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>

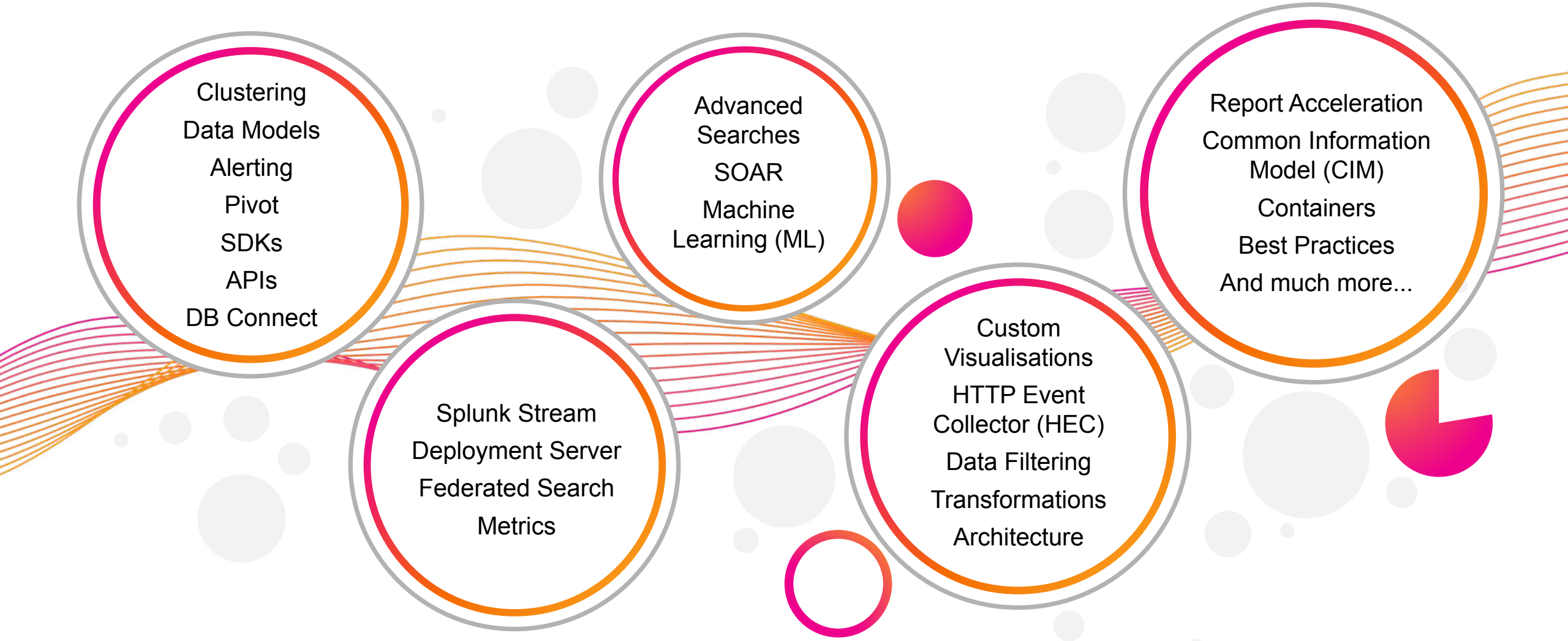
Welcome to Telco Analysts Hands-on Workshop!

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



Visit https://splunk.com/training to learn more!

splunk>

Objective

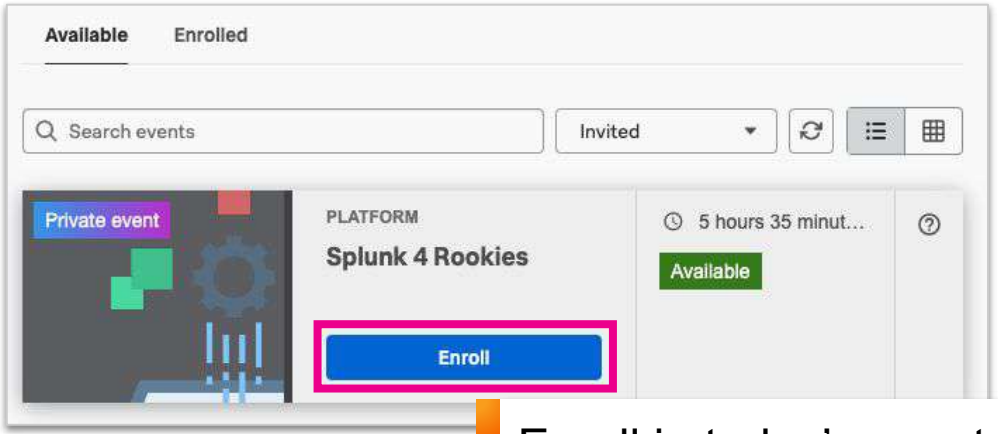
splunk>

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download a copy of today's slide deck: https://splk.it/TelcoAnalyst-Attendee

Goal



Enroll in today's event

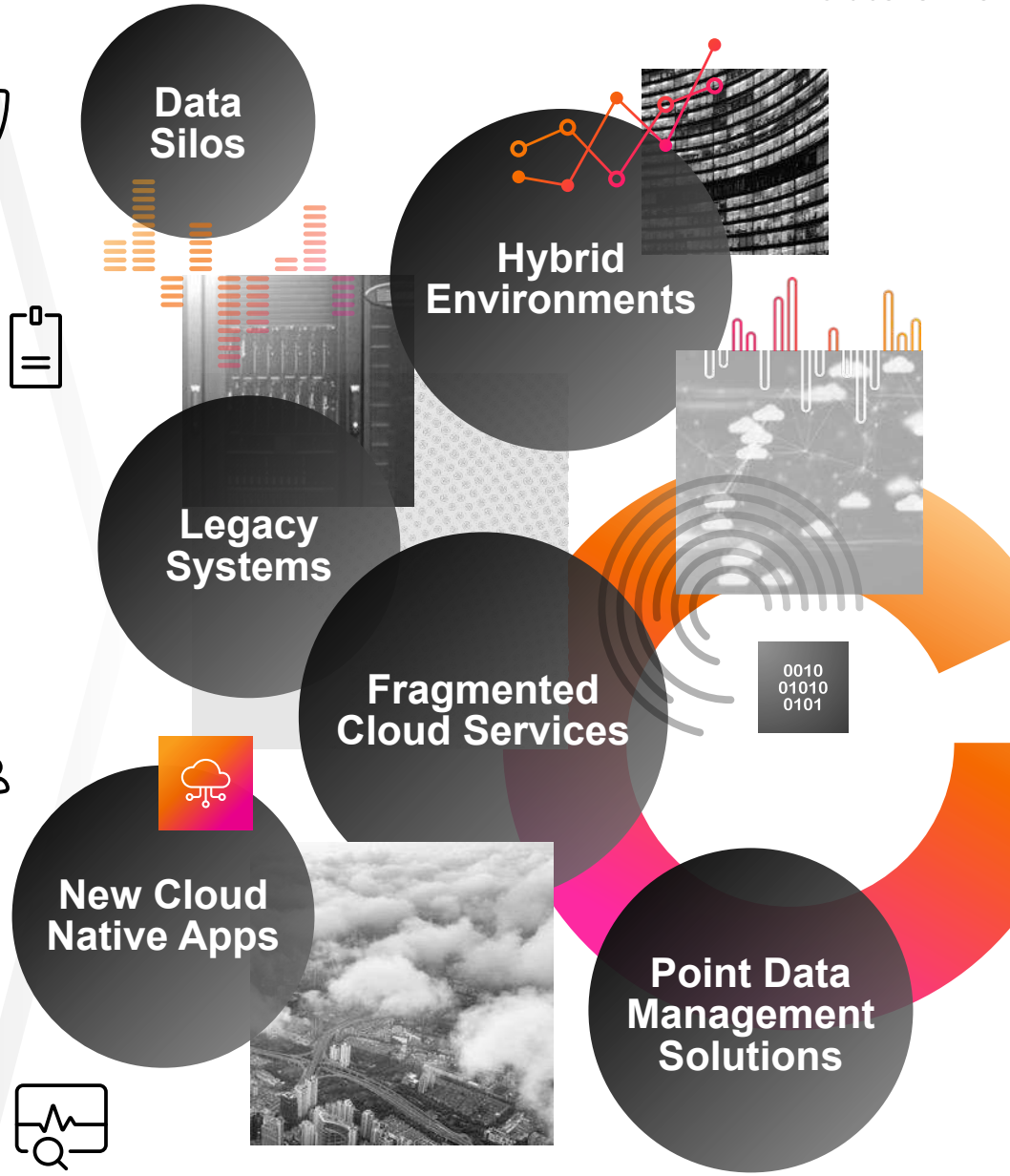
Splunk Solution Intro

Data is your Competitive Advantage

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

splunk> turn data into doing

Turning Real-time Data Into Action is Hard



splunk>

The Power of Splunk

Delivering Unified Security and Observability

See

End-to-end visibility

No sampling or blind spots

Act

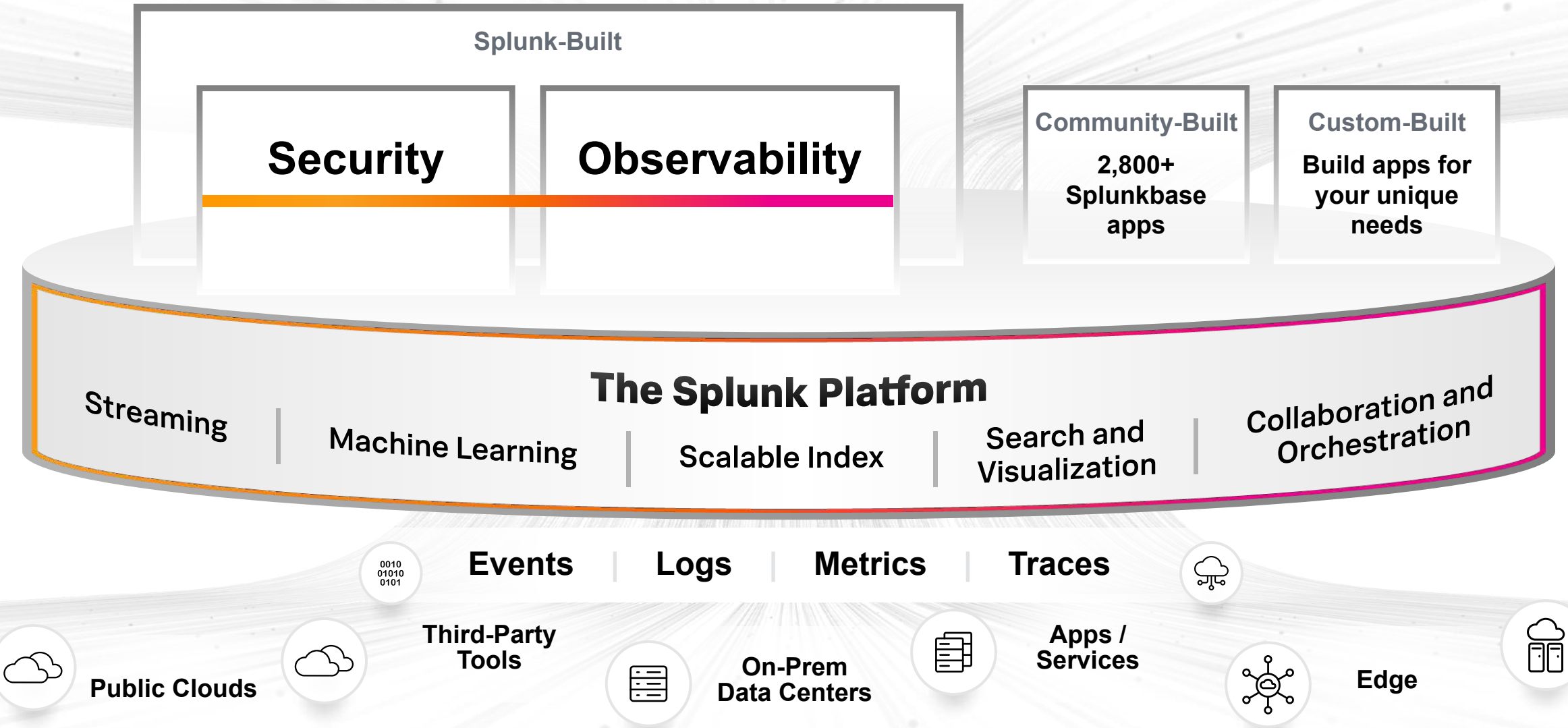
Investigate across massive data sets and take **action** fast

Extend

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

splunk>

The Unified Security and Observability Platform



Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

3 Simple Steps

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

splunk>cloud™

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

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

splunk>

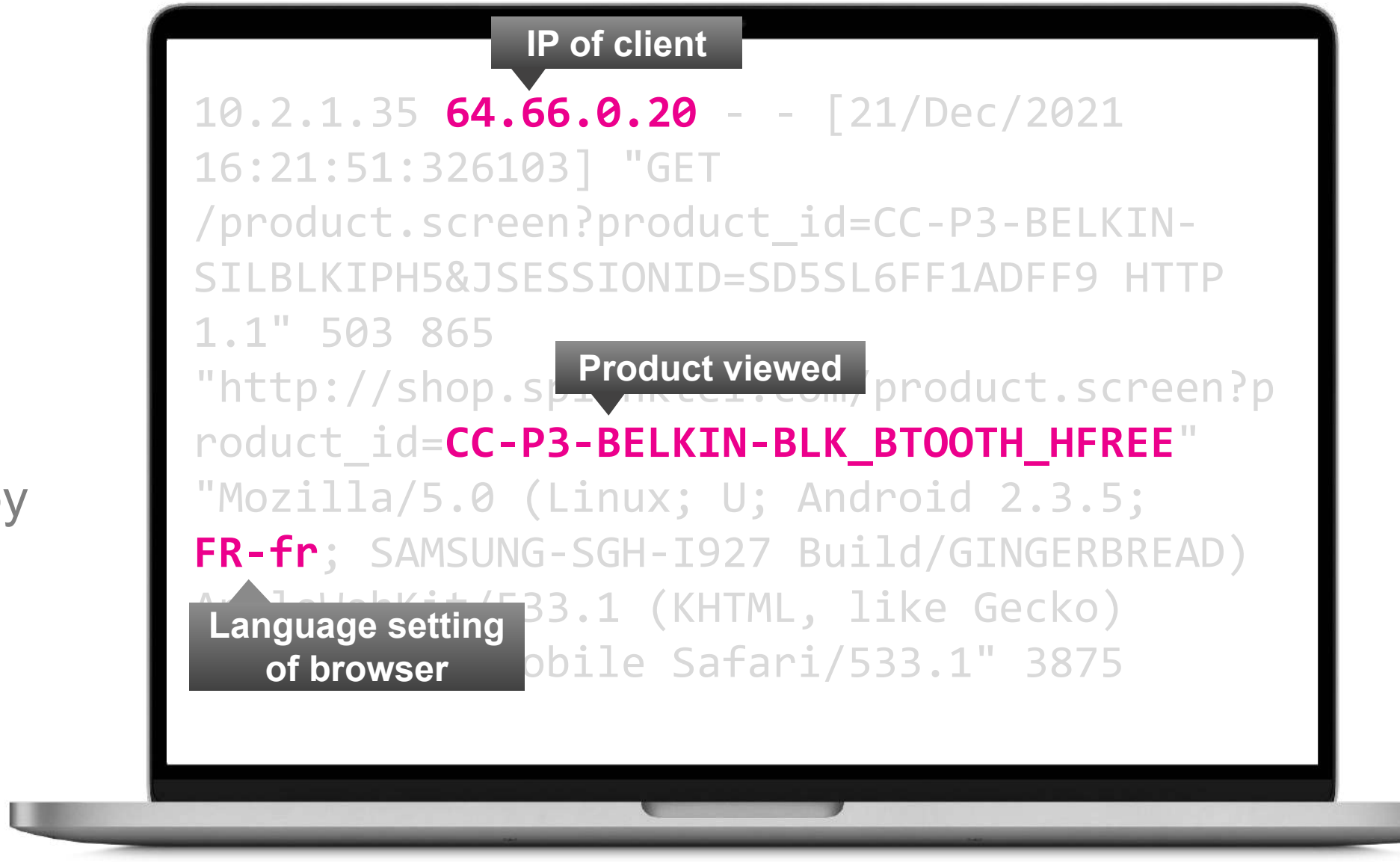
What is a Splunk Universal Forwarder?

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

Machine data is valuable not complex!

Marketing Use Case

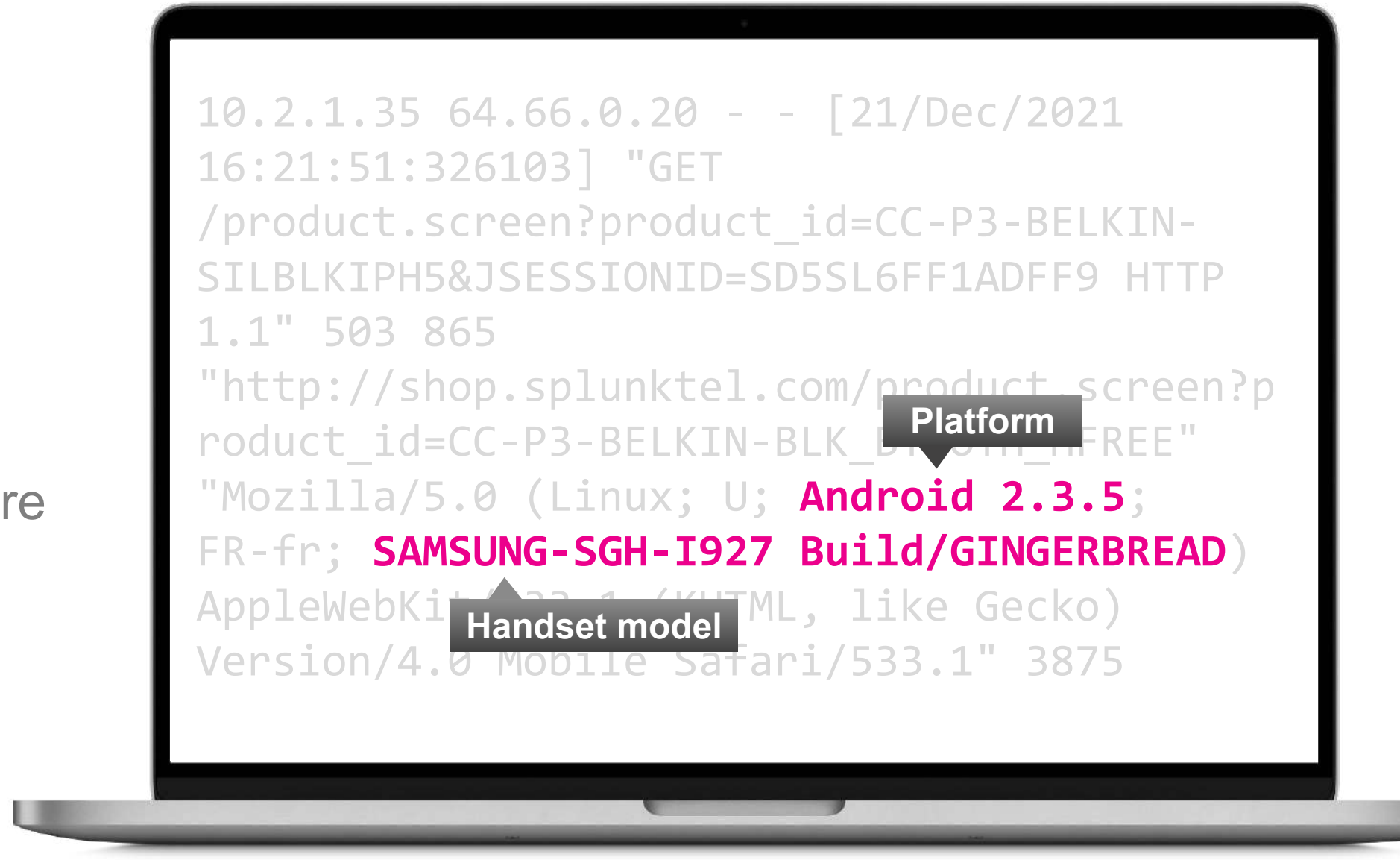
Show the top products viewed by language



splunk>

DevOps Use Case

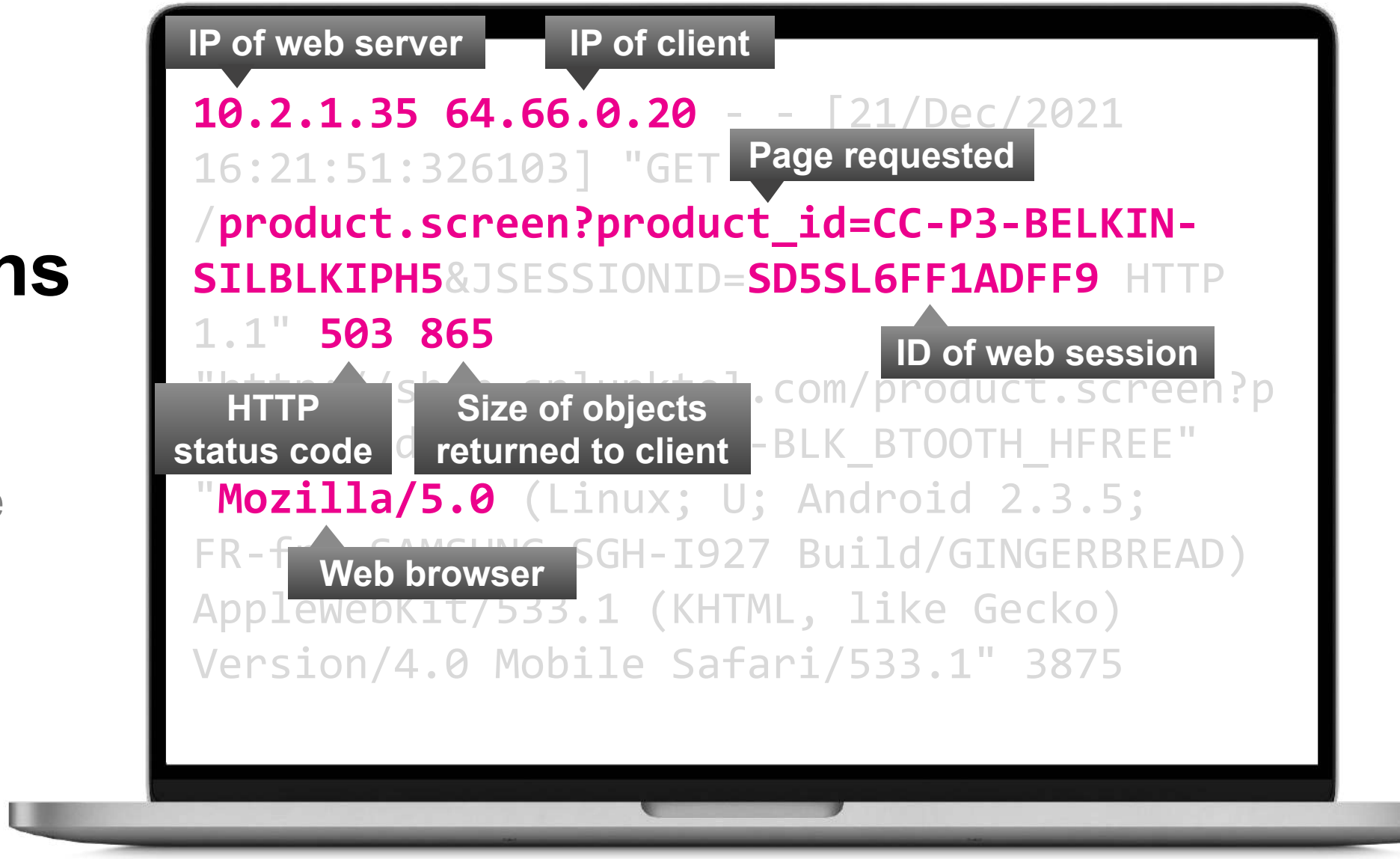
Which mobile handsets should I test the most before releasing my new app?



splunk>

IT Operations Use Case

Which web pages are generating the most errors?



splunk>

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

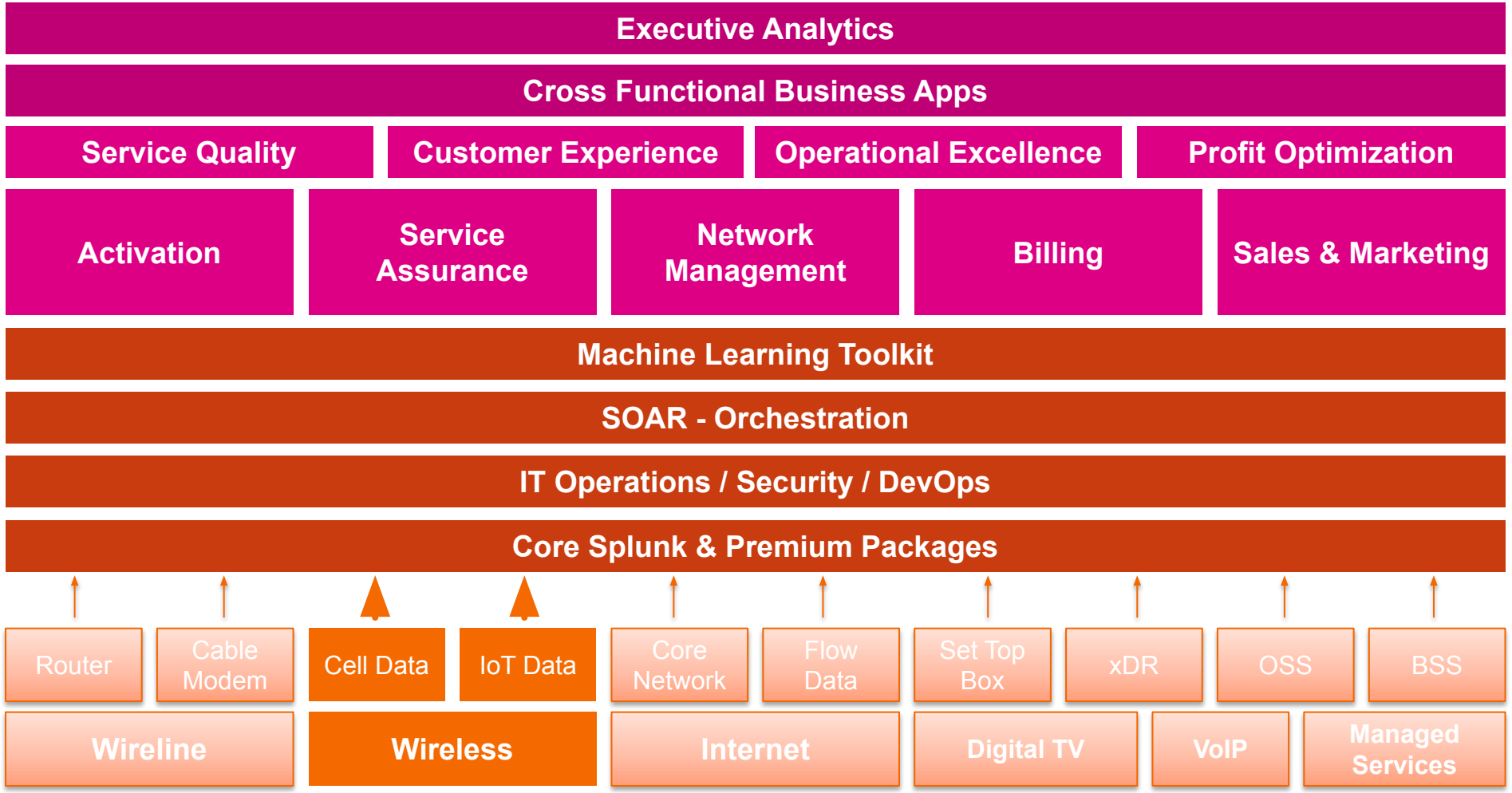
- Churn Prediction
- Truck Dispatch Analytics
- Video Subscriber Analytics
- Reducing SLA Violations
- Real-Time Vulnerability Management
- Roaming Fraud Detection
- PBX/IP-PBX Fraud Mitigation
- Subscriber Fraud Protection
- Subscriber Endpoint Security
- Automated Compliance Reporting
- Data Center 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>

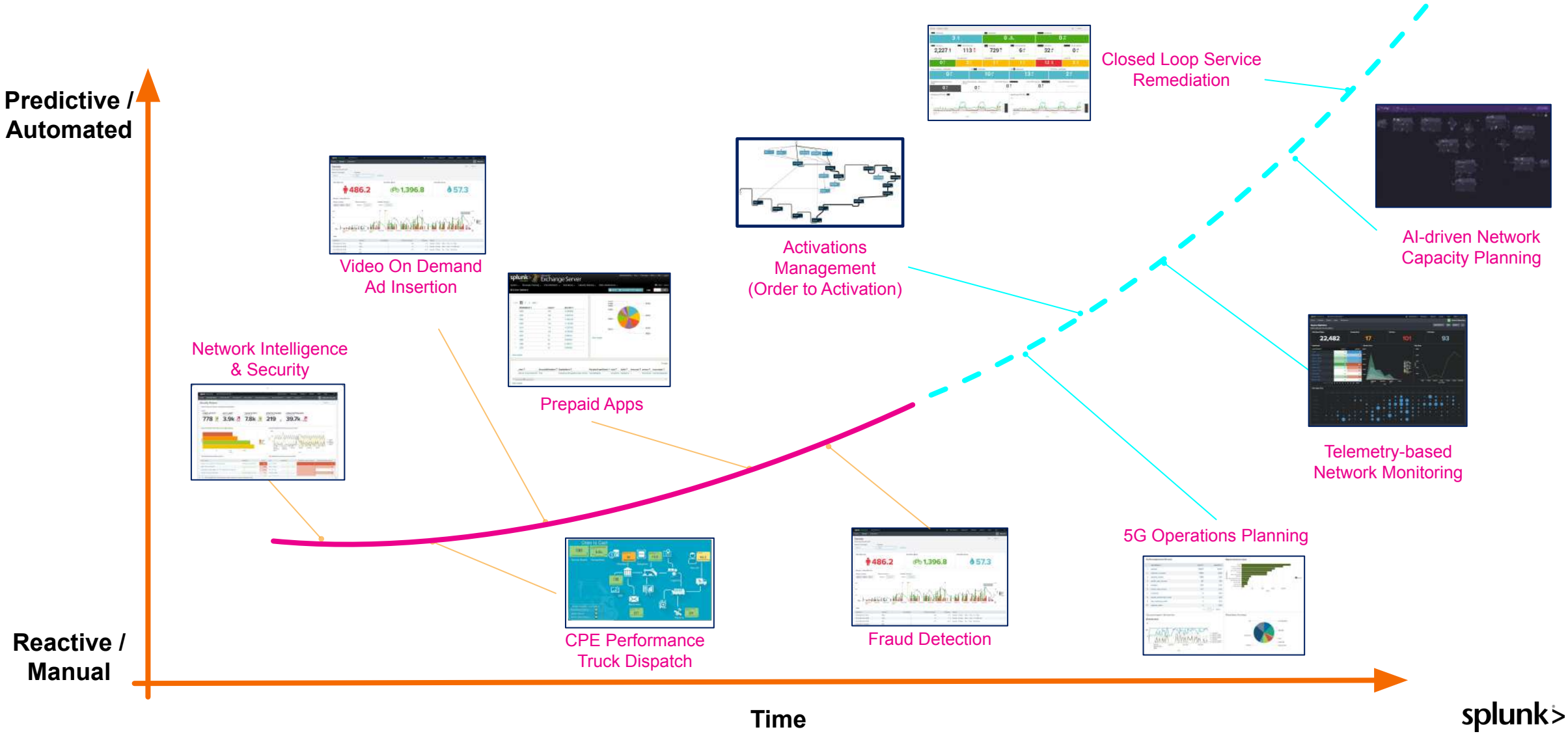
Splunk in Telco Operations



splunk>

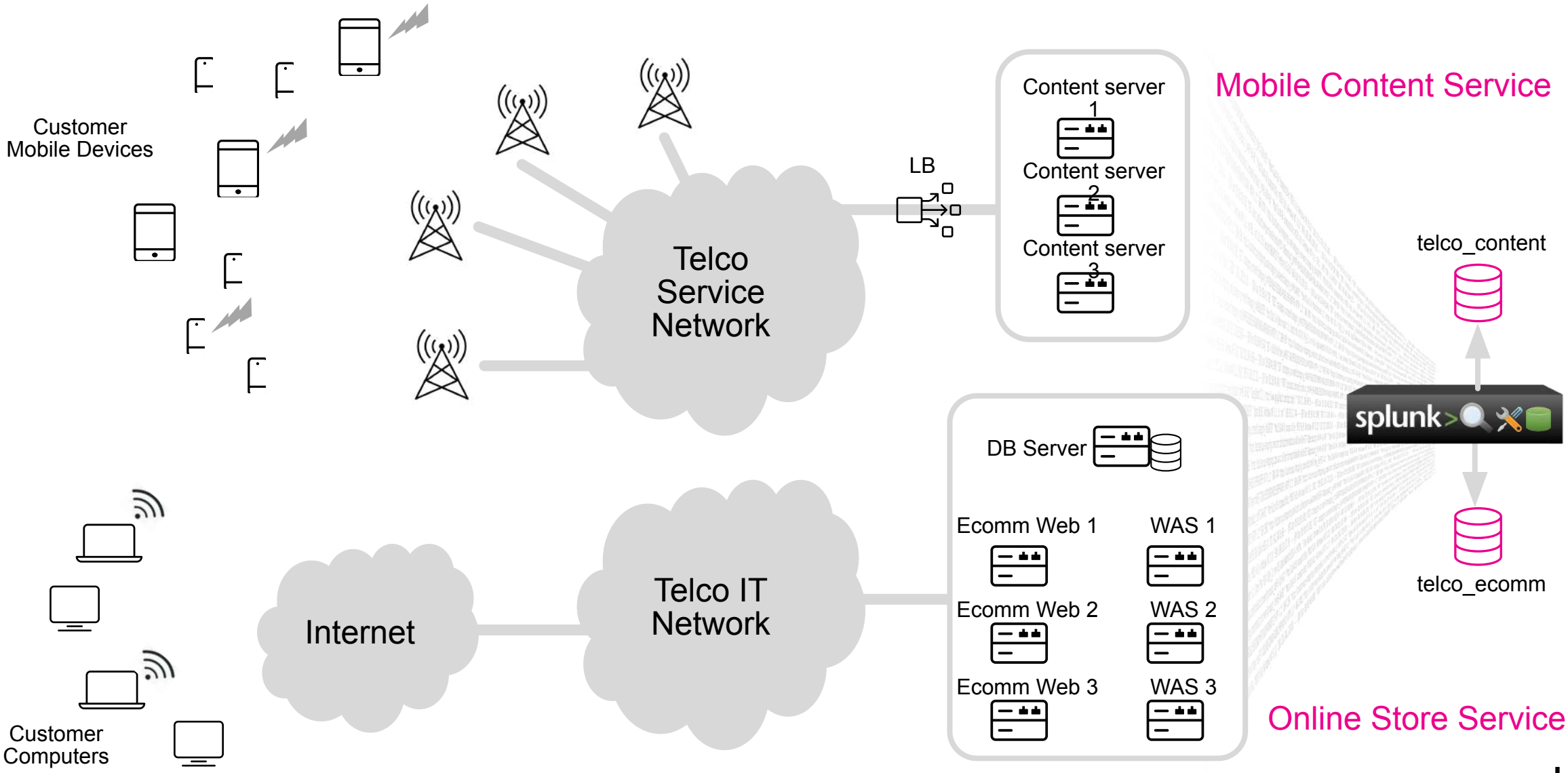
Telco Operational Maturity Model Example

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



splunk>

Today's Hands-on Environment



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

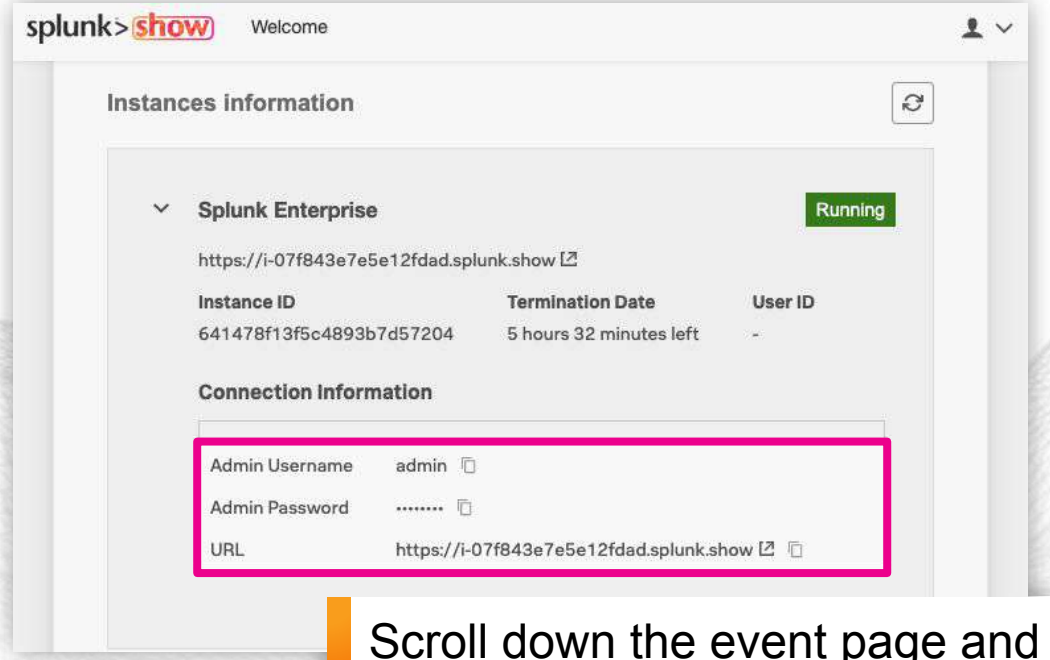
Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

splunk>

Splunk Search Intro

Login to Splunk

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



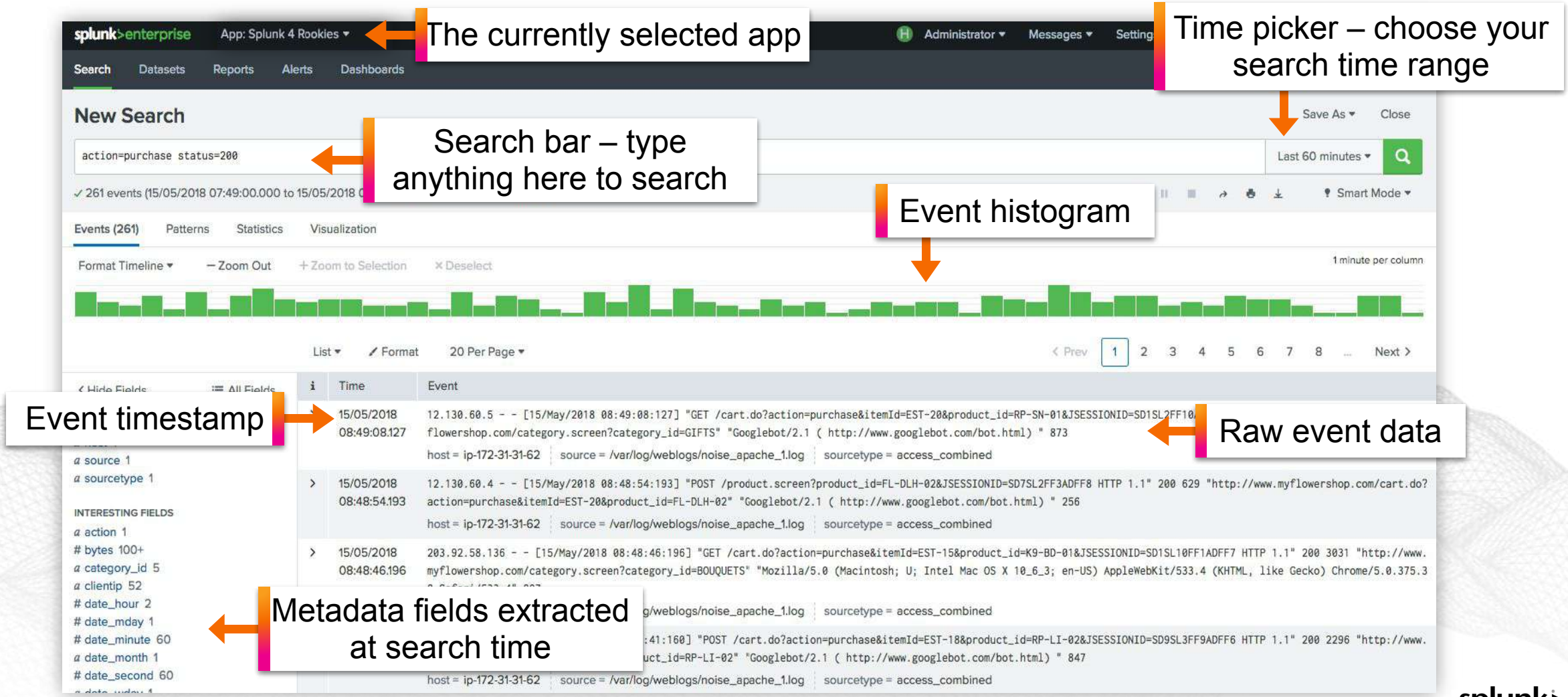
Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

Log in to your Splunk instance

Login using the credentials from Splunk Show

splunk>

Open your app and have a play!



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

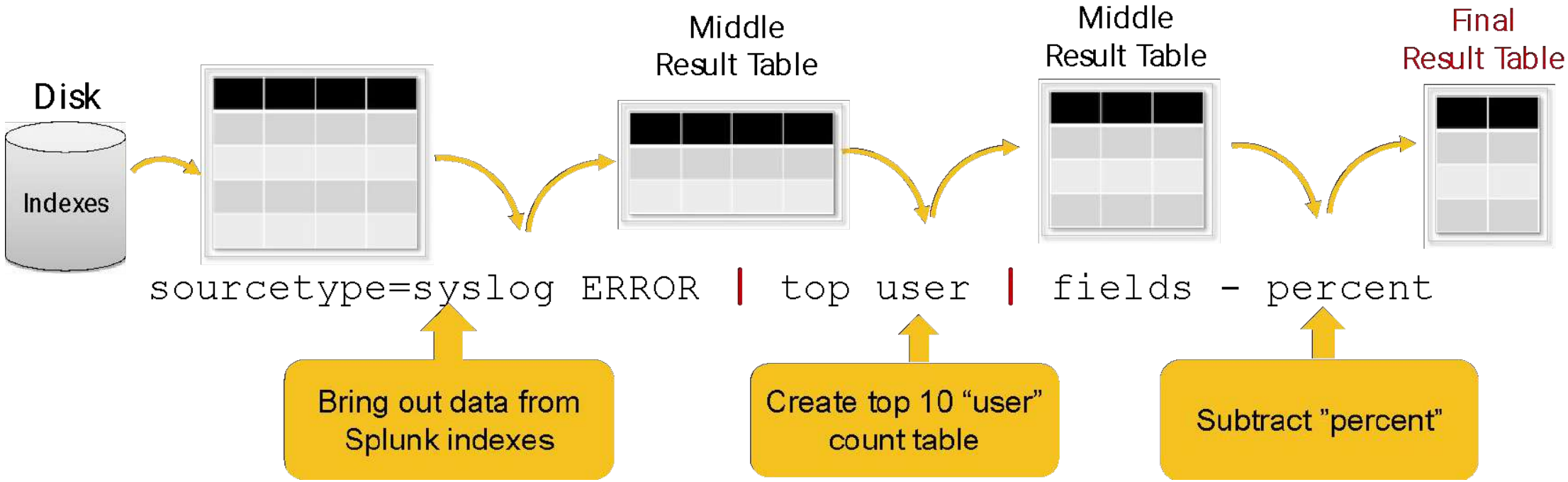
Add-ons

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

splunk>

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>

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?

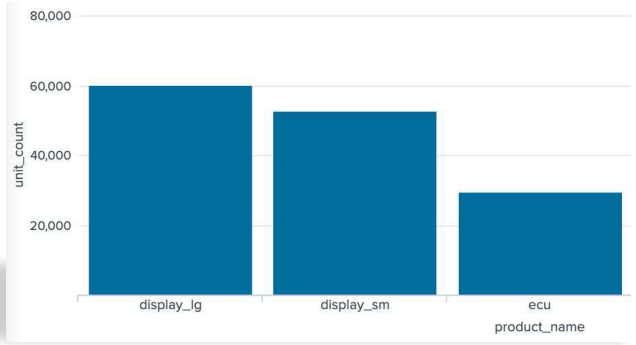
```
status=200 NOT action=purchase
status=200 action!=purchase
```

Splunk
Analysis Method Intro

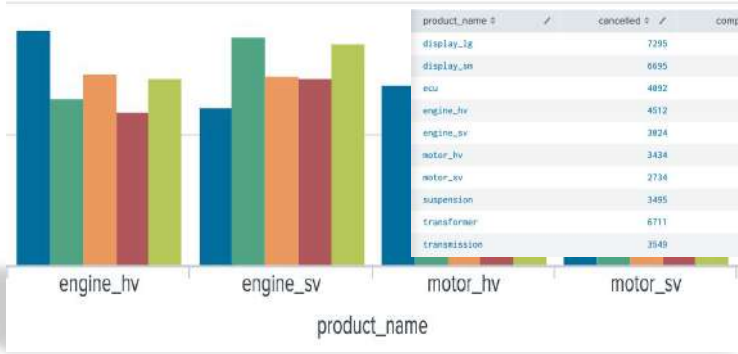
splunk>

Analysis Method Introduction

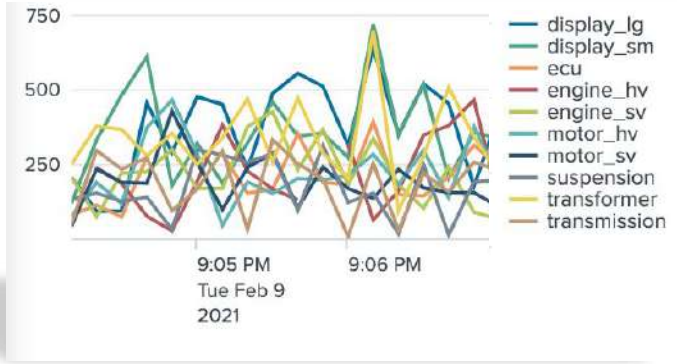
1. Distribution analysis : stats
   - Compare one to another (Example : Performance comparison between one user to another, or one type vs another)



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 on or more users purchase contents over time)



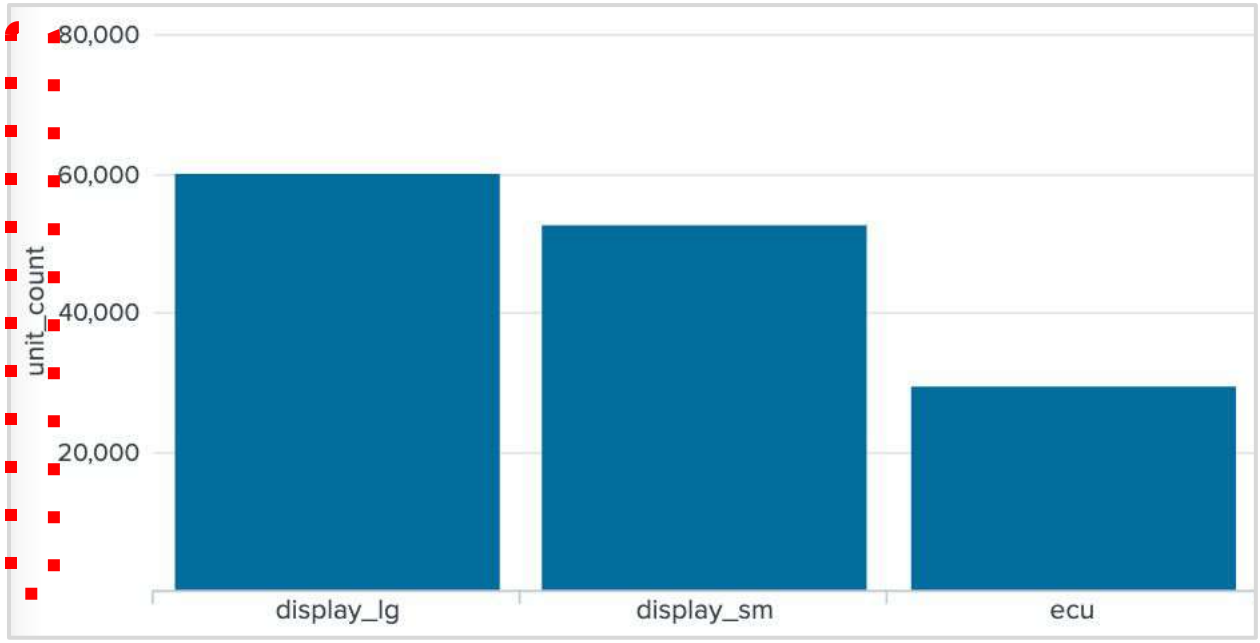
splunk>

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.

sum(unit_count)



by product_name

Function

stats sum(unit_count) **by** product_name

Group by segmentation

splunk>

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.

splunk>

Analysis Technique 1 : Distribution

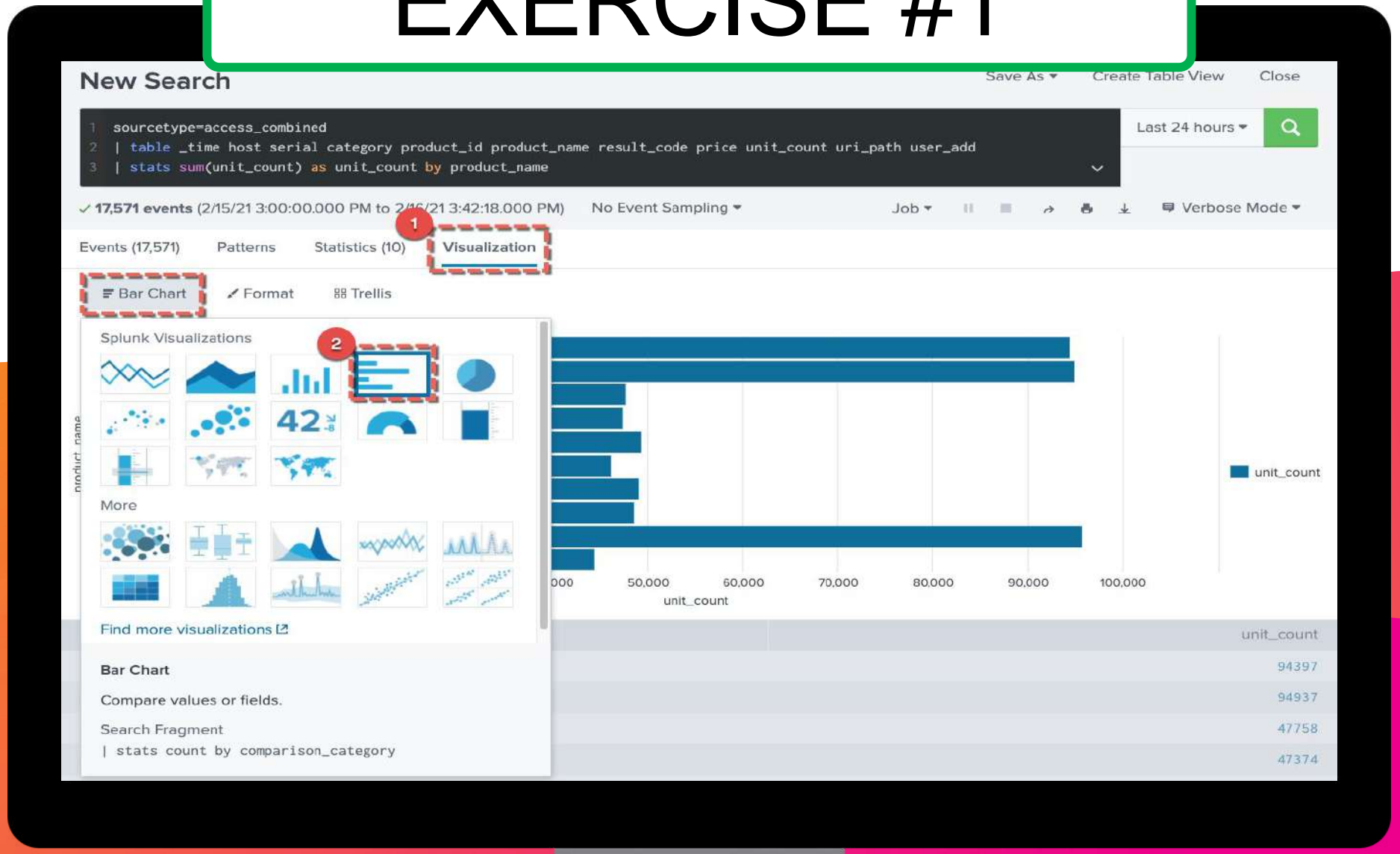
Syntax :

```
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



Today's Scenario: My Telco Content Service

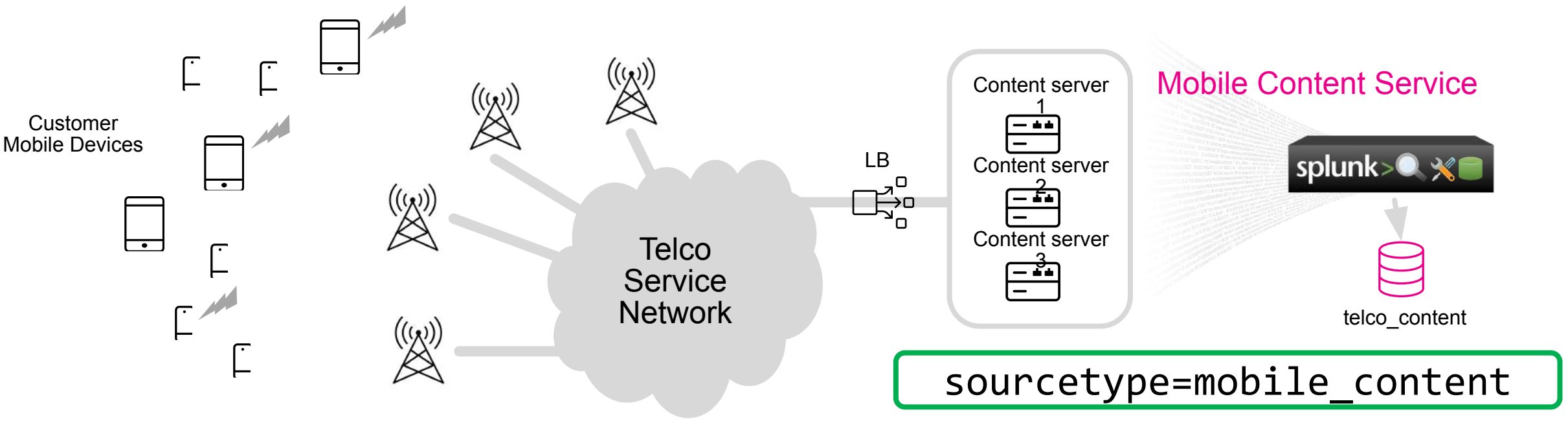
Your Company

- 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

- /category.screen
- /low_def_contents.screen
- /oldlink
- /mobile_download.do

clientip

- 150.3.146.153
- 88.194.254.1
- 39.121.36.4
- 26.63.71.69

status

- 200
- 503
- 406
- 400

bytes

- 123 bytes
- 543
- 3562
- 6524

action

- download
- purchase
- stream
- local_view

user_type

- NEW
- NORMAL
- PREMIUM

useragent

- Mozilla/5.0 (CrKey
- Mozilla/5.0 (Linux;
- Mozilla/5.0 (iPad;
- Mozilla/5.0 (iPhone9,4;
- Mozilla/5.0 (iPhone;

product_id

- RWZ-239-02
- INW-047-08
- UYV-088-08
- JYJ-901-03

method

- get
- post

timetaken

- 538 ms
- 2359
- 982
- 245

user_add

- FOOT_HILLS
- PACIFIC_NE
- NORTH_BAY
- SAN_FRANCISCO

user_age

- 40 years
- 30
- 72
- 27

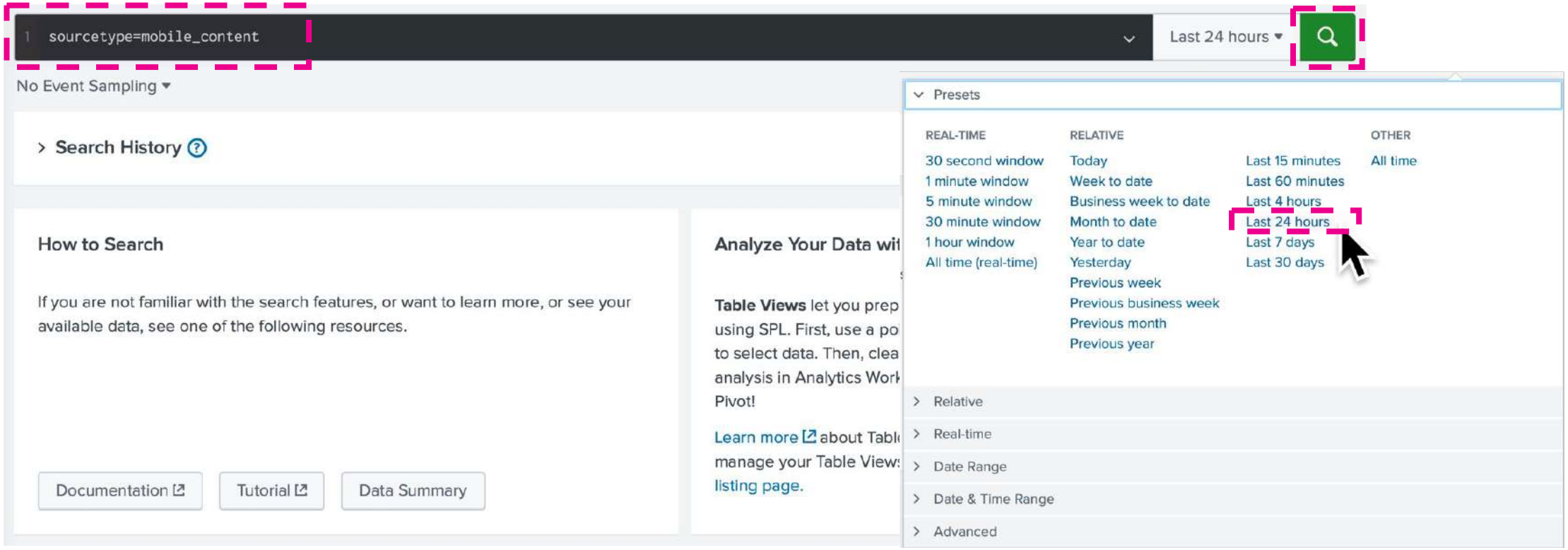
splunk>

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
```



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

splunk>

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
```

Events (42,997) Patterns Statistics (42,997) Visualization

100 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next

_time	host	clientip	SESSIONID	category_id	method	uri_path	product_id	product_name	status	action
2022-10-03 12:34:44.144	mobile-content-03.mytelco.com	62.252.205.105	SD7SL9FF1ADFF1	ACTION:CRIME:DRAMA:FILM-NOIR	GET	/mobile_contents.do.do	KNE-963-00	Nightwing	503	purchase
2022-10-03 12:34:43.125	mobile-content-03.mytelco.com	30.194.142.20	SD3SL2FF4ADFF8	DRAMA:FILM-NOIR	GET	/category.screen			200	
2022-10-03 12:34:42.149								ine and ie Go ting line et ie vont en eau)	503	download_remove
2022-10-03 12:34:42.143									400	
2022-10-03 12:34:42.140	03.mytelco.com							and Jerry: utcracker Tale	200	skip

uri_path
- /category.screen
- /low_def_contents.screen
- /oldlink
- /mobile_download.do

clientip
- 150.3.146.153
- 88.194.254.1
- 39.121.36.4
- 26.63.71.69

status
- 200
- 503
- 406
- 400

bytes
- 123 bytes
- 543
- 3562
- 6524

action
- download
- purchase
- stream
- local_view

user_type
- NEW
- NORMAL
- PREMIUM

useragent
- Mozilla/5.0 (CrKey
- Mozilla/5.0 (Linux;
- Mozilla/5.0 (iPad;
- Mozilla/5.0 (iPhone9,4;
- Mozilla/5.0 (iPhone;

product_id
- RWZ-239-02
- INW-047-08
- UYV-088-08
- JYJ-901-03

method
- get
- post

timetaken
- 538 ms
- 2359
- 982
- 245

user_add
- FOOT_HILLS
- PACIFIC_NE
- NORTH_BAY
- SAN_FRANCISCO

user_age
- 40 years
- 30
- 72
- 27

splunk> turn data into doing

Analysis Technique 1 : Exercise 1

STEP 02 – Explore data and understand context

Field Name	Value
_time	Time of event occurence
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

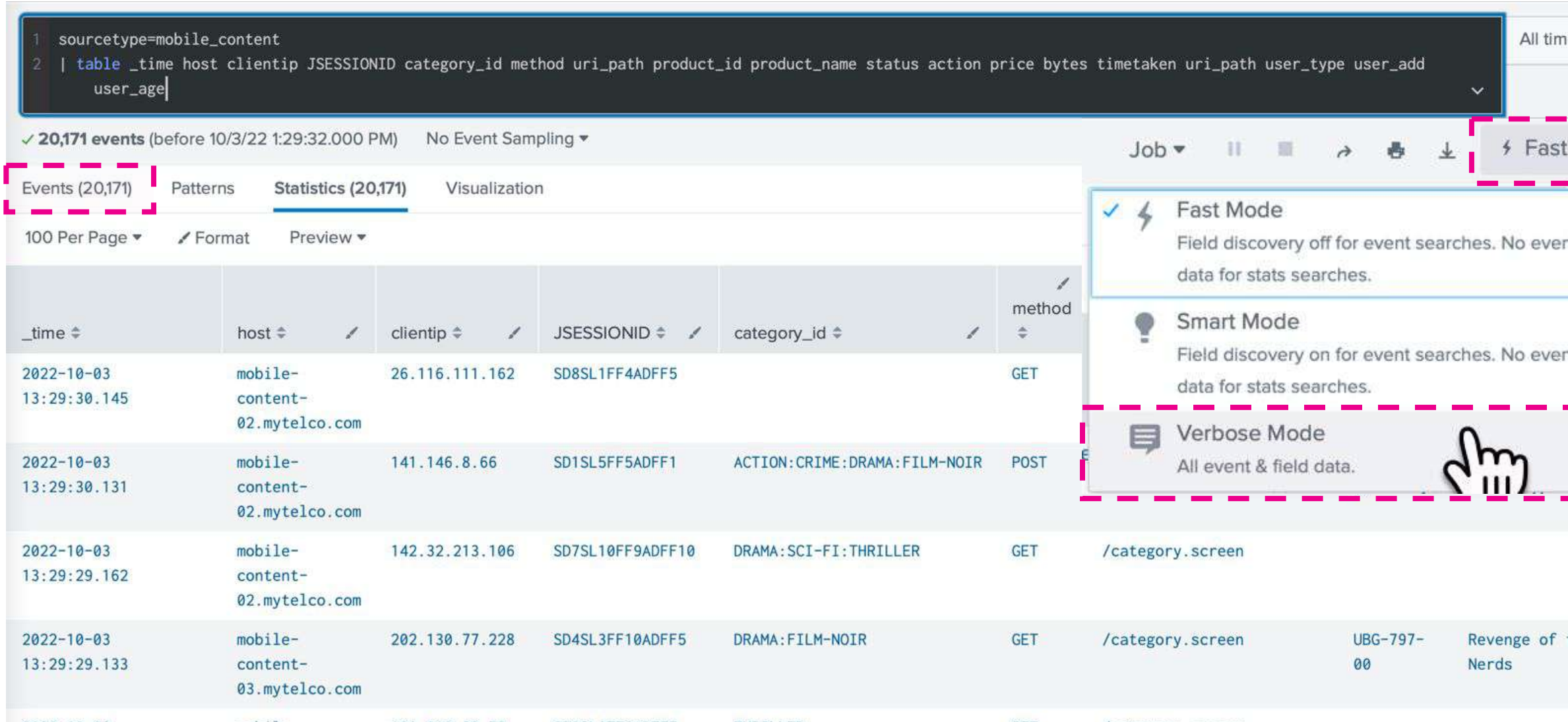
Field Name	Value
uri_path	Accessed URI, API module
user_type	Customer type
user_add	Customer address
user_age	Customer Age

splunk>

Analysis Technique 1 : Exercise 1

STEP 02 – Explore data and understand context

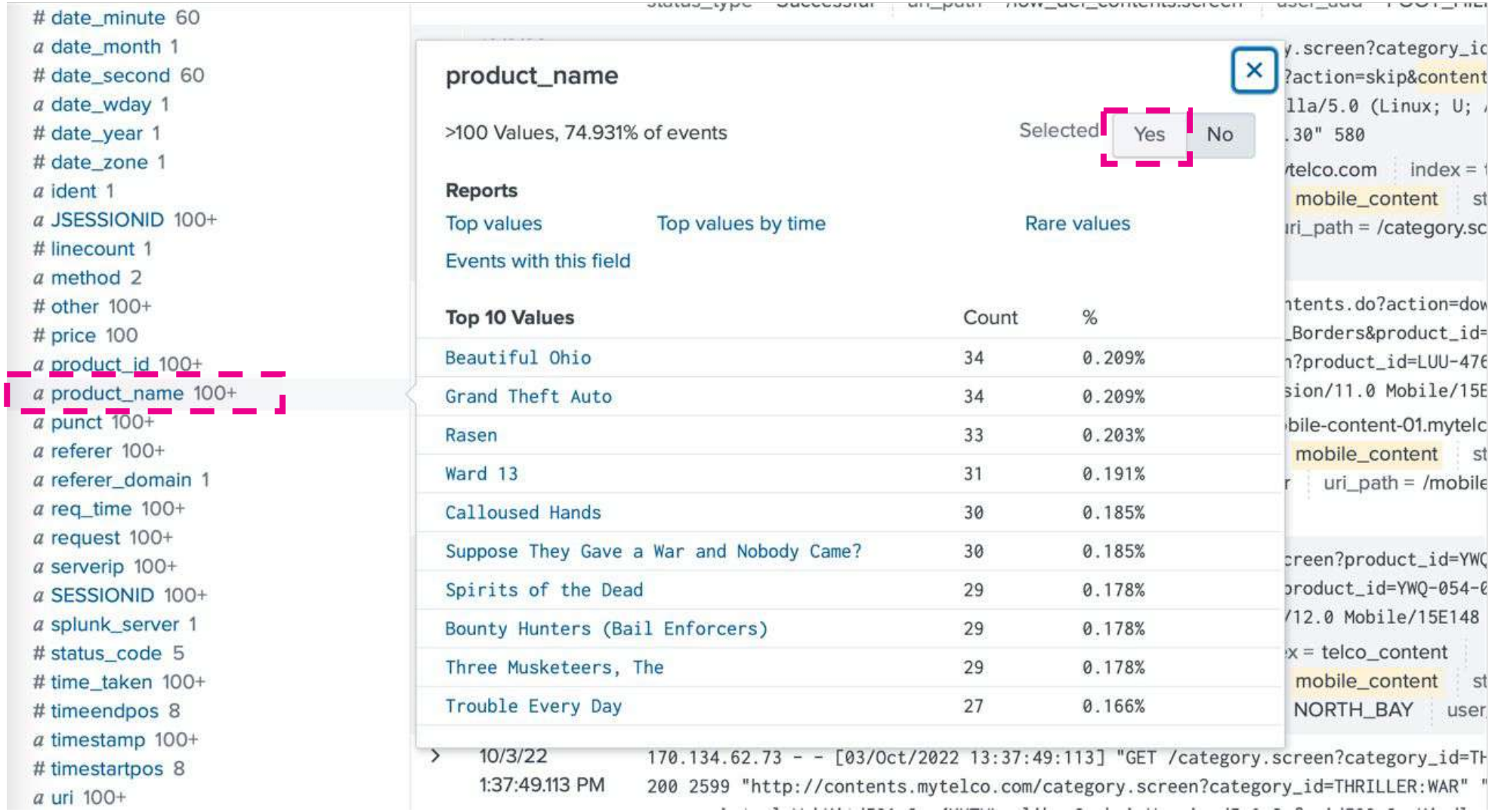
Click on “Event” tab to get back into data exploration interface. Select a few of the fields defined above to get familiarized with what information they include.



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.



splunk>

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

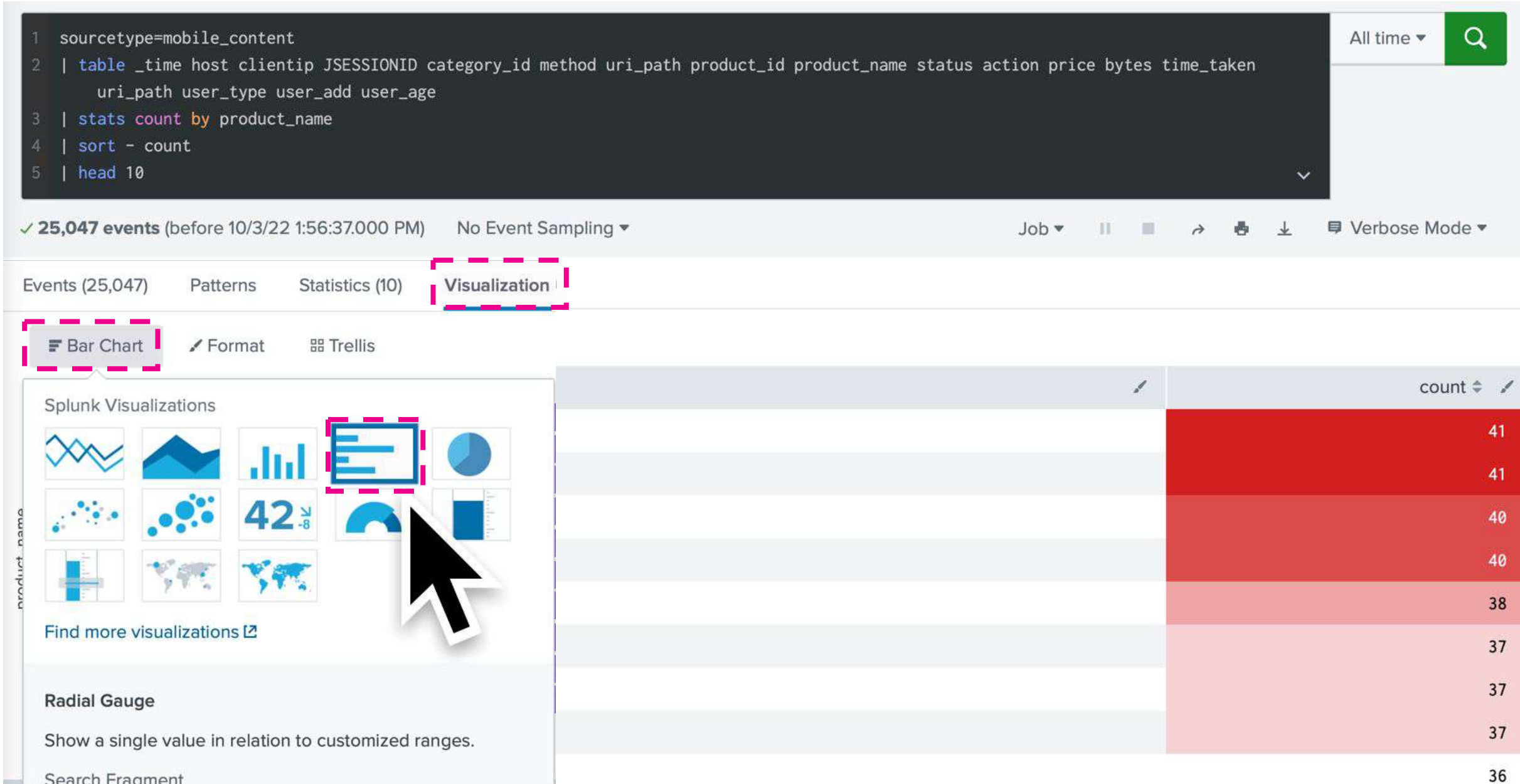
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id product_name
status action price bytes time_taken uri_path user_type user_add user_age
| stats count by product_name
| sort - count
| head 20
```

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

splunk>

Analysis Technique 1 : Exercise 1

STEP 04 – Visualization



Analysis Technique 1 : Exercise 1

STEP 04 – Visualization

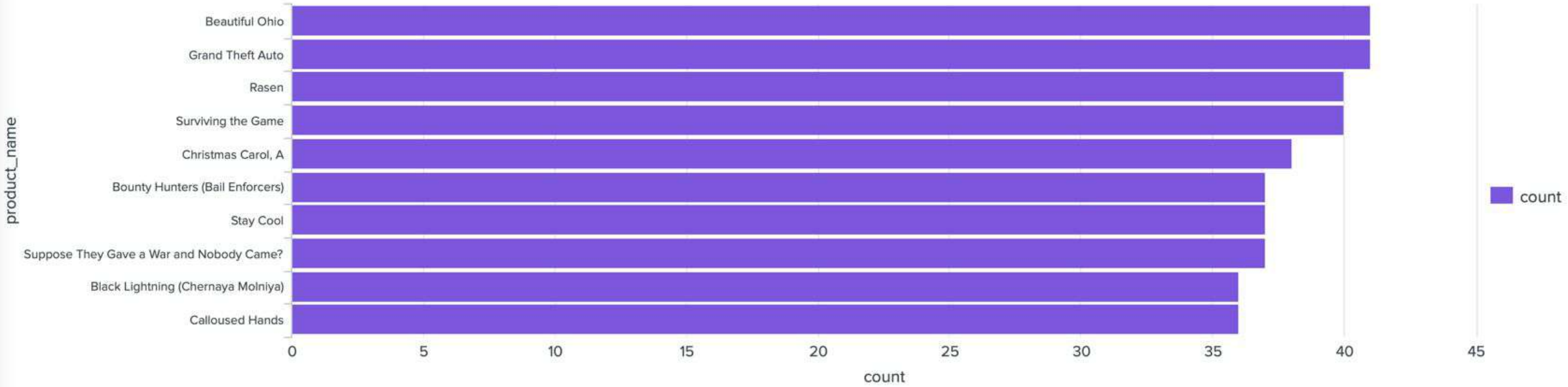

```
1 sourcetype=mobile_content
2 | table _time host clientip JSESSIONID category_id method uri_path product_id product_name status action price bytes time_taken
    uri_path user_type user_add user_age
3 | stats count by product_name
4 | sort - count
5 | head 10
```

All time

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

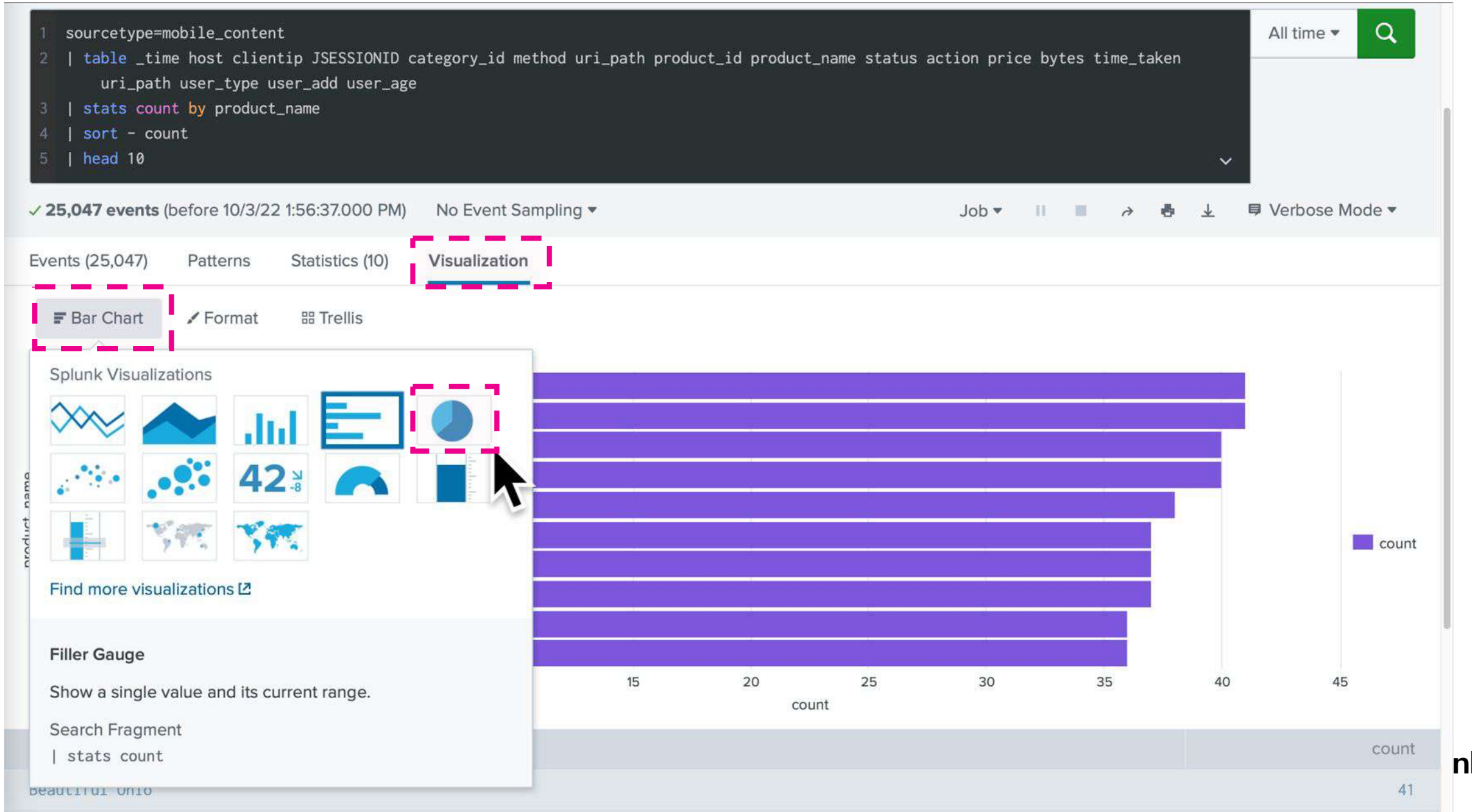
Events (25,047) Patterns Statistics (10) **Visualization**

Bar Chart Format Trellis



Analysis Technique 1 : Exercise 1

STEP 04 – Visualization



Analysis Technique 1 : Exercise 1

STEP 04 – Visualization

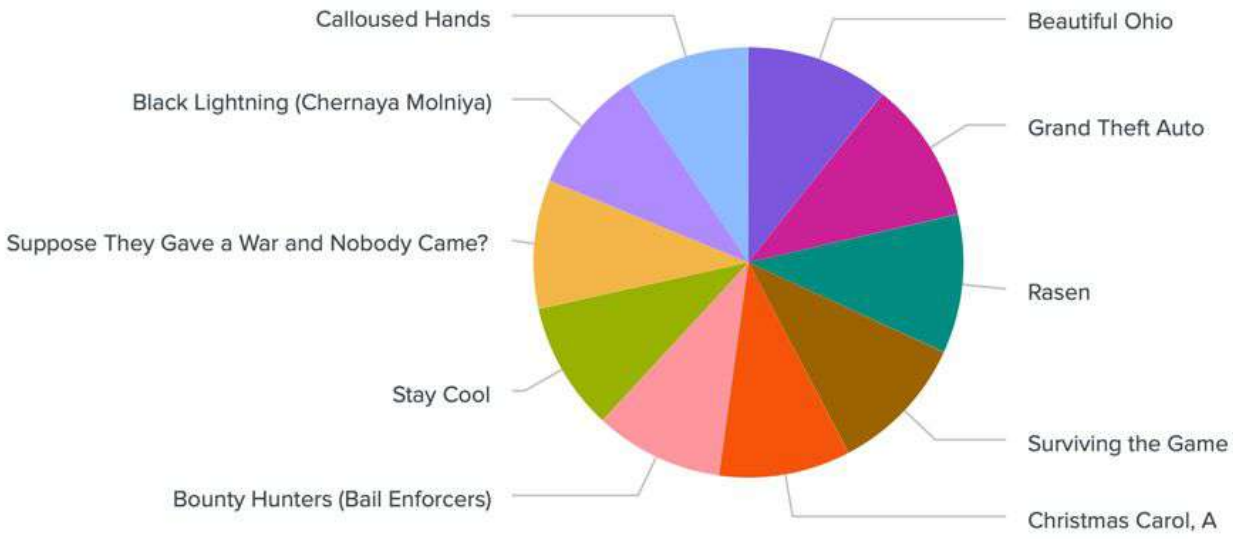

```
1 sourcetype=mobile_content
2 | table _time host clientip JSESSIONID category_id method uri_path product_id product_name status action price bytes time_taken
    uri_path user_type user_add user_age
3 | stats count by product_name
4 | sort - count
5 | head 10
```

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**

Pie Chart Format Trellis



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


```
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, avg(time_taken) as time_taken by product_name
4 | sort - count
5 | head 10
```

All time

✓ **28,103 events** (before 10/3/22 2:13:12.000 PM) No Event Sampling Job Verbose Mode

Events (28,103) Patterns Statistics (10) **Visualization**

Bar Chart Format Trellis

Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

Now let's add multiple aggerate 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√§sky)	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	1246
Beautiful Ohio	58	6	554.1379310344828	120470	58	52.41509433962264	CRIME:DRAMA	3915
Gang's All Here, The	58	9	604.1206896551724	115333	57	48.22	DOCUMENTARY	1822
Stay Cool	57	7	530.2280701754386	132645	56	44.90909090909091	COMEDY:MUSICAL:ROMANCE	3405

Analysis Technique 1 : Exercise 1

STEP 03 – Analysis

Finally, let's segement 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 Hunters (Bail Enforcers)	mobile-content-02.mytelco.com	29	4	610.6206896551724	57638	29	53.074074074074076	DOCUMENTARY
Christmas Carol, A	mobile-content-01.mytelco.com	27	6	534.5185185185185	63294	27	50.73913043478261	DRAMA
Ward 13	mobile-content-01.mytelco.com	27	4	571.2222222222222	57492	27	56.26923076923077	ANIMATION:COMEDY:SCI-FI

Technique 2
Matrix / Pivot Analysis

Analysis Technique 2 : Matrix / Pivot

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

Entity 2
`status`

Entity 1
`Uri_path`

uri_path	200	400	404
/category.screen	7588	672	730
/high_def_contents.screen	2597	227	241
/low_def_contents.screen	2546	226	230
/mobile_contents.do	2509	231	232
/mobile_contents.do.do	2617	238	238
/mobile_download.do	2589	262	254
/oldlink	2575	244	222
/product.screen	2594	224	236

`count(clientip)`

Function

```
chart count(clientip) by uri_path status
```

2 Different eneity segmentation, using X, Y axis

splunk>

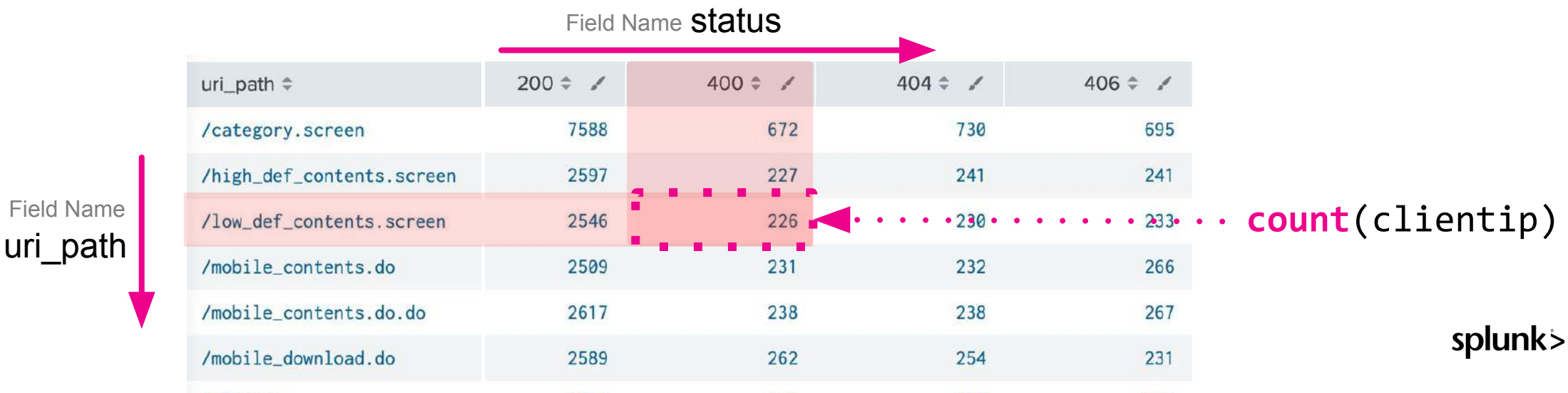
Analysis Technique 2 : Matrix / Pivot

Syntax :

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

Examples :

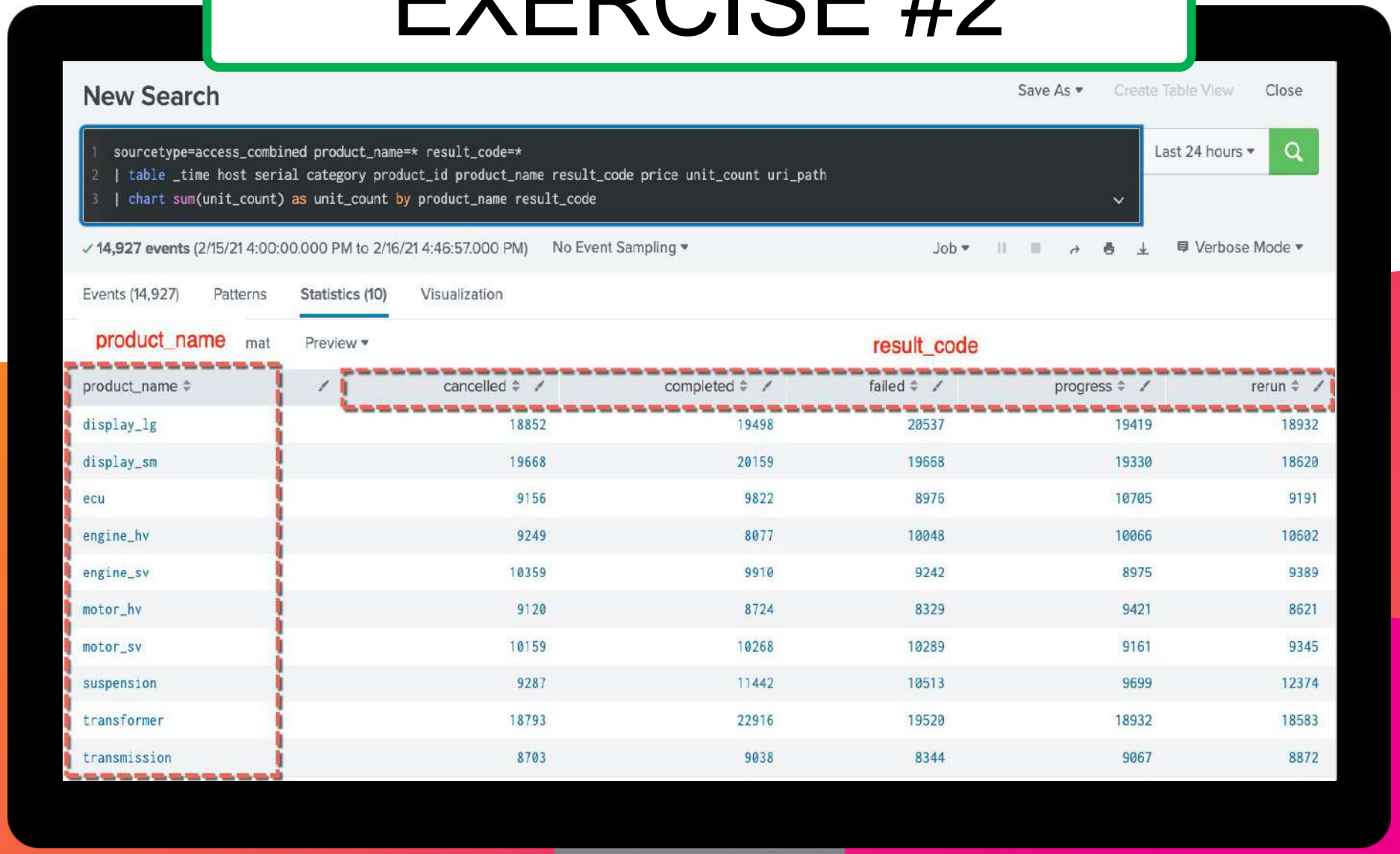
```
* | chart count(clientip) by uri_path, status
```



uri_path	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

splunk>

EXERCISE #2



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

Events (39,976) Patterns **Statistics (8)** Visualization

100 Per Page ▾ Format Preview ▾

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

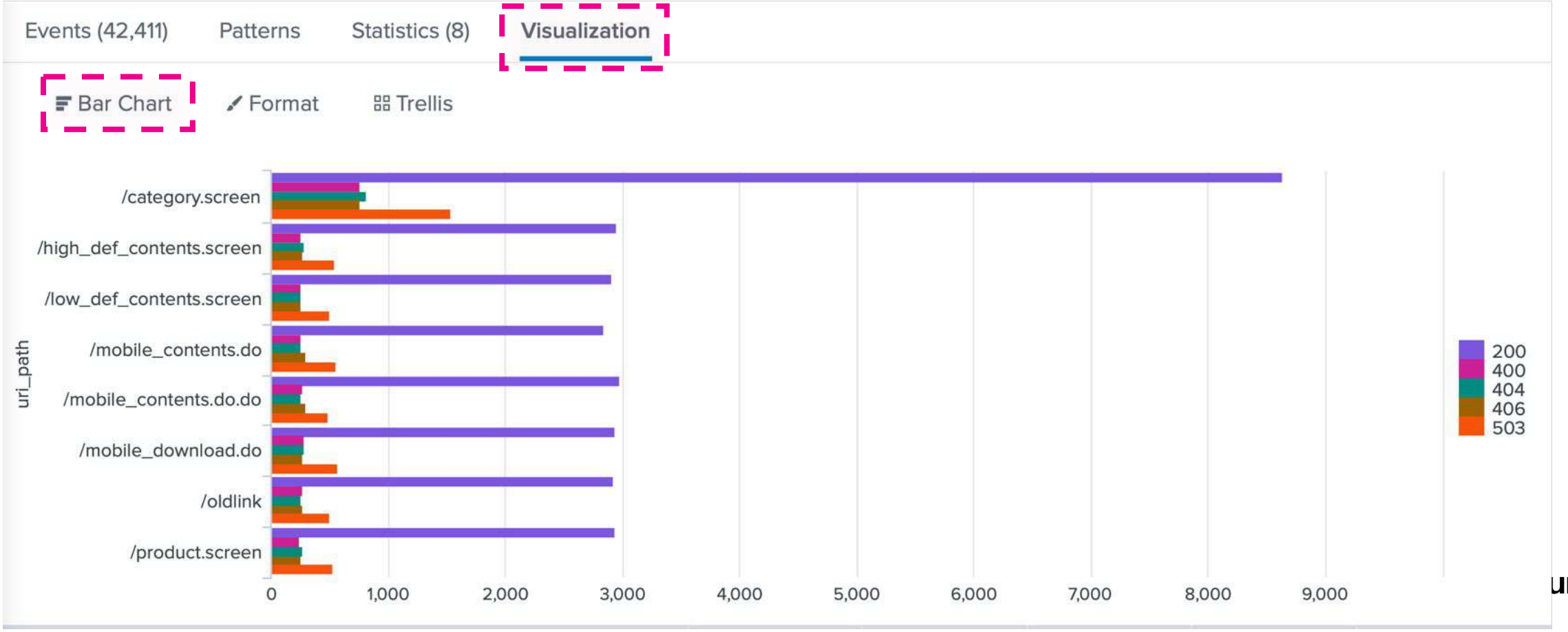
splunk>

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

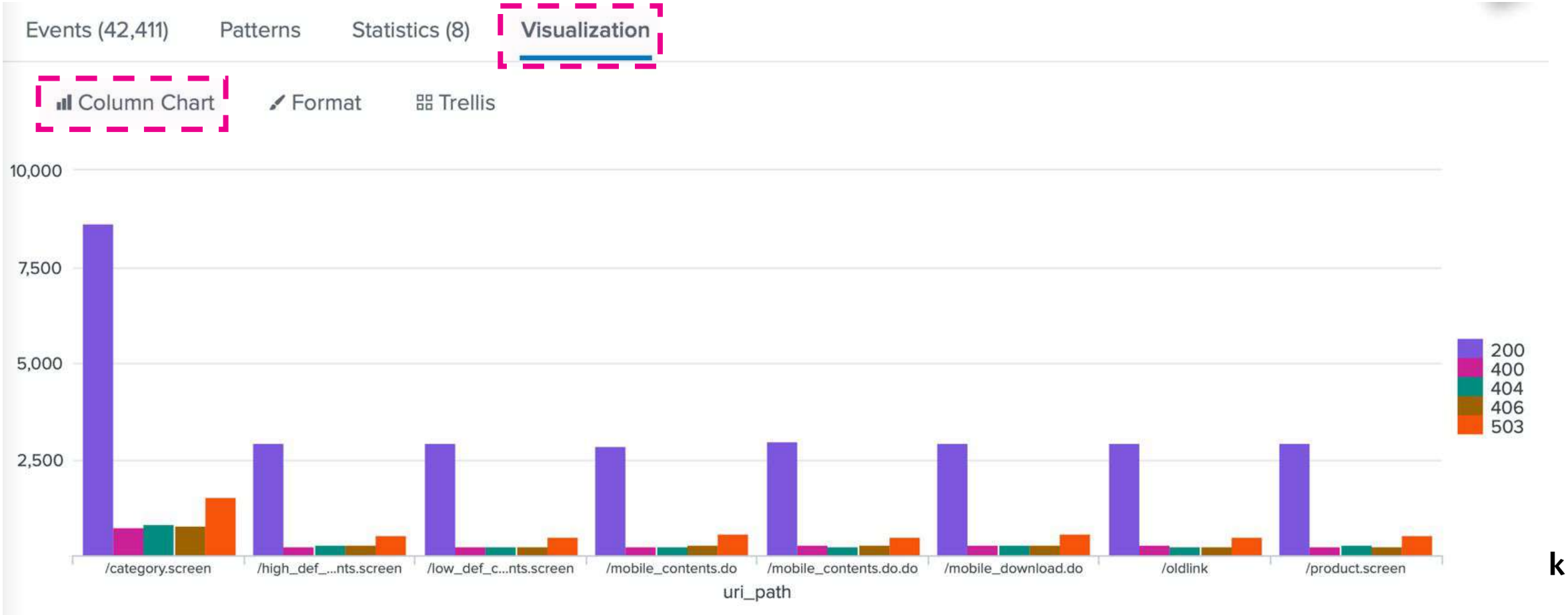


Analysis Technique 2 : Exercise 2

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



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
```

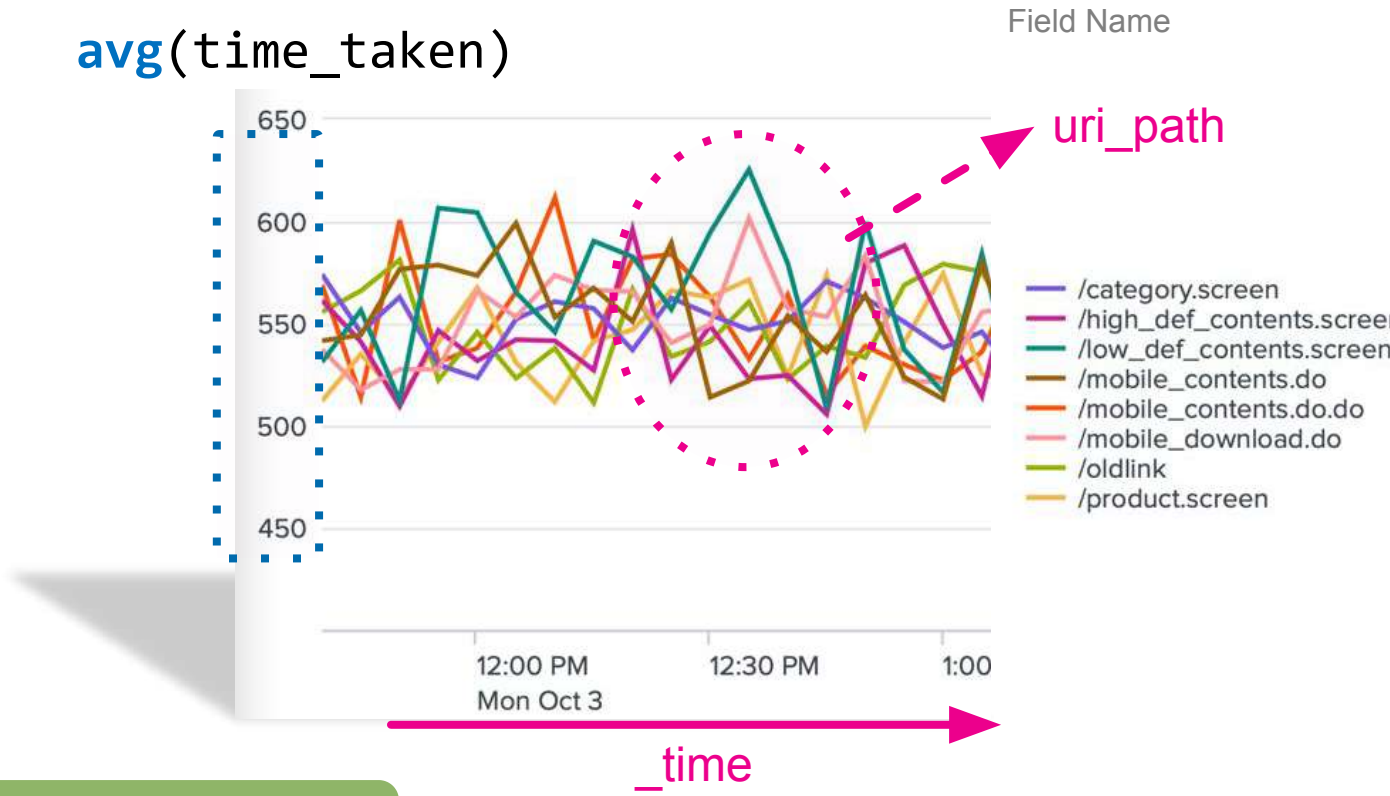
Last 24 hours

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

splunk>

Analysis Technique 3 : 3D Matrix, Trend

Syntax :

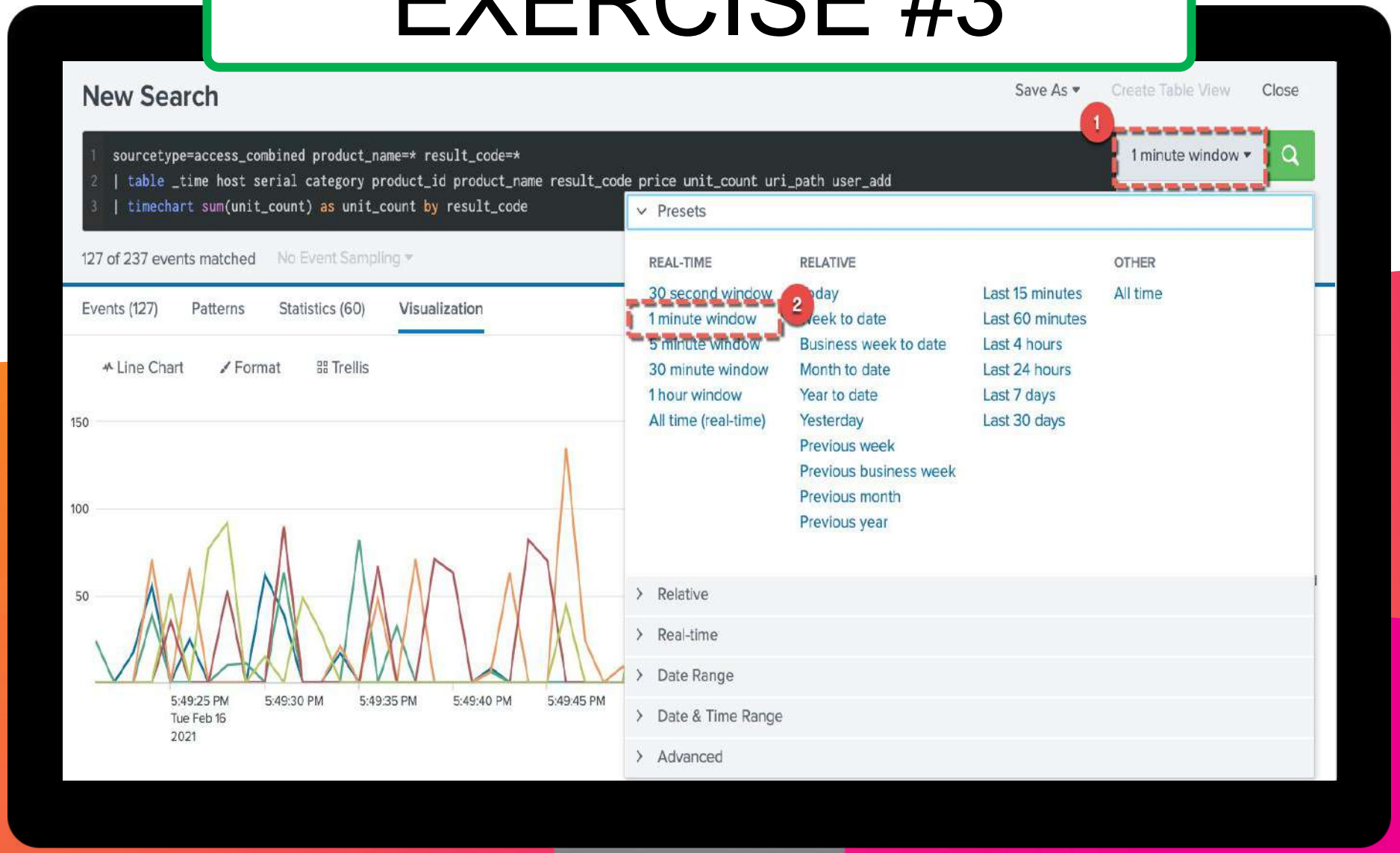
```
timechart func(field), func(field), .. by field
```

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
```

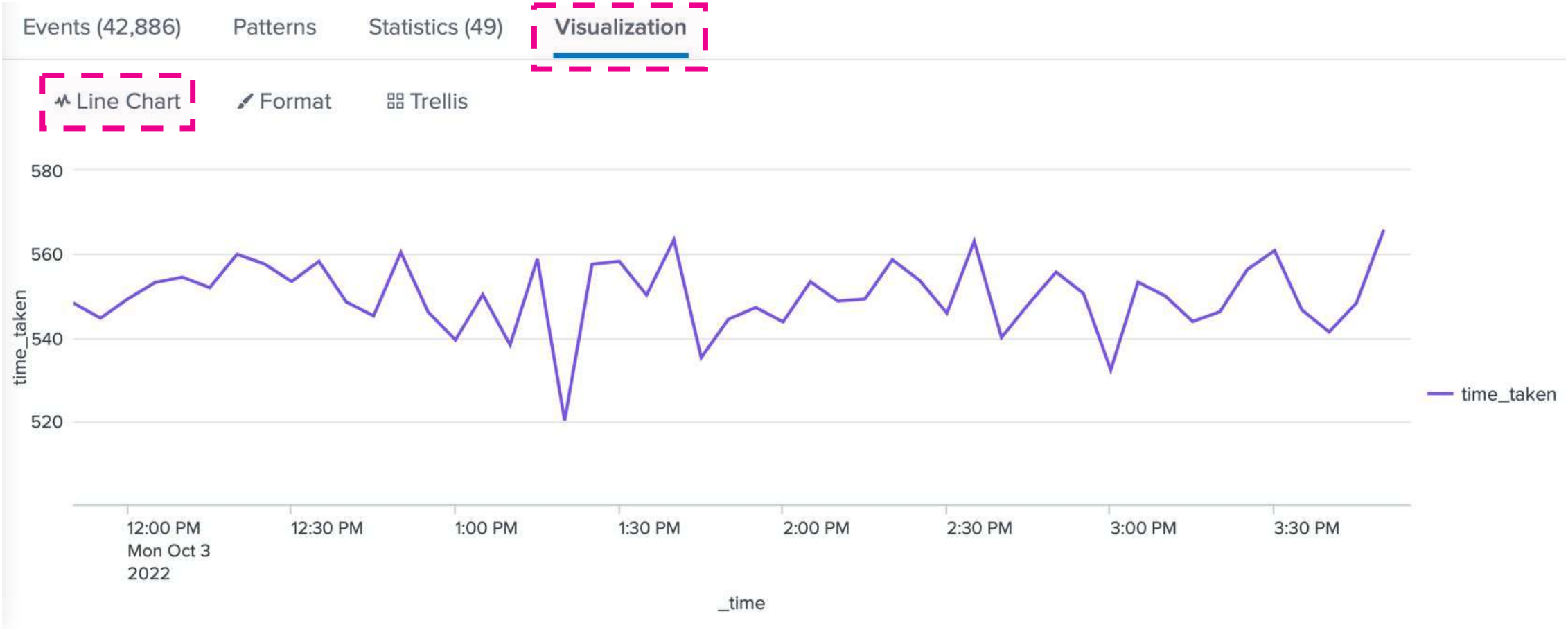
EXERCISE #3



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

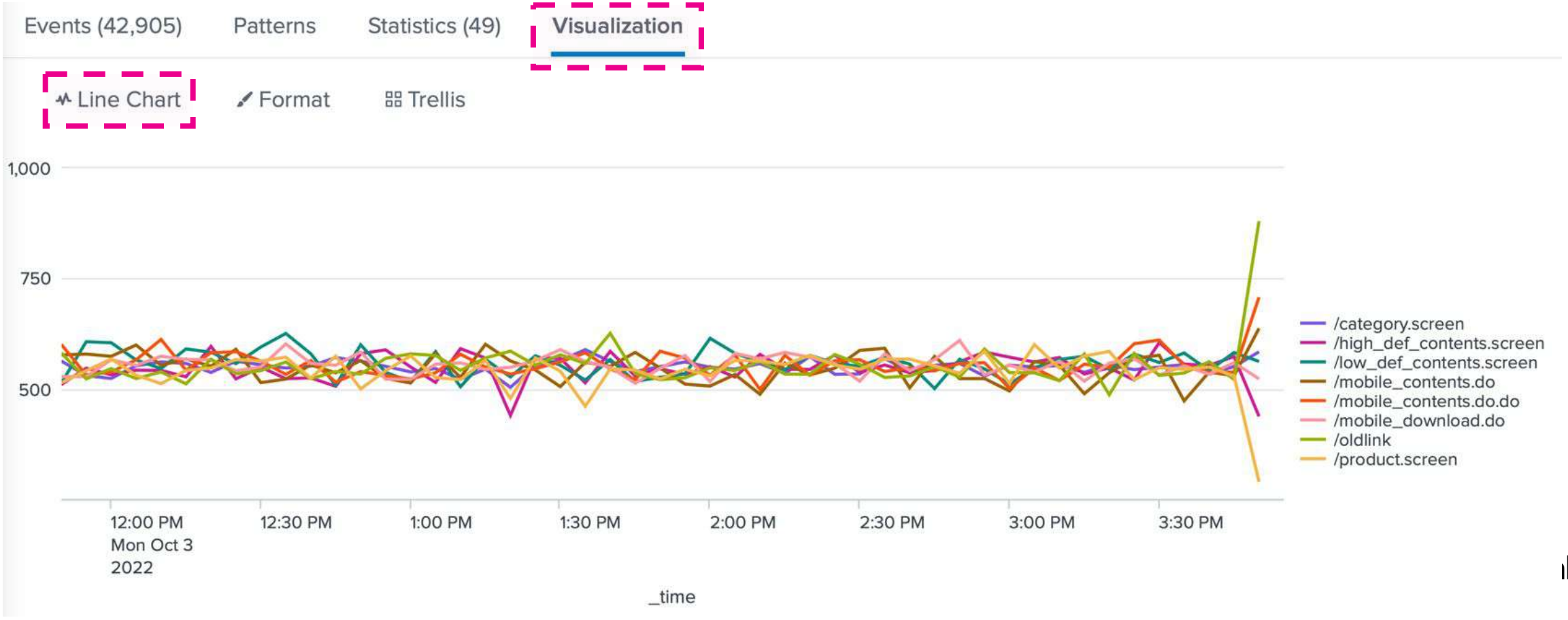
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart avg(time_taken) as time_taken
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

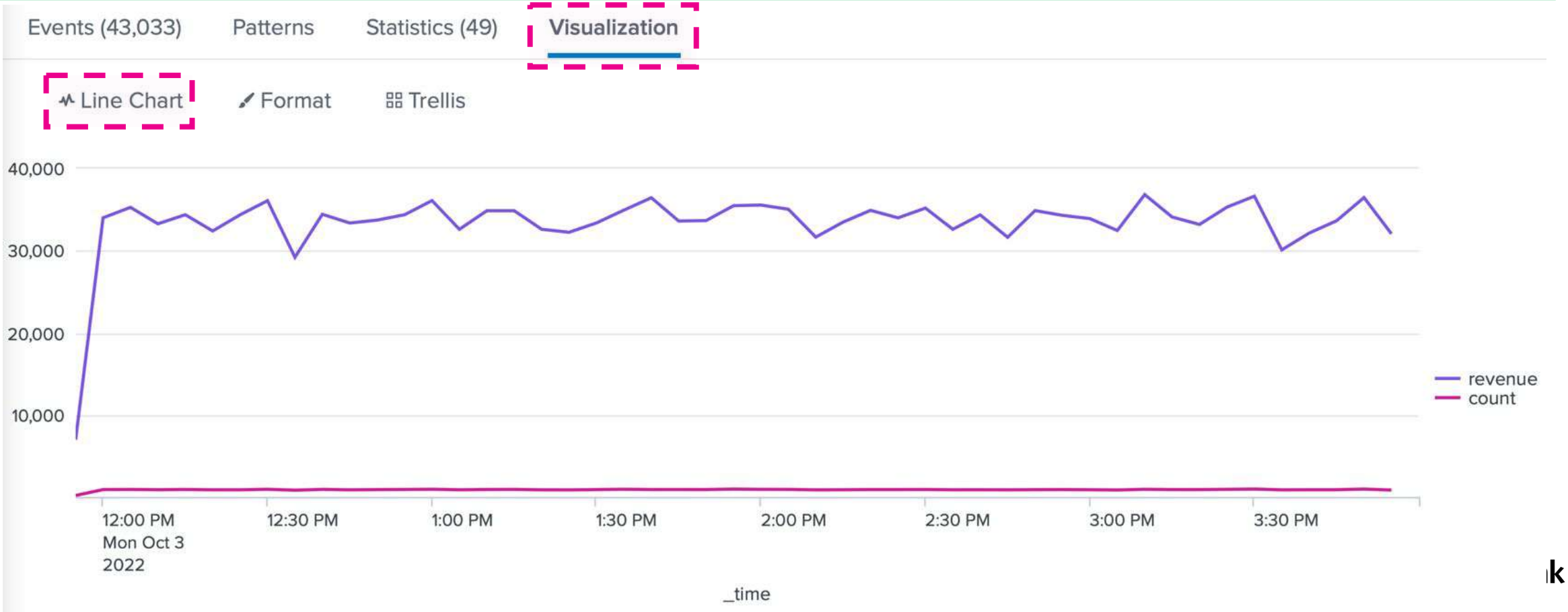
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart avg(time_taken) as time_taken by uri_path
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

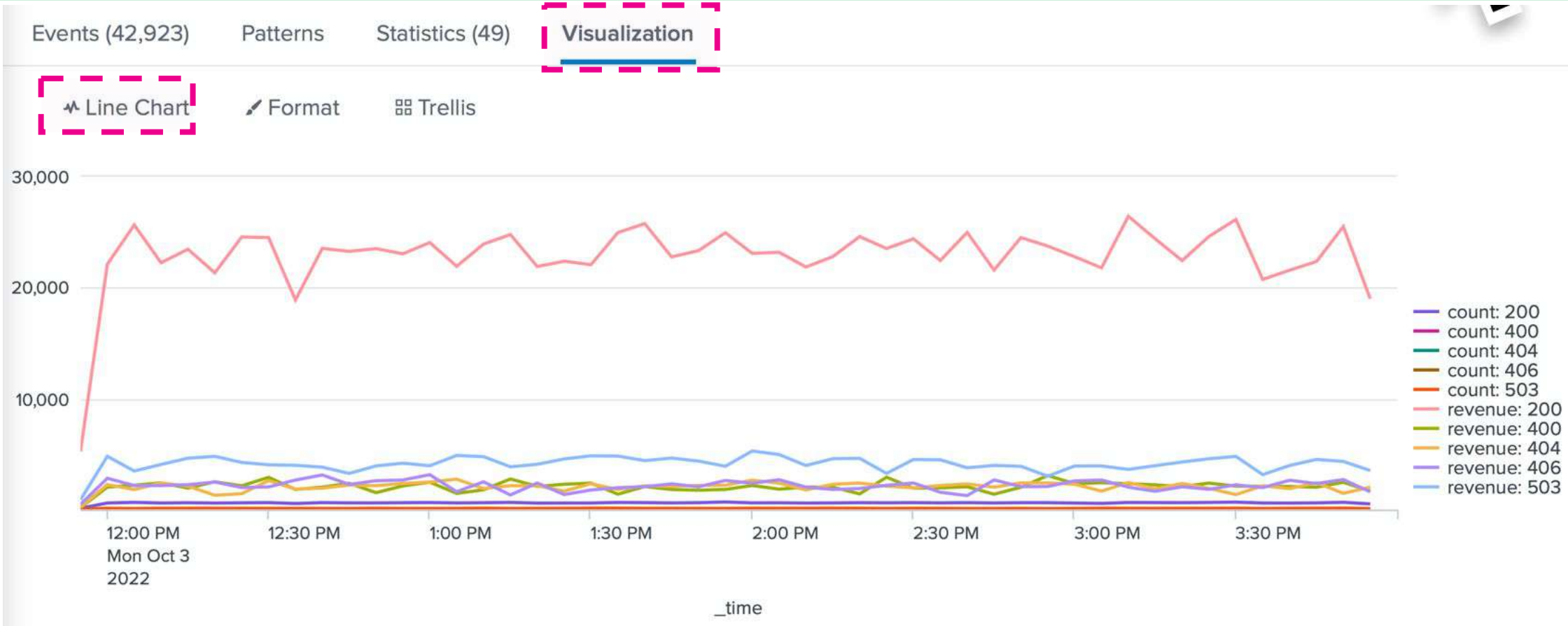
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart sum(price) as revenue, count
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

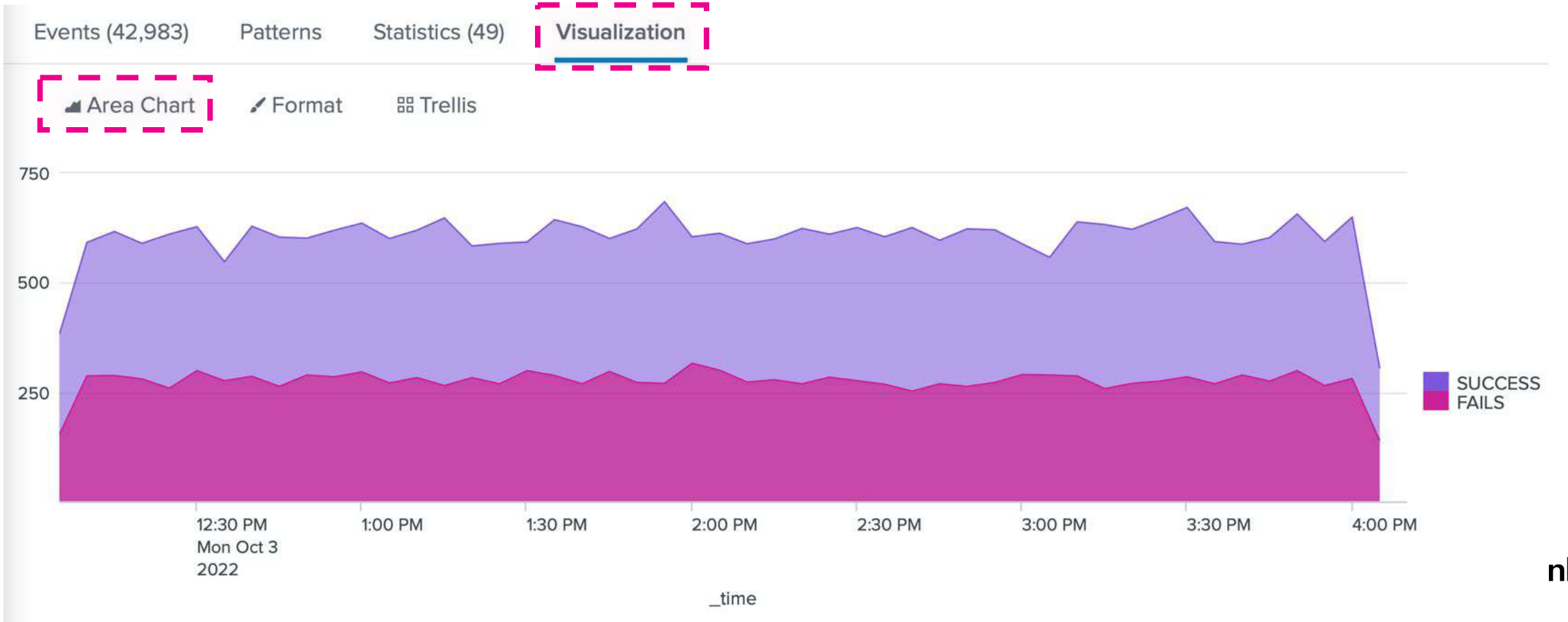
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart sum(price) as revenue, count by status
```



Analysis Technique 3 : Exercise 3

STEP 01 – Analysis

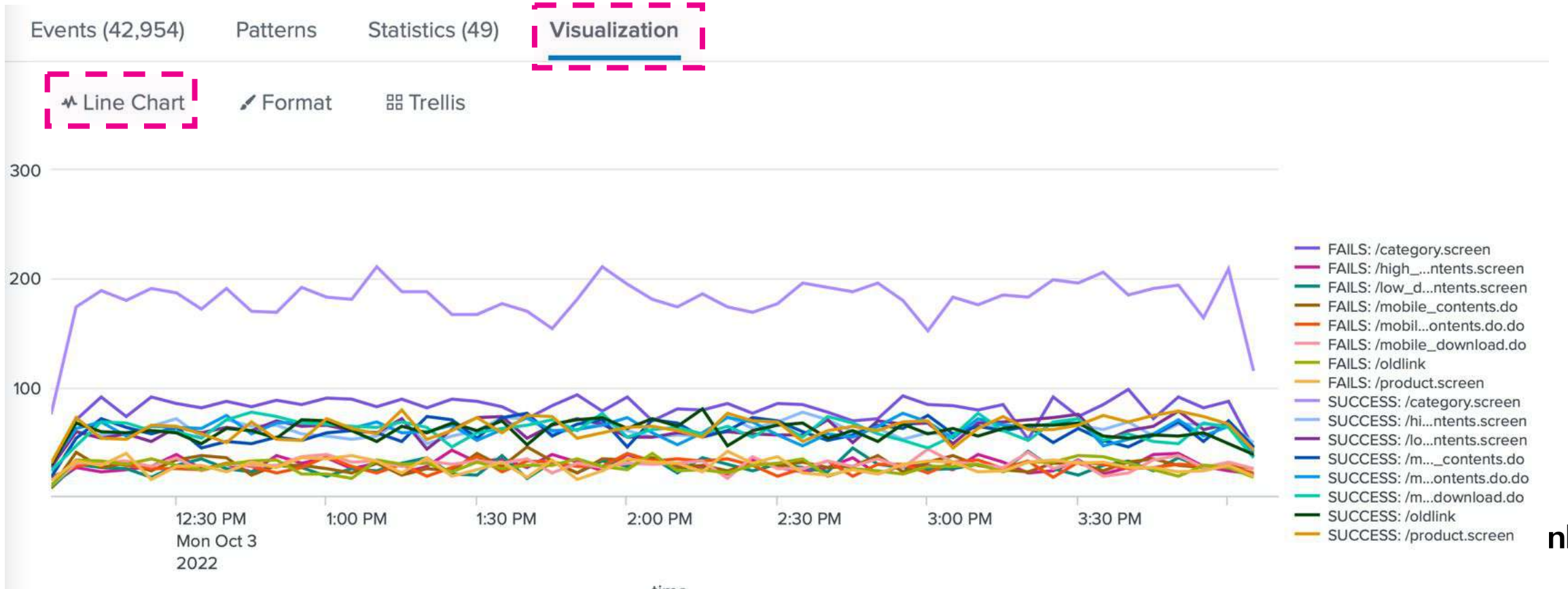
```
sourcetype=mobile_content
| table _time host clientip JSESSIONID category_id method uri_path product_id
product_name status action price bytes time_taken uri_path user_type user_add user_age
useragent
| timechart count(eval(status<300)) as SUCCESS, count(eval(status>=400)) as FAILS
```



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
```

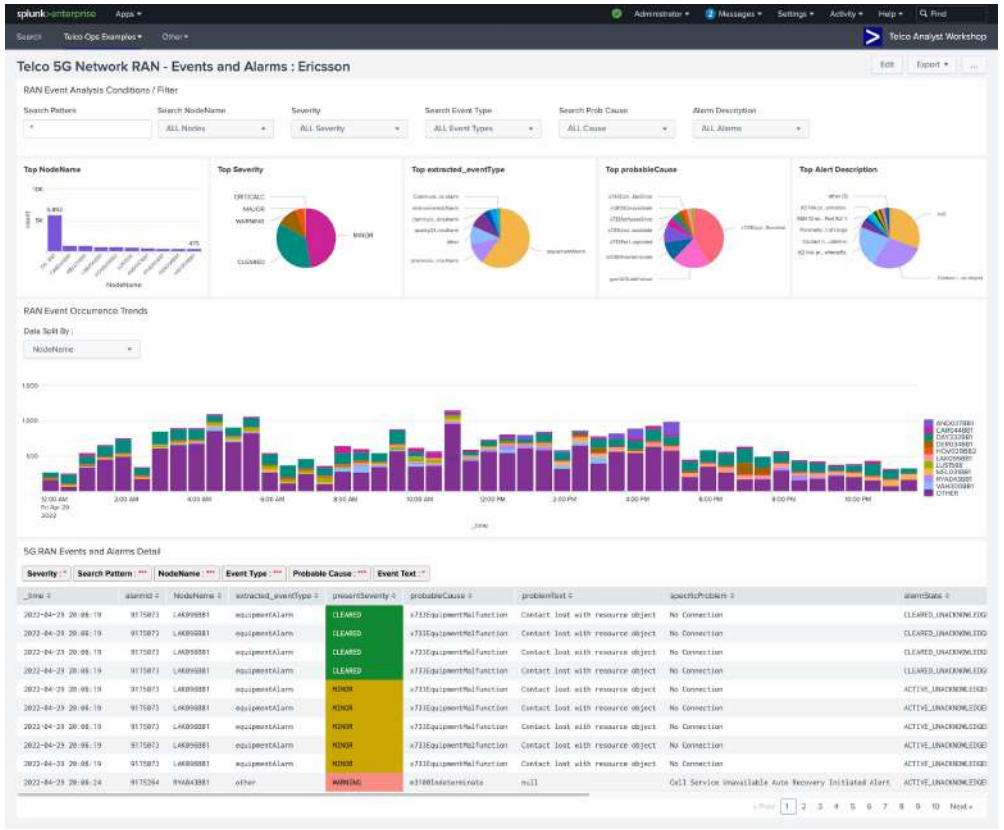


Telco Operational Dashboard

Cre 2 Operational Dashboard

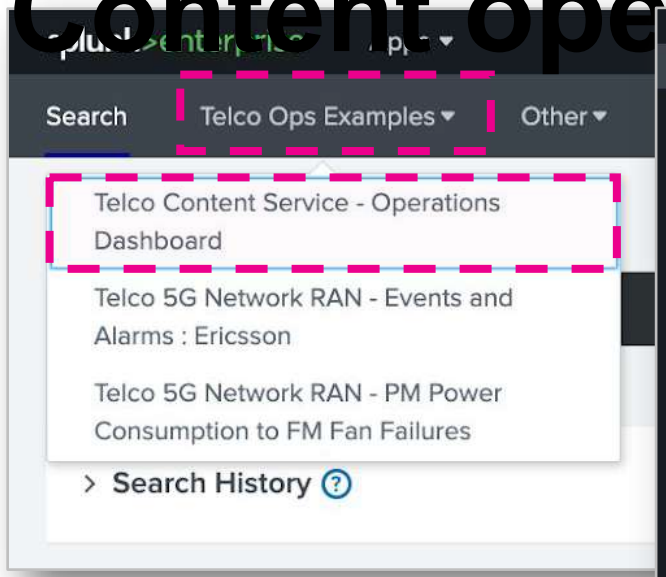
Content operational dashboard

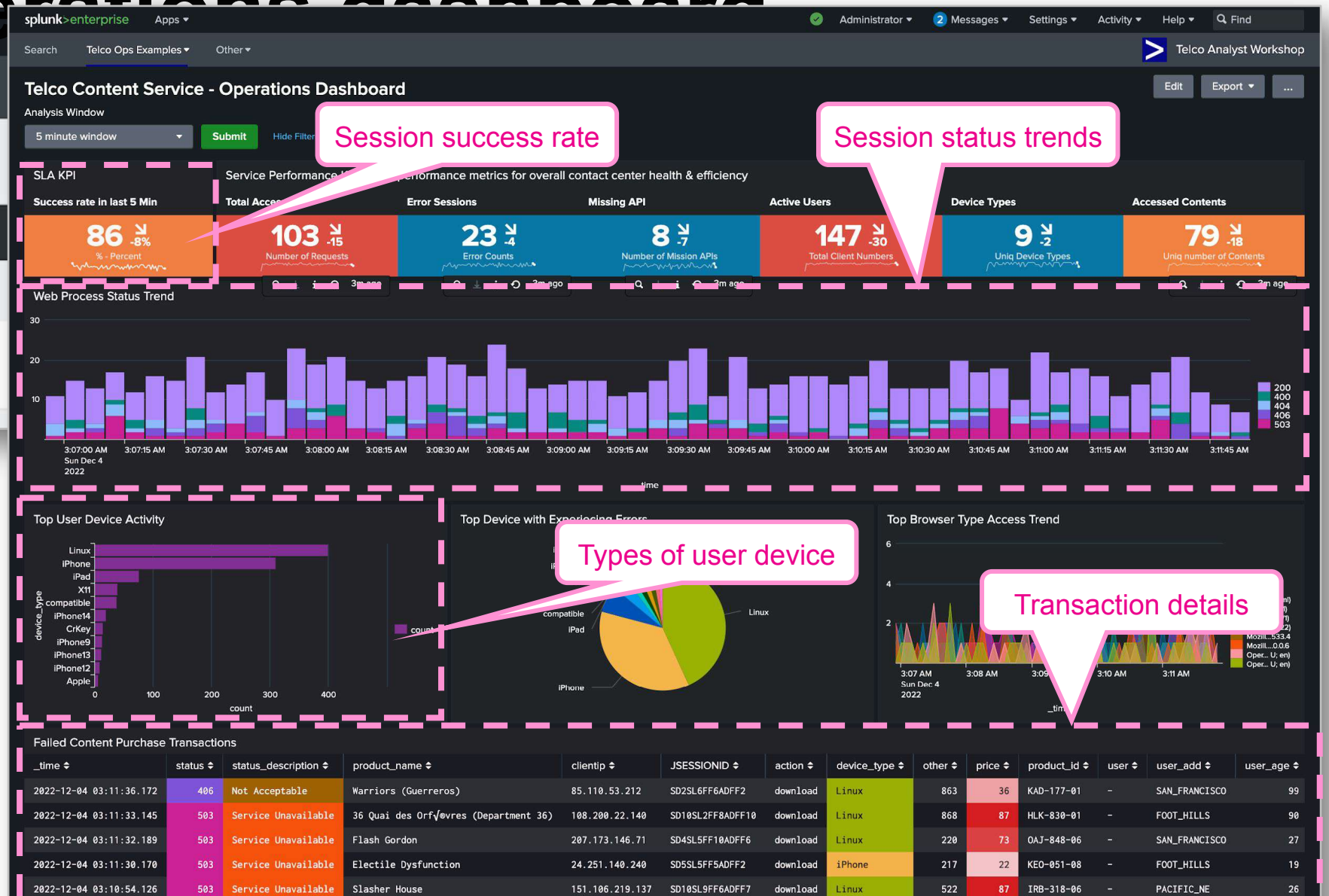
5G RAN alarm analysis



Create Content Ops Dashboards

Content operations dashboard





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:

splunk>

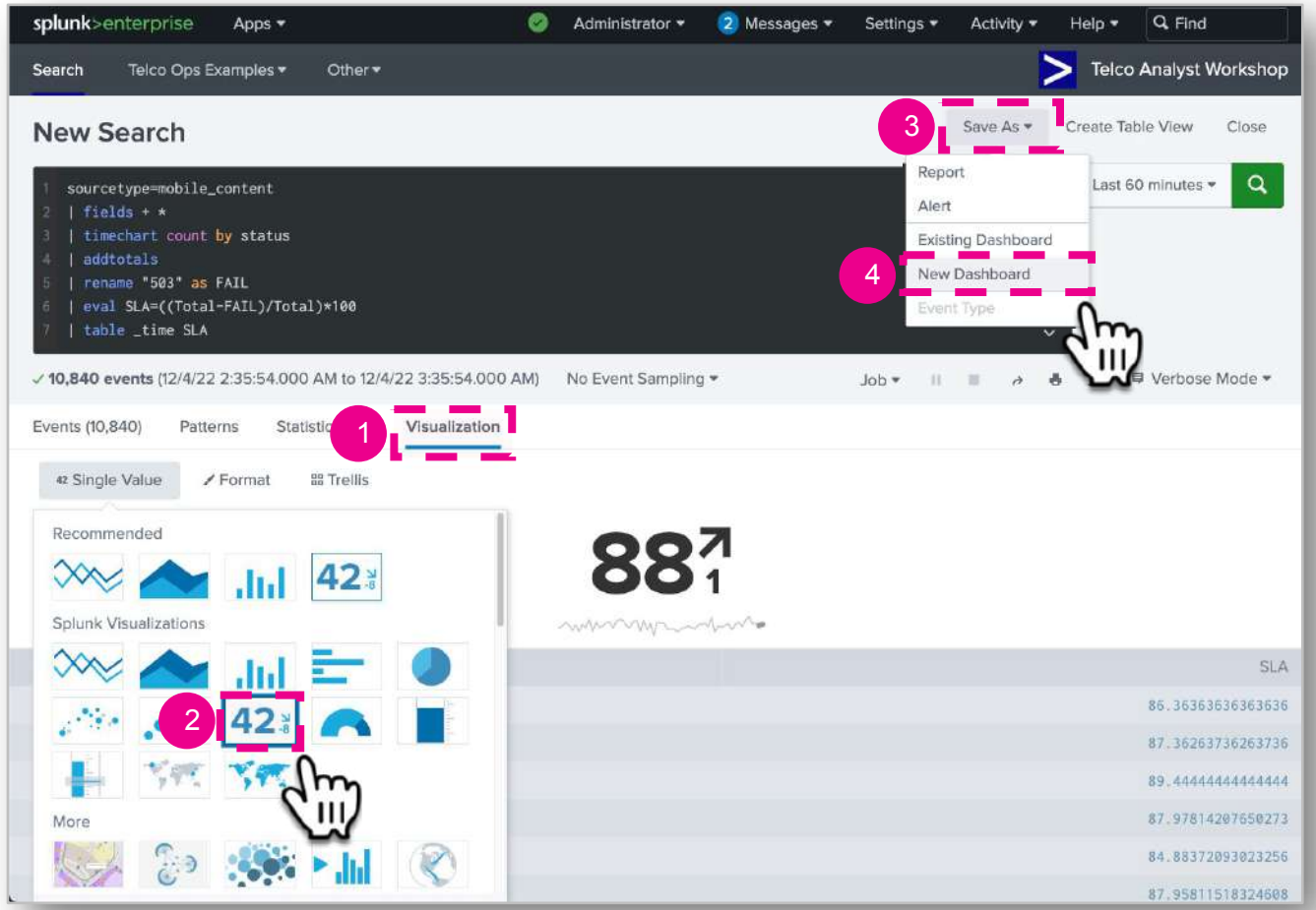
Dashboard 1 : Content operations dashboard

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

Solution:

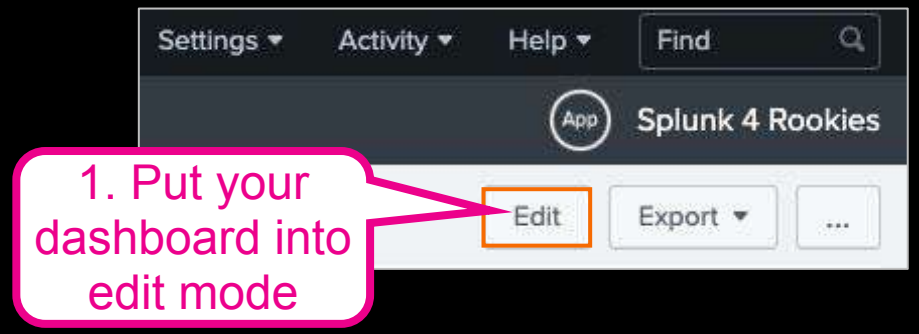
```
sourcetype=mobile_content
| timechart count by status
| addtotals
| rename "503" as FAIL
| eval SLA=((Total-FAIL)/Total)*100
| table _time SLA
```

_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	87.95811518324608
2022-12-04 02:41:00	84.30232558139535
2022-12-04 02:42:00	88.27160493827161

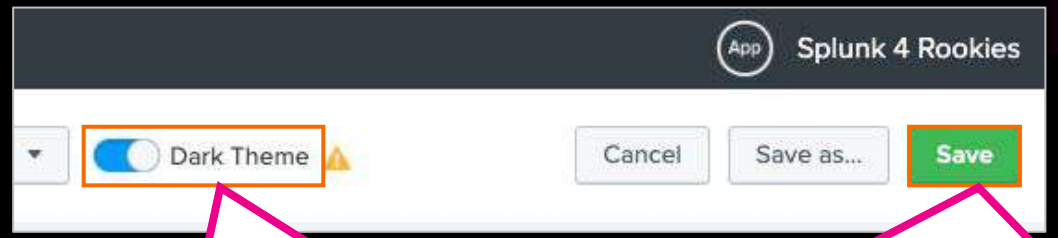


splunk>

Try Dark Mode!



1. Put your dashboard into edit mode



2. Toggle '**Dark Theme**' on

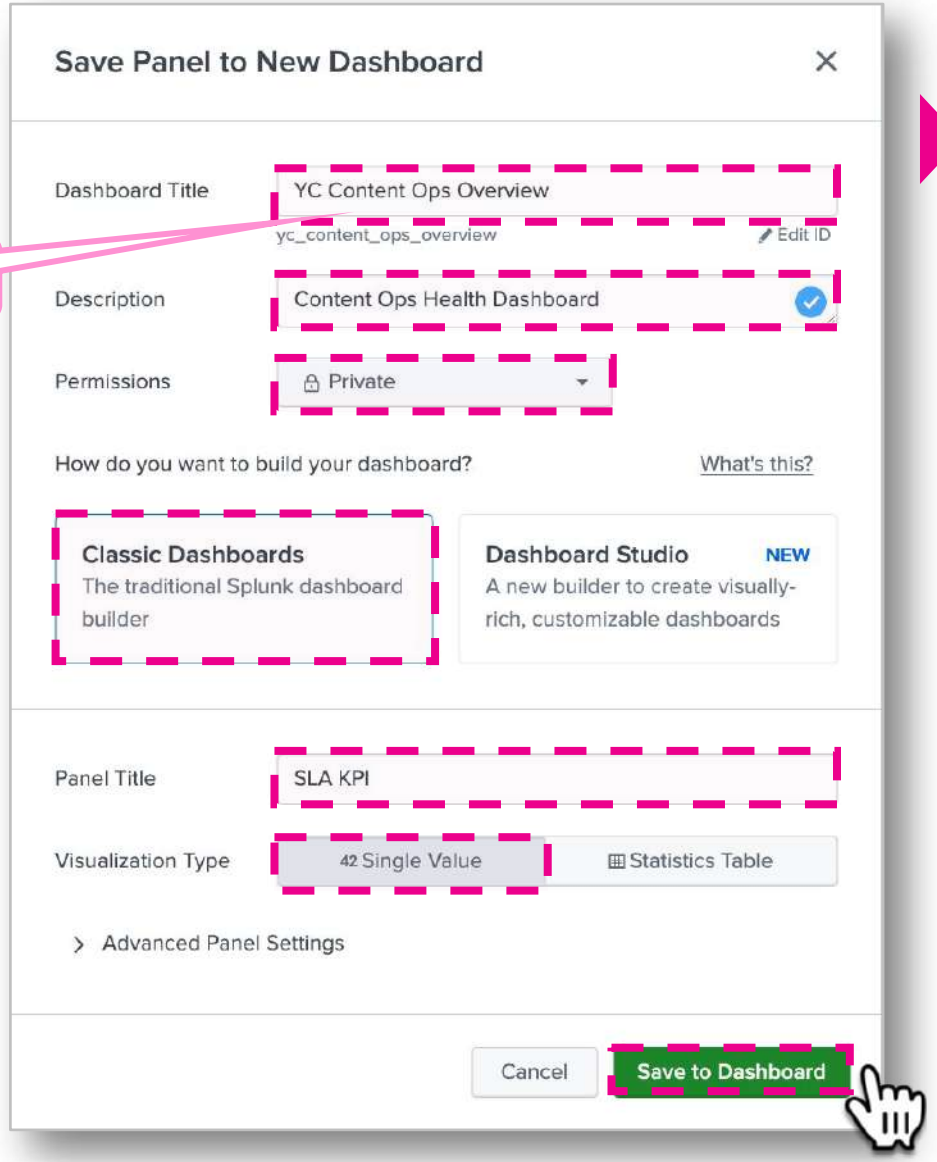
3. Save your dashboard and refresh the page to view your new dark dashboard!

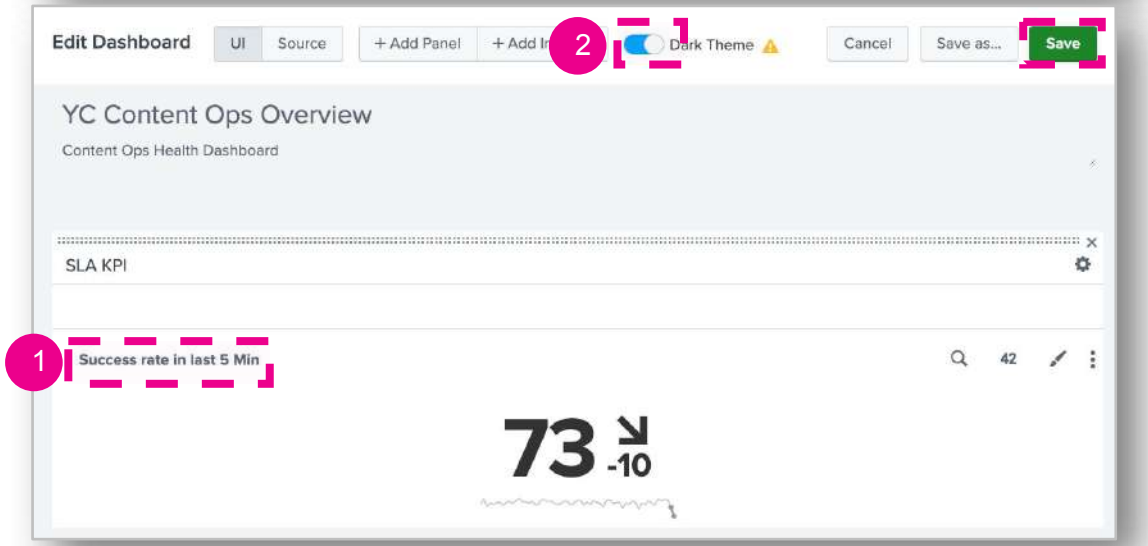
Dashboard 1 : Content operations dashboard

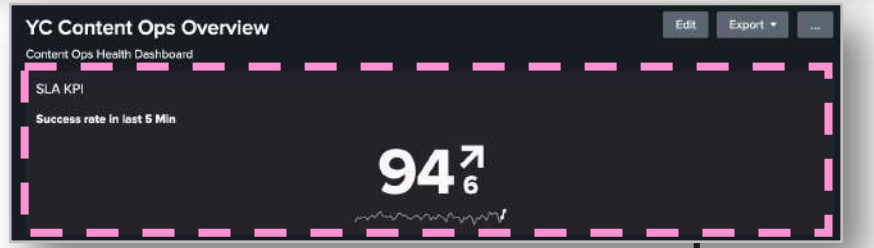
Show service success rate trends over time, based on web status code.

Solution:

Use your initial in the front of the view name







Dashboard 1 : Content operations dashboard

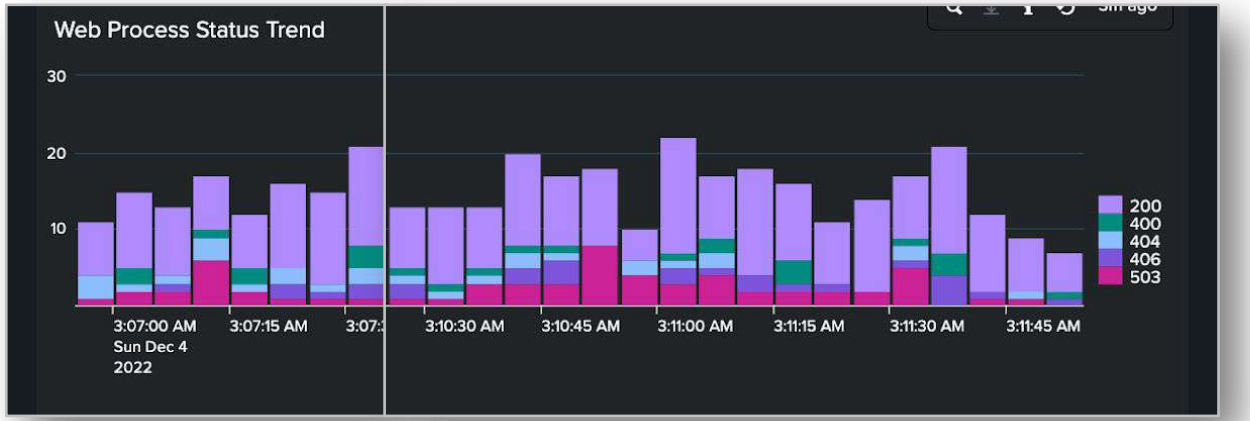
Show trends of access requests by status code

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:

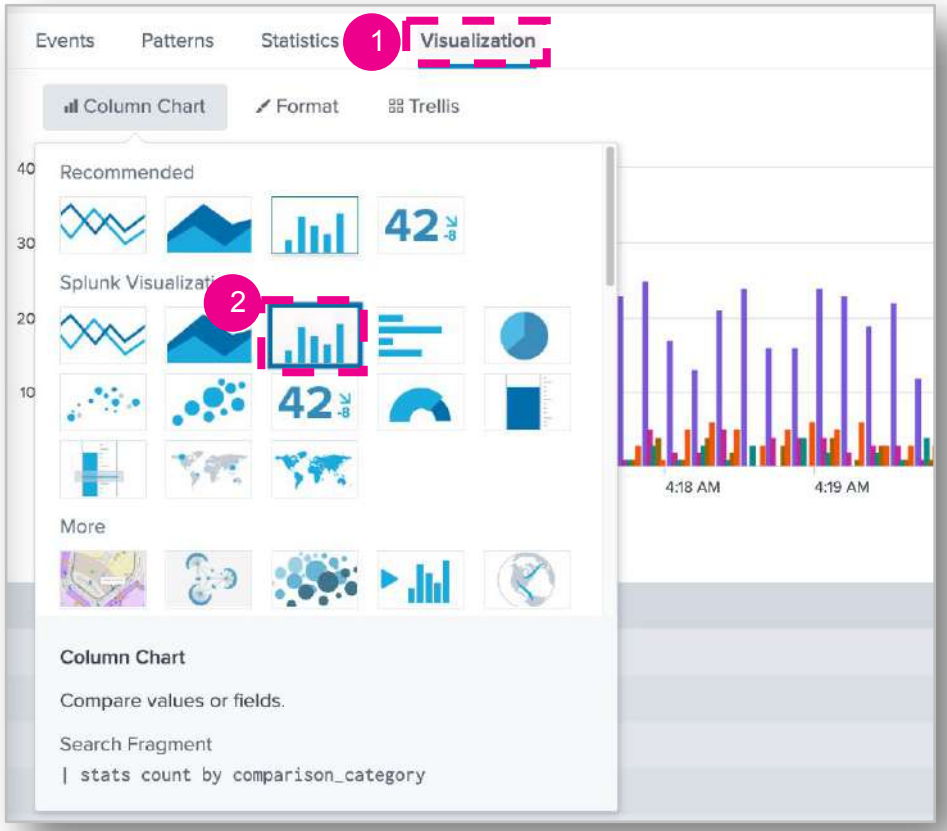


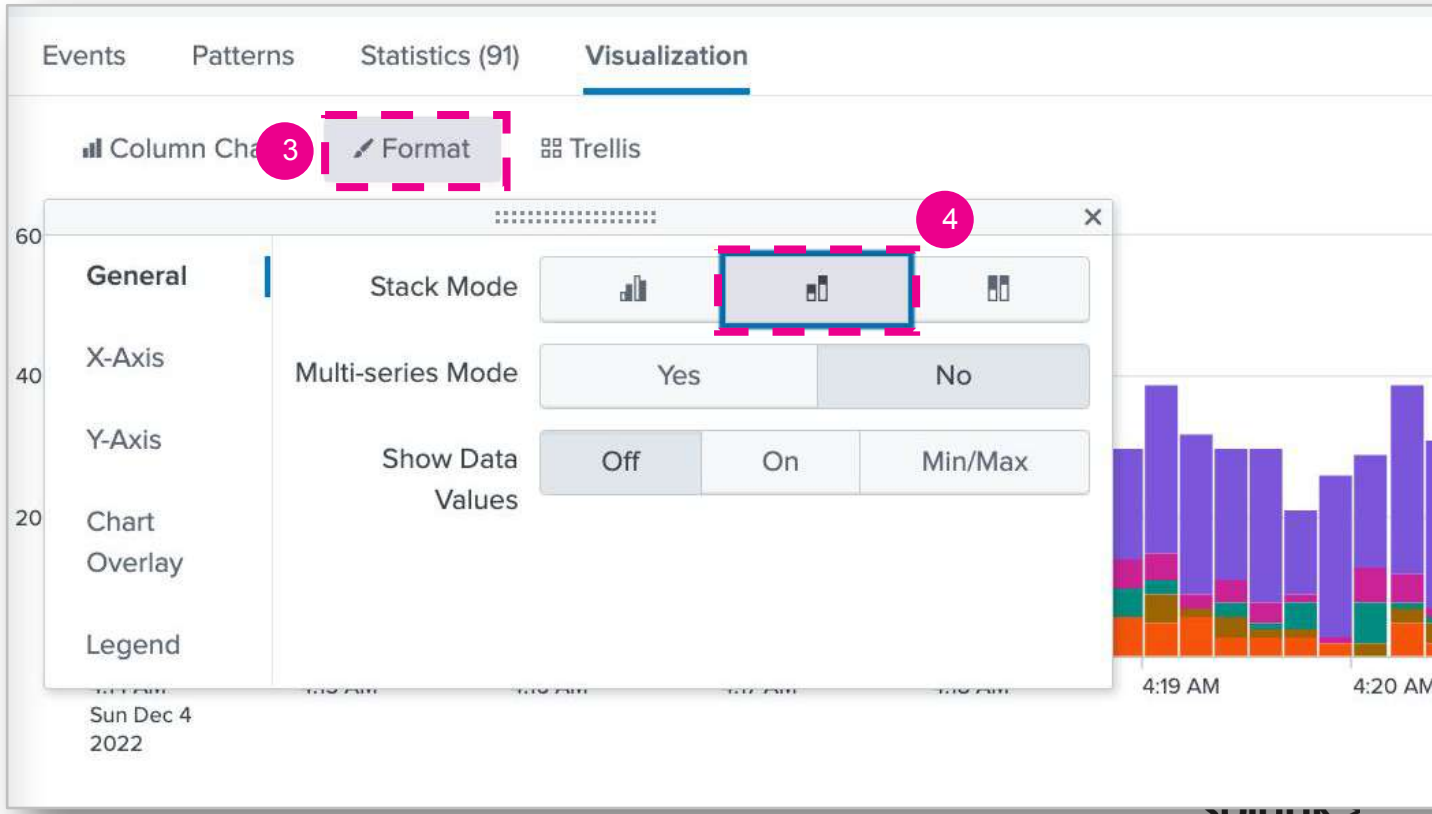
Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:

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

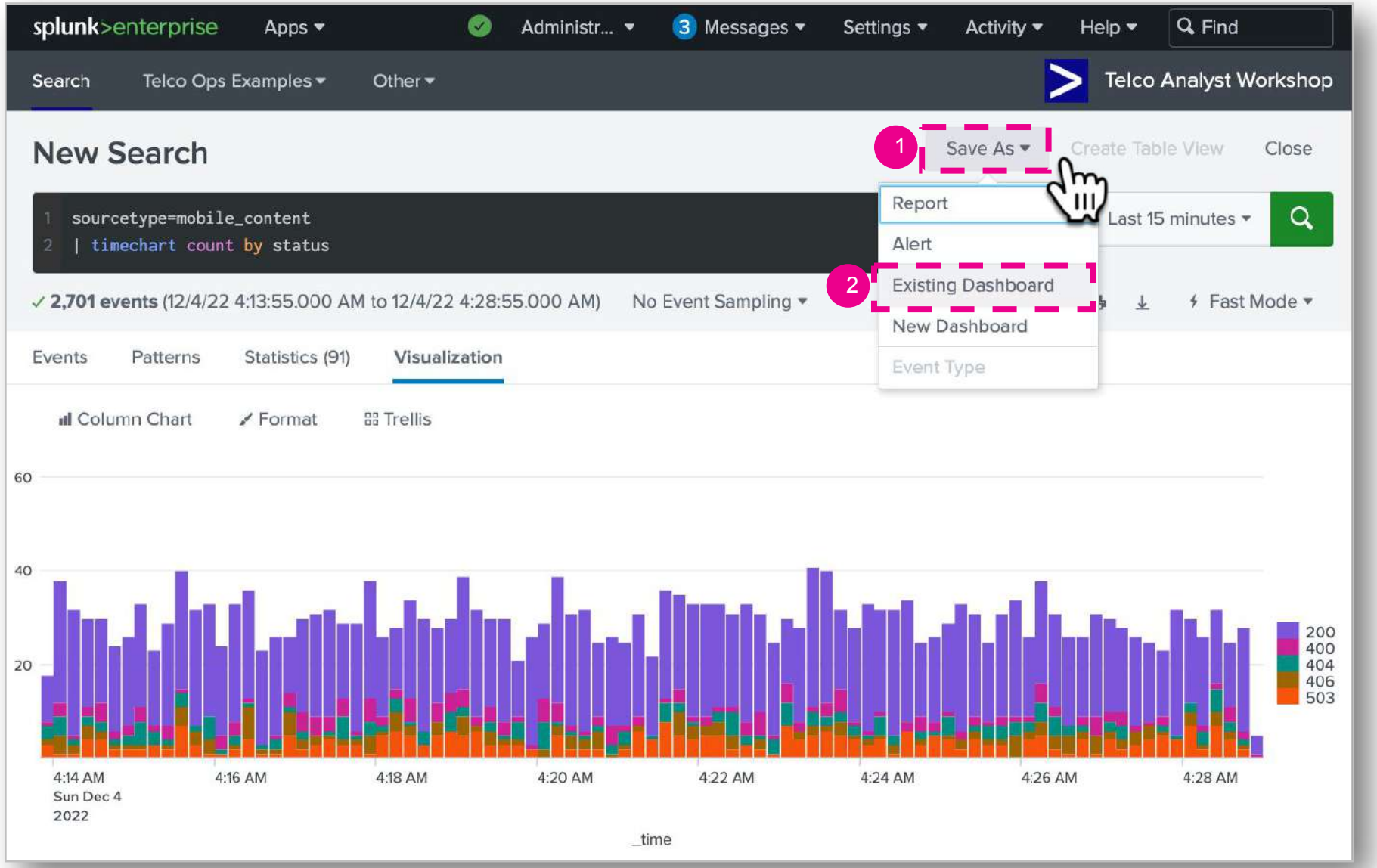




Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:

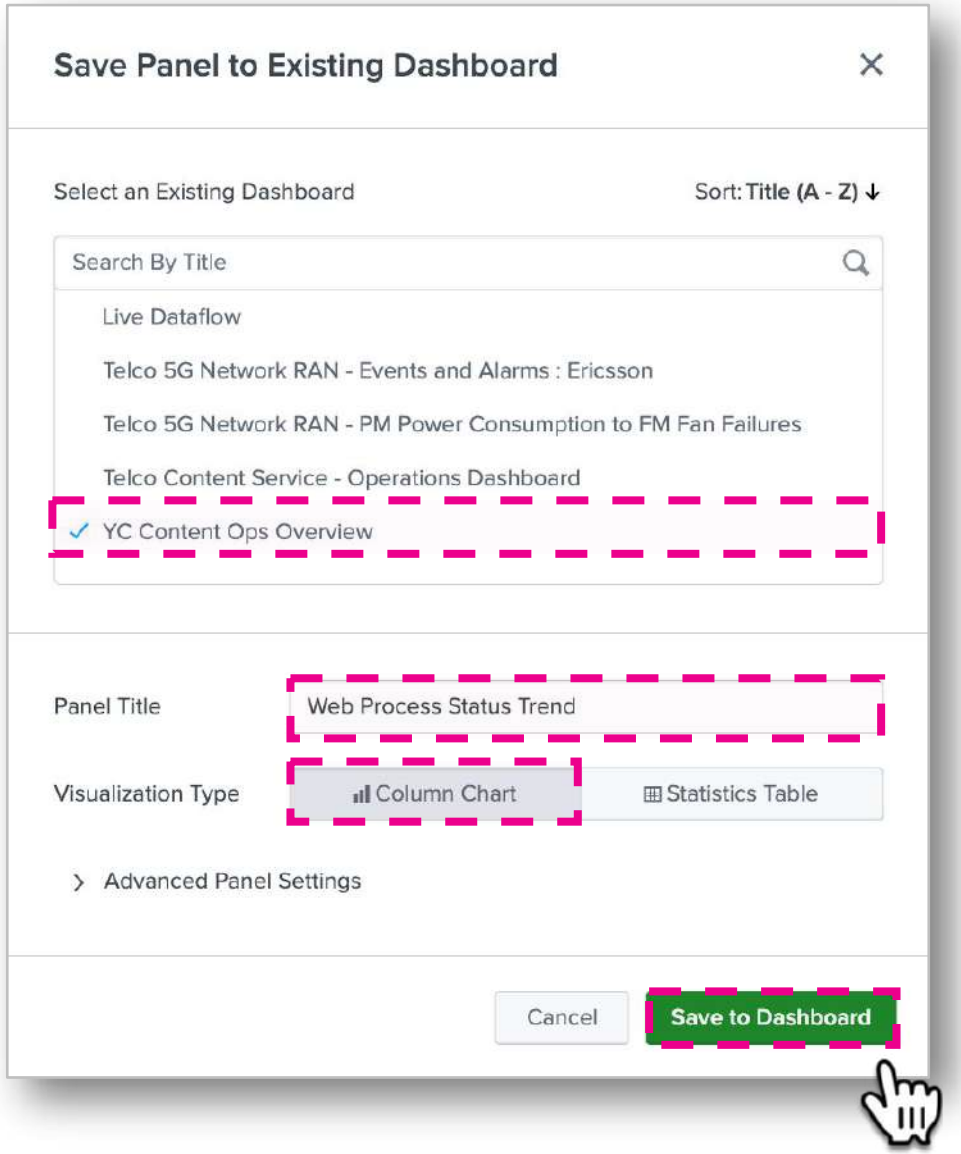


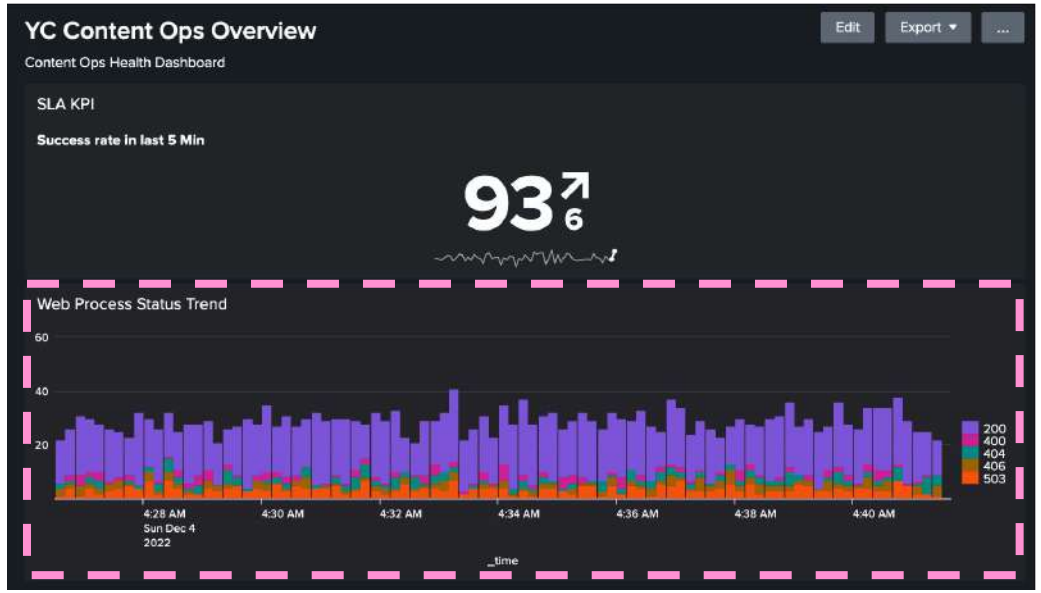
splunk>

Dashboard 1 : Content operations dashboard

Show trends of access requests by status code

Solution:





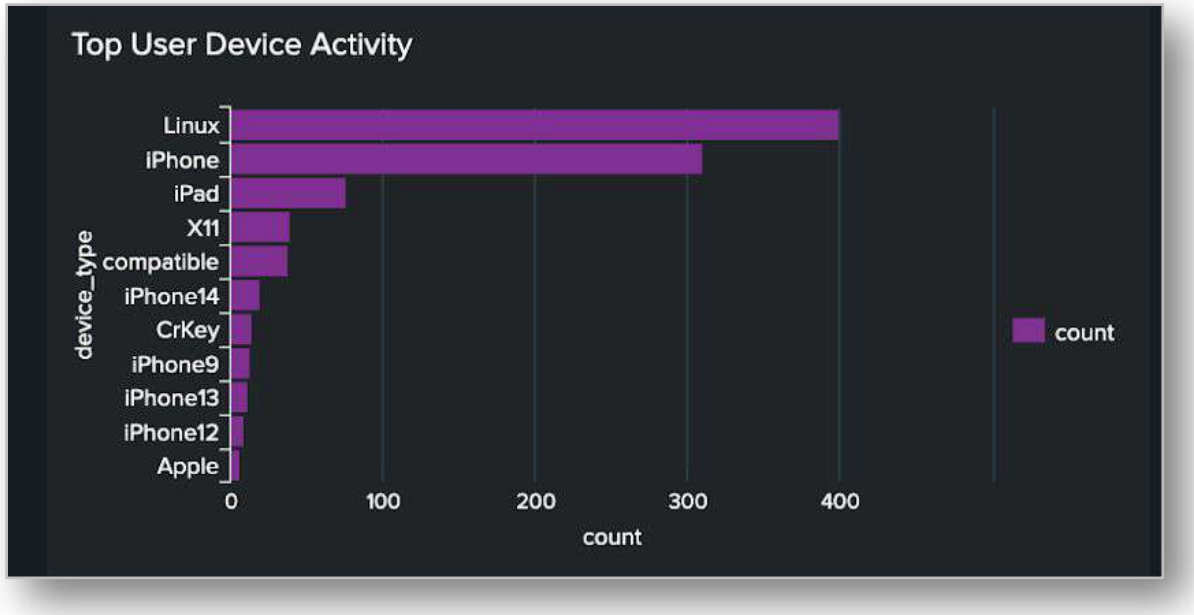
Dashboard 1 : Content operations dashboard

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:



splunk>

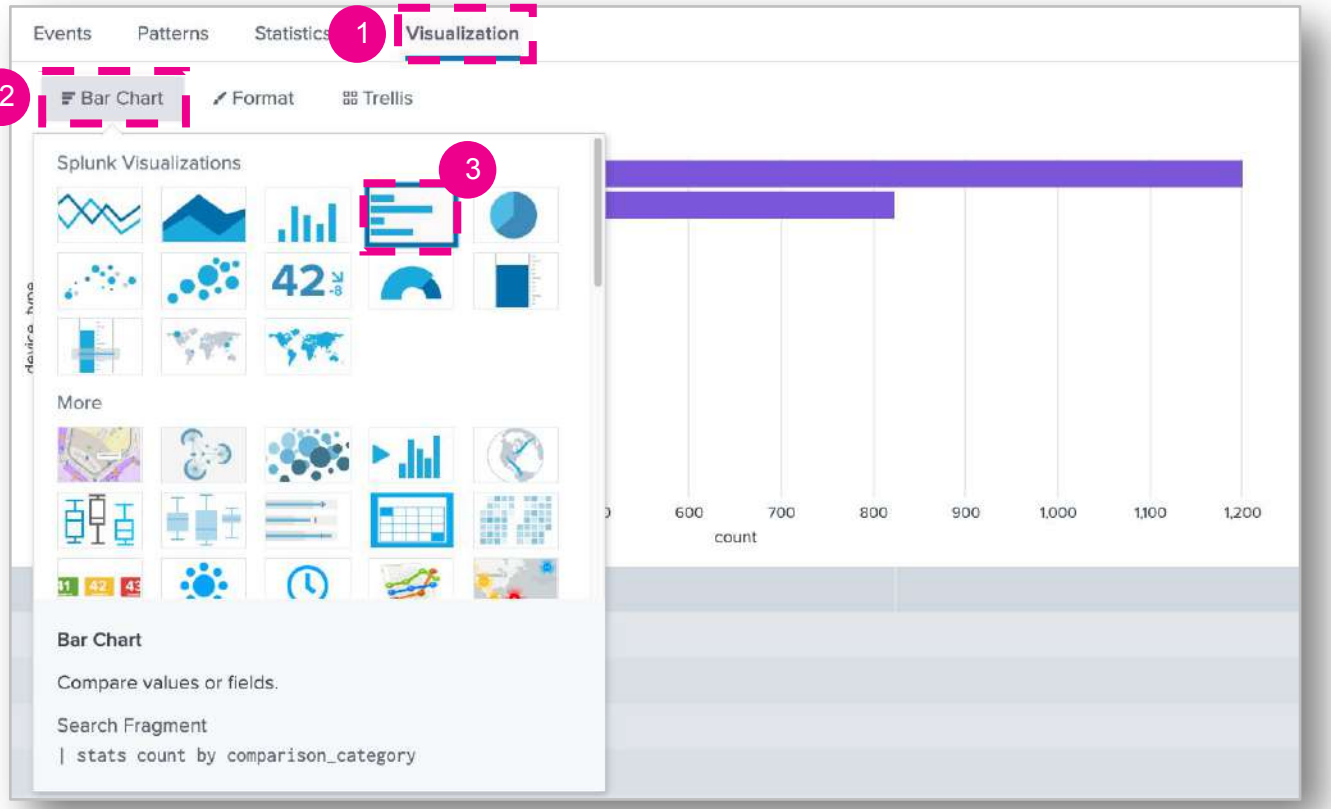
Dashboard 1 : Content operations dashboard

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

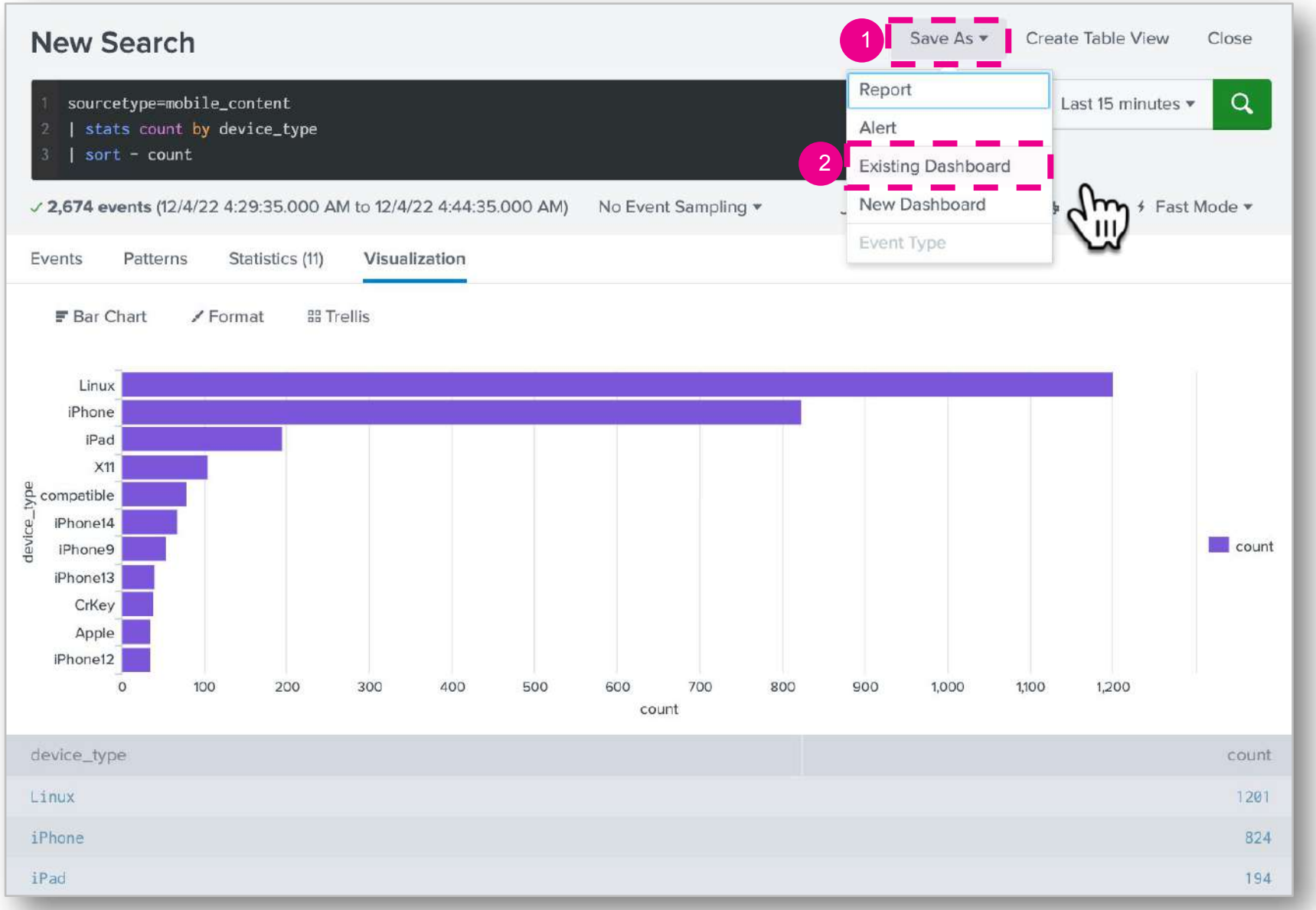


splunk>

Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

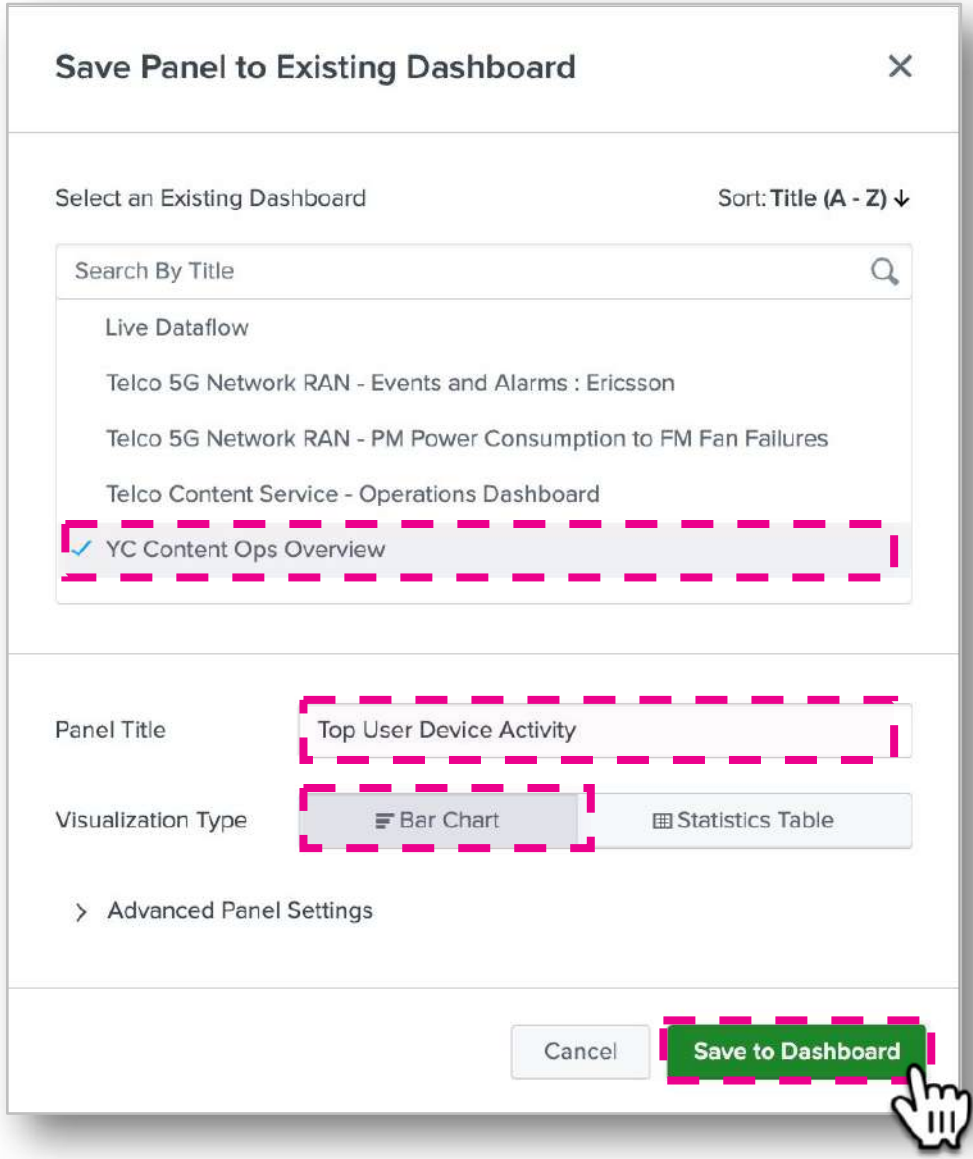


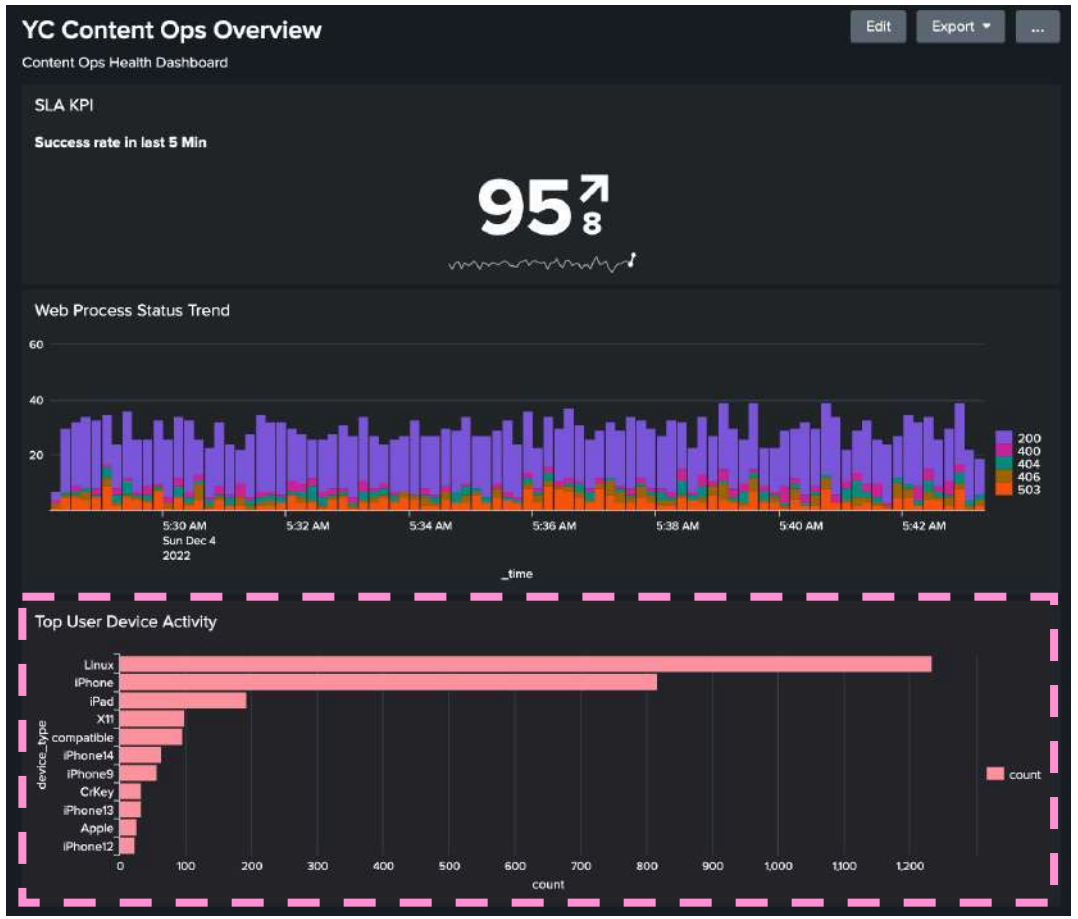
splunk>

Dashboard 1 : Content operations dashboard

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

Solution:





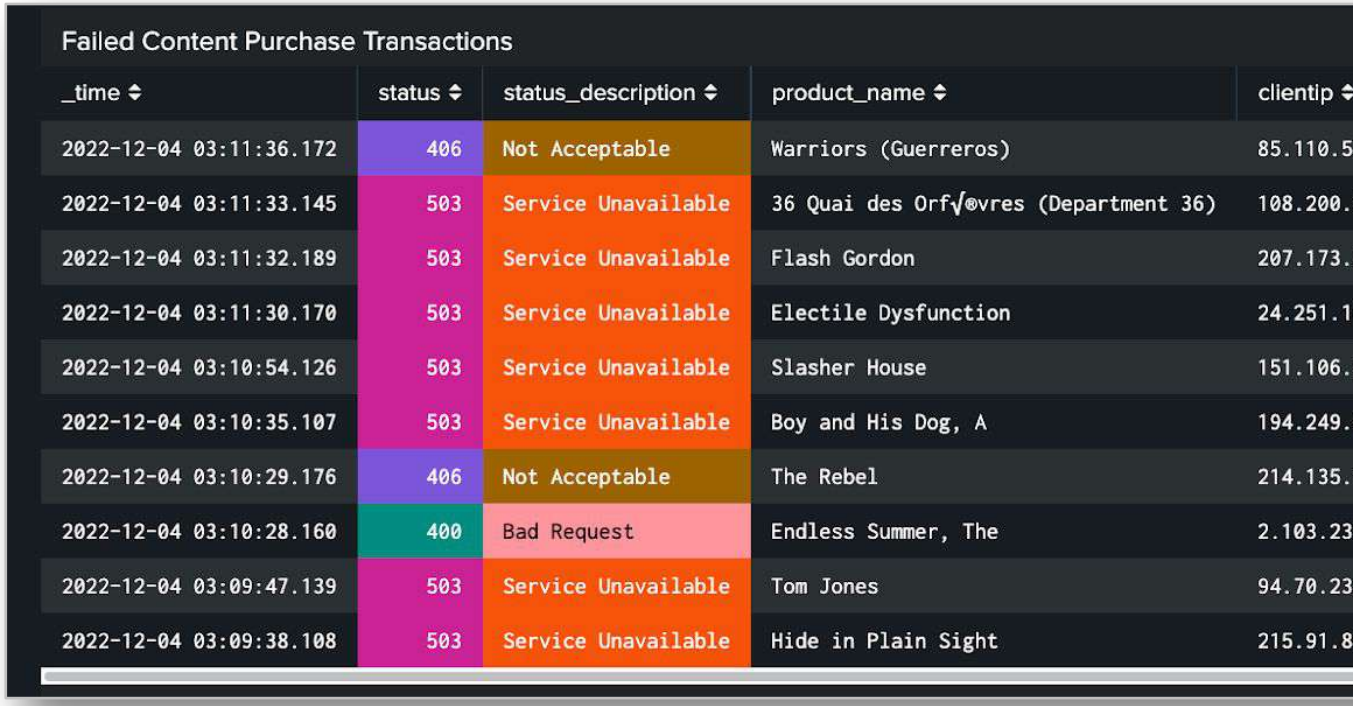
Dashboard 1 : Content operations dashboard

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 Orf√®vres (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
```

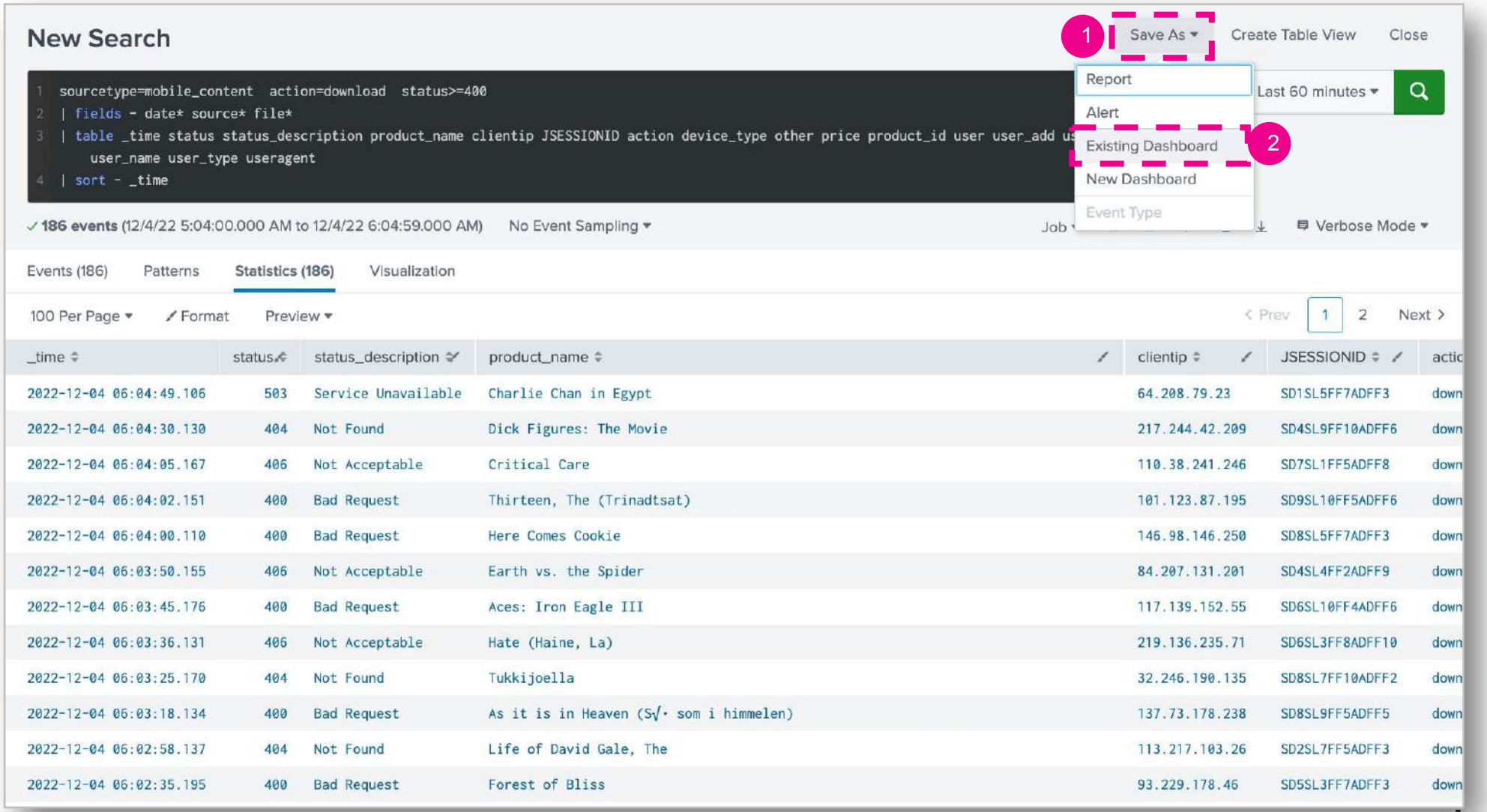
_time	status	status_description	product_name	clientip	JSESSIONID	action	device_type	other
2022-12-04 06:04:49.106	503	Service Unavailable	Charlie Chan in Egypt	64.208.79.23	SD1SL5FF7ADFF3	download	Linux	743
2022-12-04 06:04:30.130	404	Not Found	Dick Figures: The Movie	217.244.42.209	SD4SL9FF10ADFF6	download	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 (S√• som i himmelen)	137.73.178.238	SD8SL9FF5ADFF5	download	Linux	390

splunk>

Dashboard 1 : Content operations dashboard

Show top device type access requests

Solution:

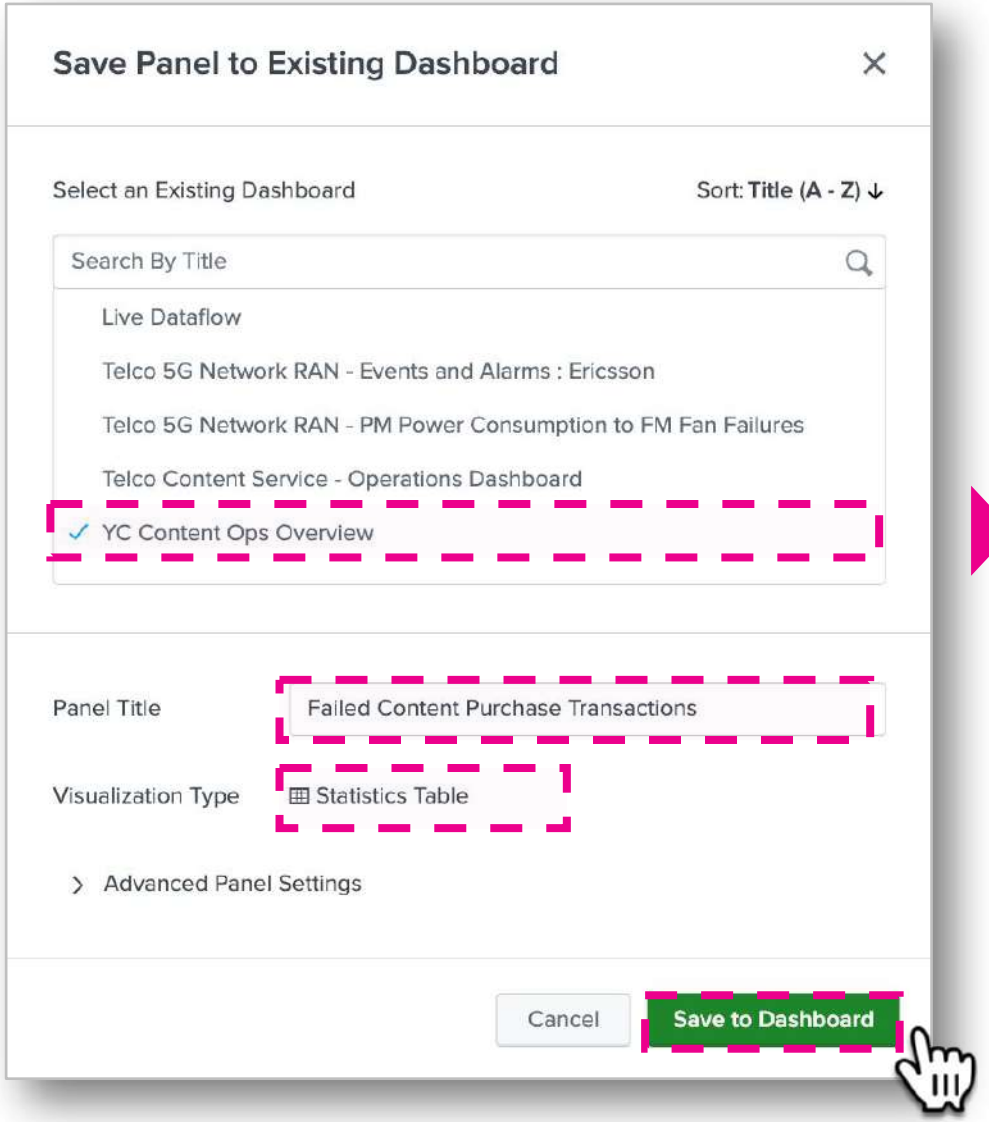


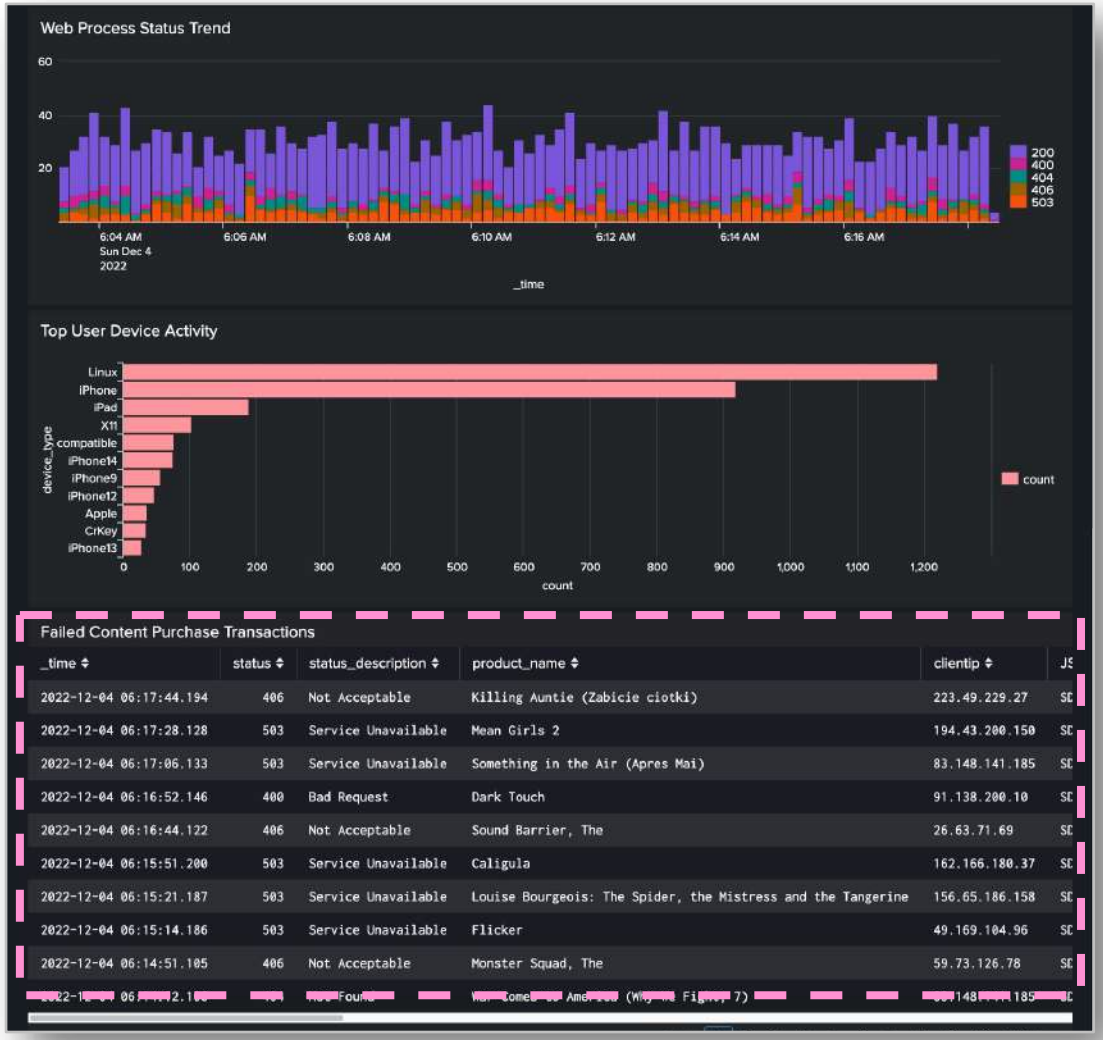
_time	status	status_description	product_name	clientip	JSESSIONID	actic
2022-12-04 06:04:49.106	503	Service Unavailable	Charlie Chan in Egypt	64.208.79.23	SD1SL5FF7ADFF3	down
2022-12-04 06:04:30.130	404	Not Found	Dick Figures: The Movie	217.244.42.209	SD4SL9FF10ADFF6	down
2022-12-04 06:04:05.167	406	Not 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 (S√· 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:



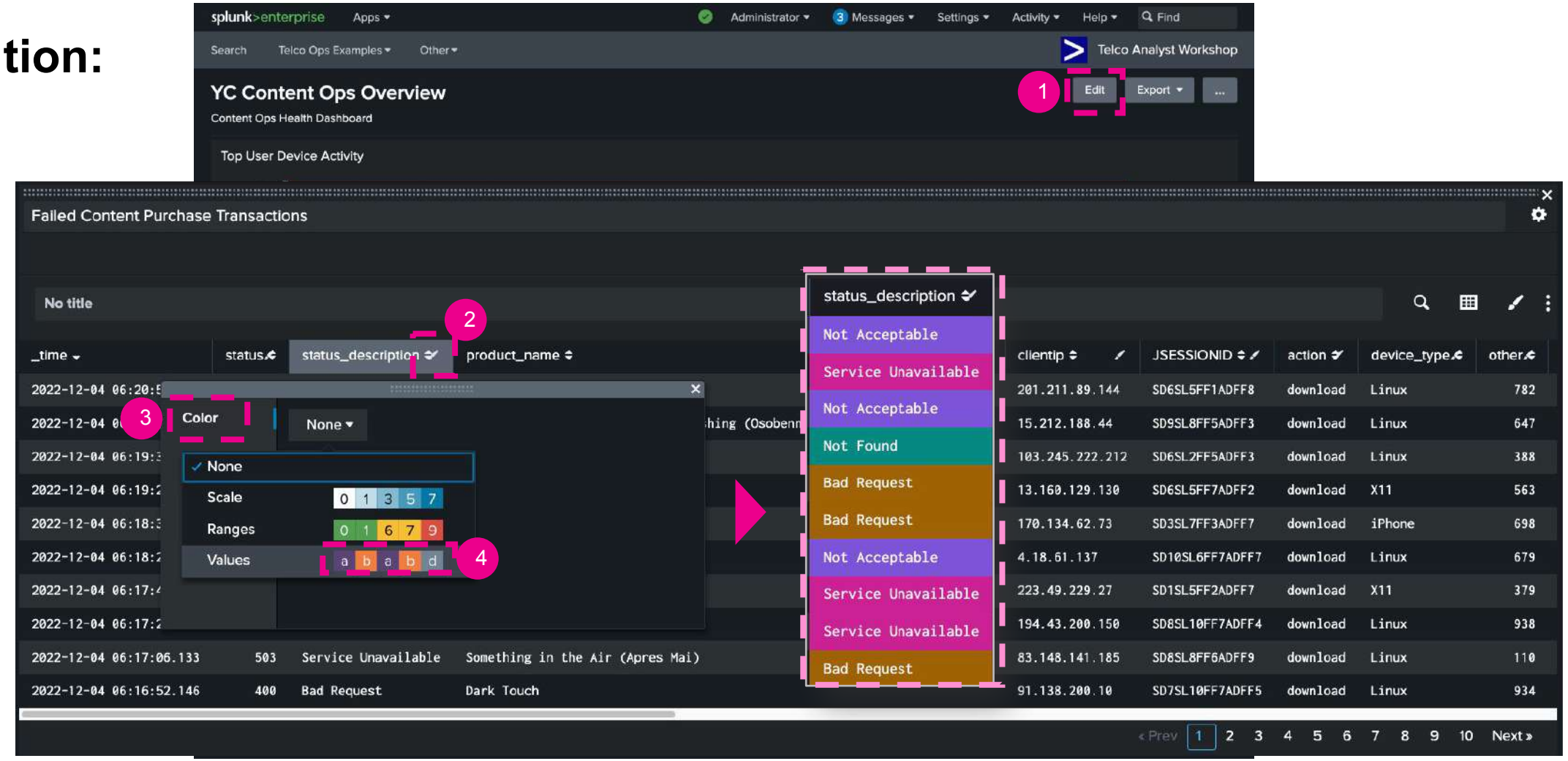


splunk>

Dashboard 1 : Content operations dashboard

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

Solution:



splunk>

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**

We're going to add one of these to our dashboard

Dashboard 1 : Content operations dashboard

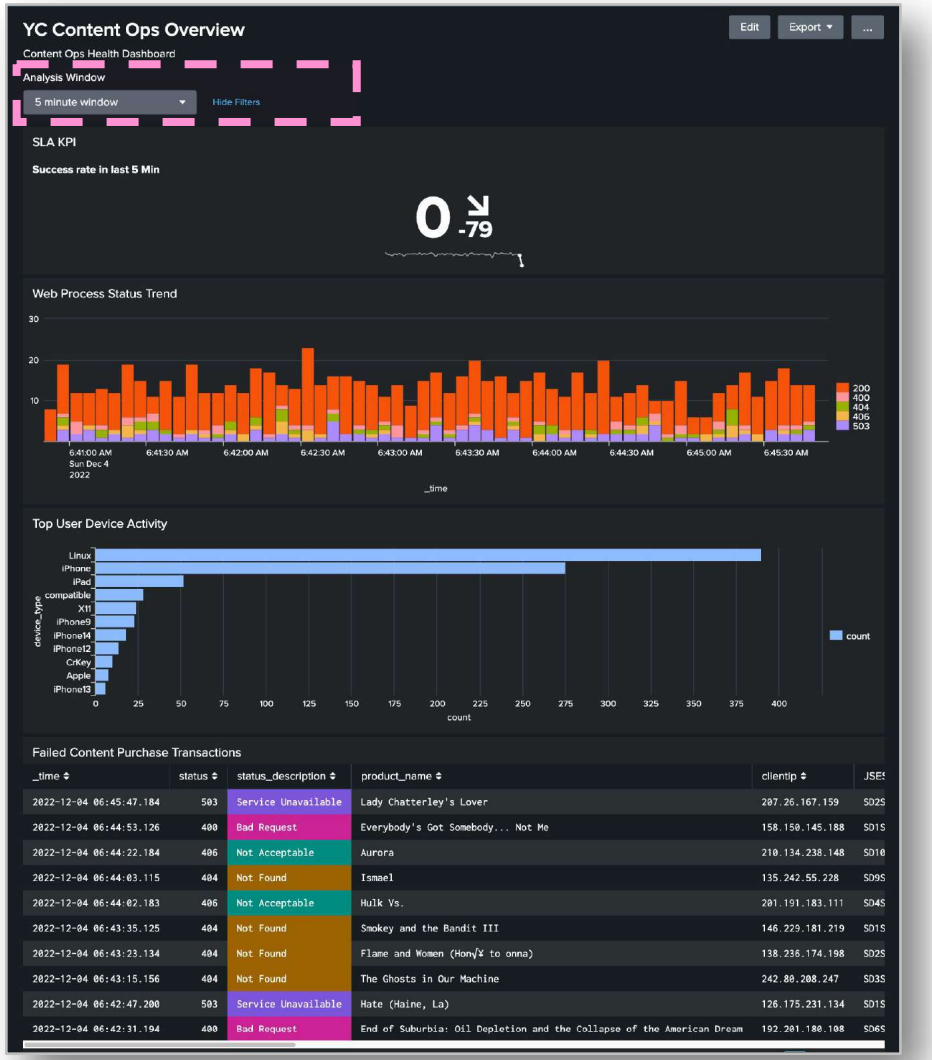
Enhance Dashboard

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.

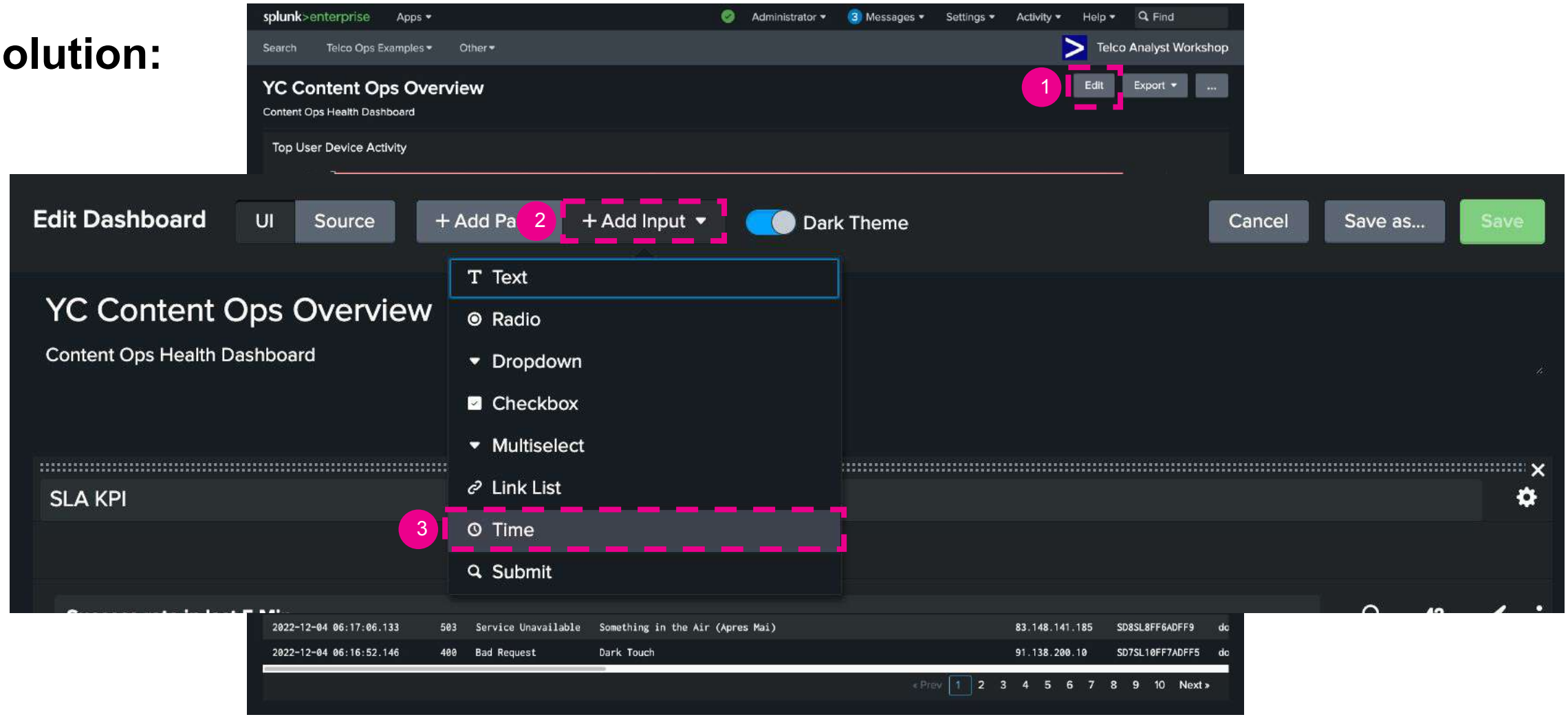
Goal:



Dashboard 1 : Content operations dashboard

Enhance Dashboard.

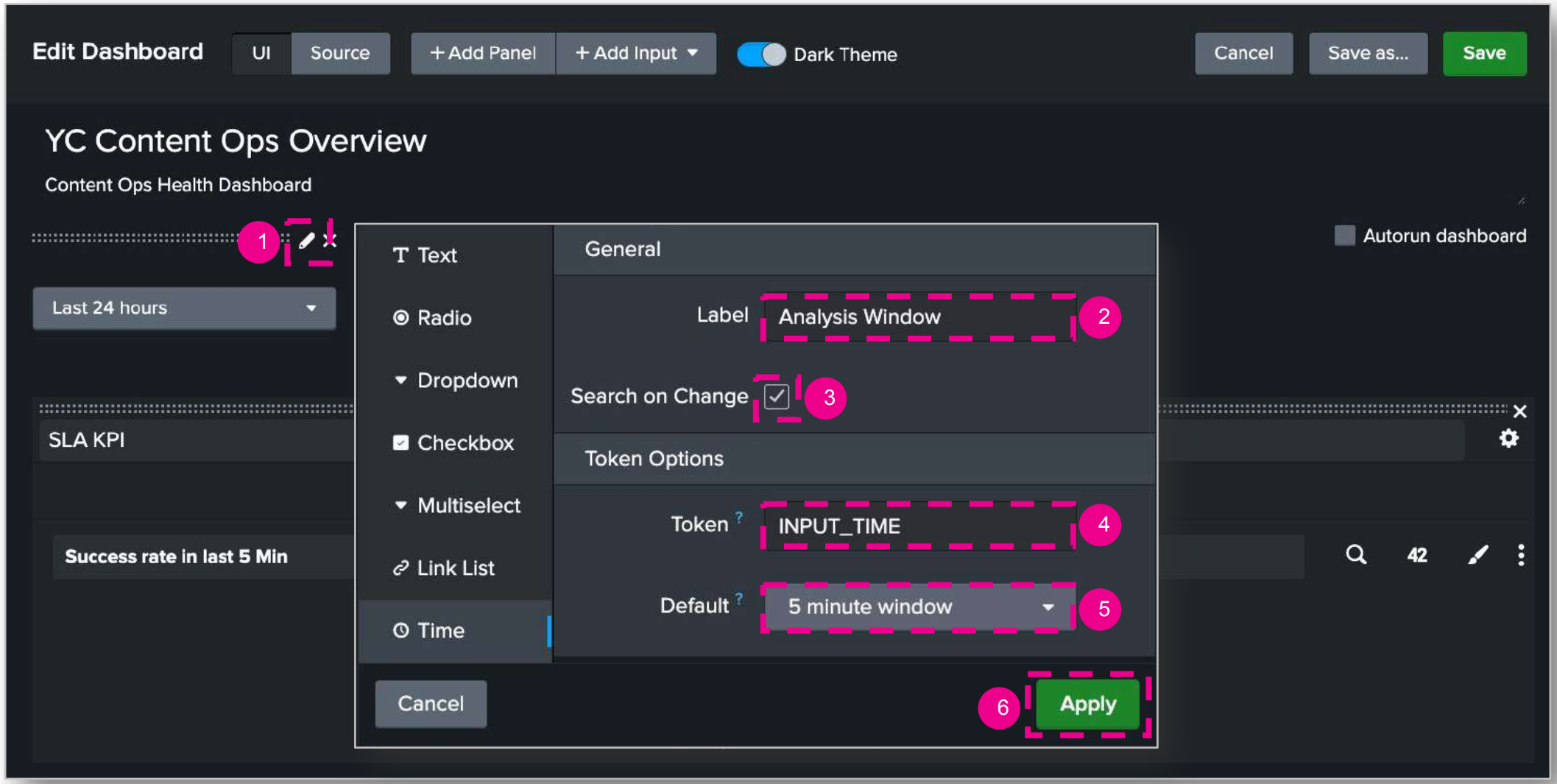
Solution:



Dashboard 1 : Content operations dashboard

Enhance Dashboard.

Solution:

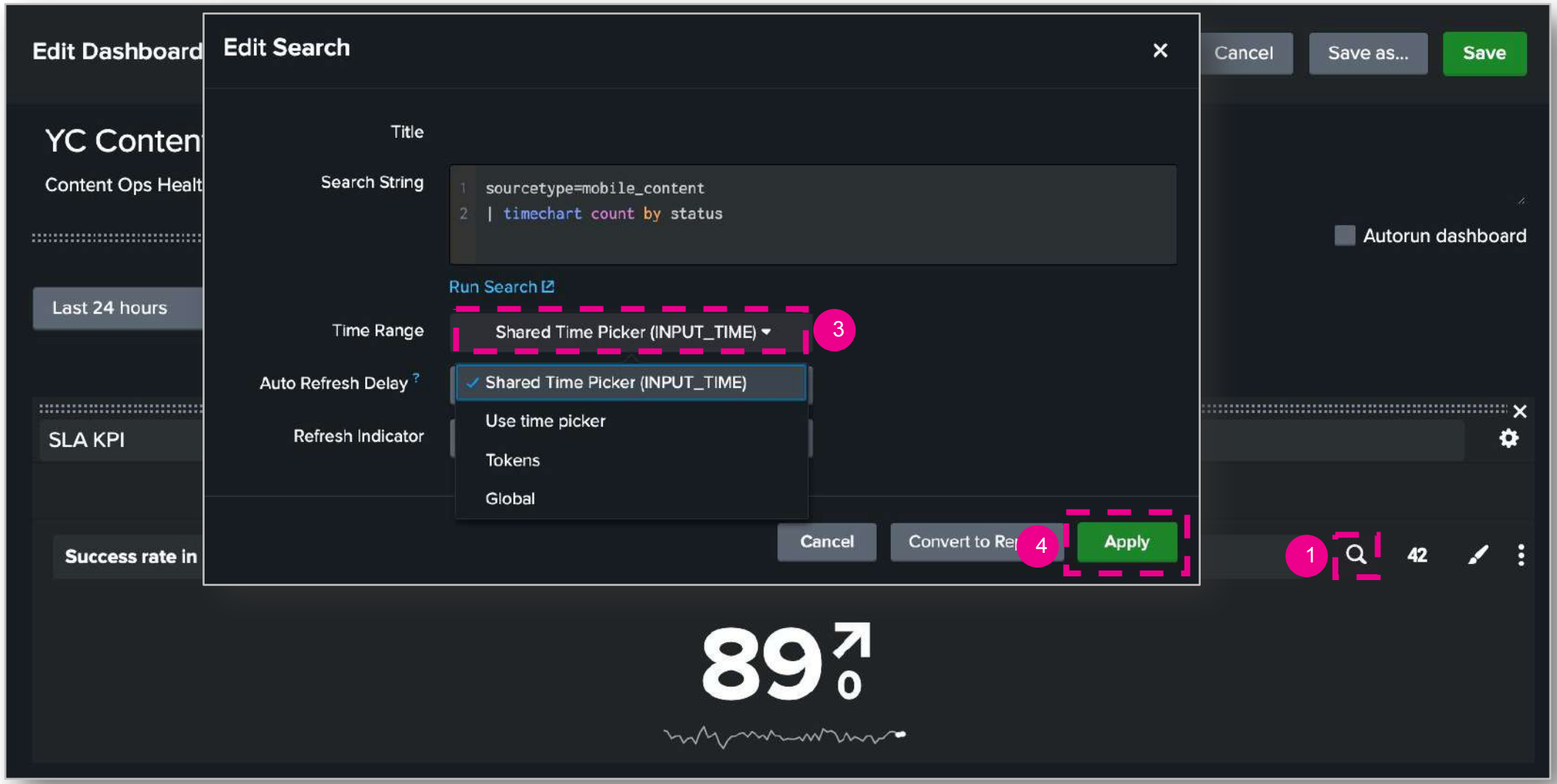


splunk>

Dashboard 1 : Content operations dashboard

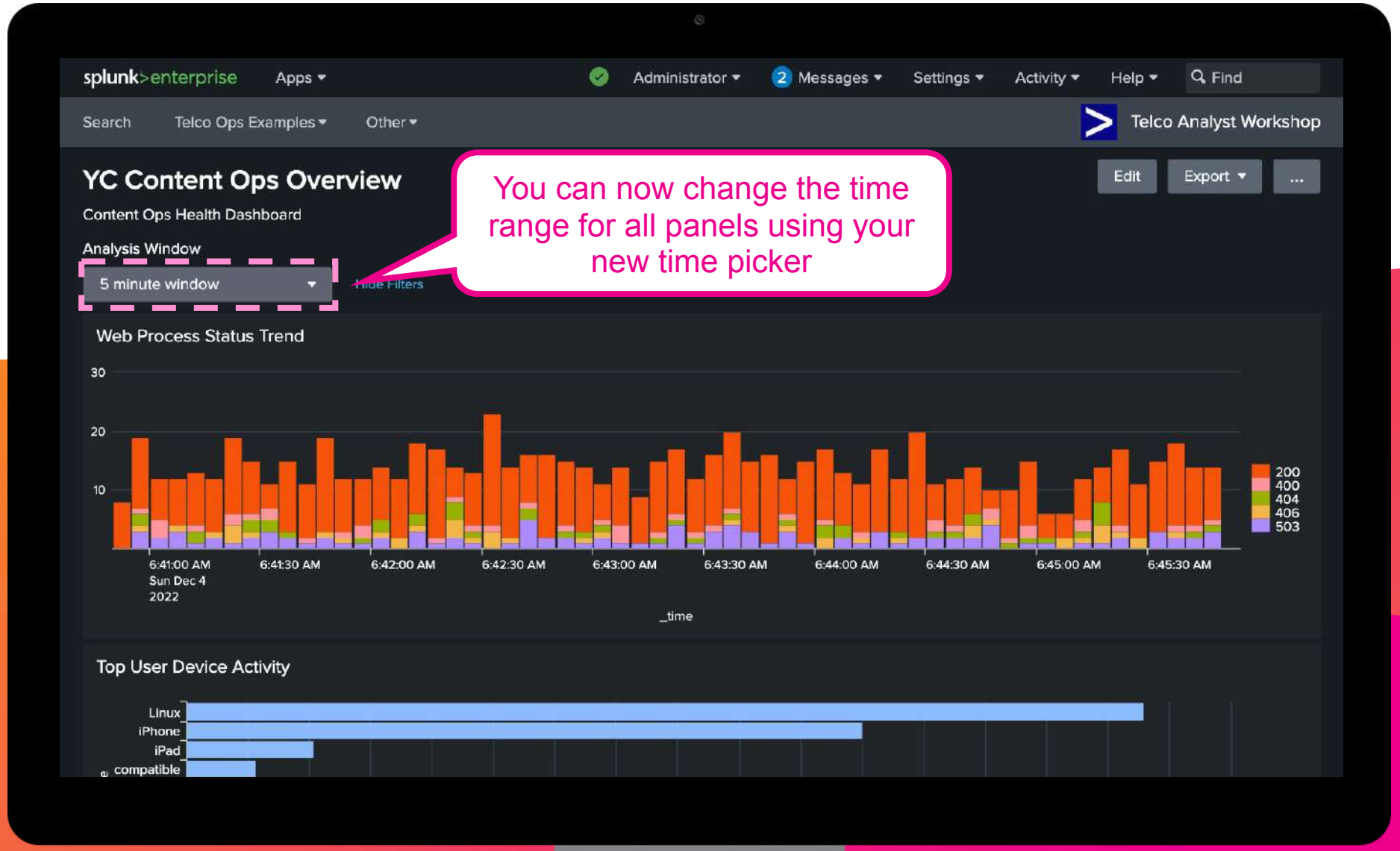
Enhance Dashboard.

Solution:



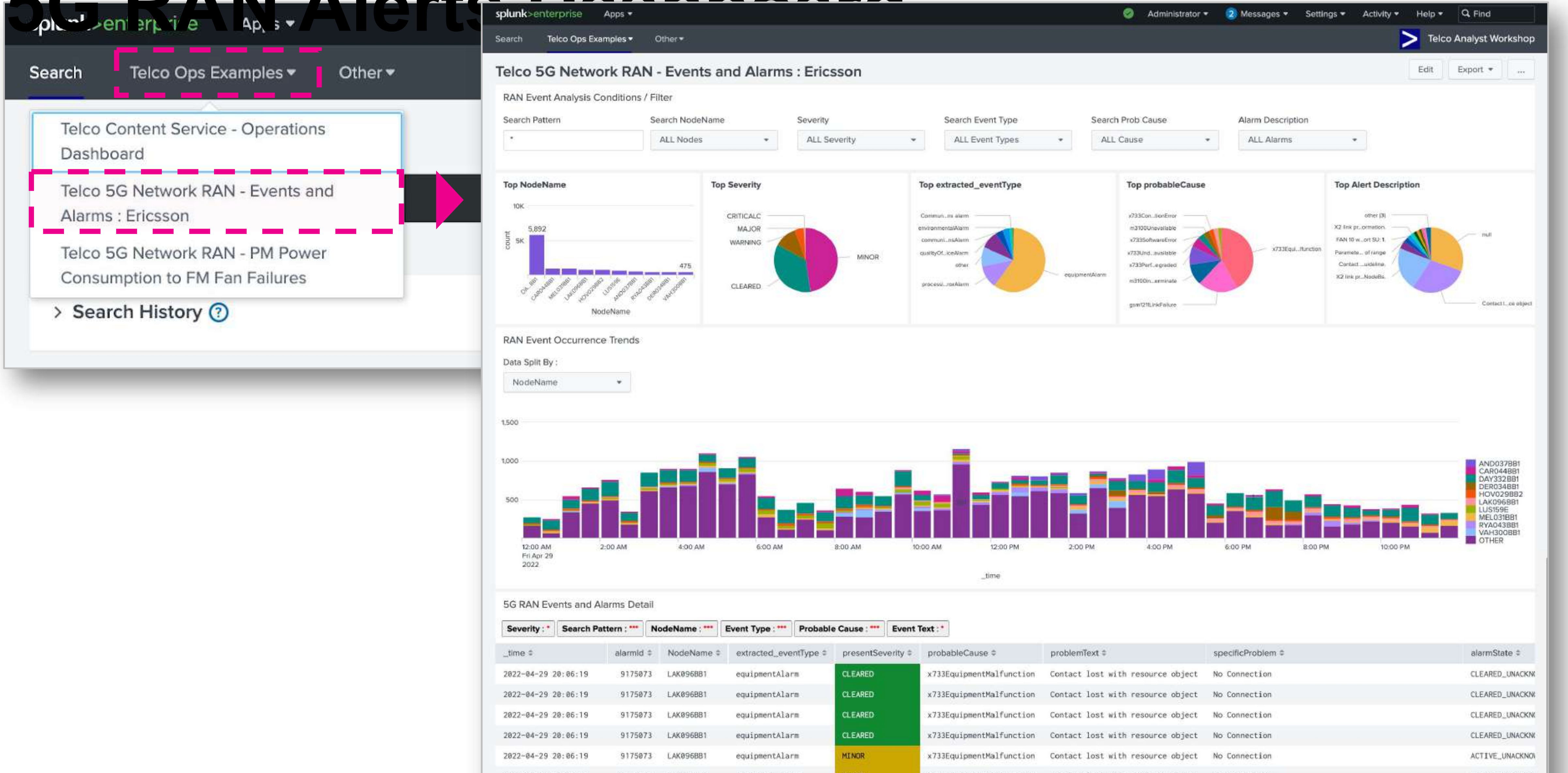
splunk>

Content Ops Dashboard Completed!



OSS 5G RAN Dashboard Dashboards

5G RAN Alerts Dashboard



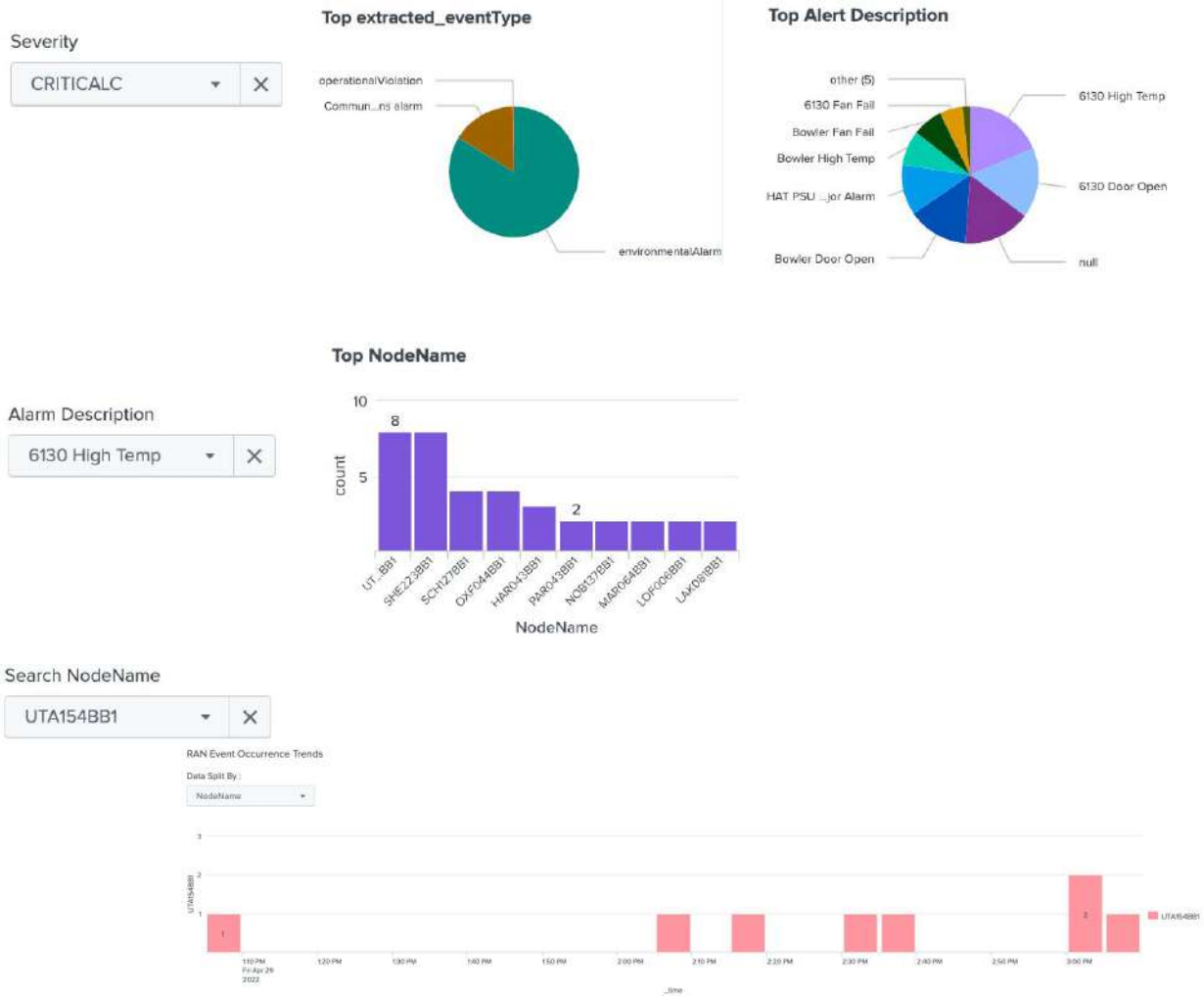
Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise

Analysis Tasks:

1. What is the most occurred events types that are “Critical”?
   - Top event types?
   - Top ”Alert Description”?
2. For “High Temp” alerts, which top 3 sites are most impacted (In term of most occurrence)?
   - Side ID for top 3 sites?
3. 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.

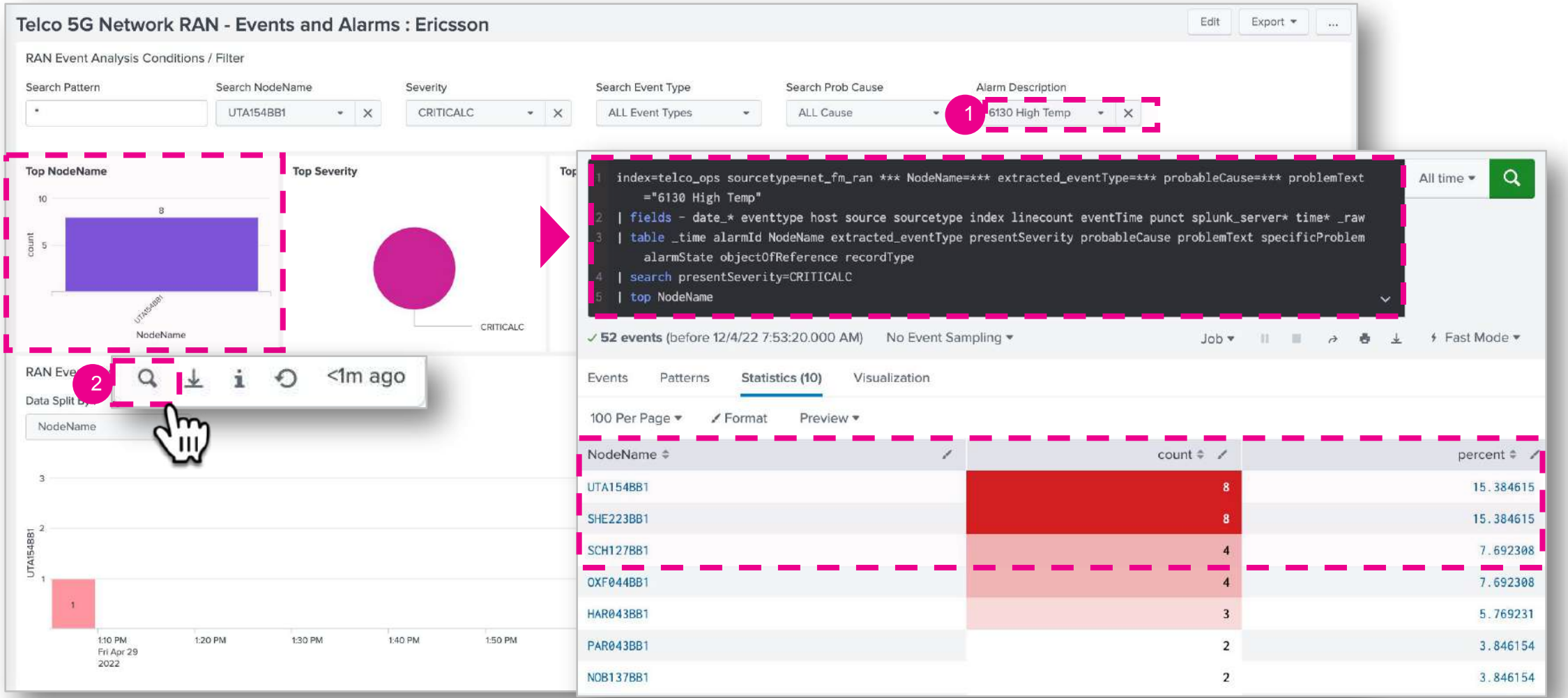
Task : What is the most occurred events types that are “Critical”?
- Top event types? - Top ”Alert Description”?

splunk>

Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

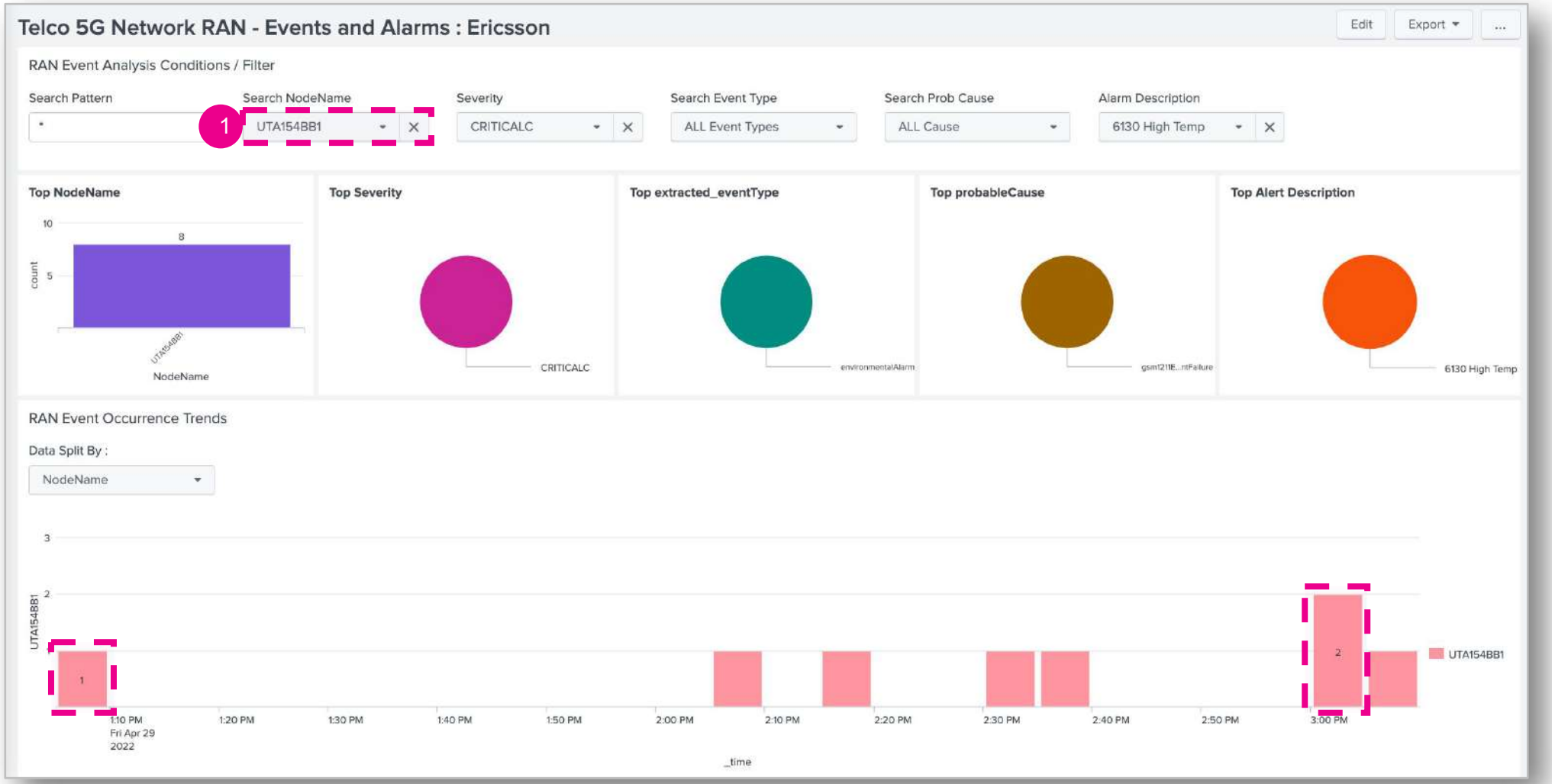
Task : For “High Temp” alerts, which top 3 sites are most impacted (In term of most occurrence)?
- Side ID for top 3 sites?



Dashboard 2 : 5G RAN Alarms Dashboard

Events analysis exercise.

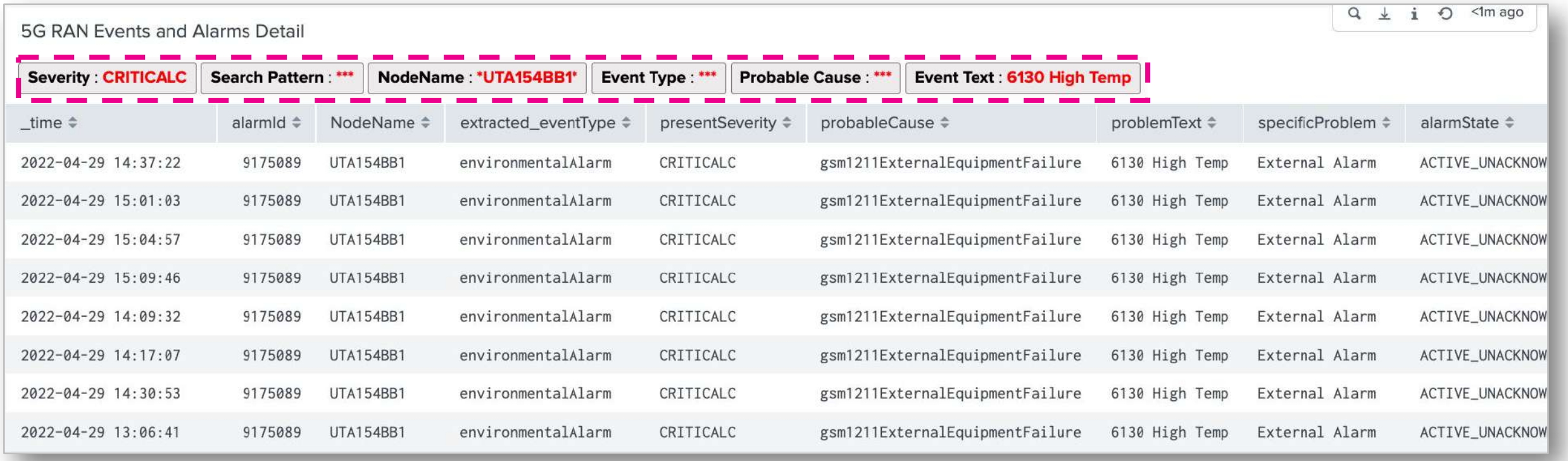
Task : For “UTA154BB1” site, when did those alerts occurred the most?
- Time for the most occurrence? - First time of occurrence?



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

<1m ago

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

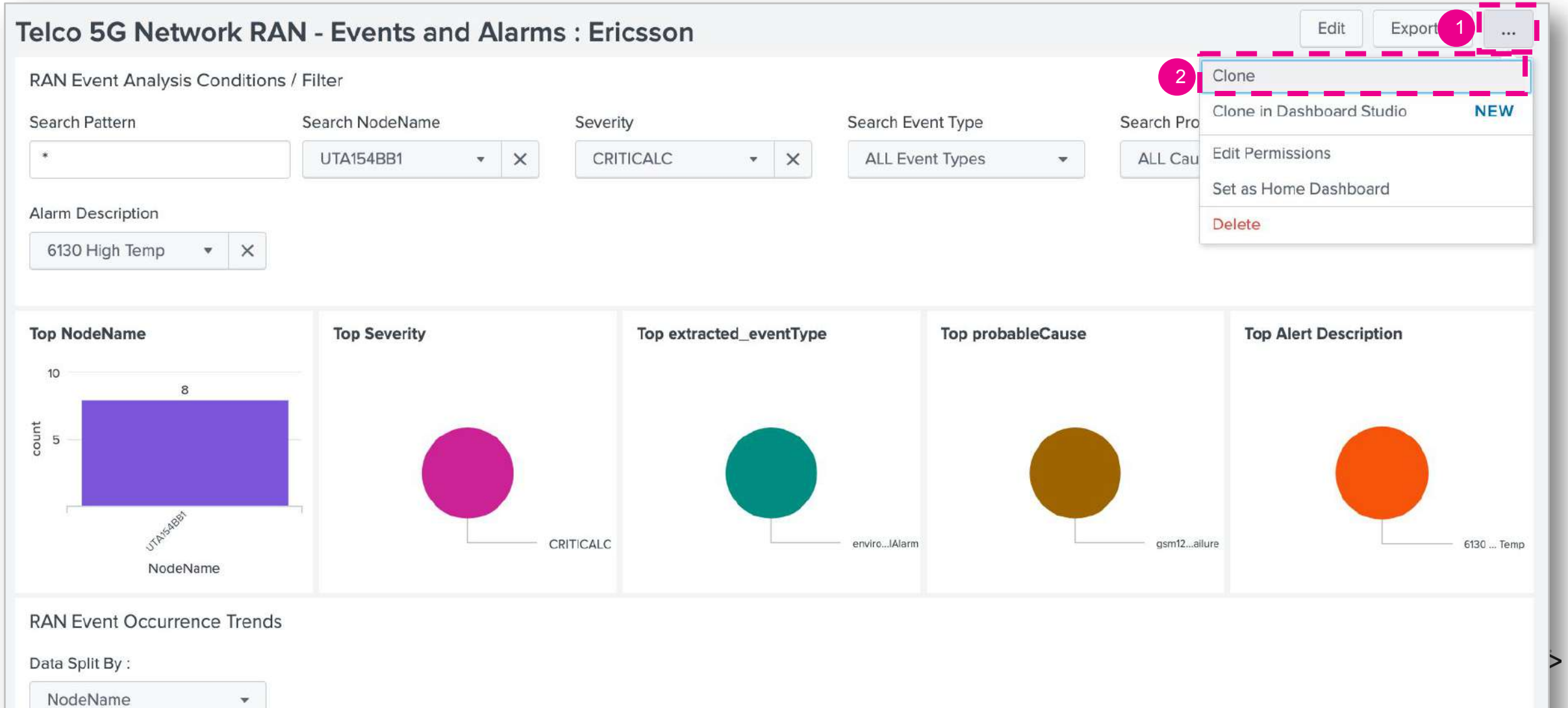
_time	alarmId	NodeName	extracted_eventType	presentSeverity	probableCause	problemText	specificProblem	alarmState
2022-04-29 14:37:22	9175089	UTA154BB1	environmentalAlarm	CRITICALC	gsm1211ExternalEquipmentFailure	6130 High Temp	External Alarm	ACTIVE_UNACKNOW
2022-04-29 15:01:03	9175089	UTA154BB1	environmentalAlarm	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

splunk>

Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

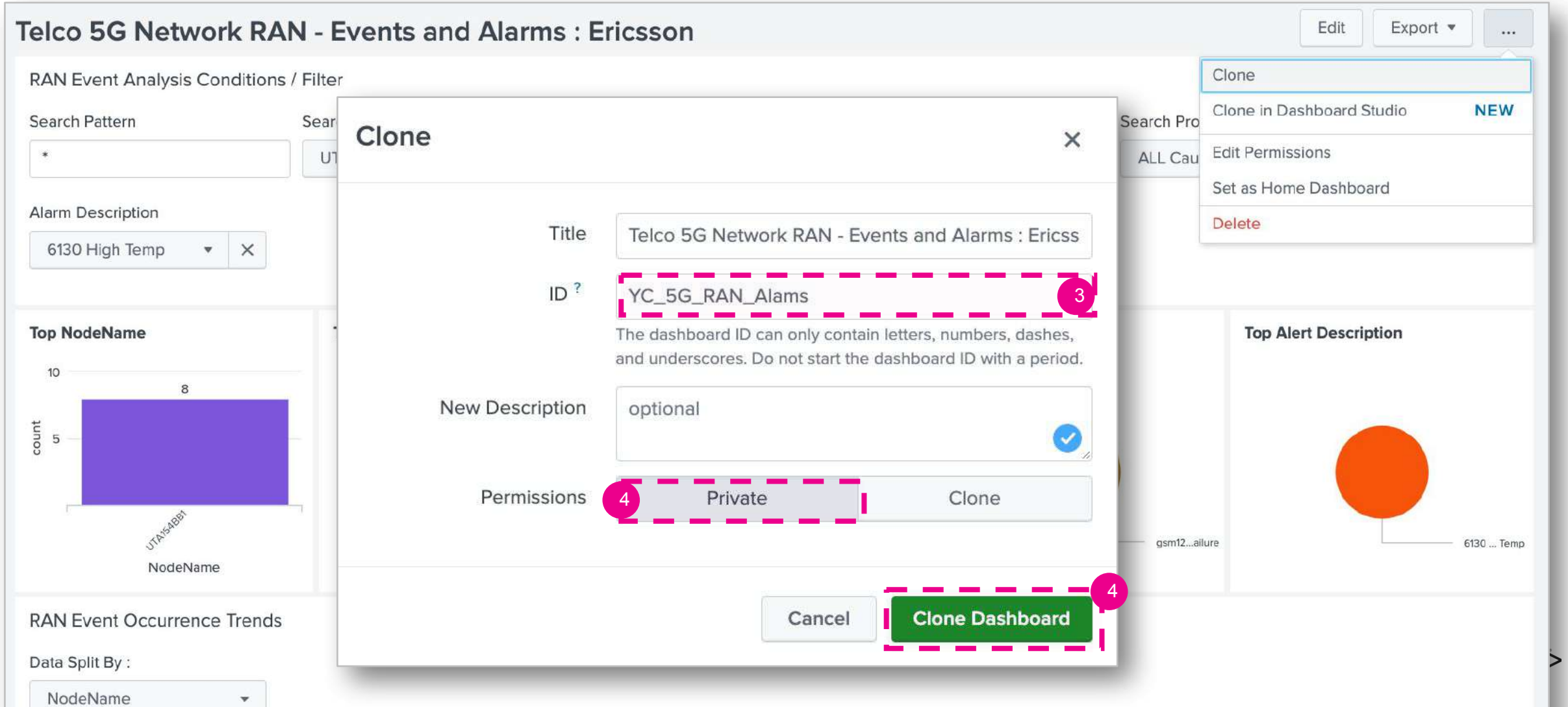
Task : For Duplicate the ”Telco 5G Network RAN” Dashboard with naming your initial in the front.



Dashboard 2 : 5G RAN Alarms Dashboard

Duplicate dashboard

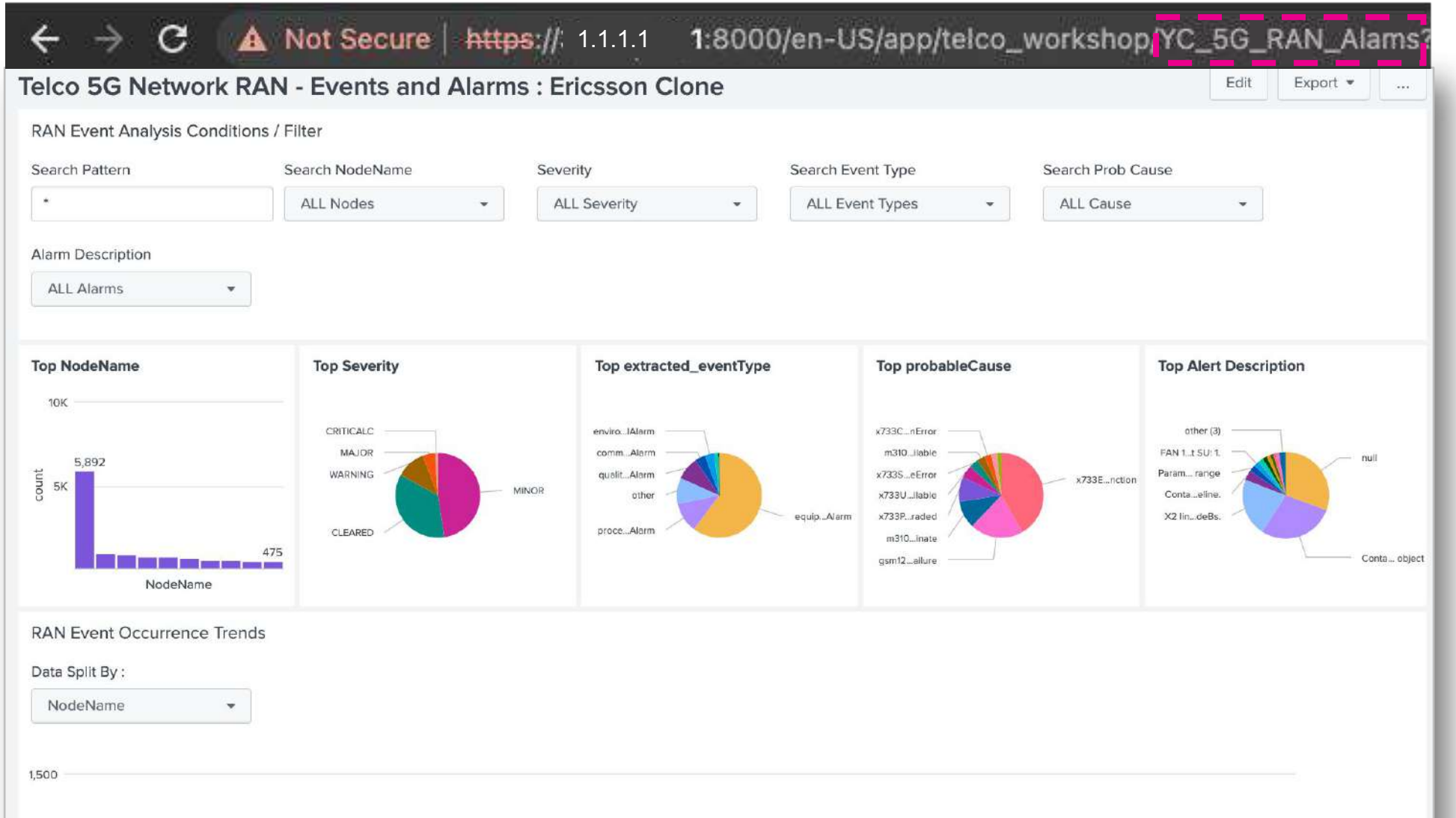
Task : For Duplicate the ”Telco 5G Network RAN” Dashboard with naming your initial in the front.



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

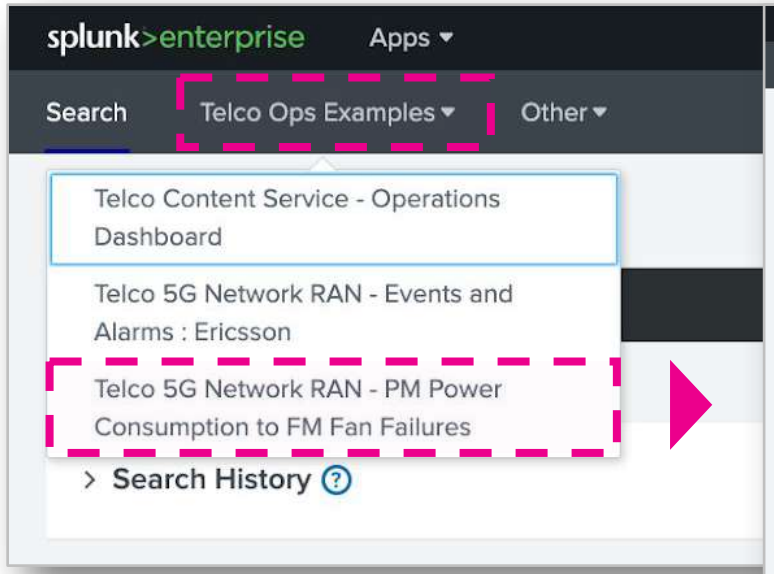
Duplicate dashboard

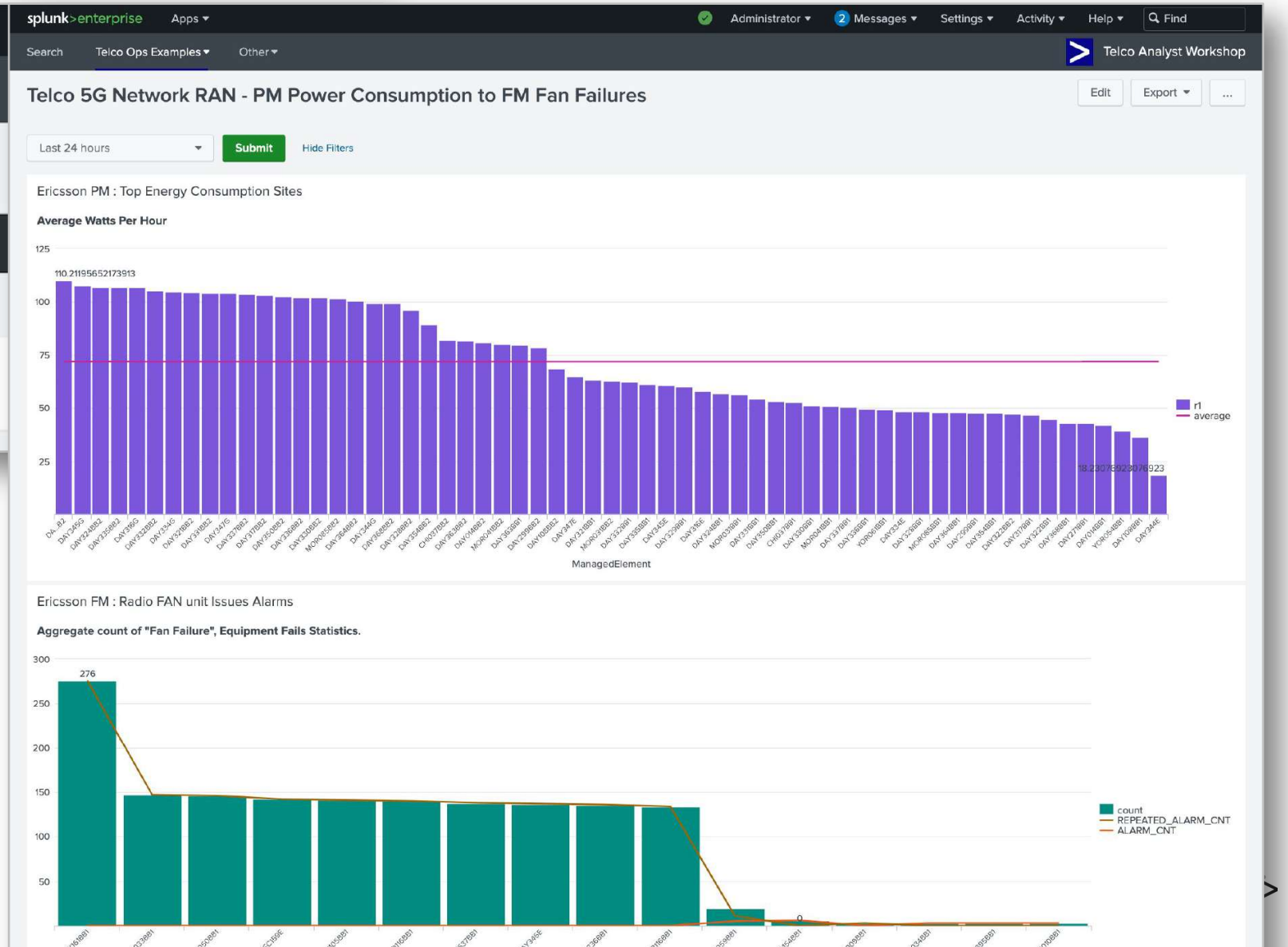
Task : With cloned dashboard, check out the dashboard XML Code

OSS 5G RAN
Event Correlations

Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis





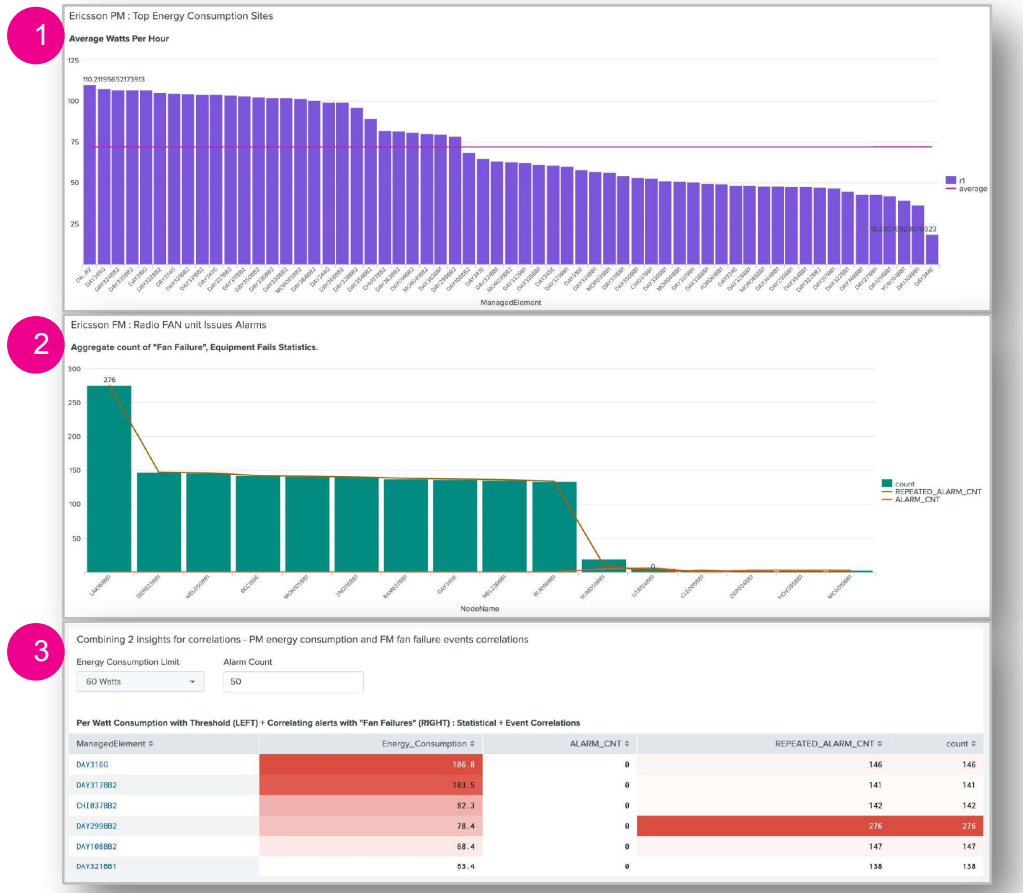
Dashboard 3 : 5G RAN Event Correlations

Events and Analytical correlation analysis

Analysis Tasks:

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.

Goal:



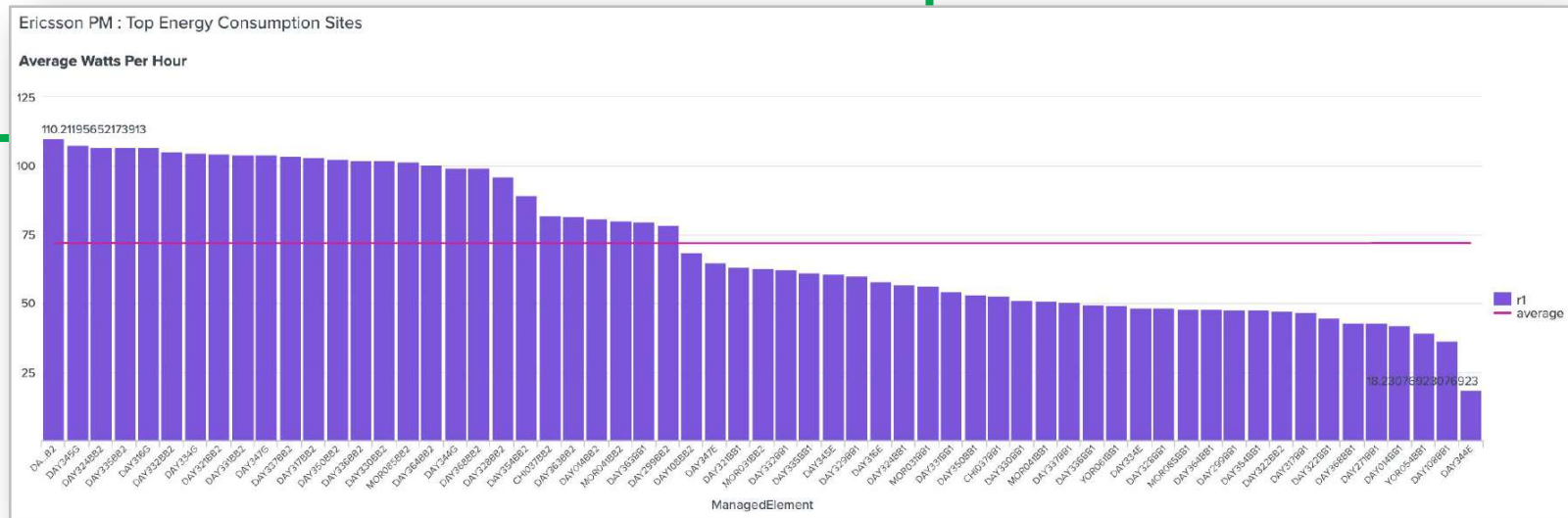
splunk>

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
```

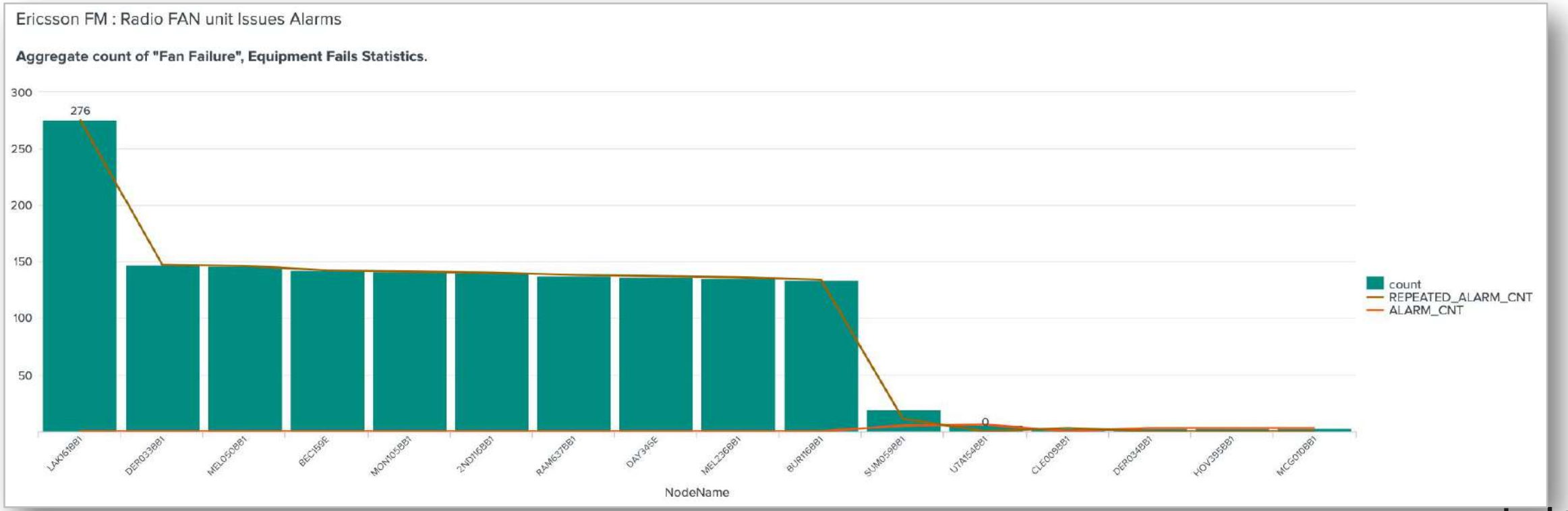


Dashboard 3 : 5G RAN Event Correlations

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
```



splunk>

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 occurence.

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

splunk>

Splunk Resources

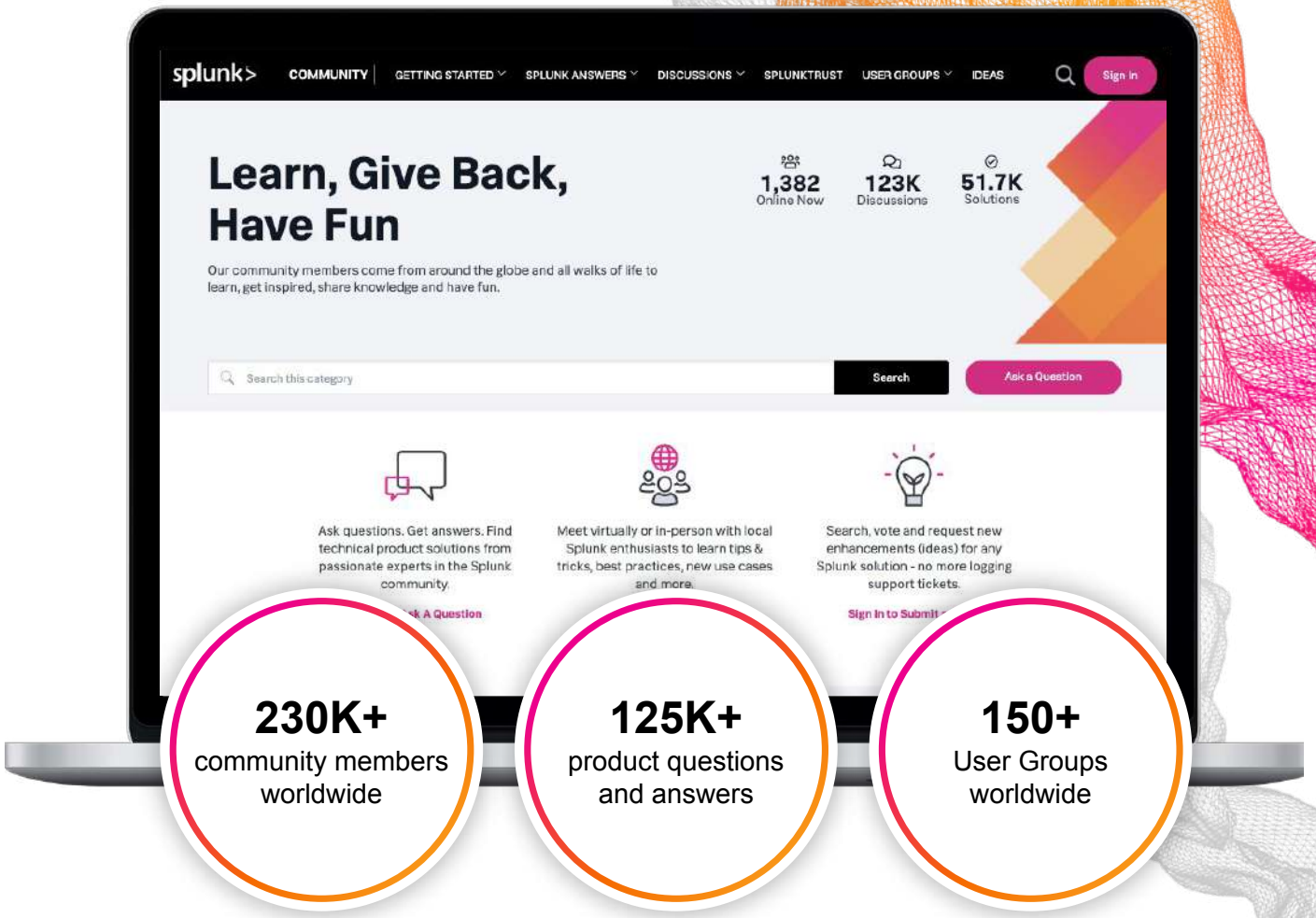
Where to go after today's workshop

splunk>

Splunk Community

https://community.splunk.com

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



splunk>

Splunk Events

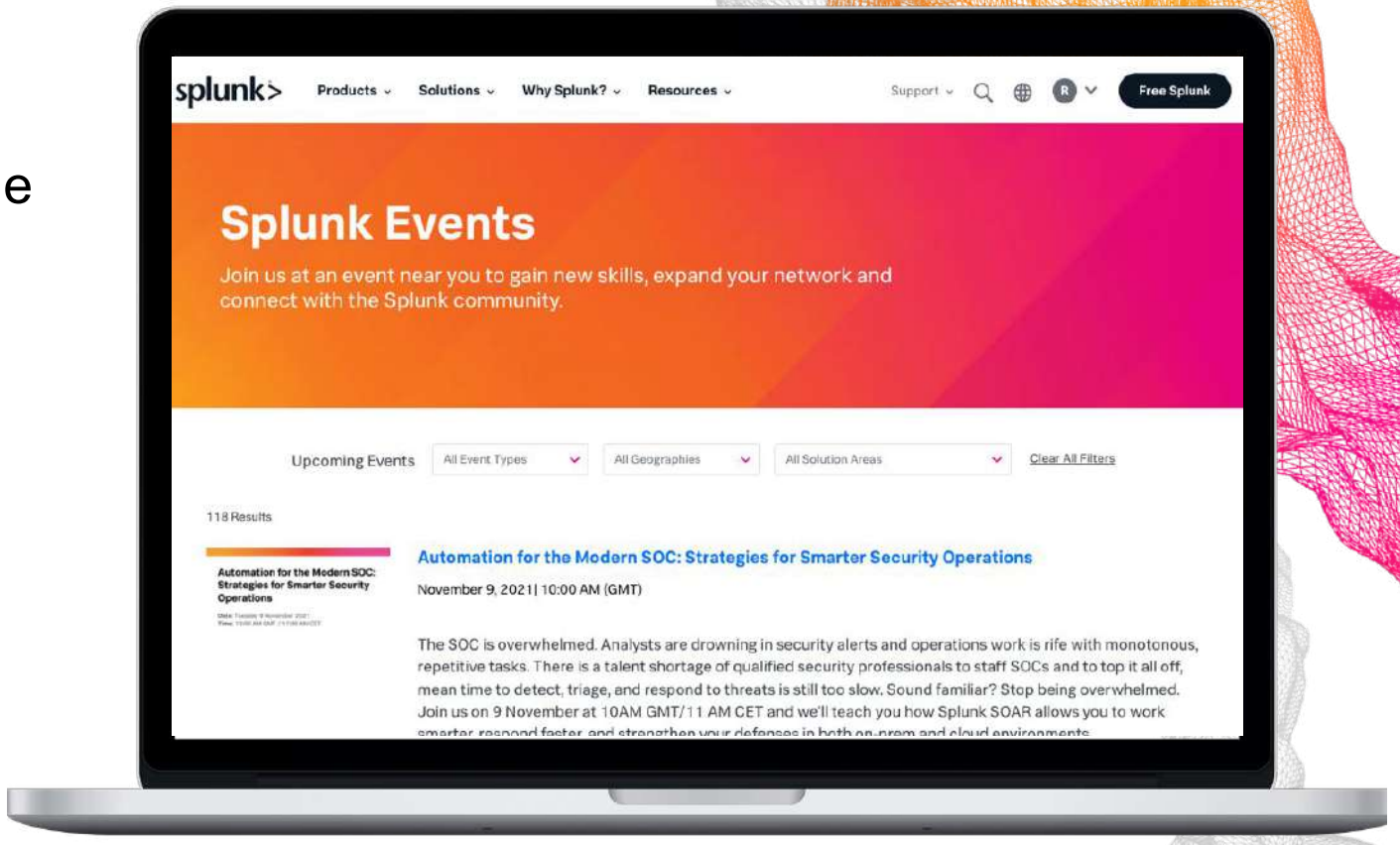
https://events.splunk.com

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

.conf

https://conf.splunk.com

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

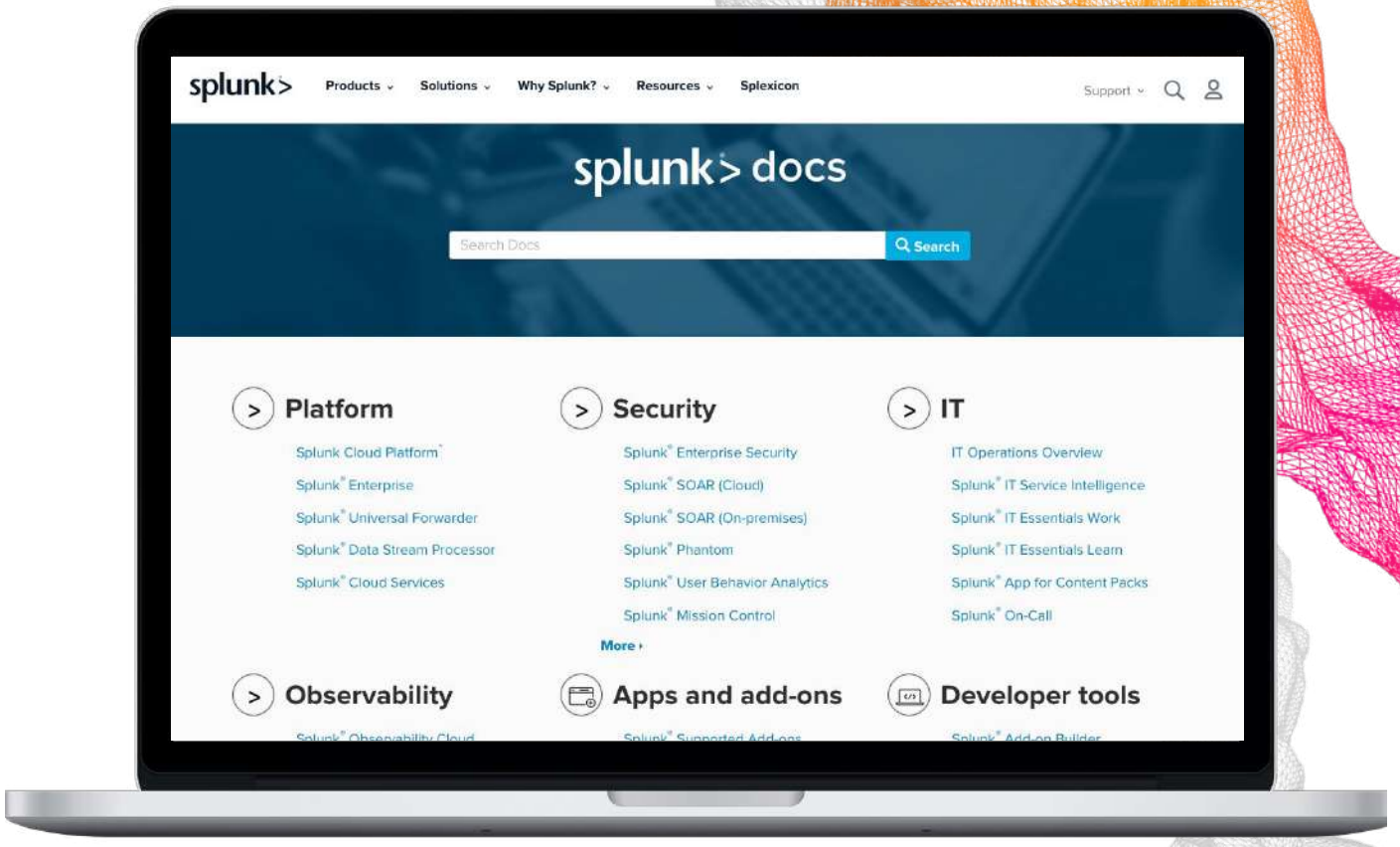


splunk>

Documentation

https://docs.splunk.com

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

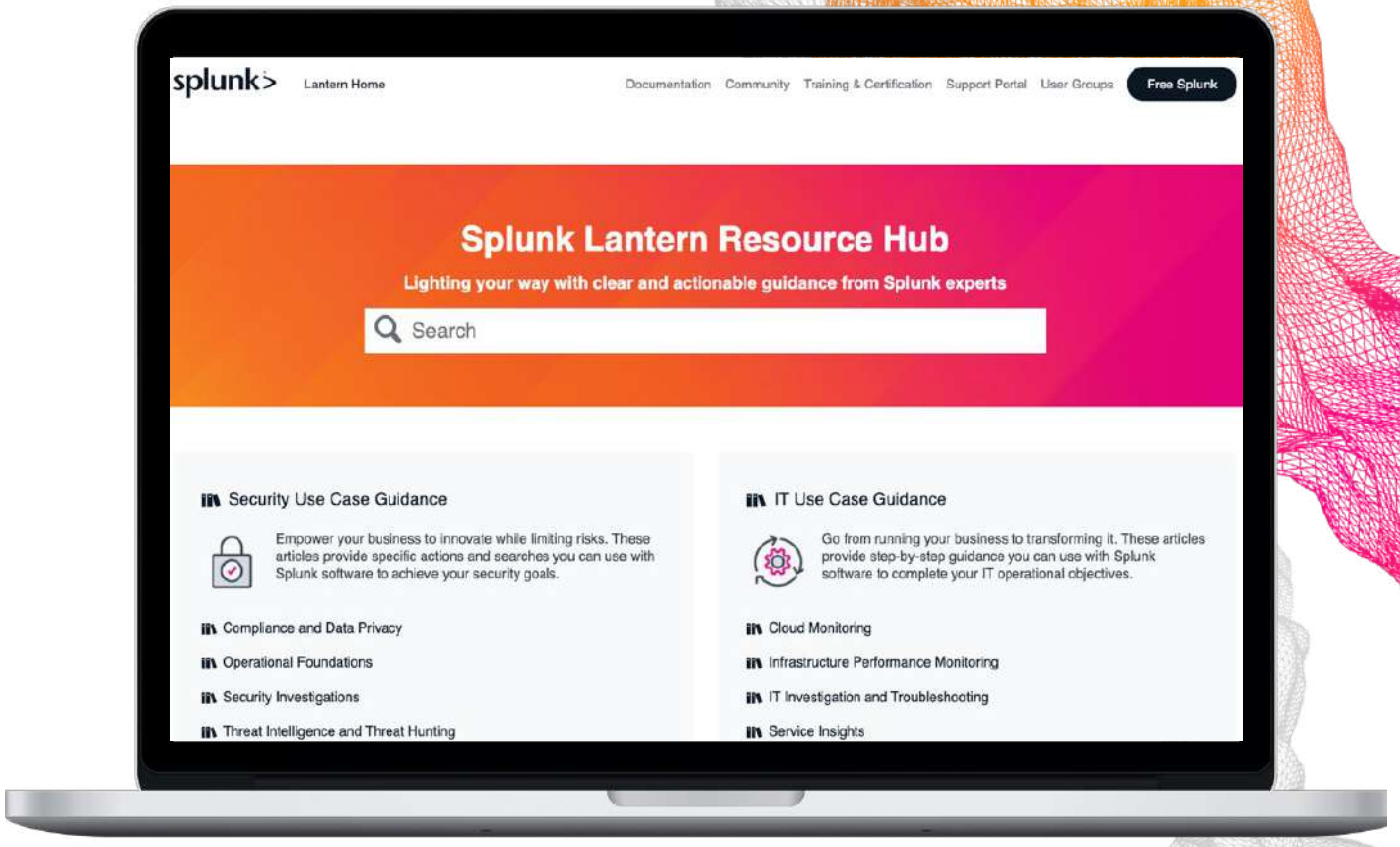


splunk>

Splunk Lantern

https://lantern.splunk.com

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

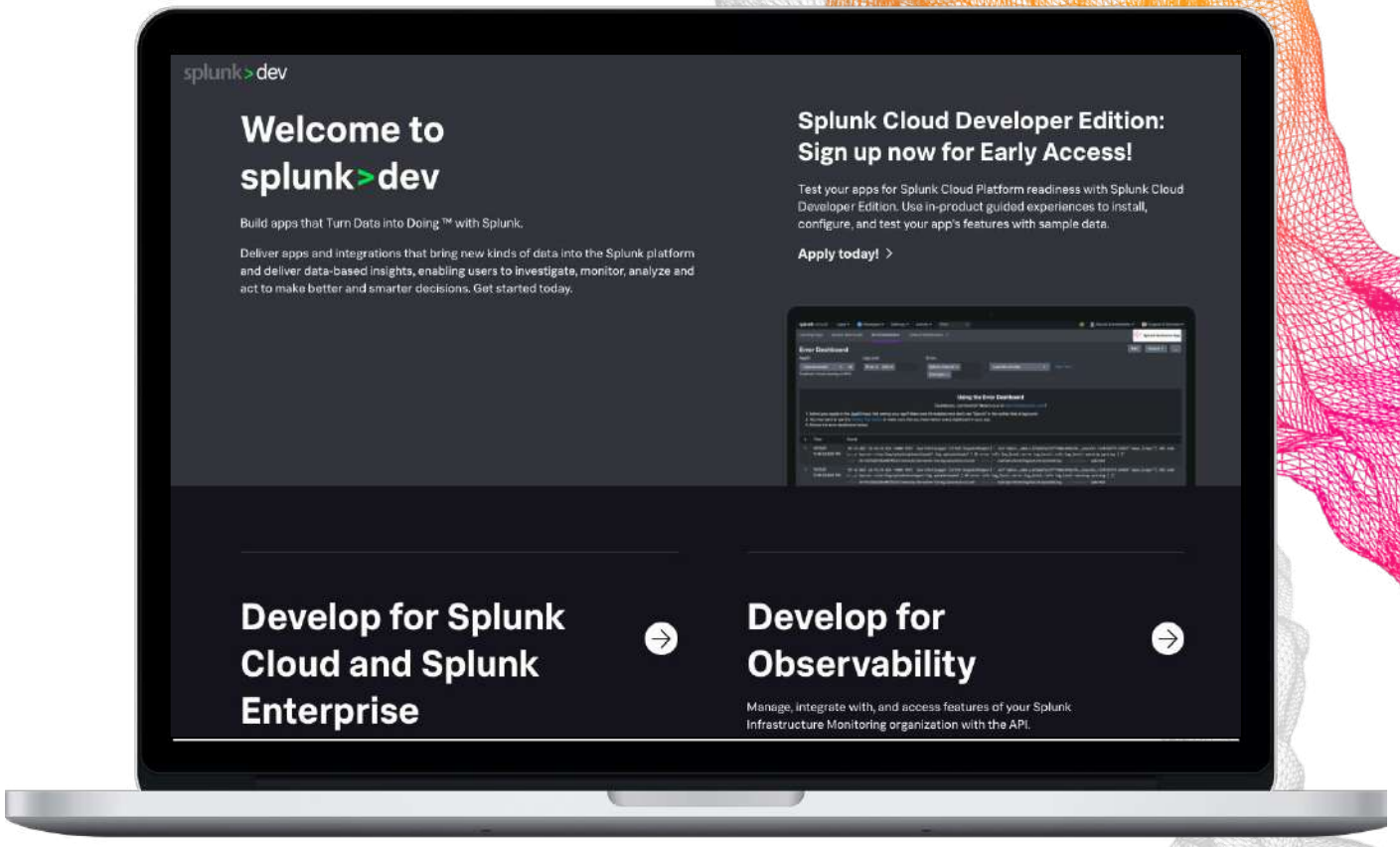


splunk>

Developer Resources

https://dev.splunk.com

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

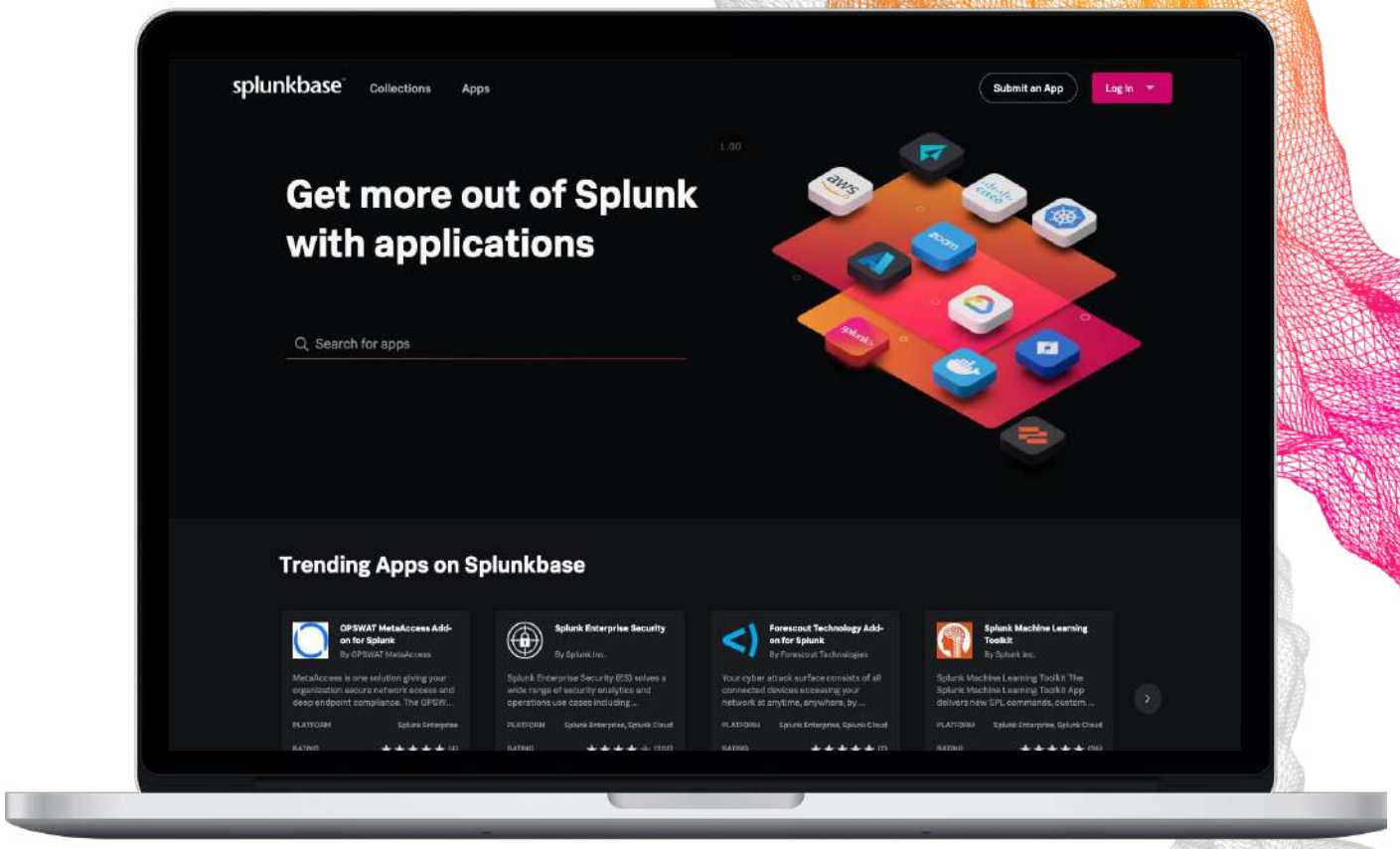


splunk>

Splunk Apps & Add-ons

https://splunkbase.splunk.com/

- 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

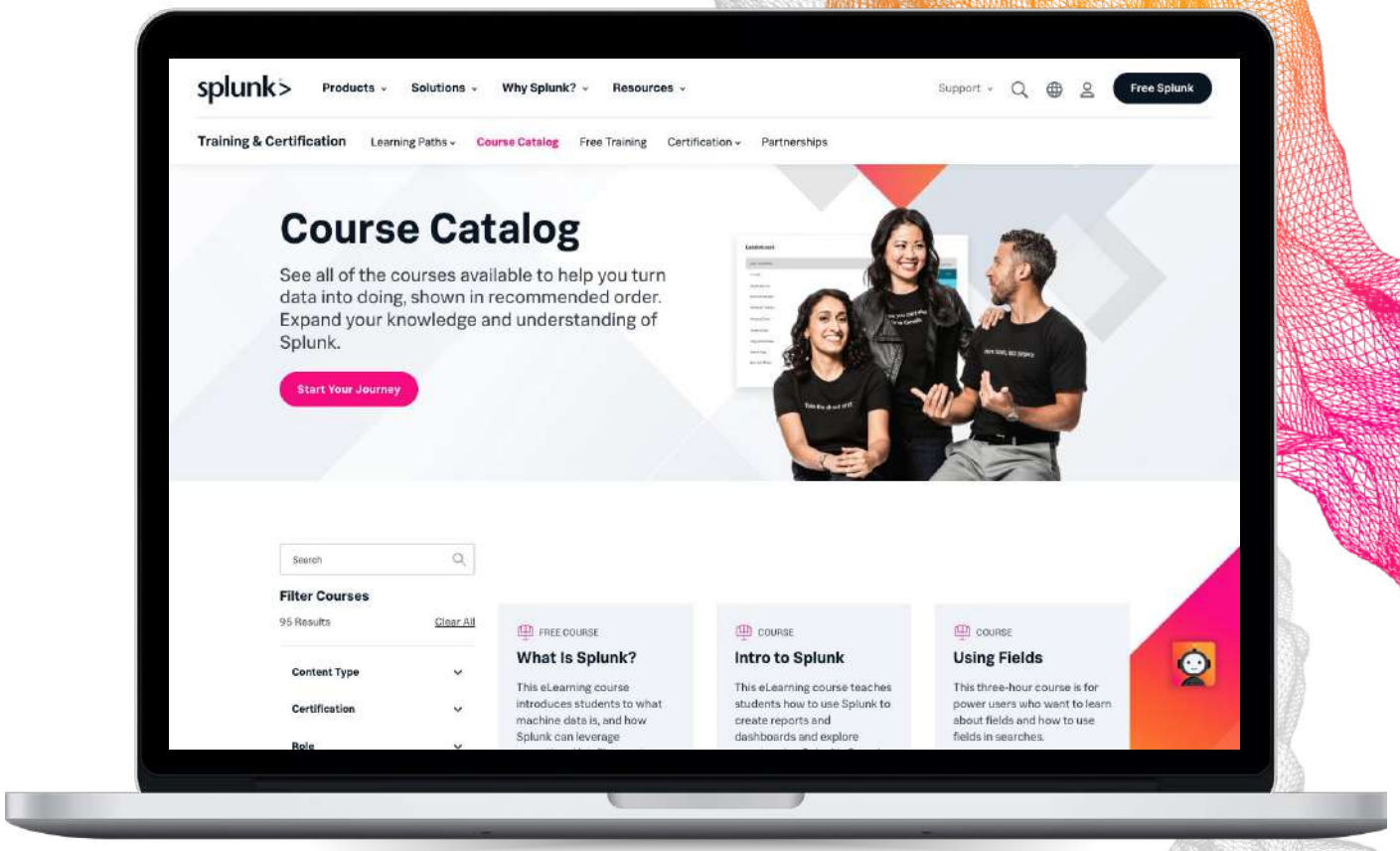
https://splunk.com/training

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



splunk>

Thank You!