splunk> 4rookies

Machine Learning Event Workshop

splunk> a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

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

splunk>

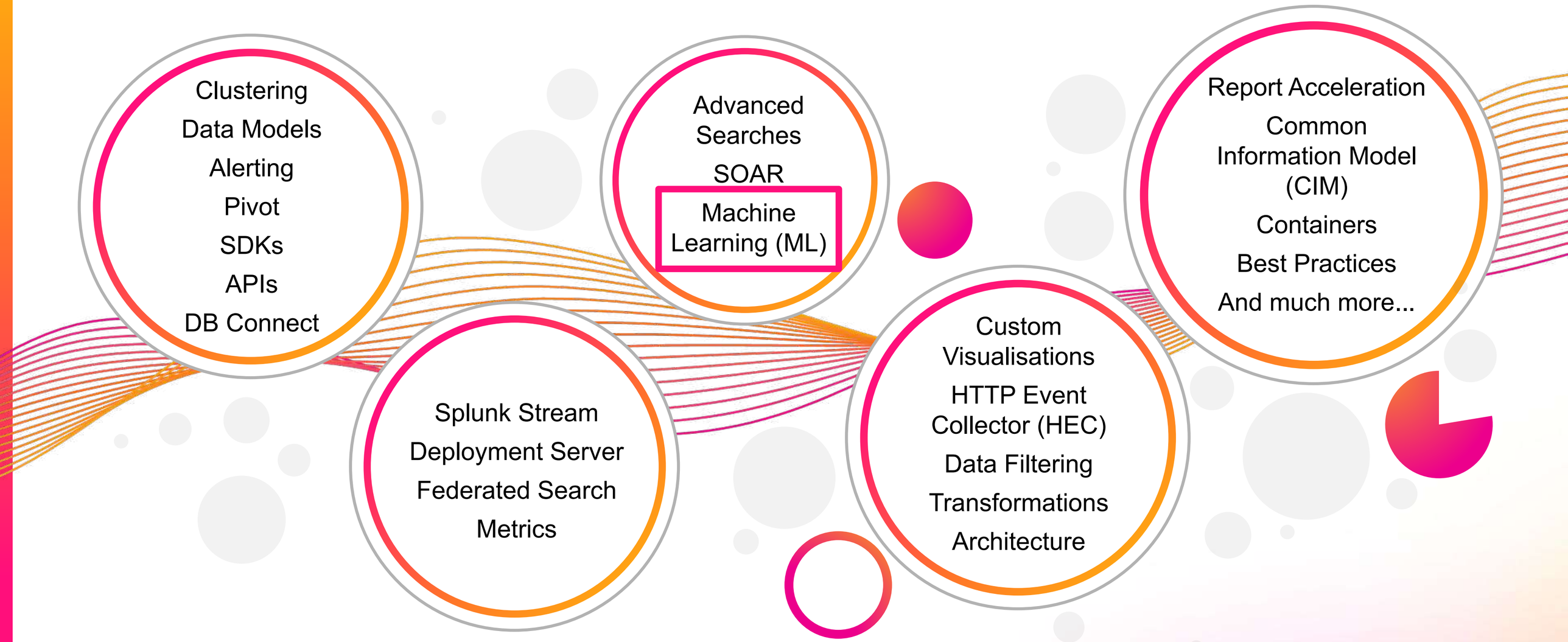
Please introduce yourself!

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

Workshop Agenda

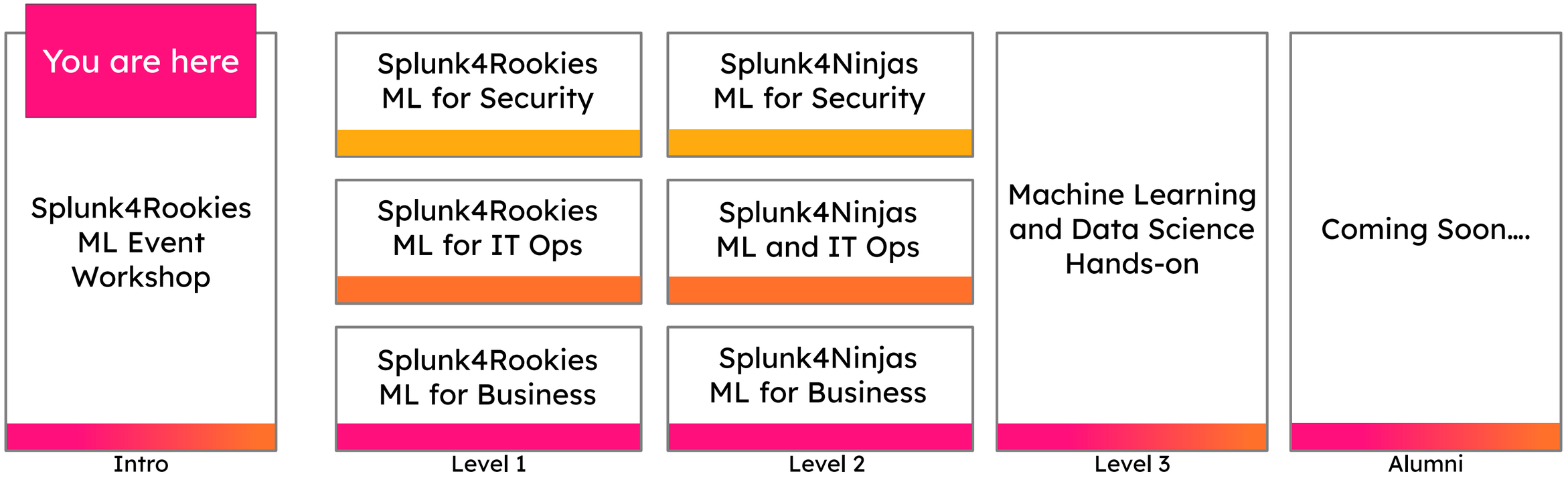
- What is Splunk
- What is Machine Learning - Terminology
- Demystify ML/AI
- The Process
- Onboard and Cleanse Data
- Data Analysis and Insights
- Advanced Capabilities
- What next…

Splunk4Rookies Machine Learning



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

Splunk Machine Learning Workshops



Boss of Machine Learning (Coming Soon)

Introductory → **Advanced**

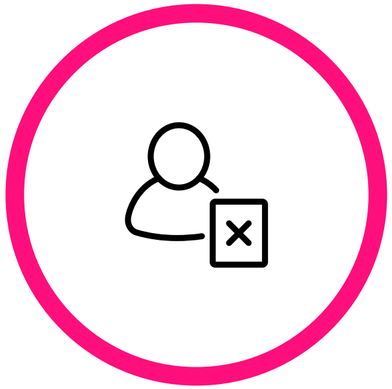
Legend

Security | IT Ops | Business | All

Objective for Today

An Understanding of

User Access Anomalies



Insider Threat

Anomalous Login Quantities

IT Operations

Forecast CPU Utilisation

Infrastructure

Outliers in Utilisation Telemetry

All

REGISTRATION 5 MINS

Enroll in Today's Workshop

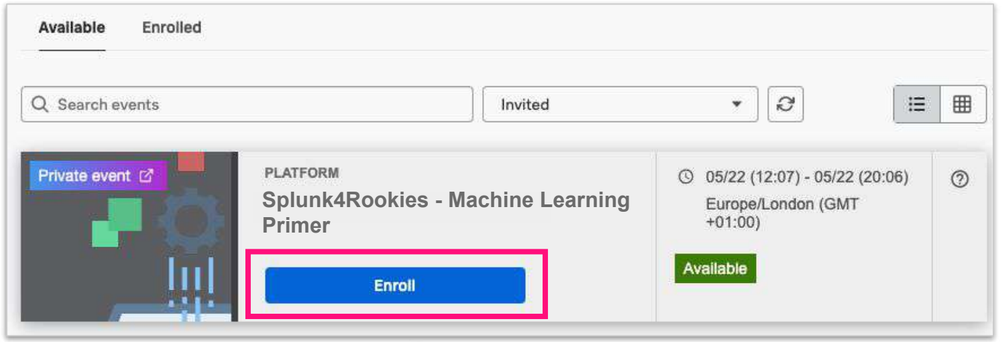
Tasks

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/S4RML-Primer-Attendee

Goal



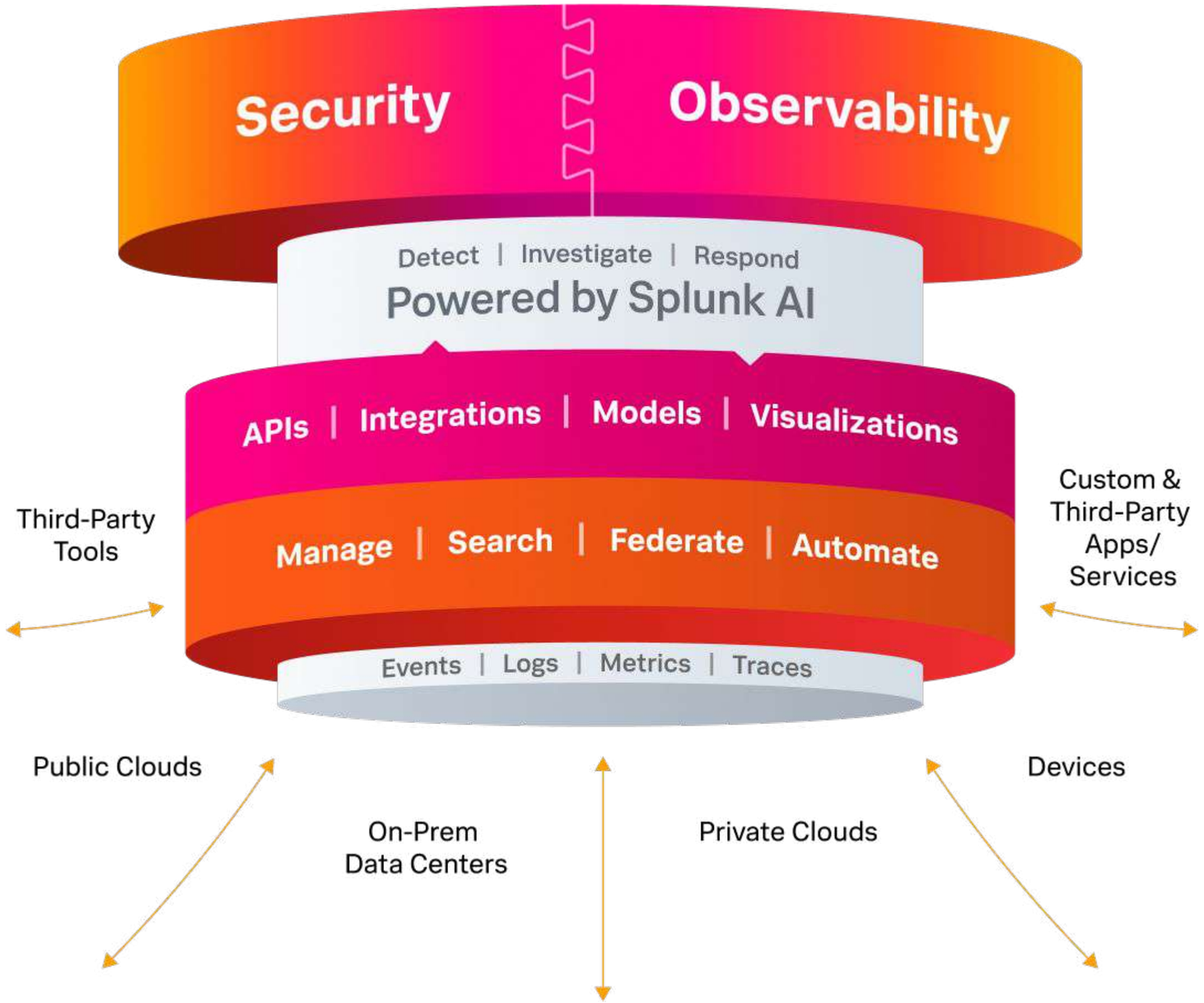
Enroll in today's event

What is Splunk?

Our product vision.

To provide visibility and insights across an enterprise's **entire digital footprint**, powering actions that improve security, reliability and innovation velocity

The Unified Security and Observability Platform



SECURITY

Power the SOC of the future.

Strengthen digital resilience by modernizing your SOC with unified threat detection, investigation and response.

5x
faster response to threats

70%
time reduction researching security events

80%
potential reduction in alert volumes

Data optimization

Security monitoring

Risk-based alerting

Anomaly detection

Automation & orchestration

Automate complete TDIR life cycle

OBSERVABILITY

Deliver superior digital services.

Find and fix problems faster, improve reliability, and build exceptional customer experiences.

97%
reduction in alert noise

83%
reduction in mean time to resolve (MTTR)

96%
faster application development, increasing developer productivity

Troubleshooting mission-critical apps & infrastructure

Optimize cloud monitoring

Analyze IT service health

Understand impact of change

Debug problems in microservices

Enable self-service observability

PLATFORM

Unified platform to maximize data value and solve limitless use cases.

Monitor, investigate and respond rapidly at scale with comprehensive visibility and shared tooling.

3K+
apps & add-ons on Splunkbase

1K+
purpose built data source integrations

8B
monthly searches

Flexible deployment options

End-to-end data management

Scalable index and storage

Powerful search and visualization

Expanded view with federated analytics

Increased efficiency with AI and ML

AI and ML capabilities across our portfolio accelerate detection, investigation, and response.

Our approach

Domain and Splunk specific

Human-in-the-loop and trusted

Open and extensible

What we offer

Generative AI

Make sense of the signal to improve user productivity and outcomes

Foundational AI

Find the signal from the noise in vast amounts of data

Cisco + Splunk
power and protect the AI revolution.

Infrastructure
for AI

Networking and compute solutions for training AI models at scale.

Data
for AI

Massive breadth and depth of data across domains is the foundation for AI models.

Observability
for AI

Observability supports trustworthy, performant, and reliable AI deployment.

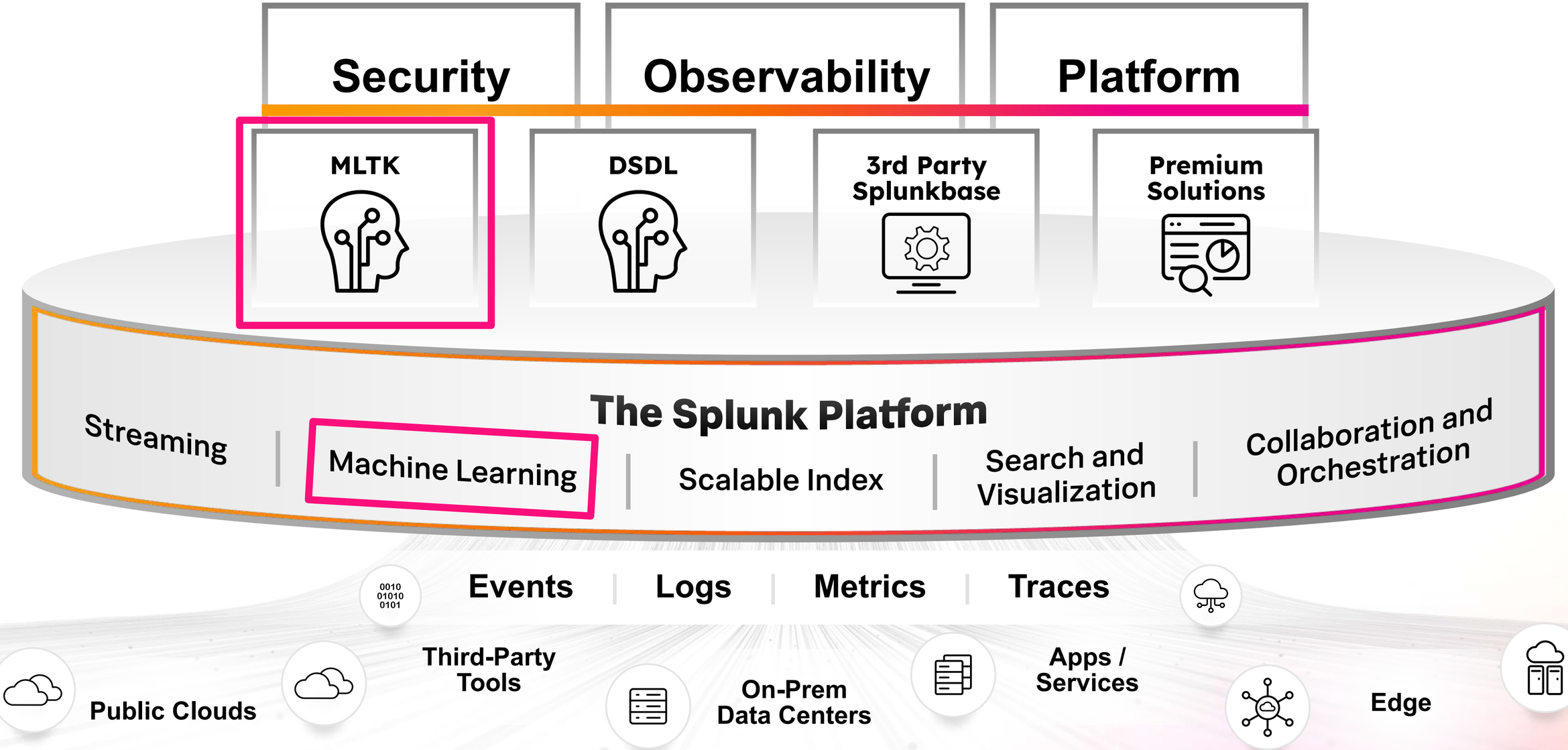
AI
for Security

AI solutions improve efficiency, efficacy, and economics of defending against security threats.

Security
for AI

Cisco's Identity Intelligence and User Protection and Splunk's analytics help protect enterprises in their use of AI from within.

The Unified Security and Observability Platform

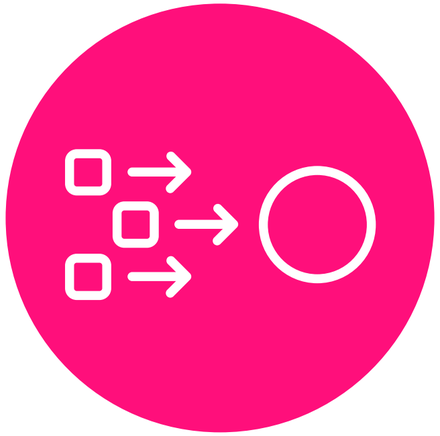


Machine Learning

The Truth

Machine Learning

The capability of systems to acquire their own knowledge, by extracting patterns

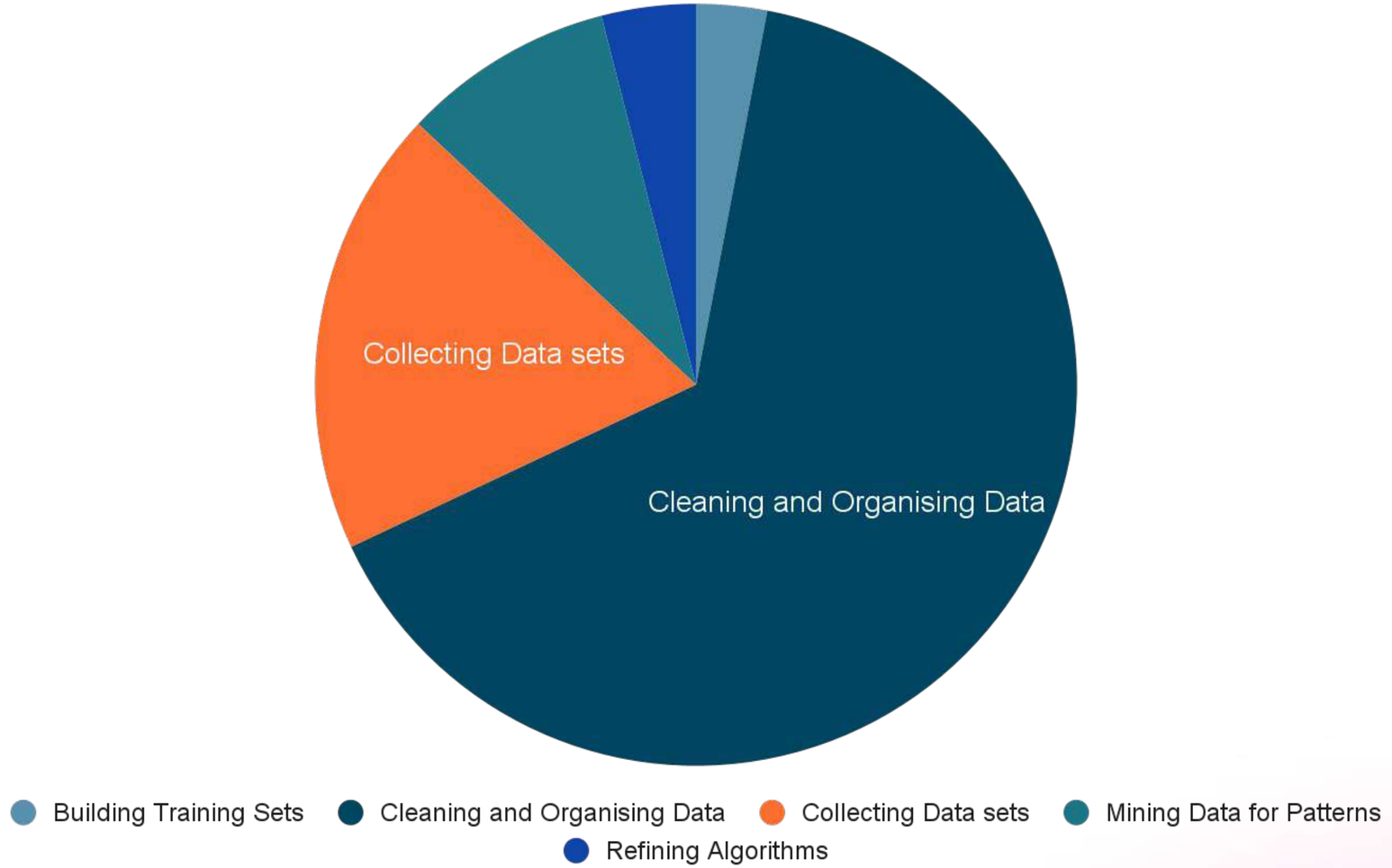


Use complex statistical or probabilistic models to identify patterns in information

Catalog the patterns and in some cases iterate them as new data is received

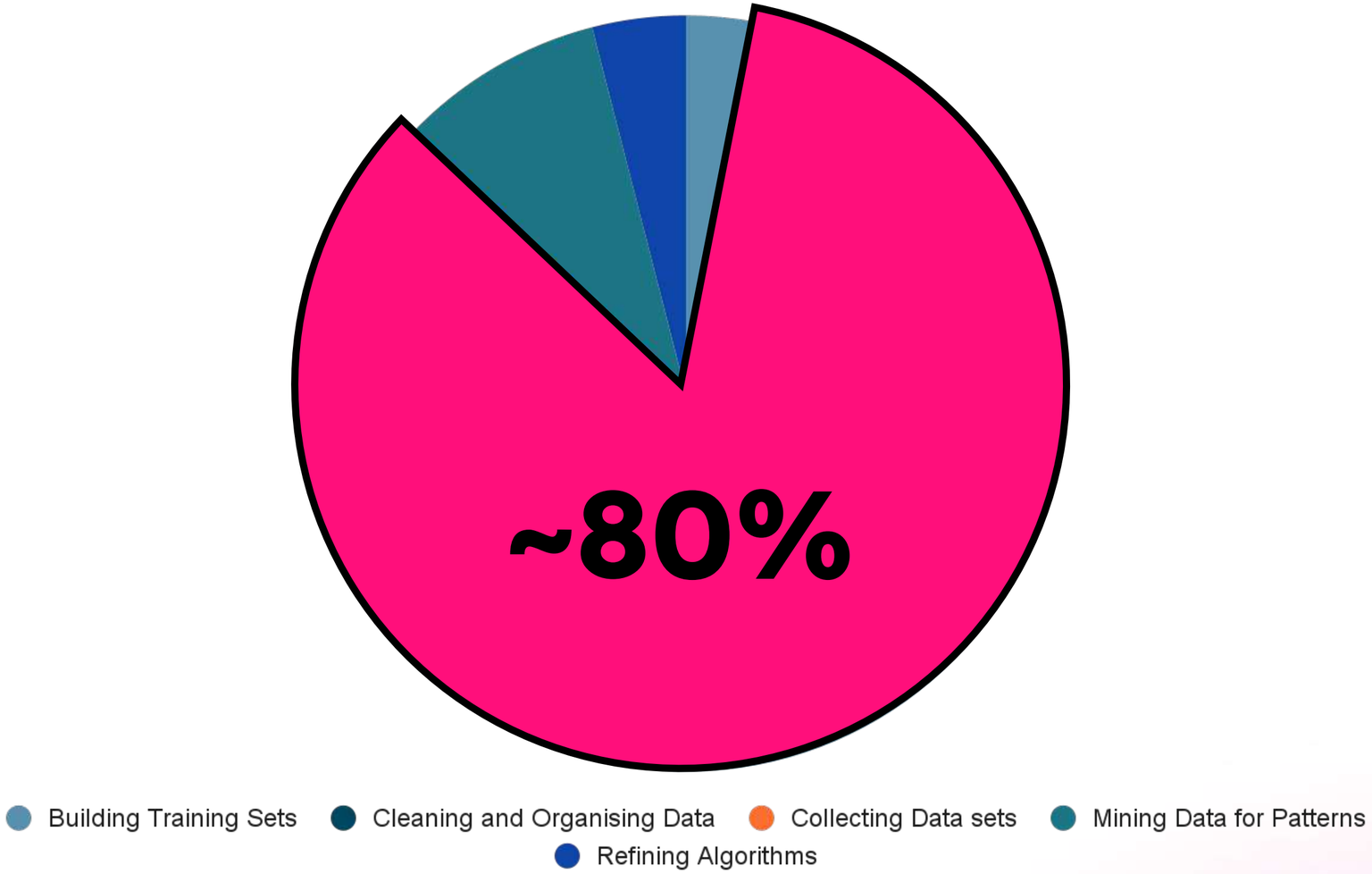
Use information from learnt patterns to understand and interpret new data or make predictions

What Data Scientists Really Do



What Data Scientists Really Do

Data Preparation accounts for about 80% of the work of data scientists



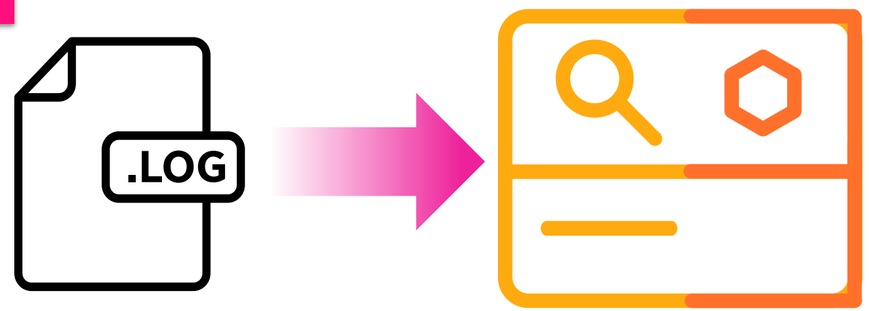
Cleaning Big Data, the Most Time-Consuming, Least Enjoyable Data Science Task

Forbes Survey

March 23

Today’s Environment

BOSS of the SOC data…



Indexer & Search Head combined in a single instance

Hands-On

One Last Thing...

The following tools & datasets have been provided in your Splunk instance for this workshop:

Machine Learning Toolkit (MLTK)

Python Scientific Computing (PSC)

Splunk App for Anomaly Detection

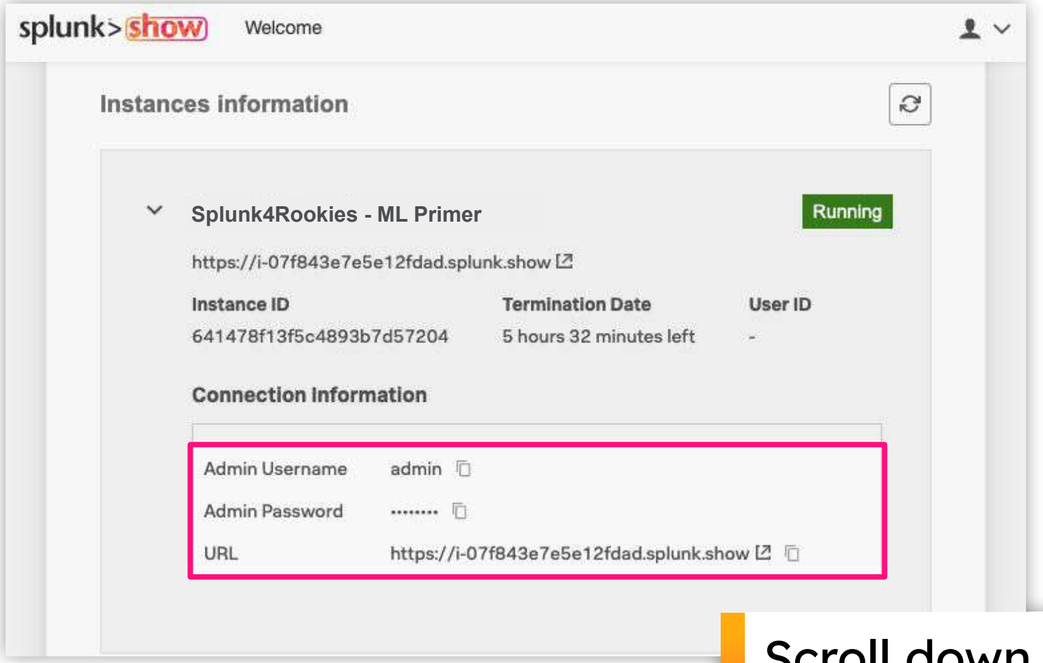
BOTS v2 Dataset (Full)

Splunk Add-on for Microsoft Windows

If you would like to run through this workshop in your own Splunk environment, please ensure you have the above listed apps and add-ons installed in your Splunk instance.

Login to Splunk

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

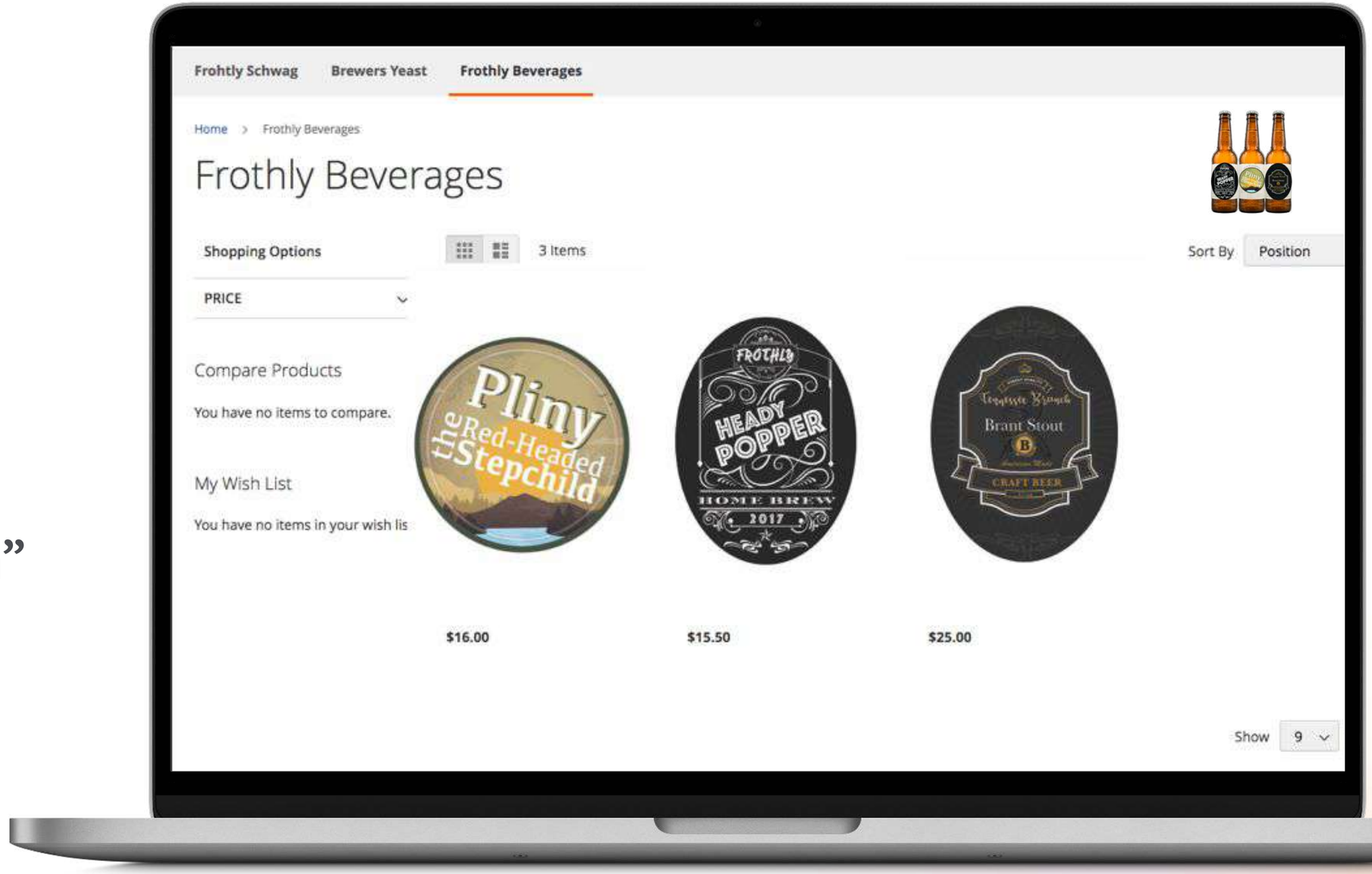


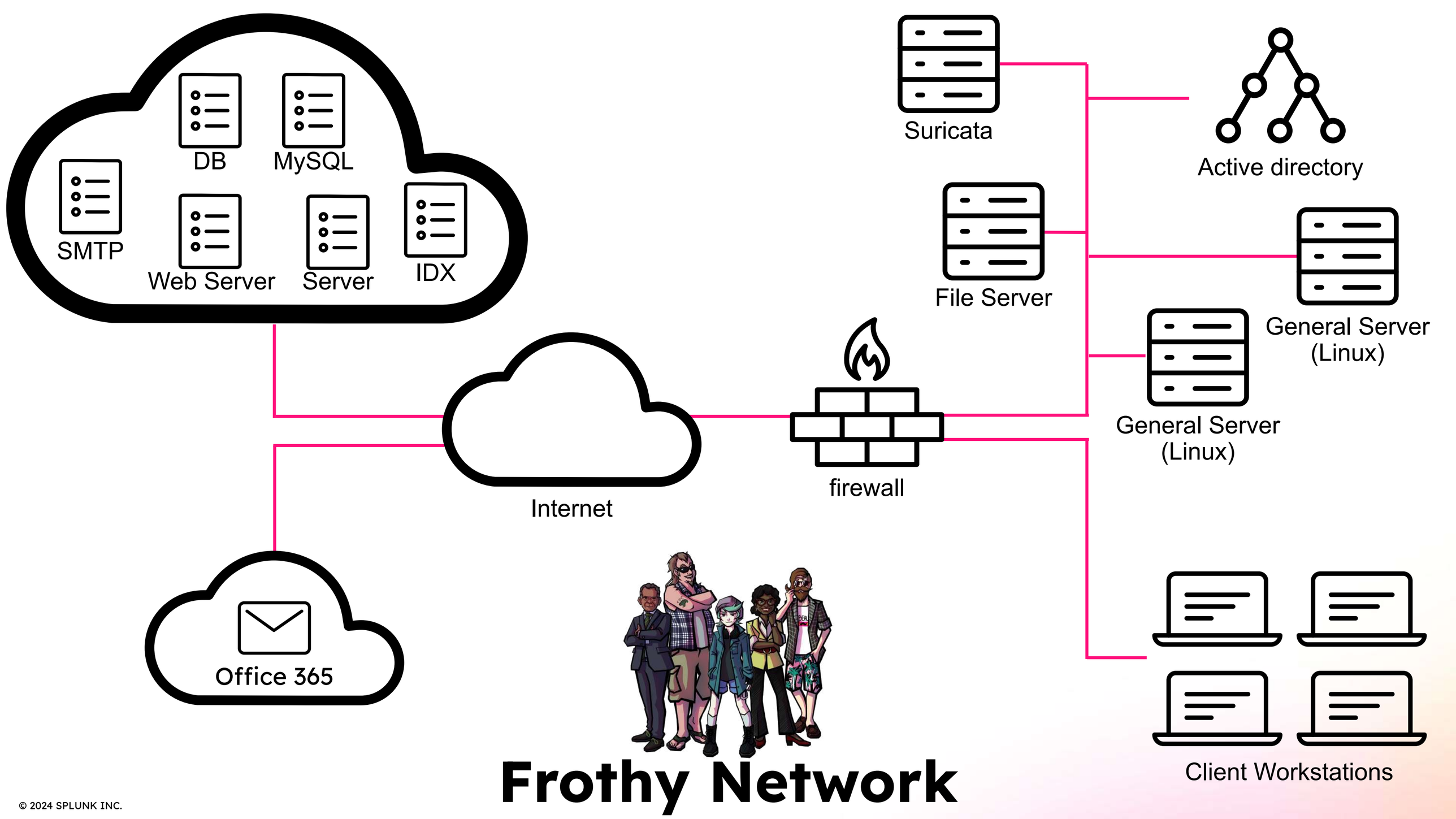
Log in to your Splunk instance

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

A Buttercup Company

Not just “a neigh” Old Beer





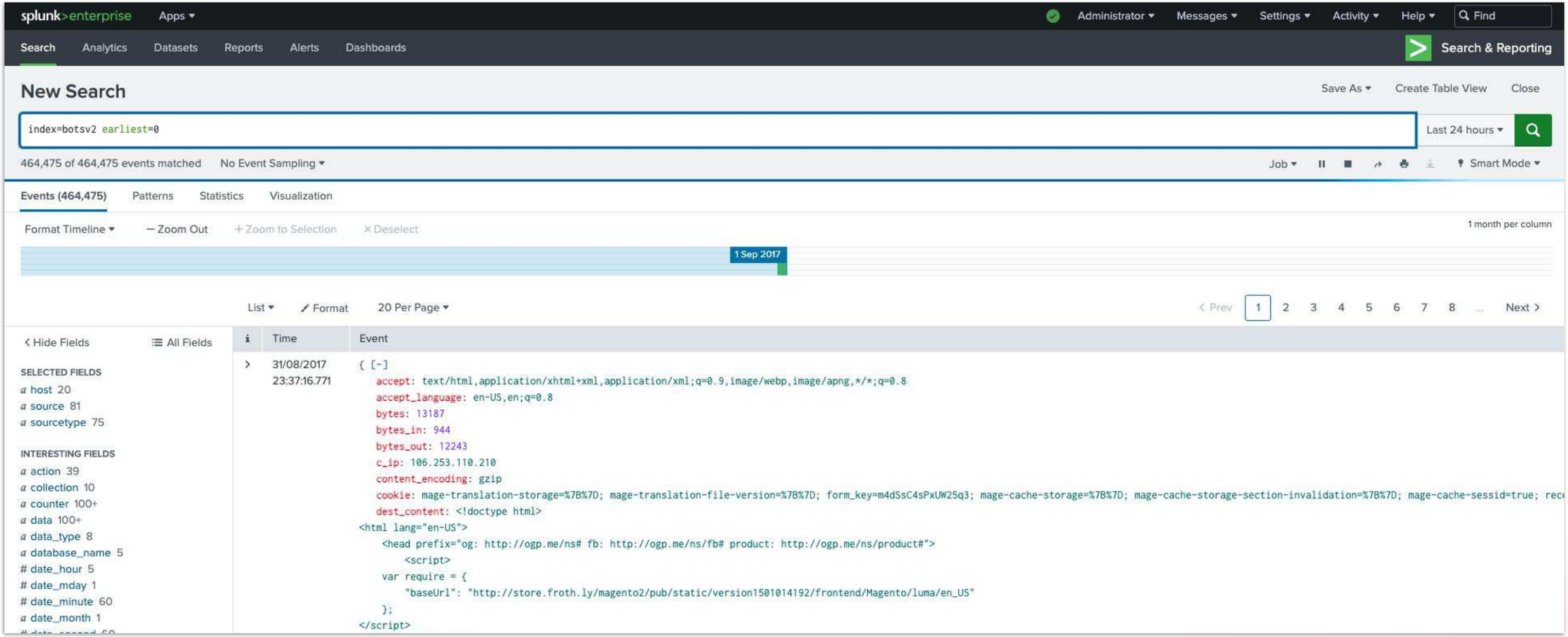
Frothy Network

Explore

Understanding the Data and Navigating Splunk

The Data

Search 0-1



Scenario 1

Detecting User Access Anomalies

Detecting User Access Anomalies

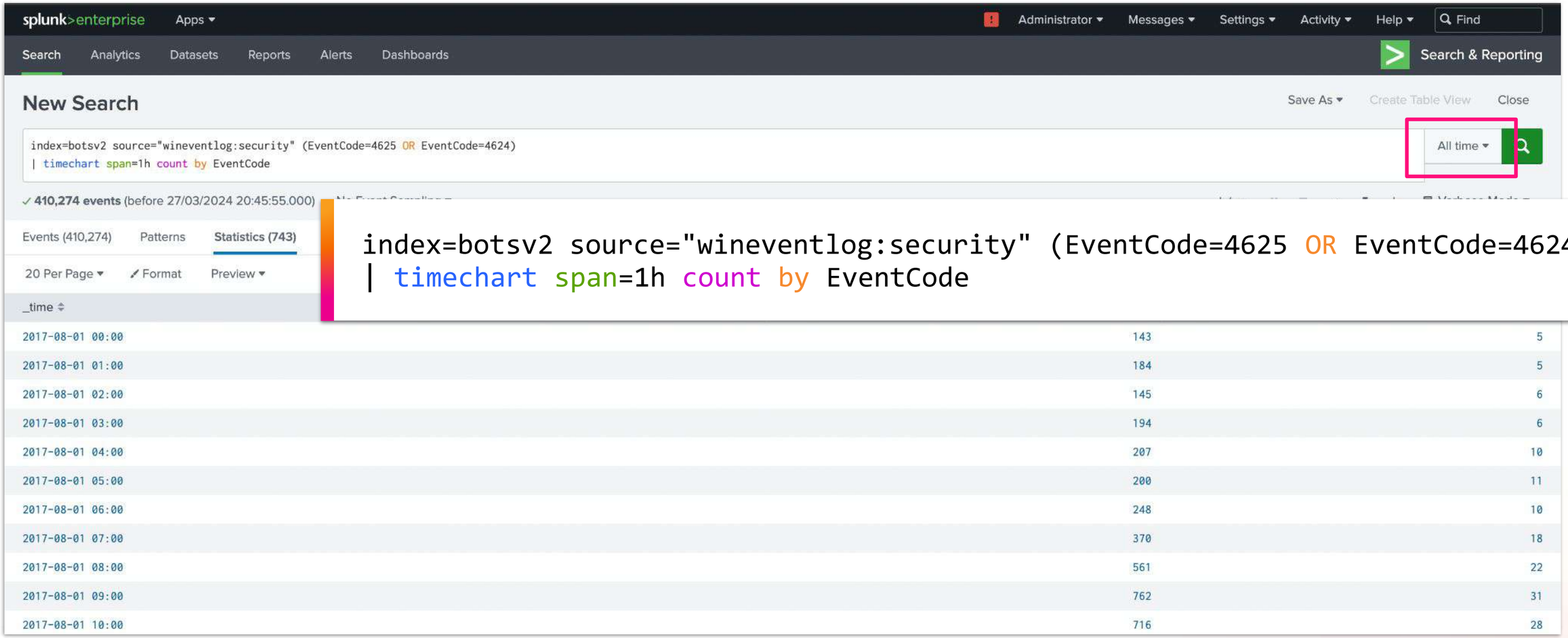
You’re a SOC analyst at Frothly, who’s just been notified that some accounts in the company might have been hacked.

You’re tasked with tracing back to where this hack may have originated, and identifying the potentially compromised accounts in the system.

To do this, you need to analyse Windows Security Event logs that contain records of successful and unsuccessful login/logout activity, as well as other security-related events

Authentication Events

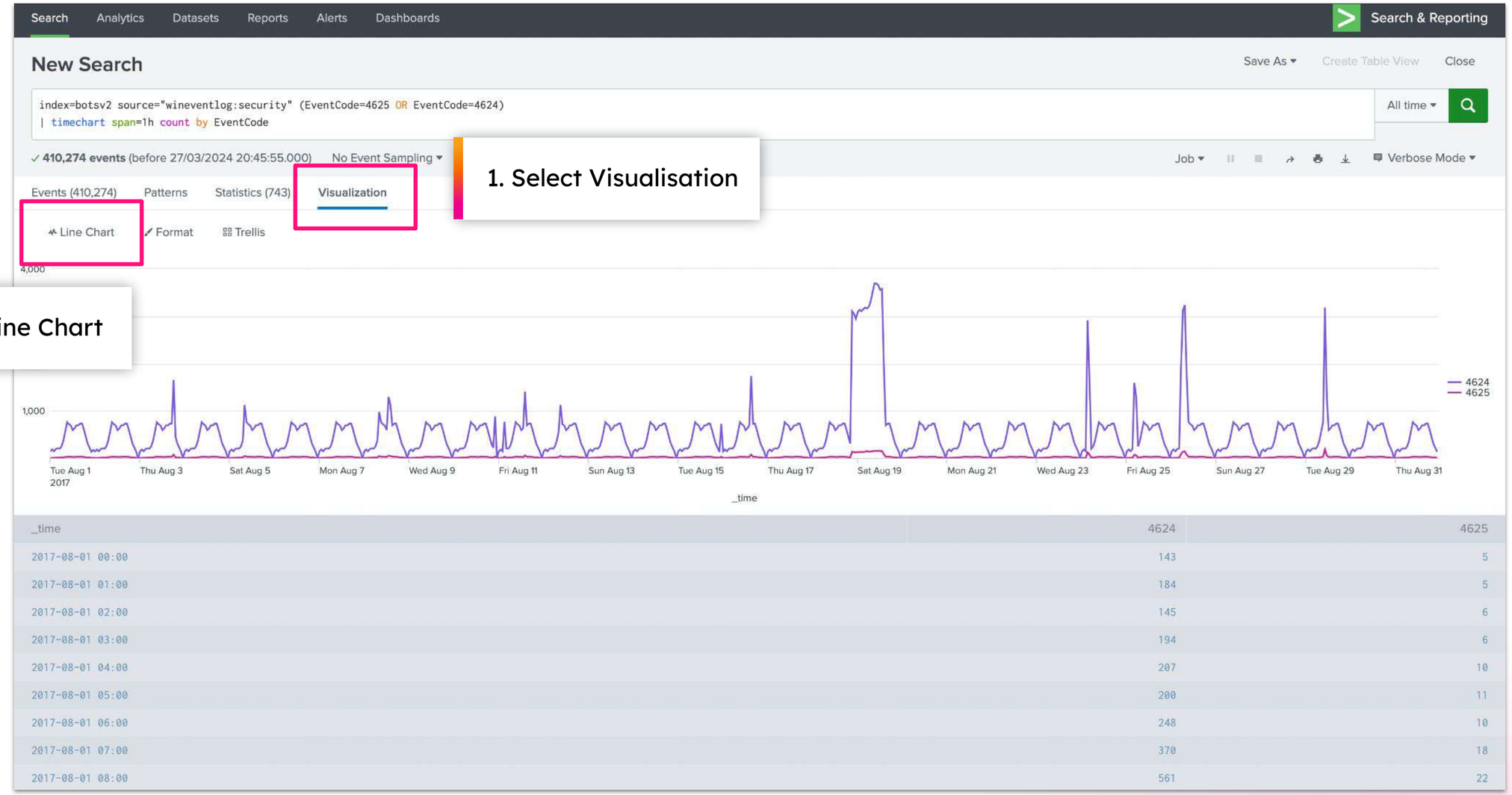
Search 1-1




```
index=botsv2 source="wineventlog:security" (EventCode=4625 OR EventCode=4624)
| timechart span=1h count by EventCode
```

Authentication Events

Search 1-2

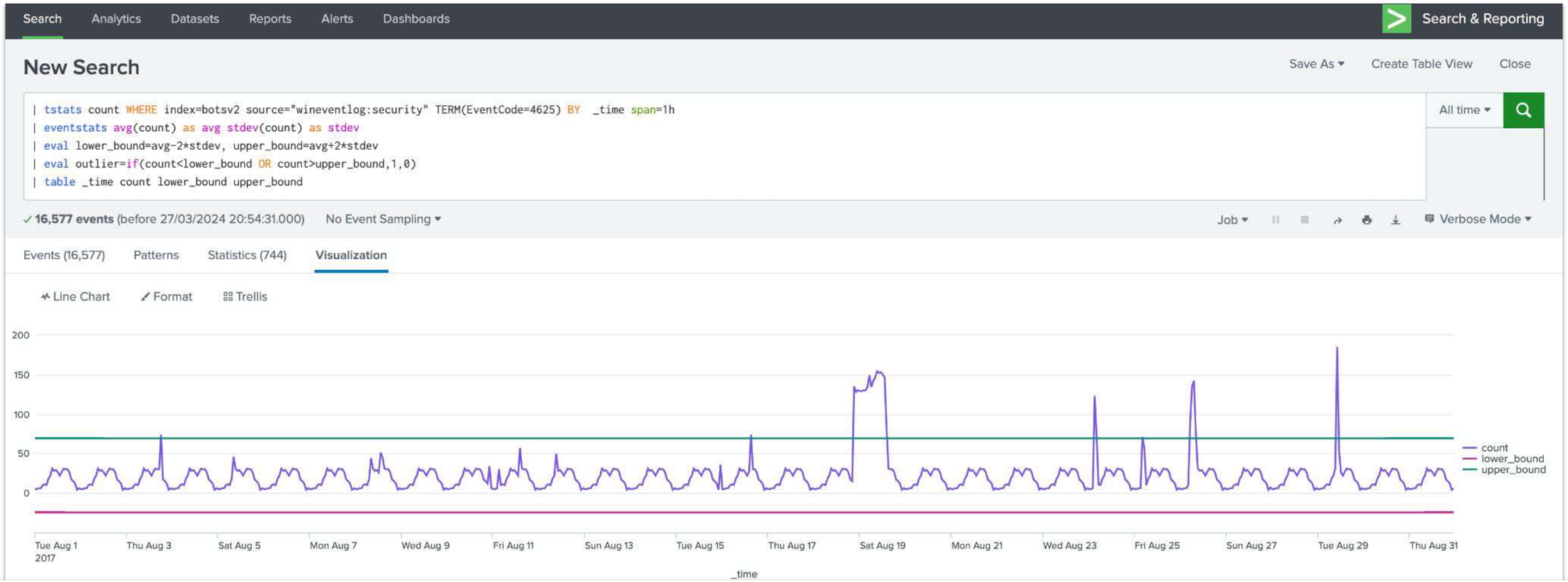


_time	4624	4625
2017-08-01 00:00	143	5
2017-08-01 01:00	184	5
2017-08-01 02:00	145	6
2017-08-01 03:00	194	6
2017-08-01 04:00	207	10
2017-08-01 05:00	200	11
2017-08-01 06:00	248	10
2017-08-01 07:00	370	18
2017-08-01 08:00	561	22

```
| tstats
```

Authentication Bounds

Search 1-3



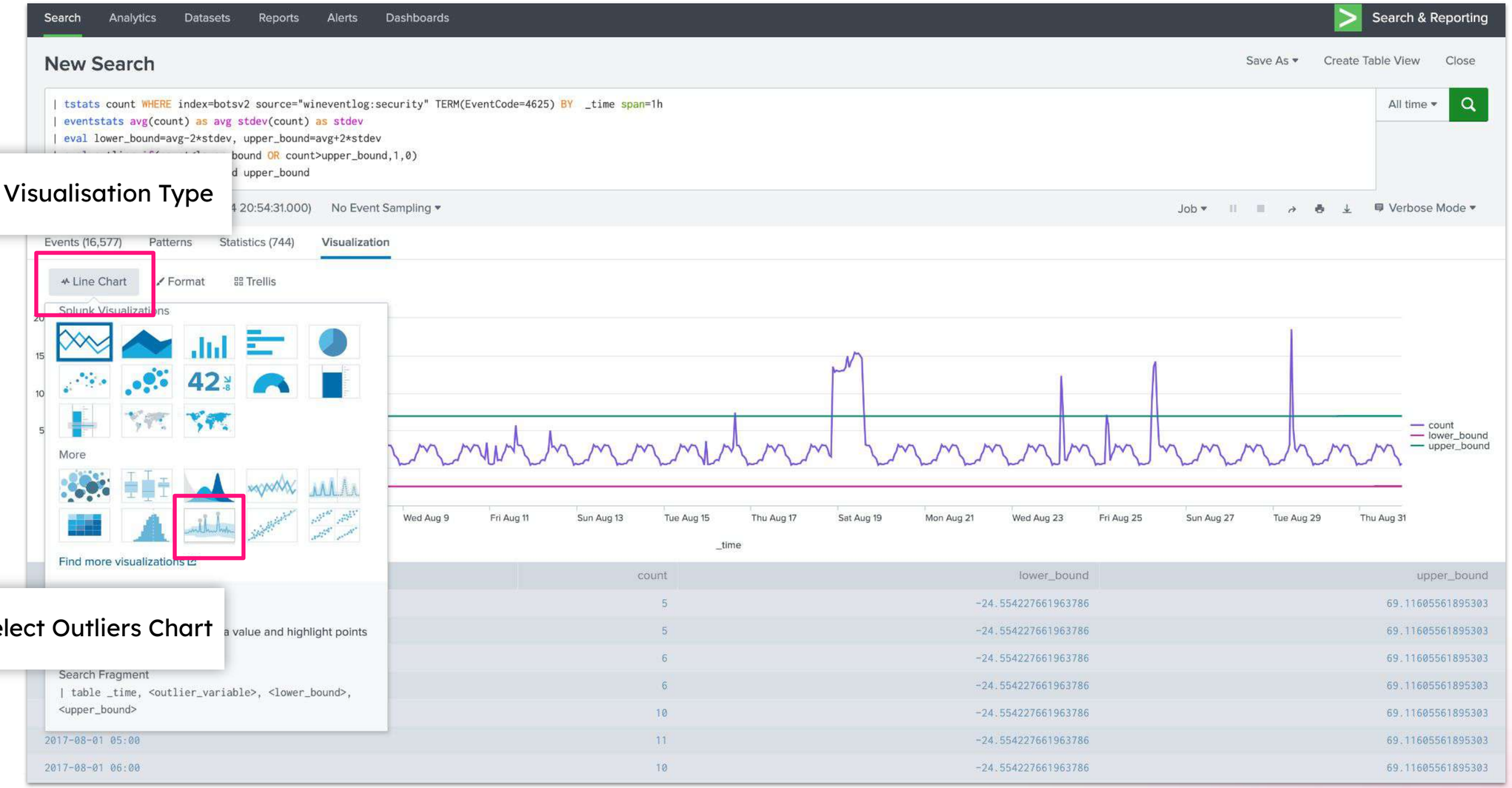

```
| tstats count WHERE index=botsv2 source="wineventlog:security" TERM(EventCode=4625) BY _time span=1h
| eventstats avg(count) as avg stdev(count) as stdev
| eval lower_bound=avg-2*stdev, upper_bound=avg+2*stdev
| eval outlier=if(count<lower_bound OR count>upper_bound,1,0)
| table _time count lower_bound upper_bound
```

Authentication Bounds

Search 1-3

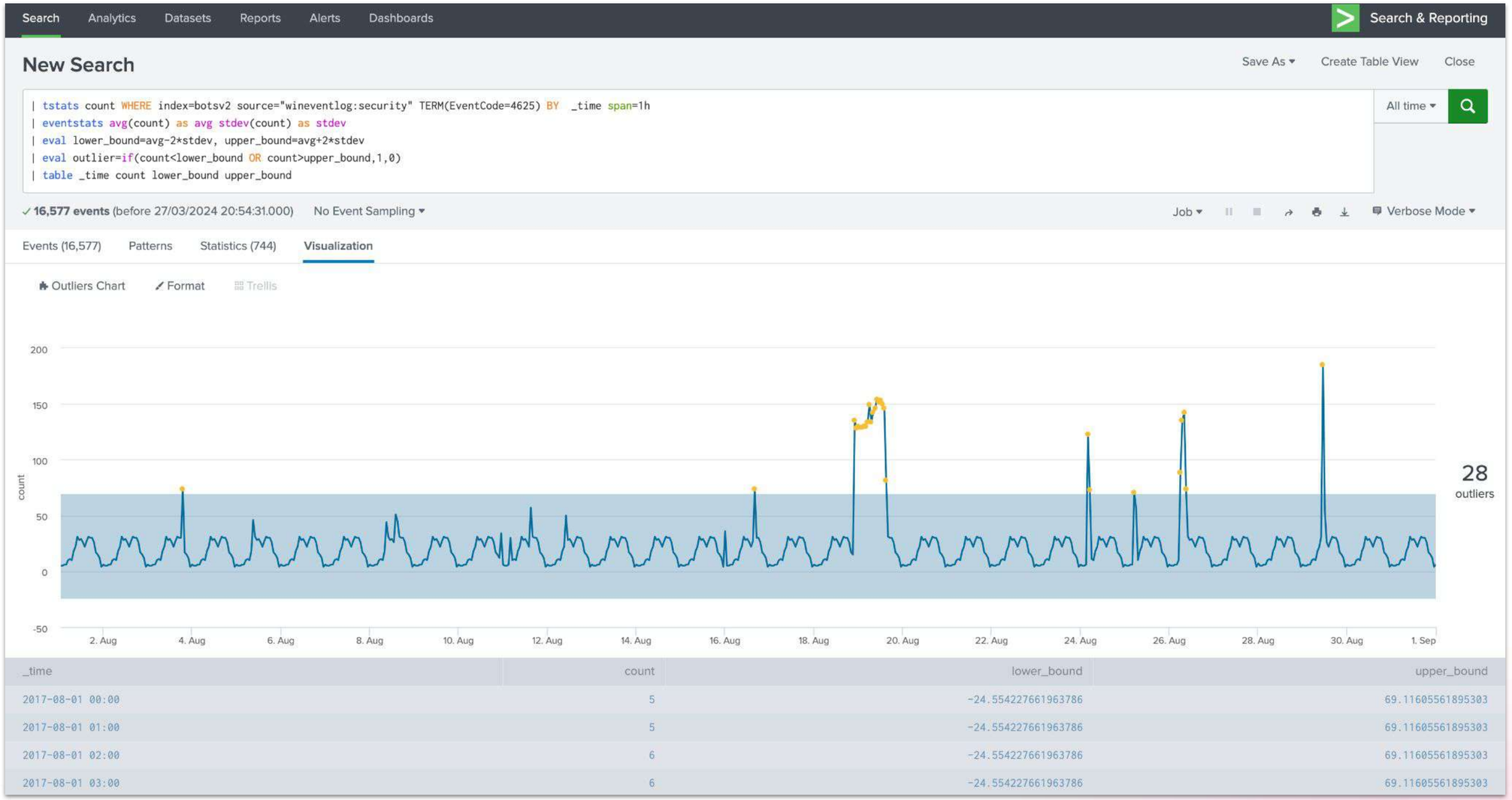
1. Select Visualisation Type

2. Select Outliers Chart



Authentication Outliers

Search 1-3



Authentication Outliers

Search 1-4


```
| tstats count WHERE index=botsv2 source="wineventlog:security" TERM(EventCode=4625) BY _time span=1h
| eval HourOfDay=strftime(_time, "%H")
| eventstats avg(count) as avg stdev(count) as stdev by HourOfDay
| eval lower_bound=avg-2*stdev, upper_bound=avg+2*stdev
| eval outlier=if(count<lower_bound OR count>upper_bound,1,0)
| table _time count lower_bound upper_bound
```

Fit Command

Train a model from search results

```
... | fit <ALGORITHM> <TARGET> from <VARIABLES ...>
        <PARAMETERS> into <MODEL>
```

Examples:

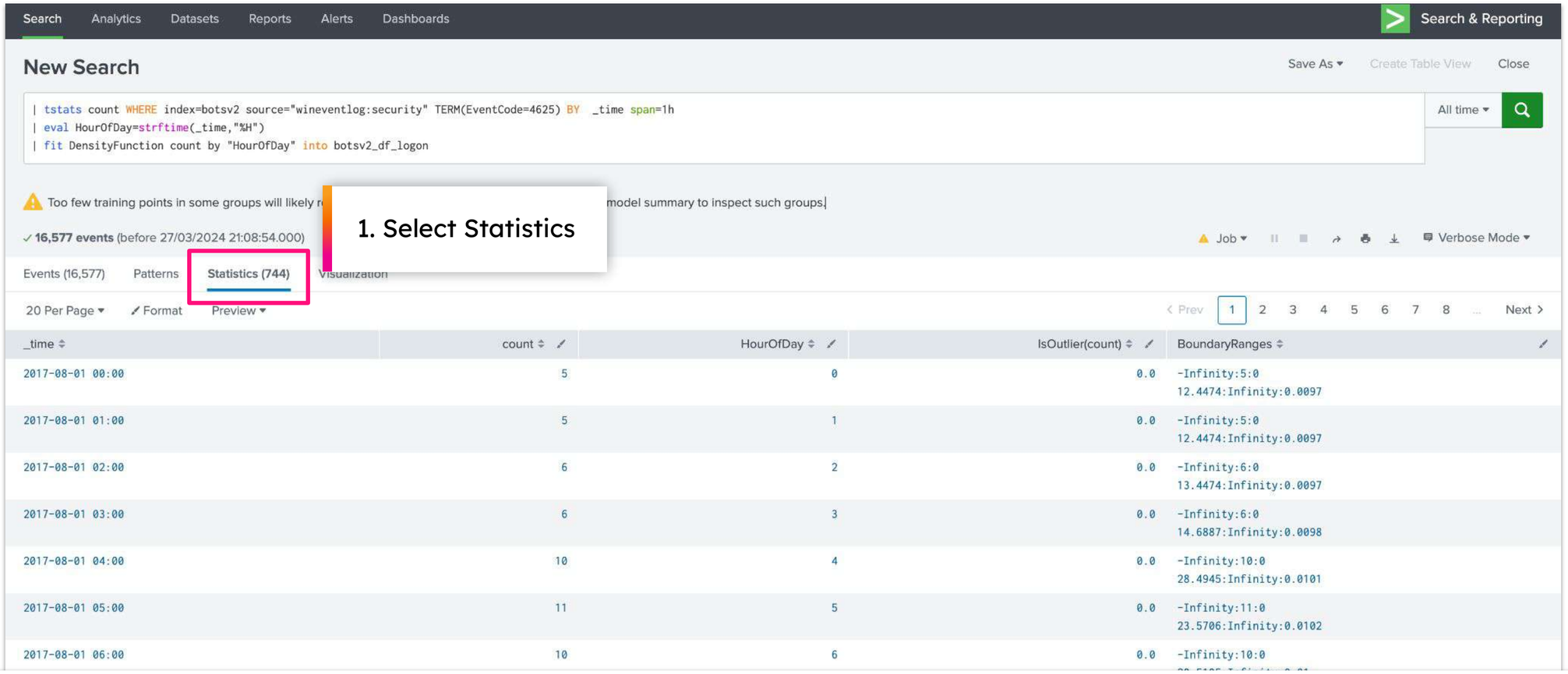
```
... | fit LinearRegression system_temp from cpu_load fan_rpm
        into temp_model

... | fit KMeans k=10 downloads purchases posts days_active visits_per_day
        into user_behavior_clusters

... | fit LinearRegression petal_length from species
```

Authentication Fit

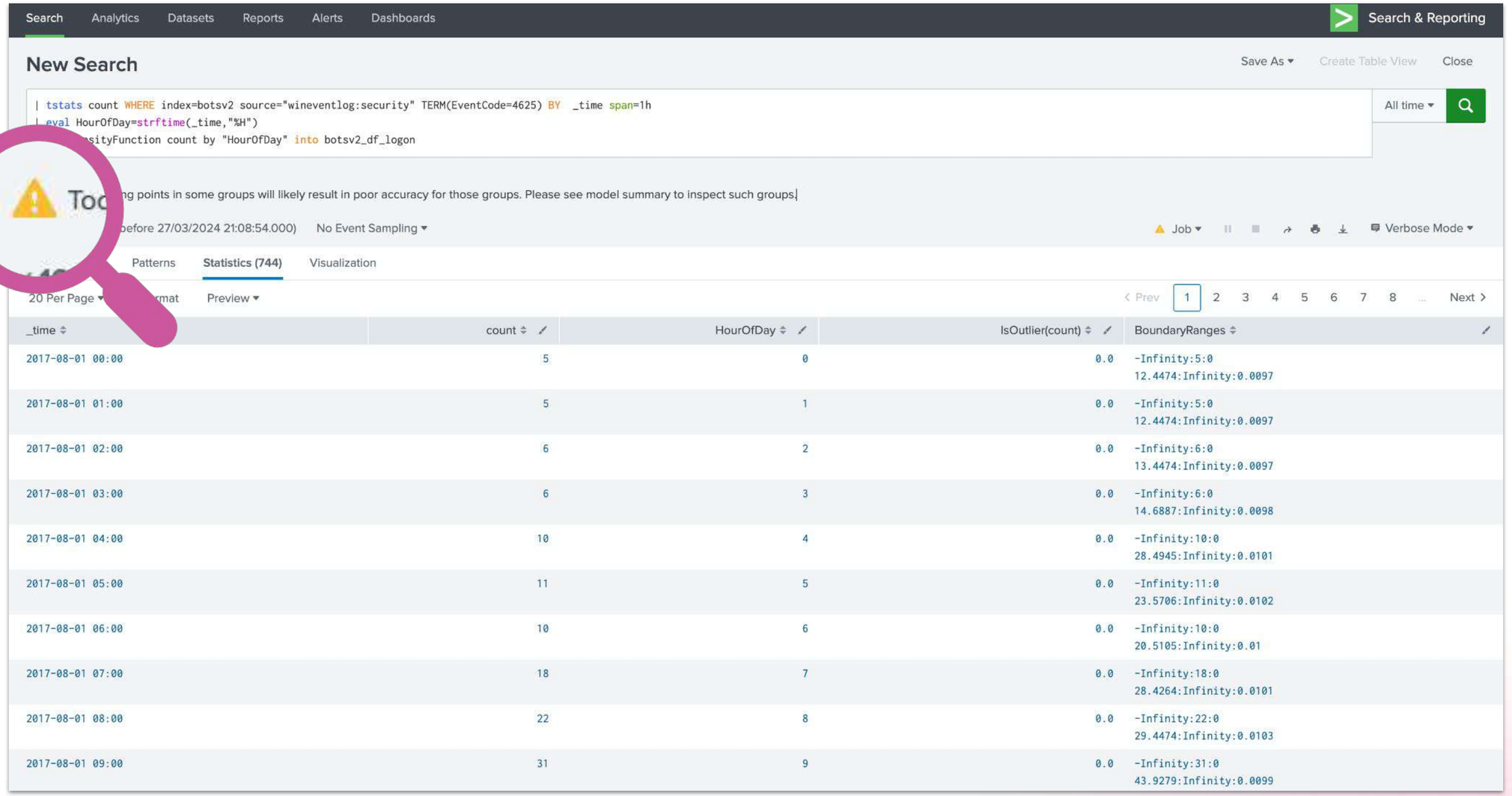
Search 1-5




```
| tstats count WHERE index=botsv2 source="wineventlog:security" TERM(EventCode=4625) BY _time span=1h
| eval HourOfDay=strftime(_time,"%H")
| fit DensityFunction count by "HourOfDay" into botsv2_df_logon
```

Authentication Fit

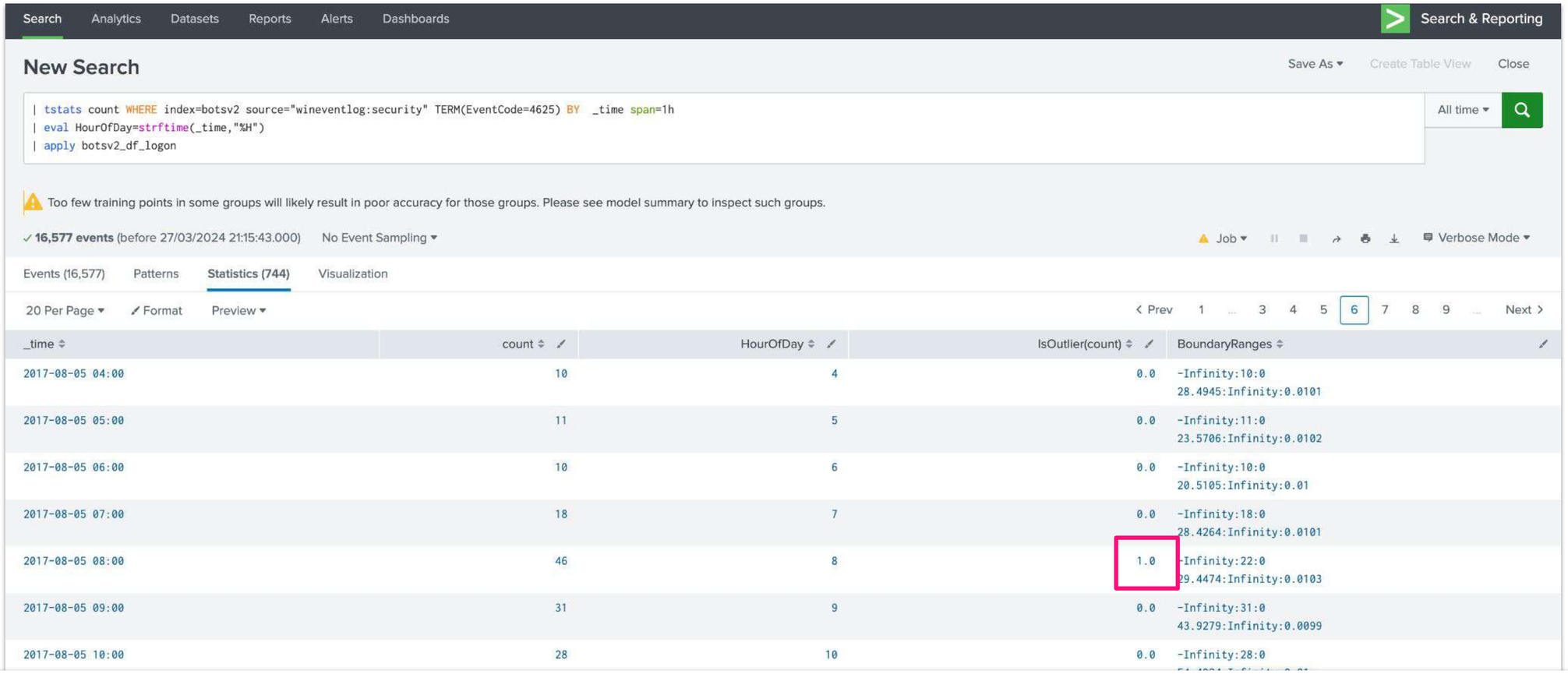
Search 1-5



_time	count	HourOfDay	IsOutlier(count)	BoundaryRanges
2017-08-01 00:00	5	0	0.0	-Infinity:5:0 12.4474:Infinity:0.0097
2017-08-01 01:00	5	1	0.0	-Infinity:5:0 12.4474:Infinity:0.0097
2017-08-01 02:00	6	2	0.0	-Infinity:6:0 13.4474:Infinity:0.0097
2017-08-01 03:00	6	3	0.0	-Infinity:6:0 14.6887:Infinity:0.0098
2017-08-01 04:00	10	4	0.0	-Infinity:10:0 28.4945:Infinity:0.0101
2017-08-01 05:00	11	5	0.0	-Infinity:11:0 23.5706:Infinity:0.0102
2017-08-01 06:00	10	6	0.0	-Infinity:10:0 20.5105:Infinity:0.01
2017-08-01 07:00	18	7	0.0	-Infinity:18:0 28.4264:Infinity:0.0101
2017-08-01 08:00	22	8	0.0	-Infinity:22:0 29.4474:Infinity:0.0103
2017-08-01 09:00	31	9	0.0	-Infinity:31:0 43.9279:Infinity:0.0099

Authentication Apply

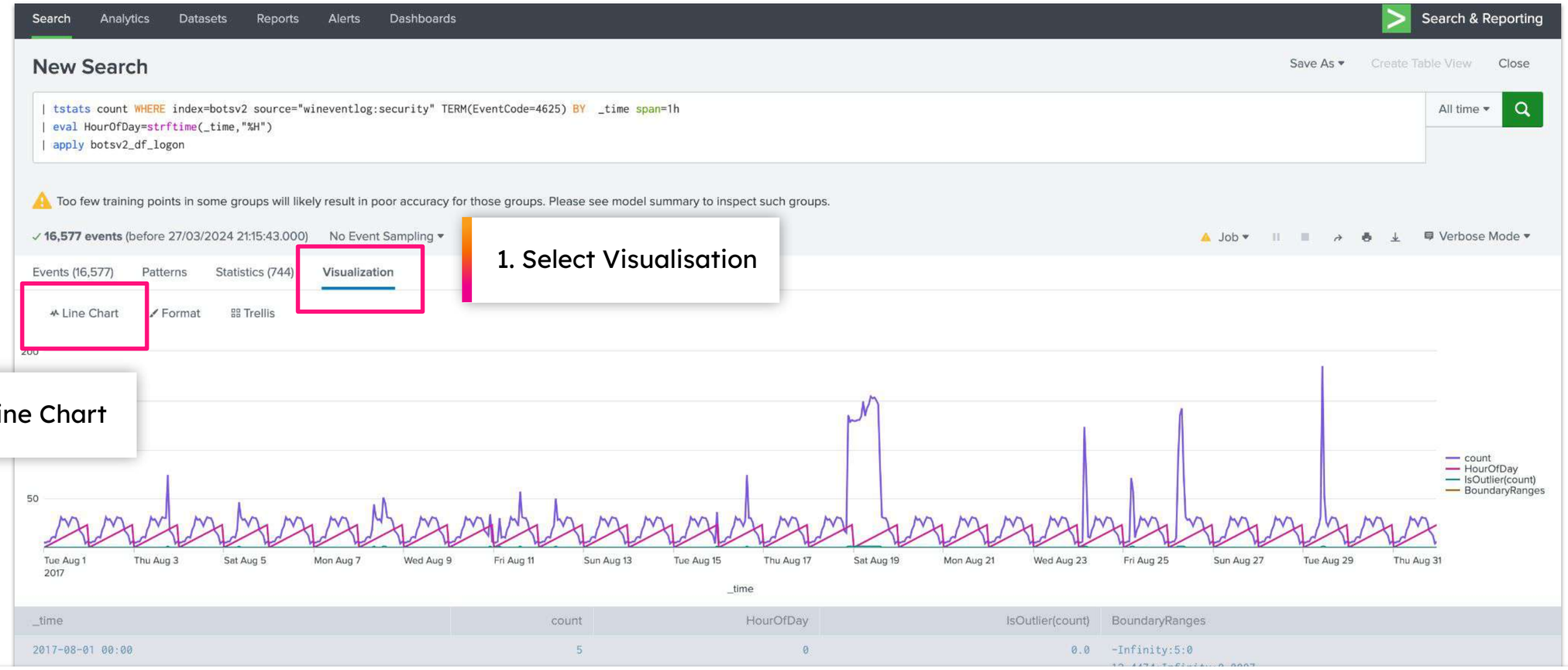
Search 1-6




```
| tstats count WHERE index=botsv2 source="wineventlog:security" TERM(EventCode=4625) BY _time span=1h
| eval HourOfDay=strftime(_time,"%H")
| apply botsv2_df_logon
```

Authentication Apply

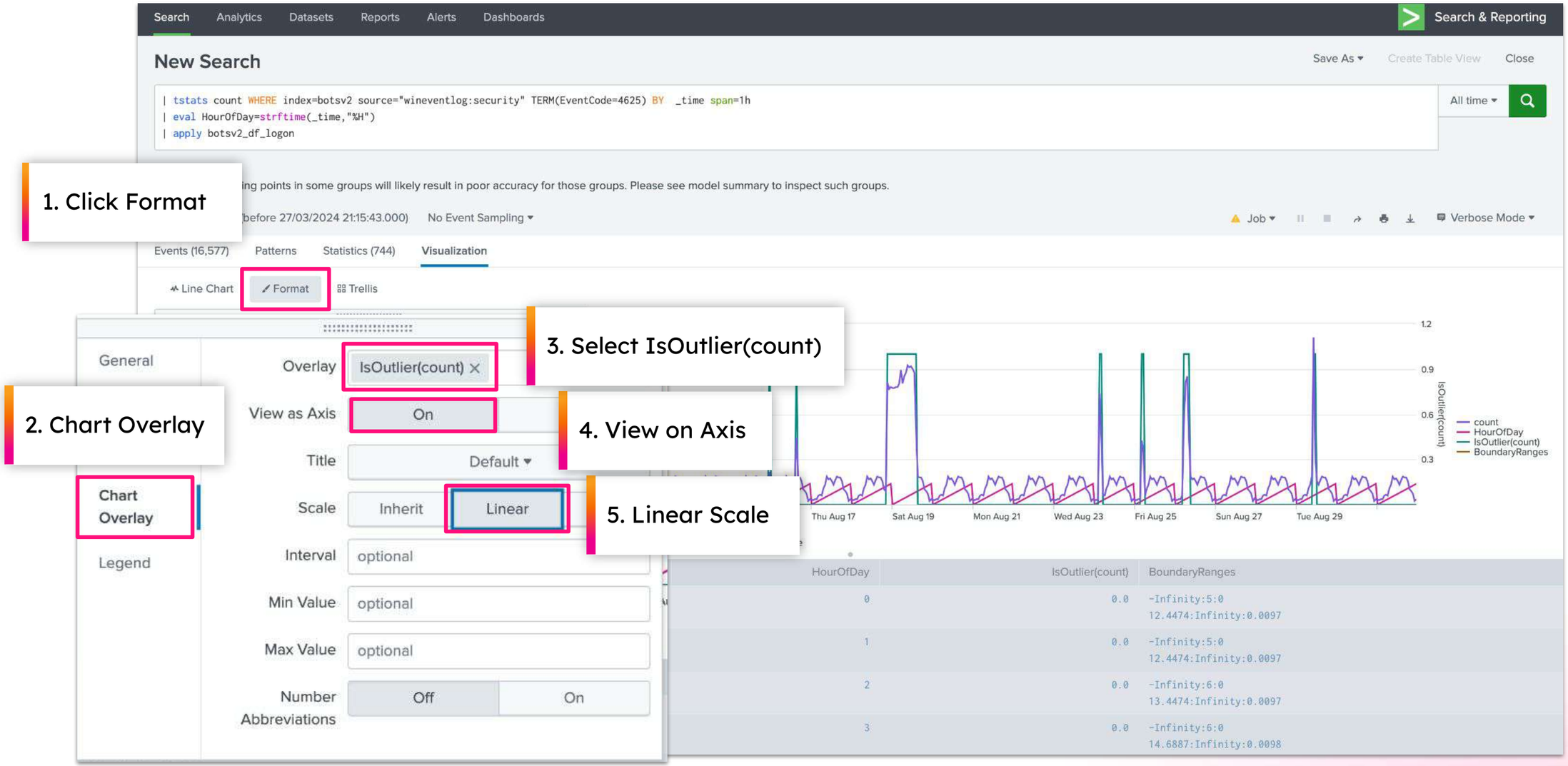
Search 1-6




```
| tstats count WHERE index=botsv2 source="wineventlog:security" TERM(EventCode=4625) BY _time span=1h
| eval HourOfDay=strftime(_time,"%H")
| apply botsv2_df_logon
```

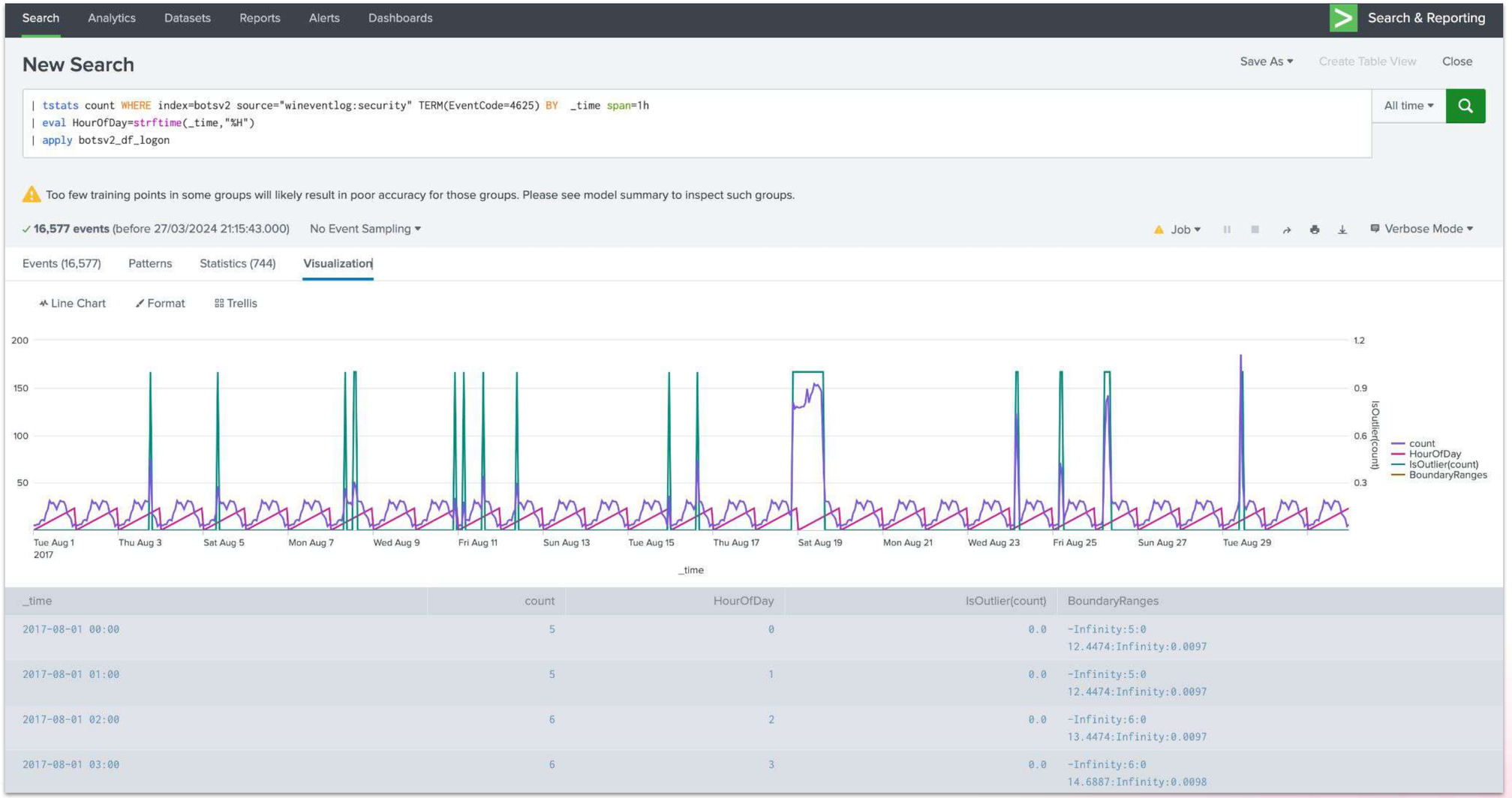
Authentication Apply

Search 1-6



Authentication Apply

Search 1-6



_time	count	HourOfDay	IsOutlier(count)	BoundaryRanges
2017-08-01 00:00	5	0	0.0	-Infinity:5:0 12.4474:Infinity:0.0097
2017-08-01 01:00	5	1	0.0	-Infinity:5:0 12.4474:Infinity:0.0097
2017-08-01 02:00	6	2	0.0	-Infinity:6:0 13.4474:Infinity:0.0097
2017-08-01 03:00	6	3	0.0	-Infinity:6:0 14.6887:Infinity:0.0098

Search Breakdown

Bookmark

Splunk search	Description
index=botsv2 source="wineventlog:security" (EventCode=4625 OR EventCode=4624)	Search for windows event logs with failed log-ins from accounts (EventCode = 4625) and successful logins (EventCode = 4624).
… | timechart span=1h count by EventCode	Time chart is statistical aggregation applied to a field to produce a chart, with time used as the X-axis and the specified field as the Y-axis. In this case, that field is calculated as the total count of event codes for each hour
… | eventstats avg(count) as avg stdev(count) as stdev	Calculate the average and standard deviation across all events, in this case with EventCode 4625
… | eval lower_bound=avg-2*stdev, upper_bound=avg+2*stdev	The average and standard deviation are used with the eval command to calculate the lower and upper boundaries. A sensitivity is added into the calculation by multiplying the stdev by 2, as in any distribution, about 95% of values should be within 2 standard deviations of the mean.
… | eval outlier=if(count<lower_bound OR count>upper_bound,1,0)	The lower and upper bounds calculated earlier are used to identify the outliers
… | table _time count lower_bound upper_bound	Returns a table with fields time, count, lower bound, and upper bound
… | eval HourOfDay=strftime(_time,"%H")	Returns the hour from the _time field. strftime(_time,"%H") takes a UNIX time value and returns the time as a string in the specified format, in this case the hour.
… | fit DensityFunction count by "HourOfDay" into botsv2_df_logon	- Fit a density function model to the data - The into option lets the fit command know you want to save the model. Your model will now be saved as botsv2_df_logon *Note: Model names should not have spaces, and will be stored as a type of lookup*
… | apply botsv2_df_logons	Apply the saved model * The apply command can only be used when MLTK & PSC are installed

Scenario 2

Detecting Anomalies in User Login Quantity

Detecting Anomalies in User Login Quality

With the Splunk App for Anomaly Detection

You are an IT admin at Frothly, you are tasked with identifying and investigating any unusual user logins.

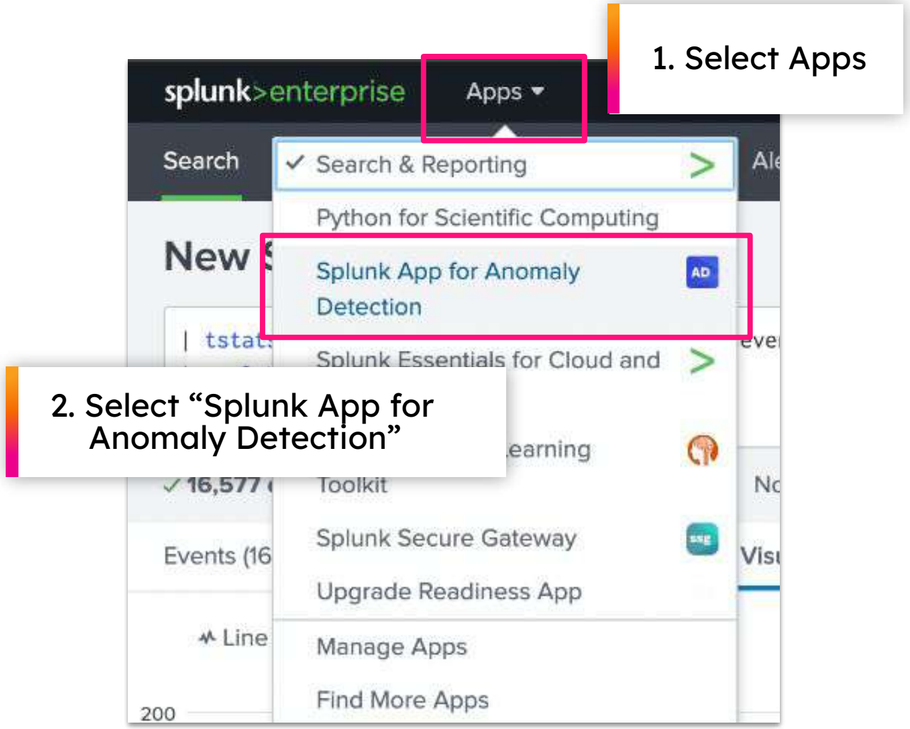
A significant variation in normal behavior could be due to a new system issue, errors in the IT infrastructure, or a security threat. T

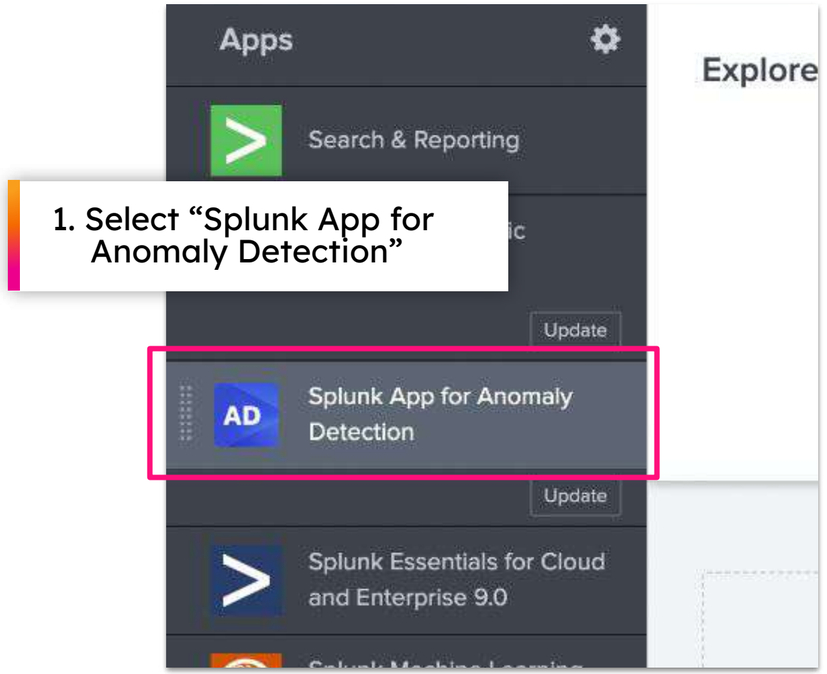
The previous IT admin happened to be proficient in SPL and familiar with foundational data science concepts. Unfortunately, you are less familiar with machine learning, but still want to use an ML workflow to complete your task.

Luckily for you, Splunk recently launched an assistive app that will take care of all of the heavy lifting of ML for you!

Search & Reporting

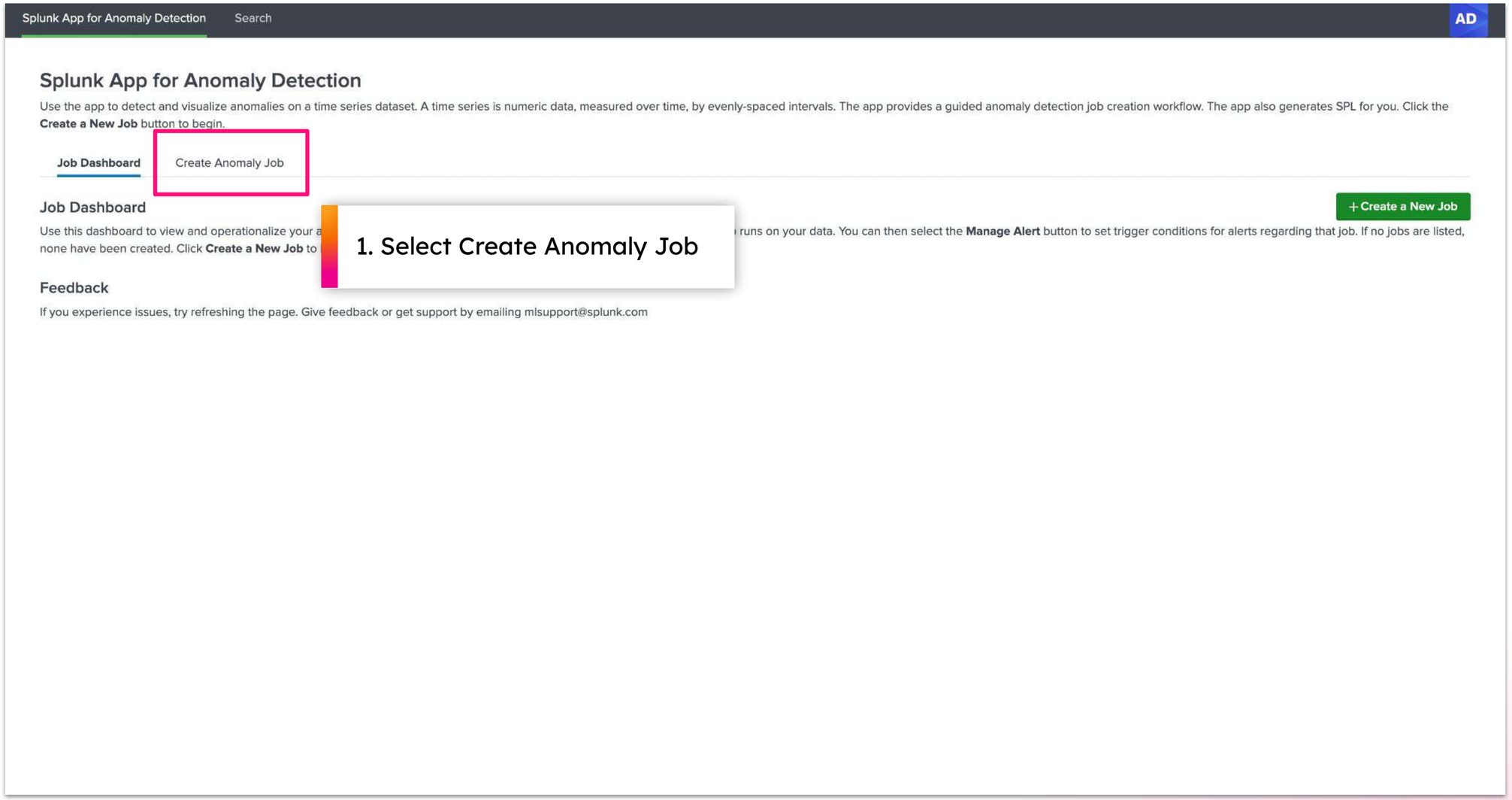
Navigation Options





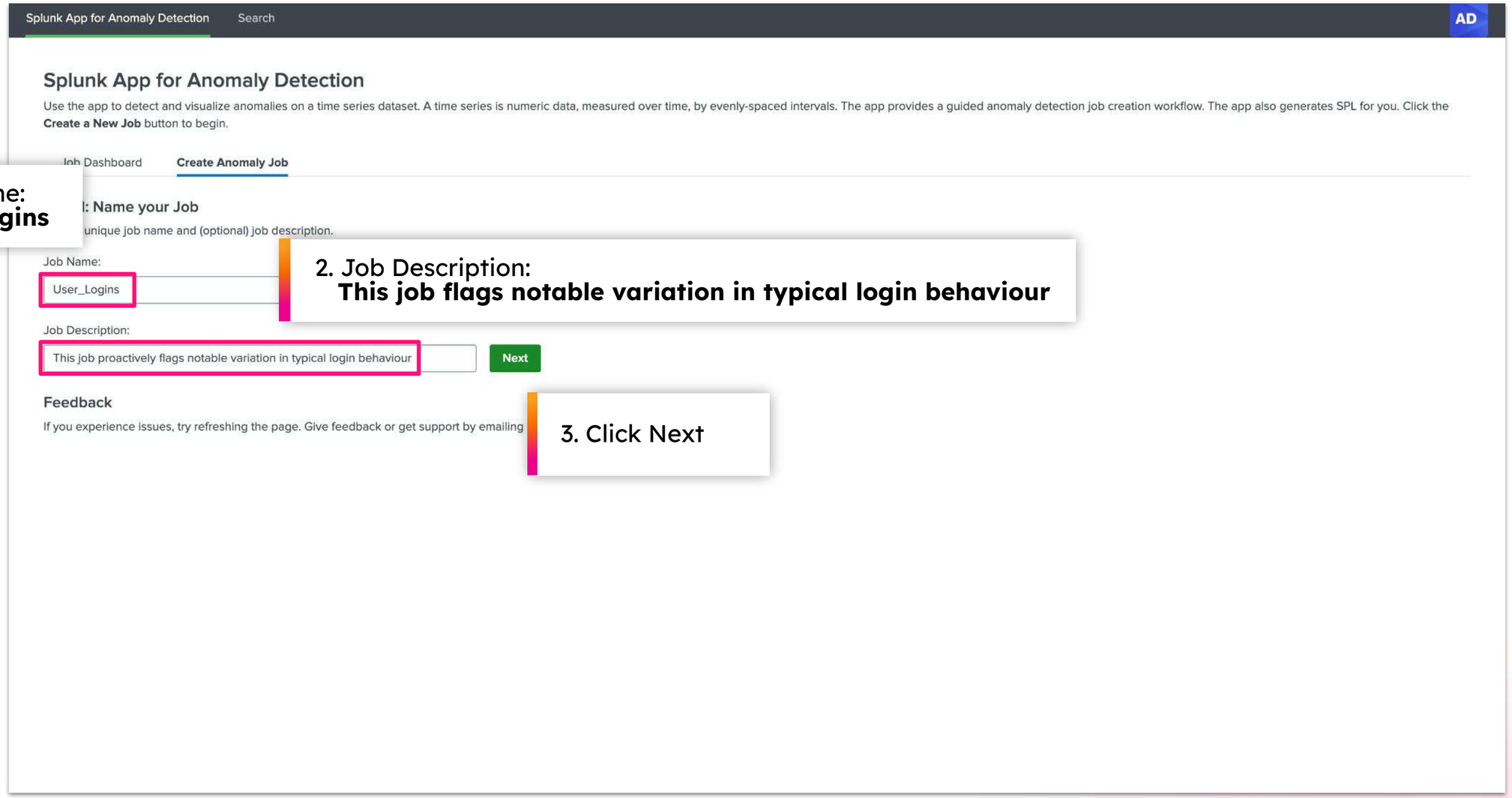
Create Anomaly Job

Start Point



Anomaly Job Details

Search 2-1



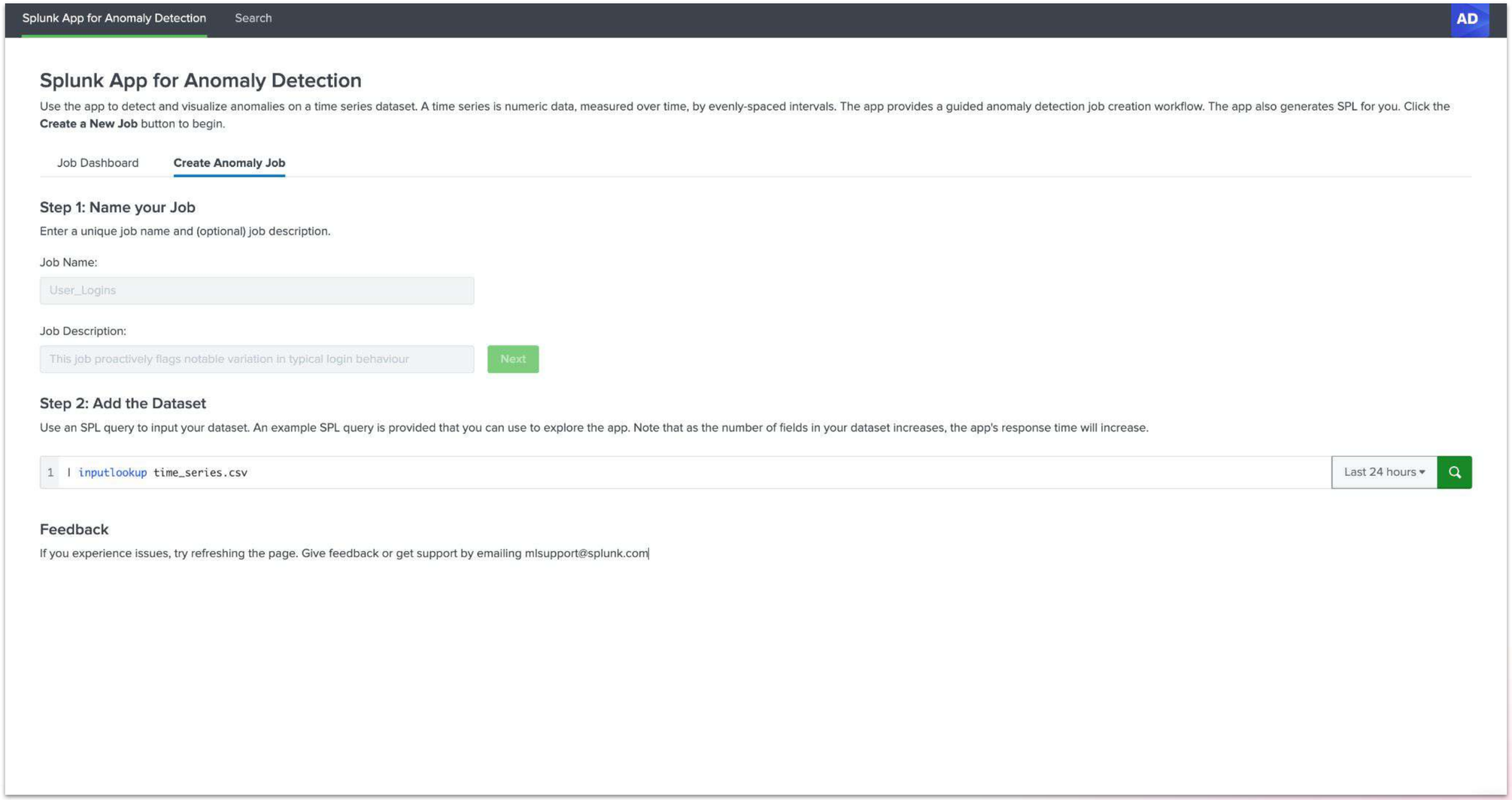
1. Job Name:
   User_Logins

2. Job Description:
   This job flags notable variation in typical login behaviour

3. Click Next

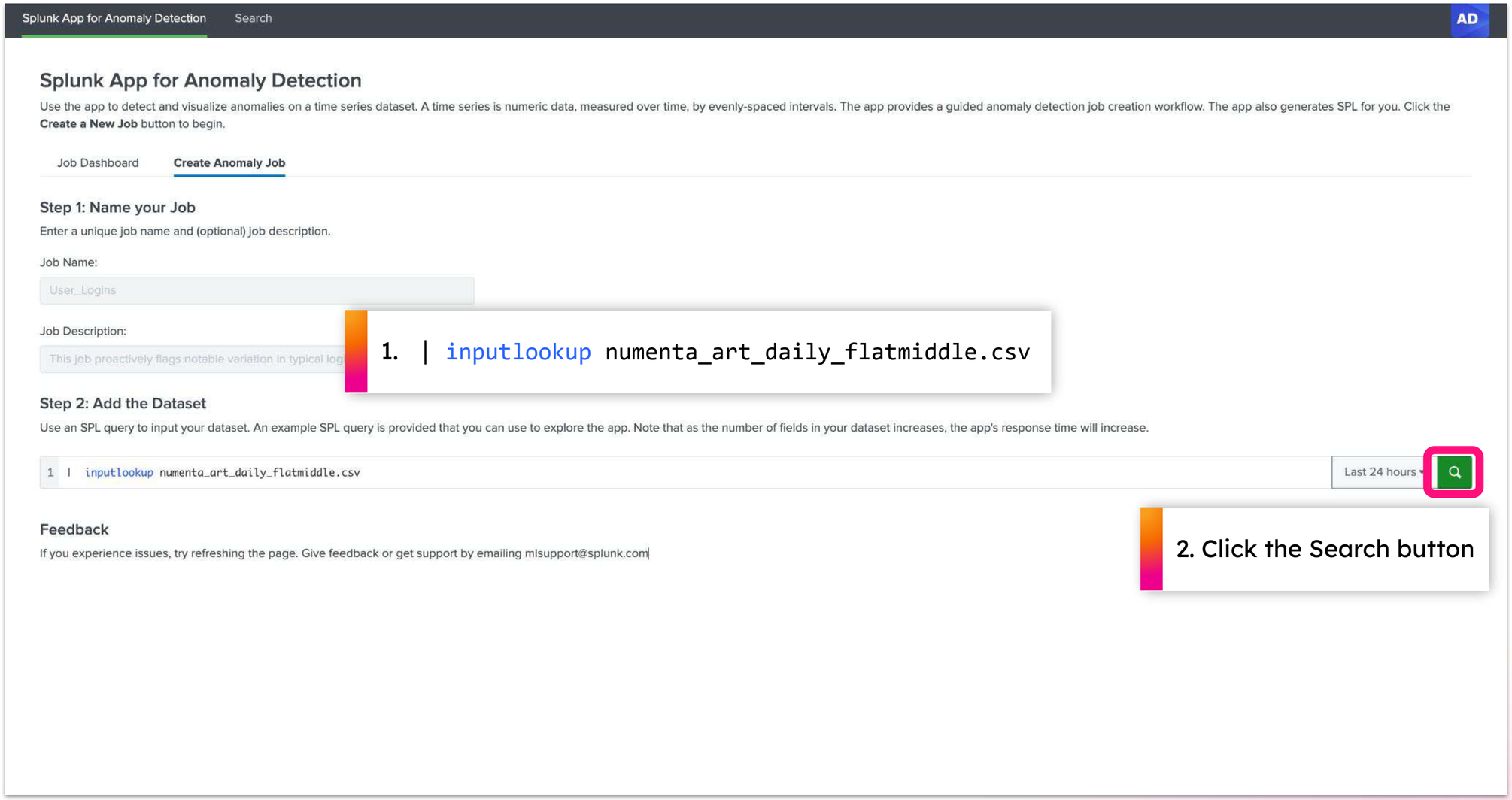
Anomaly Job Details

Default



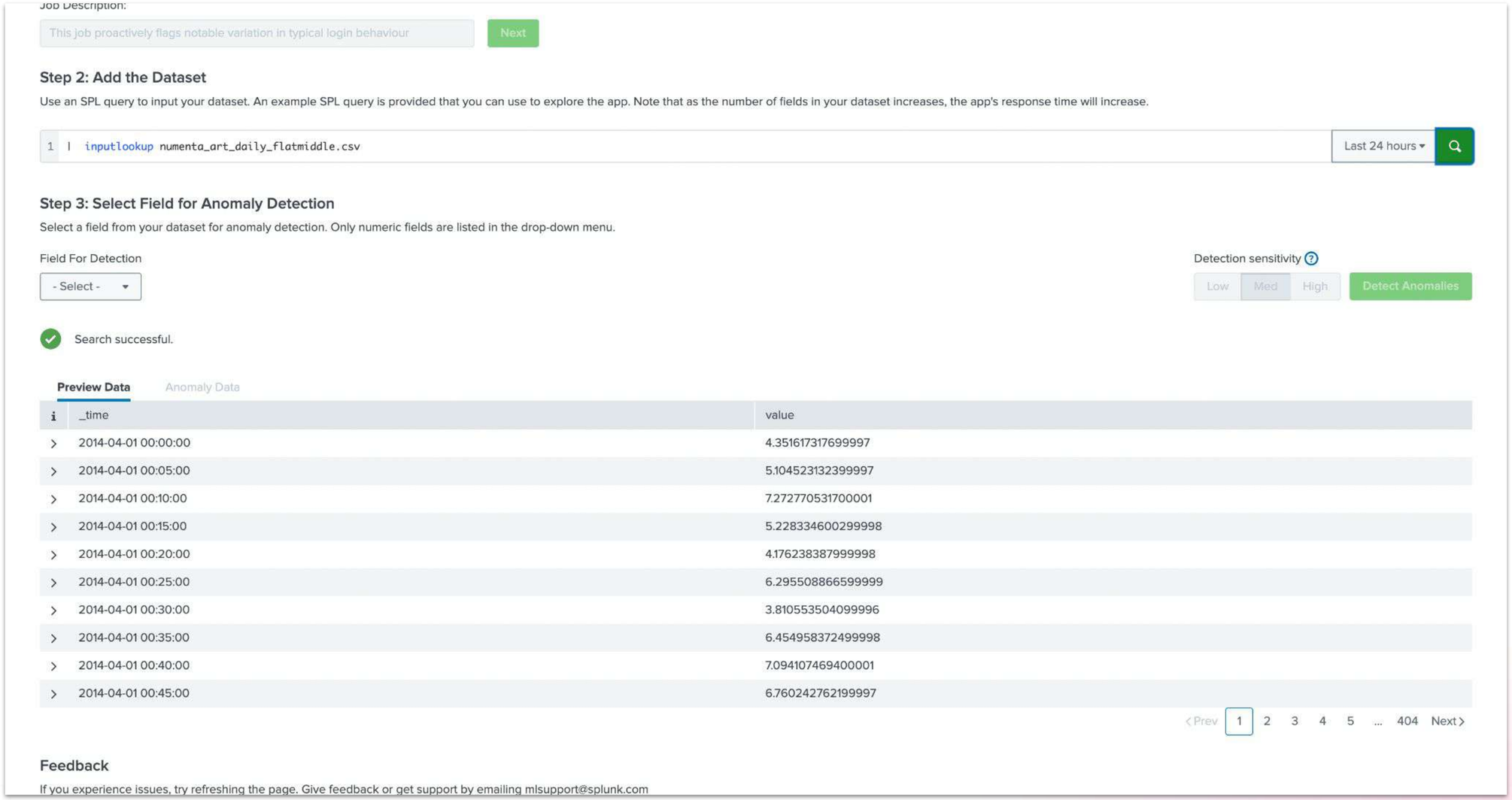
Anomaly Job Details

Search 2-2



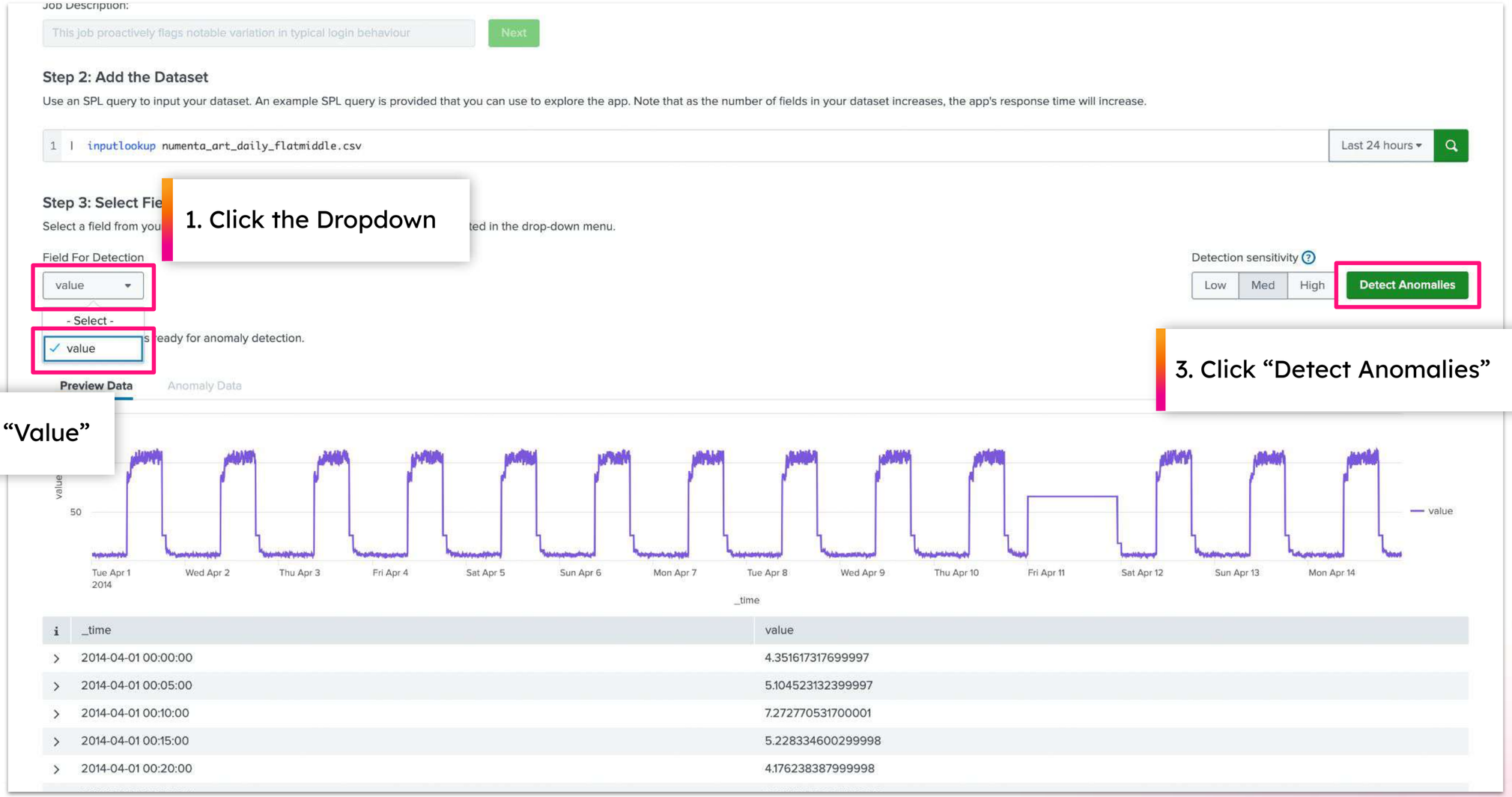
Anomaly Job Details

Search Complete



Anomaly Job

Detect



i	_time	value
>	2014-04-01 00:00:00	4.351617317699997
>	2014-04-01 00:05:00	5.104523132399997
>	2014-04-01 00:10:00	7.272770531700001
>	2014-04-01 00:15:00	5.228334600299998
>	2014-04-01 00:20:00	4.176238387999998

Anomaly Job

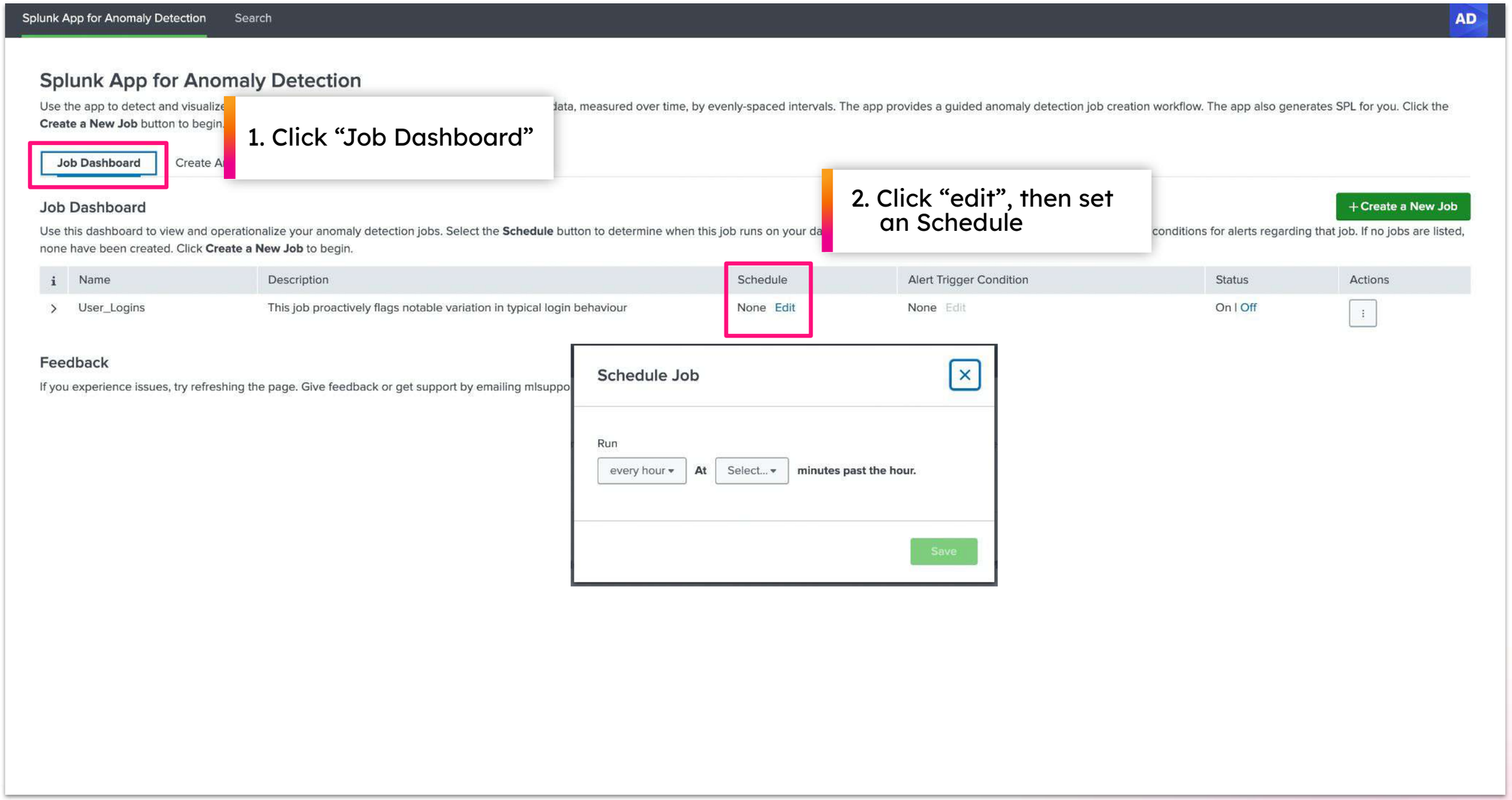
Configuration

Anomaly Job

Save Job

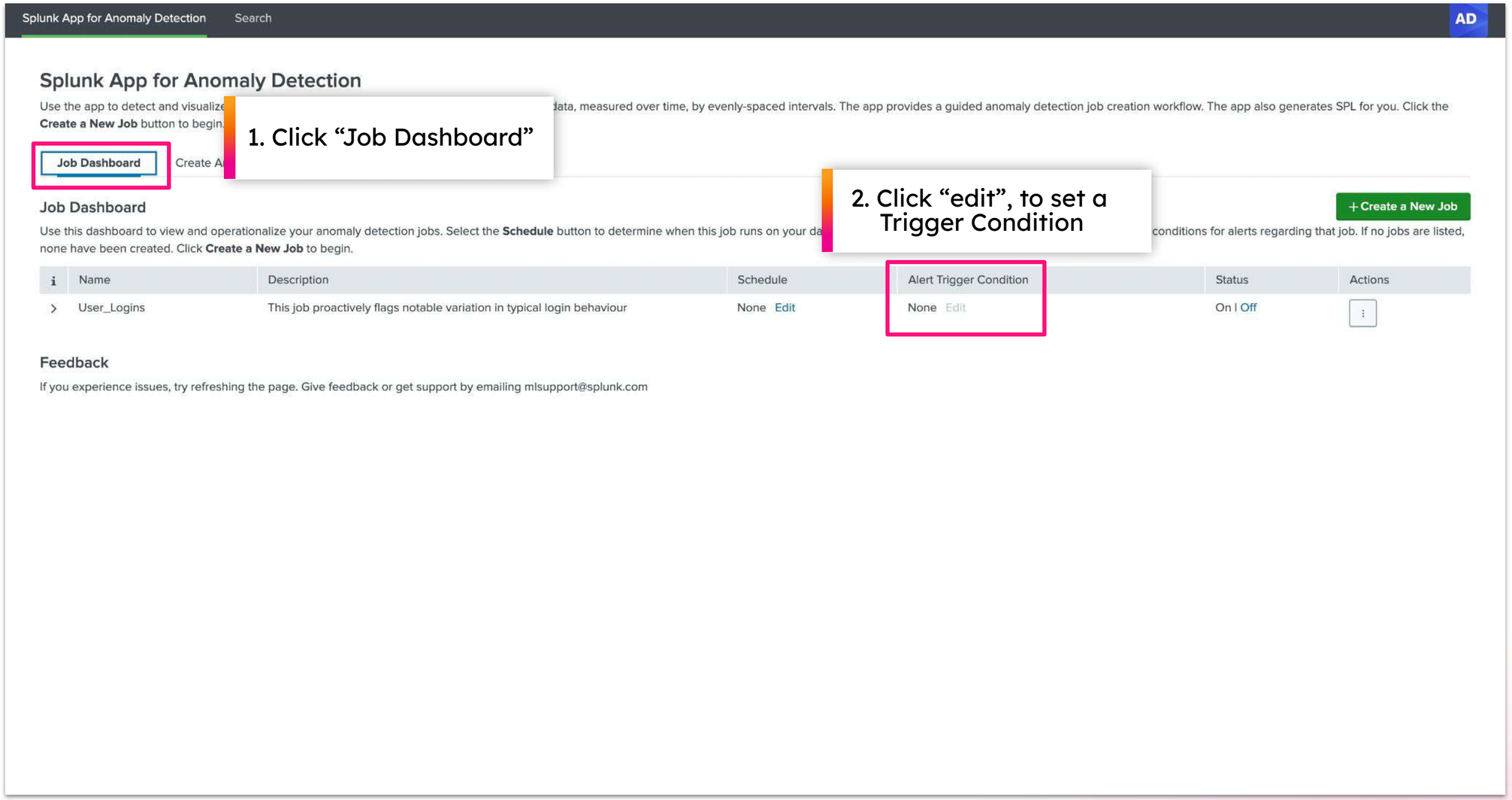
Anomaly Job

Schedule



Anomaly Job

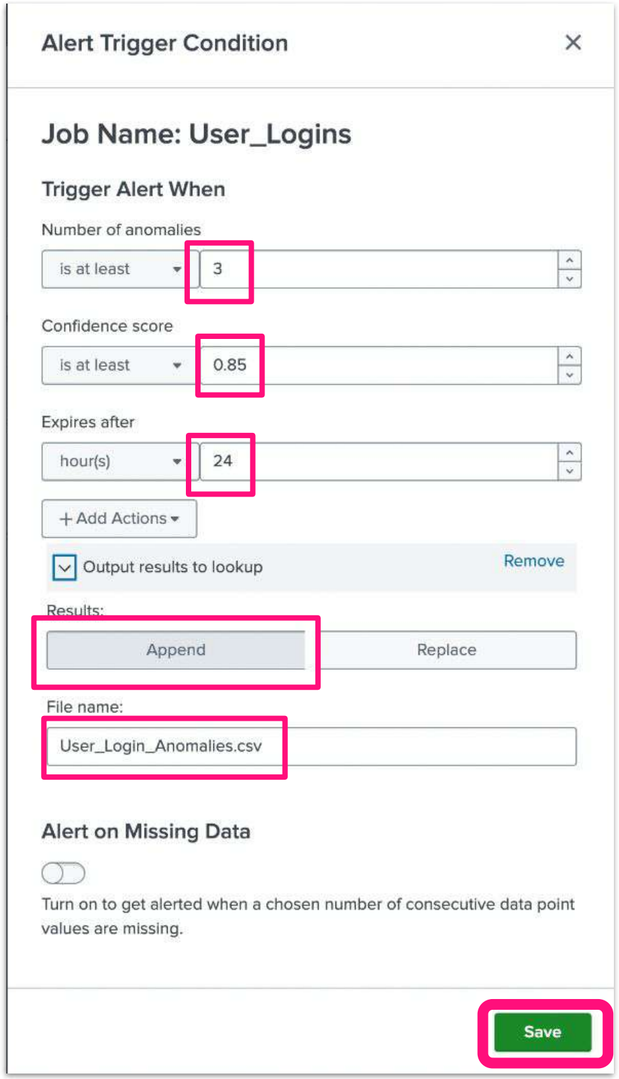
Trigger



Anomaly Job

Trigger

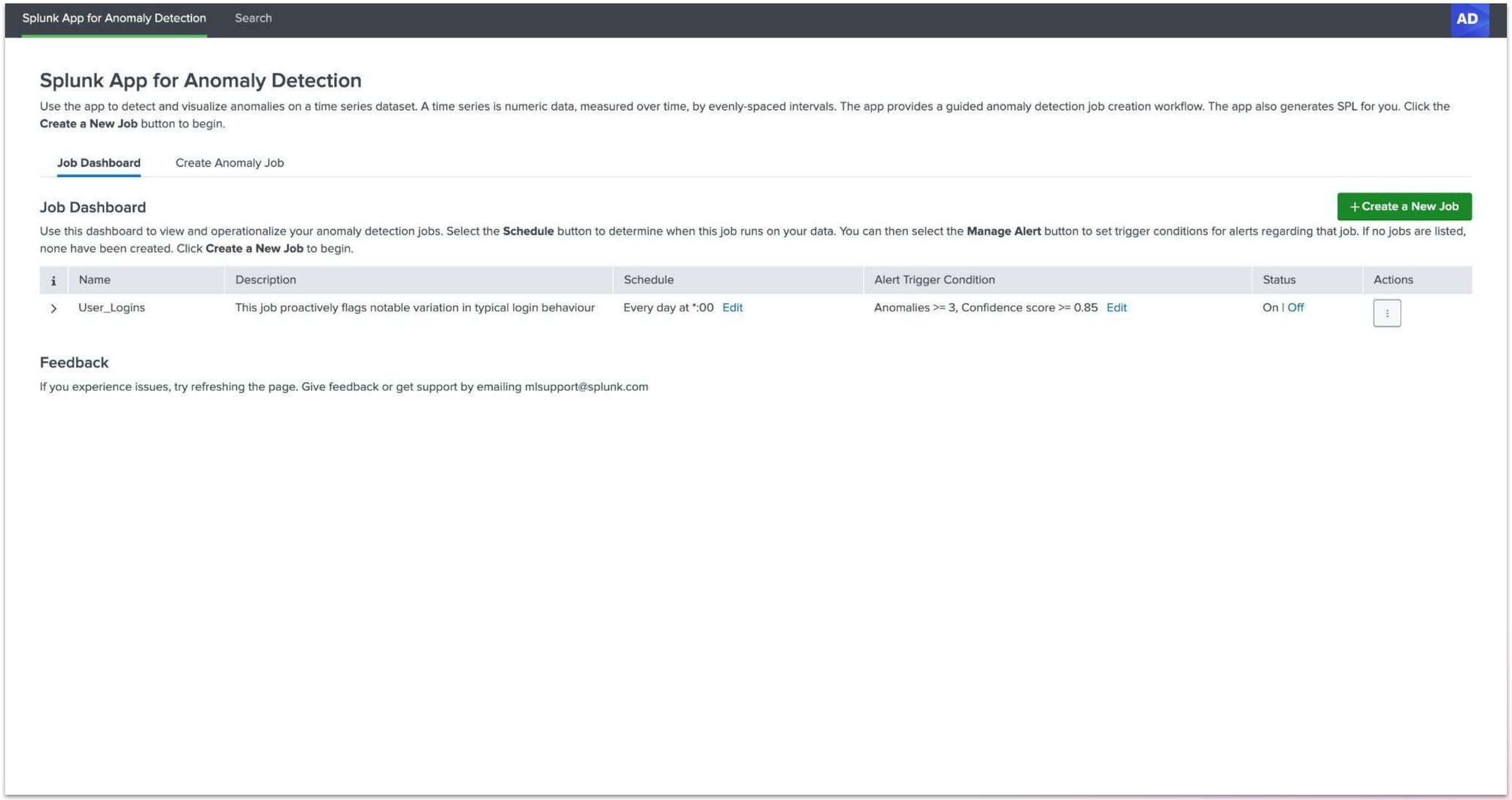
1. Enter the Trigger Condition Details



2. Click “Save”

Anomaly Job

Complete



Scenario 3

Forecasting CPU Utilisation

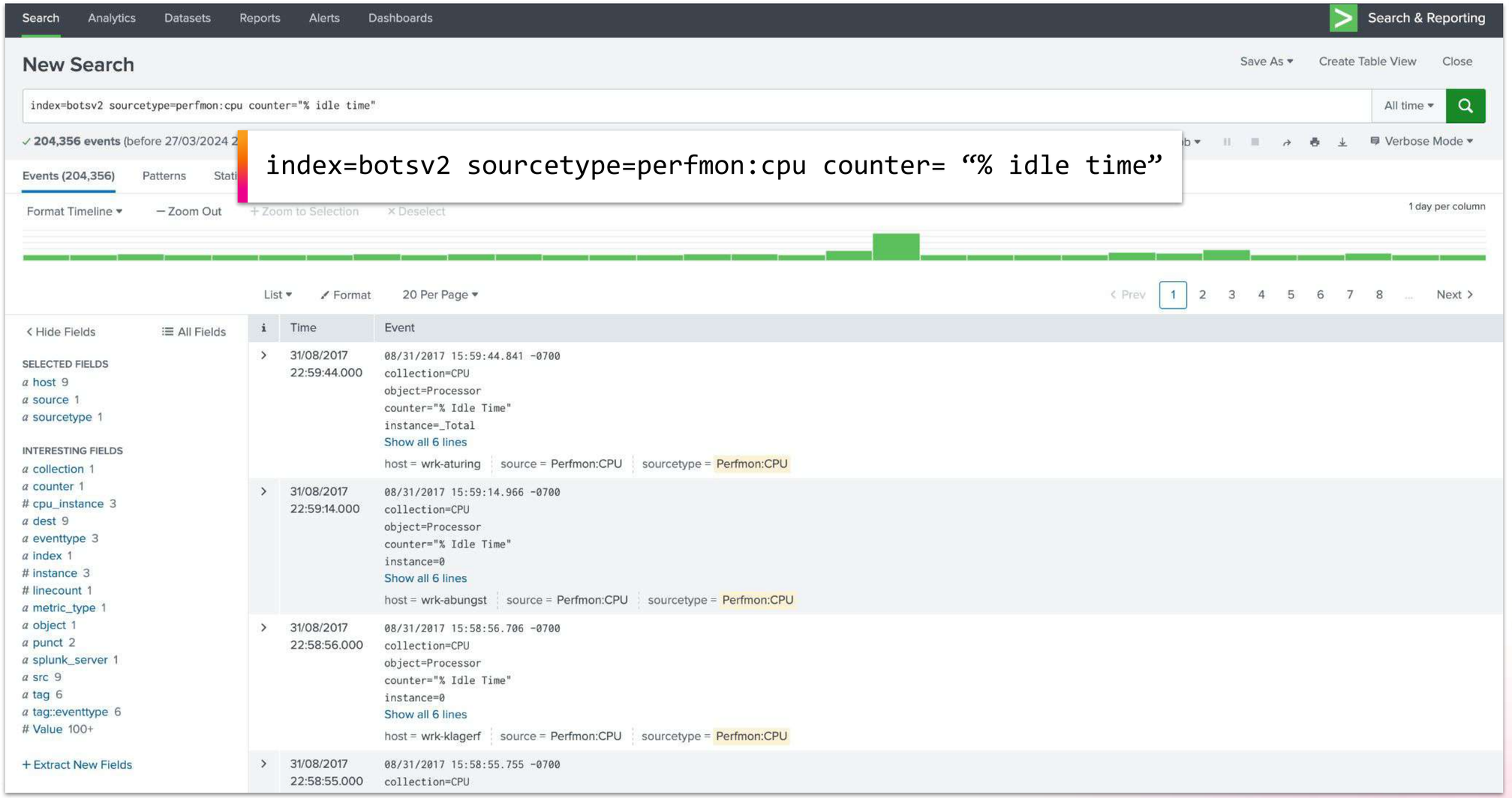
Forecasting CPU Utilisation

You are a IT Operations Analyst at Frothly, you have been asked to investigate if we could predict when CPU utilisation is going to spike again to help the team proactively resolve potential incidents before they occur.

Some reports have come into Buttercup Games that users are reporting crashes, with the game seizing up before exiting unexpectedly. Root cause analysis of these incidents has identified that CPU utilisation on a few servers was running pretty high during these crashes.

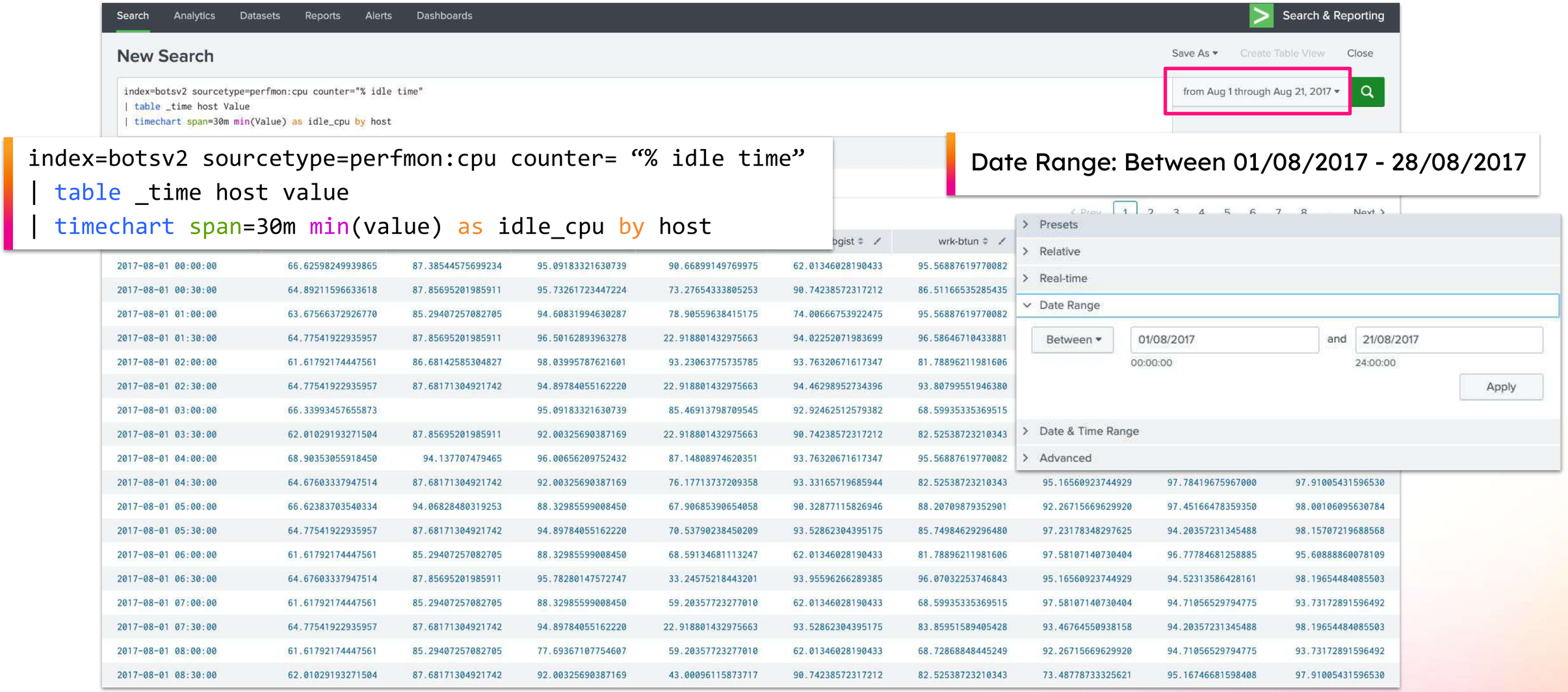
CPU Counters

Search 3-1



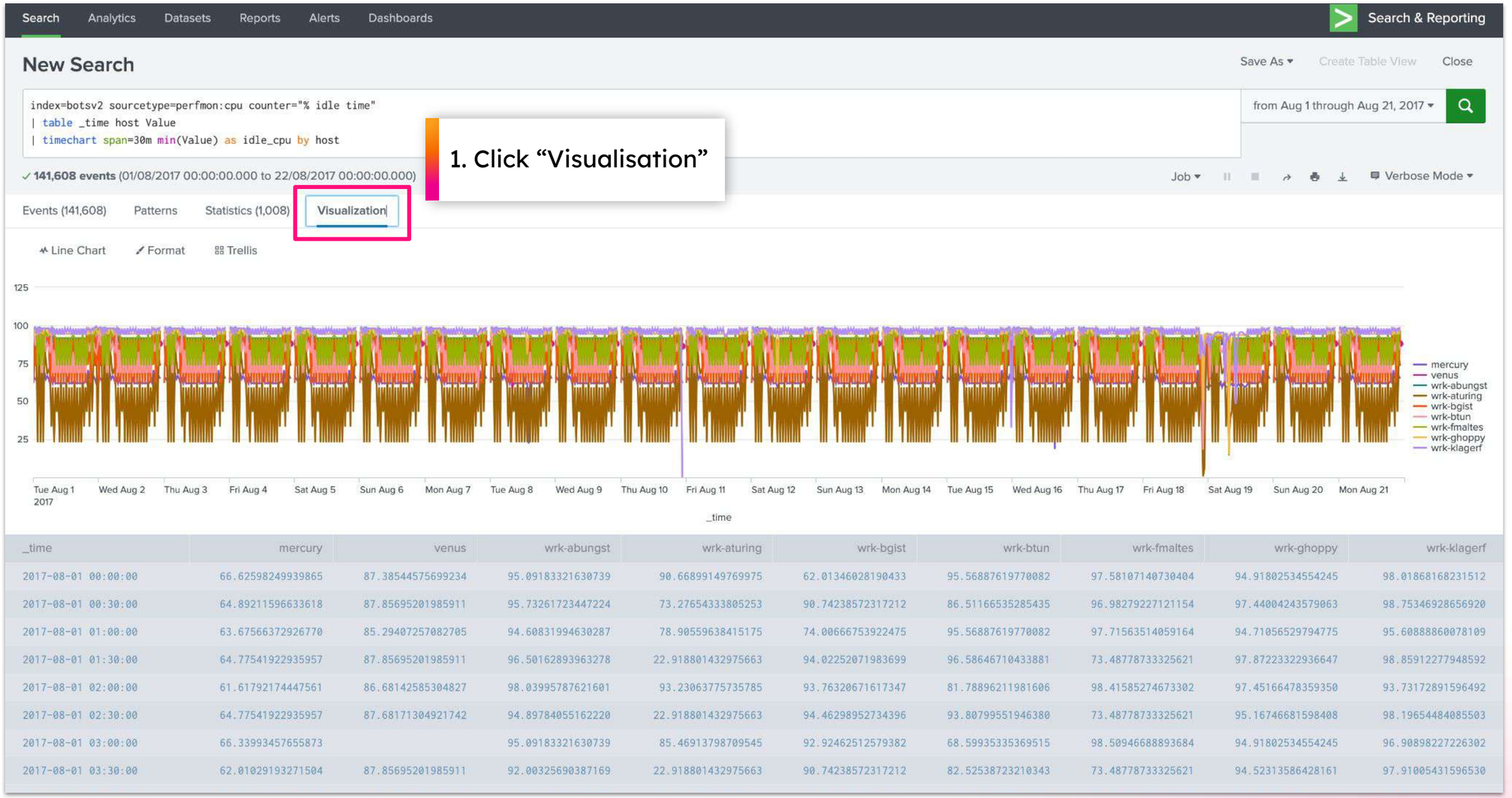
Time Series CPU Counters

Search 3-2



Time Series CPU Counters

Visualisation



_time	mercury	venus	wrk-abungst	wrk-aturing	wrk-bgist	wrk-btun	wrk-fmaltes	wrk-ghoppy	wrk-klagerf
2017-08-01 00:00:00	66.62598249939865	87.38544575699234	95.09183321630739	90.66899149769975	62.01346028190433	95.56887619770082	97.58107140730404	94.91802534554245	98.01868168231512
2017-08-01 00:30:00	64.89211596633618	87.85695201985911	95.73261723447224	73.27654333805253	90.74238572317212	86.51166535285435	96.98279227121154	97.44004243579063	98.75346928656920
2017-08-01 01:00:00	63.67566372926770	85.29407257082705	94.60831994630287	78.90559638415175	74.00666753922475	95.56887619770082	97.71563514059164	94.71056529794775	95.60888860078109
2017-08-01 01:30:00	64.77541922935957	87.85695201985911	96.50162893963278	22.918801432975663	94.02252071983699	96.58646710433881	73.48778733325621	97.87223322936647	98.85912277948592
2017-08-01 02:00:00	61.61792174447561	86.68142585304827	98.03995787621601	93.23063775735785	93.76320671617347	81.78896211981606	98.41585274673302	97.45166478359350	93.73172891596492
2017-08-01 02:30:00	64.77541922935957	87.68171304921742	94.89784055162220	22.918801432975663	94.46298952734396	93.80799551946380	73.48778733325621	95.16746681598408	98.19654484085503
2017-08-01 03:00:00	66.33993457655873		95.09183321630739	85.46913798709545	92.92462512579382	68.59935335369515	98.50946688893684	94.91802534554245	96.90898227226302
2017-08-01 03:30:00	62.01029193271504	87.85695201985911	92.00325690387169	22.918801432975663	90.74238572317212	82.52538723210343	73.48778733325621	94.52313586428161	97.91005431596530

Time Series CPU Counters

Search 3-3


```
index=botsv2 sourcetype=perfmon:cpu counter= “% idle time” host=wrk-aturing
| table _time host value
| timechart span=30m min(value) as idle_cpu
```

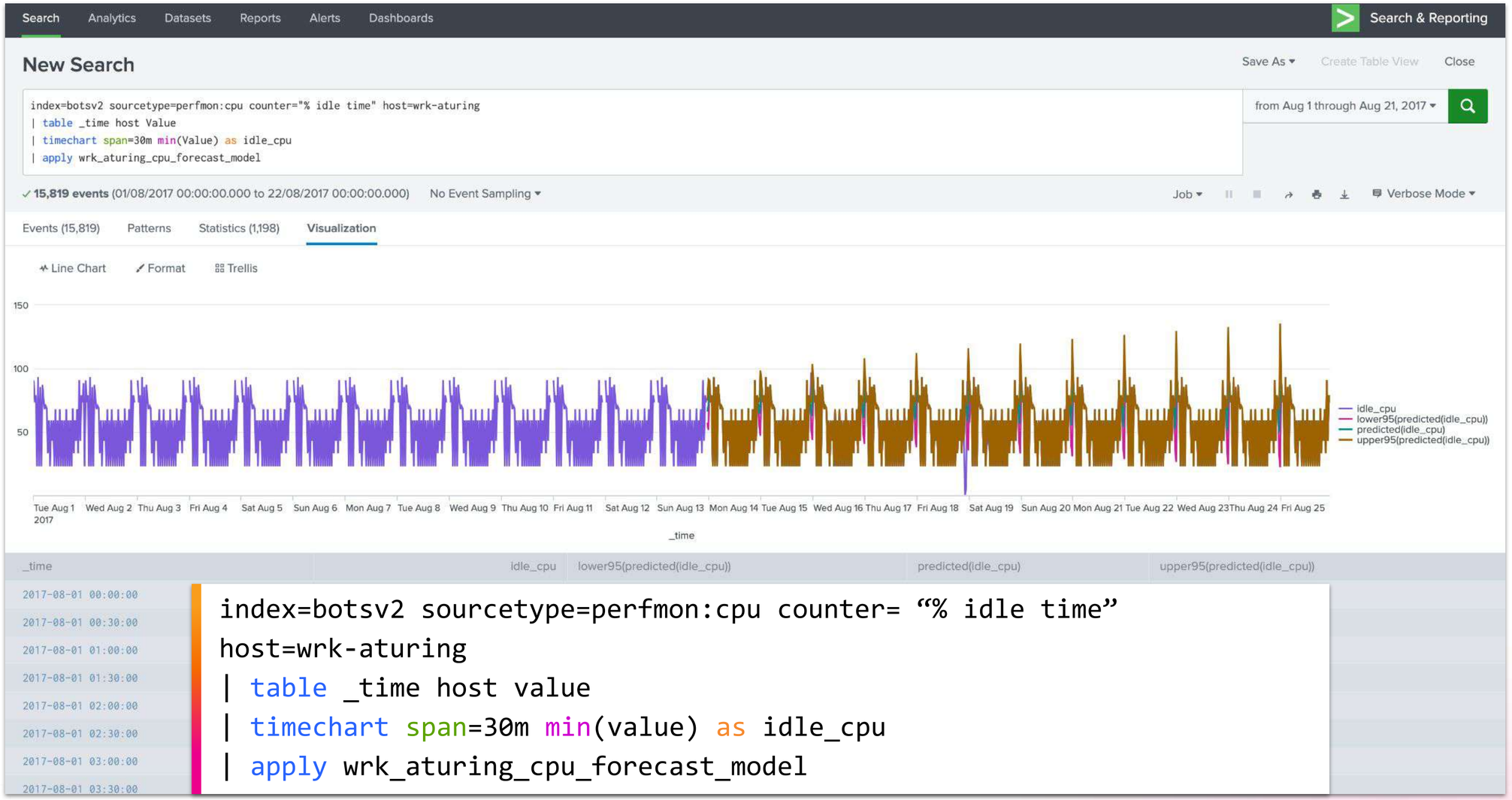
Fit Model on CPU Counters

Search 3-4


```
index=botsv2 sourcetype=perfmon:cpu counter= “% idle time” host=wrk-aturing
| table _time host value
| timechart span=30m min(value) as idle_cpu
| fit StateSpaceForecast idle_cpu holdback=8d forecast_k=12d into wrk_aturing_cpu_forecast_model
```

Apply Model on CPU Counters

Search 3-5




```
index=botsv2 sourcetype=perfmon:cpu counter= “% idle time”
host=wrk-aturing
| table _time host value
| timechart span=30m min(value) as idle_cpu
| apply wrk_aturing_cpu_forecast_model
```

Search Breakdown

Bookmark

Splunk search	Description
index=botsv2 sourcetype=perfmon:cpu counter="% idle time"	Search the perfmon:cpu logs in the botsv2 index to see CPU idle time
… | table _time host Value	Create a table from our raw results containing the time, host and CPU idle value
… | timechart span=30m min(Value) as idle_cpu by host	Calculate for each host the minimum CPU idle time over each 30 minute window
… | fit StateSpaceForecast idle_cpu holdback=8d forecast_k=12d into wrk_aturing_cpu_forecast_model	Train a StateSpaceForecast model to create a forecast on the CPU idle data. The model will forecast 12 days into the future, and is trained on all of the input data except for the final 8 days of information.
… | apply wrk_aturing_cpu_forecast_model	Apply the saved model named wrk_aturing_cpu_forecast_model on the data

Scenario 4

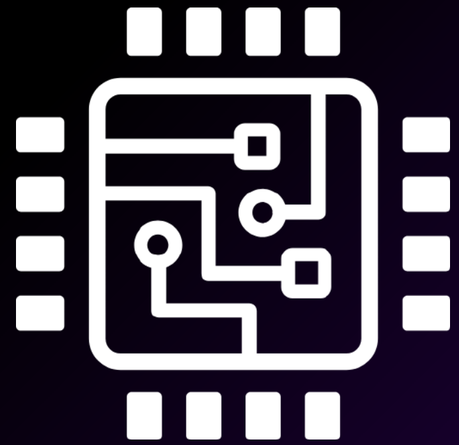
Detecting Outliers in Network Utilisation Telemetry

Detecting Outliers
in Network Utilisation Telemetary

You are an App Developer at Frothly. Despite resolving the CPU utilisation issues, you have been getting some customer complaints that the app periodically stops responding to their inputs, making it irritating to use.

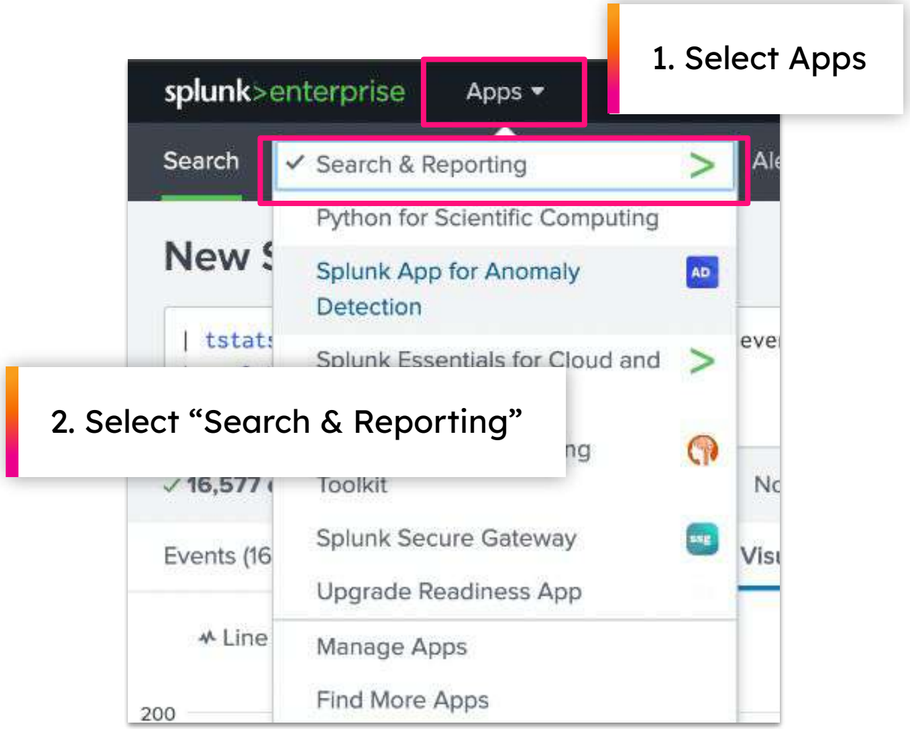
To troubleshoot what might be going on, you decide to analyze your network to look for signs of lag between your services.

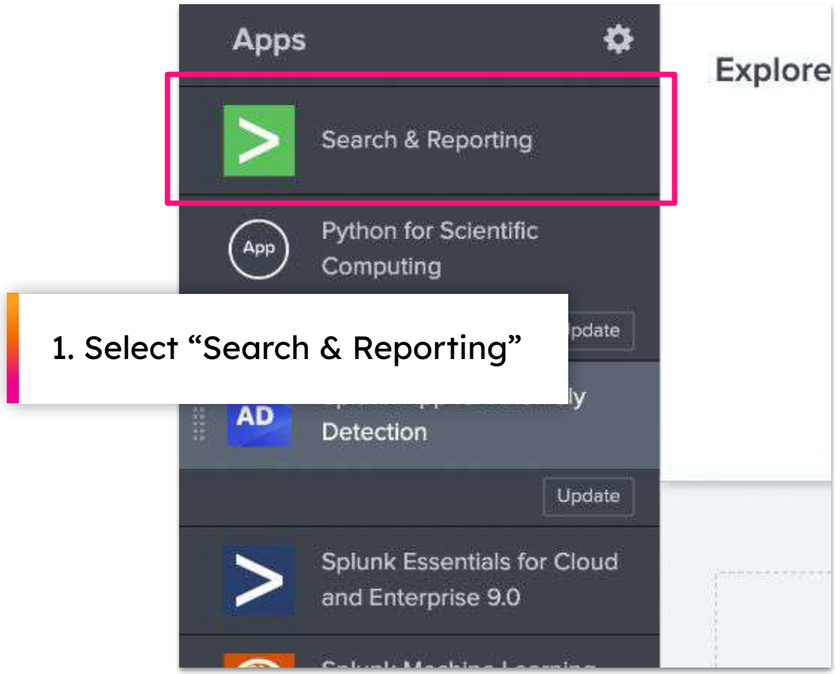
For the investigation, you use the **round-trip time (RTT)**, or the time it takes for a network request to go from a starting point to a destination and back again to the starting point. In this case, finding the average client RTT indicates the network latency.



Search & Reporting

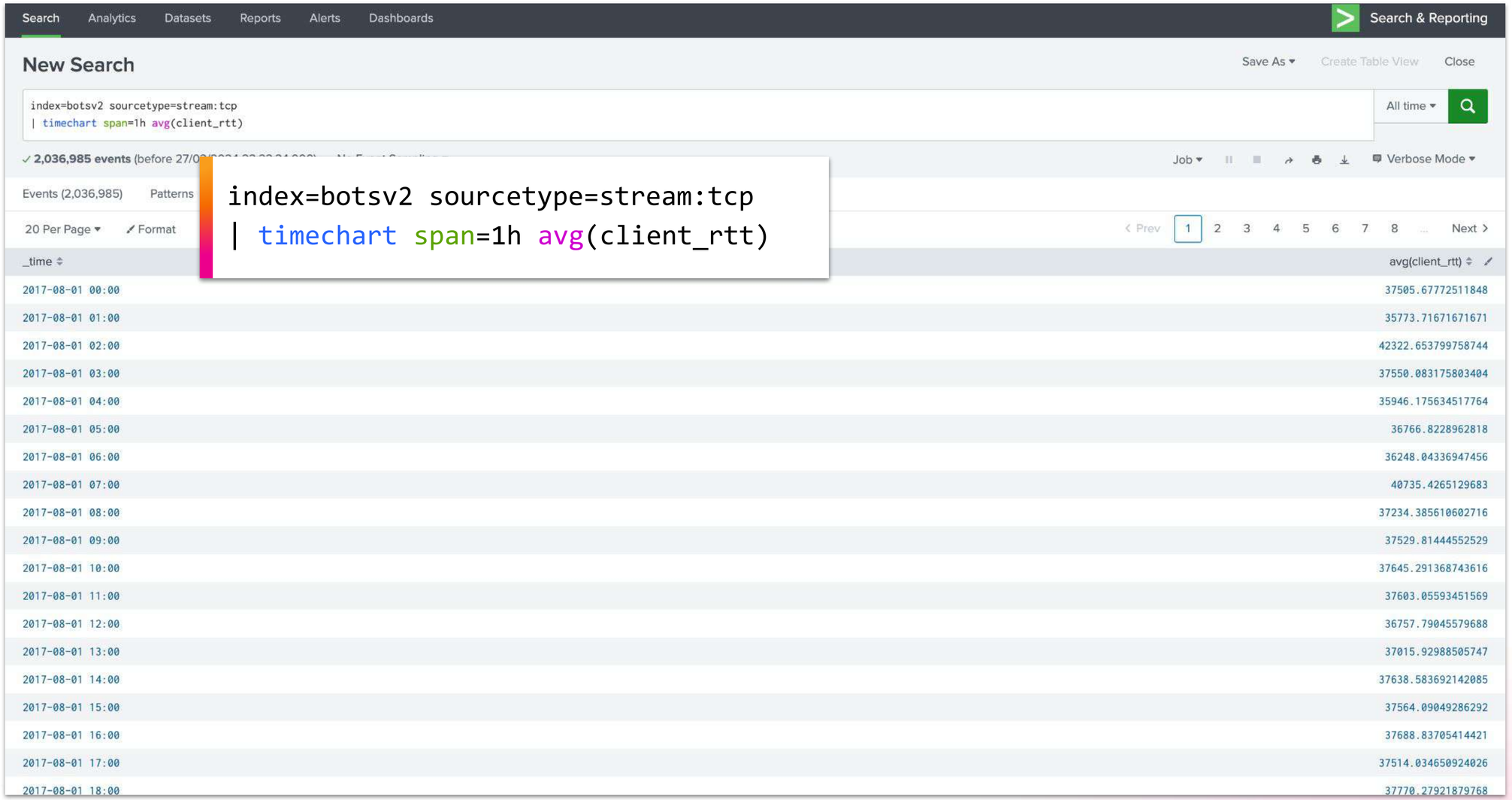
Navigation Options





Stream Data

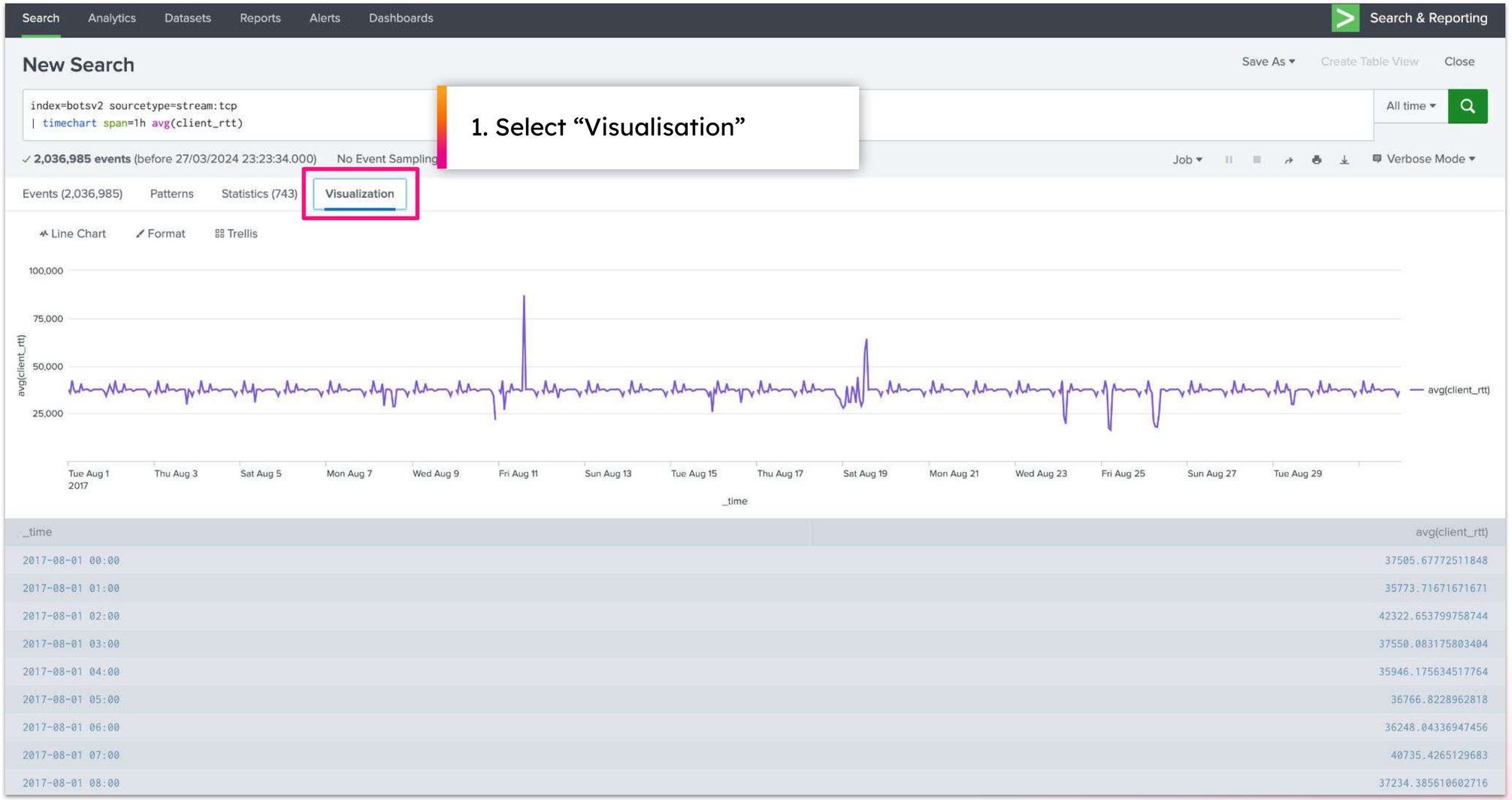
Search 4-1




```
index=botsv2 sourcetype=stream:tcp
| timechart span=1h avg(client_rtt)
```

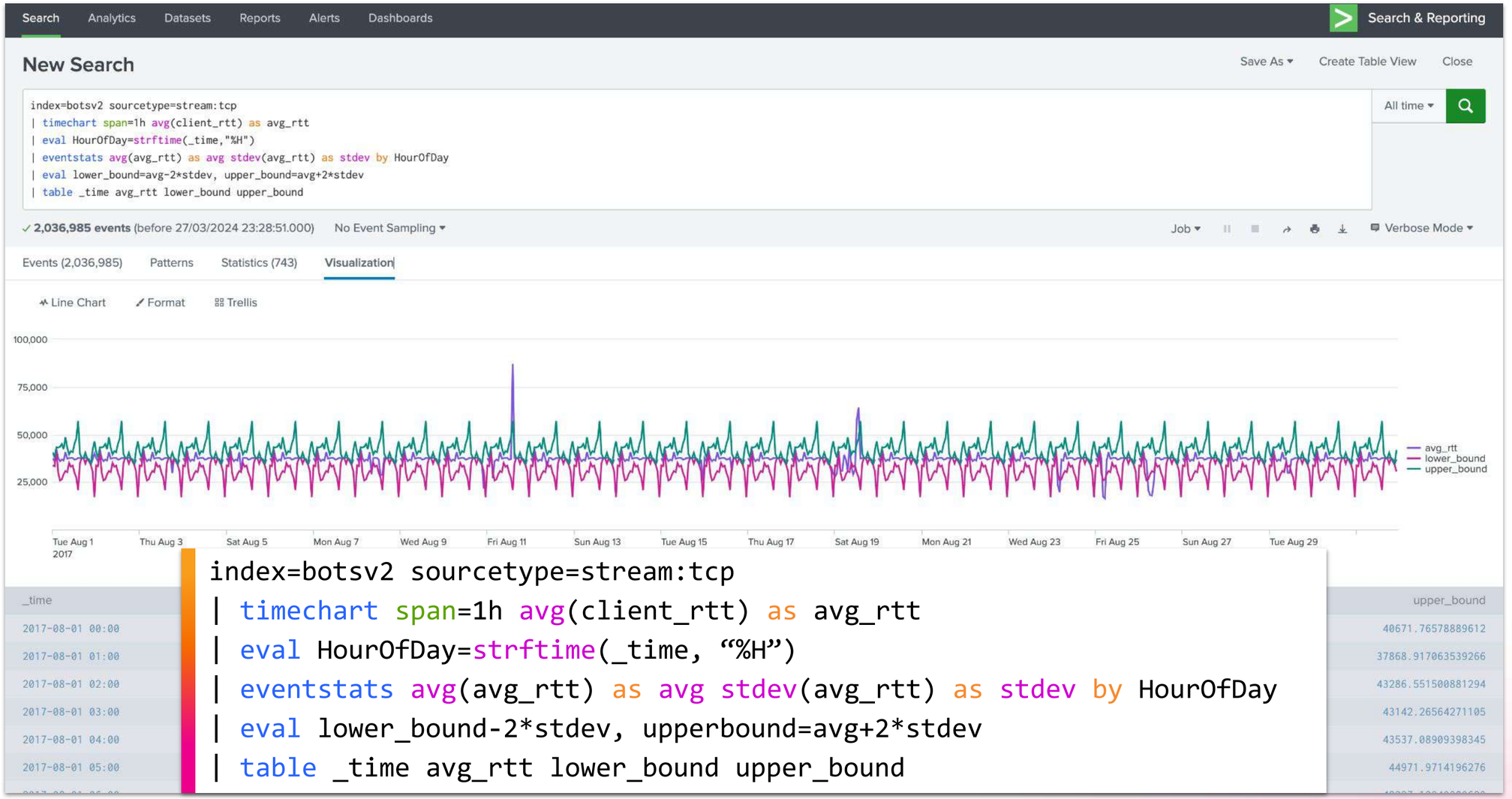
Stream Data

Visualisation



Stream Data

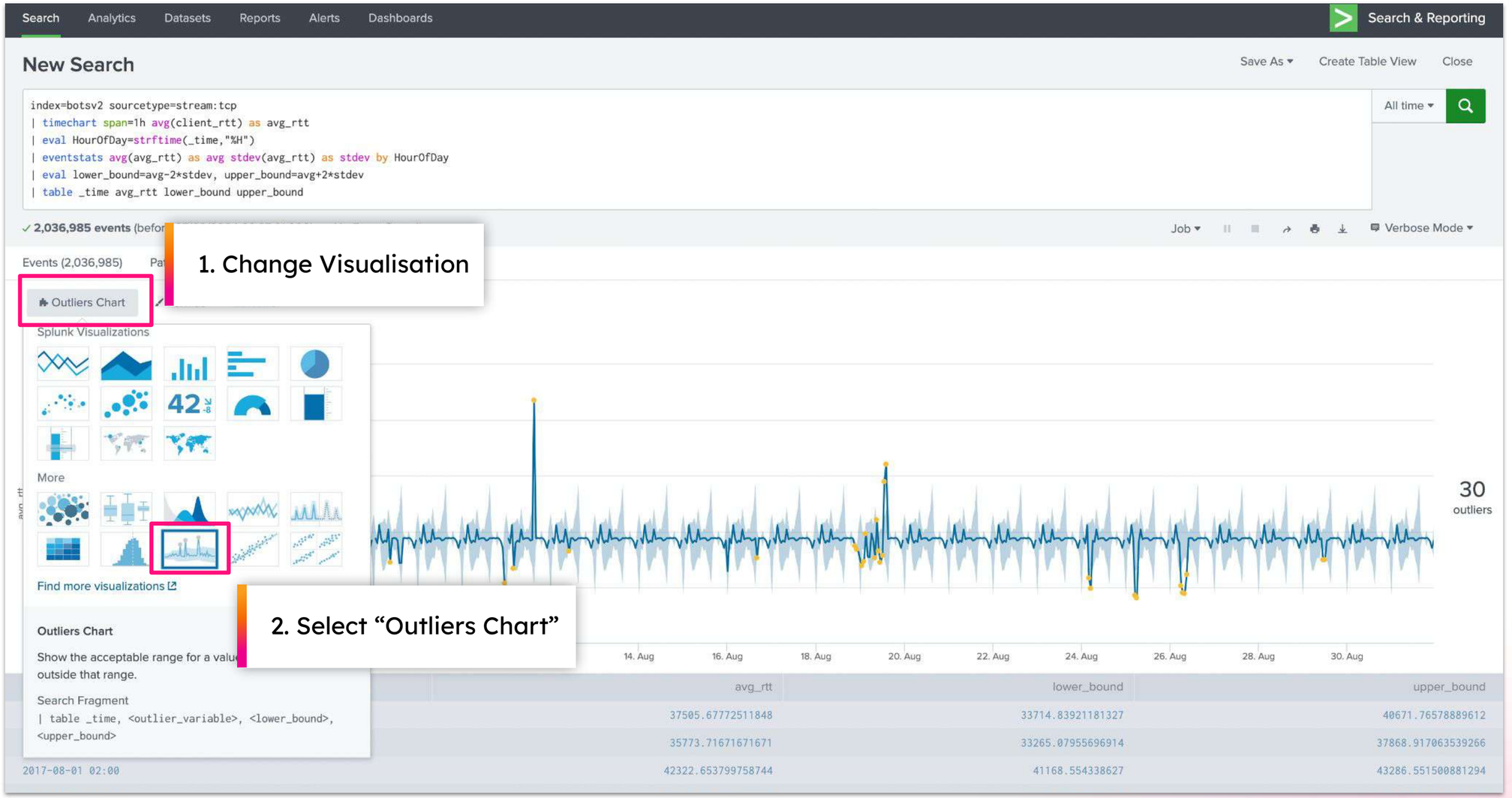
Search 4-2




```
index=botsv2 sourcetype=stream:tcp
| timechart span=1h avg(client_rtt) as avg_rtt
| eval HourOfDay=strftime(_time, "%H")
| eventstats avg(avg_rtt) as avg stdev(avg_rtt) as stdev by HourOfDay
| eval lower_bound-2*stdev, upperbound=avg+2*stdev
| table _time avg_rtt lower_bound upper_bound
```

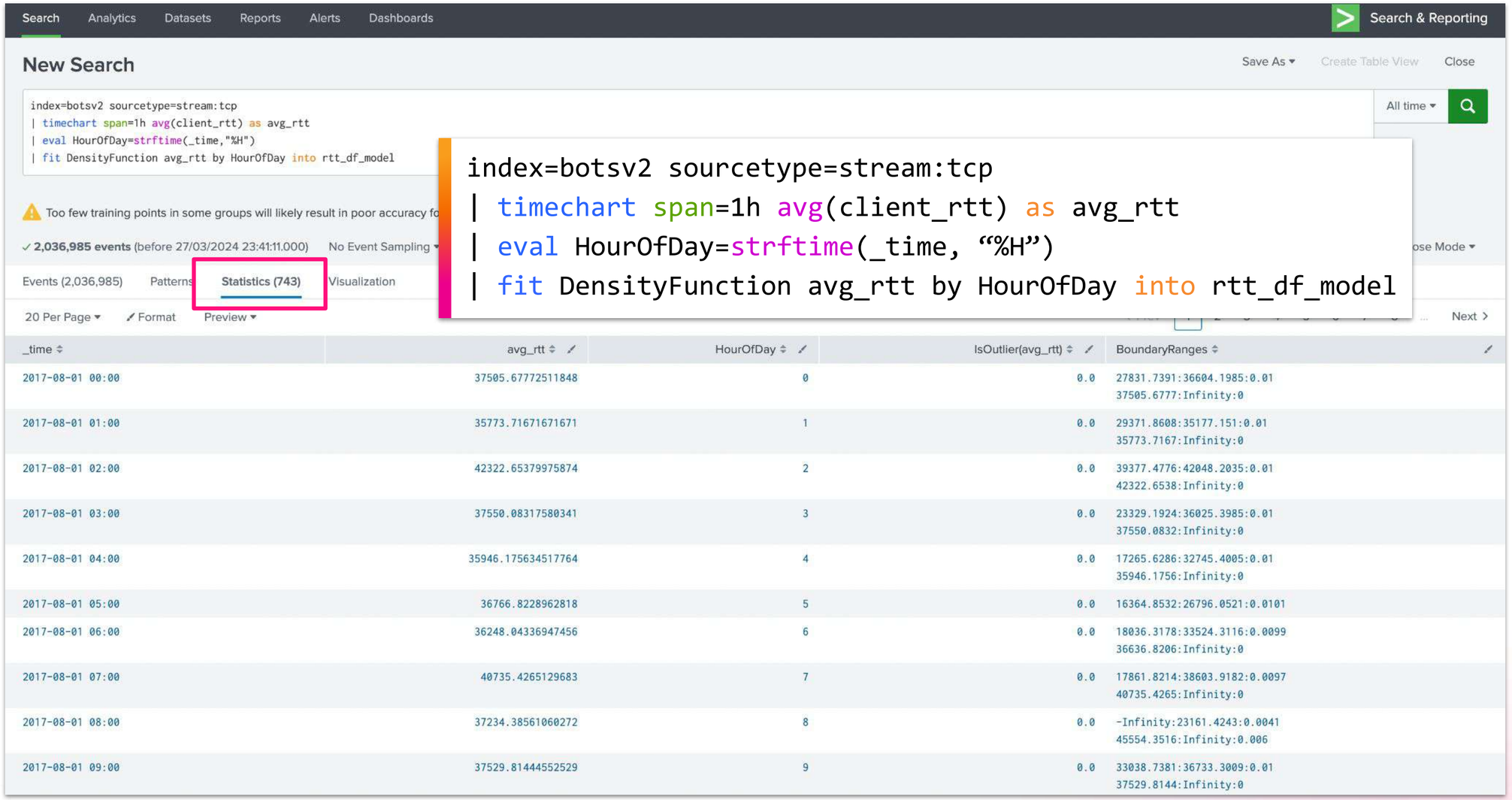
Stream Data

Outliers



Fit Model on Stream Data

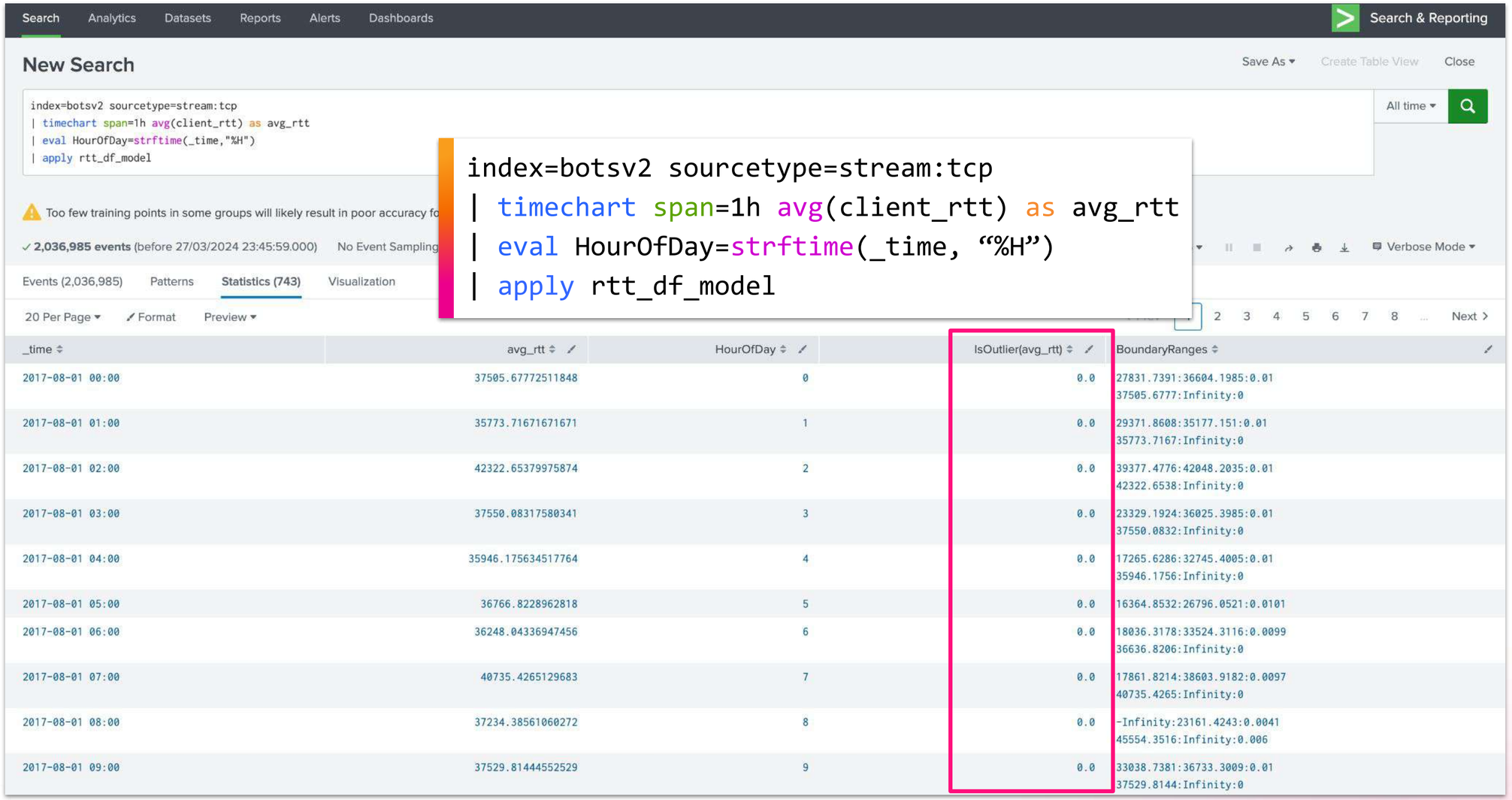
Search 4-3



_time	avg_rtt	HourOfDay	IsOutlier(avg_rtt)	BoundaryRanges
2017-08-01 00:00	37505.67772511848	0	0.0	27831.7391:36604.1985:0.01 37505.6777:Infinity:0
2017-08-01 01:00	35773.71671671671	1	0.0	29371.8608:35177.151:0.01 35773.7167:Infinity:0
2017-08-01 02:00	42322.65379975874	2	0.0	39377.4776:42048.2035:0.01 42322.6538:Infinity:0
2017-08-01 03:00	37550.08317580341	3	0.0	23329.1924:36025.3985:0.01 37550.0832:Infinity:0
2017-08-01 04:00	35946.175634517764	4	0.0	17265.6286:32745.4005:0.01 35946.1756:Infinity:0
2017-08-01 05:00	36766.8228962818	5	0.0	16364.8532:26796.0521:0.0101
2017-08-01 06:00	36248.04336947456	6	0.0	18036.3178:33524.3116:0.0099 36636.8206:Infinity:0
2017-08-01 07:00	40735.4265129683	7	0.0	17861.8214:38603.9182:0.0097 40735.4265:Infinity:0
2017-08-01 08:00	37234.38561060272	8	0.0	-Infinity:23161.4243:0.0041 45554.3516:Infinity:0.006
2017-08-01 09:00	37529.81444552529	9	0.0	33038.7381:36733.3009:0.01 37529.8144:Infinity:0

Apply Model on Stream Data

Search 4-4




```
index=botsv2 sourcetype=stream:tcp
| timechart span=1h avg(client_rtt) as avg_rtt
| eval HourOfDay=strftime(_time, "%H")
| apply rtt_df_model
```

Search Breakdown

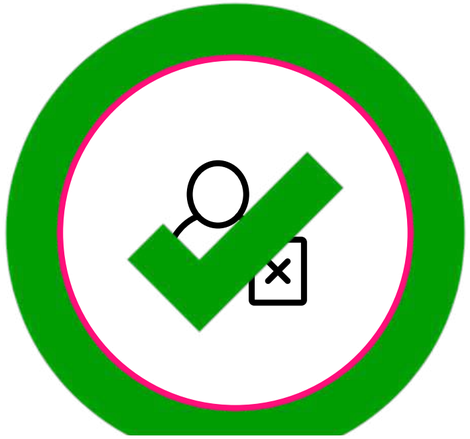
Bookmark

Splunk search	Description
index=botsv2 sourcetype=stream:tcp	Search the stream:tcp logs in the botsv2 index
… | timechart span=1h avg(client_rtt) as avg_rtt	For each hour, calculate the average client RTT and save it as avg_rtt
… | eval HourOfDay=strftime(_time,"%H")	Returns the hour from the _time field, and store it as HourOfDay strftime(_time,"%H") takes a UNIX time value and returns the time as a string in the specified format, in this case the hour.
… | eventstats avg(avg_rtt) as avg stdev(avg_rtt) as stdev by HourOfDay	Calculate the average and standard deviation of the average hourly RTT and save them as avg and stdev
… | eval lower_bound=avg-2*stdev, upper_bound=avg+2*stdev	The average and standard deviation are used with the eval command to calculate the lower and upper boundaries. A sensitivity is added into the calculation by multiplying the stdev by 2, as in any distribution, about 95% of values should be within 2 standard deviations of the mean.
… | table _time avg_rtt lower_bound upper_bound	Returns a table with fields time, average RTT, lower bounds, and upper bounds
… | fit DensityFunction avg_rtt by HourOfDay into rtt_df_model	Fit the DensityFunction algorithm over the average RTT data by hour into the model name, rtt_df_model
… | apply rtt_df_model	Apply the saved model named rtt_df_model on the data

Objective for Today

An Understanding of

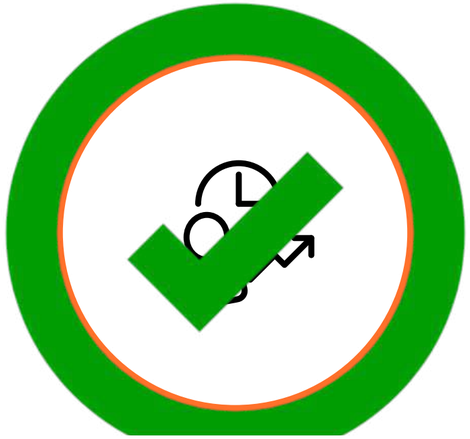
User Access Anomalies



Insider Threat

DensityFunction

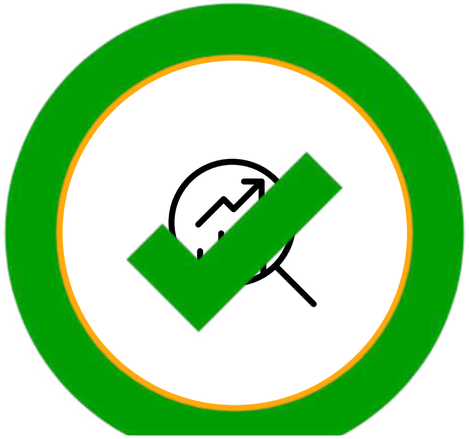
Anomalous Login Quantities



IT Operations

Splunk App

Forecast CPU Utilisation



Infrastructure

StateSpaceForecast

Outliers in Utilisation Telemetry

All

DensityFunction

Splunk Resources

Where to go after today's workshop

Splunk Community

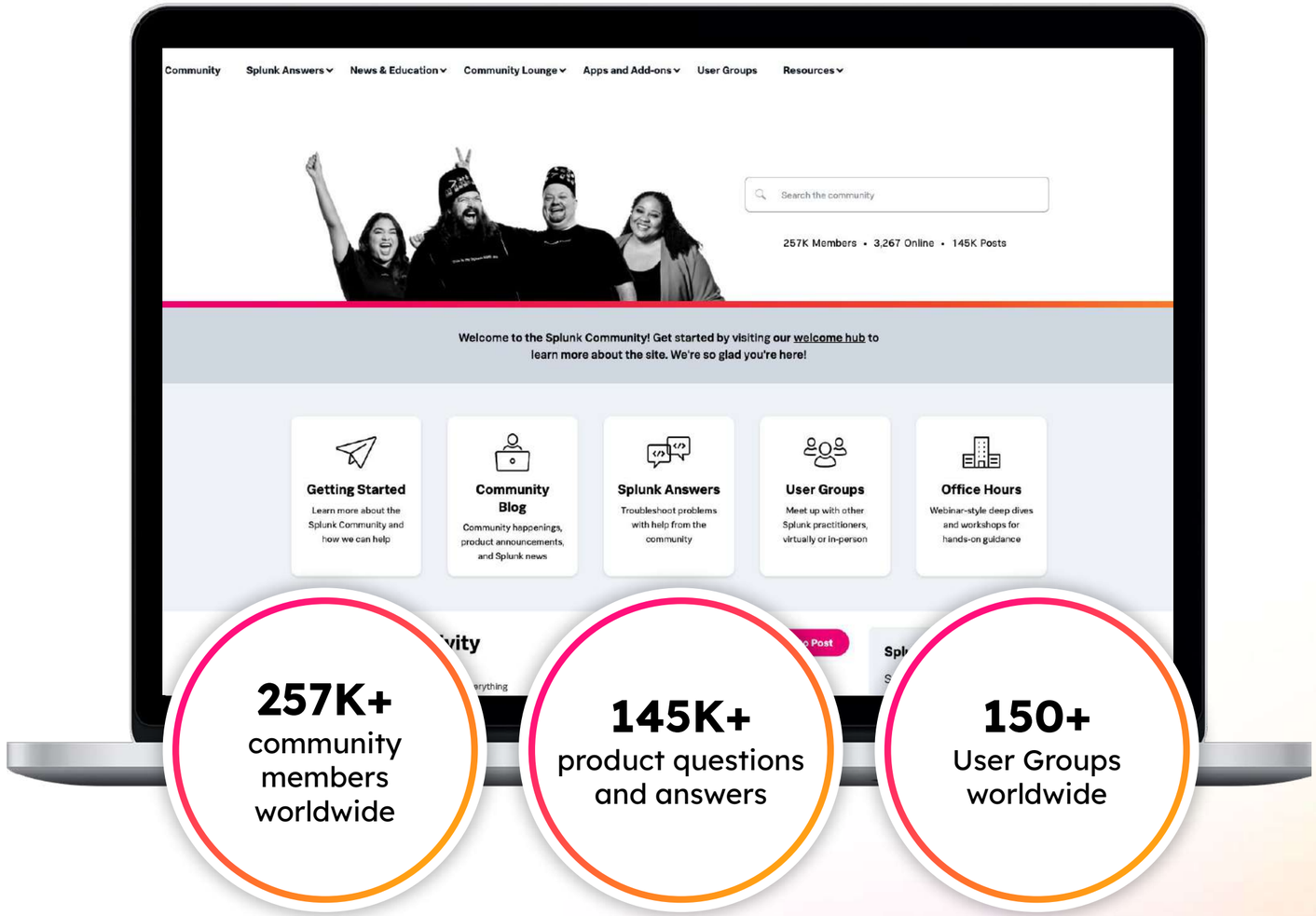
https://community.splunk.com

A free way to connect, learn, have fun, and find success with Splunk

Ask questions, get answers, and find solutions from passionate experts in the community

Meet in-person or virtually with like-minded enthusiasts, in your area or by interest

Search for, vote on, or submit your own ideas for new enhancements for any product or solution



Splunk Events

https://events.splunk.com

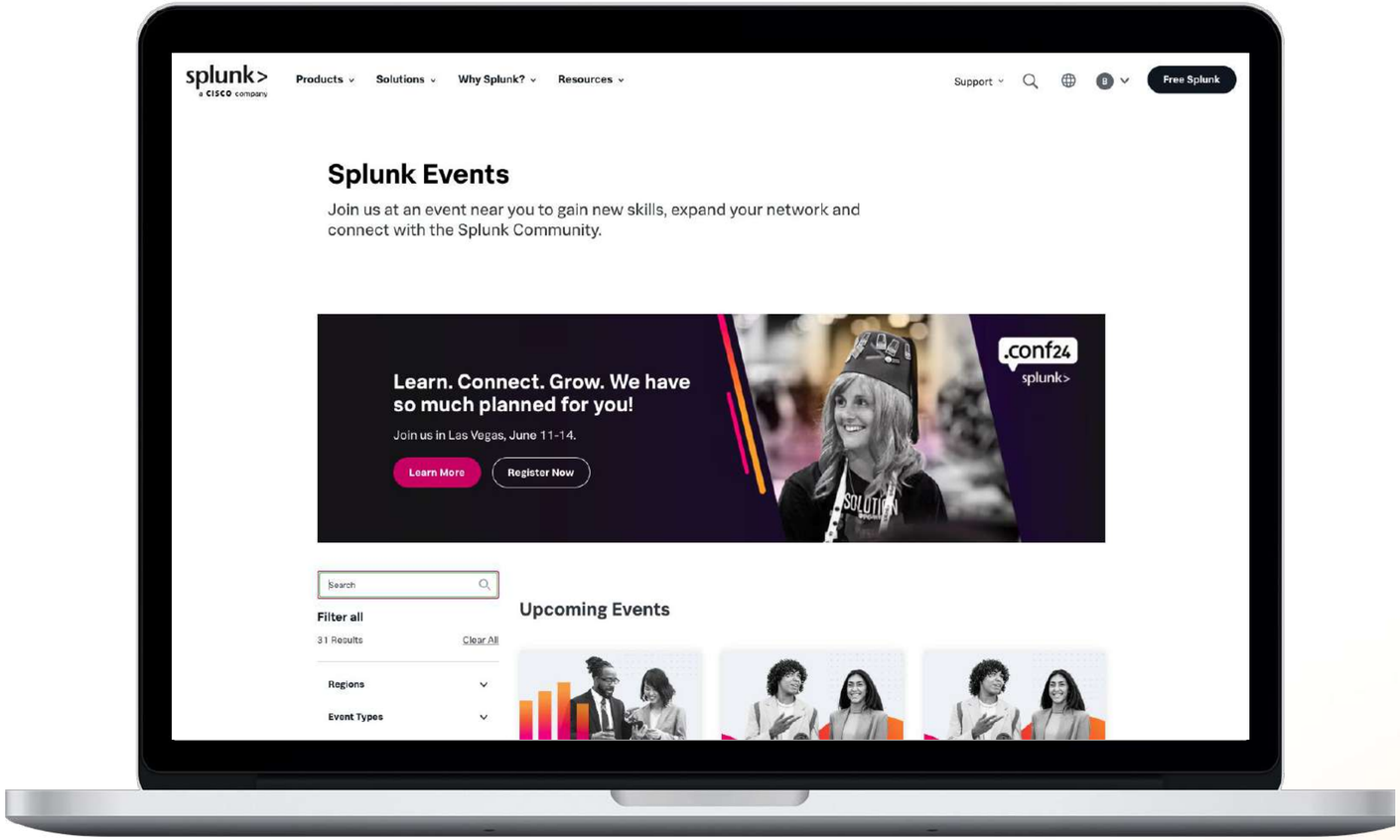
Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

Join us at .conf24!

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



Documentation

https://docs.splunk.com

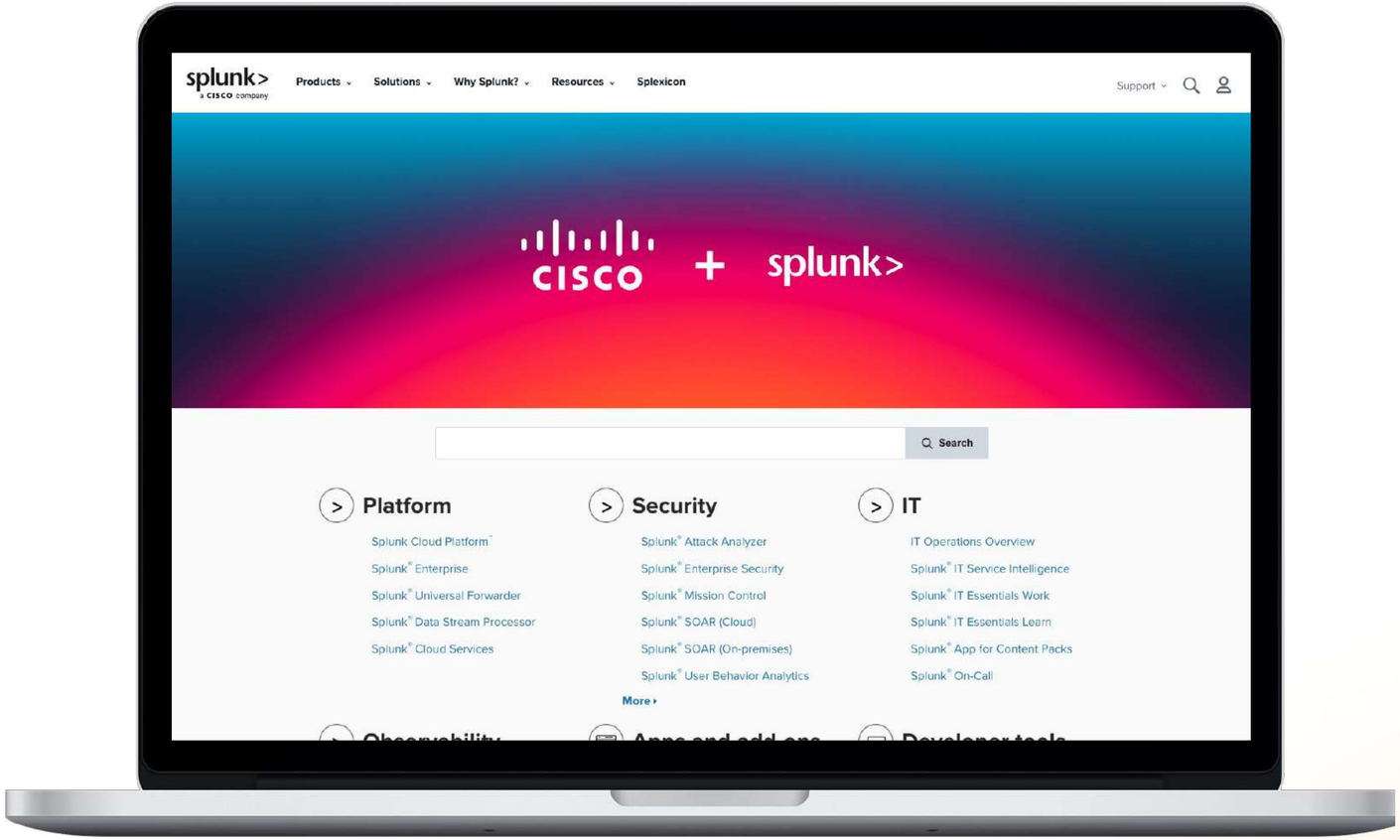
Search reference for SPL

Machine Learning
https://splk.it/3xcroUX

Product references

Procedures/guides

And more!



Splunk Lantern

https://lantern.splunk.com

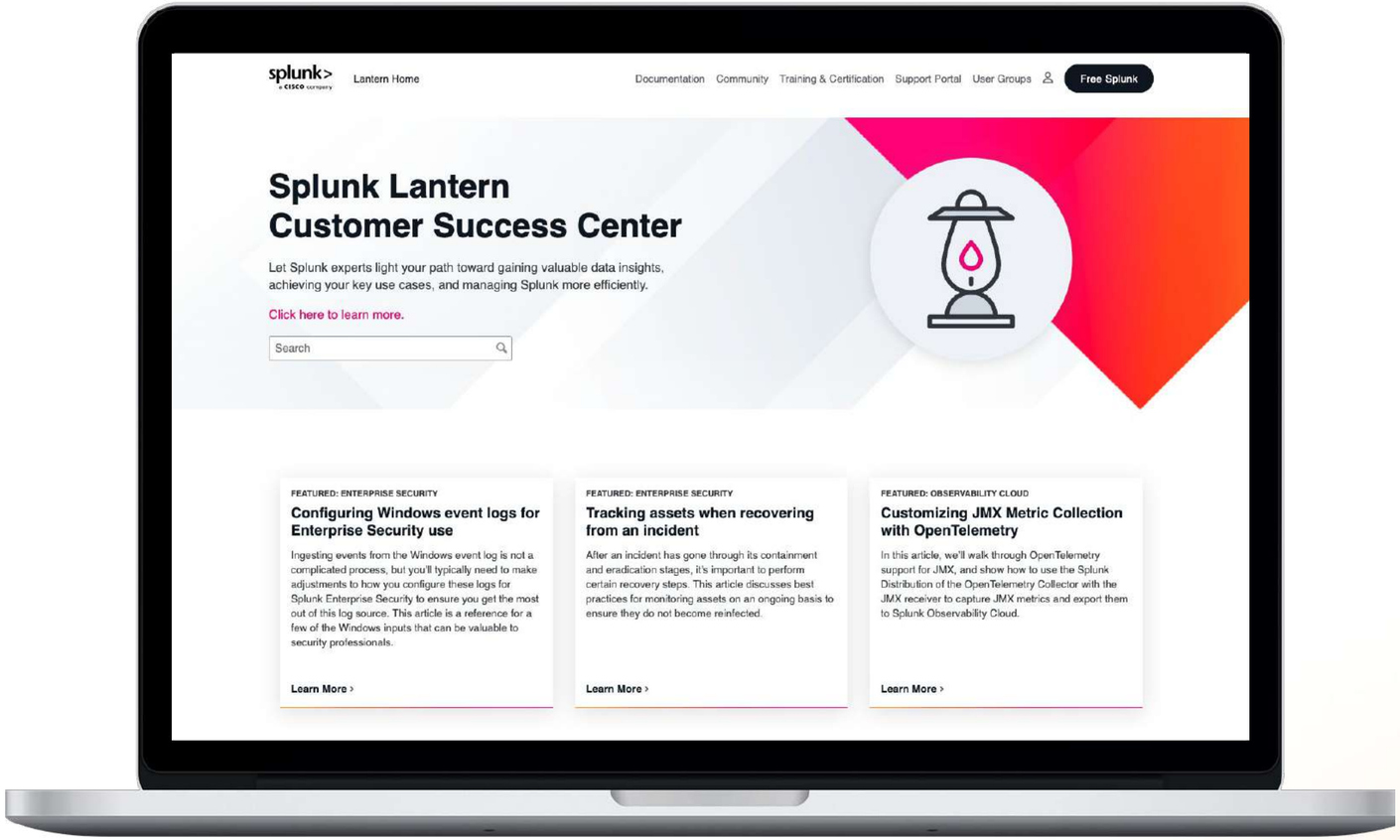
Use case library

Step-by-step procedures

Map use cases to data sources

Splunk Success Framework to realize value across your organisation

Machine Learning
https://splk.it/3TU9DCp



Developer Resources

https://dev.splunk.com

Developer Guide

API Reference

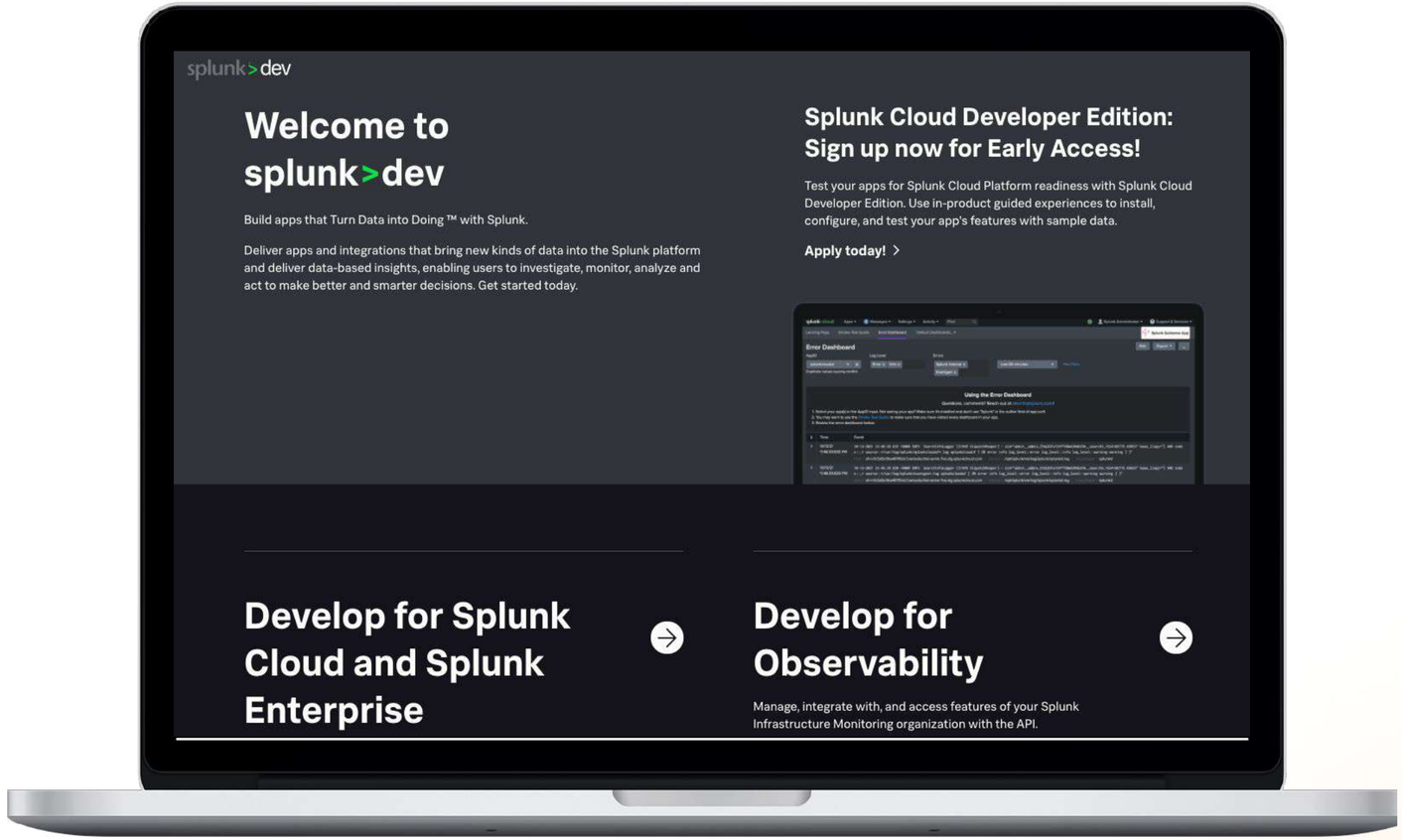
Tutorials

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/

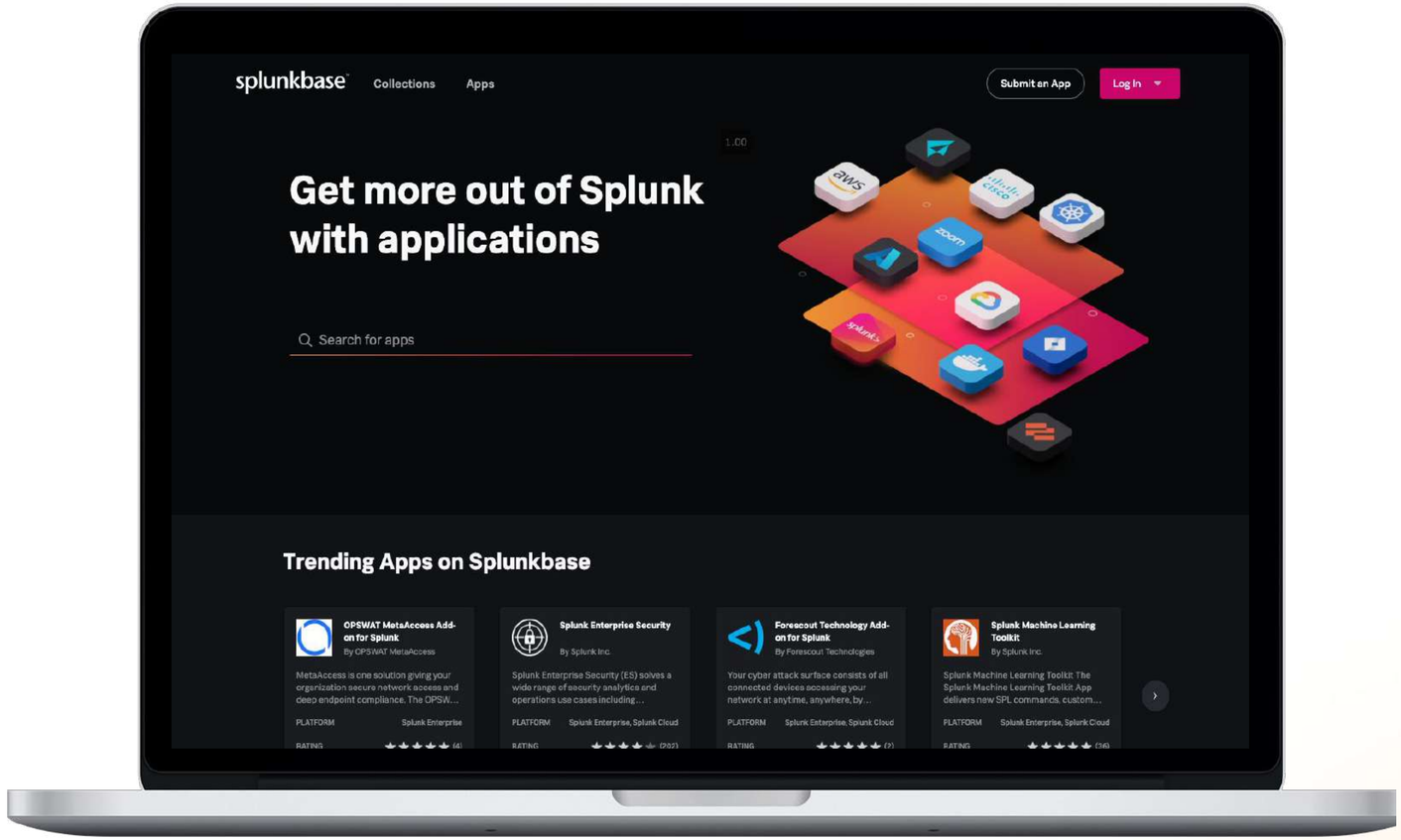
3200+ apps and add-ons

Pre-built searches, reports, visualisations and integrations

Splunk Machine Learning Toolkit (MLTK)
https://splk.it/3x67rPl

Python for Scientific Computing
https://splk.it/43C7kHy

Splunk App for Data Science and Deep Learning (DSDL)
https://splk.it/3VBuQm8



Training & Certification

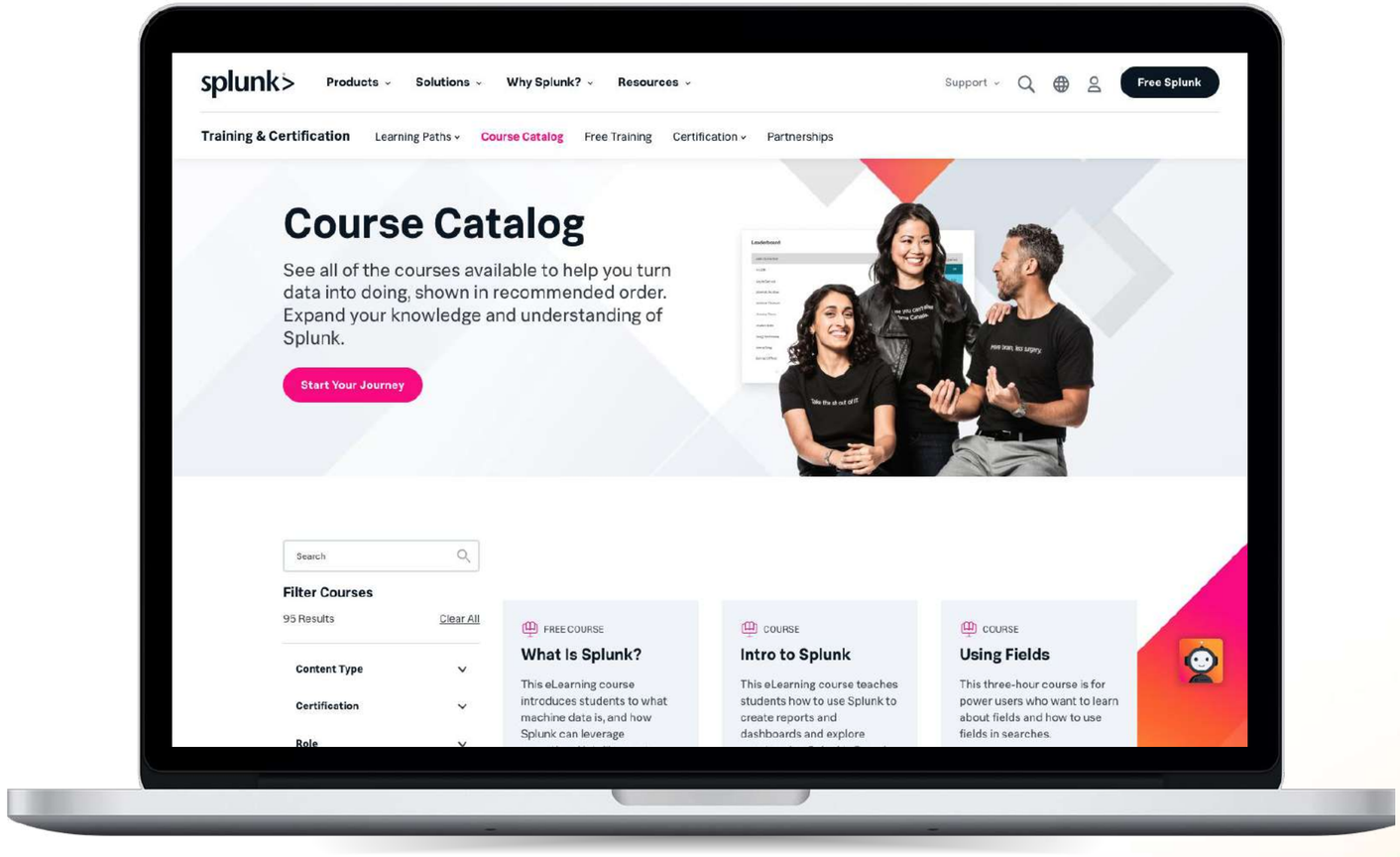
https://splunk.com/training

Online education classes
Instructor-led and self-paced eLearning

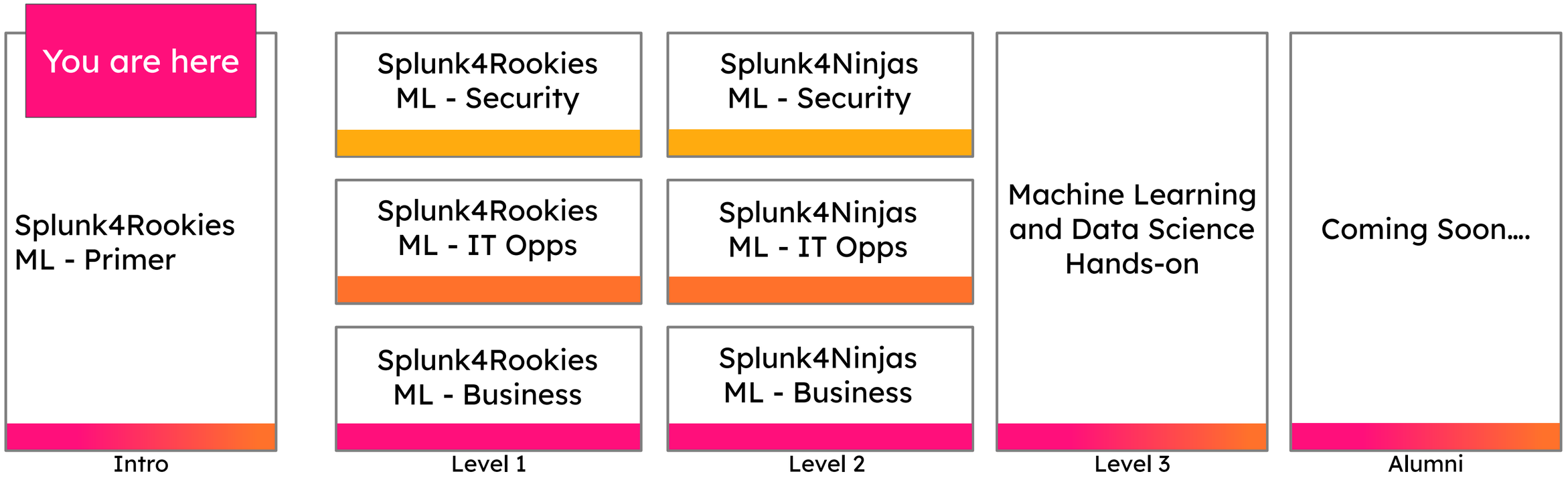
Certification tracks for different roles
User, Power User, Admin, Architect and Developer

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

Splunk for Analytics and Data Science
https://splk.it/43E7CxE



Splunk Machine Learning Workshops



Boss of Machine Learning (Coming Soon)

Introductory → **Advanced**

Legend

Security | IT Ops | Business | All

Thank you

splunk>