshot shows the Splunk Enterprise search interface. At the top, the navigation bar includes the 'splunk>enterprise' logo, a dropdown for 'App: Splunk 4 Rookies', and links for 'Administrator', 'Messages', and 'Settings'. Below the navigation is a 'New Search' bar with a search bar containing 'action=purchase status=200', a results count of '261 events (15/05/2018 07:49:00.000 to 15/05/2018 08:49:00.000)', and a time picker set to 'Last 60 minutes'. The main search area displays an 'Event histogram' showing event counts over time, with a note '1 minute per column'. Below the histogram is a table of raw event data. The table has columns for 'Time' and 'Event'. The first event is: '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'. The second event is: '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'. The third event is: '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/5.0.375.3 8 Safari/533.4" 897 host = ip-172-31-31-62 | source = /var/log/weblogs/noise_apache_1.log | sourcetype = access_combined'. The bottom left of the search interface lists 'INTERESTING FIELDS' including 'action', '# bytes 100+', 'category_id 5', 'clientip 52', 'date_hour 2', 'date_mday 1', 'date_minute 60', 'date_month 1', 'date_second 60', and 'date_time 1'. Annotations with arrows point to various parts of the interface:

- 'The currently selected app' points to the 'App: Splunk 4 Rookies' dropdown.
- 'Time picker - choose your search time range' points to the time picker at the top right.
- 'Search bar - type anything here to search' points to the search bar in the 'New Search' bar.
- 'Event histogram' points to the histogram visualization.
- 'Event timestamp' points to the timestamp column in the event table.
- 'Raw event data' points to the event table.
- 'Metadata fields extracted at search time' points to the list of interesting fields on the left.

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"
```

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=SD6SL6FF10ADCF3 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/A546BXXU1AWE7) 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	131.178.33.243 - - [16/Jan/2024 11:03:08] "POST /product.screen?uid=5ac99574-edc7-417d-ad38-df91f883d280&product_id=PP-&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	12.130.60.1 - - [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_1 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

Commands

Functions

```
| stats count by status
```

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>

Generative
Commands

Fields : UC v Ic

Transformative
Commands

More Interesting Searches

A teaser to show a quick showing of some more interesting searches that do a bit more

- Difference in statistical usage and display
- Different ways to filter or search

Interesting Searches - 1

Differences between statistics call behavior and display

```
index=main  
sourcetype=access_combined  
action=purchase  
| stats count by status, useragent
```

status	useragent	count
200	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)	367
200	Mozilla/5.0 (Linux; Android 12.0.0; SM-S901B Build/S908EXXU2BVJA) AppleWebKit/537.36 Chrome/114.0.5735.131 Mobile Safari/537.36	381
200	Mozilla/5.0 (Linux; Android 13.0.0; Pixel Build/TQ1A.230205.001.D2) AppleWebKit/537.36 Chrome/100.0.4896.127 Mobile Safari/537.36	393

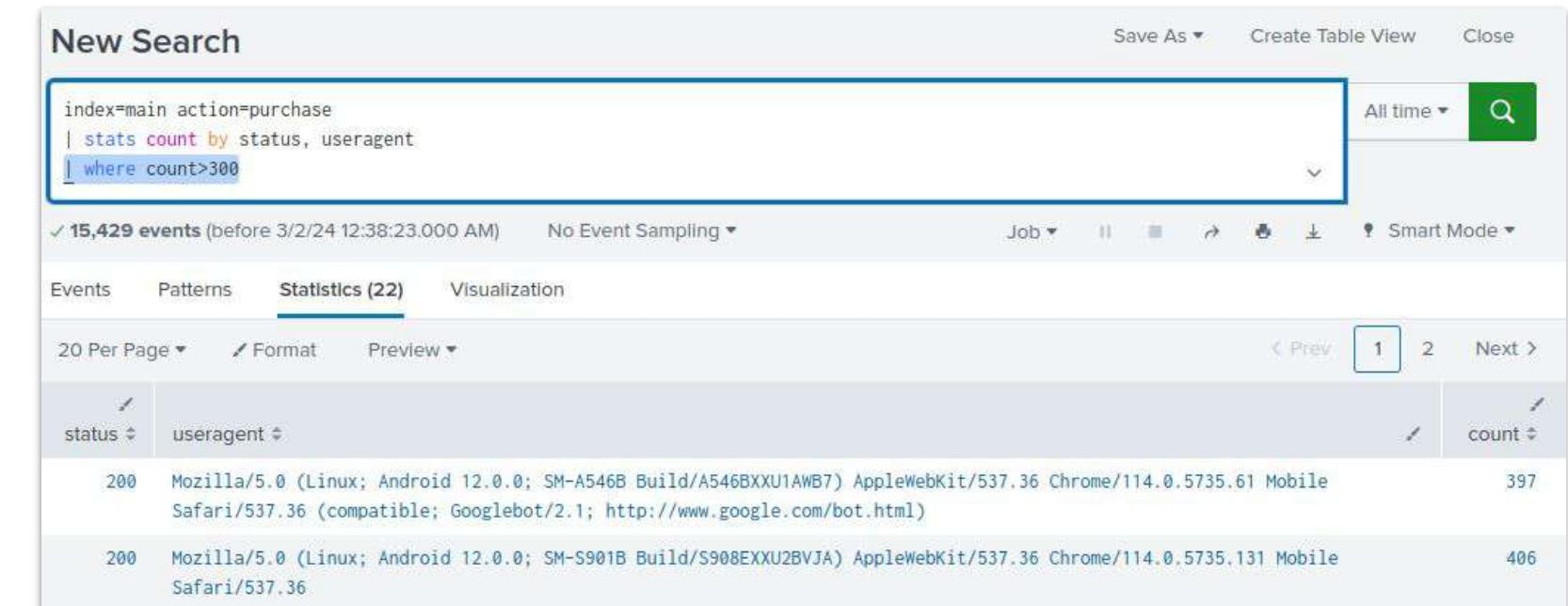
```
index=main  
sourcetype=access_combined  
action=purchase  
| stats count by status,  
useragent  
| stats list(status) by useragent
```

useragent	list(status)
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)	200 400 401 402 403 404 406 503 505
Mozilla/5.0 (Linux; Android 12.0.0; SM-S901B Build/S908EXXU2BVJA) AppleWebKit/537.36 Chrome/114.0.5735.131 Mobile Safari/537.36	200 400 401 402 403 404 406 503 505

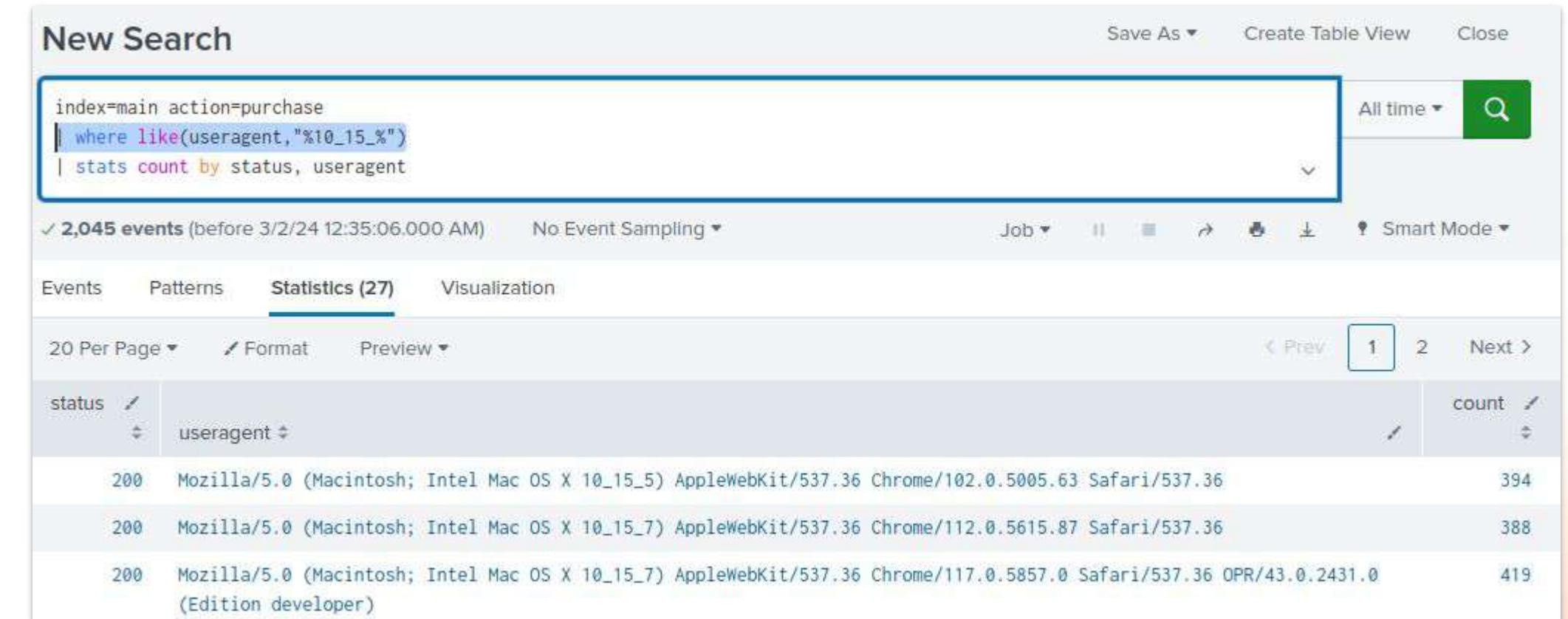
Interesting Searches - 2

Differences between filter/search behavior

```
index=main action=purchase  
| stats count by status, useragent  
| where count > 300
```



```
index=main action=purchase  
| where like(useragent,"%10_1%_%")  
| stats list(useragent) by status
```



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**



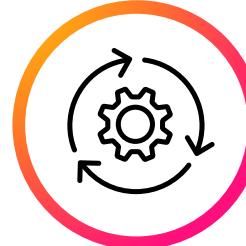
**BUTTERCUP
ENTERPRISES**

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



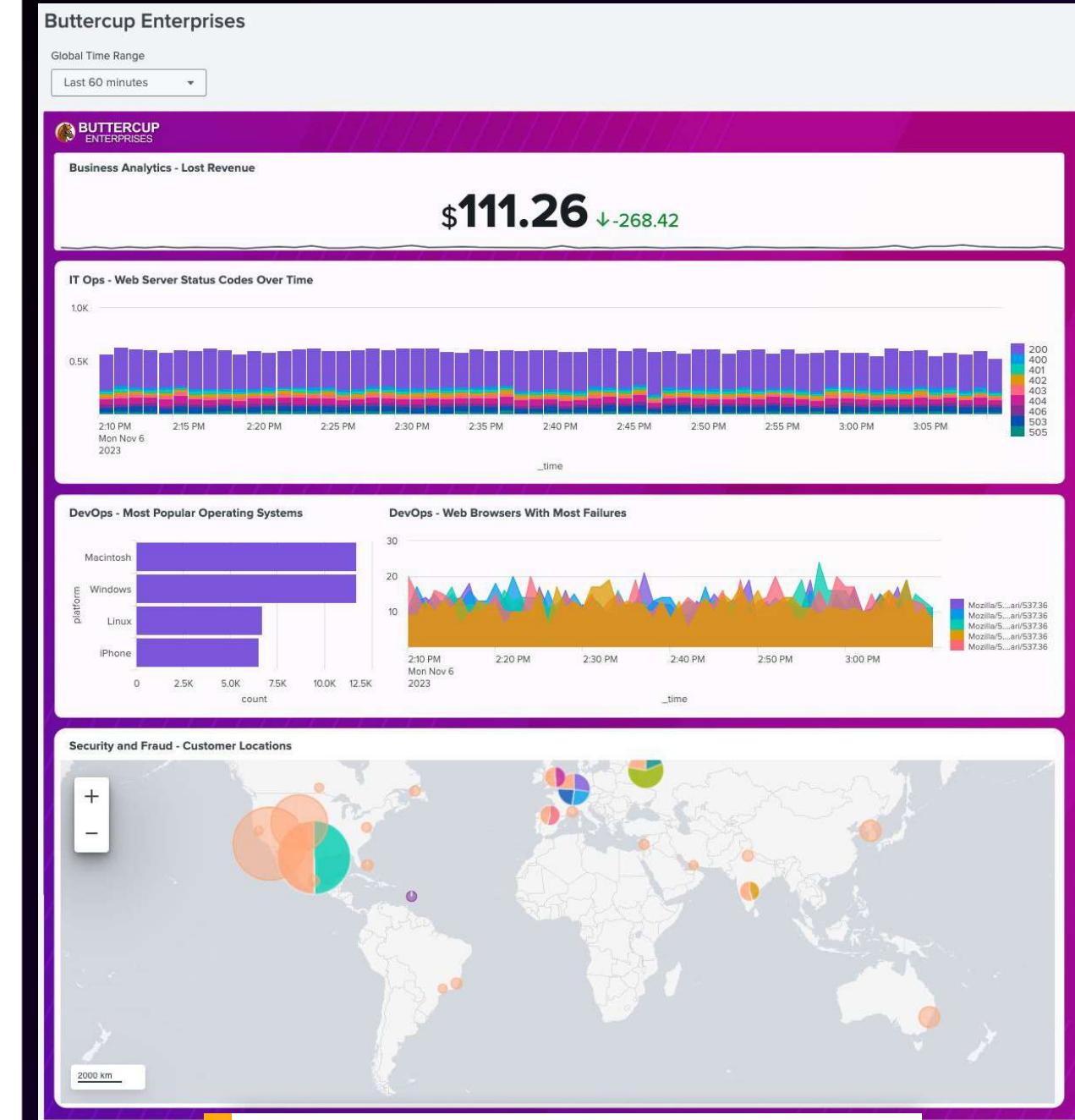
Business Analytics team: Show lost revenue from the Buttercup Enterprises website



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!



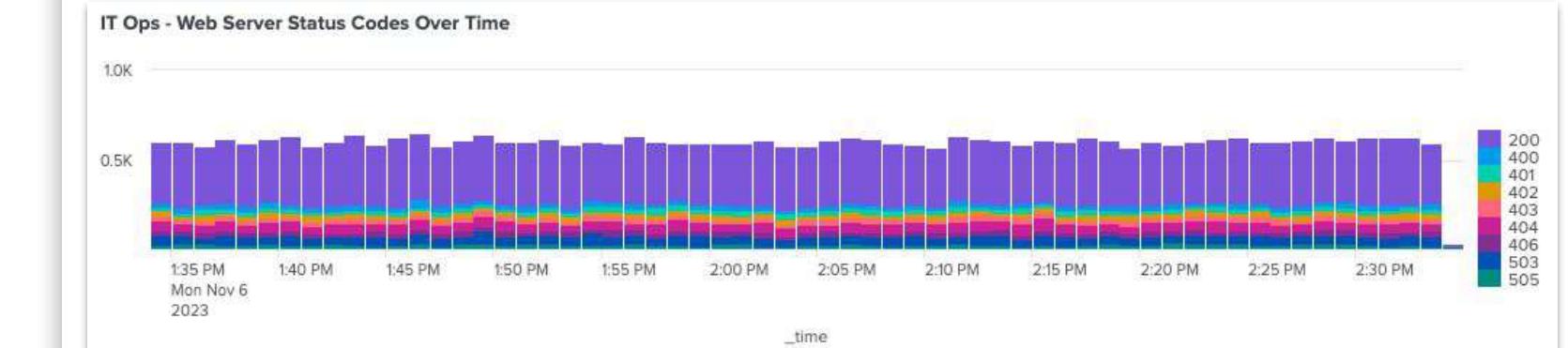
IT Operations Team

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**

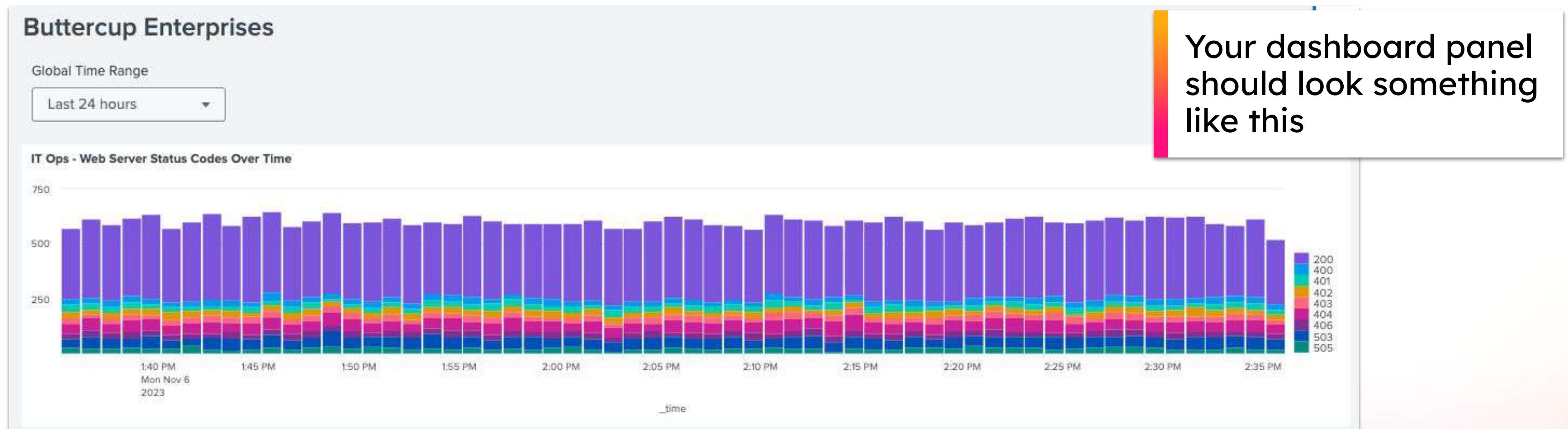


IT Operations Team

Investigate successful versus unsuccessful web server requests over time

Solution:

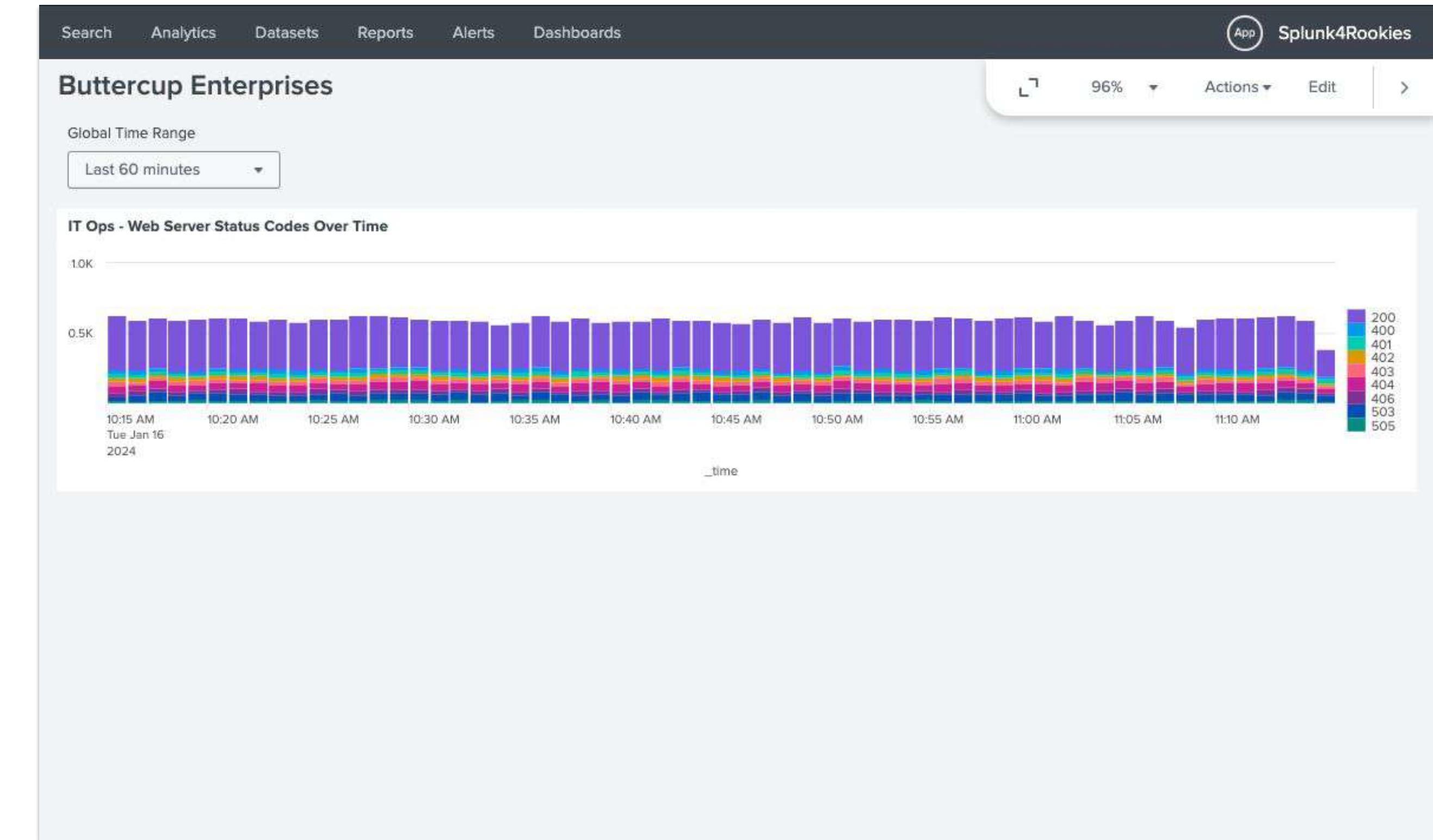
```
index=main sourcetype=access_combined | timechart count by status limit=10
```



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, revealing more details. A red box highlights the 'Event Actions' button in the bottom right corner of the expanded event area.

2. Click on Event Actions

3. Click on Extract Fields

A screenshot of the Splunk interface showing the 'Regular Expression' section. It displays a green placeholder '(.*?)' in a text input field. Below it, a note states: 'Splunk Enterprise will extract fields using a Regular Expression.'

4. Click on Regular Expression

A screenshot of the 'Select Fields' step in the 'Extract Fields' wizard. The wizard has four steps: 'Select Method' (green dot), 'Select Fields' (white dot), 'Validate' (white dot), and 'Save' (white dot). A red box highlights the 'Next >' button. The main area shows a sample event with several fields. A red box highlights the word 'Macintosh' in the 'platform' field. Below the event, there's a form to define the new field: 'Field Name' is set to 'platform', 'Sample Value' is 'Macintosh', and a 'Add Extraction' button is visible.

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](#)

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

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

5. Click Next



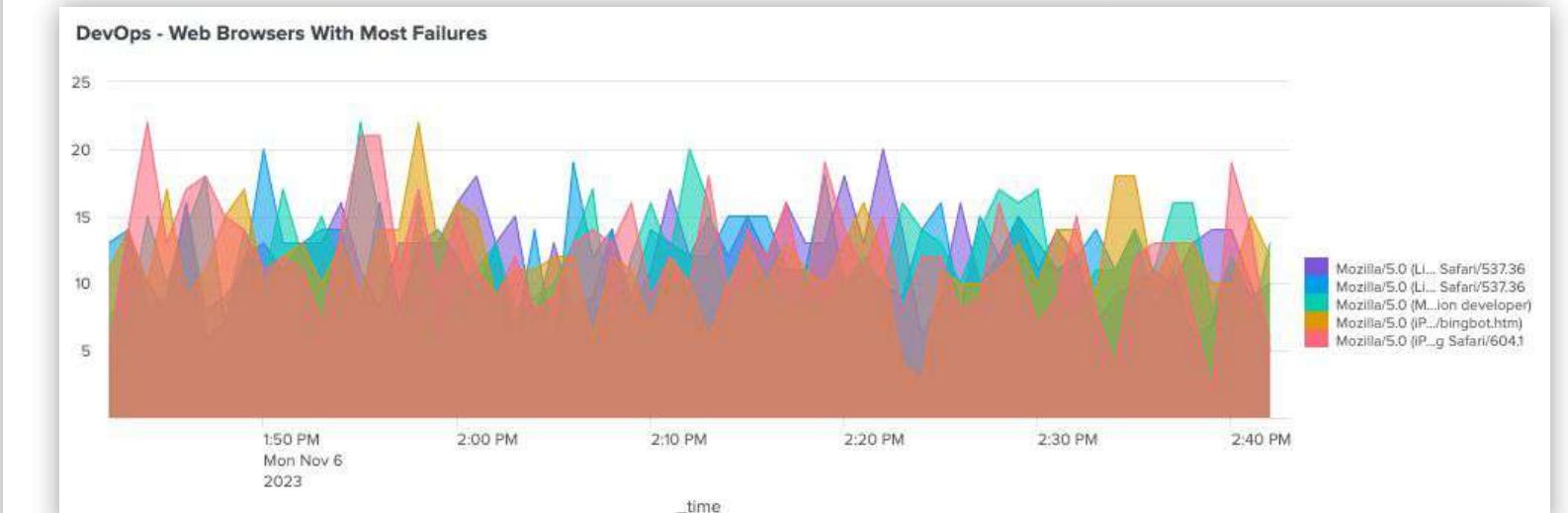
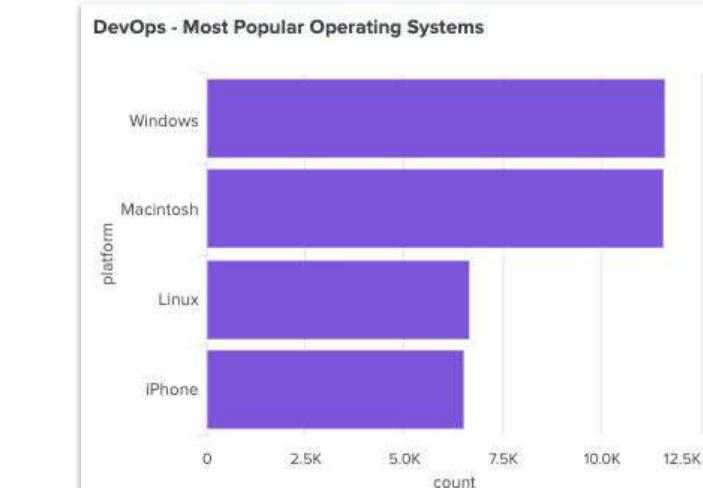
DevOps Team

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

God





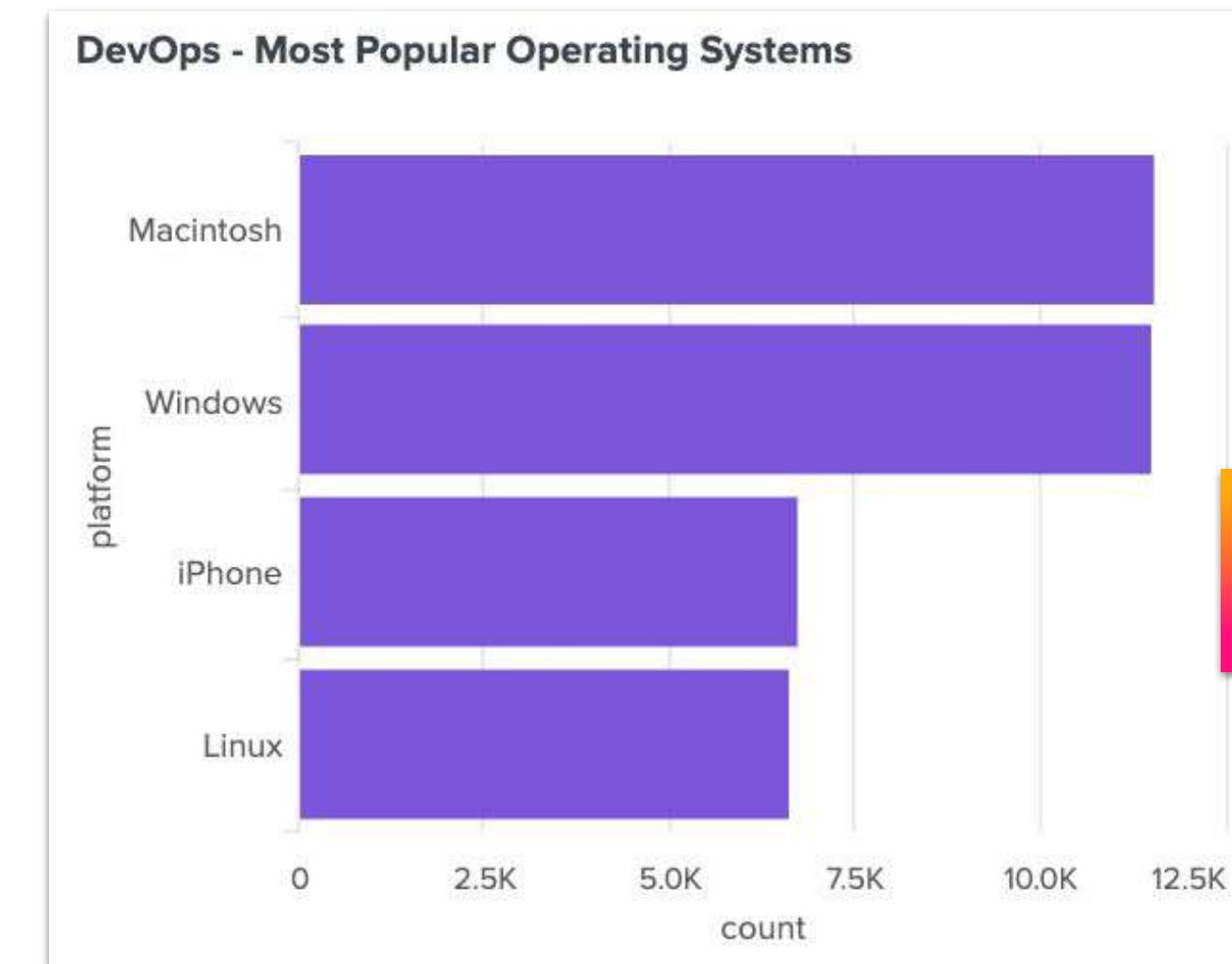
LAB EXERCISE 4

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!



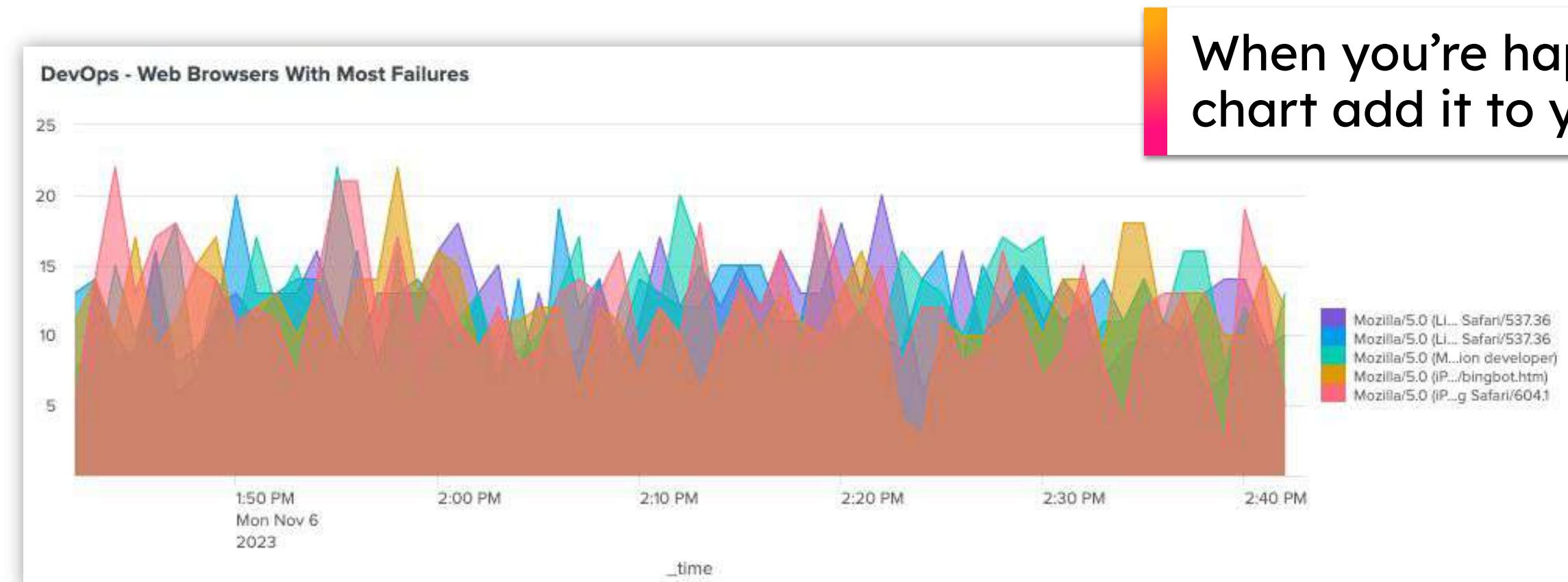
LAB EXERCISE 4

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
```



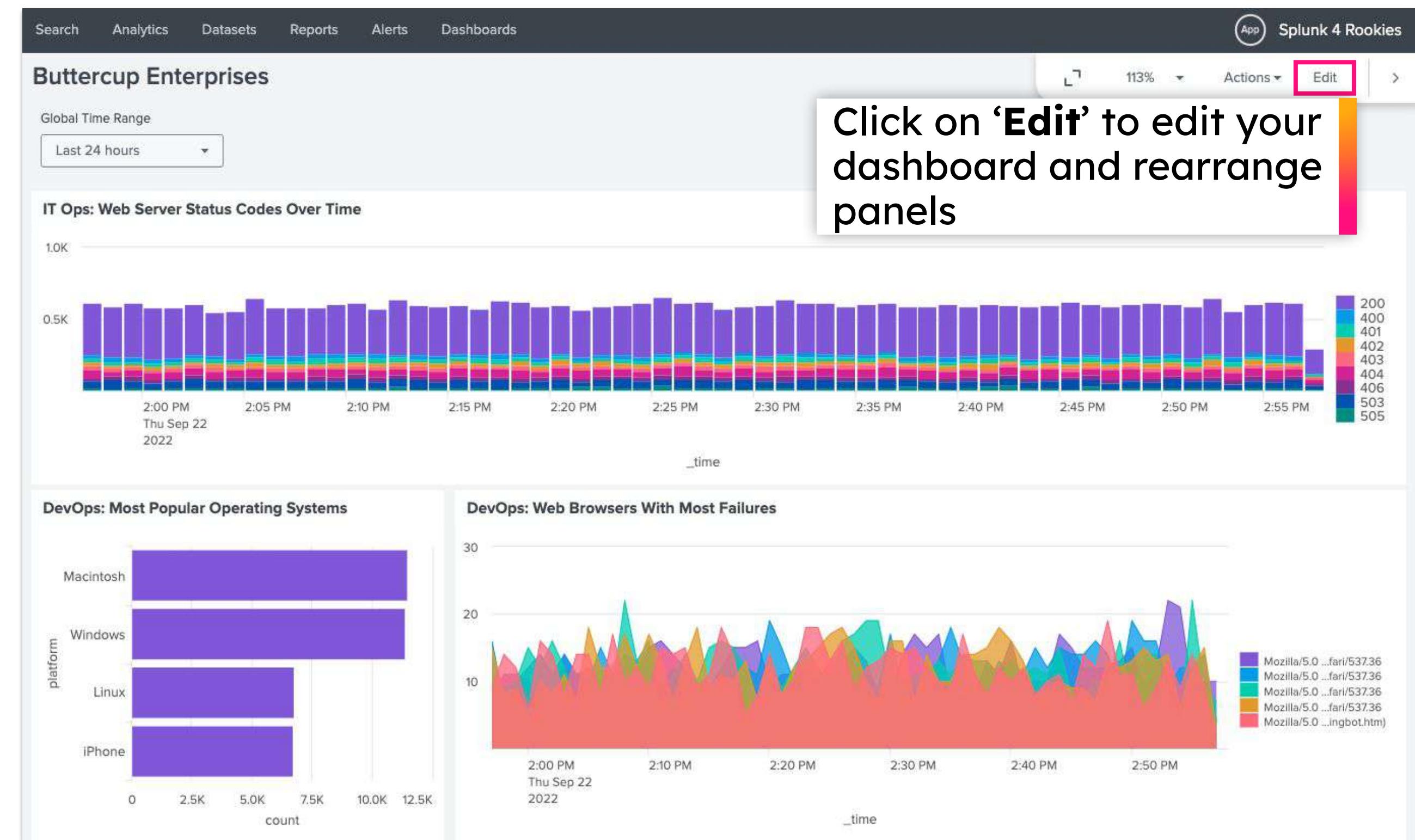
Your dashboard so far...



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>
```

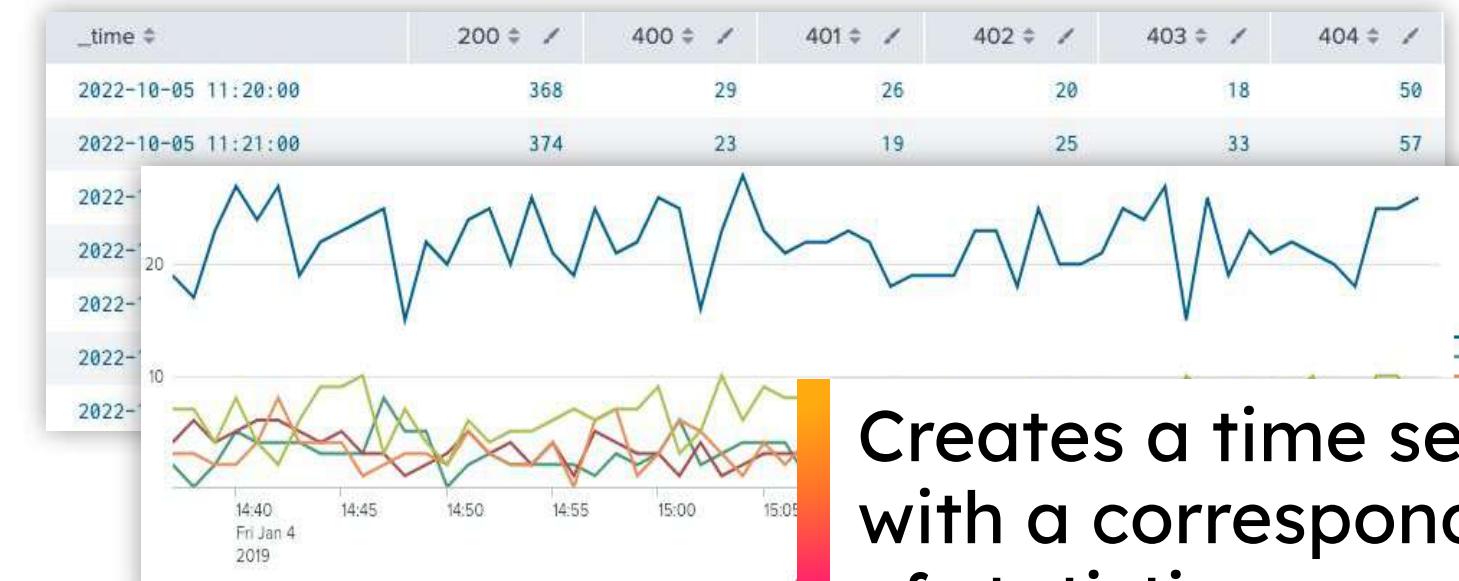
Examples:

```
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!

The screenshot shows the Splunk Settings interface. At the top, there are links for Administrator, Messages, Settings (which is highlighted with a red box), Activity, and Help. Below this, there's a sidebar with options like Add Data, Data models, Event types, Tags, Fields, and Lookups (which is also highlighted with a red box). The main content area is titled "Lookups" and contains the sub-section "Create and configure lookups".

1. Click on **Settings**

2. Click on **Lookups**

This screenshot shows the "Lookups" page with the sub-section "Lookup table files". It displays a list of existing lookup tables or a placeholder for uploading a new file. The "Lookup table files" link is highlighted with a red box.

3. Click on **Lookup table files**

This screenshot shows the "Lookup table files" list page. The title is "Lookup table files" and the subtitle is "Lookups > Lookup table files". It shows five items listed under "Showing 1-5 of 5 items". The paths of the files are listed as follows:

- /opt/splunk/etc/apps/search/lookups/geo_attr_countries.csv
- /opt/splunk/etc/apps/search/lookups/geo_attr_us_states.csv
- /opt/splunk/etc/apps/search/lookups/geo_attr_us_cities.csv
- /opt/splunk/etc/apps/search/lookups/geo_attr_ip.csv
- /opt/splunk/etc/apps/search/lookups/product_codes.csv

4. Check for **product_codes.csv**

Enriching Data with the `lookup` Command

Usage:

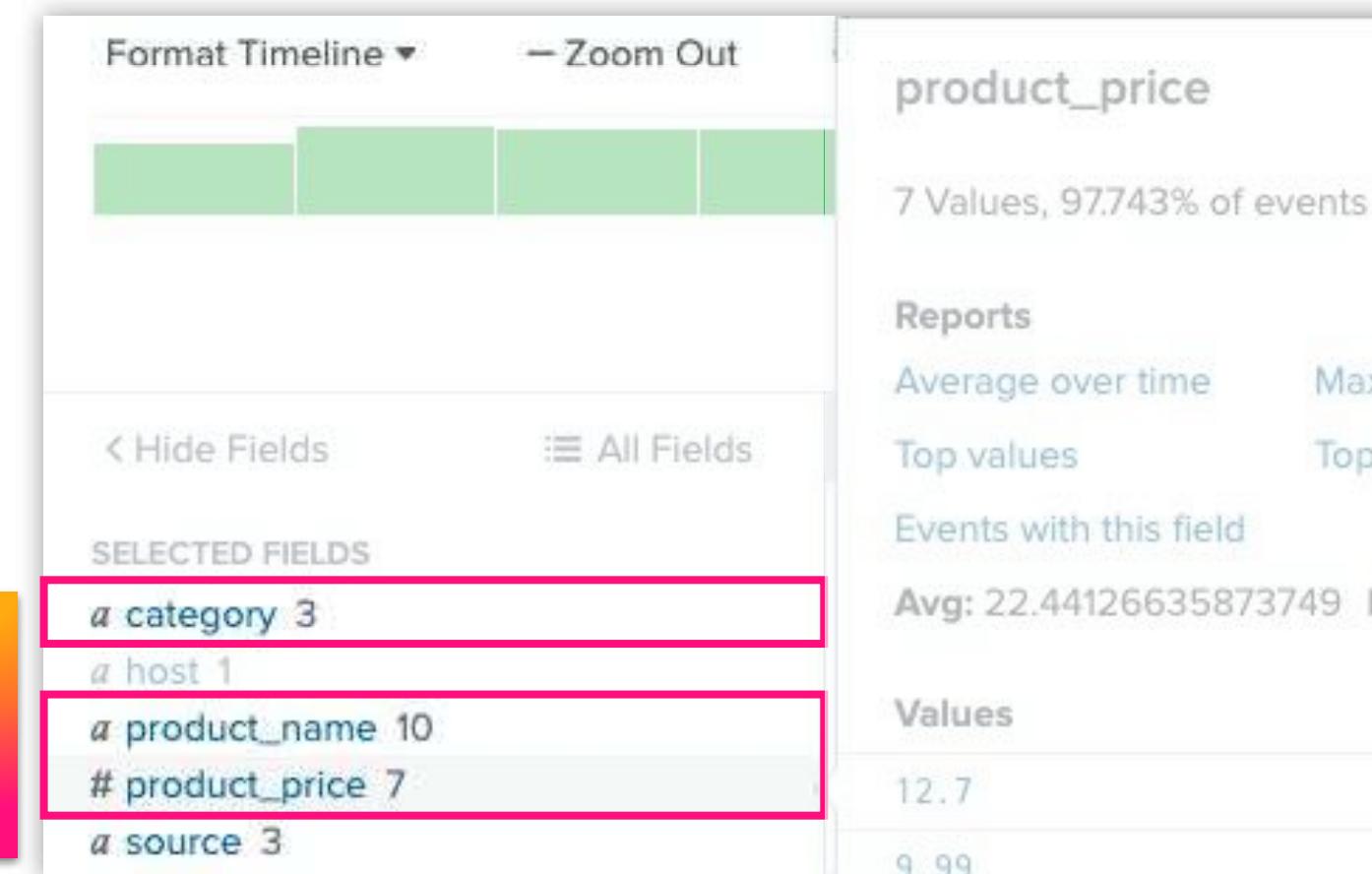
```
<your search> | lookup product_codes.csv product_id
```

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

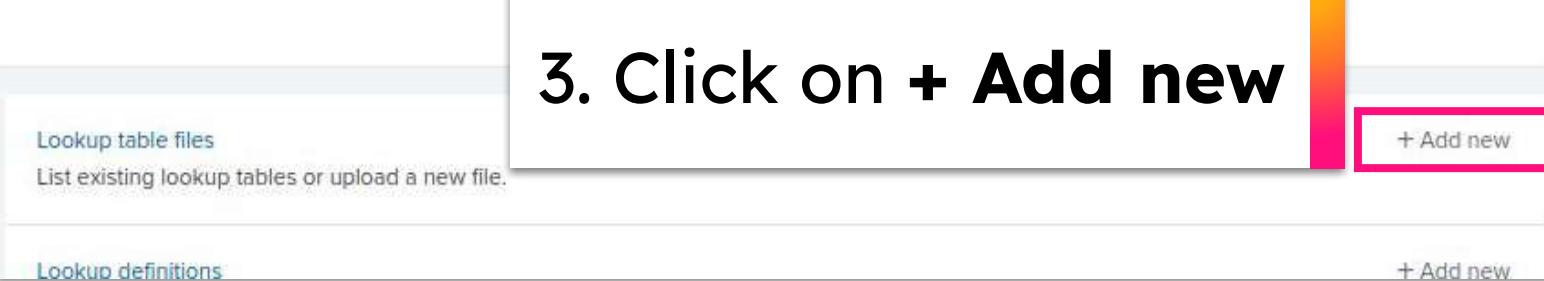
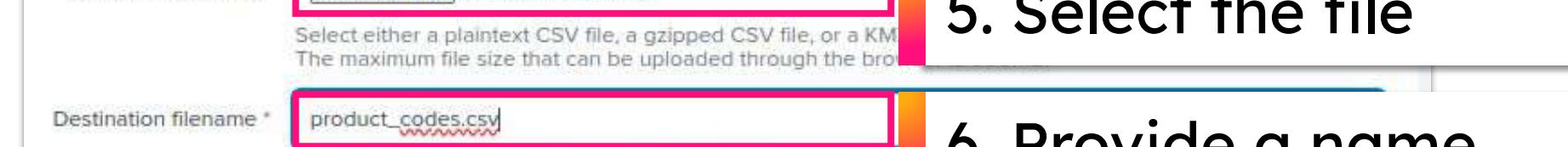
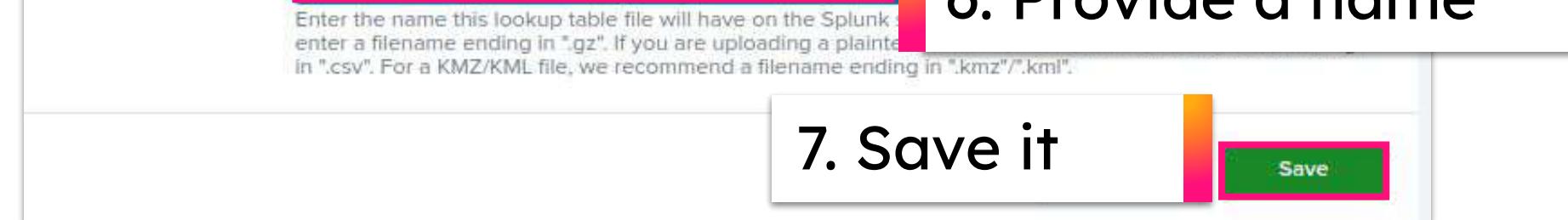
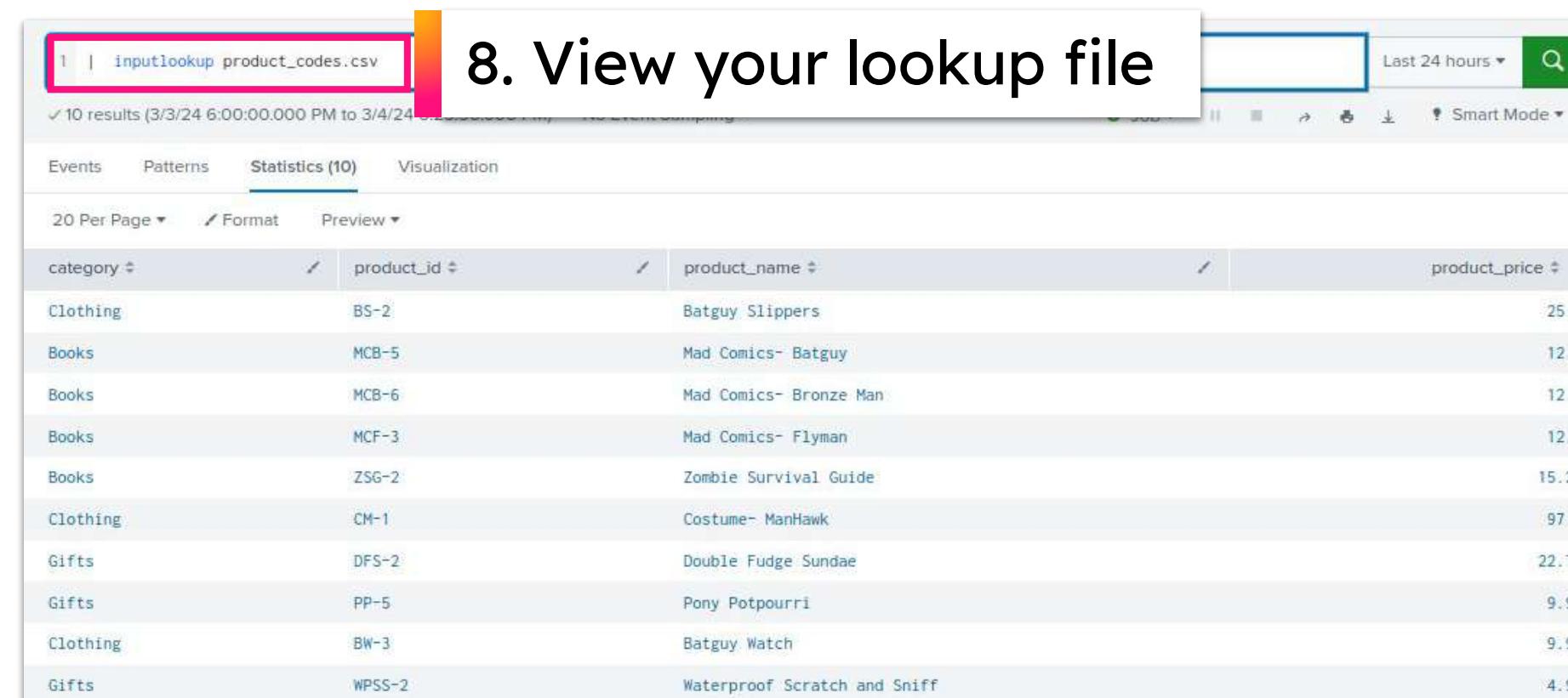
Goal

Business Analytics - Lost Revenue

\$35.69 ↓ -199.03



How to Create a Lookup File

1. Click on **Settings**
2. Click on **Lookups**
3. Click on **+ Add new**
4. Select the context
5. Select the file
6. Provide a name
7. Save it
8. View your lookup file

category	product_id	product_name	product_price
Clothing	BS-2	Batguy Slippers	25.7
Books	MCB-5	Mad Comics- Batguy	12.7
Books	MCB-6	Mad Comics- Bronze Man	12.7
Books	MCF-3	Mad Comics- Flyman	12.7
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



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...



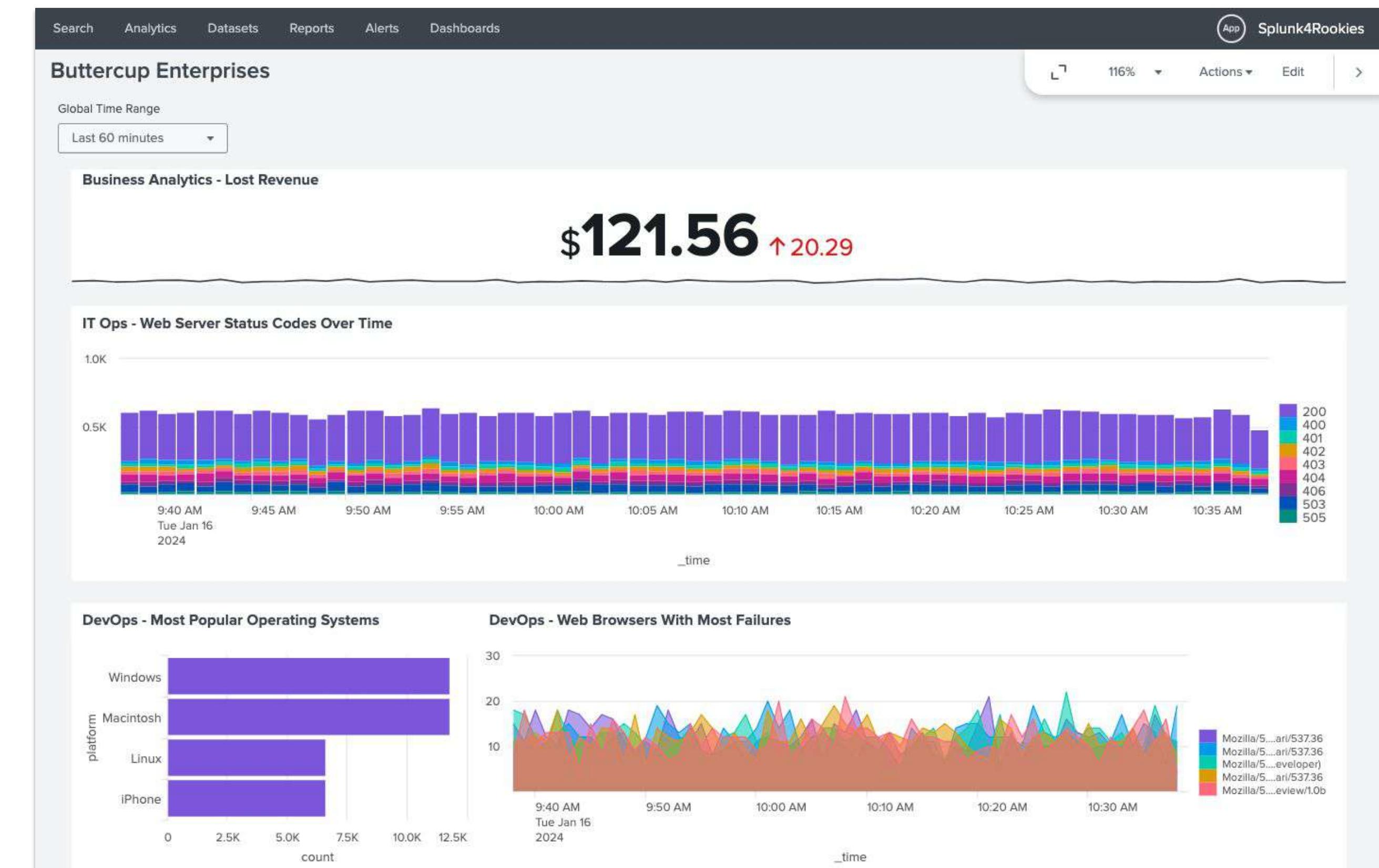
IT Operations team ✓



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

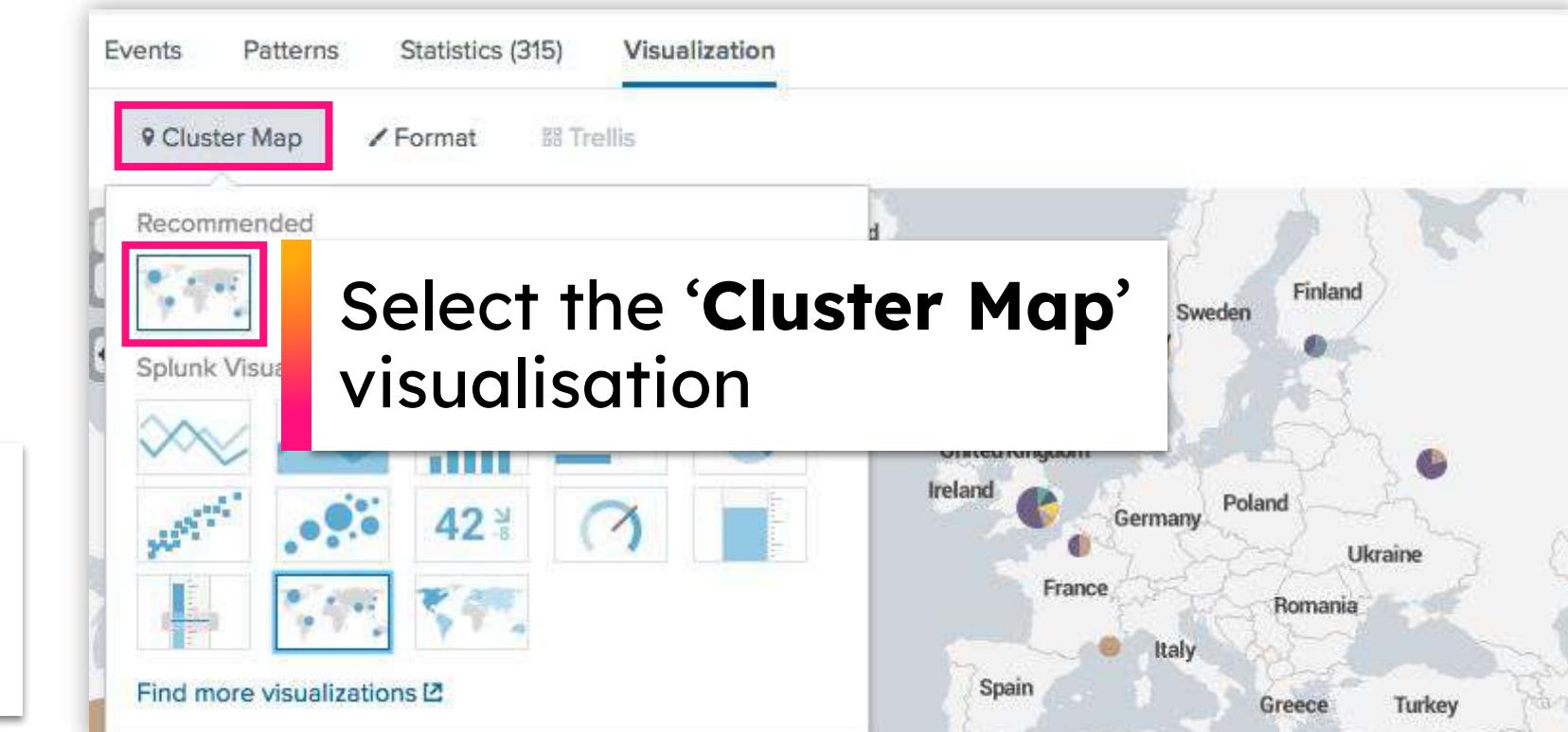
Split your results by a specific field for more detailed analysis

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

Enriches IP data on-the-fly with location data

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 ✓



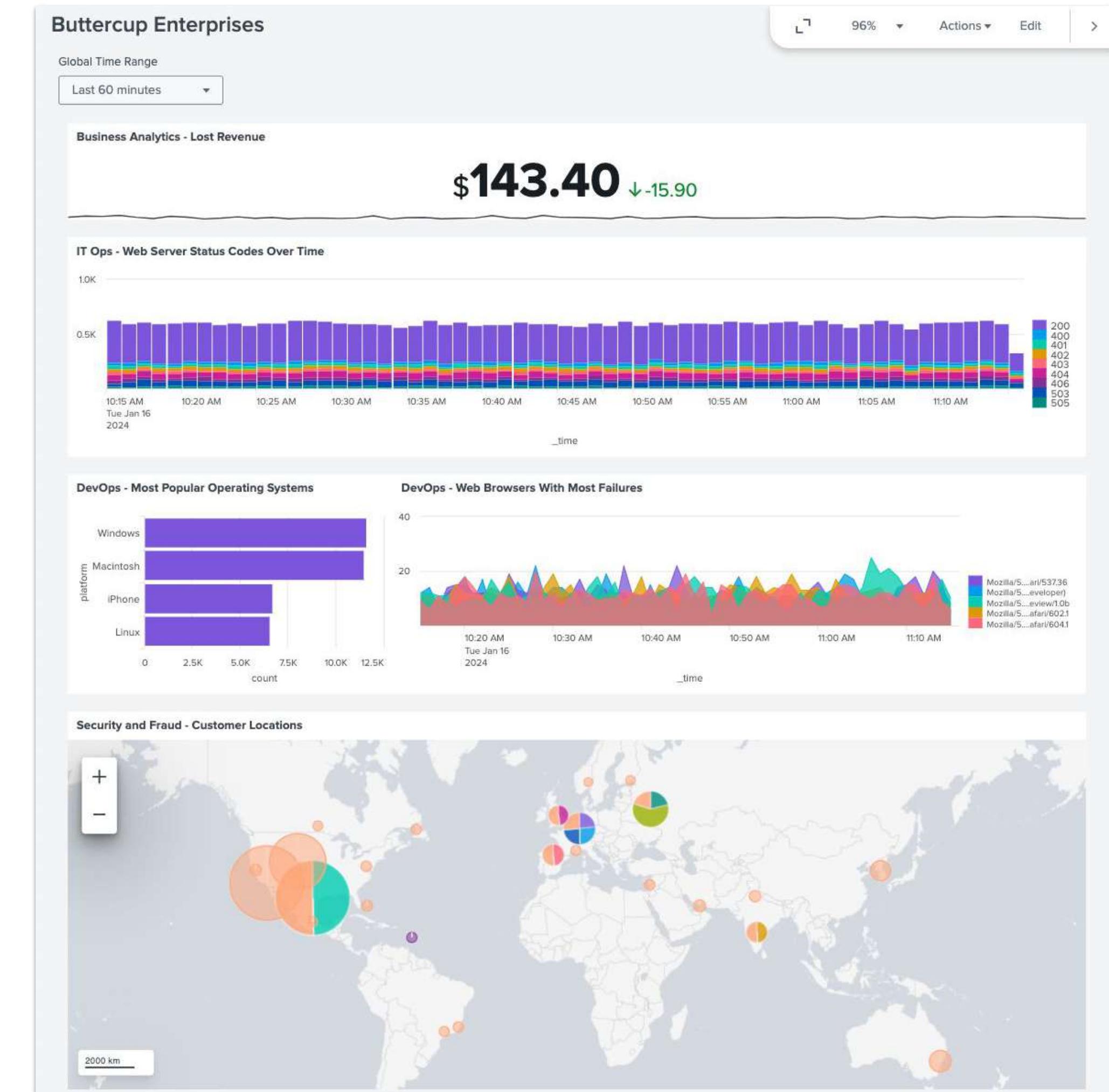
DevOps team ✓



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

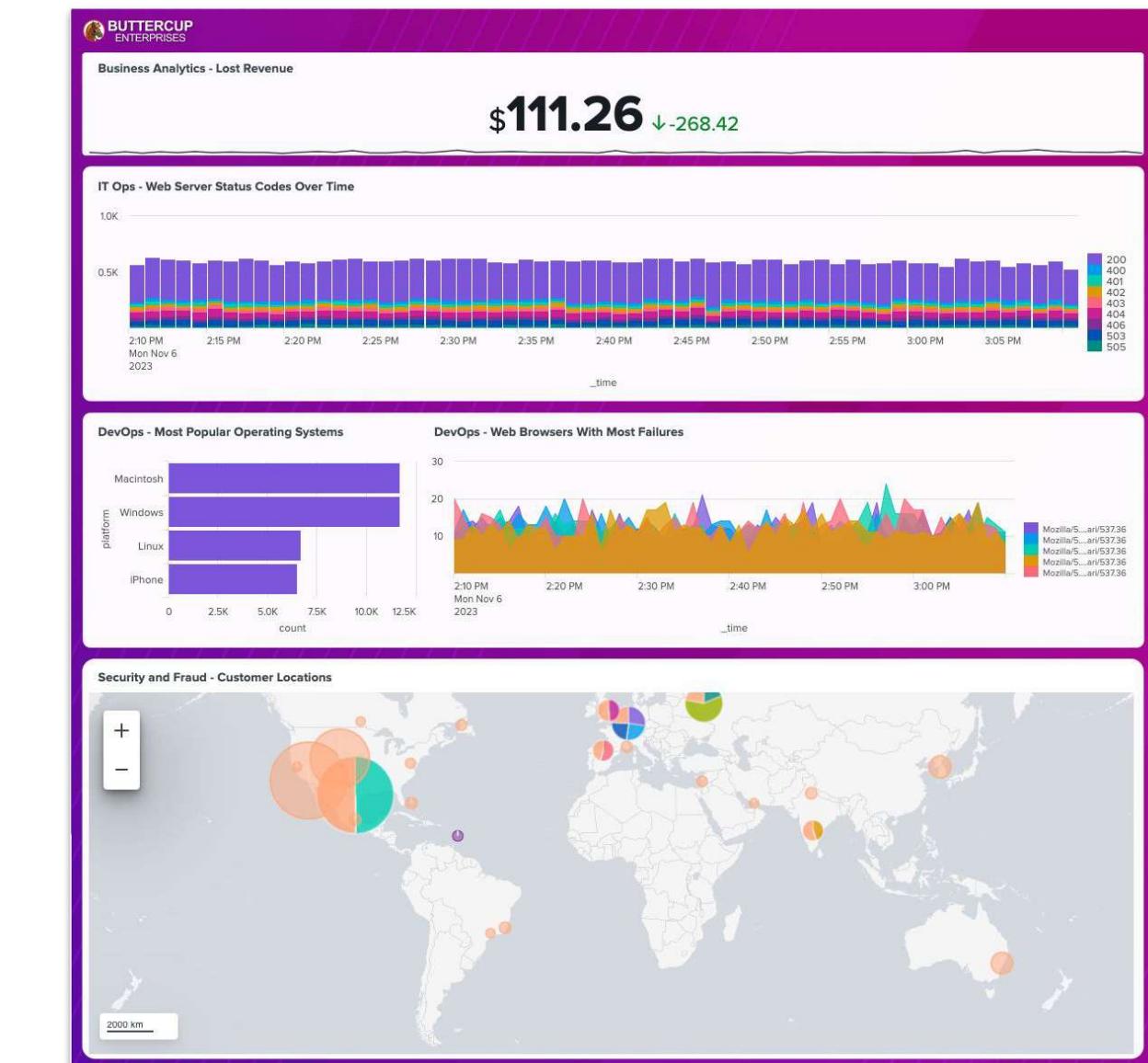


Customise Your Dashboard

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



Some Search & Dashboard Best Practices

Search: Always use two of index=<>, source=<>, sourcetype=<>

Search: Never use leading “*” in any use – never is a really long time, but be truly aware of what you are doing

Search: Understand the importance of the first “|” character – for the most part, everything after it is done on the searchhead, maximize to the left of the “|”

Search: Be aware of the architecture – Map/Reduce parallelization implies push the work onto the indexers

Search: Use stats rather than other inefficient agglutination commands, such as join or transaction

Search: Minimize the use of subsearches – understand how they work and how to be as efficient as possible with them

Search: No Real-Time searches, use shortest time possible, avoid “All Time” as well

Search: Avoid “index=main”. Be sure that events go into appropriate indexes

Search: Use fields and filters as much as possible, be inclusive rather than exclusive (avoid “NOT”, know your data)

Dashboard: Be as efficient in your dashboard searches as you are with the adhoc/saved searches

Dashboard: Use base or chained searches

Dashboard: Understand your data and how to present it

Dashboard: Don’t use auto-updating dashboards unless an admin builds the dashboard ... don’t permit auto-updates unless an admin makes it available to the larger audience



Users & Roles

Tasks

1. Discover Roles in Splunk
 - ↳ Find the definitions of roles in the Splunk interface
2. Discover Users in Splunk
 - ↳ Find the user definitions in Splunk and assign a role to the user
3. Observe the assigned ability in Splunk

Goal

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last Login	Status
buttercup_user	Edit	Splunk	changeme		launcher	system		user		✓ Active

1. See a new user with the “user” role
2. Experience how the role sets the user’s abilities

Users -> Roles

The screenshot shows the Splunk Settings menu. On the left, there's a sidebar with 'Add Data', 'Monitoring Console', and 'SYSTEM' sections. Under 'SYSTEM', 'Tokens' is highlighted with a red box. A dropdown menu is open over the 'Tokens' item, showing 'Roles', 'Users', and 'Tokens' again, with 'Tokens' also highlighted with a red box.

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data

Monitoring Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Federated search
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- RapidDiag
- Instrumentation
- Workload management

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens

Manage users and roles via the **Settings** menu

The screenshot shows the Splunk 'Users' list. It displays two users: 'admin' and 'mallison'. The 'admin' user is highlighted with a red box around the 'Roles' column, which shows 'admin'. The 'mallison' user has the roles 'power' and 'user'. The table includes columns for Name, Actions, Authentication system, Full name, Email address, Time zone, Default app, Default app inherited from, Roles, Last Login, and Status.

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last Login	Status
admin	Edit	Splunk	Administrator	changeme@example.com		launcher	system	admin	3/12/2024, 9:42:51 AM	✓ Active
mallison	Edit	Splunk	Michael Allison			launcher	system	power, user		✓ Active

Here we see that the **admin** user has the “**admin**” role

Roles -> Ability

Ability = inheritance, capabilities, indexes, restrictions, resources

Edit Role power

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes are added to this role. If no roles are specified, this role inherits capabilities and indexes from all selected roles.

<input type="checkbox"/> Role name	filter
<input type="checkbox"/> admin	
<input type="checkbox"/> can_delete	
<input type="checkbox"/> mitk_model_admin	
<input type="checkbox"/> power	
<input type="checkbox"/> splunk-system-role	
<input checked="" type="checkbox"/> user	

Roles inherit capabilities from other roles via layering

Edit Role power

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Select specific capabilities for this role.

<input type="checkbox"/> Capability Name	filter
<input type="checkbox"/> accelerate_datamodel	
<input checked="" type="checkbox"/> accelerate_search	
<input type="checkbox"/> admin_all_objects	
<input type="checkbox"/> apps_backup	
<input type="checkbox"/> apps_restore	
<input type="checkbox"/> capture_ingest_events	
<input type="checkbox"/> change_audit	

Roles carry their own capabilities (that layer)

Edit Role power

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Wildcards
Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes under a specific prefix. Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes under a specific prefix. Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes under a specific prefix.

Enter a value that contains *** Add

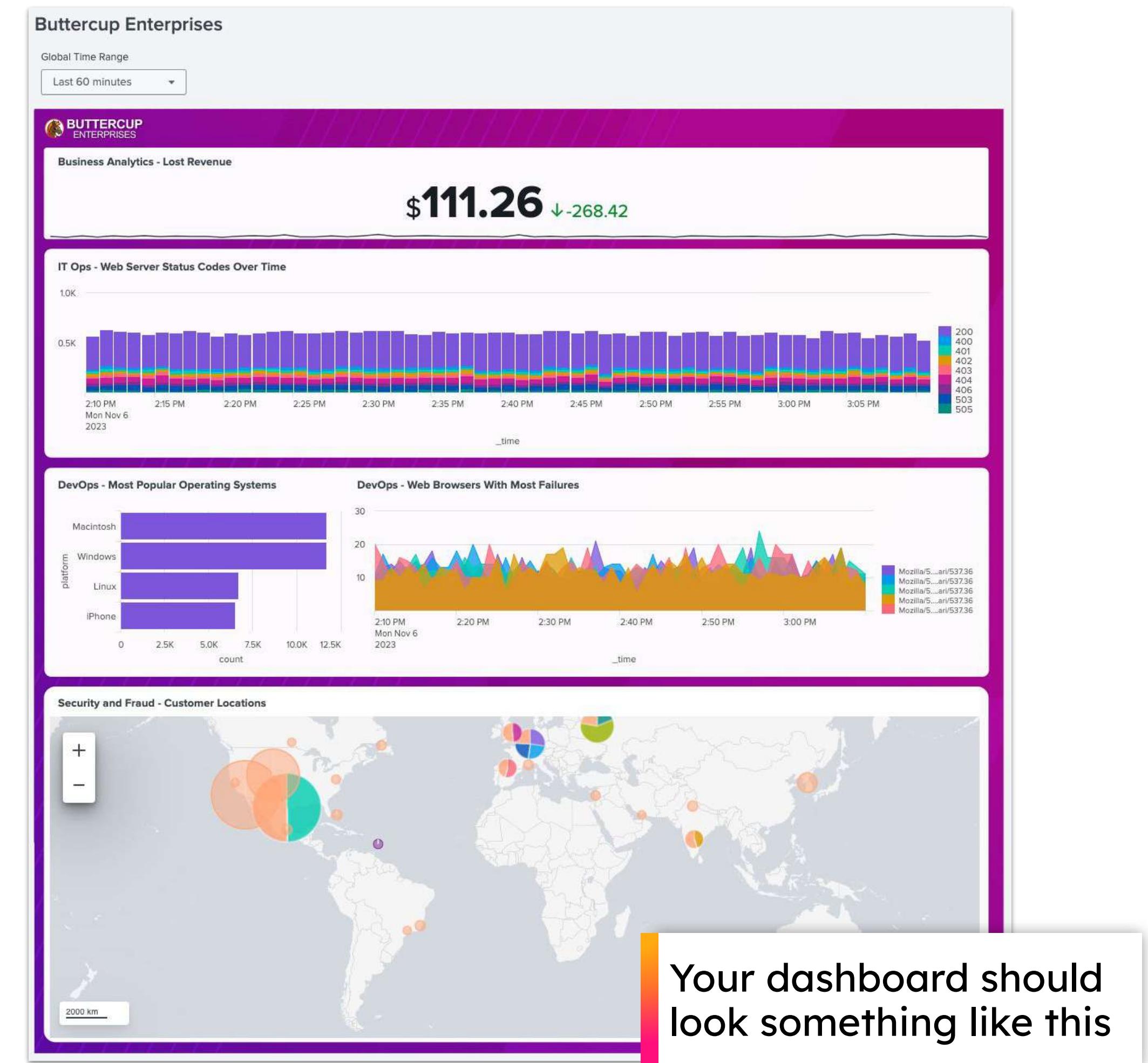
Indexes
Enable both the "Included" and "Default" checkboxes for an index to make that index searchable by users. You must enable both checkboxes for an index to make it searchable. You must enable both checkboxes for an index to make it searchable. You must enable both checkboxes for an index to make it searchable.

Index Name	filter	Included	Default
_telemetry		<input checked="" type="checkbox"/>	<input type="checkbox"/>
_thefishbucket		<input checked="" type="checkbox"/>	<input type="checkbox"/>
history		<input checked="" type="checkbox"/>	<input type="checkbox"/>
main		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
oidemo		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
oidemo_notable		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
summary		<input checked="" type="checkbox"/>	<input type="checkbox"/>
wineeventlog		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Roles (and therefore users) gain access to indexes

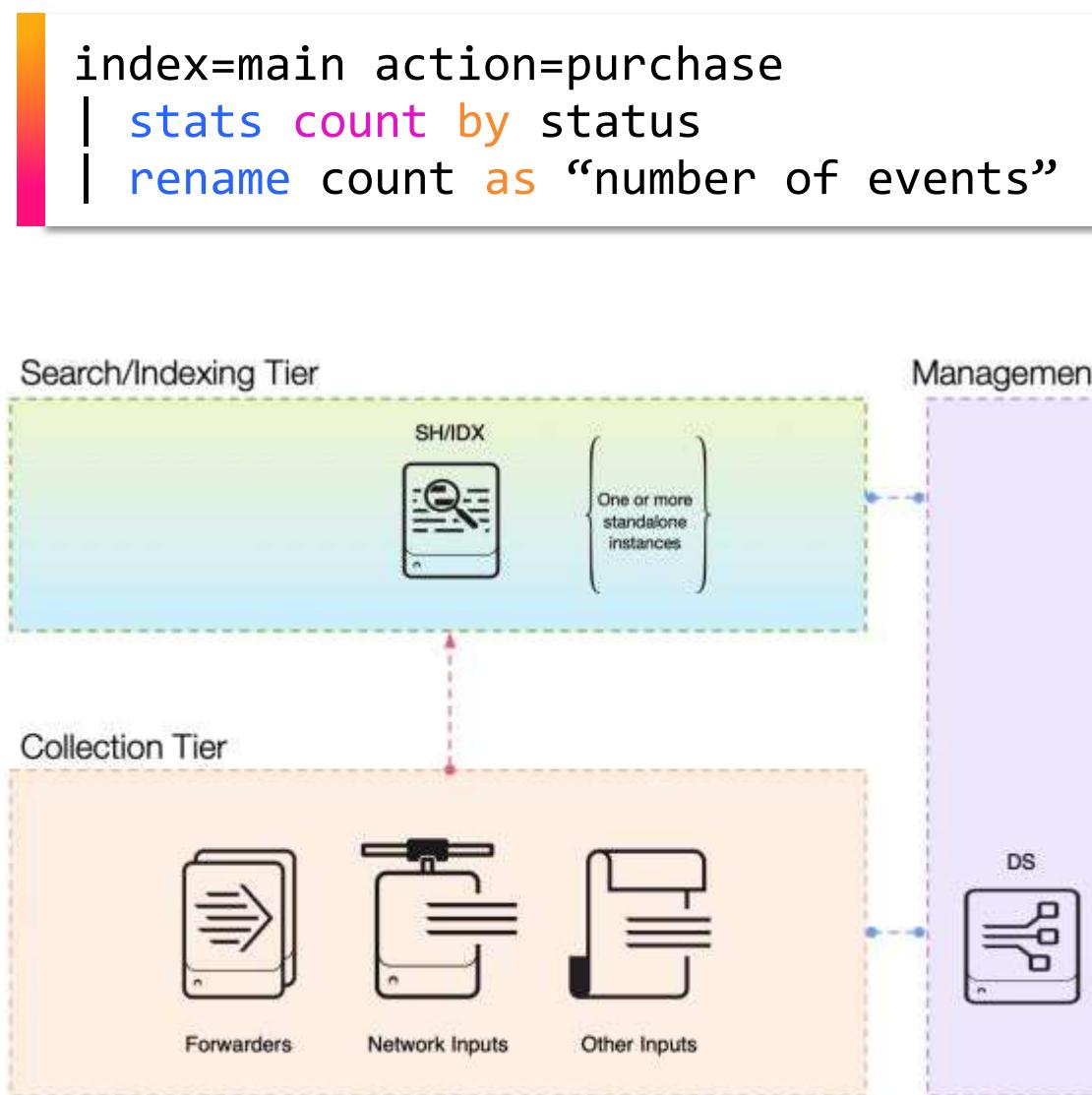
You've Finished the Hands-on Exercises!

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

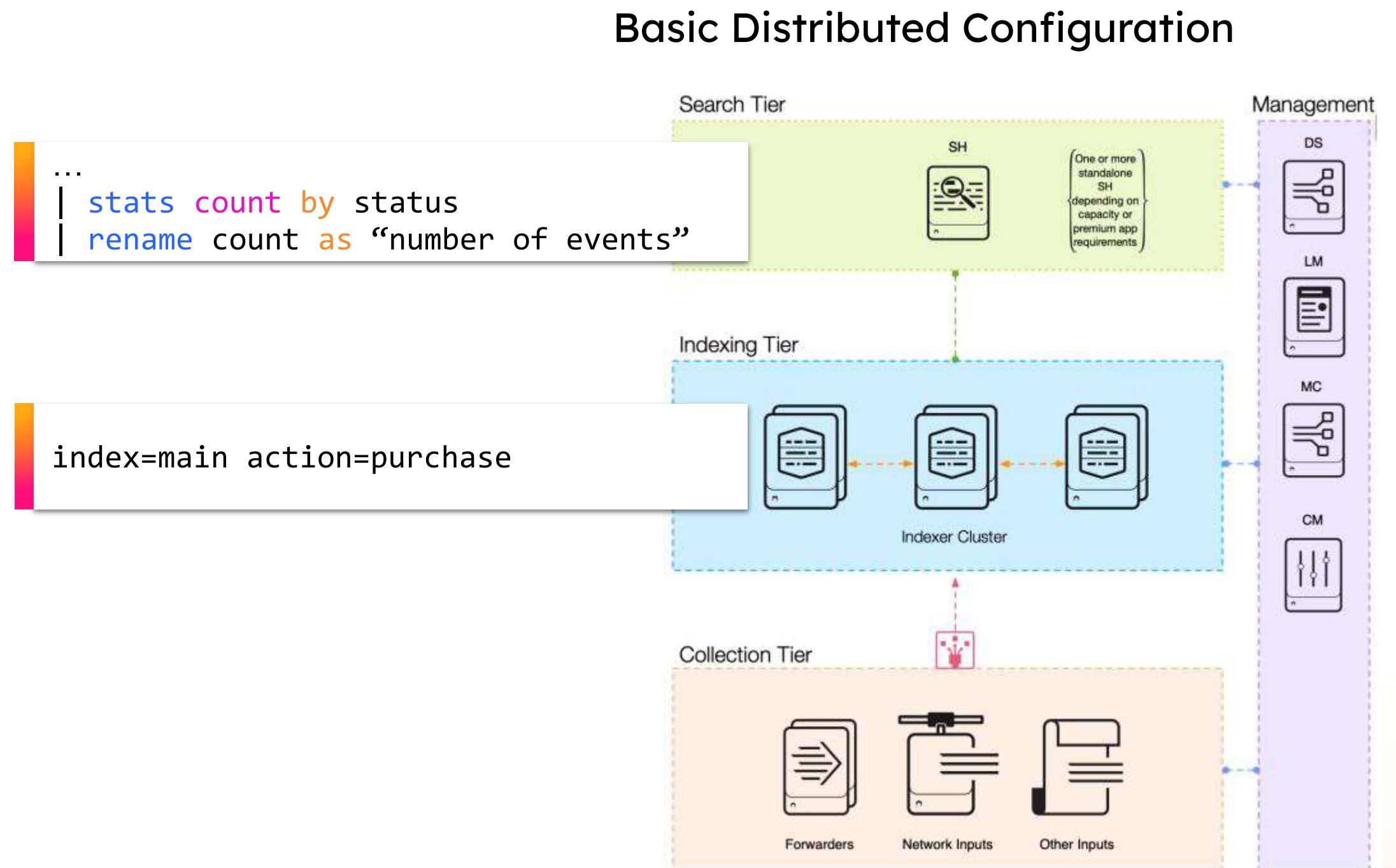


Splunk Architecture

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



Basic Configuration



Basic Distributed Configuration

Splunk Resources

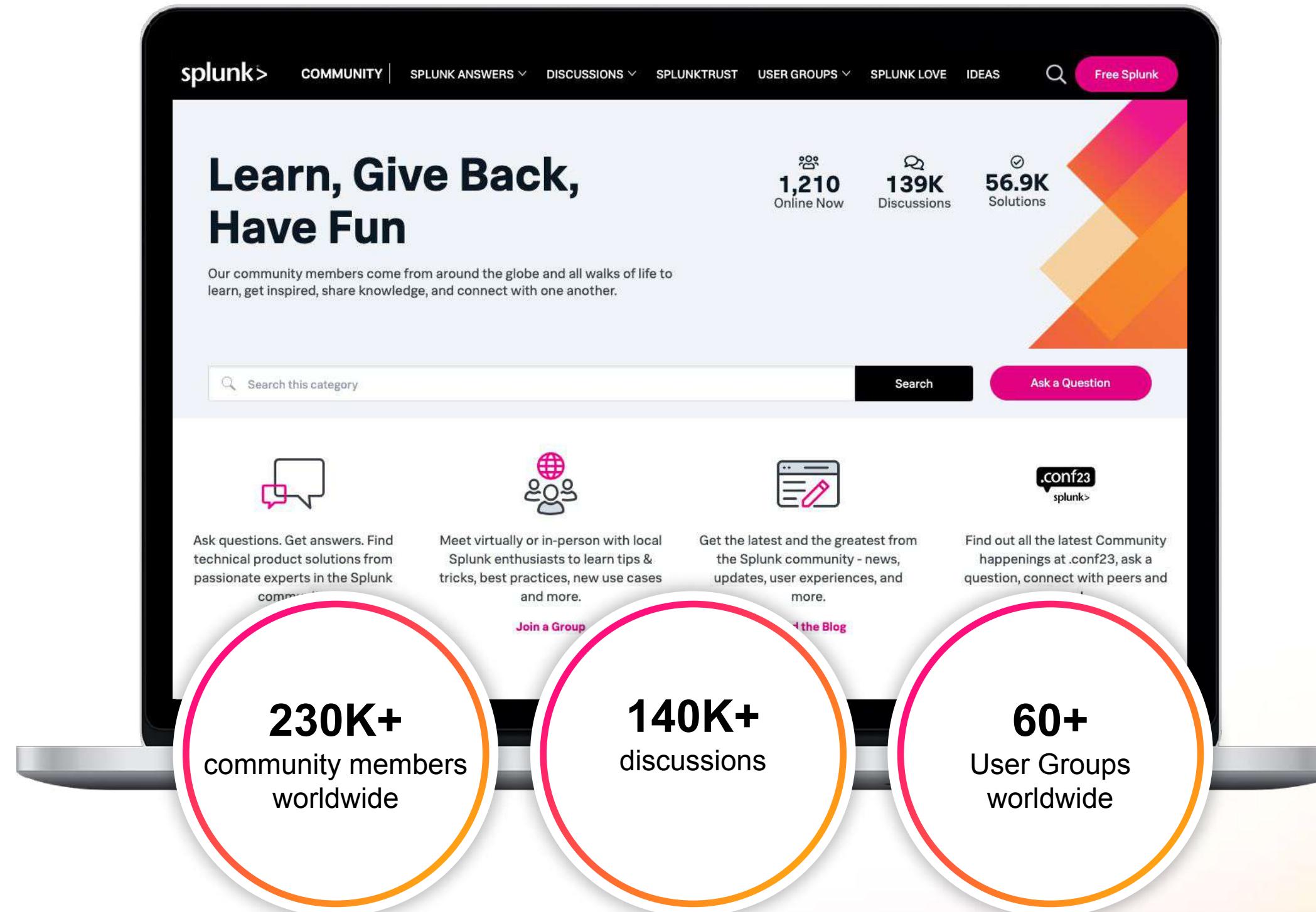
Where to go after today's workshop



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 Events

<https://splunk.com/events>

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



<https://conf.splunk.com>

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

A screenshot of a laptop displaying the Splunk Events website. The page has a dark header with the Splunk logo and navigation links for Products, Solutions, Why Splunk?, and Resources. Below the header is a search bar and a "Free Splunk" button. The main content area features a section titled "Splunk Events" with a sub-section "Join us at an event near you to gain new skills, expand your network and connect with the Splunk Community." On the left, there's a sidebar with a search bar, a "Filter all" section showing 39 results, and dropdown menus for Regions, Event Types, and Solutions. The main content area is divided into "Featured Events" and "Upcoming Events". Under "Featured Events", there are cards for "Gartner IT SYMPOSIUM Xpo.", "KubeCon CloudNativeCon North America 2023", and "AWS re:Invent". Each card includes details like location, date, and a "Register Now" button. Under "Upcoming Events", there are three more cards, each with a "Register Now" button.

Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search:

<https://splk.it/SplunkSearchTutorial>

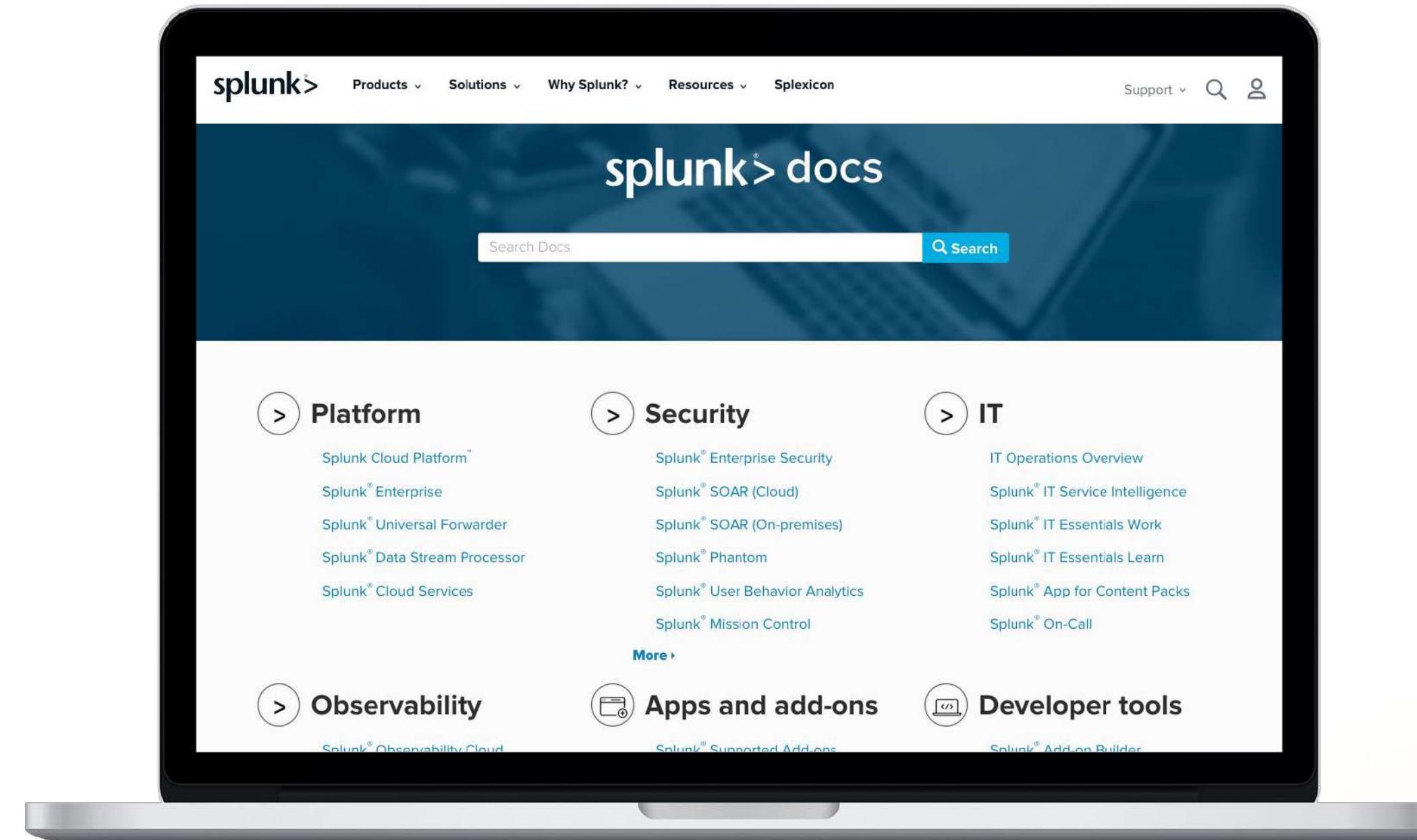
Dashboard Studio:

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

- And more!



Splunk Lantern

<https://lantern.splunk.com>

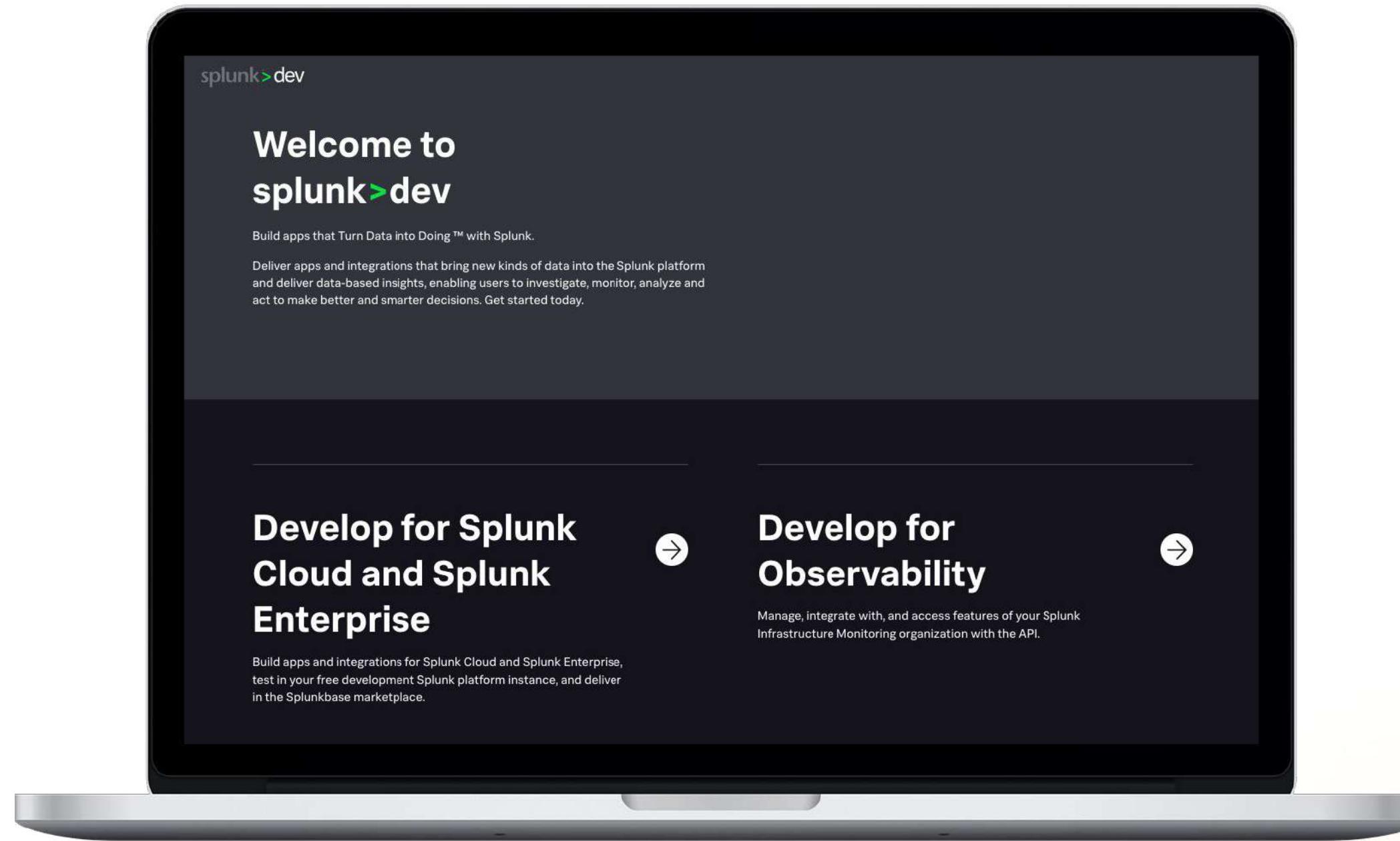
- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation

The screenshot shows the Splunk Lantern Customer Success Center homepage. At the top, there's a navigation bar with links for Documentation, Community, Training & Certification, Support Portal, User Groups, and a Free Splunk button. The main header reads "Splunk Lantern Customer Success Center". Below it, a sub-header says "Let Splunk experts light your path toward gaining valuable data insights, achieving your key use cases, and managing Splunk more efficiently." A "Click here to learn more." button and a search bar are also present. The page features three main content cards: "FEATURED: DATA QUALITY Solving data quality issues", "FEATURED: SPLUNK + GITLAB Getting GitLab CI/CD data into the Splunk platform", and "FEATURED: KUBERNETES METRICS Summarizing high-cardinality metrics by using metrics pipeline management". Each card includes a "Learn More" link. A decorative graphic of a lit lantern is visible on the right side. A banner at the bottom left of the page claims a "50% reduction in alert volume".

Developer Resources

<https://dev.splunk.com>

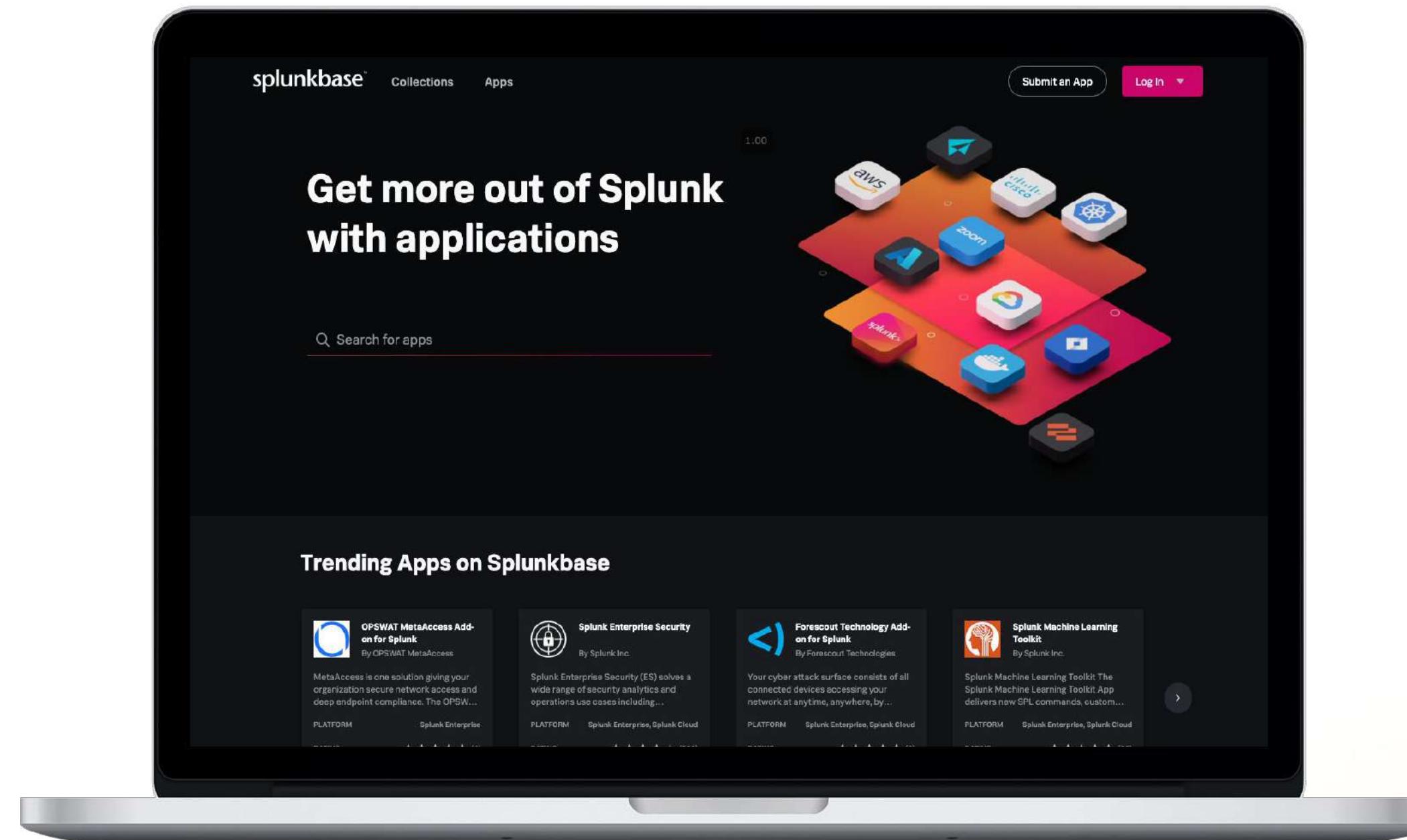
- Developer Guide
- API Reference
- Tutorials
- Downloads
APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

<https://splunkbase.splunk.com>

- 3100+ 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

The image shows a laptop screen displaying the Splunk Course Catalog. The header includes the Splunk logo and navigation links for Products, Solutions, Why Splunk, Resources, Support, and a Free Splunk button. Below the header, there are tabs for Training & Certification, Learning Paths, Course Catalog (which is highlighted in pink), Free Training, Certification, and Partnerships. A banner features three people smiling. The main content area is titled "Course Catalog" and contains a search bar and filter options for Content Type and Certification. It lists several courses: "What Is Splunk?", "Intro to Splunk", and "Using Fields".

Thank you

