

Splunk Telco Analyst 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. © 2023 Splunk Inc. All rights reserved.



Welcome to Telco Analysts Hands-on Workshop!

Please get your browser and logins for Splunk workshop server.

Workshop Agenda

- The value of data
- Splunk's approach to data
- Splunk Search / SPL Intro
- Splunk Analysis Intro
- Analysis Technique 1 : Distribution Analysis
- Analysis Technique 2 : Matrix/Pivot Analysis
- Analysis Technique 3 : 3D Matrix/Trend Analysis

There's a Lot More to Splunk

- Clustering
- Data Models
- Alerting
- Pivot
- SDKs
- APIs
- DB Connect

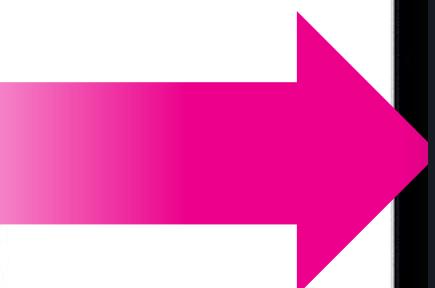
- Advanced Searches
- SOAR
- Machine Learning (ML)

- 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...

Objective



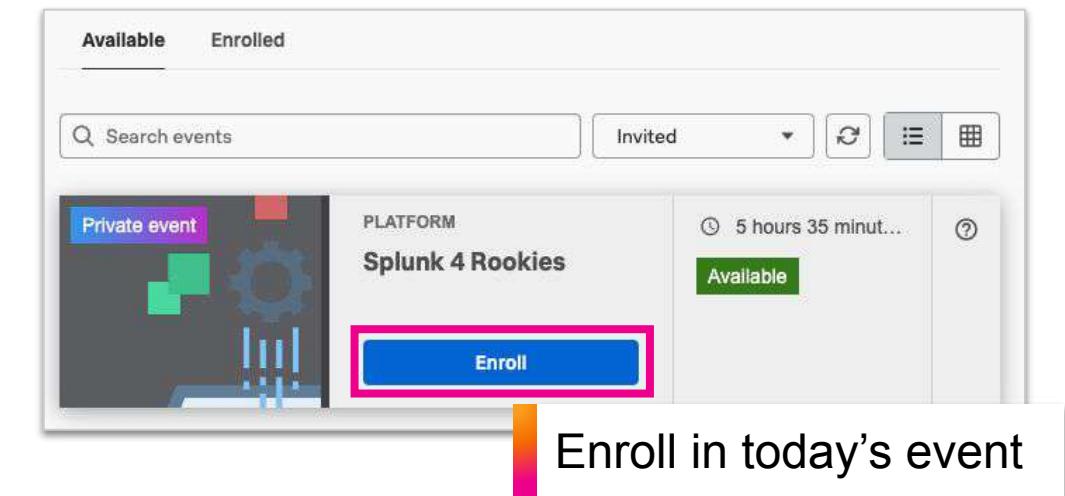


Enroll in Today's Workshop

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 a copy of today's slide deck:
<https://splk.it/TelcoAnalyst-Attendee>

Goal



The screenshot shows a user interface for enrolling in an event. At the top, there are two tabs: "Available" (which is selected) and "Enrolled". Below the tabs is a search bar with placeholder text "Search events" and a dropdown menu set to "Invited". To the right of the search bar are several icons: a magnifying glass, a refresh symbol, and three small squares. The main content area displays a card for an event titled "Splunk 4 Rookies". The card includes a thumbnail image labeled "Private event", the platform "Splunk 4 Rookies", a duration of "5 hours 35 minut...", and a status "Available". A large blue "Enroll" button is prominently displayed at the bottom of the card. A callout bubble with a pink-to-orange gradient points to this "Enroll" button with the text "Enroll in today's event".

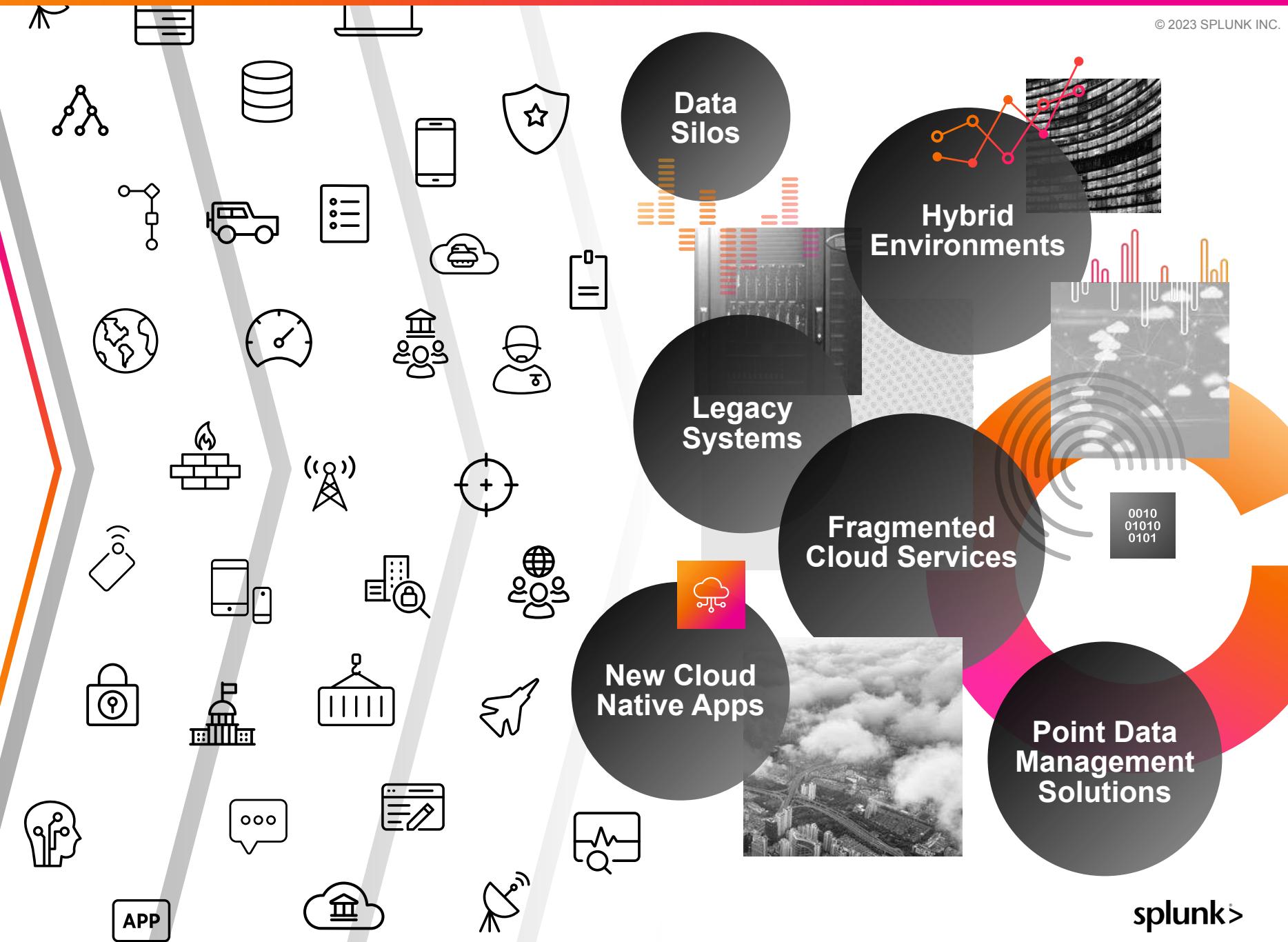


Splunk Solution Intro

Data is your Competitive Advantage

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

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

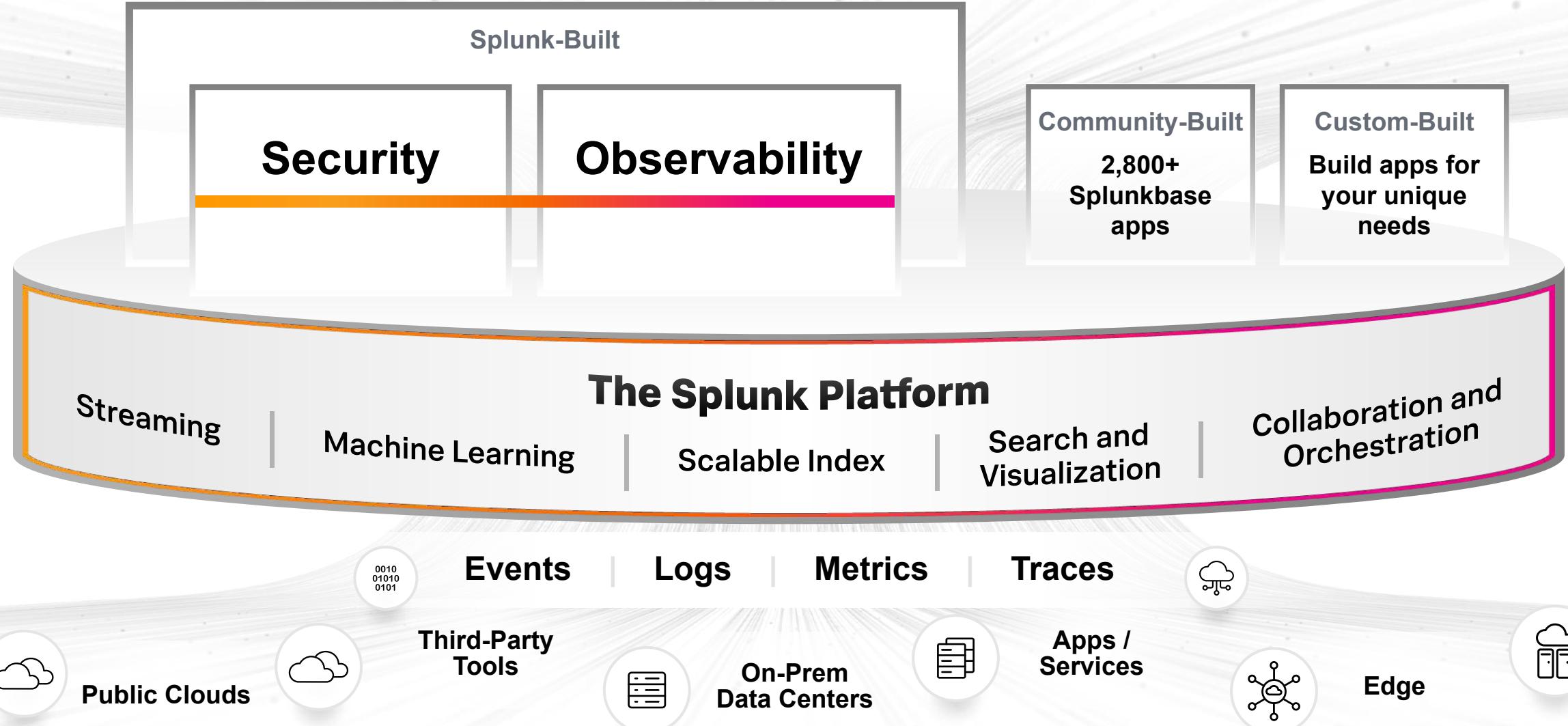
Investigate across massive data sets and take **action** fast

Extend

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



The Unified Security and Observability Platform



Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

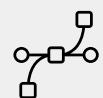
3 Simple Steps

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



- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI, HIPAA, FedRAMP (Moderate)
- **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



Wire Data



API



SDKs



HEC



TCP/UDP



RDBMS



Containers



Apps



Cloud Services



OpenTelemetry

Splunk
Forwarders

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!

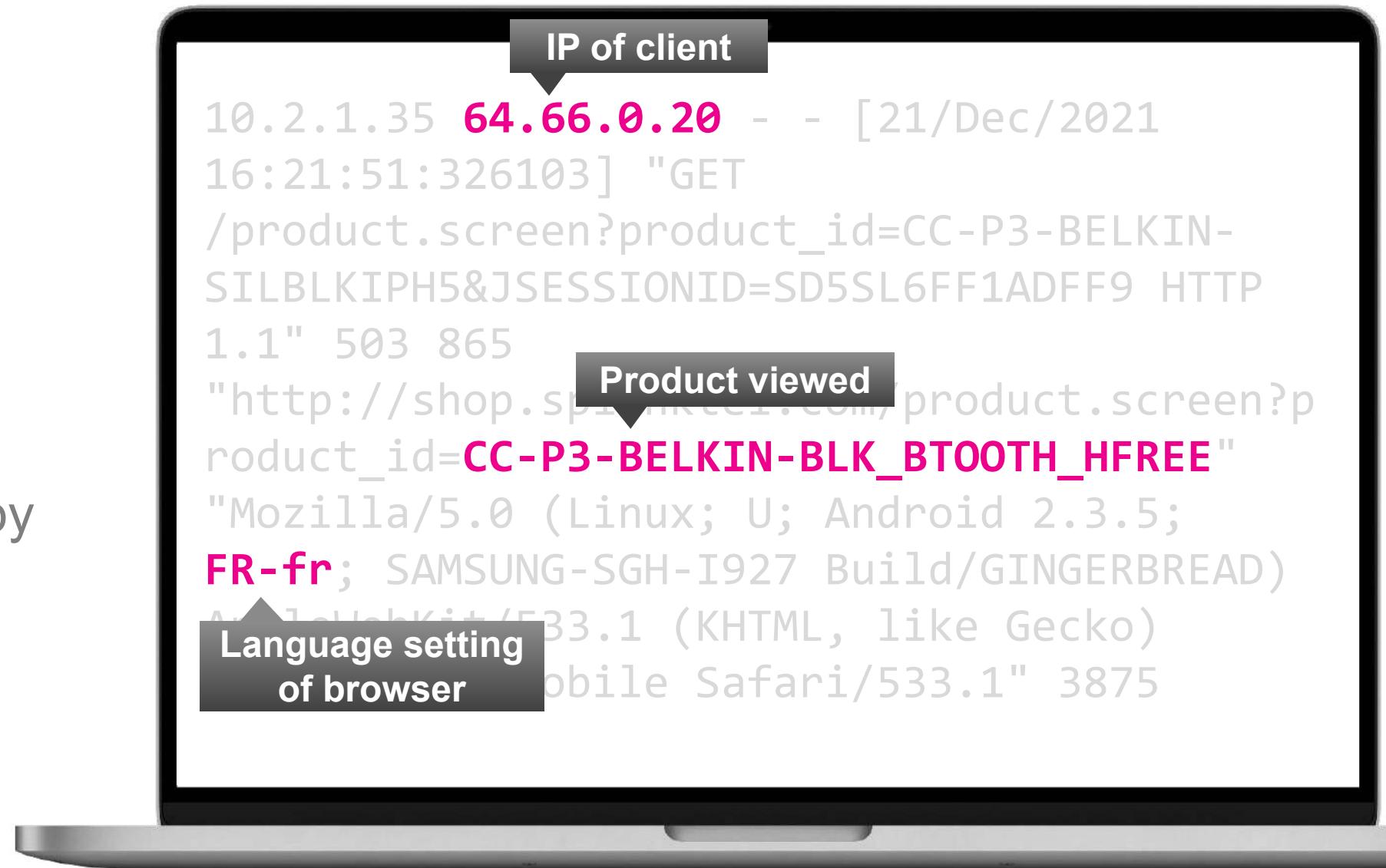


**Machine data
is valuable
not complex!**

```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BT0OTH_HFREE"  
"Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

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?

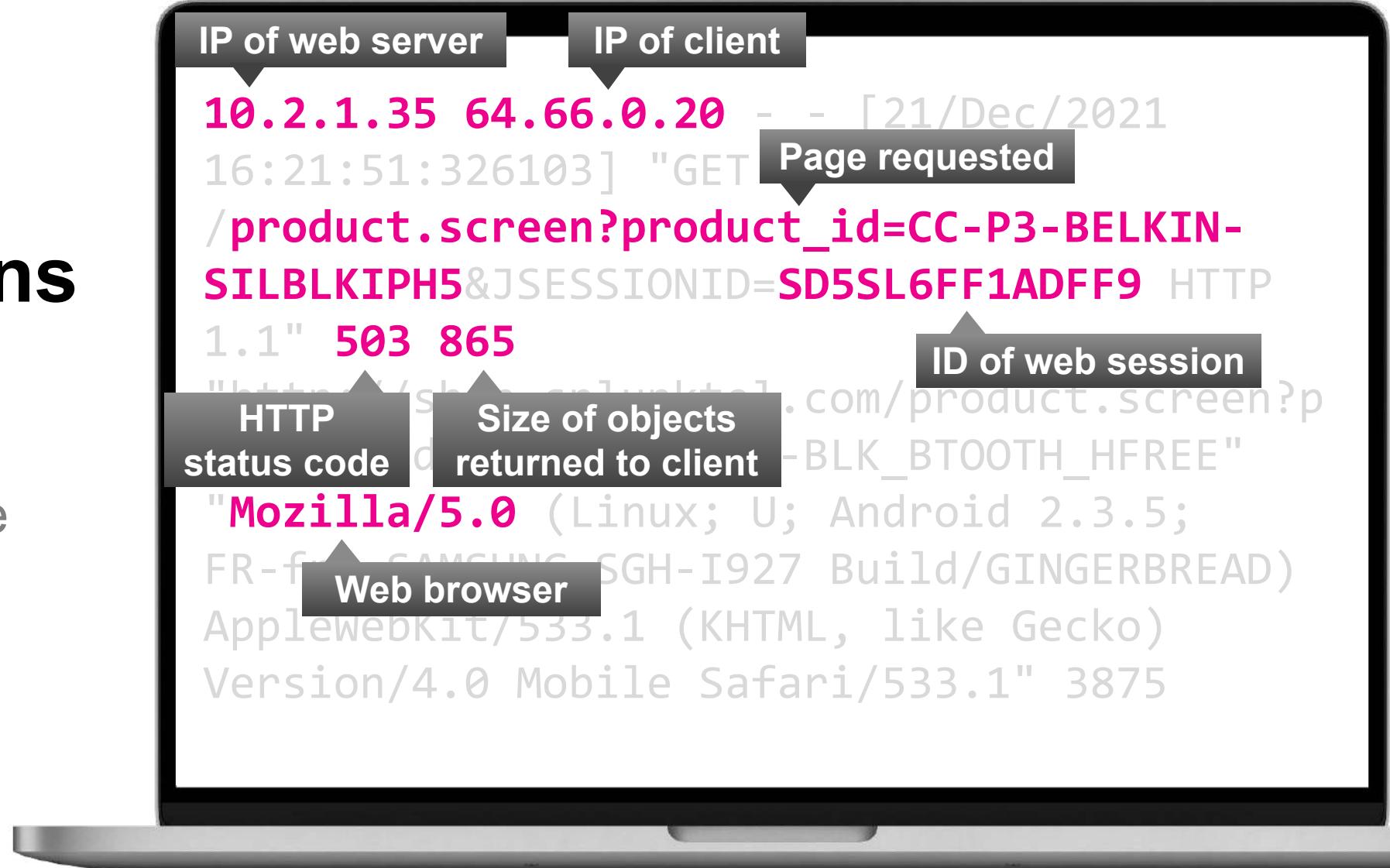
```
10.2.1.35 64.66.0.20 - - [21/Dec/2021  
16:21:51:326103] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?p  
roduct_id=CC-P3-BELKIN-BLK_BRIGHT_FREE"  
Mozilla/5.0 (Linux; U; Android 2.3.5;  
FR-fr; SAMSUNG-SGH-I927 Build/GINGERBREAD)  
AppleWebKit/533.1 (KHTML, like Gecko)  
Version/4.0 Mobile Safari/533.1" 3875
```

Platform

Handset model

IT Operations Use Case

Which web pages
are generating the
most errors?





Top 50 Telco Use cases

Operations + Service



SERVICE ASSURANCE

- [Order to Activation](#)
- [Contact Center Analytics](#)
- [CPE Monitoring](#)
- [Mobile Application Health](#)
- [Field Services Performance Optimization](#)
- [Emergency Services Monitoring](#)
- [Video Performance Monitoring](#)
- [Content Delivery Network Performance](#)
- [Enterprise Service Assurance](#)
- [Radio Access Network Monitoring](#)
- [IMS Core and VoLTE Monitoring](#)
- [Broadband Service Optimization](#)

OPERATIONAL EXCELLENCE

- [Enterprise Data Platform](#)
- [Enterprise Network Nerve Center](#)
- [Enterprise Security Nerve Center](#)
- [Managed Security Services](#)
- [Hybrid Cloud Monitoring](#)
- [Network Function Virtualization](#)
- [SDN and SD-WAN](#)
- [Core Network Monitoring](#)
- [Carrier Media Gateway Performance Monitoring](#)
- [DevOps Monitoring and Capacity Management](#)
- [Wireline Data Capture](#)
- [Network Access Monitoring](#)
- [Government Hosted Solutions](#)

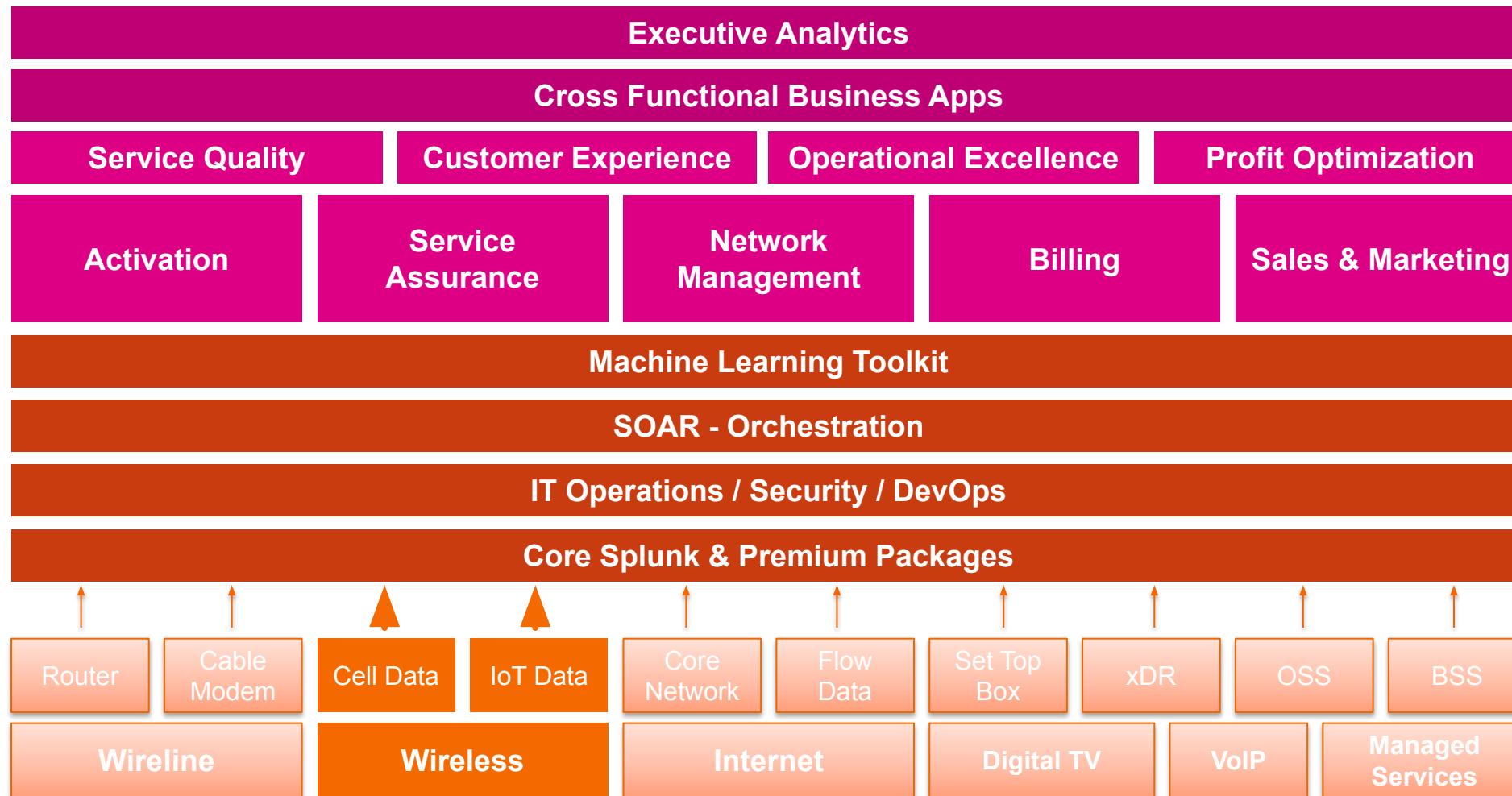
REVENUE ASSURANCE

- [Churn Prediction](#)
- [Truck Dispatch Analytics](#)
- [Video Subscriber Analytics](#)
- [Reducing SLA Violations](#)
- [Real-Time Vulnerability Management](#)
- [Roaming Fraud Detection](#)
- [PBX/IP-PBX Fraud Mitigation](#)
- [Subscriber Fraud Protection](#)
- [Subscriber Endpoint Security](#)
- [Automated Compliance Reporting](#)
- [Data Center ICS Monitoring](#)
- [Outage Impact](#)
- [Voice/VoIP Revenue Assurance](#)
- [Prepaid Billing Account Analysis](#)
- [License Exhaustion Prediction](#)
- [Real-Time Service Reporting](#)
- [Least Cost Routing Optimization](#)

IMAGINE THE POSSIBILITIES

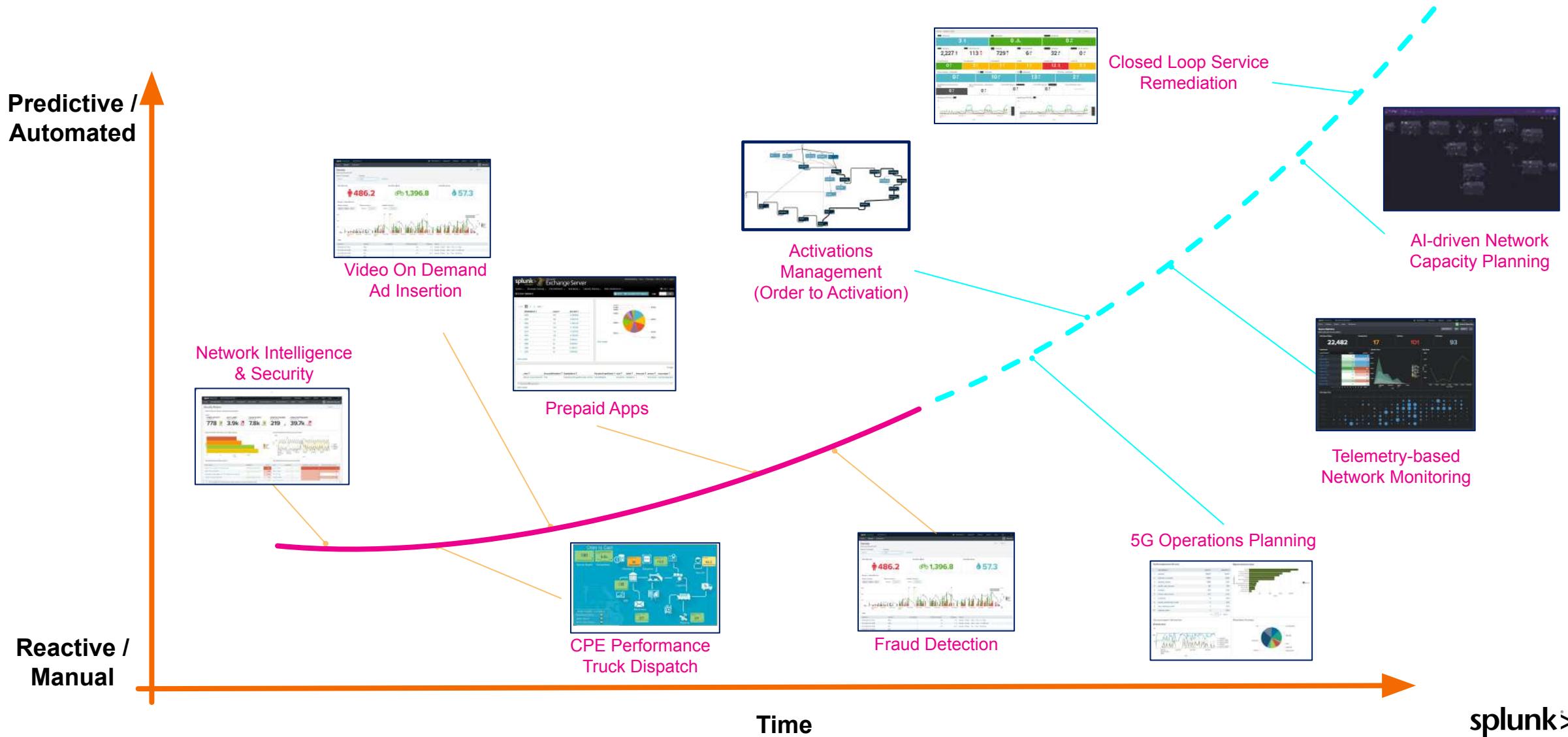
- [Data Integrity with Blockchain](#)
- [Mobile Banking/Mobile Payments](#)
- [5G Service Excellence](#)
- [Targeted Advertising with Small Cell](#)
- [Closed Loop Service Remediation](#)
- [Connected Experiences](#)
- [Customer 360](#)
- [Micro Weather Forecasting](#)

Splunk in Telco Operations

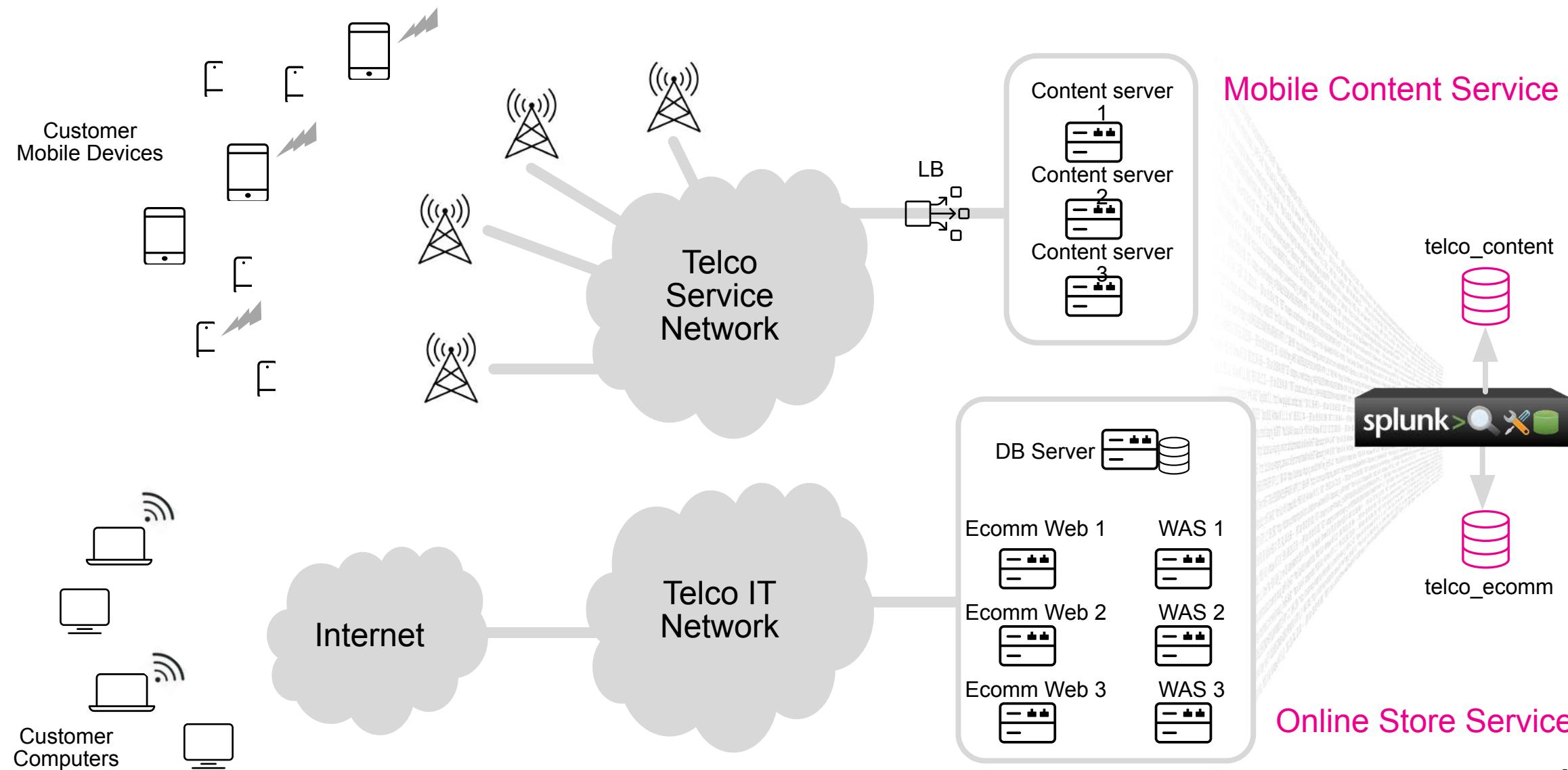


Telco Operational Maturity Model Example

Transforming from Reactive Ad-Hoc Analytics to Automated, Self Learning Systems



Today's Hands-on Environment



Apps and Add-ons

- 2800+ 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**

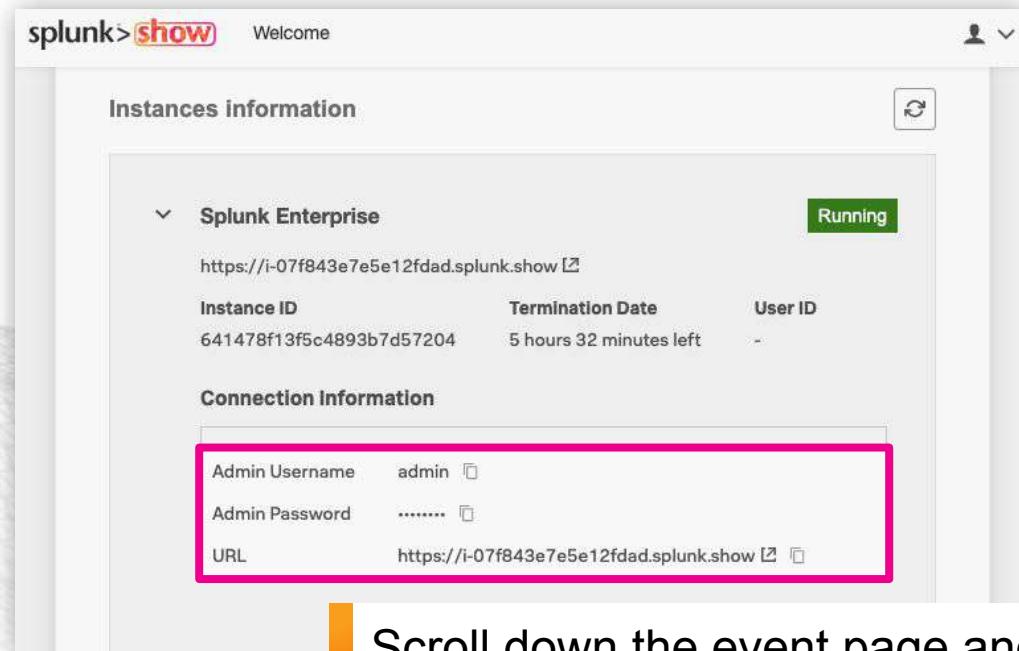




Splunk Search Intro

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:** https://i-07f843e7e5e12fdad.splunk.show
- 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



Login using the credentials
from Splunk Show

Open your app and have a play!

The currently selected app

Time picker – choose your search time range

Search bar – type anything here to search

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time

Splunk Enterprise App: Splunk 4 Rookies ▾ Administrator ▾ Messages ▾ Settings ▾

New Search

action=purchase status=200

✓ 261 events (15/05/2018 07:49:00.000 to 15/05/2018 08:49:00.000)

Last 60 minutes ▾

Events (261) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out Zoom to Selection Deselect

1 minute per column

List ▾ Format 20 Per Page ▾

1 2 3 4 5 6 7 8 ... Next >

Time	Event
15/05/2018 08:49:08.127	12.130.60.5 - - [15/May/2018 08:49:08:127] "GET /cart.do?action=purchase&itemId=EST-20&product_id=RP-SN-01&JSESSIONID=SD1SL2FF10 flowershop.com/category.screen?category_id=GIFTS" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 873 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:54.193	12.130.60.4 - - [15/May/2018 08:48:54:193] "POST /product.screen?product_id=FL-DLH-02&JSESSIONID=SD7SL2FF3ADFF8 HTTP/1.1" 200 629 "http://www.myflowershop.com/cart.do? action=purchase&itemId=EST-20&product_id=FL-DLH-02" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 256 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:46.196	203.92.58.136 - - [15/May/2018 08:48:46:196] "GET /cart.do?action=purchase&itemId=EST-15&product_id=K9-BD-01&JSESSIONID=SD1SL10FF1ADFF7 HTTP/1.1" 200 3031 "http://www. myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.3 g/weblogs/noise_apache_1.log sourcetype = access_combined :41:160] "POST /cart.do?action=purchase&itemId=EST-18&product_id=RP-LI-02&JSESSIONID=SD9SL3FF9ADFF6 HTTP/1.1" 200 2296 "http://www. product_id=RP-LI-02" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 847 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined

splunk>

Apps and Add-ons

- 2800+ 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**



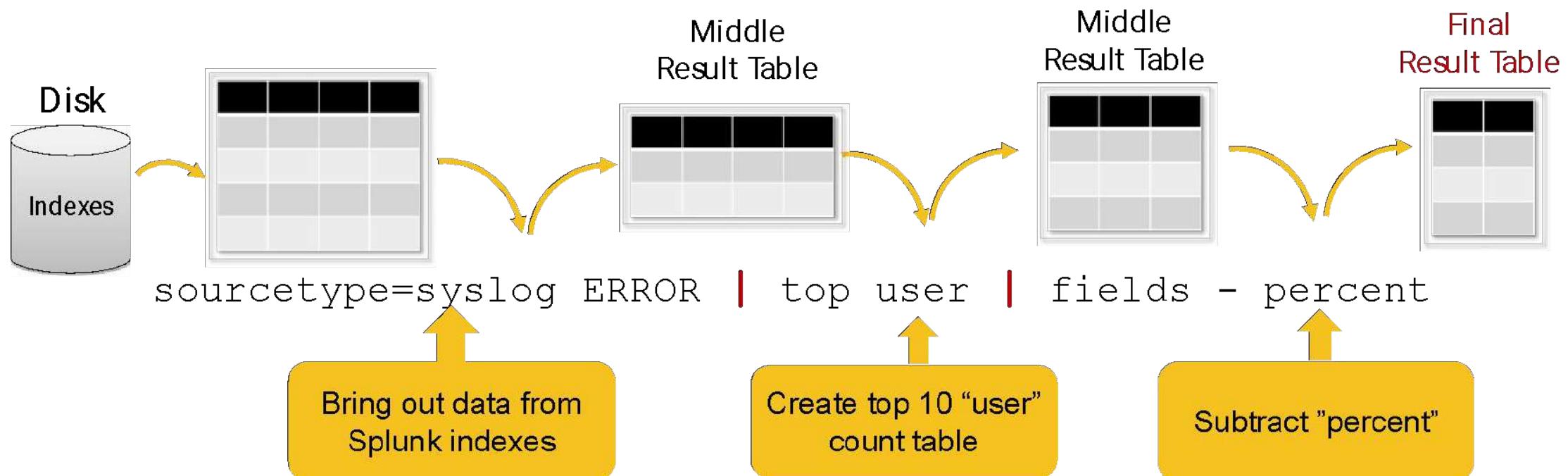
Add-ons

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



How SPL search pipeline works

- Search in the front bring out the data from Splunk indexes.
- Searched data goes through “pipeline” then passed on.





Splunk Search Basics

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 Analysis Method Intro

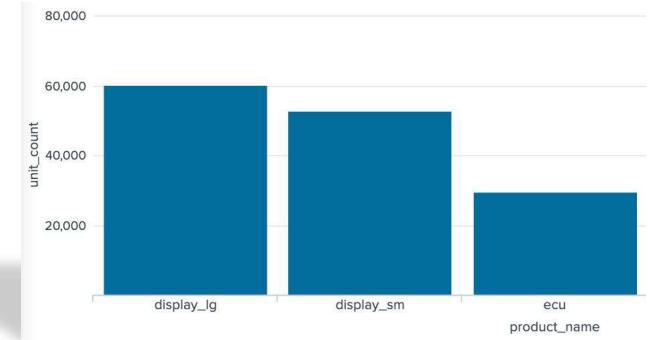


splunk>

Analysis Method Introduction

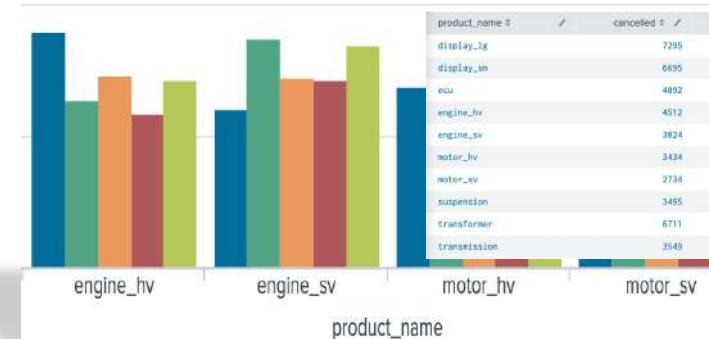
1. Distribution analysis : **stats**

- Compare one to another (Example : Performance comparison between one user to another, or one type vs another)



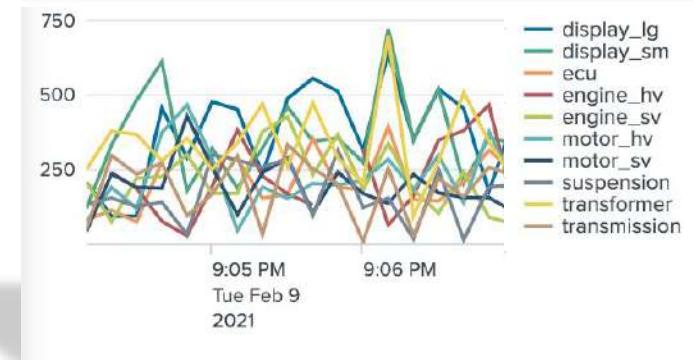
2. Matrix analysis : **chart**

- Create analysis matrix using 2 different data entity (Example : Compare activity between contents broken down into multiple dimension)



3. 3D Matrix analysis: **timechart**

- Analyzing trend and also compare the trend of different entities in data. (Example : Seeing the trend of either one or more users purchase contents over time)





Technique 1 Distribution Analysis

Analysis Technique 1 : Distribution

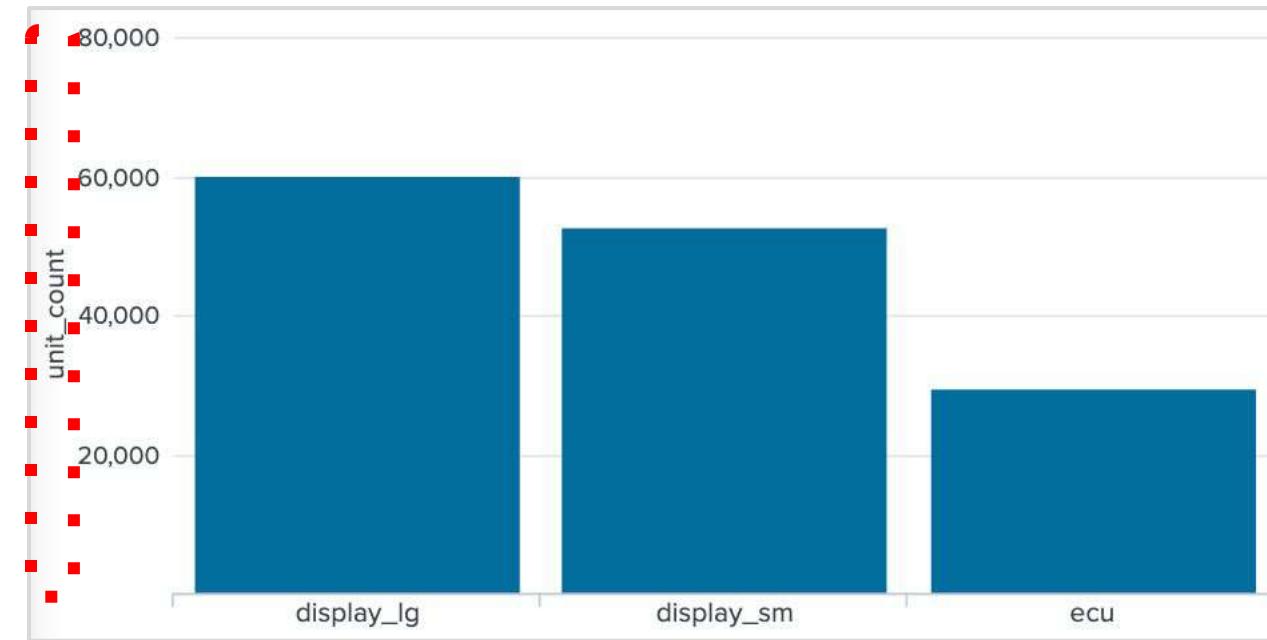
- Using **stats** Command
- 2D Distribution / comparison
- Goal : Compare between different **entities** with a single or multiple defined calculation **function**.

Function

```
stats sum(unit_count) by product_name
```

Group by segmentation

sum(unit_count)



product_name

by product_name

Analysis / Statistics Functions

FUNCTION	DESCRIPTION
avg (X)	Returns the average of the values of field X.
count (X)	Returns the number of occurrences of the field X. To indicate a specific field value to match, format X as eval(field="value").
dc (X)	Returns the count of distinct values of the field X.
first (X)	Returns the first seen value of the field X. In general, the first seen value of the field is the chronologically most recent instance of field.
last (X)	Returns the last seen value of the field X.
list (X)	Returns the list of all values of the field X as a multi-value entry. The order of the values reflects the order of input events.
max (X)	Returns the maximum value of the field X. If the values of X are non-numeric, the max is found from lexicographic ordering.
median (X)	Returns the middle-most value of the field X.
min (X)	Returns the minimum value of the field X. If the values of X are non-numeric, the min is found from lexicographic ordering.
mode (X)	Returns the most frequent value of the field X.
perc<X> (Y)	Returns the X-th percentile value of the field Y. For example, perc5(total) returns the 5th percentile value of a field "total".
range (X)	Returns the difference between the max and min values of the field X.
stdev (X)	Returns the sample standard deviation of the field X.
stdevp (X)	Returns the population standard deviation of the field X.
sum (X)	Returns the sum of the values of the field X.
sumsq (X)	Returns the sum of the squares of the values of the field X.
values (X)	Returns the list of all distinct values of the field X as a multi-value entry. The order of the values is lexicographical.
var (X)	Returns the sample variance of the field X.

Analysis Technique 1 : Distribution

Syntax :

```
stats func(field), func(field), ... by field_1, field_2 ...
```

Examples :

```
* | stats count  
* | stats count by status  
* | stats sum(price) by product_name  
* | stats sum(price), dc(user_name) by product_name  
* | stats sum(price), dc(user_name) by user_type action
```

EXERCISE #1

New Search

Save As ▾ Create Table View Close

```
1 sourcetype=access_combined  
2 | table _time host serial category product_id product_name result_code price unit_count uri_path user_agent  
3 | stats sum(unit_count) as unit_count by product_name
```

Last 24 hours

✓ 17,571 events (2/15/21 3:00:00.000 PM to 2/16/21 3:42:18.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (17,571) Patterns Statistics (10) **Visualization**

Bar Chart Format 88 Trellis

Splunk Visualizations

product_name	unit_count
unit_1	94397
unit_2	94937
unit_3	47758
unit_4	47374

More

Find more visualizations

Bar Chart

Compare values or fields.

Search Fragment

```
| stats count by comparison_category
```

Today's Scenario: My Telco Content Service

Your Company

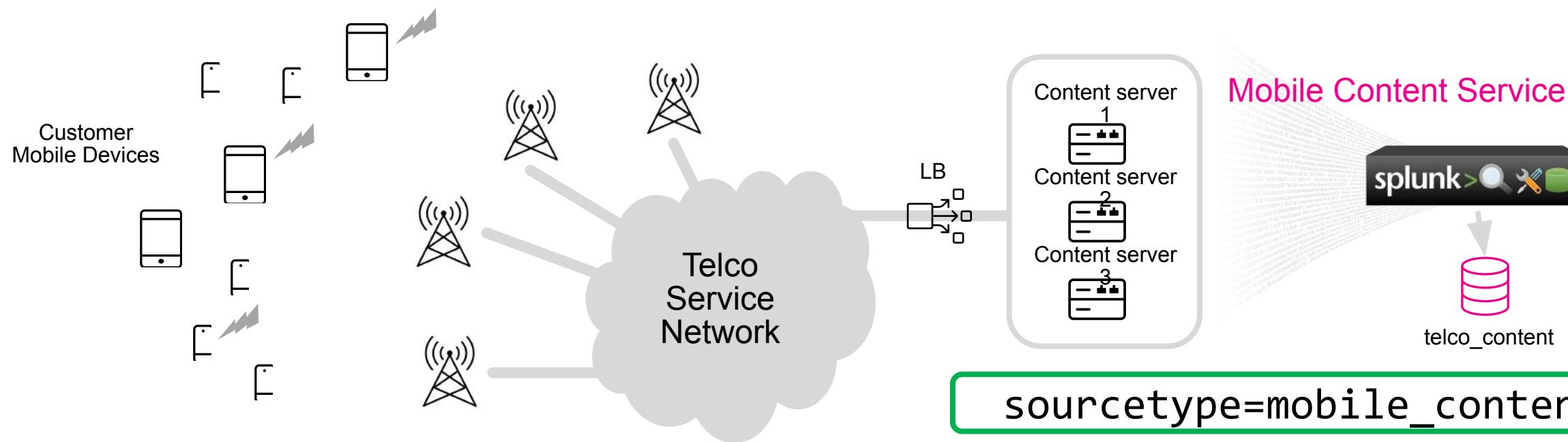
- MyTelco is a large communication service provider that provide network, contents services.
- MyTelco also has e-commerce portal that sells phones / devices to their customers.

Your Role

- You are one of the chosen few: a Splunk power user!
- Your responsibility is to provide information to users throughout the company
- You gather data and statistics, and report on:
 - **Security**
 - **IT operations**
 - **Development**
 - **Business intelligence**



Mobile Content Service Data



sourcetype=mobile_content

uri_path	clientip	status	bytes	action	user_type
• /category.screen	• 150.3.146.153	• 200	• 123 bytes	• download	• NEW
• /low_def_contents.screen	• 88.194.254.1	• 503	• 543	• purchase	• NORMAL
• /oldlink	• 39.121.36.4	• 406	• 3562	• stream	• PREMIUM
• /mobile_download.do	• 26.63.71.69	• 400	• 6524	• local_view	
useragent	product_id	method	timetaken	user_add	user_age
• Mozilla/5.0 (CrKey	• RWZ-239-02	• get	• 538 ms	• FOOT_HILLS	• 40 years
• Mozilla/5.0 (Linux;	• INW-047-08	• post	• 2359	• PACIFIC_NE	• 30
• Mozilla/5.0 (iPad;	• UYV-088-08		• 982	• NORTH_BAY	• 72
• Mozilla/5.0 (iPhone9,4;	• JYJ-901-03		• 245	• SAN_FRANCISCO	• 27
• Mozilla/5.0 (iPhone;					

Analysis Technique 1 : Exercise 1

STEP 01 – Select Telco content access data

Select the data from 3 web servers serving mobile contents service. By defining the “sourcetype=mobile_content”, you are selecting entire content access data from your 3 different content servers running.

sourcetype=mobile_content

The screenshot shows the Splunk search interface. At the top, there is a search bar with the query "1 sourcetype=mobile_content". To the right of the search bar is a dropdown menu set to "Last 24 hours" with a magnifying glass icon. Below the search bar is a "No Event Sampling" button. On the left, there is a "Search History" link and a "How to Search" section with a "Documentation" button. In the center, there is an "Analyze Your Data with..." section and a "Table Views" section with links to "Pivot!" and "Learn more about Table Views". On the right, a large dropdown menu titled "Presets" is open, showing various time ranges under "REAL-TIME", "RELATIVE", and "OTHER". The "Last 24 hours" option is highlighted with a pink dashed box and a mouse cursor. Other options include "30 second window", "Today", "Last 15 minutes", "1 minute window", "Week to date", "Last 60 minutes", "5 minute window", "Business week to date", "Last 4 hours", "30 minute window", "Month to date", "Last 24 hours", "1 hour window", "Year to date", "Yesterday", "All time (real-time)", "Previous week", "Previous business week", "Relative", "Real-time", "Date Range", "Date & Time Range", and "Advanced".

After type in the search query, select the search time window to “**Last 24 Hours**” then click “**Search**” icon.

Analysis Technique 1 : Exercise 1

STEP 01 – Select manufacturing data

Use table command to nicely format the data, so that it's easy to see each records with important fields we may care about.

```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name  
status action price bytes time_taken uri_path user_type user_add user_age
```

Analysis Technique 1 : Exercise 1

STEP 02 – Explore data and understand context

Field Name	Value
_time	Time of event occurrence
host	Servicing web server host
clientip	Connecting client IP
JSESSIONID	Session ID for the interaction
category_id	Content category information
method	Web interaction method
uri_path	Process status
product_id	Product ID
product_name	Product name
status	Web access respond status
action	Request action type
useragent	User browser information
bytes	Amount of data exchange
price	Price of the content
time_taken	Time taken to process the request

Field Name	Value
uri_path	Accessed URI, API module
user_type	Customer type
user_addr	Customer address
user_age	Customer Age

Analysis Technique 1 : Exercise 1

STEP 02 – Explore data and understand context

Click on “Event” tab to get back into data exploration interface. Select a few of the fields defined above to get familiarized with what information they include.

1 sourcetype=mobile_content
2 | table _time host clientip JSESSIONID category_id method uri_path product_id product_name status action price bytes timetaken uri_path user_type user_add user_age|

✓ 20,171 events (before 10/3/22 1:29:32.000 PM) No Event Sampling ▾

Events (20,171) Patterns Statistics (20,171) Visualization

100 Per Page ▾ Format Preview ▾

⚡ Fast Mode
Field discovery off for event searches. No event data for stats searches.

💡 Smart Mode
Field discovery on for event searches. No event data for stats searches.

🗣️ Verbose Mode
All event & field data.

_time	host	clientip	JSESSIONID	category_id	method			
2022-10-03 13:29:30.145	mobile-content-02.mytelco.com	26.116.111.162	SD8SL1FF4ADFF5		GET			
2022-10-03 13:29:30.131	mobile-content-02.mytelco.com	141.146.8.66	SD1SL5FF5ADFF1	ACTION:CRIME:DRAMA:FI	POST			
2022-10-03 13:29:29.162	mobile-content-02.mytelco.com	142.32.213.106	SD7SL10FF9ADFF10	DRAMA:SCI-FI:THRILLER	GET	/category.screen		
2022-10-03 13:29:29.133	mobile-content-03.mytelco.com	202.130.77.228	SD4SL3FF10ADFF5	DRAMA:FI	GET	/category.screen	UBG-797-00	Revenge of Nerds

Analysis Technique 1 : Exercise 1

STEP 03 – Explore data and understand context

For exploring data example click on “product_name” field in the “Selected Field” panel to see what kinds of contents are being accessed. Also explore other data fields from the table above.

```
# date_minute 60
# date_month 1
# date_second 60
# date_wday 1
# date_year 1
# date_zone 1
# ident 1
# JSESSIONID 100+
# linecount 1
# method 2
# other 100+
# price 100
# product_id 100+
# product_name 100+
# punct 100+
# referer 100+
# referer_domain 1
# req_time 100+
# request 100+
# serverip 100+
# SESSIONID 100+
# splunk_server 1
# status_code 5
# time_taken 100+
# timeendpos 8
# timestamp 100+
# timestartpos 8
# uri 100+
```

Top 10 Values	Count	%
Beautiful Ohio	34	0.209%
Grand Theft Auto	34	0.209%
Rasen	33	0.203%
Ward 13	31	0.191%
Calloused Hands	30	0.185%
Suppose They Gave a War and Nobody Came?	30	0.185%
Spirits of the Dead	29	0.178%
Bounty Hunters (Bail Enforcers)	29	0.178%
Three Musketeers, The	29	0.178%
Trouble Every Day	27	0.166%

> 10/3/22 170.134.62.73 - - [03/Oct/2022 13:37:49:113] "GET /category.screen?category_id=THRILLER:WAR" 200 2599 "http://contents.mytelco.com/category.screen?category_id=THRILLER:WAR" "

Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

Create a quick analysis using Splunk “**stats**” command to aggregate total number of **content accessed** by **product_name** (Content). Then sort by the most amount of content access count.

The fields that are relevant here are :

- * **product_name**, which we want to total split by the produce name

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age
| stats count by product_name
| sort - count
| head 20
```

product_name	count
Beautiful Ohio	41
Grand Theft Auto	41
Rasen	40
Surviving the Game	40
Christmas Carol, A	38
Bounty Hunters (Bail Enforcers)	37

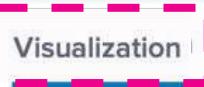
Analysis Technique 1 : Exercise 1

STEP 04 – Visualization

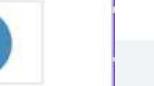
1 sourcetype=mobile_content
2 | table _time host clientip JSESSIONID category_id method uri_path product_id product_name status action price bytes time_taken
 uri_path user_type user_add user_age
3 | stats count by product_name
4 | sort - count
5 | head 10

All time 

✓ 25,047 events (before 10/3/22 1:56:37.000 PM) No Event Sampling ▾ Job ▾  Verbose Mode ▾

Events (25,047) Patterns Statistics (10) **Visualization** 

Bar Chart  Format Trellis

Splunk Visualizations 




Find more visualizations 

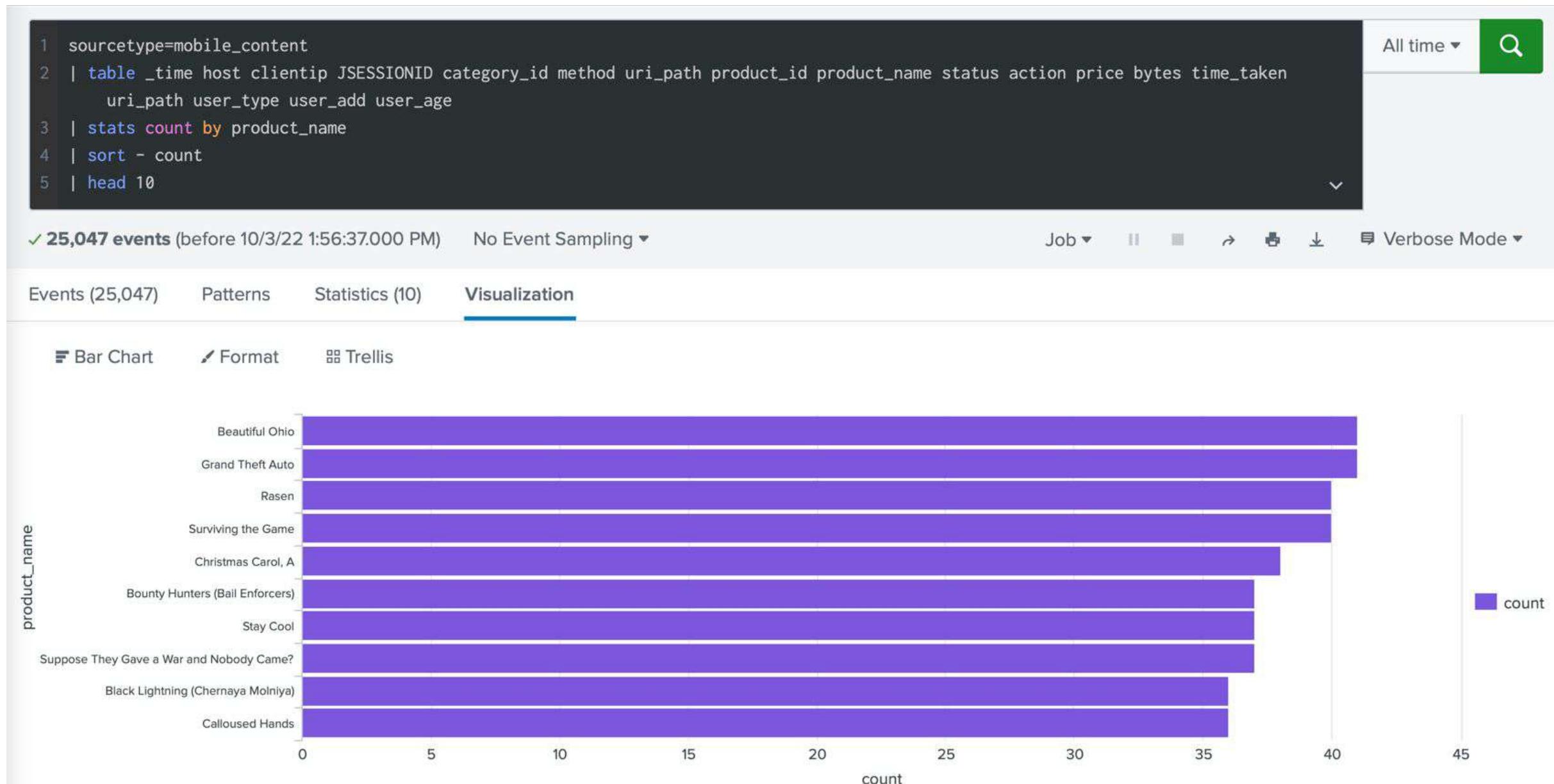
Radial Gauge
Show a single value in relation to customized ranges.

Search Fragment

product_name	count
41	41
41	40
40	40
38	37
37	37
37	36

Analysis Technique 1 : Exercise 1

STEP 04 – Visualization



Analysis Technique 1 : Exercise 1

STEP 04 – Visualization

1 sourcetype=mobile_content
 2 | table _time host clientip JSESSIONID category_id method uri_path product_id product_name status action price bytes time_taken
 3 | stats count by product_name
 4 | sort - count
 5 | head 10

All time Q

✓ 25,047 events (before 10/3/22 1:56:37.000 PM) No Event Sampling ▾ Job ▾ II ▾ ↗ Verbose Mode ▾

Events (25,047) Patterns Statistics (10) **Visualization**

Bar Chart Format Trellis

Splunk Visualizations

product_name	count
product_1	42
product_2	40
product_3	38
product_4	37
product_5	36
product_6	35
product_7	34
product_8	33
product_9	32
product_10	31

Find more visualizations ↗

Filler Gauge
 Show a single value and its current range.

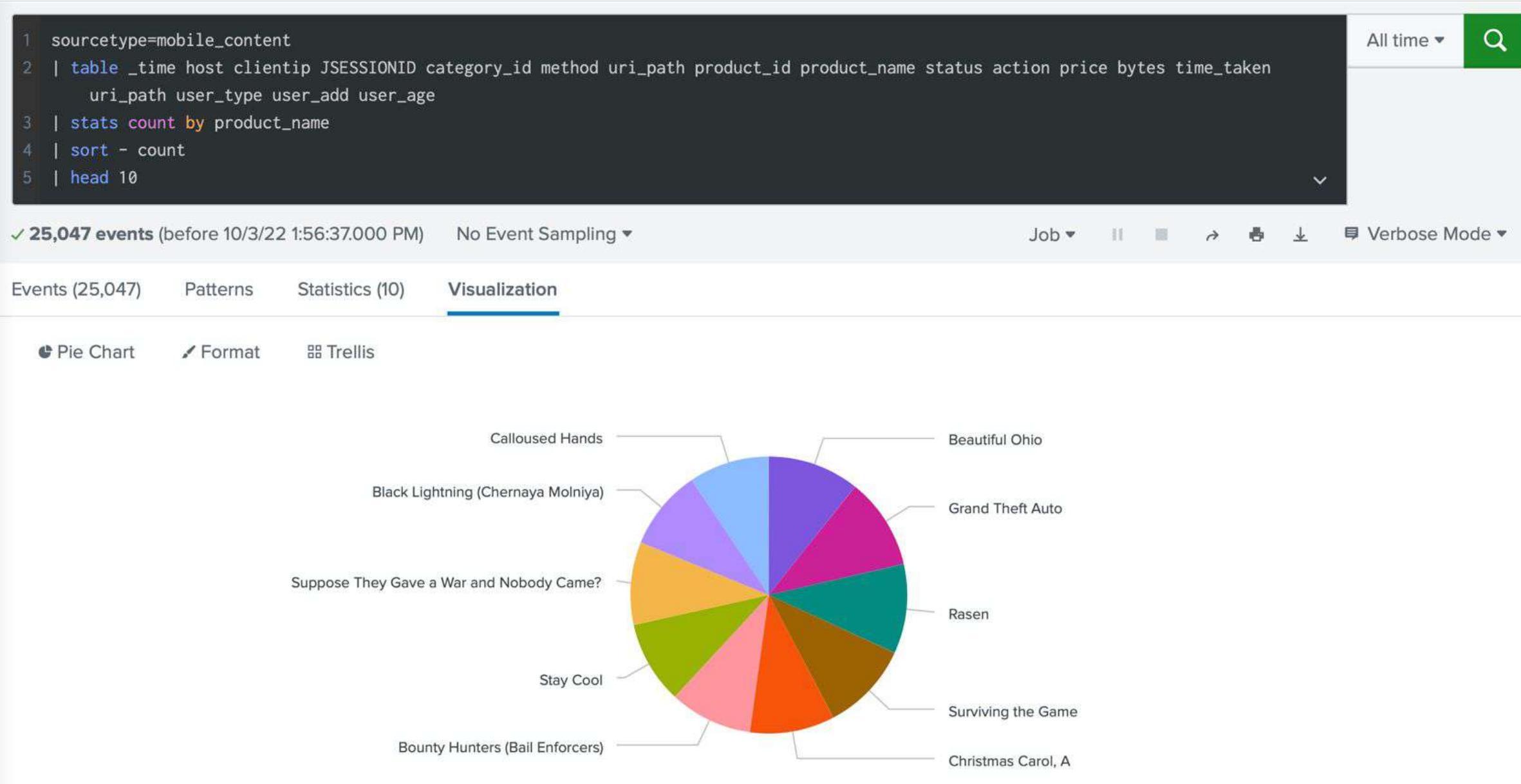
Search Fragment
 | stats count

nk> 41

Analysis Technique 1 : Exercise 1

© 2023 SPLUNK INC.

STEP 04 – Visualization



Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

From the previous total access count analysis, add average time_taken to process the contents. Use avg(time_taken) to aggregate another dimension on the statistics.

The fields that are relevant here are :

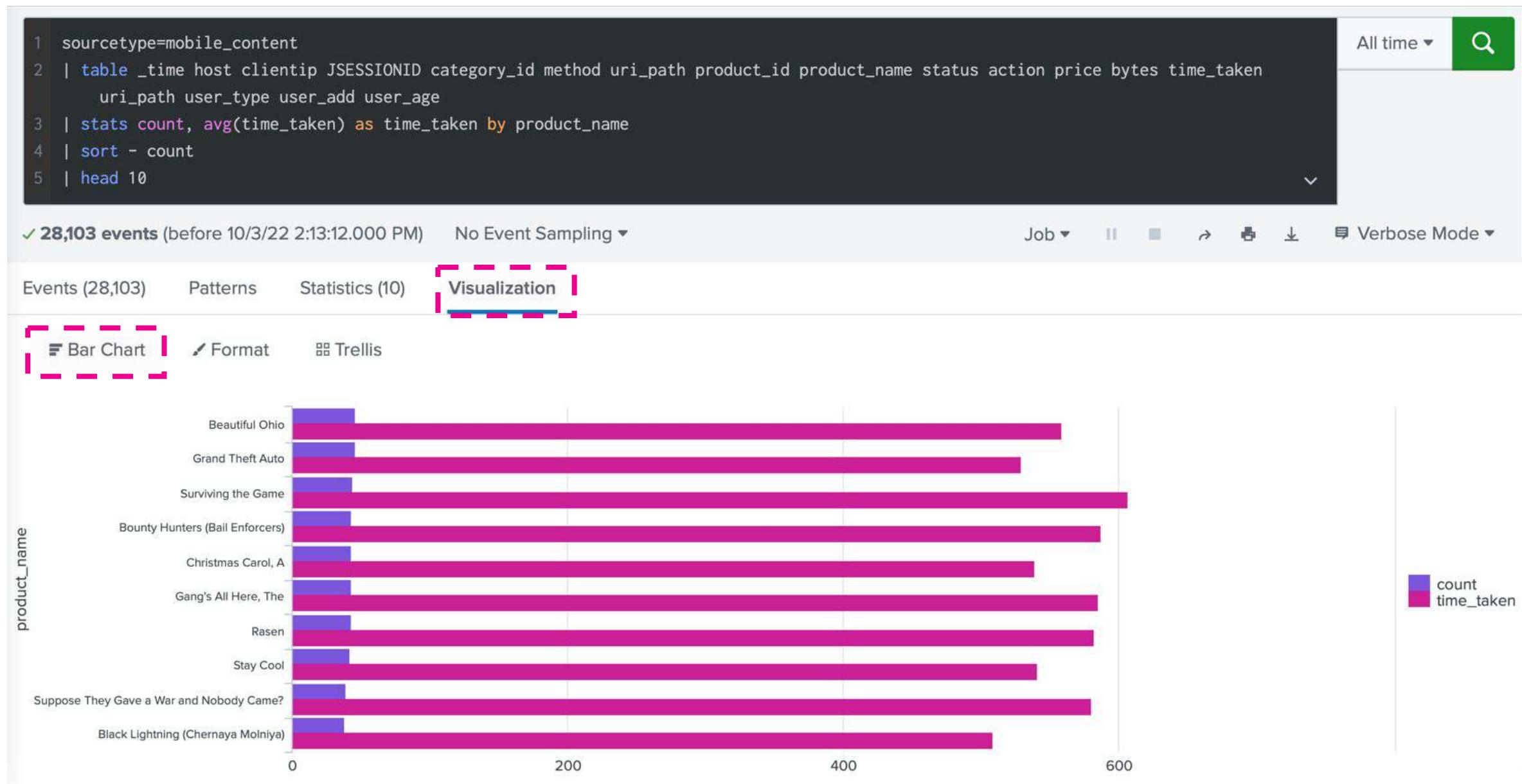
- * product_name, which we want to total split by the produce name
- * timetaken, that represents the amount of ms took to process the request

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age useragent
| stats count, avg(time_taken) as avg_time_taken by product_name
| sort - count
```

product_name	count	time_taken
Beautiful Ohio	46	558.4782608695652
Grand Theft Auto	46	528.9782608695652
Surviving the Game	44	606.6363636363636
Bounty Hunters (Bail Enforcers)	43	587.1395348837209
Christmas Carol, A	43	538.7441860465116
Gang's All Here, The	43	585.7441860465116
Rasen	43	582.4651162790698
Stay Cool	42	541.047619047619

Analysis Technique 1 : Exercise 1

STEP 04 – Visualization



Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

Now let's add multiple aggregate statistics to the analysis. Here are additional functions to add statistics that could be a lot meaningful to see together for the product_name, the content :

- avg(time_taken) : Average time took to process request.
- sum(bytes) : What was the amount of data exchanged?
- dc(clientip) : How many unique users access the content?
- avg(user_age) : What is the average age of viewers?
- last(category_id) : What is the content's category?
- sum(price) : What is the total revenue?

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age user_agent
sourcetype=mobile_content
| stats count, avg(time_taken) as time_taken, sum(bytes) as sum_bytes, dc(clientip) as
uniq_client_cnt, avg(user_age) as avg_user_age, last(category_id) as category, sum(price) as
revenue by product_name
| sort - count
| head 10
```

product_name	count	time_taken	sum_bytes	uniq_client_cnt	avg_user_age	category	revenue
Bounty Hunters (Bail Enforcers)	41	567.0487804878048	85364	41	48.23076923076923	DOCUMENTARY	854
Tears of April (K/\$ky)	37	517.972972972973	79734	37	49.82857142857143	DRAMA:SCI-FI:THRILLER	624
Stay Cool	35	493.4	81054	34	44.885714285714286	DOCUMENTARY:WAR	2165
Beautiful Ohio	34	600.0294117647059	67436	34	53.03125	ACTION:COMEDY	2354
Grand Theft Auto	33	525.7272727272727	78395	33	61.32258064516129	ANIMATION:CHILDREN:FANTASY	2679

Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

One of the powerful ways to calculate statistics is to apply a logical condition on function that matches a condition. In this example when the status code is 500 or more (which means server error) to be only counted. :

```
•count(eval(if(status>=500, clientip, NULL()))) AS process_error_count : What's the total number of server errors when processing the request.
```

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age user_agent
sourcetype=mobile_content
| stats count, count(eval(if(status>=500, clientip, NULL()))) AS process_error_count,
avg(time_taken) as time_taken, sum(bytes) as sum_bytes, dc(clientip) as uniq_client_cnt,
avg(user_age) as avg_user_age, last(category_id) as category, sum(price) as revenue by
product_name
| sort - count
| head 10
```

product_name	count	process_error_count	time_taken	sum_bytes	uniq_client_cnt	avg_user_age	category	revenue
Bounty Hunters (Bail Enforcers)	62		6	552.5483870967741	127795	62	50.166666666666664	ANIMATION:CHILDREN:FANTASY
Beautiful Ohio	58		6	554.1379310344828	120470	58	52.41509433962264	CRIME:DRAMA
Gang's All Here, The	58		9	604.1206896551724	115333	57	48.22	DOCUMENTARY
Stay Cool	57		7	530.2280701754386	132645	56	44.90909090909091	COMEDY:MUSICAL:ROMANCE

nk>

Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

Finally, let's segment more with additional condition. Previously we only used “product_name” as the segmentation, we can split that further with breaking it down further with “product_name” + “host” combination. :

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age user_agent
sourcetype=mobile_content
| stats count, count(eval(if(status>=500, clientip, NULL()))) AS process_error_count,
avg(time_taken) as time_taken, sum(bytes) as sum_bytes, dc(clientip) as uniq_client_cnt,
avg(user_age) as avg_user_age, last(category_id) as category, sum(price) as revenue by
product_name host
| sort - count
| head 10
```

product_name	host	count	process_error_count	time_taken	sum_bytes	uniq_client_cnt	avg_user_age	category
Bounty	mobile-content-02.mytelco.com	29	4	610.6206896551724	57638	29	53.074074074074076	DOCUMENTARY
Hunters (Bail Enforcers)	mobile-content-02.mytelco.com	27	6	534.5185185185185	63294	27	50.73913043478261	DRAMA
Christmas Carol, A	mobile-content-01.mytelco.com	27	4	571.2222222222222	57492	27	56.26923076923077	ANIMATION:COMEDY:SCI-FI

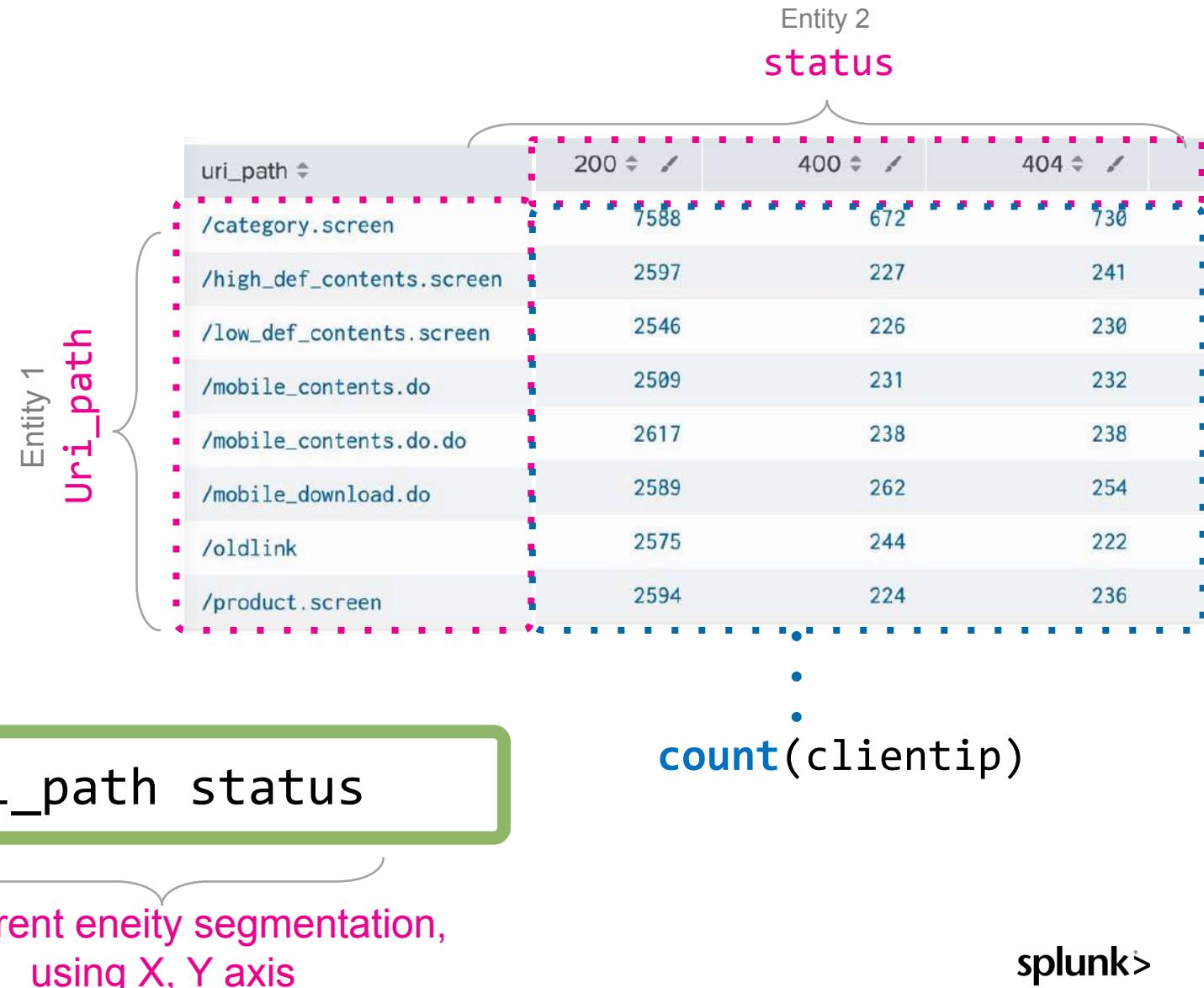


Technique 2 Matrix / Pivot Analysis

splunk>

Analysis Technique 2 : Matrix / Pivot

- ✓ Using `chart` command
- ✓ Matrix analysis, pivot analysis
- ✓ Goal : Compare using **2 different entity segmentation** for a single calculation **function**.



Analysis Technique 2 : Matrix / Pivot

Syntax :

```
chart func(field_3) over field_1 by field_2  
chart func(field_3) by field_1, field_2
```

Examples :

```
* | chart count(clientip) by uri_path, status
```

Field Name uri_path	Field Name status			
	200	400	404	406
/category.screen	7588	672	730	695
/high_def_contents.screen	2597	227	241	241
/low_def_contents.screen	2546	226	230	233
/mobile_contents.do	2509	231	232	266
/mobile_contents.do.do	2617	238	238	267
/mobile_download.do	2589	262	254	231

A pink arrow points from the 'status' column header to the 404 column. A pink arrow points from the 'uri_path' field name to the first column. A pink dashed box highlights the cell containing the value 226 in the row for '/low_def_contents.screen' and the column for '404'. To the right of the table, the text '... count(clientip)' is shown with ellipses indicating continuation.

EXERCISE #2

New Search

```
1 sourcetype=access_combined product_name=* result_code=*
2 | table _time host serial category product_id product_name result_code price unit_count uri_path
3 | chart sum(unit_count) as unit_count by product_name result_code
```

Last 24 hours 

✓ 14,927 events (2/15/21 4:00:00.000 PM to 2/16/21 4:46:57.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (14,927) Patterns Statistics (10) Visualization

product_name mat Preview ▾

product_name	cancelled	completed	failed	progress	rerun
display_lg	18852	19498	20537	19419	18932
display_sm	19668	20159	19668	19330	18620
ecu	9156	9822	8976	10705	9191
engine_hv	9249	8077	10048	10066	10602
engine_sv	10359	9910	9242	8975	9389
motor_hv	9120	8724	8329	9421	8621
motor_sv	10159	10268	10289	9161	9345
suspension	9287	11442	10513	9699	12374
transformer	18793	22916	19520	18932	18583
transmission	8703	9038	8344	9067	8872

Analysis Technique 2 : Exercise 2

STEP 01 – Select manufacturing data

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add
user_age
| chart count by uri_path status
```

Last 24 hours ▾



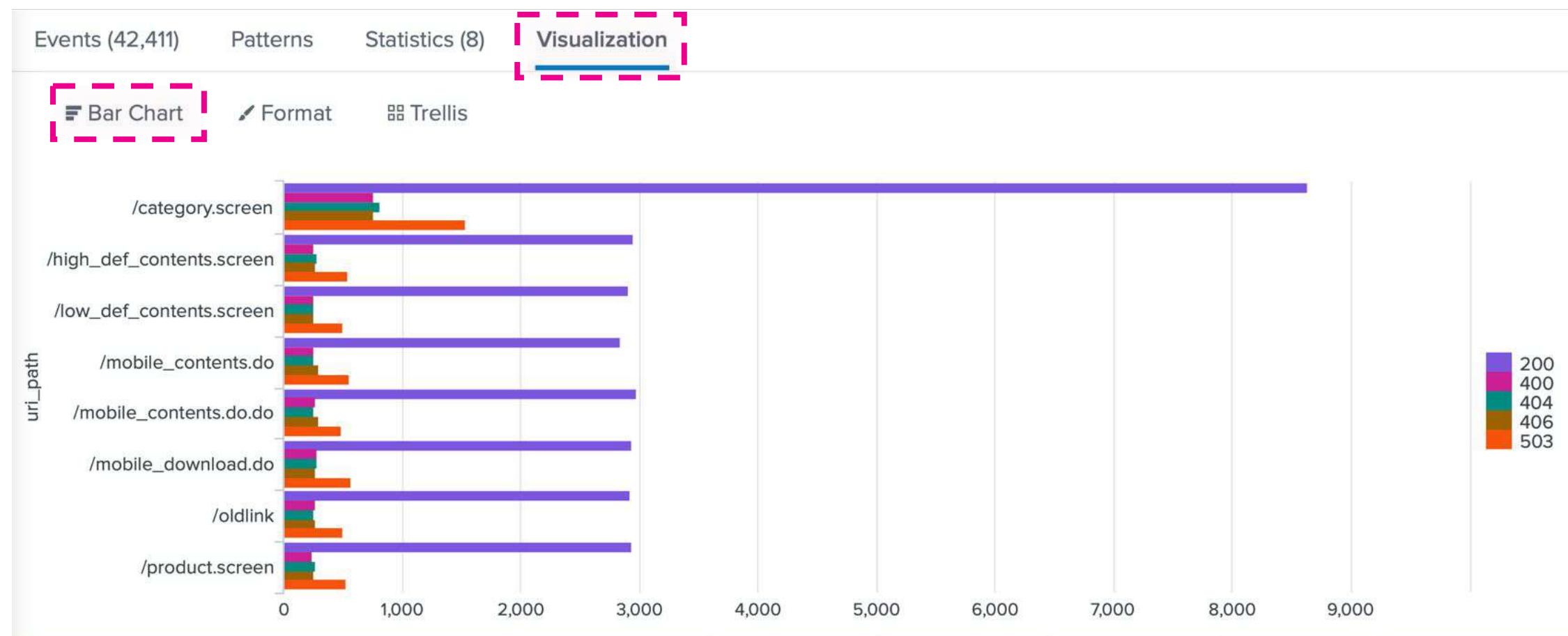
uri_path	200	400	404	406	503
/category.screen	8137	718	779	735	1448
/high_def_contents.screen	2780	248	264	261	526
/low_def_contents.screen	2731	241	245	247	472
/mobile_contents.do	2691	247	244	290	533
/mobile_contents.do.do	2809	257	255	282	460
/mobile_download.do	2779	274	270	251	529
/oldlink	2754	263	236	249	463

Analysis Technique 2 : Exercise 2

STEP 01 – Select manufacturing data

```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add  
user_age  
| chart count by uri_path status
```

Last 24 hours ▾



Analysis Technique 2 : Exercise 2

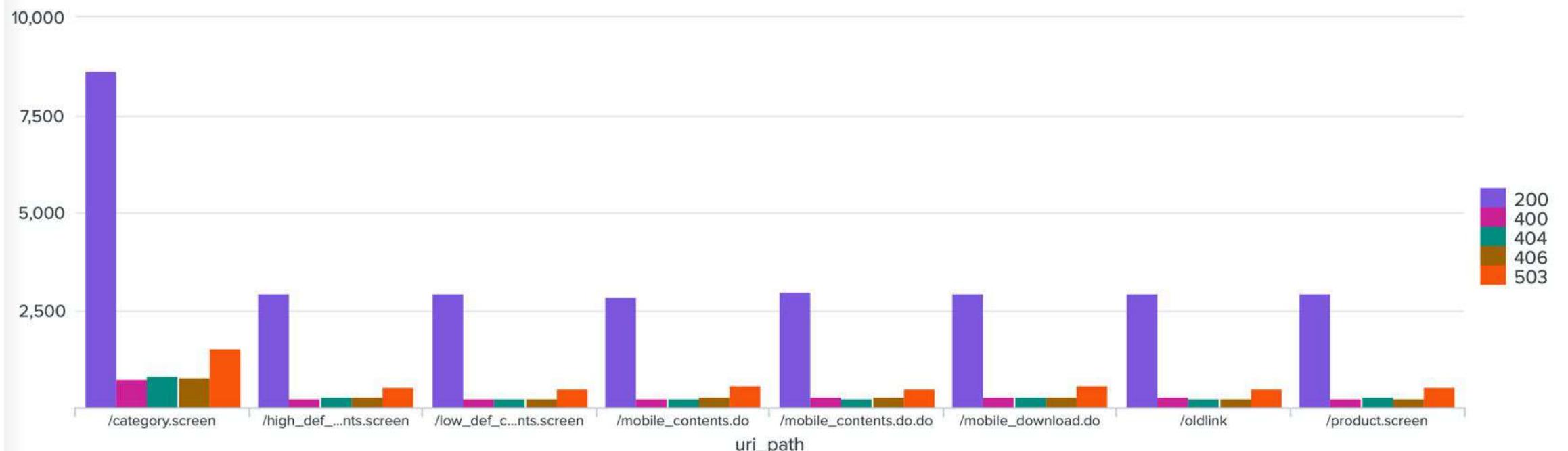
STEP 01 – Select manufacturing data

```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add  
user_age  
| chart count by uri_path status
```

Last 24 hours ▾



Events (42,411) Patterns Statistics (8) **Visualization**
Column Chart Format Trellis



k>

Analysis Technique 2 : Exercise 2

STEP 01 – Select manufacturing data

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add
user_age
| chart sum(price) by product_name action
| sort - skip
```

Last 24 hours ▾



product_name	download	download_remove	local_view	purchase	resume	skip	stream
Haunted, The	98	294	196	294	294	882	196
Enfer, L'	285	380	475	95	380	665	190
The Mascot	364	637	455	364	182	637	273
Home Page	198		66	264	198	594	264
Mala Noche	285	190	475	190	285	570	380
Quick and the Dead, The	188	658	564	94	94	564	376
Matter of Dignity, A (To teleftaio psema)	210	280	210	140	210	560	140
Kidnapping of the President, The	279	186	186	465	279	558	93



Technique 3 3D Matrix / Trend Analysis

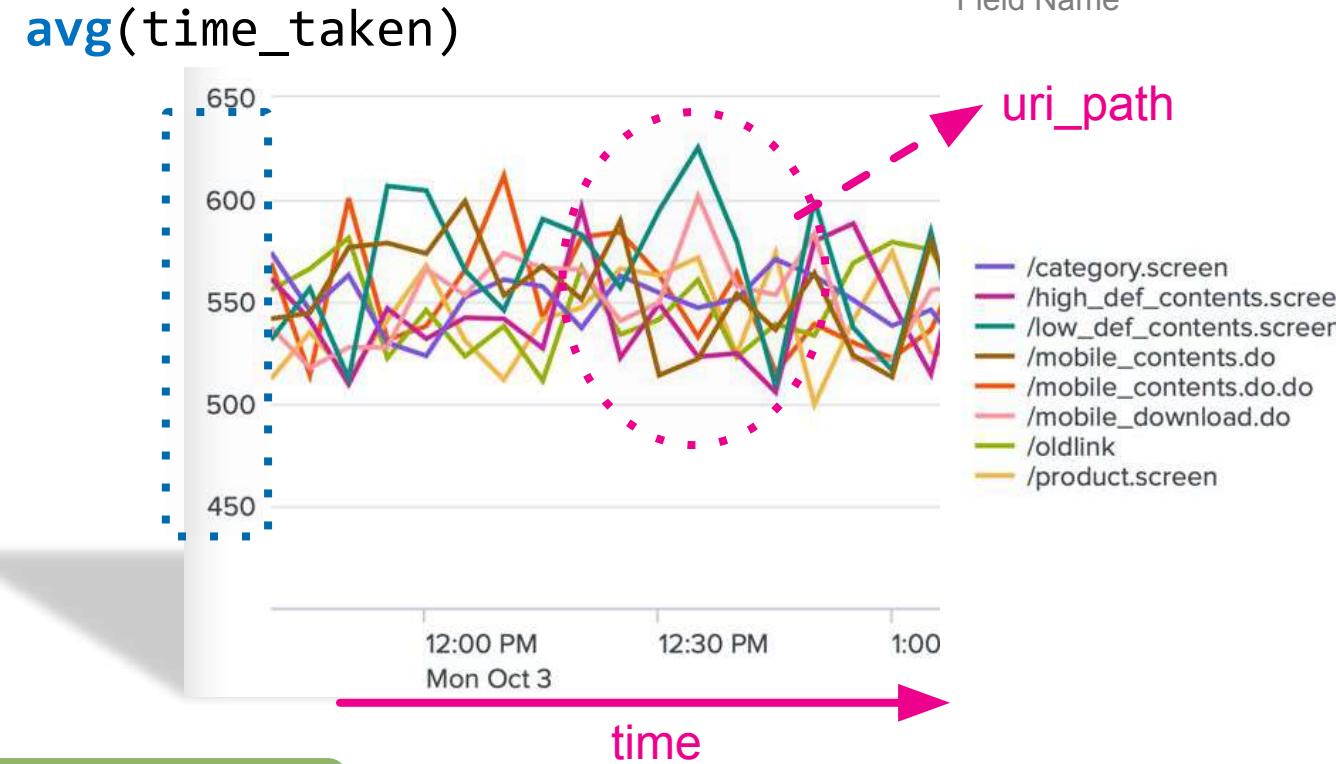
Analysis Technique 3 : 3D Matrix / Trend

- ✓ Using `timechart` Command
- ✓ 3D Matrix / trend analysis
- ✓ Goal : Visualize a **single trend** or compare **multiple trends** group by a **single entity segmentation**.

Function

```
timechart avg(time_taken) by uri_path
```

Group by segmentation



Analysis Technique 3 : 3D Matrix, Trend

Syntax :

```
timechart func(field), func(field), .. by field
```

Examples :

```
* | timechart count by host  
* | timechart avg(time_taken) by uri_path  
* | timechart avg(time_taken), sum(bytes) by uri_path
```

```
* | timechart count(eval(status="200")) as SUCCESS,  
count(eval(result_code="503")) as FAILS by uri_path
```

EXERCISE #3

New Search

```
1 sourcetype=access_combined product_name=* result_code=*
2 | table _time host serial category product_id product_name result_code price unit_count uri_path user_add
3 | timechart sum(unit_count) as unit_count by result_code
```

127 of 237 events matched No Event Sampling ▾

Events (127) Patterns Statistics (60) **Visualization**

Line Chart Format Trellis

5:49:25 PM
Tue Feb 16
2021

Save As ▾ Create Table View Close

1 minute window ▾ **1**

Presets

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute Window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

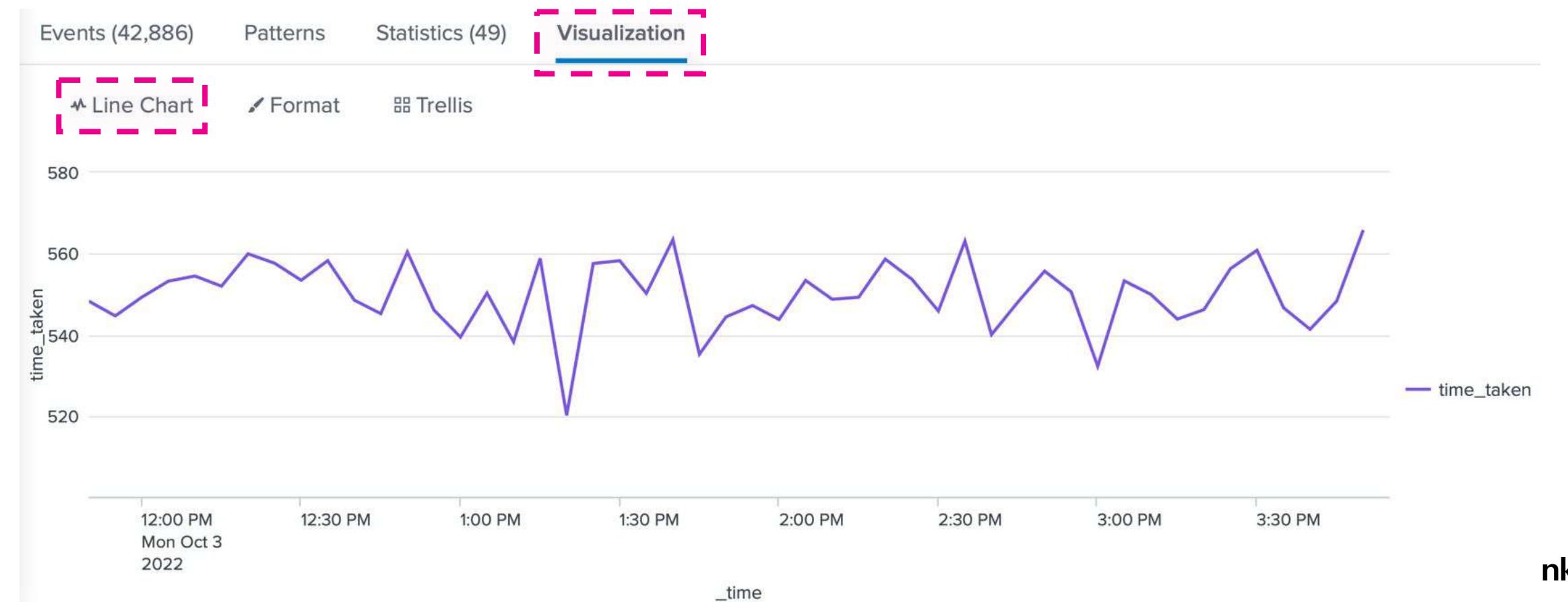
2

> Relative
> Real-time
> Date Range
> Date & Time Range
> Advanced

Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

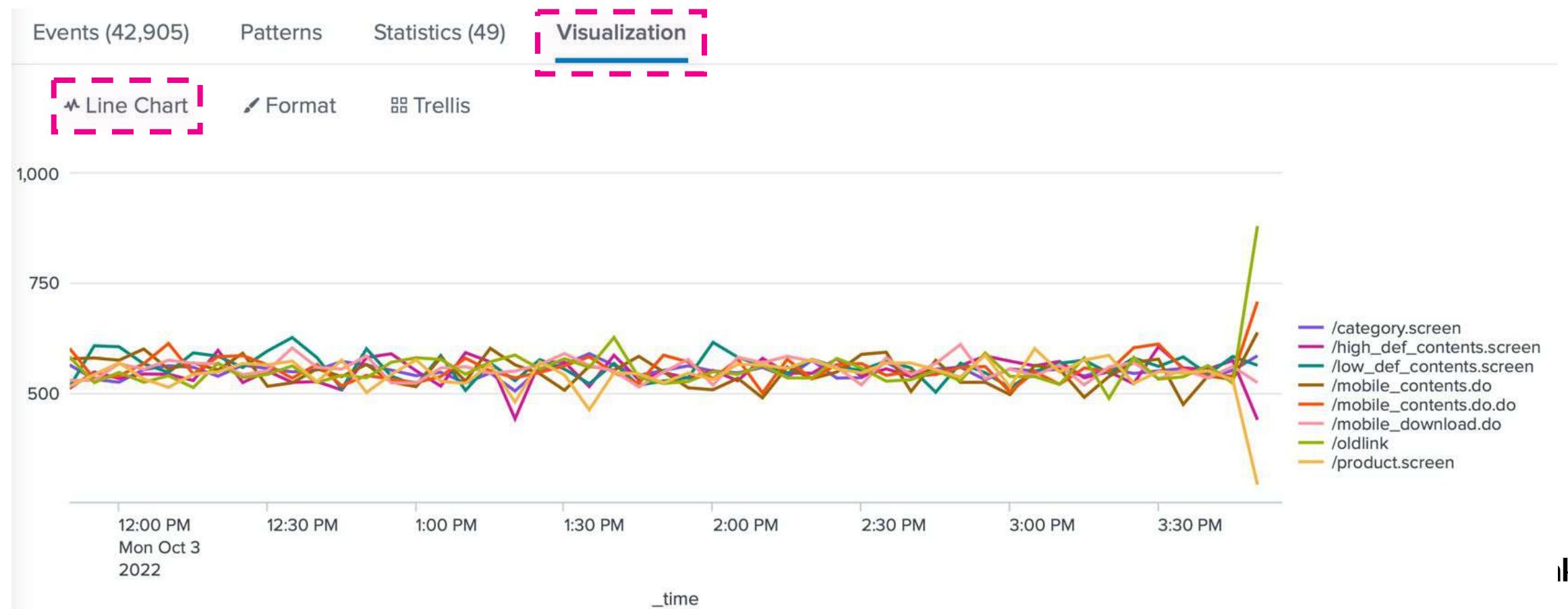
```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add user_age  
useragent  
| timechart avg(time_taken) as time_taken
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

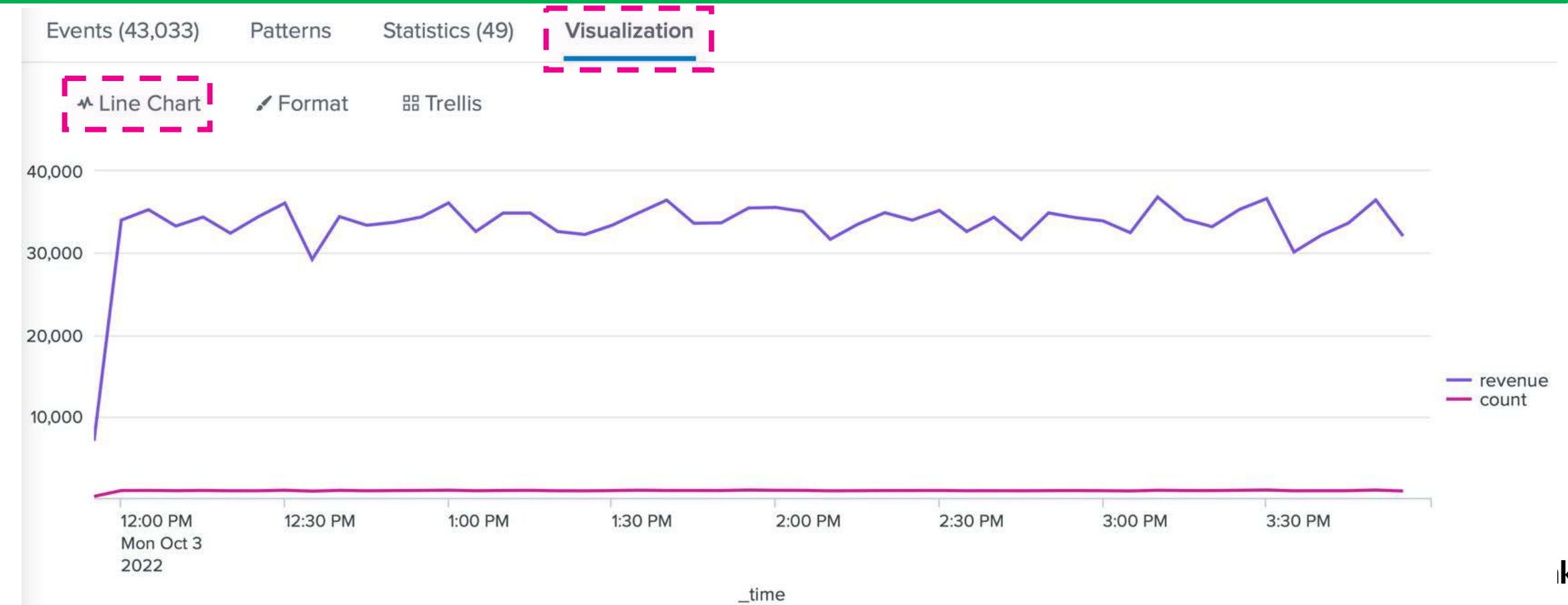
```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add user_age  
useragent  
| timechart avg(time_taken) as time_taken by uri_path
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

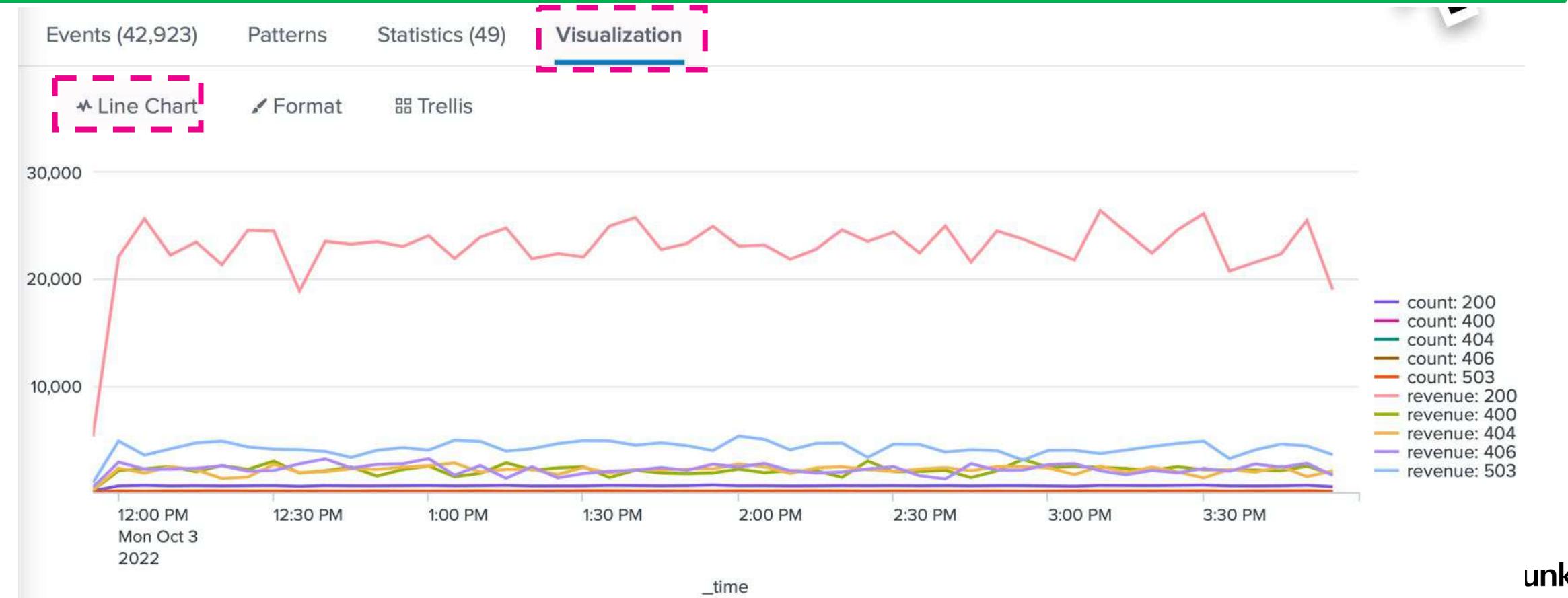
```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add user_age  
useragent  
| timechart sum(price) as revenue, count
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

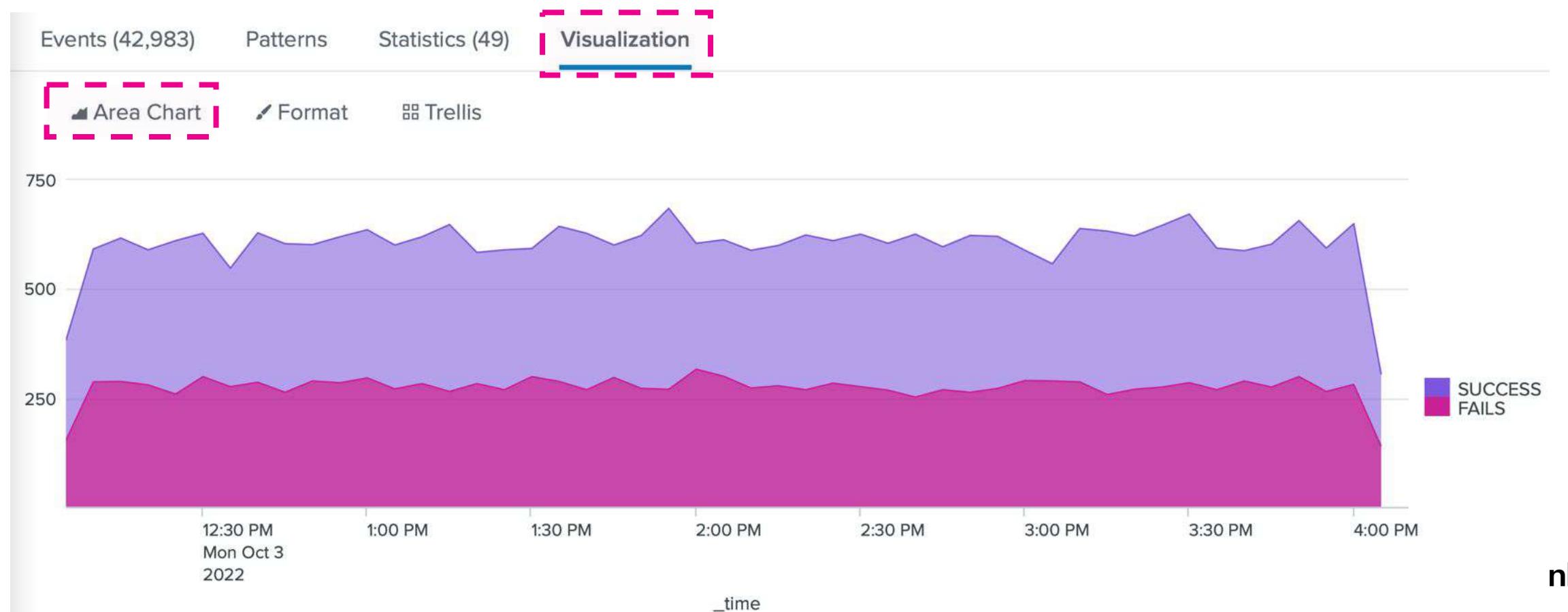
```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add user_age  
useragent  
| timechart sum(price) as revenue, count by status
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

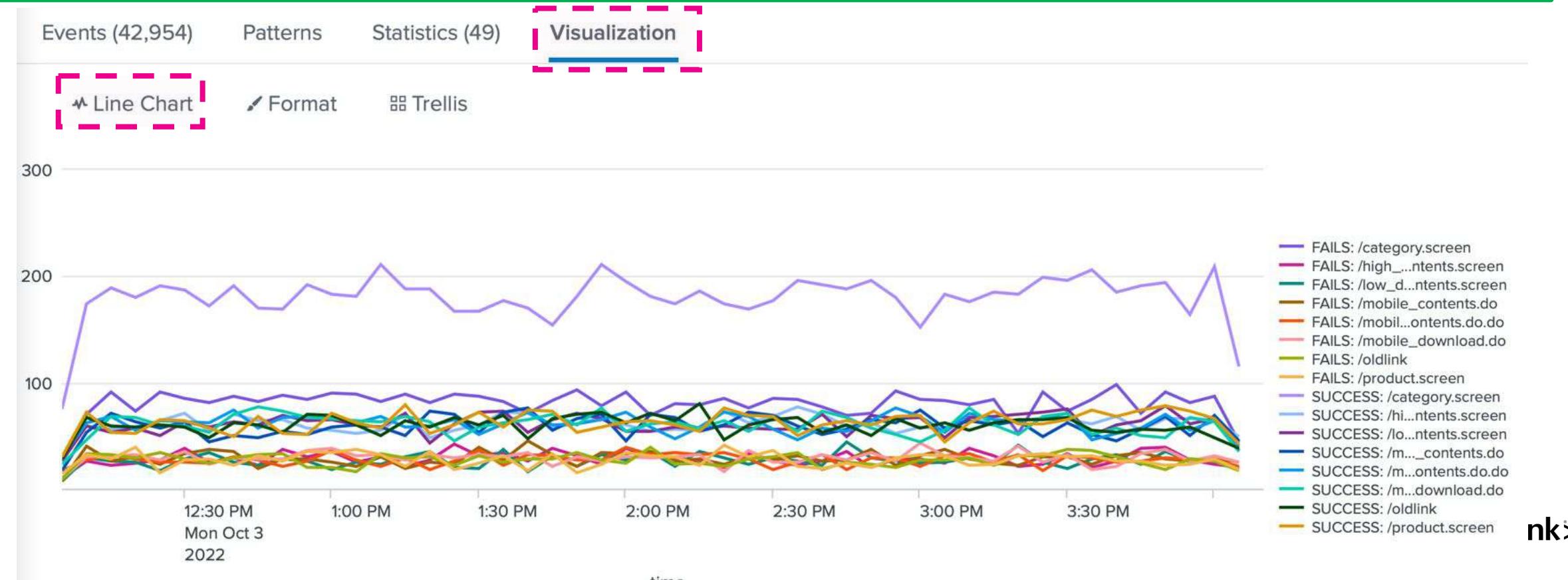
```
sourcetype=mobile_content  
| table _time host clientip JSESSIONID category_id method uri_path product_id  
product_name status action price bytes time_taken uri_path user_type user_add user_age  
useragent  
| timechart count(eval(status<300)) as SUCCESS, count(eval(status>=400)) as FAILS
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart count(eval(status<300)) as SUCCESS, count(eval(status>=400)) as FAILS by
uri_path
```

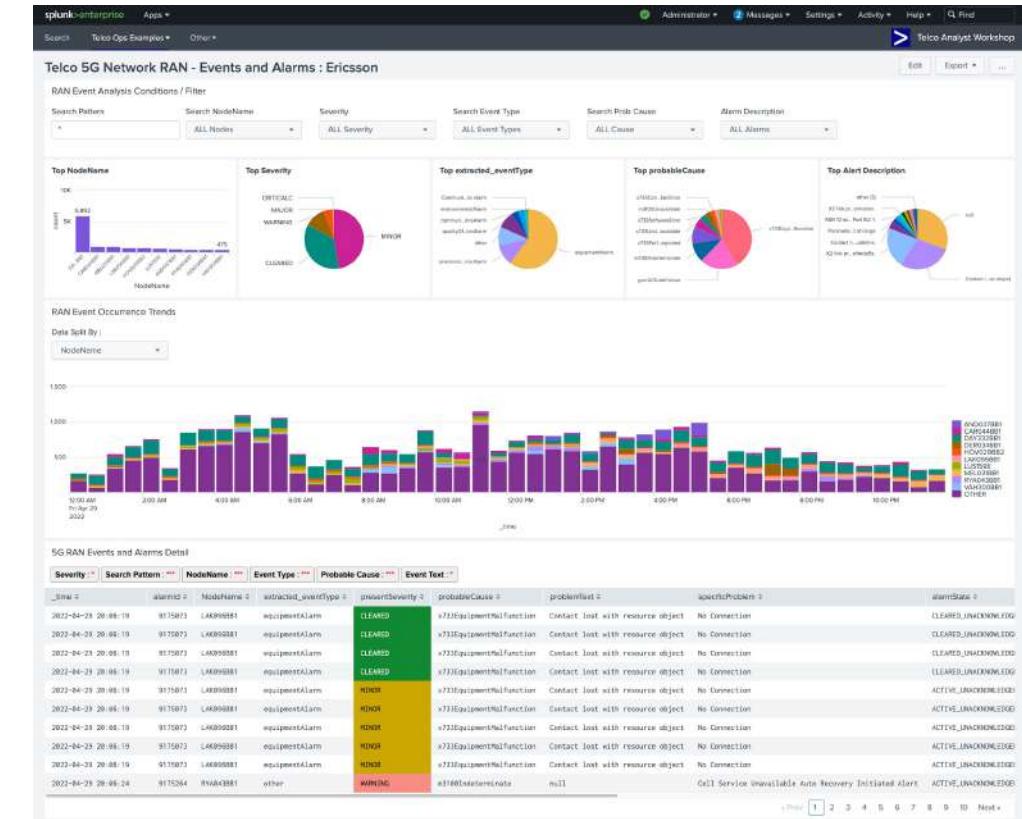


Telco Operational Dashboard

Create 2 Operational Dashboard Content operational dashboard



5G RAN alarm analysis



Create Content Ops Dashboards



Content operations dashboard

Telco Content Service - Operations Dashboard

Session success rate

Session status trends

Types of user device

Transaction details

The dashboard displays several key performance indicators (KPIs) and trend charts:

- SLA KPI:** Success rate in last 5 Min: 86.8%.
- Service Performance:** Total Access: 103, Error Sessions: 23, Missing API: 8.
- Active Users:** 147.
- Device Types:** 9.
- Accessed Contents:** 79.
- Web Process Status Trend:** A stacked bar chart showing activity over time from 3:07:00 AM Sun Dec 4 2022 to 3:11:45 AM Sun Dec 4 2022. The legend indicates values ranging from 200 to 503.
- Top User Device Activity:** A horizontal bar chart showing device types and their counts. The top devices are Linux, iPhone, iPad, X11, compatible, iPhone14, CrKey, iPhone13, iPhone12, and Apple.
- Top Device with Experiencing Errors:** A pie chart showing the distribution of error types. The largest category is Linux, followed by iPhone, iPad, and compatible.
- Top Browser Type Access Trend:** A line chart showing the trend of browser types over time. The legend includes Mozilla, Opera, and others.
- Failed Content Purchase Transactions:** A table listing failed transactions with columns: _time, status, status_description, product_name, clientip, JSESSIONID, action, device_type, other, price, product_id, user, user_add, and user_age.



Dashboard 1 : Content operations dashboard

Show service success rate trends over time, based on web status code.

Tasks:

1. Show success rate for web sessions.
Aggregate number of failed session vs other sessions.
 - Failed sessions : status => 500
 - All sessions : status < 500
2. Use a timechart command to generate "Success rate trend" over time.

Goal:



Dashboard 1 : Content operations dashboard

Show service success rate trends over time, based on web status code.

Solution:

```
sourcetype=mobile_content
| timechart count by status
| addtotals
| rename "503" as FAIL
| eval SLA=((Total-FAIL)/Total)*100
| table _time SLA
```

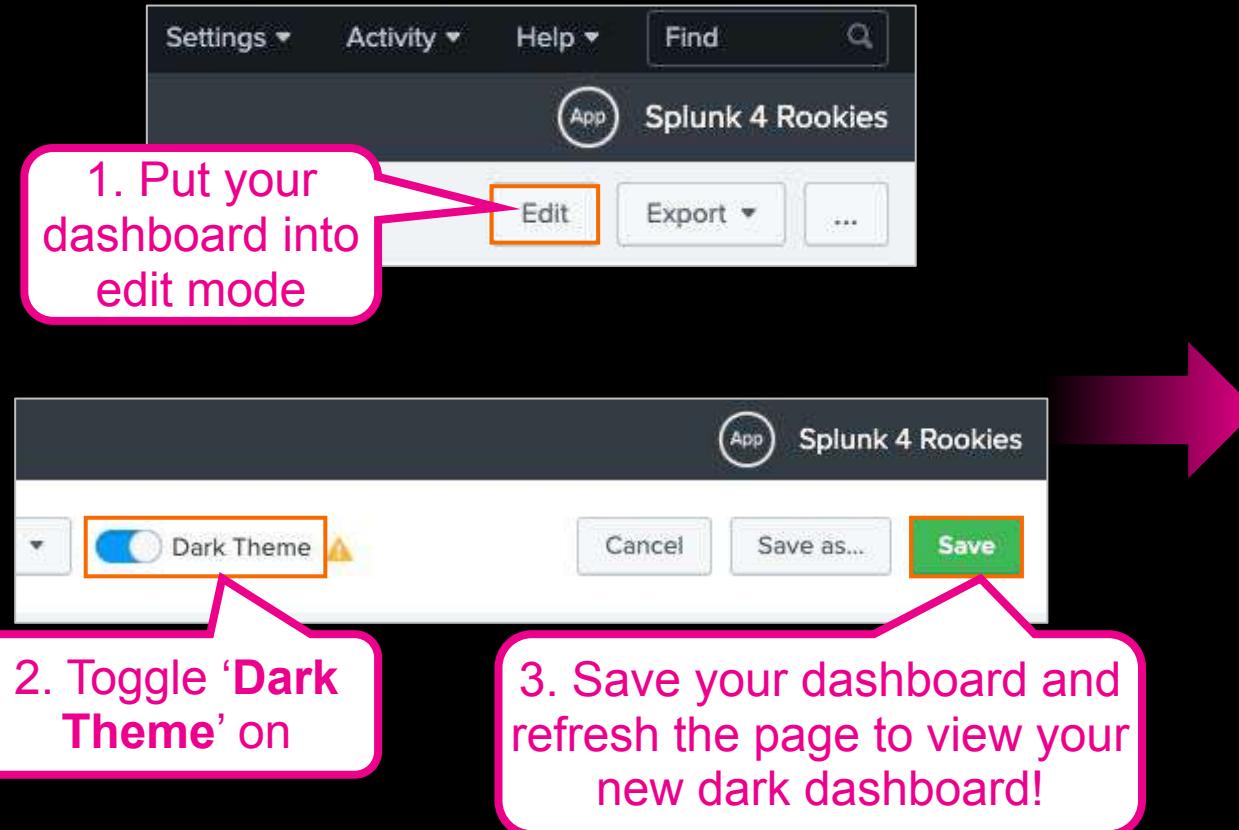
_time	SLA
2022-12-04 02:35:00	86.36363636363636
2022-12-04 02:36:00	87.36263736263736
2022-12-04 02:37:00	89.44444444444444
2022-12-04 02:38:00	87.97814207650273
2022-12-04 02:39:00	84.88372093023256
2022-12-04 02:40:00	87.95811518324688
2022-12-04 02:41:00	84.30232558139535
2022-12-04 02:42:00	88.27160493827161

The screenshot shows the Splunk Enterprise search interface. A search bar at the top contains the following SPL command:

```
sourceType=mobile_content
| fields + *
| timechart count by status
| addtotals
| rename "503" as FAIL
| eval SLA=((Total-FAIL)/Total)*100
| table _time SLA
```

The results pane shows 10,840 events from December 4, 2022, between 02:35:00 and 02:42:00. The visualization tab is selected, indicated by a pink arrow pointing to it. A hand cursor is clicking on the '42' icon in the recommended visualizations section, which is highlighted with a pink box and numbered 2. Another hand cursor is clicking on the 'New Dashboard' button in the top right corner of the search bar area, which is highlighted with a pink box and numbered 4. A pink circle labeled 1 is on the visualization tab. A pink circle labeled 3 is on the 'Save As' dropdown menu, which is open and shows options like Report, Alert, Existing Dashboard, New Dashboard, and Event Type. A pink circle labeled 4 is on the 'New Dashboard' button.

Try Dark Mode!



Dashboard 1 : Content operations dashboard

Show service success rate trends over time, based on web status code.

Solution:

Use your initial in the front of the view name

Save Panel to New Dashboard

Dashboard Title: YC Content Ops Overview
yc_content_ops_overview

Description: Content Ops Health Dashboard

Permissions: Private

How do you want to build your dashboard?

Classic Dashboards: The traditional Splunk dashboard builder

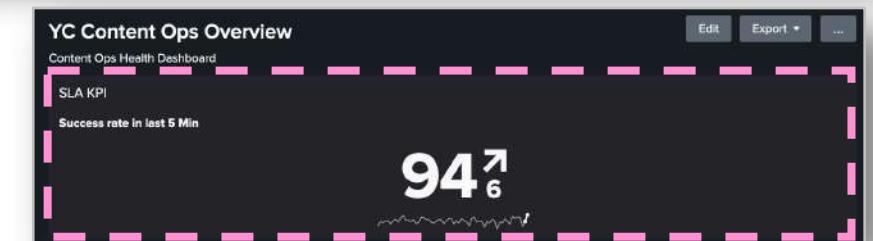
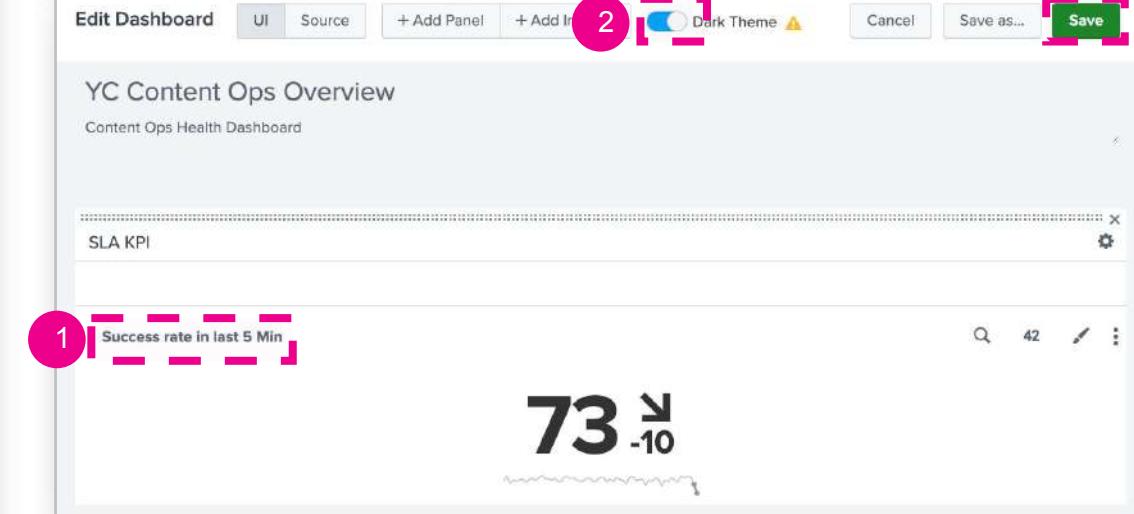
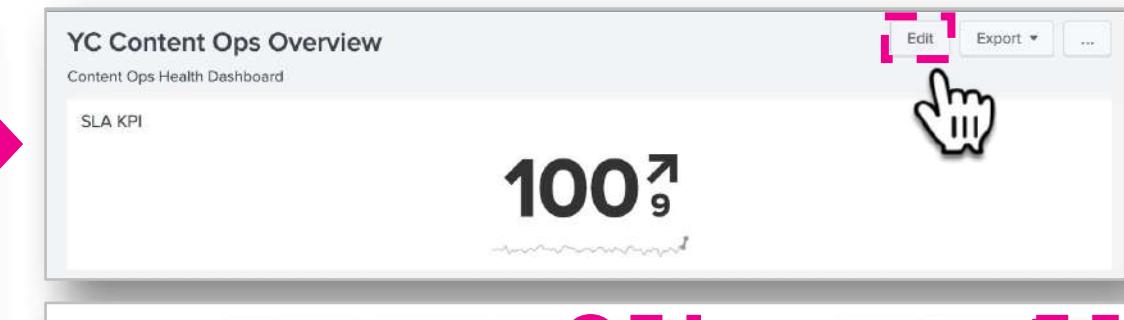
Dashboard Studio NEW: A new builder to create visually-rich, customizable dashboards

Panel Title: SLA KPI

Visualization Type: Single Value

Advanced Panel Settings

Cancel Save to Dashboard



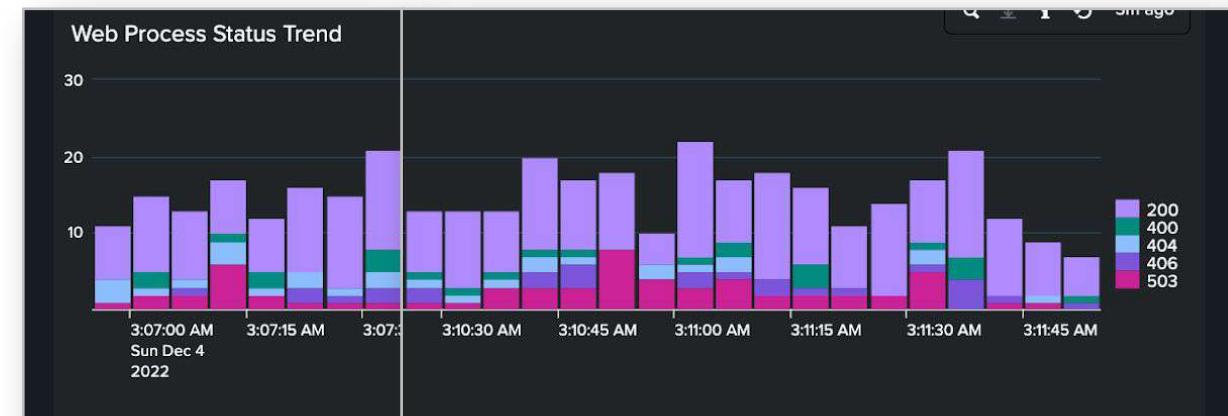
Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Tasks:

1. Show the trend of session process status by using status code
2. Use a timechart command split by the status code return codes.

Goal:



Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:

```
sourcetype=mobile_content
| timechart count by status
```

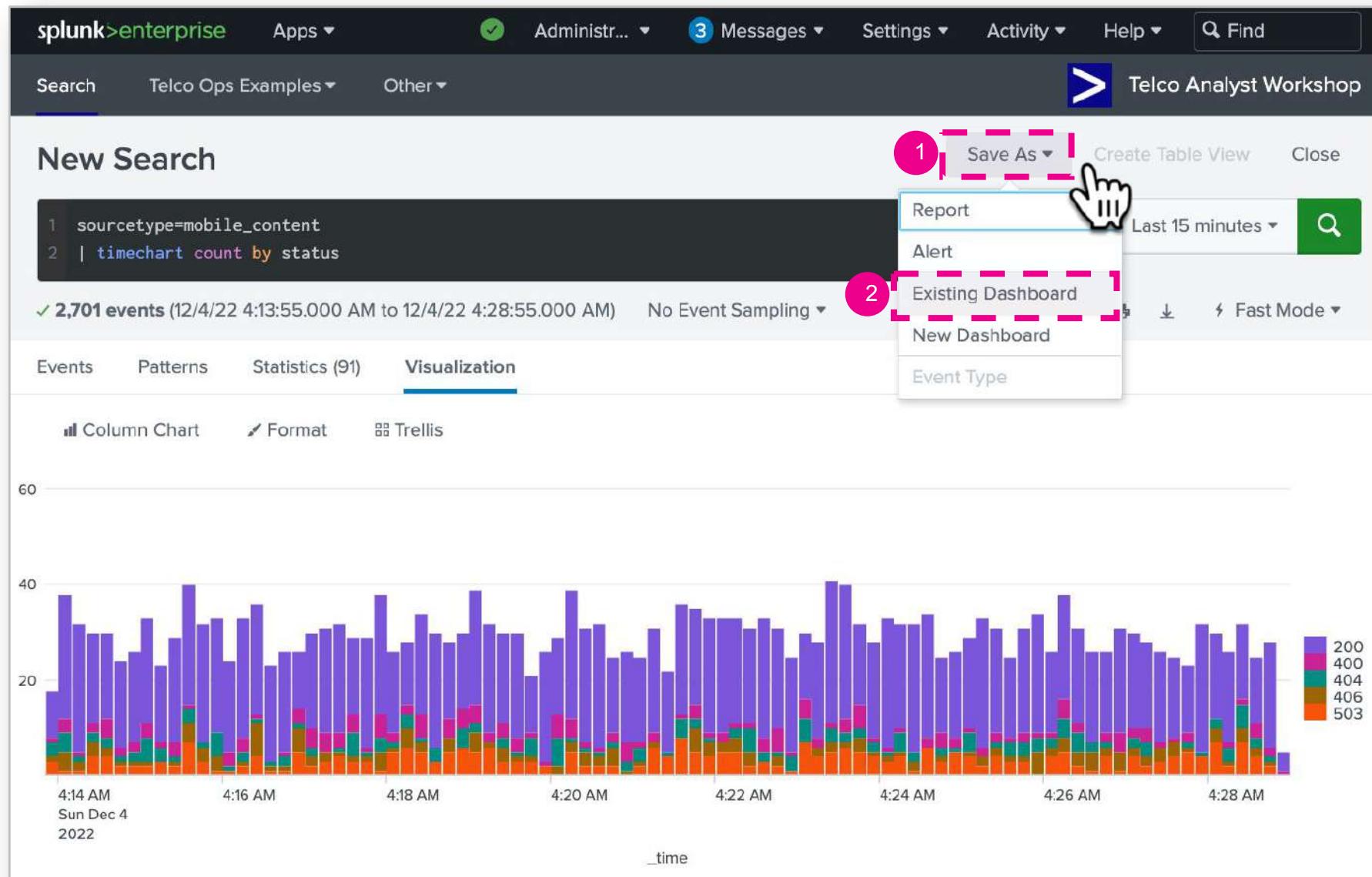
The screenshot shows the Splunk search interface. At the top, there are tabs for Events, Patterns, Statistics, and Visualization. The Visualization tab is selected, indicated by a pink circle with the number 1. Below the tabs, there are several visualization icons: Column Chart, Format, and Trellis. A pink circle with the number 2 points to the Column Chart icon. The main area displays a recommended visualization for a "Column Chart" showing data from 4:18 AM to 4:19 AM. The chart has multiple colored bars representing different status codes. At the bottom, there is a section for "Column Chart" with instructions to "Compare values or fields" and a search fragment: "stats count by comparison_category".

The screenshot shows the configuration interface for the visualization. At the top, there are tabs for Events, Patterns, Statistics (91), and Visualization. The Visualization tab is selected, indicated by a pink circle with the number 4. Below the tabs, there are sections for General, X-Axis, Y-Axis, Chart Overlay, and Legend. On the right, there are buttons for Stack Mode (Yes, No), Multi-series Mode (Yes, No), and Show Data Values (Off, On, Min/Max). A pink circle with the number 3 points to the "Format" tab. A pink dashed box highlights the "Stack Mode" button, which is set to "Yes". The bottom of the screen shows a preview of the stacked bar chart with multiple colored segments representing different status codes over time.

Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:



Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:

Save Panel to Existing Dashboard

Select an Existing Dashboard Sort: Title (A - Z) ↓

Search By Title

Live Dataflow

Telco 5G Network RAN - Events and Alarms : Ericsson

Telco 5G Network RAN - PM Power Consumption to FM Fan Failures

Telco Content Service - Operations Dashboard

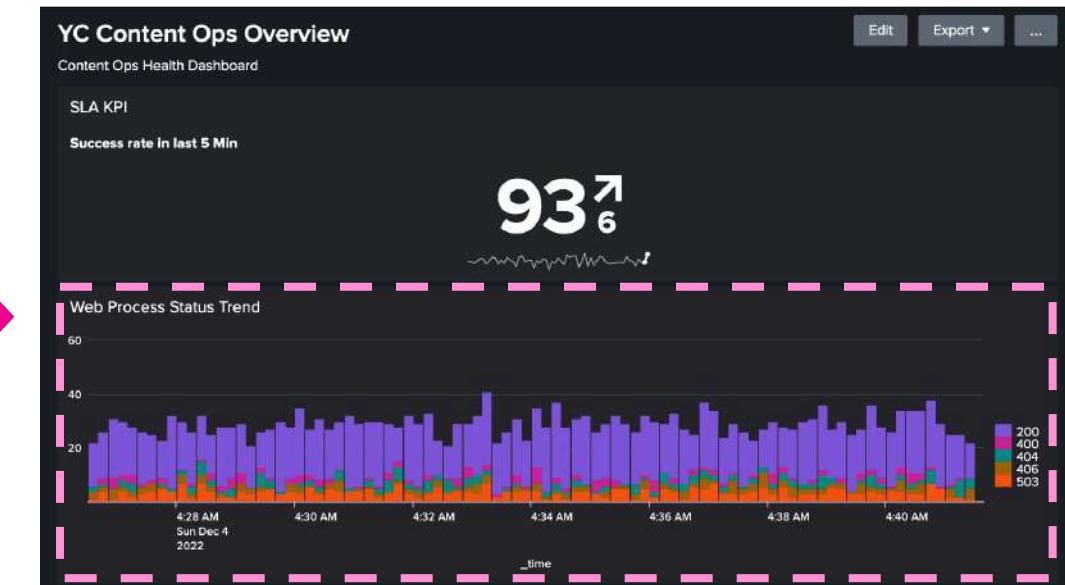
YC Content Ops Overview

Panel Title Web Process Status Trend

Visualization Type Column Chart Statistics Table

Advanced Panel Settings

Cancel **Save to Dashboard**



Dashboard 1 : Content operations dashboard

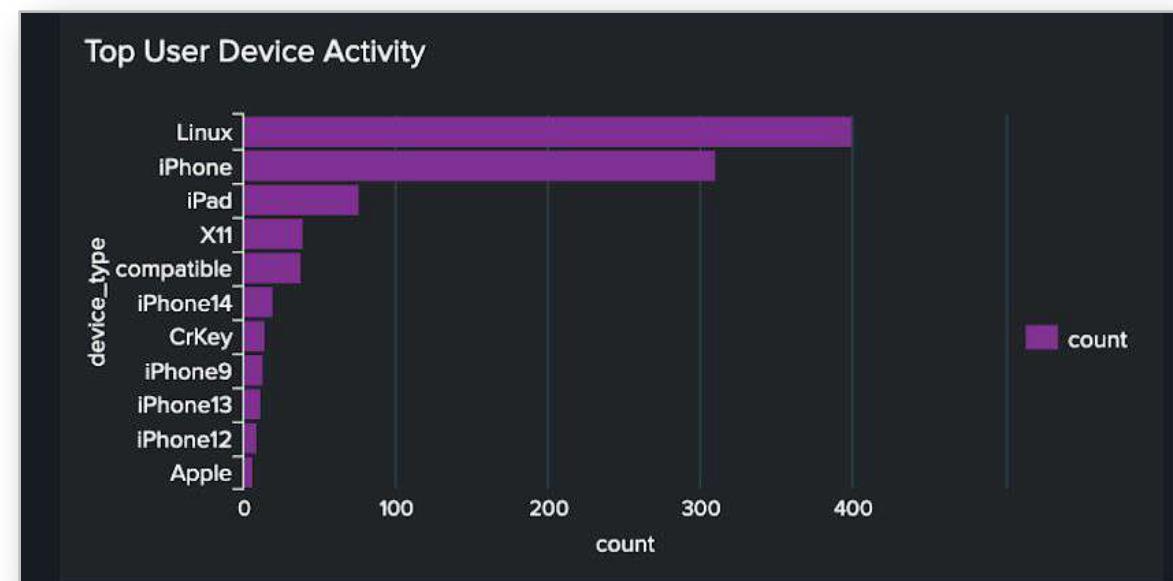
Show top device type access requests



Tasks:

1. Show the aggregated session request totals by device type
 - Field : device_type
2. Use stats command to calculate simple aggregated counts
 - Function : count
3. Sort the highest number of device types access from the top.
 - Command : sort - count

Goal:



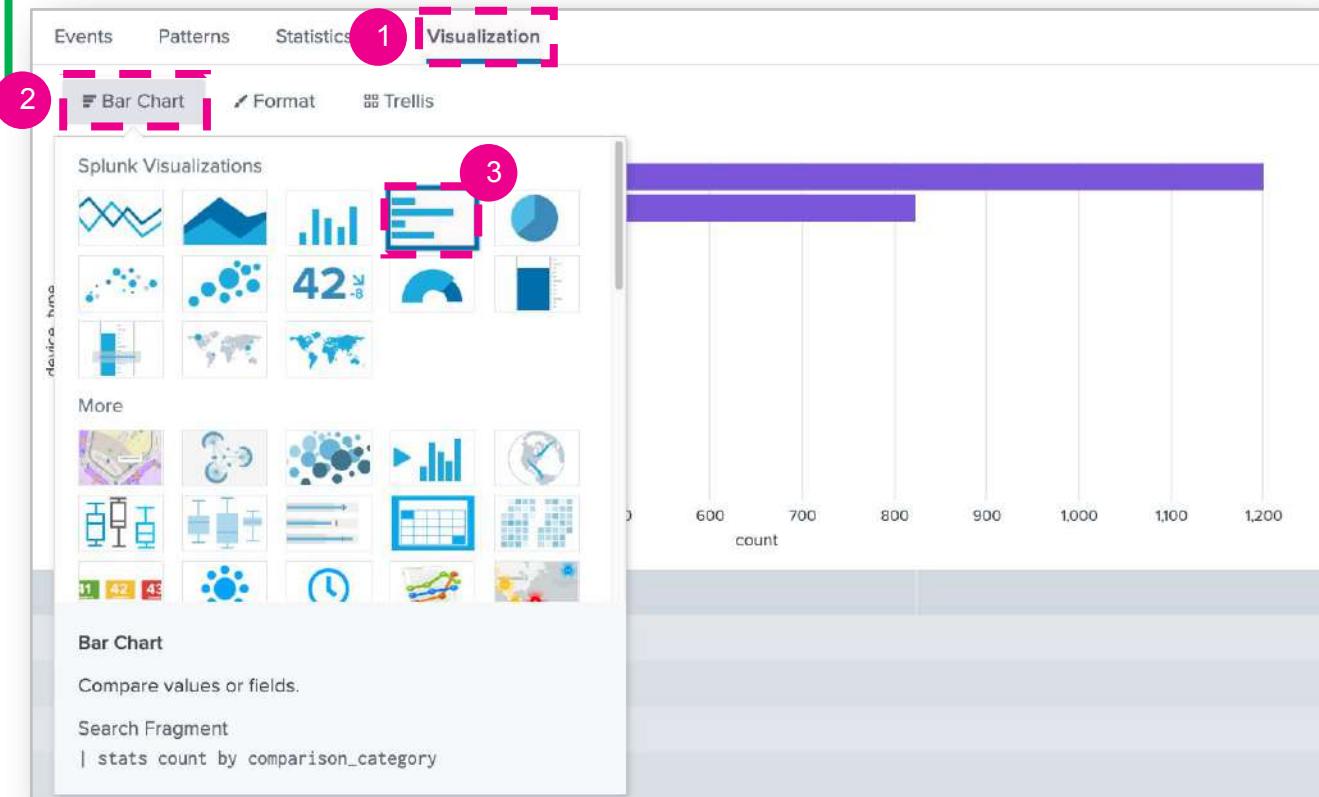
Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

```
sourcetype=mobile_content  
| stats count by device_type  
| sort - count
```

device_type	count
Linux	1201
iPhone	824
iPad	194
X11	105
compatible	79
iPhone14	68
iPhone9	54
iPhone13	40
CrKey	39
Apple	35
iPhone12	35



Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

New Search

```
1 sourcetype=mobile_content  
2 | stats count by device_type  
3 | sort - count
```

✓ 2,674 events (12/4/22 4:29:35.000 AM to 12/4/22 4:44:35.000 AM) No Event Sampling ▾

Events Patterns Statistics (11) Visualization

Bar Chart Format Trellis

device_type

device_type	count
Linux	1201
iPhone	824
iPad	194
X11	~110
compatible	~80
iPhone14	~70
iPhone9	~60
iPhone13	~50
CrKey	~40
Apple	~30
iPhone12	~20

1 Save As ▾ Create Table View Close

Report Last 15 minutes ▾

Alert

2 Existing Dashboard

New Dashboard

Event Type

Fast Mode ▾

splunk>

Dashboard 1 : Content operations dashboard

Show service success rate trends over time, based on web status code.

Solution:

Save Panel to Existing Dashboard

Select an Existing Dashboard Sort: Title (A - Z) ↓

Search By Title

- Live Dataflow
- Telco 5G Network RAN - Events and Alarms : Ericsson
- Telco 5G Network RAN - PM Power Consumption to FM Fan Failures
- Telco Content Service - Operations Dashboard
- YC Content Ops Overview

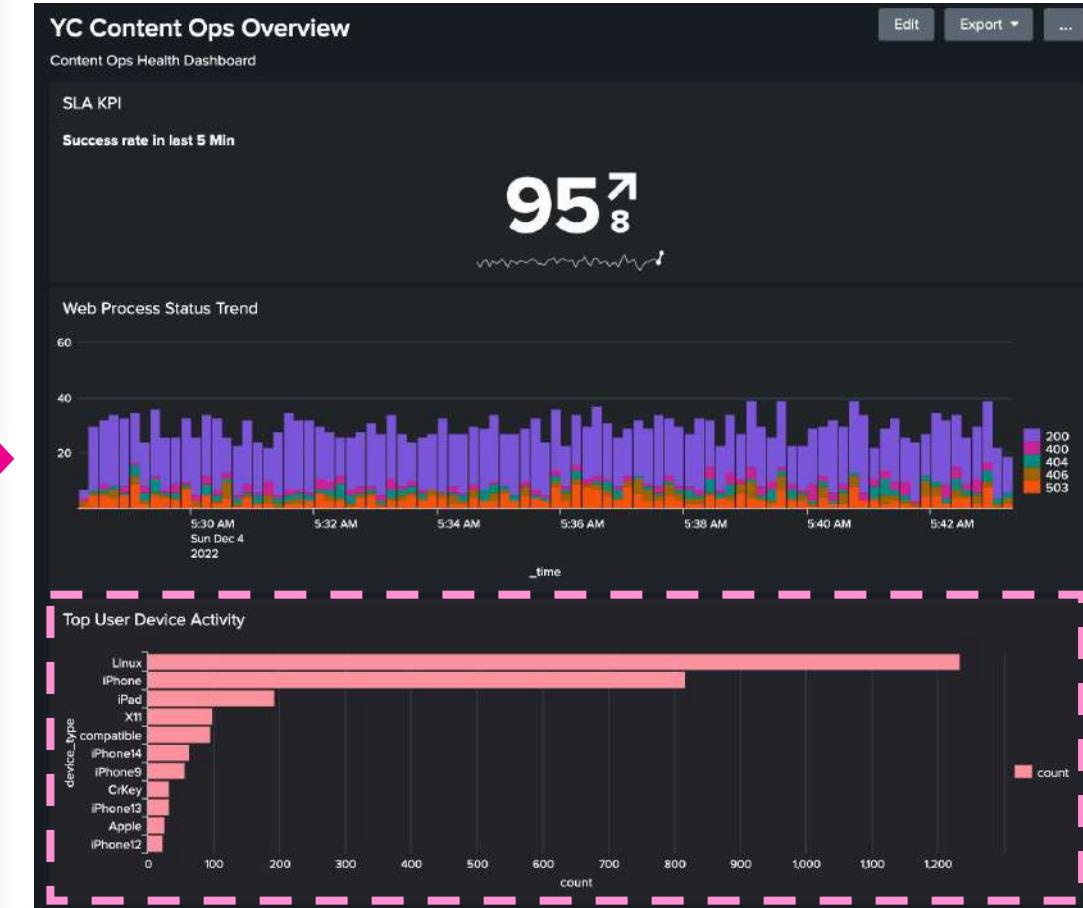
Panel Title: Top User Device Activity

Visualization Type: Bar Chart

Statistics Table

> Advanced Panel Settings

Cancel Save to Dashboard



Dashboard 1 : Content operations dashboard

Show each client access records in events table



Tasks:

1. Show details of content request activities in an event table
2. Use table command to calculate simple aggregated counts
 - Including fields : _time, status, status_description, product_name, clientip, JSESSIONID, action, device_type, other, price, product_id, user, user_add, user_age, user_gender, user_name, user_type, useragent
3. Sort the events by time.
 - Command : sort - _time

Goal:

Failed Content Purchase Transactions				
_time	status	status_description	product_name	clientip
2022-12-04 03:11:36.172	406	Not Acceptable	Warriors (Guerreros)	85.110.5
2022-12-04 03:11:33.145	503	Service Unavailable	36 Quai des Orfèvres (Department 36)	108.200.
2022-12-04 03:11:32.189	503	Service Unavailable	Flash Gordon	207.173.
2022-12-04 03:11:30.170	503	Service Unavailable	Electile Dysfunction	24.251.1
2022-12-04 03:10:54.126	503	Service Unavailable	Slasher House	151.106.
2022-12-04 03:10:35.107	503	Service Unavailable	Boy and His Dog, A	194.249.
2022-12-04 03:10:29.176	406	Not Acceptable	The Rebel	214.135.
2022-12-04 03:10:28.160	400	Bad Request	Endless Summer, The	2.103.23
2022-12-04 03:09:47.139	503	Service Unavailable	Tom Jones	94.70.23
2022-12-04 03:09:38.108	503	Service Unavailable	Hide in Plain Sight	215.91.8



Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

```
sourcetype=mobile_content action=download status>=400
| table _time status status_description product_name clientip JSESSIONID action
device_type other price product_id user user_add user_age user_gender user_name
user_type useragent
| sort - _time
```

_time	status	status_description	product_name	clientip	JSESSIONID	action	device_type	other
2022-12-04 06:04:49.106	503	Service Unavailable	Charlie Chan in Egypt	64.208.79.23	SD1SL5FF7ADFF3	download	Linux	743
2022-12-04 06:04:30.130	404	Not Found	Dick Figures: The Movie	217.244.42.209	SD4SL9FF10ADFF6	download	Linux	369
2022-12-04 06:04:05.167	406	Not Acceptable	Critical Care	110.38.241.246	SD7SL1FF5ADFF8	download	iPhone	992
2022-12-04 06:04:02.151	400	Bad Request	Thirteen, The (Trinadtsat)	101.123.87.195	SD9SL10FF5ADFF6	download	Linux	724
2022-12-04 06:04:00.110	400	Bad Request	Here Comes Cookie	146.98.146.250	SD8SL5FF7ADFF3	download	Linux	433
2022-12-04 06:03:50.155	406	Not Acceptable	Earth vs. the Spider	84.207.131.201	SD4SL4FF2ADFF9	download	X11	886
2022-12-04 06:03:45.176	400	Bad Request	Aces: Iron Eagle III	117.139.152.55	SD6SL10FF4ADFF6	download	compatible	539
2022-12-04 06:03:36.131	406	Not Acceptable	Hate (Haine, La)	219.136.235.71	SD6SL3FF8ADFF10	download	X11	443
2022-12-04 06:03:25.170	404	Not Found	Tukkijoella	32.246.190.135	SD8SL7FF10ADFF2	download	iPhone	201
2022-12-04 06:03:18.134	400	Bad Request	As it is in Heaven (Som i himmelen)	137.73.178.238	SD8SL9FF5ADFF5	download	Linux	390

Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

New Search

```

1 sourcetype=mobile_content action=download status>=400
2 | fields - date* source* file*
3 | table _time status status_description product_name clientip JSESSIONID action device_type other price product_id user user_add us
    user_name user_type useragent
4 | sort - _time

```

✓ 186 events (12/4/22 5:04:00.000 AM to 12/4/22 6:04:59.000 AM) No Event Sampling ▾ Job ▾ Event Type ▾ Verbose Mode ▾

Events (186) Patterns Statistics (186) Visualization

100 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

_time	status	status_description	product_name	clientip	JSESSIONID	action
2022-12-04 06:04:49.106	503	Service Unavailable	Charlie Chan in Egypt	64.208.79.23	SD1SL5FF7ADFF3	down
2022-12-04 06:04:30.130	404	Not Found	Dick Figures: The Movie	217.244.42.209	SD4SL9FF10ADFF6	down
2022-12-04 06:04:05.167	406	Not Acceptable	Critical Care	110.38.241.246	SD7SL1FF5ADFF8	down
2022-12-04 06:04:02.151	400	Bad Request	Thirteen, The (Trinadtsat)	101.123.87.195	SD9SL10FF5ADFF6	down
2022-12-04 06:04:00.110	400	Bad Request	Here Comes Cookie	146.98.146.250	SD8SL5FF7ADFF3	down
2022-12-04 06:03:50.155	406	Not Acceptable	Earth vs. the Spider	84.207.131.201	SD4SL4FF2ADFF9	down
2022-12-04 06:03:45.176	400	Bad Request	Aces: Iron Eagle III	117.139.152.55	SD6SL10FF4ADFF6	down
2022-12-04 06:03:36.131	406	Not Acceptable	Hate (Haine, La)	219.136.235.71	SD6SL3FF8ADFF10	down
2022-12-04 06:03:25.170	404	Not Found	Tukkijoella	32.246.190.135	SD8SL7FF10ADFF2	down
2022-12-04 06:03:18.134	400	Bad Request	As it is in Heaven (Sv· som i himmelen)	137.73.178.238	SD8SL9FF5ADFF5	down
2022-12-04 06:02:58.137	404	Not Found	Life of David Gale, The	113.217.103.26	SD2SL7FF5ADFF3	down
2022-12-04 06:02:35.195	400	Bad Request	Forest of Bliss	93.229.178.46	SD5SL3FF7ADFF3	down

Dashboard 1 : Content operations dashboard

Show service success rate trends over time, based on web status code.

Solution:

Save Panel to Existing Dashboard X

Select an Existing Dashboard Sort: Title (A - Z) ↓

Search By Title 🔍

Live Dataflow

Telco 5G Network RAN - Events and Alarms : Ericsson

Telco 5G Network RAN - PM Power Consumption to FM Fan Failures

Telco Content Service - Operations Dashboard

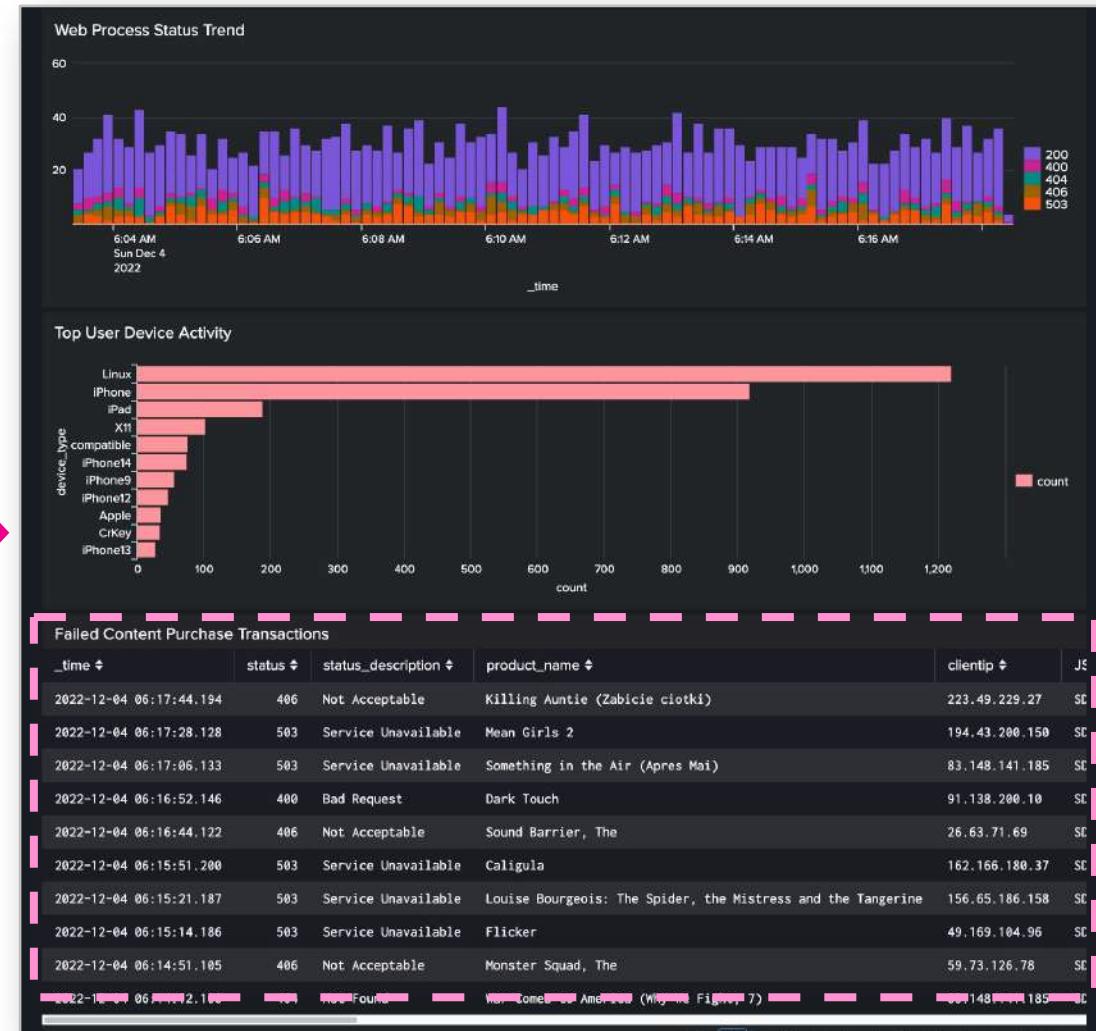
YC Content Ops Overview

Panel Title Failed Content Purchase Transactions

Visualization Type Statistics Table

> Advanced Panel Settings

Cancel Save to Dashboard

Dashboard 1 : Content operations dashboard

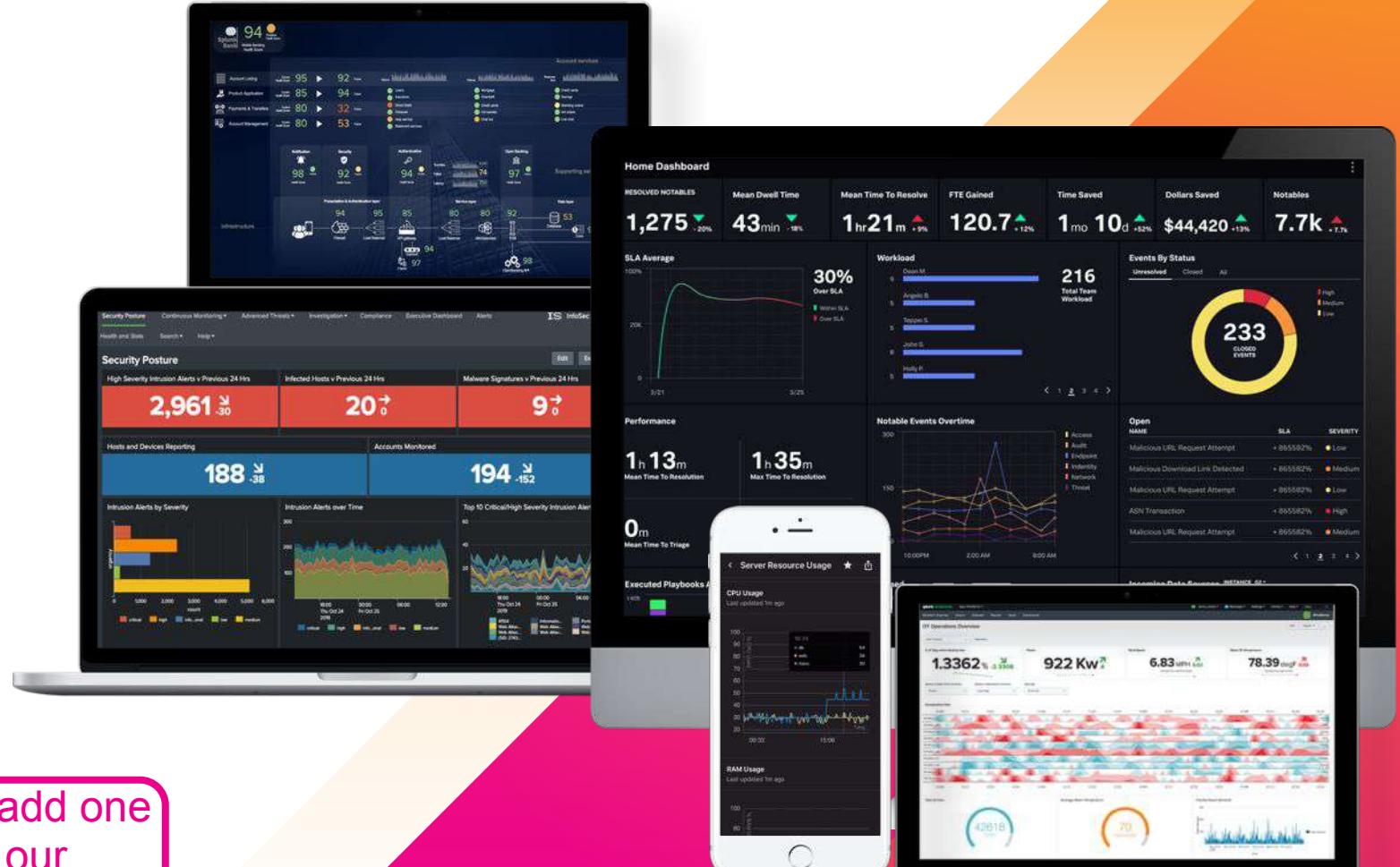
Show service success rate trends over time, based on web status code.

Solution:

The screenshot shows a Splunk Enterprise interface with a dark theme. At the top, there's a navigation bar with 'splunk>enterprise', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a header for 'YC Content Ops Overview' and 'Content Ops Health Dashboard'. A sub-header 'Top User Device Activity' is also visible. In the center, there's a table titled 'Failed Content Purchase Transactions' with columns for '_time', 'status', 'status_description', and 'product_name'. One row from the table is selected and has a context menu open. The context menu includes options for 'Color' (with a dropdown showing 'None' as the current selection), 'Scale' (with a slider from 0 to 7), 'Ranges' (with a color scale from green to red), and 'Values' (with a grid of colored squares labeled a through d). To the right of the table, a sidebar lists various status codes with their descriptions: Not Acceptable, Service Unavailable, Not Found, Bad Request, and Not Acceptable again. At the bottom of the table, there are navigation links for 'Prev' and 'Next'.

Make Your Dashboard Dynamic

- > Use tokens to control your dashboard panel searches
- > Available inputs:
 - > Text boxes
 - > Radio buttons
 - > Dropdown lists
 - > Checkboxes
 - > Multiselects
 - > Link lists
 - > Time picker



Dashboard 1 : Content operations dashboard

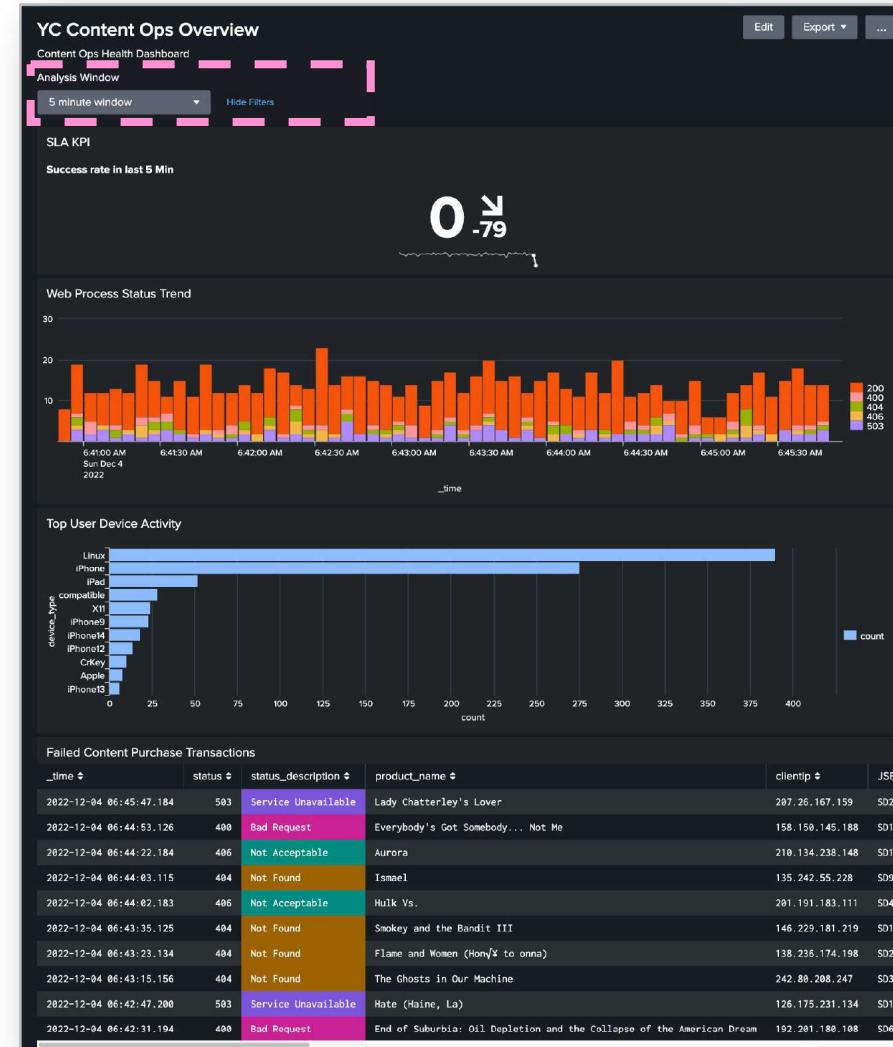
Enhance Dashboard



Tasks:

1. Add options for selecting the time window of analysis for the dashboard, allowing the user to choose the window of analysis.
2. Use the real-time last 5 minutes as the default time window for the dashboard.

Goal:



Dashboard 1 : Content operations dashboard

Enhance Dashboard.

Solution:

The screenshot shows the Splunk UI interface for editing a dashboard. At the top, there's a navigation bar with 'splunk>enterprise', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a header for 'YC Content Ops Overview' and 'Content Ops Health Dashboard'. On the left, there's a sidebar with 'Edit Dashboard', 'UI', 'Source', and buttons for '+ Add Panel' (highlighted with a pink box and number 2), '+ Add Input' (highlighted with a pink box and number 2), and 'Dark Theme'. On the right, there are buttons for 'Cancel', 'Save as...', and 'Save'. The main area displays the 'YC Content Ops Overview' dashboard with a title 'Content Ops Health Dashboard' and a section titled 'SLA KPI'. A context menu is open over a 'Text' input field, listing options: Radio, Dropdown, Checkbox, Multiselect, Link List, Time (highlighted with a pink box and number 3), and Submit. The entire interface is in dark mode.

Dashboard 1 : Content operations dashboard

Enhance Dashboard.

Solution:

The screenshot shows the Splunk UI interface for editing a dashboard. The top navigation bar includes 'Edit Dashboard', 'UI', 'Source', '+ Add Panel', '+ Add Input', a 'Dark Theme' toggle, and buttons for 'Cancel', 'Save as...', and 'Save'. The main title of the dashboard is 'YC Content Ops Overview' under the heading 'Content Ops Health Dashboard'. On the left, there's a panel titled 'SLA KPI' with a sub-section 'Success rate in last 5 Min'. A dropdown menu is open over a 'Time' input field, which has been set to 'Last 24 hours'. The configuration modal lists various input types: 'Text', 'Radio', 'Dropdown', 'Checkbox', 'Multiselect', 'Link List', and 'Time'. The 'Time' option is selected. The configuration pane shows the 'General' tab with a 'Label' set to 'Analysis Window' (circled in pink), a checked 'Search on Change' checkbox (circled in pink), a 'Token Options' section with a token 'INPUT_TIME' (circled in pink), and a 'Default' dropdown set to '5 minute window' (circled in pink). At the bottom of the configuration pane is an 'Apply' button (circled in pink).

Dashboard 1 : Content operations dashboard

Enhance Dashboard.

Solution:

The screenshot shows the 'Edit Search' dialog box from the Splunk interface. The search string is set to:

```
1 sourcetype=mobile_content  
2 | timechart count by status
```

The 'Time Range' section has a dropdown menu open, with the option "Shared Time Picker (INPUT_TIME)" selected. This option is highlighted with a pink dashed rectangle and a pink circle containing the number 3. Other options in the menu include "Use time picker", "Tokens", and "Global".

At the bottom right of the dialog, there are three buttons: "Cancel", "Convert to Report", and "Apply". The "Apply" button is also highlighted with a pink dashed rectangle and a pink circle containing the number 4.

In the background, the main dashboard view is visible, featuring a large KPI card with the value "89" and an upward arrow, along with other cards for "YC Content" and "SLA KPI".

Content Ops Dashboard Completed!

The screenshot shows the 'YC Content Ops Overview' dashboard in Splunk Enterprise. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. A secondary header 'Telco Analyst Workshop' is visible. The main content area features a 'Web Process Status Trend' chart and a 'Top User Device Activity' chart. A pink callout bubble points to the 'Analysis Window' dropdown, which is set to '5 minute window'. The callout contains the text: 'You can now change the time range for all panels using your new time picker'.

You can now change the time range for all panels using your new time picker

YC Content Ops Overview

Content Ops Health Dashboard

Analysis Window

5 minute window

Hide Filters

Web Process Status Trend

30

20

10

0

200

400

404

406

503

6:41:00 AM Sun Dec 4 2022

time

Top User Device Activity

Linux

iPhone

iPad

compatible

OSS 5G RAN Dashboard

Dashboards



5G RAN Alerts Dashboard

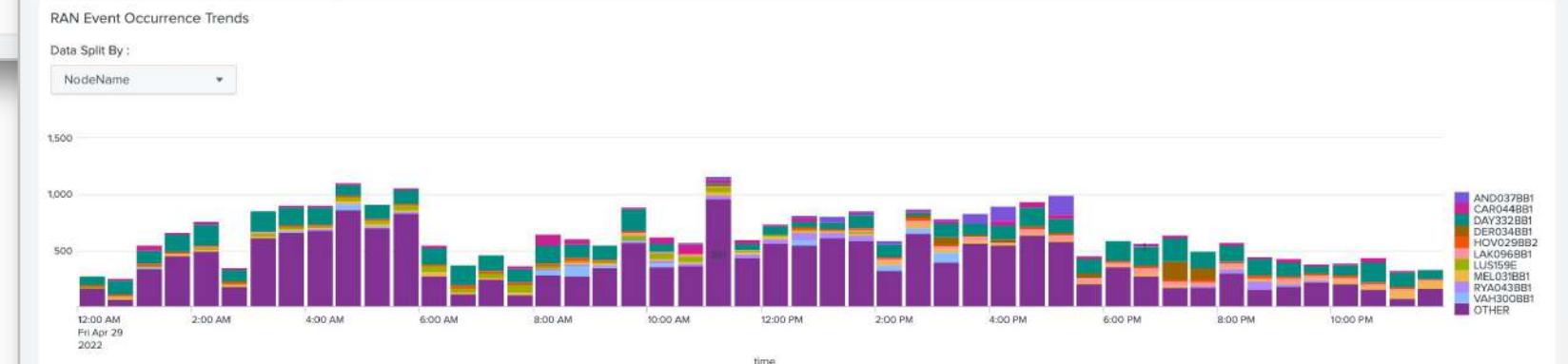
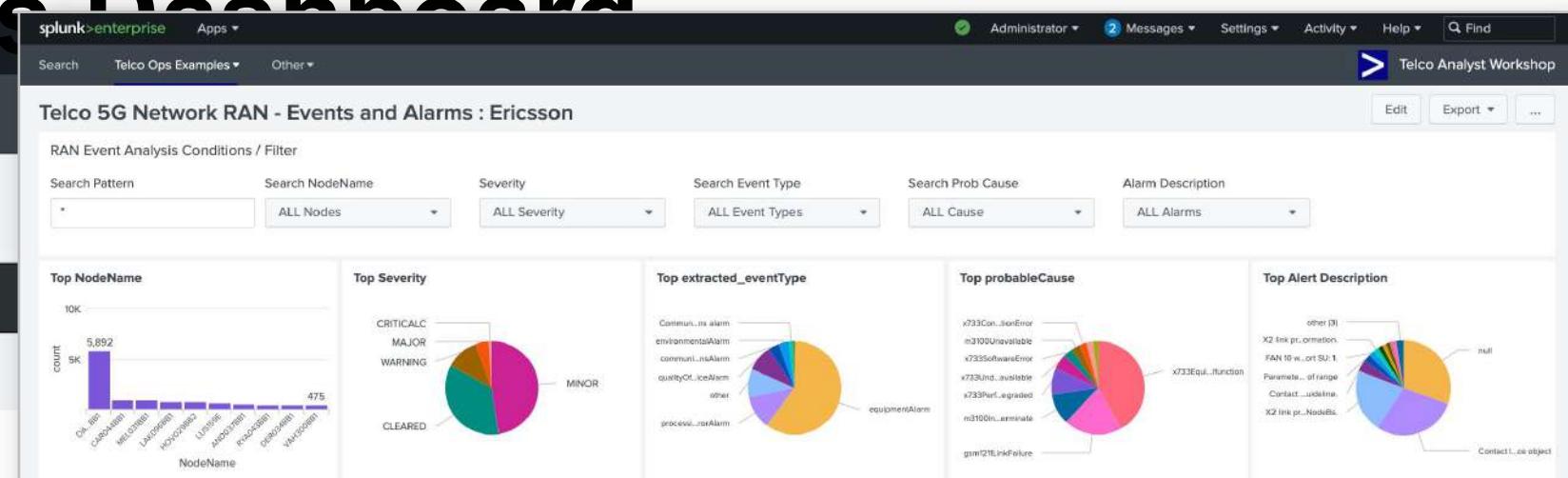
Search Telco Ops Examples ▾ Other ▾

Telco Content Service - Operations Dashboard

Telco 5G Network RAN - Events and Alarms : Ericsson

Telco 5G Network RAN - PM Power Consumption to FM Fan Failures

> Search History ?



5G RAN Events and Alarms Detail

Severity: * Search Pattern: *** NodeName: *** Event Type: *** Probable Cause: *** Event Text: *

_time	alarmId	nodeName	extracted_eventType	presentSeverity	probableCause	problemText	specificProblem	alarmState
2022-04-29 20:06:19	9175073	LAK096BB1	equipmentAlarm	CLEARED	x733EquipmentMalfunction	Contact lost with resource object	No Connection	CLEARED_UNACKN
2022-04-29 20:06:19	9175073	LAK096BB1	equipmentAlarm	CLEARED	x733EquipmentMalfunction	Contact lost with resource object	No Connection	CLEARED_UNACKN
2022-04-29 20:06:19	9175073	LAK096BB1	equipmentAlarm	CLEARED	x733EquipmentMalfunction	Contact lost with resource object	No Connection	CLEARED_UNACKN
2022-04-29 20:06:19	9175073	LAK096BB1	equipmentAlarm	CLEARED	x733EquipmentMalfunction	Contact lost with resource object	No Connection	CLEARED_UNACKN
2022-04-29 20:06:19	9175073	LAK096BB1	equipmentAlarm	MINOR	x733EquipmentMalfunction	Contact lost with resource object	No Connection	ACTIVE_UNACKN

Dashboard 2 : 5G RAN Alarms Dashboard

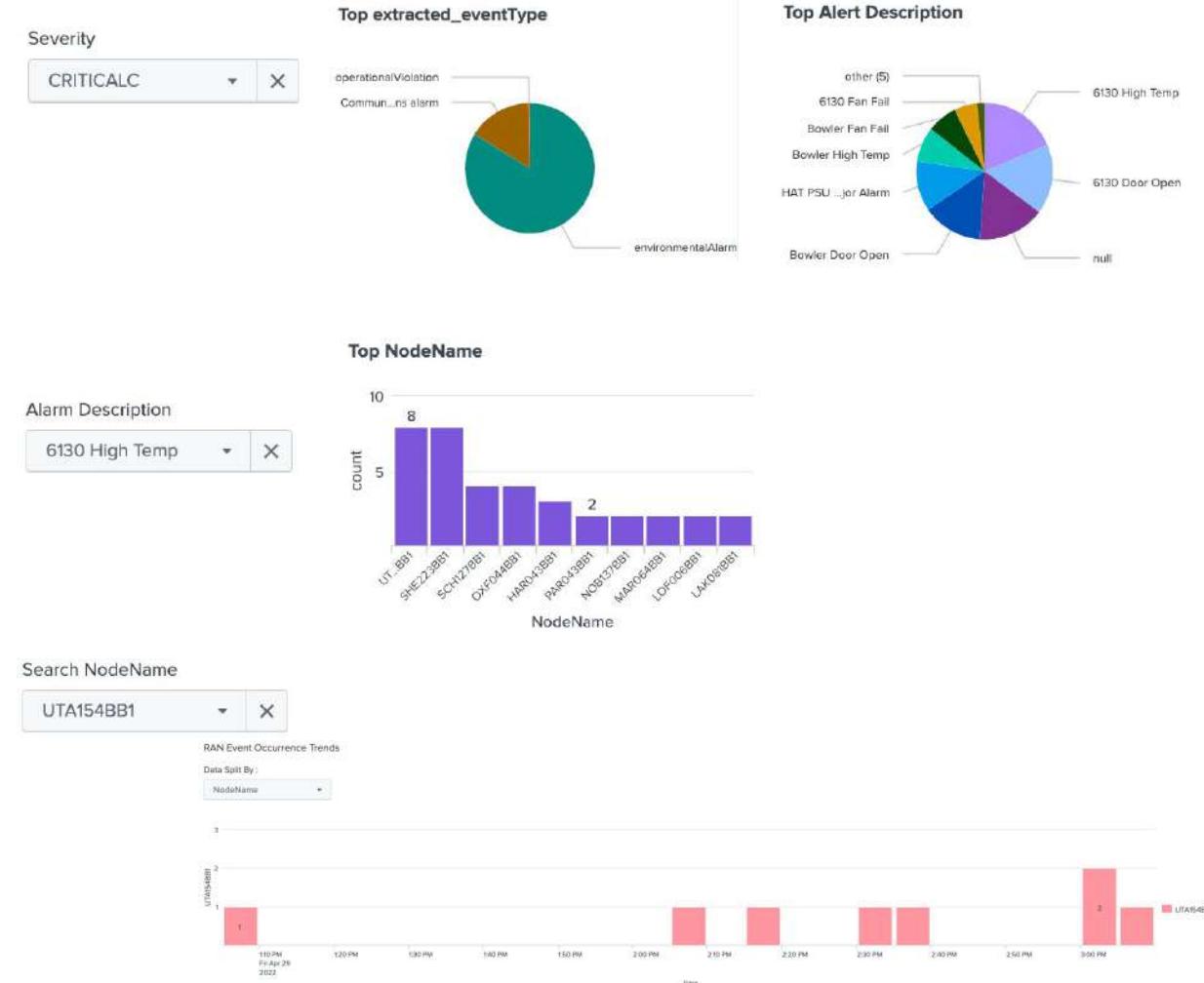
Events analysis exercise



Analysis Tasks:

- What is the most occurred events types that are “Critical”?
 - Top event types?
 - Top “Alert Description”?
- For “High Temp” alerts, which top 3 sites are most impacted (In term of most occurrence)?
 - Site ID for top 3 sites?
- For “UTA154BB1” site, when did those alerts occurred the most?
 - Time for the most occurrence?
 - First time of occurrence?

Goal:



Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

Task : What is the most occurred events types that are “Critical”?
 - Top event types? - Top “Alert Description”?



Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

Task : For “High Temp” alerts, which top 3 sites are most impacted (In term of most occurrence)?
 - Side ID for top 3 sites?

Telco 5G Network RAN - Events and Alarms : Ericsson

RAN Event Analysis Conditions / Filter

Search Pattern: * Search NodeName: UTA154BB1 Severity: CRITICALC Search Event Type: ALL Event Types Search Prob Cause: ALL Cause Alarm Description: 1 6130 High Temp

Top NodeName: count: 8 (UTA154BB1)

Top Severity: CRITICALC

RAN Event: <1m ago

Data Split by: NodeName

1: Click on the search bar for Alarm Description: 1 6130 High Temp

2: Click on the magnifying glass icon in the RAN Event section

Event Search Results:

```

1 index=telco_ops sourcetype=net_fm_ran *** NodeName=*** extracted_eventType=*** probableCause=*** problemText
   = "6130 High Temp"
2 | fields - date_* eventtype host source sourcetype index linecount eventTime punct splunk_server* time* _raw
3 | table _time alarmId NodeName extracted_eventType presentSeverity probableCause problemText specificProblem
4 | search presentSeverity=CRITICALC
5 | top NodeName

```

52 events (before 12/4/22 7:53:20.000 AM) No Event Sampling

Events Patterns Statistics (10) Visualization

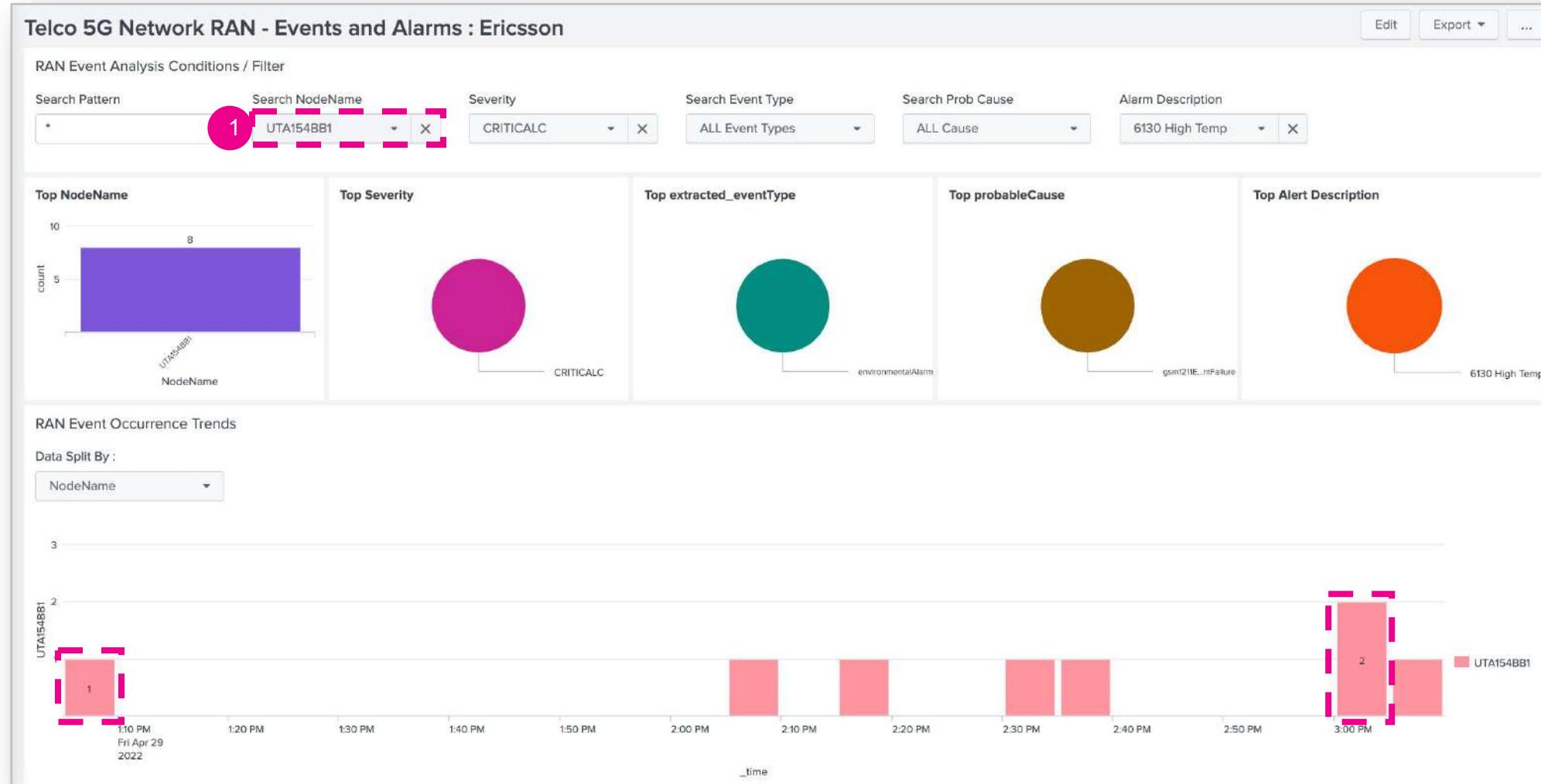
100 Per Page Format Preview

NodeName	count	percent
UTA154BB1	8	15.384615
SHE223BB1	8	15.384615
SCH127BB1	4	7.692308
OXF044BB1	4	7.692308
HAR043BB1	3	5.769231
PAR043BB1	2	3.846154
NOB137BB1	2	3.846154

Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

Task : For “UTA154BB1” site, when did those alerts occurred the most?
 - Time for the most occurrence? - First time of occurrence?



Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

Task : For “UTA154BB1” site, when did those alerts occurred the most?
 - Time for the most occurrence? - First time of occurrence?



5G RAN Events and Alarms Detail

Severity : CRITICALC Search Pattern : *** NodeName : *UTA154BB1* Event Type : *** Probable Cause : *** Event Text : 6130 High Temp

1m ago

_time	alarmId	NodeName	extracted_eventType	presentSeverity	probableCause	problemText	specificProblem	alarmState
2022-04-29 14:37:22	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 15:01:03	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 15:04:57	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 15:09:46	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 14:09:32	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 14:17:07	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 14:30:53	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 13:06:41	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW

Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

Task : For Duplicate the "Telco 5G Network RAN" Dashboard with naming your initial in the front.

Telco 5G Network RAN - Events and Alarms : Ericsson

RAN Event Analysis Conditions / Filter

Search Pattern: * Search NodeName: UTA154BB1 Severity: CRITICALC Search Event Type: ALL Event Types Search Pro: ALL Cau

Alarm Description: 6130 High Temp

More Options: Edit, Export, ... (1)

Clone (2) Clone in Dashboard Studio NEW Edit Permissions Set as Home Dashboard Delete

Top NodeName

NodeName	Count
UTA154BB1	8

Top Severity

Severity	Count
CRITICALC	~4

Top extracted_eventType

extracted_eventType	Count
enviro...lAlarm	~4

Top probableCause

probableCause	Count
gsm12...allure	~4

Top Alert Description

Alert Description	Count
6130 ... Temp	~4

RAN Event Occurrence Trends

Data Split By: NodeName

Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

Task : For Duplicate the "Telco 5G Network RAN" Dashboard with naming your initial in the front.

Telco 5G Network RAN - Events and Alarms : Ericsson

RAN Event Analysis Conditions / Filter

Search Pattern: *

Alarm Description: 6130 High Temp

Clone

Title: Telco 5G Network RAN - Events and Alarms : Ericss

ID: YC_5G_RAN_Alarms 3

The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.

New Description: optional

Permissions: Private 4 Clone

Cancel 4 Clone Dashboard

Export ...

Search Pro ALL Cau

Clone

Clone in Dashboard Studio NEW

Edit Permissions

Set as Home Dashboard

Delete

Top NodeName

Count: 8
NodeName: UTA5ABB1

Top Alert Description

gsm12...allure
6130 ... Temp

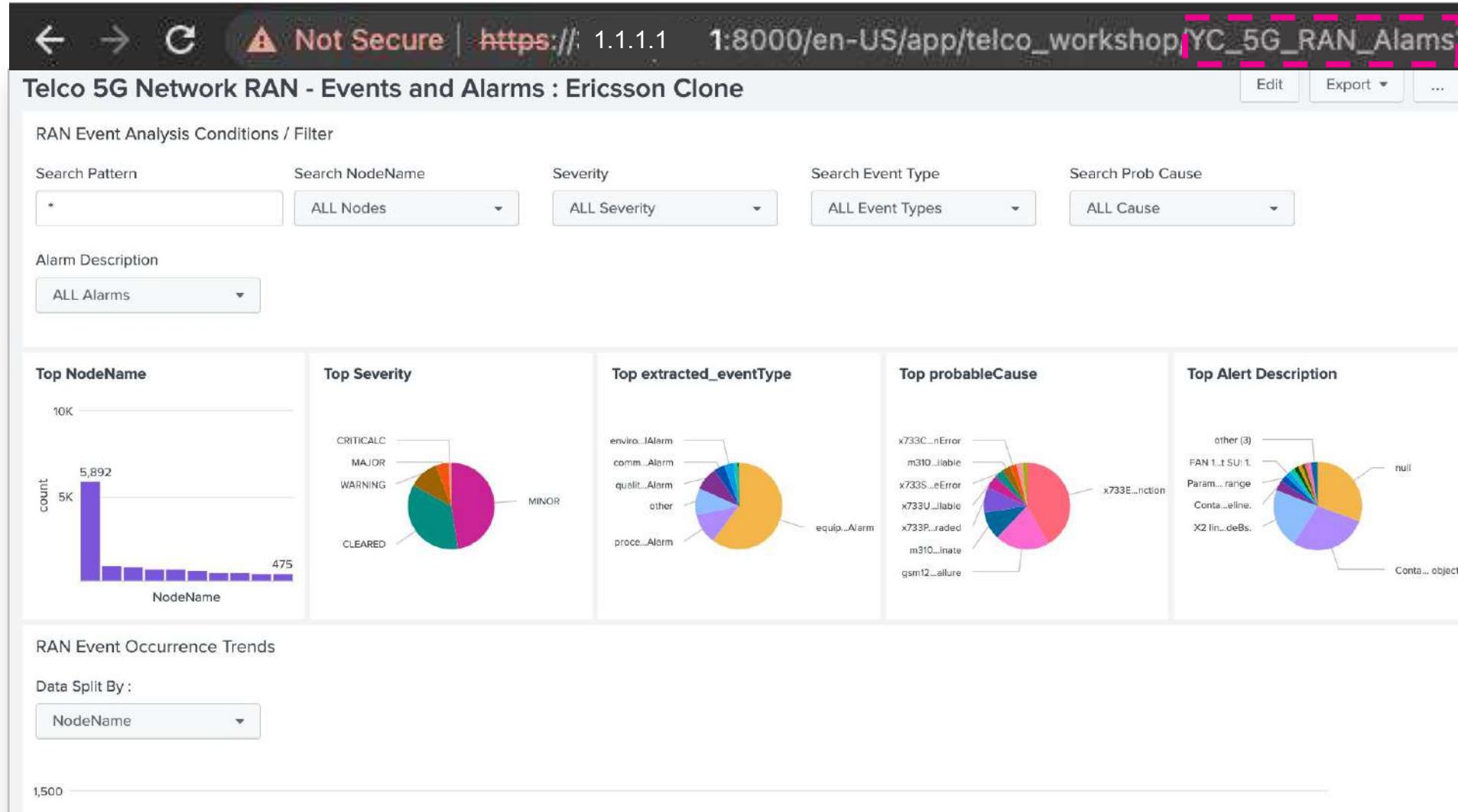
RAN Event Occurrence Trends

Data Split By : NodeName

Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

Task : Check the ID of the dashboard changed, added with your initials.



Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

Task : With cloned dashboard, check out the dashboard XML Code

Telco 5G Network RAN - Events and Alarms : Ericsson Clone

1
Edit
Export ▾
...

Edit Dashboard
UI
Source
2

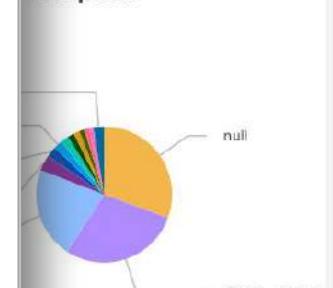
Cancel
Save as...
Save
...

No validation issues

```

1<form version="1.1" theme="light">
2  <label>Telco 5G Network RAN - Events and Alarms : Ericsson Clone</label>
3  <fieldset submitButton="false" autoRun="true"></fieldset>
4<row>
5  <panel>
6    <title>RAN Event Analysis Conditions / Filter</title>
7  <input type="text" token="SEARCH_PATT_RAN" searchWhenChanged="true">
8    <label>Search Pattern</label>
9    <default>*</default>
10   <prefix>*</prefix>
11   <suffix>*</suffix>
12   <initialValue>*</initialValue>
13 </input>
14 <input type="dropdown" token="SEARCH_RAN_NODENAME" searchWhenChanged="true">
15   <label>Search NodeName</label>
16   <default>*</default>
17   <prefix>*</prefix>
18   <suffix>*</suffix>
19   <initialValue>*</initialValue>
20   <choice value="*">>ALL Nodes</choice>
21 </input>
22 <input type="dropdown" token="INPUT_RAN_SEV" searchWhenChanged="true">
23   <label>Severity</label>
24   <choice value="*">>ALL Severity</choice>
25   <choice value="Cleared">>Cleared</choice>
26   <choice value="Minor">>Minor</choice>
27   <choice value="Warning">>Warning</choice>
28   <choice value="Critical">>Critical</choice>
29   <default>*</default>
30   <initialValue>*</initialValue>
31 </input>
32 <input type="dropdown" token="SEARCH_RAN_EVENTTYPE" searchWhenChanged="true">

```

Description


OSS 5G RAN

Event Correlations





Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis

splunk>enterprise Apps ▾

Search Telco Ops Examples ▾ Other ▾

Telco Content Service - Operations Dashboard

Telco 5G Network RAN - Events and Alarms : Ericsson

Telco 5G Network RAN - PM Power Consumption to FM Fan Failures

> Search History ②

splunk>enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Telco Ops Examples ▾ Other ▾

Telco 5G Network RAN - PM Power Consumption to FM Fan Failures

Last 24 hours ▾ Submit Hide Filters

Ericsson PM : Top Energy Consumption Sites

Average Watts Per Hour

ManagedElement

Legend: r1 (purple bars), average (red line)

ManagedElement	Average Watts Per Hour
04-82	110.21195652173913
04-1265	100
04-22682	100
04-23692	100
04-32426	100
04-32681	100
04-34178	100
04-37182	100
04-37882	100
04-38182	100
04-38282	100
04-38882	100
04-39882	100
04-39982	100
04-40182	100
04-40282	100
04-40382	100
04-40482	100
04-40582	100
04-40682	100
04-40782	100
04-40882	100
04-40982	100
04-41082	100
04-41182	100
04-41282	100
04-41382	100
04-41482	100
04-41582	100
04-41682	100
04-41782	100
04-41882	100
04-41982	100
04-42082	100
04-42182	100
04-42282	100
04-42382	100
04-42482	100
04-42582	100
04-42682	100
04-42782	100
04-42882	100
04-42982	100
04-43082	100
04-43182	100
04-43282	100
04-43382	100
04-43482	100
04-43582	100
04-43682	100
04-43782	100
04-43882	100
04-43982	100
04-44082	100
04-44182	100
04-44282	100
04-44382	100
04-44482	100
04-44582	100
04-44682	100
04-44782	100
04-44882	100
04-44982	100
04-45082	100
04-45182	100
04-45282	100
04-45382	100
04-45482	100
04-45582	100
04-45682	100
04-45782	100
04-45882	100
04-45982	100
04-46082	100
04-46182	100
04-46282	100
04-46382	100
04-46482	100
04-46582	100
04-46682	100
04-46782	100
04-46882	100
04-46982	100
04-47082	100
04-47182	100
04-47282	100
04-47382	100
04-47482	100
04-47582	100
04-47682	100
04-47782	100
04-47882	100
04-47982	100
04-48082	100
04-48182	100
04-48282	100
04-48382	100
04-48482	100
04-48582	100
04-48682	100
04-48782	100
04-48882	100
04-48982	100
04-49082	100
04-49182	100
04-49282	100
04-49382	100
04-49482	100
04-49582	100
04-49682	100
04-49782	100
04-49882	100
04-49982	100
04-50082	100
04-50182	100
04-50282	100
04-50382	100
04-50482	100
04-50582	100
04-50682	100
04-50782	100
04-50882	100
04-50982	100
04-51082	100
04-51182	100
04-51282	100
04-51382	100
04-51482	100
04-51582	100
04-51682	100
04-51782	100
04-51882	100
04-51982	100
04-52082	100
04-52182	100
04-52282	100
04-52382	100
04-52482	100
04-52582	100
04-52682	100
04-52782	100
04-52882	100
04-52982	100
04-53082	100
04-53182	100
04-53282	100
04-53382	100
04-53482	100
04-53582	100
04-53682	100
04-53782	100
04-53882	100
04-53982	100
04-54082	100
04-54182	100
04-54282	100
04-54382	100
04-54482	100
04-54582	100
04-54682	100
04-54782	100
04-54882	100
04-54982	100
04-55082	100
04-55182	100
04-55282	100
04-55382	100
04-55482	100
04-55582	100
04-55682	100
04-55782	100
04-55882	100
04-55982	100
04-56082	100
04-56182	100
04-56282	100
04-56382	100
04-56482	100
04-56582	100
04-56682	100
04-56782	100
04-56882	100
04-56982	100
04-57082	100
04-57182	100
04-57282	100
04-57382	100
04-57482	100
04-57582	100
04-57682	100
04-57782	100
04-57882	100
04-57982	100
04-58082	100
04-58182	100
04-58282	100
04-58382	100
04-58482	100
04-58582	100
04-58682	100
04-58782	100
04-58882	100
04-58982	100
04-59082	100
04-59182	100
04-59282	100
04-59382	100
04-59482	100
04-59582	100
04-59682	100
04-59782	100
04-59882	100
04-59982	100
04-60082	100
04-60182	100
04-60282	100
04-60382	100
04-60482	100
04-60582	100
04-60682	100
04-60782	100
04-60882	100
04-60982	100
04-61082	100
04-61182	100
04-61282	100
04-61382	100
04-61482	100
04-61582	100
04-61682	100
04-61782	100
04-61882	100
04-61982	100
04-62082	100
04-62182	100
04-62282	100
04-62382	100
04-62482	100
04-62582	100
04-62682	100
04-62782	100
04-62882	100
04-62982	100
04-63082	100
04-63182	100
04-63282	100
04-63382	100
04-63482	100
04-63582	100
04-63682	100
04-63782	100
04-63882	100
04-63982	100
04-64082	100
04-64182	100
04-64282	100
04-64382	100
04-64482	100
04-64582	100
04-64682	100
04-64782	100
04-64882	100
04-64982	100
04-65082	100
04-65182	100
04-65282	100
04-65382	100
04-65482	100
04-65582	100
04-65682	100
04-65782	100
04-65882	100
04-65982	100
04-66082	100
04-66182	100
04-66282	100
04-66382	100
04-66482	100
04-66582	100
04-66682	100
04-66782	100
04-66882	100
04-66982	100
04-67082	100
04-67182	100
04-67282	100
04-67382	100
04-67482	100
04-67582	100
04-67682	100
04-67782	100
04-67882	100
04-67982	100
04-68082	100
04-68182	100
04-68282	100
04-68382	100
04-68482	100
04-68582	100
04-68682	100
04-68782	100
04-68882	100
04-68982	100
04-69082	100
04-69182	100
04-69282	100
04-69382	100
04-69482	100
04-69582	100
04-69682	100
04-69782	100
04-69882	100
04-69982	100
04-70082	100
04-70182	100
04-70282	100
04-70382	100
04-70482	100
04-70582	100
04-70682	100
04-70782	100
04-70882	100
04-70982	100
04-71082	100
04-71182	100
04-71282	100
04-71382	100
04-71482	100
04-71582	100
04-71682	100
04-71782	100
04-71882	100
04-71982	100
04-72082	100
04-72182	100
04-72282	100
04-72382	100
04-72482	100
04-72582	100
04-72682	100
04-72782	100
04-72882	100
04-72982	100
04-73082	100
04-73182	100
04-73282	100
04-73382	100
04-73482	100
04-73582	100
04-73682	100
04-73782	100
04-73882	100
04-73982	100
04-74082	100
04-74182	100
04-74282	100
04-74382	100
04-74482	100
04-74582	100
04-74682	100
04-74782	100
04-74882	100
04-74982	100
04-75082	100
04-75182	100
04-75282	100
04-75382	100
04-75482	100
04-75582	100
04-75682	100
04-75782	100
04-75882	100
04-75982	100
04-76082	100
04-76182	100
04-76282	100
04-76382	100
04-76482	100
04-76582	100
04-76682	100
04-76782	100
04-76882	100
04-76982	100
04-77082	100
04-77182	100
04-77282	100
04-77382	100
04-77482	100
04-77582	100
04-77682	100
04-77782	100
04-77882	100
04-77982	100
04-78082	100
04-78182	100
04-78282	100
04-78382	100
04-78482	100
04-78582	100
04-78682	100
04-78782	100
04-78882	100
04-78982	100
04-79082	100
04-79182	100
04-79282	100
04-79382	100
04-79482	100
04-79582	100
04-79682	100
04-79782	100
04-79882	100
04-79982	100
04-80082	100
04-80182	100
04-80282	100
04-80382	100
04-80482	100
04-80582	100
04-80682	100
04-80782	100
04-80882	100
04-80982	100
04-81082	100
04-81182	100
04-81282	100
04-81382	100
04-81482	100
04-81582	100
04-81682	100
04-81782	100
04-81882	100
04-81982	100
04-82082	100
04-82182	100
04-82282	100
04-82382	100
04-82482	100
04-82582	100
04-82682	100
04-82782	100
04-82882	100
04-82982	100
04-83082	100
04-83182	100
04-83282	100
04-83382	100
04-83482	100
04-83582	100
04-83682	100
04-83782	100
04-83882	100
04-83982	100
04-84082	100
04-84182	100
04-84282	100
04-84382	100
04-84482	100
04-84582	100
04-84682	100
04-84782	100
04-84882	100
04-84982	100
04-85082	100
04-85182	100
04-85282	100
04-85382	100
04-85482	100
04-85582	100
04-85682	100
04-85782	100
04-85882	100
04-85982	100
04-86082	100
04-86182	100
04-86282	100
04-86382	100
04-86482	100
04-86582	100
04-86682	100
04-86782	100



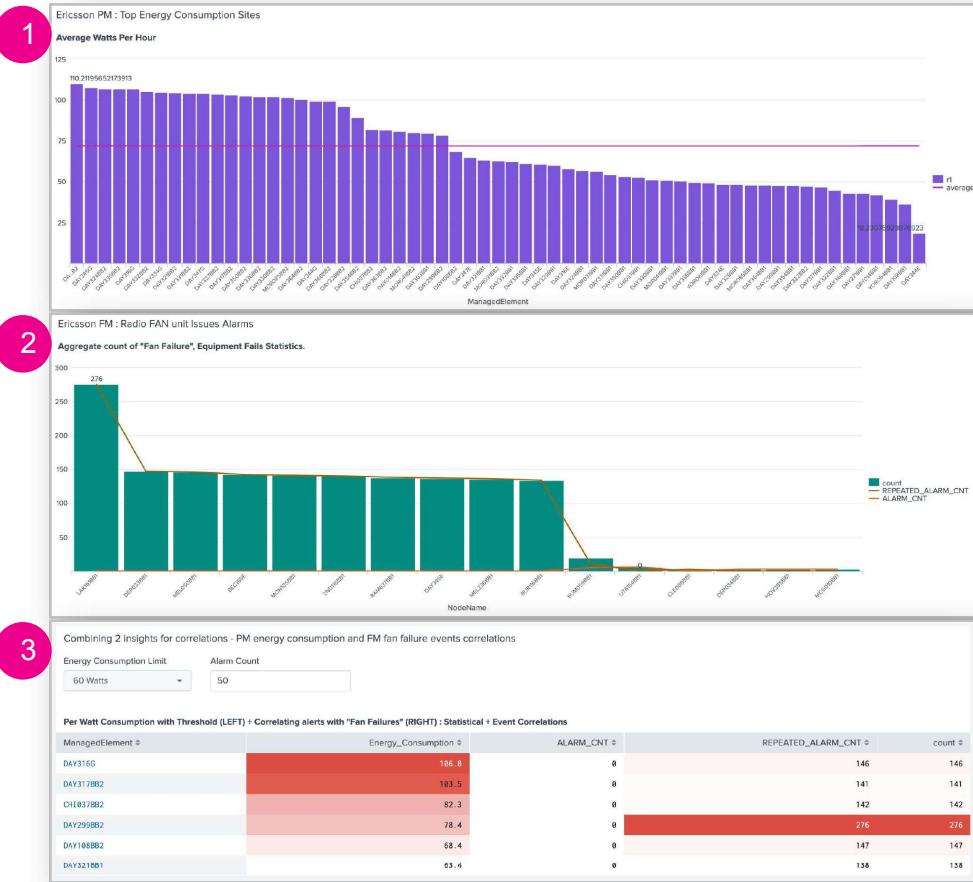
Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis

Analysis Tasks:

Goal:

1. Analyze sites with power consumption – PM data
 - Sites with average 60 watts or above
 2. Analyze sites with “Fan Failures” – FM data
 - Side ID for top 3 sites?
 3. Find sites with combinations of conditions, above 2 conditions,
 - Condition 1 : Sites with 60 watts above average power consumption
 - Condition 2 : Sites with “Fan Failures”, repeated alarm count of 10 or more.



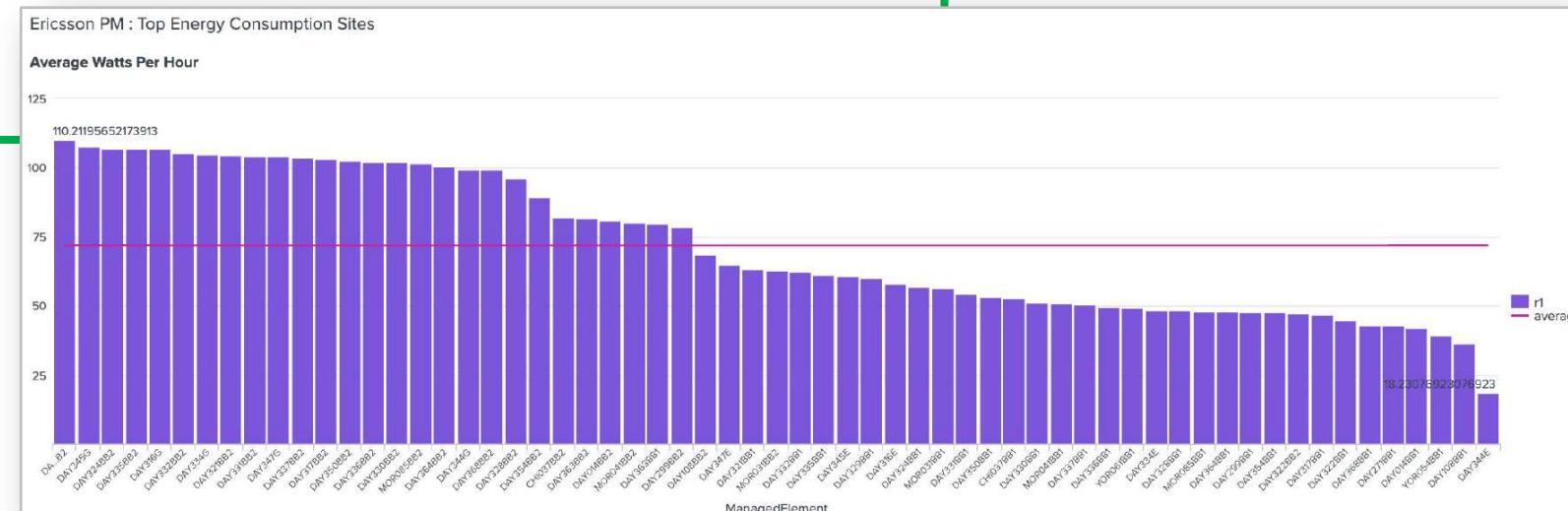


Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis.

Task : What Analyze sites with power consumption? Sites with average 60 watts or above.

```
index=telco_ops sourcetype=net_pm_ran PmGroup=EnergyMeter
| rex mode=sed field=_raw "s/[\\r\\n]+//g"
| rex mode=sed field=_raw "s/\\s+/ /g"
| rex mode=sed field=_raw "s/\\<measValue/\\n<measValue/g"
| rex field=_raw max_match=100 "(?<V1>\\<measValue.*measValue\\>)"
| table _time measObjLdn V1 ManagedElement
| mvexpand V1
| spath input=V1 measValue
| spath input=measValue r{1}
| rename "r{1}" as r1
| stats avg(r1) as r1 by ManagedElement
| eventstats avg(r1) as average
| sort - r1
```

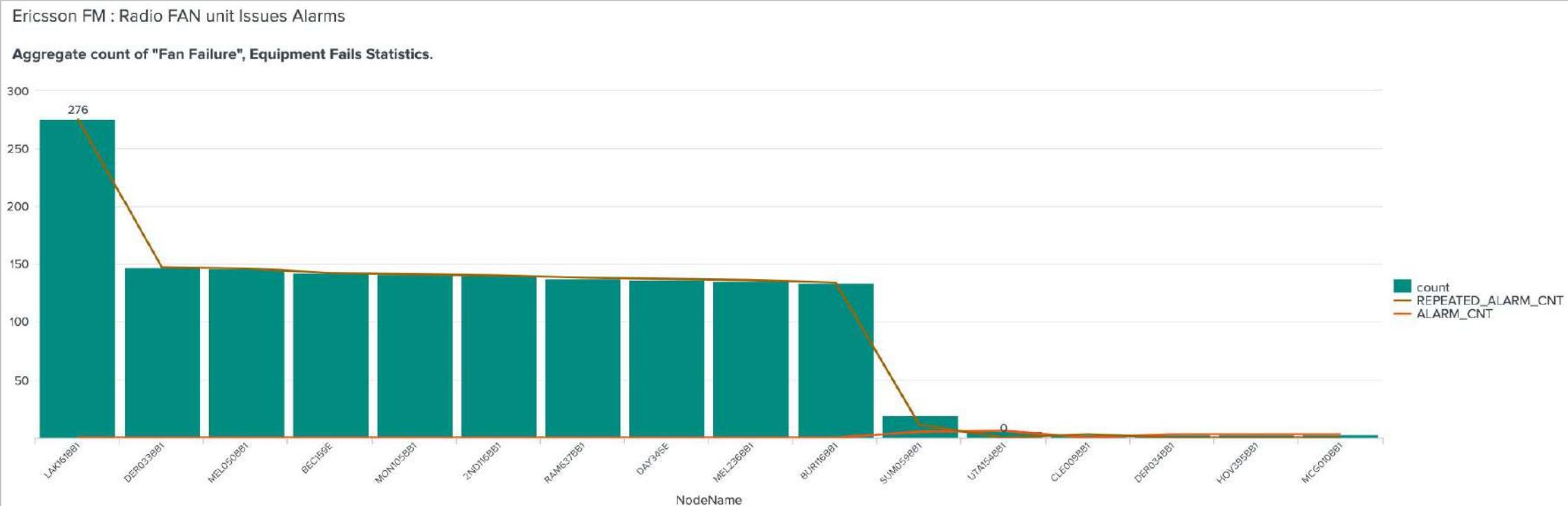


Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis.

Task : What Analyze sites with power consumption? Sites with average 60 watts or above.

```
index=telco_ops sourcetype=net_fm_ran problemText="FAN*"
| stats count, count(eval(recordType="REPEATED_ALARM")) AS REPEATED_ALARM_CNT,
count(eval(recordType="ALARM")) as ALARM_CNT by NodeName
| sort - count
```





Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis.

Task : Find sites with combinations of conditions, above 2 conditions : Correlations results

```
index=telco_ops sourcetype=net_pm_ran PmGroup=EnergyMeter
| rex mode=sed field=_raw "s/[\r\n]+//g"
| rex mode=sed field=_raw "s/\s+/ /g"
| rex mode=sed field=_raw "s/\<measValue/\n<measValue/g"
| rex field=_raw max_match=100 "(?<V1>\<measValue.*measValue\>)"
| table _time measObjLdn V1 ManagedElement
| mvexpand V1
| spath input=V1 measValue
| spath input=measValue r{1}
| rename "r{1}" as Energy_Consumption
| stats avg(Energy_Consumption) as Energy_Consumption by ManagedElement
| appendcols
  [ search index=telco_ops sourcetype=net_fm_ran problemText="FAN *"
    | rename NodeName as ManagedElement
    | stats count, count(eval(recordType="REPEATED_ALARM")) AS REPEATED_ALARM_CNT,
count(eval(recordType="ALARM")) as ALARM_CNT by ManagedElement ]
| sort - Energy_Consumption
| search Energy_Consumption>60 REPEATED_ALARM_CNT>50
```

Search 1 – Aggregating average watts use per site, processing 3GPP performance stats.

Search 2 – Fault event stats, counting number of occurrence.

Applying Threshold / Logic – Defining PM stats thresholding and FM alarm occurrence



Splunk Resources

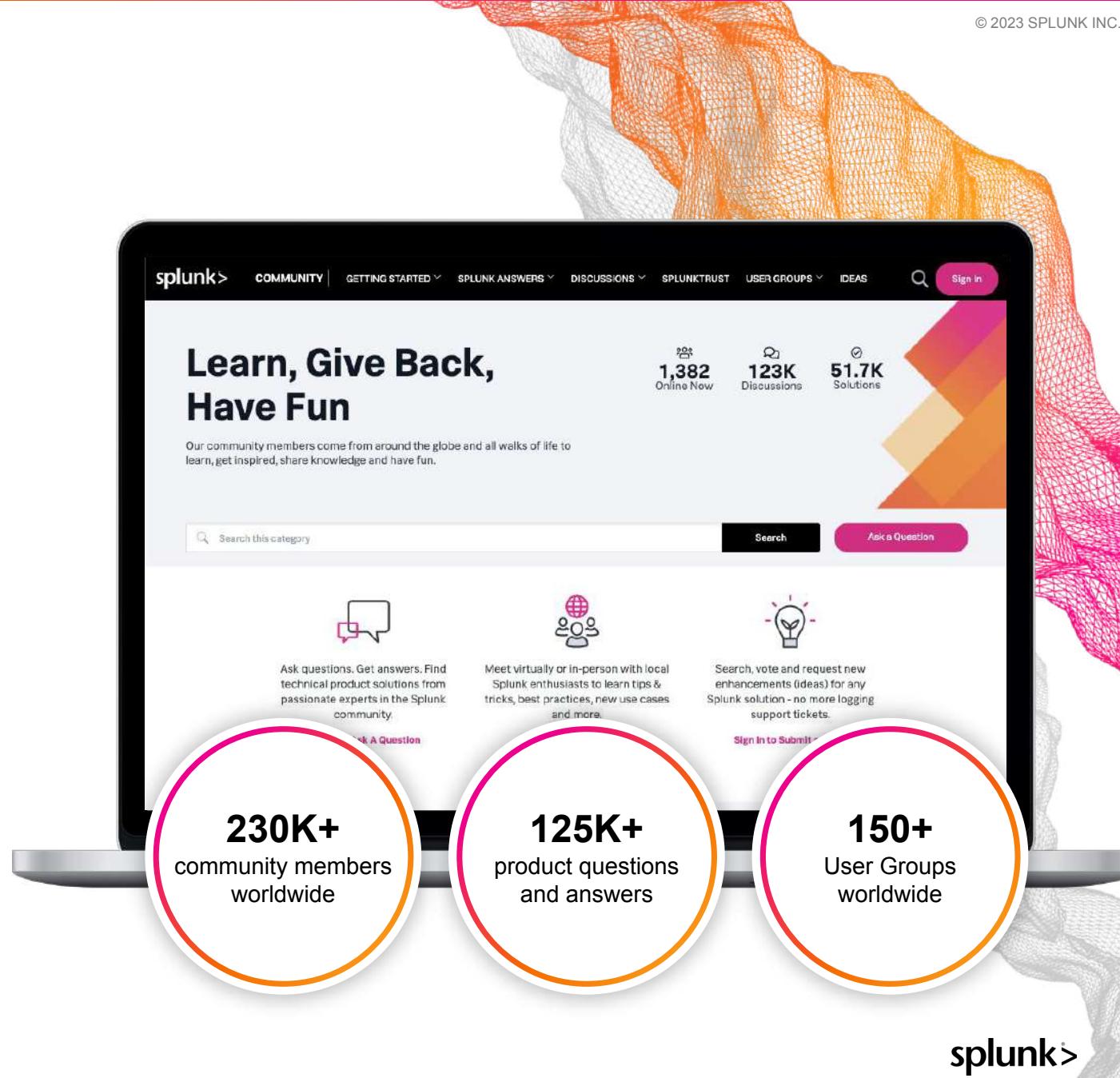
Where to go after
today's workshop

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 Events

<https://events.splunk.com>

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



<https://conf.splunk.com>

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

Splunk Events

Join us at an event near you to gain new skills, expand your network and connect with the Splunk community.

Upcoming Events All Event Types All Geographies All Solution Areas Clear All Filters

118 Results

Automation for the Modern SOC: Strategies for Smarter Security Operations

November 9, 2021 | 10:00 AM (GMT)

The SOC is overwhelmed. Analysts are drowning in security alerts and operations work is rife with monotonous, repetitive tasks. There is a talent shortage of qualified security professionals to staff SOCs and to top it all off, mean time to detect, triage, and respond to threats is still too slow. Sound familiar? Stop being overwhelmed. Join us on 9 November at 10AM GMT/11 AM CET and we'll teach you how Splunk SOAR allows you to work smarter, respond faster, and strengthen your defenses in both on-prem and cloud environments.

Documentation

<https://docs.splunk.com>

- Search reference for SPL

- Step-by-step tutorials

Search

<https://splk.it/SplunkSearchTutorial>

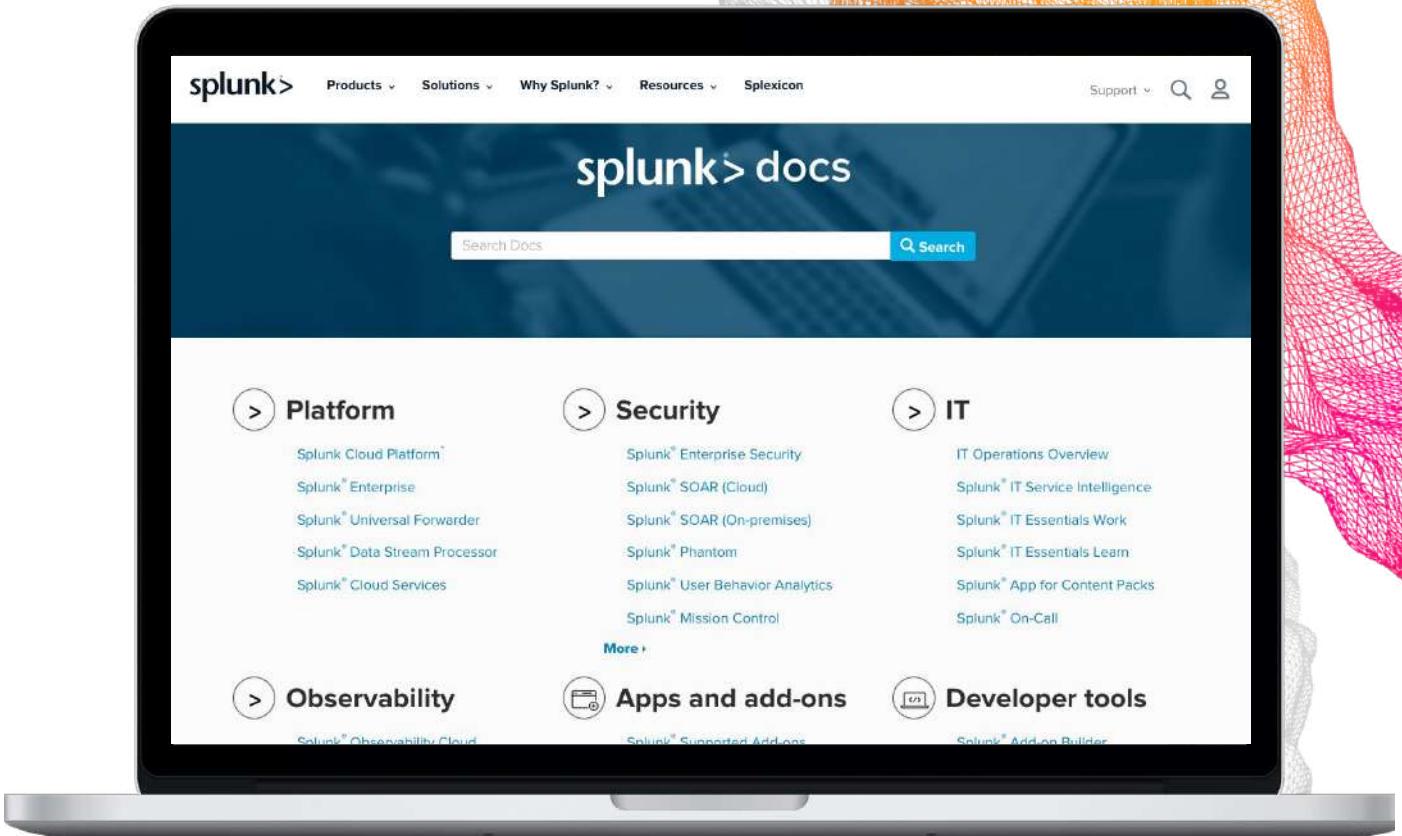
Dashboard Studio

<https://splk.it/SplunkDashStudioTutorial>

- Product references

- Procedures/guides

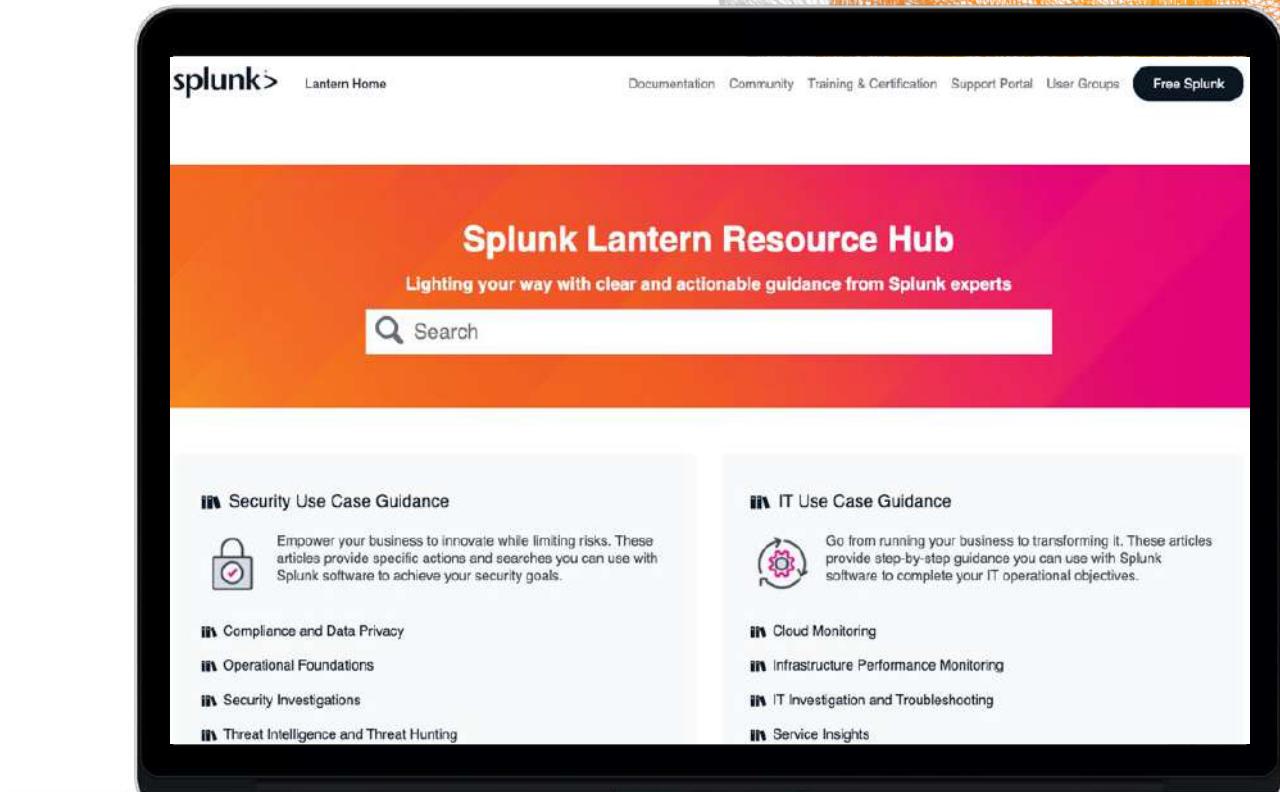
- And more!



Splunk Lantern

<https://lantern.splunk.com>

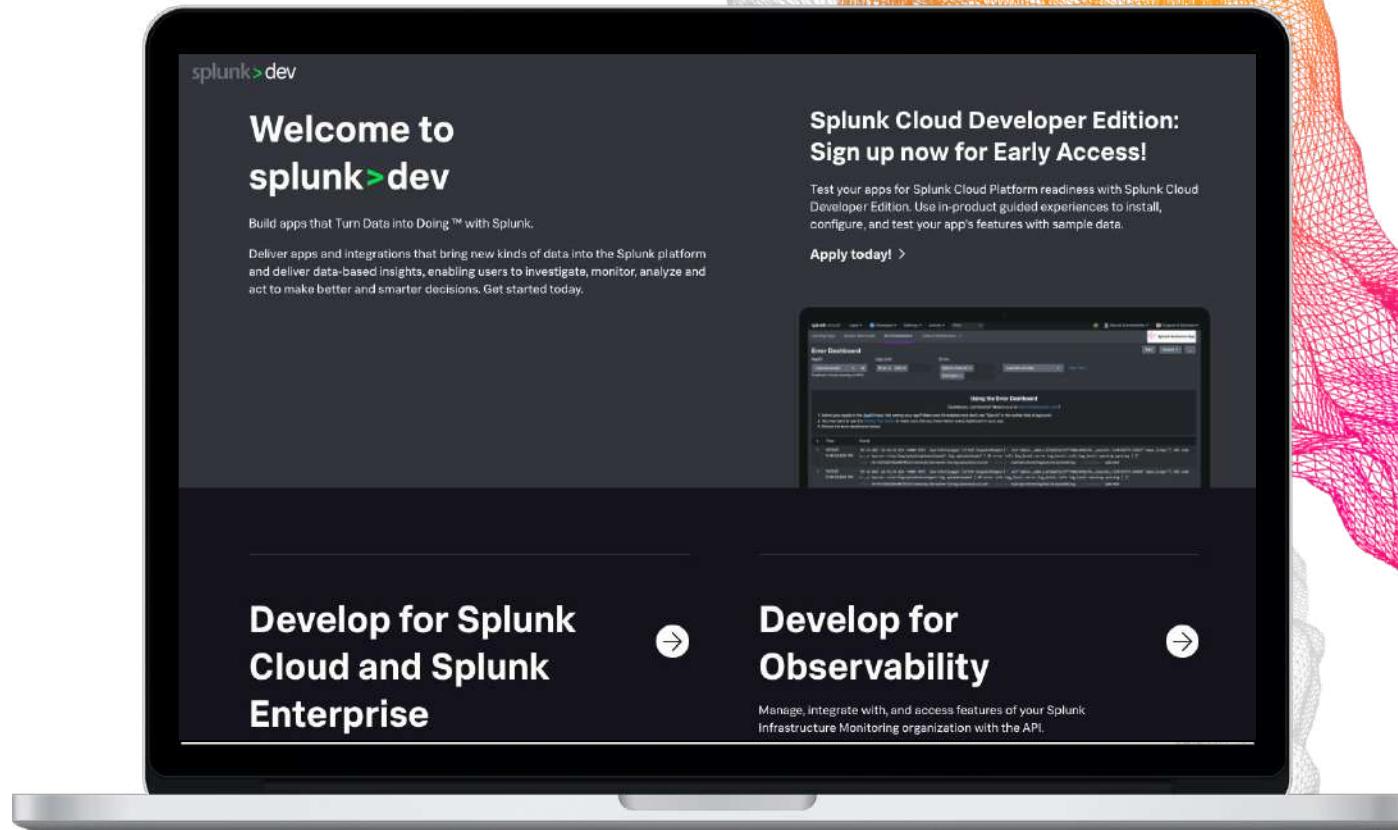
- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation



Developer Resources

<https://dev.splunk.com>

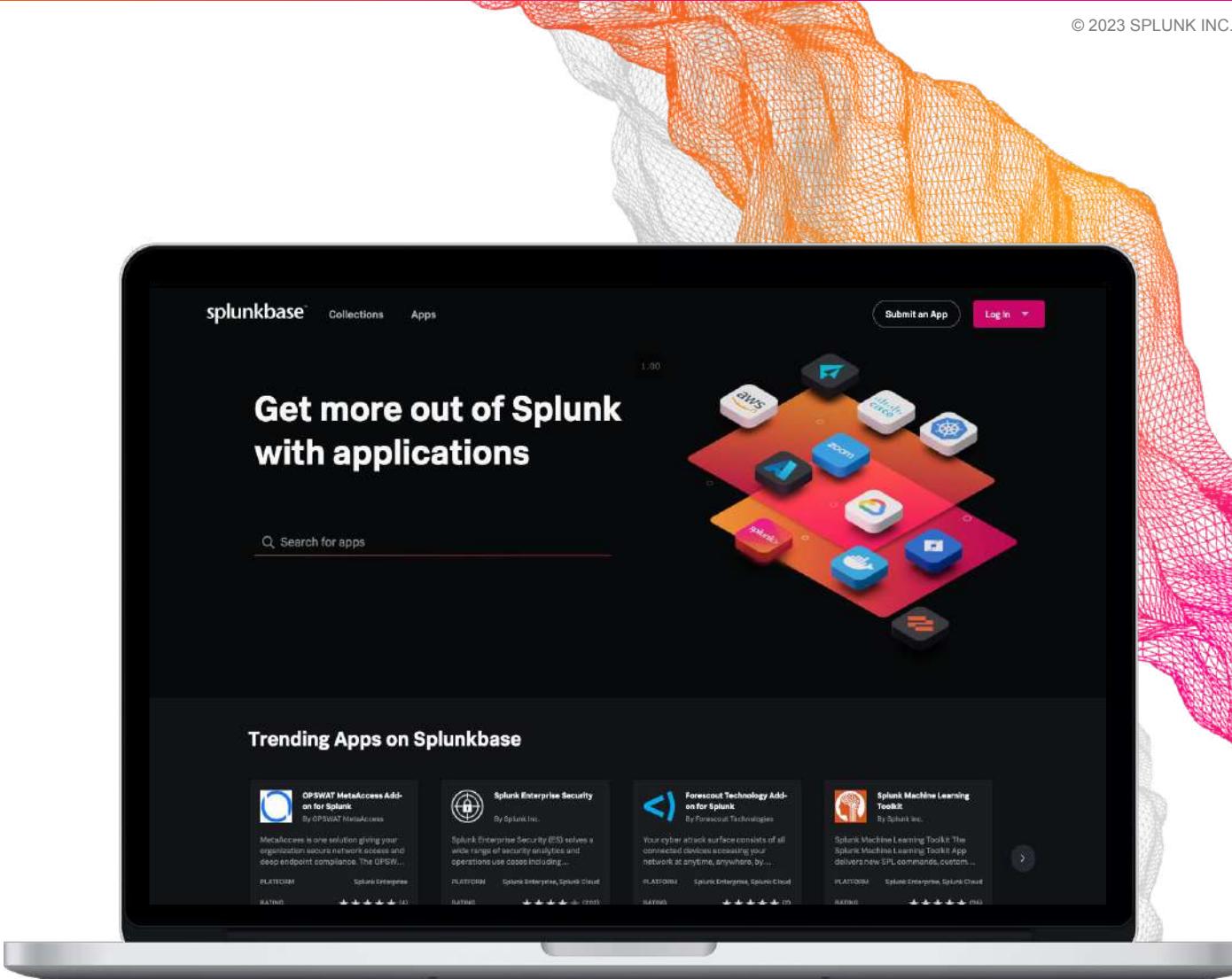
- Developer Guide
- API Reference
- Tutorials
- Downloads
APIs, libraries, tools
- Code examples
- Free Developer licence
- Splunk Cloud Developer Edition
Test your apps for Splunk Cloud readiness



Splunk Apps & Add-ons

<https://splunkbase.splunk.com/>

- 2800+ 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

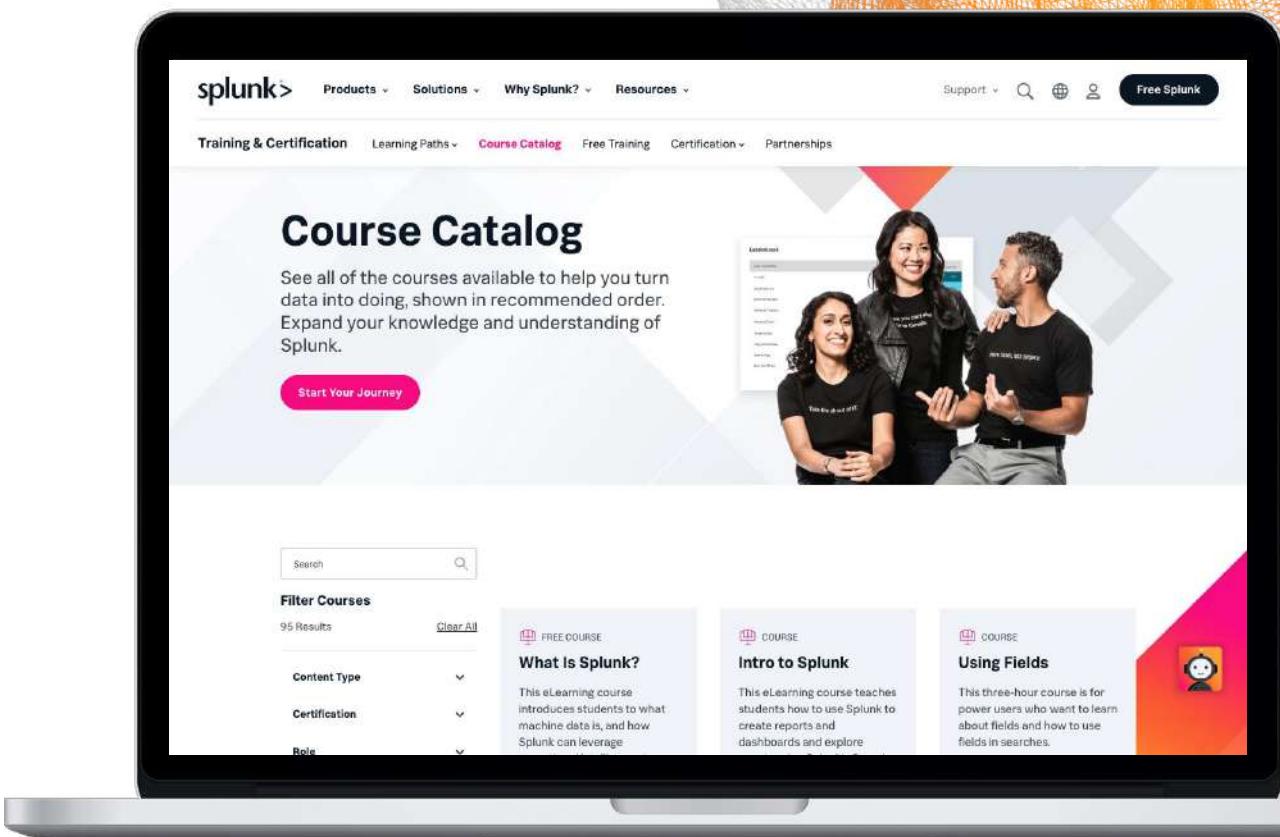
User, Power User, Admin, Architect and Developer

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



Thank You!

