

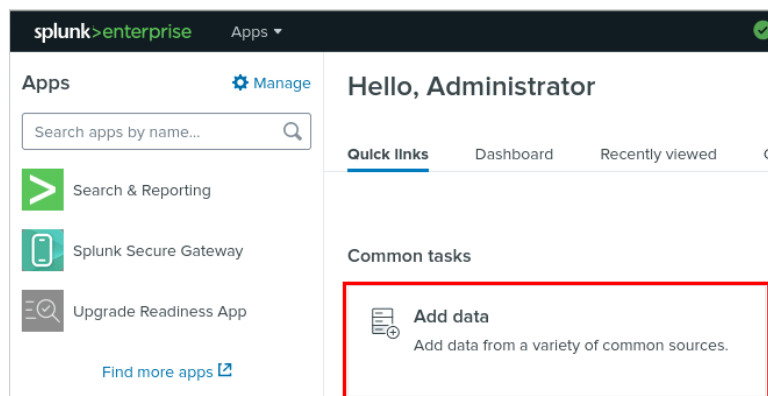
Basic Monitoring & Detection with Splunk Enterprise

For this lab, I'll be utilizing the Pluralsight virtual environment since an instance of Splunk is temporarily provided free of any extra charges. I will go through uploading data, performing searches, creating & sharing reports, and creating dashboards.


Table of Contents

Uploading Data (Traffic File).....	1
Performing Searches in Splunk	4
Create and Share Reports	7
Create Dashboards in Splunk	10
Utilizing Learned Skills to Create Another Report & Dashboard	14


Uploading Data (Traffic File)




What data do you want to send to the Splunk platform?



Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

Add Data


Select Source Input Settings Review Done

< Back

Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn](#)

 Preview is not supported for this archive file, but it can still be indexed.

Selected File: **tutorialdata (1).zip**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic

Select

New

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☐ Constant value

☐ Regular expression on path

☒ Segment in path

Segment number

splunk>enterprise

Apps

Administrator

1 Messages

Settings

Add Data

Select Source

Input Settings

Review

Done

< Back

Submit >

Review

Input Type Uploaded File

File Name tutorialdata (1).zip

Source Type Automatic

Host Source path segment number: 1

Index Default

Data Successfully Added:

New Search Save As ▾ Create Table View Close

source="tutorialdata (1).zip:*" All time ▾ 🔍

✓ 109,864 events (before 3/3/25 5:15:58.000 PM) No Event Sampling ▾ Job ▾ || ■ ↶ 📄 ⬇ 🔔 Smart Mode ▾

Events (109,864) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

✓ Format ▾ Show: 20 Per Page ▾ View: List ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 5 a source 8 a sourcetype 3 INTERESTING FIELDS # AcctID 100+ # bytes 100+ a clientip 100+ a Code 14 # date_hour 24 # date_mday 8 # date_minute 60 a date_month 1		>	2/8/24 6:24:02.000 PM	[08/Feb/2024:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = vendor_sales : source = tutorialdata (1).zip:/vendor_sales/vendor_sales.log : sourcetype = vendor_sales
		>	2/8/24 6:23:46.000 PM	[08/Feb/2024:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = vendor_sales : source = tutorialdata (1).zip:/vendor_sales/vendor_sales.log : sourcetype = vendor_sales
		>	2/8/24 6:23:31.000 PM	[08/Feb/2024:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = vendor_sales : source = tutorialdata (1).zip:/vendor_sales/vendor_sales.log : sourcetype = vendor_sales
		>	2/8/24 6:22:59.000 PM	[08/Feb/2024:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = vendor_sales : source = tutorialdata (1).zip:/vendor_sales/vendor_sales.log : sourcetype = vendor_sales
		>	2/8/24 6:22:48.000 PM	[08/Feb/2024:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = vendor_sales : source = tutorialdata (1).zip:/vendor_sales/vendor_sales.log : sourcetype = vendor_sales

Performing Searches in Splunk

Note: the AND operator is implied when a space is between two words. OR or NOT must be explicitly stated

Keyword Search:

New Search Save As ▾ Create Table View Close

buttercupgames error All time ▾ 🔍

✓ 427 events (before 3/3/25 5:18:52.000 PM) No Event Sampling ▾ Job ▾ || ■ ↶ 📄 ⬇ 🔔 Smart Mode ▾

Events (427) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column

✓ Format ▾ Show: 20 Per Page ▾ View: List ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 3 a source 3 a sourcetype 1 INTERESTING FIELDS a action 1 # bytes 100+ a clientip 100+ # date_hour 24 # date_mday 8 # date_minute 60 a date_month 1 # date_second 60		>	2/8/24 5:57:58.000 PM	12.130.60.5 - - [08/Feb/2024:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP 1.1" 200 1167 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232 host = www1 : source = tutorialdata (1).zip:/www1/access.log : sourcetype = access_combined_wcookie
		>	2/8/24 5:53:57.000 PM	64.66.0.20 - - [08/Feb/2024:17:53:57] "POST /cart/error.do?msg=NothingInCart&JSESSIONID=SD6SL4FF1ADFF52990 HTTP 1.1" 200 420 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-27" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 521 host = www2 : source = tutorialdata (1).zip:/www2/access.log : sourcetype = access_combined_wcookie
		>	2/8/24 5:44:02.000 PM	74.53.23.135 - - [08/Feb/2024:17:44:02] "POST /cart/error.do?msg=CreditNotAccepted&JSESSIONID=SD8SL10FF9ADFF52956 HTTP 1.1" 200 3531 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-12" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 839 host = www3 : source = tutorialdata (1).zip:/www3/access.log : sourcetype = access_combined_wcookie

Next click all fields to get to the next step below

Adding a Field

New Search Save As ▾ Create Table View Close

buttercupgames error All event ▾ 🔍

✓ **427 events** (before 3/3/25 5:18:52.000 PM) No Event Sampling ▾ Job ▾ || ■ → 📎 ⬇ 🔔 Smart Mode ▾

Events (427) Patterns Statistics

Timeline format ▾ Zoom Out

Hide Fields All Fields

SELECTED FIELDS

- `a clientip` 100+
- `a host` 3
- `a source` 3
- `a sourcetype` 1

INTERESTING FIELDS

- `a action` 1
- `# bytes` 100+
- `# date_hour` 24
- `# date_mday` 4
- `# date_minute` 60
- `a date-month` 1

clientip ×

>100 Values, 100% of events Selected Yes No

Reports

- Top values
- Top values by time
- Rare values
- Events with this field

Top 10 Values

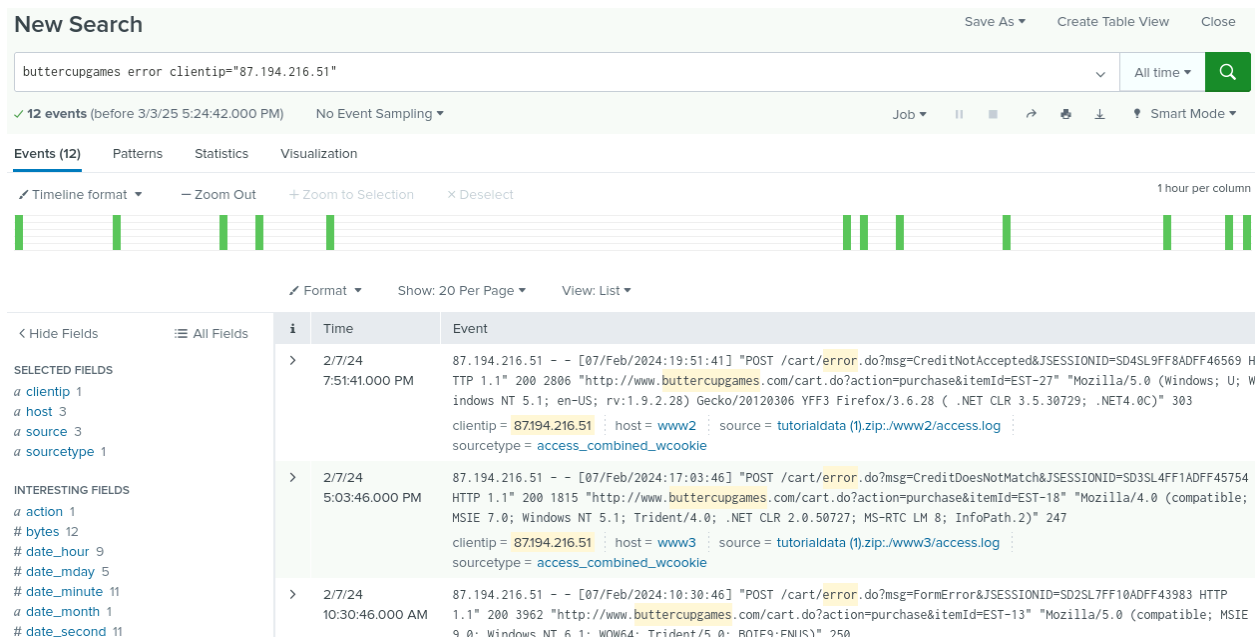
Value	Count	%
87.194.216.51	12	2.81%
90.205.111.169	8	1.874%
128.241.220.82	7	1.639%
198.35.1.10	7	1.639%
211.166.11.101	7	1.639%
97.117.230.183	7	1.639%
187.231.45.62	6	1.405%
108.65.113.83	5	1.171%
117.21.246.164	5	1.171%
192.188.106.240	5	1.171%

Timeline view: 1 day per column

Timeline view: 1 2 3 4 5 6 7 8 ... Next >

Log entries (partial):

- `g="CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP`
- `purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE`
- `http://www1/access.log : sourcetype = access_combined_wcookie`
- `"=NothingInCart&JSESSIONID=SD6SL4FF1ADFF52990 HTTP 1.1"`
- `&itemId=EST-27" "Mozilla/5.0 (Macintosh; Intel Mac OS`
- `84.46 Safari/536.5" 521`
- `http://www2/access.log :`
- `g="CreditNotAccepted&JSESSIONID=SD8SL10FF9ADFF52956 HT`
- `purchase&itemId=EST-12" "Mozilla/5.0 (Windows NT 6.1;`
- `46 Safari/536.5" 839`



Transformational Search:

Note: This is a type of search that uses transformational commands - these are command that take events returned in a search and convert them into numerical values that Splunk can use for statistical purposes. Transformational commands include: chart, timechart, stats, top, rare, contingency, and highlight.

Breakdown of search arguments:

- `sourcetype=access_* status=200 action=purchase` filters out all events that have a status code of 200 and an action of purchase.
- `|` takes the output of the first part of the command and forwards it to the second part of our command, which is the transformational command.
- `top categoryId` searches the output of the first portion of the command and returns all `categoryIds`, ranked in descending order.

Search: sourcetype=access_* status=200 action=purchase | top categoryId

New Search Save As Create Table View Close

sourcetype=access_* status=200 action=purchase | [top](#) categoryId All time 🔍

✓ **5,224 events** (before 3/3/25 5:28:55.000 PM) No Event Sampling Job ⏏ 🔄 🖨 ⬇ 🔔 Smart Mode

Events Patterns **Statistics (7)** Visualization

Show: 20 Per Page 🔧 Format 🔘 Preview: On

categoryId	count	percent
STRATEGY	806	30.495649
ARCADE	493	18.653046
TEE	367	13.885736
ACCESSORIES	348	13.166856
SIMULATION	246	9.307605
SHOOTER	245	9.269769
SPORTS	138	5.221339

Create and Share Reports

New Search Save As Create Table View Close

sourcetype=access_* status=200 action=purchase | [top](#) categoryId All time 🔍

✓ **5,224 events** (before 3/3/25 5:33:37.000 PM) No Event Sampling Job ⏏ 🔄 🖨 ⬇ 🔔 Smart Mode

Events Patterns **Statistics (7)** Visualization

Show: 20 Per Page 🔧 Format 🔘 Preview: On

Report
Alert
Existing Dashboard
New Dashboard
Event Type

Save As Report ✕

Title

Description

Content 📊 Statistics Table

Time Range Picker Yes No

Cancel Save

Click save then view to get here:

Most popular categories

Highest Ranked CategoryIds

All time ▾

✓ 5,224 events (before 3/3/25 5:33:37.000 PM)

7 results 20 per page ▾

categoryId ▴	count ▴	percent ▴
STRATEGY	806	30.495649
ARCADE	493	18.653046
TEE	367	13.885736
ACCESSORIES	348	13.166856
SIMULATION	246	9.307605

Edit ▾

More Info ▾

Add to Dashboard ▾

Open In Search

Edit Description

Edit Permissions

Edit Schedule

Edit Acceleration

Clone

Embed

Delete

Edit Permissions

×

Report Most popular categories

Owner admin

App search

Display For Owner App All apps

Run As Owner User

[Learn More](#)

	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
splunk_system_upgrader	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets **Reports** Alerts Dashboards Search & Reporting

Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

filter This app's 8 Reports 20 per page 1 of 1 pages

i	Title	Actions	Next scheduled time	Owner	App	Sharing	Status
>	Bucket Merge Retrieve Conf Settings	Open in search Edit	None	nobody	search	App	Enabled
>	Errors in the last 24 hours	Open in search Edit	None	nobody	search	App	Enabled
>	Errors in the last hour	Open in search Edit	None	nobody	search	App	Enabled
>	License Usage Data Cube	Open in search Edit	None	nobody	search	App	Enabled
>	Messages by minute last 3 hours	Open in search Edit	None	nobody	search	App	Enabled
▼	Most popular categories	Open in search Edit	None	admin	search	App	Enabled

Highest Ranked CategoryIds

Creator Created by Search.
 App search
 Schedule Not scheduled.
 Actions 0 Actions
 Acceleration Disabled
 Permissions Shared in app. Owned by admin.
 Modified March 3, 2025 5:37:30 PM
 Embedding Disabled.

Will create a data visualization with this search (select All time along with this query)
 sourcetype=access_* status=200 action=purchase | top limit=10 clientip

New Search Save As Create Table View Close

sourcetype=access_* status=200 action=purchase | top limit=10 clientip All time

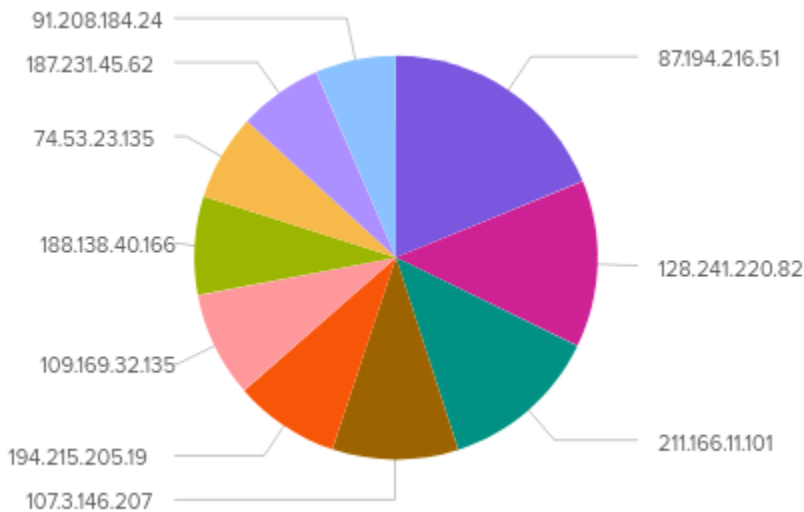
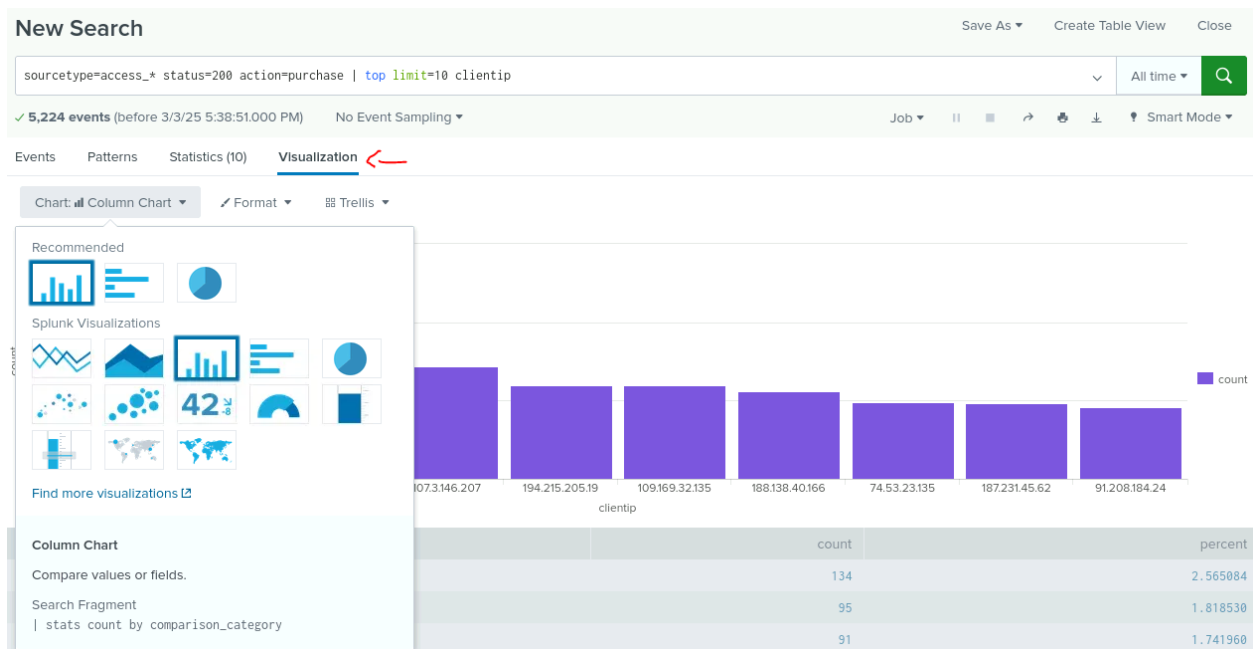
✓ 5,224 events (before 3/3/25 5:38:51.000 PM) No Event Sampling Job Visualization

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page Format Preview: On

clientip	count	percent
87.194.216.51	134	2.565084

Within Visualizations, you may customize the chart



Create Dashboards in Splunk

First run the search `sourcetype=access_* status=200 action=purchase`. This will bring up all the results related to purchases made on the web application. Then click “All fields”.

Select “date_mday”, “date_month”, and “Itemid”.

Select Fields

Select All Within Filter Deselect All Coverage: 1% or more ▾ Filter + Extract New Fields

i	✓ ▾	Field ▾	# of Values ▾	Event Coverage ▾	Type ▾
>	<input checked="" type="checkbox"/>	clientip	>100	100%	String
>	<input checked="" type="checkbox"/>	host	3	100%	String
>	<input checked="" type="checkbox"/>	source	3	100%	String
>	<input checked="" type="checkbox"/>	sourcetype	1	100%	String
>	<input type="checkbox"/>	JSESSIONID	>100	100%	String
>	<input type="checkbox"/>	action	1	100%	String
>	<input type="checkbox"/>	bytes	>100	100%	Number
>	<input type="checkbox"/>	categoryid	7	50.59%	String
>	<input type="checkbox"/>	date_hour	24	100%	Number
>	<input type="checkbox"/>	date_mday ←	8	100%	Number
>	<input type="checkbox"/>	date_minute	60	100%	Number
>	<input type="checkbox"/>	date_month ←	1	100%	String
>	<input type="checkbox"/>	date_second	60	100%	Number
>	<input type="checkbox"/>	date_wday	7	100%	String
>	<input type="checkbox"/>	date_year	1	100%	Number
>	<input type="checkbox"/>	date_zone	1	100%	String

Utilizing the extra fields, we will run a search to outline the most sold items grouped by `itemid`. `sourcetype=access_* status=200 action=purchase | top itemid`. Next we will save this search as a dashboard.

New Search

Save As ▾ Create Table View Close

sourcetype=access_* status=200 action=purchase | top itemid

✓ 5,224 events (before 3/3/25 6:18:41.000 PM) No Event Sampling ▾ Job

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Report
Alert
Existing Dashboard
New Dashboard
Event Type

Itemid ▾	count ▾	percent ▾
EST-15	407	7.790965
EST-14	399	7.637825
EST-21	398	7.618683
EST-26	382	7.312404
EST-6	376	7.197550
EST-7	373	7.140123
EST-12	373	7.140123

Save Panel to New Dashboard



Dashboard Title

Top Item Purchases

top_item_purchases

Edit ID

Description

Optional

Permissions

Private

How do you want to build your dashboard?

[What's this?](#)

Classic Dashboards

The traditional Splunk dashboard builder

Dashboard Studio

NEW

A new builder to create visually-rich, customizable dashboards

Panel Title

Optional

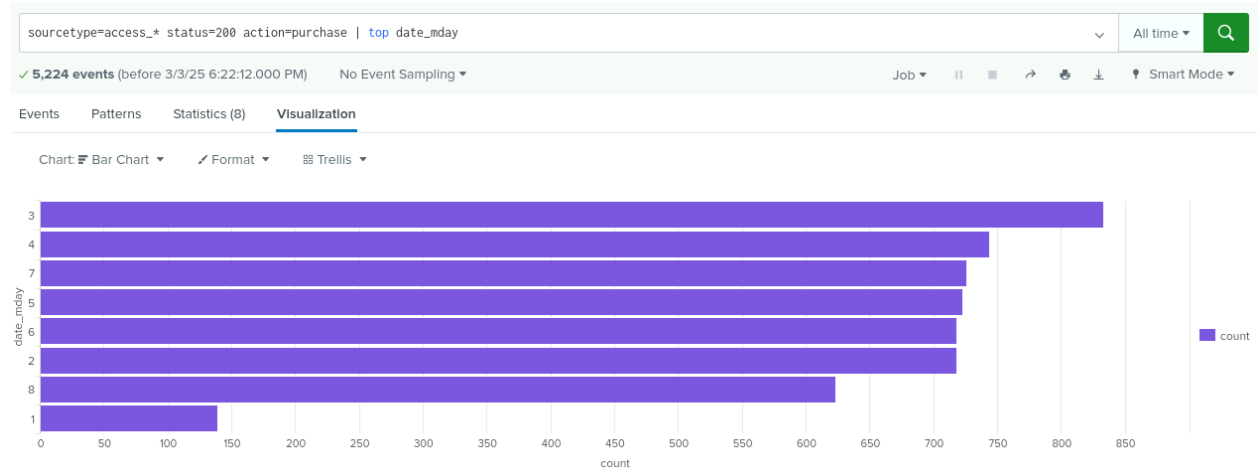
Visualization Type

Statistics Table

Cancel

Save to Dashboard

Close the dashboard creation pop-up to return to the **Search** page. Enter the following search: `sourcetype=access_* status=200 action=purchase | top date_mday`. Then go to the **Visualization** tab and change it to a **Bar Chart**.



Next, we'll save this as an existing dashboard, select the **Top Item Purchases** dashboard, click **Save to Dashboard** then click **View Dashboard**.

Save Panel to Existing Dashboard

Select an Existing Dashboard

Sort: Title (A - Z) ↓

Search By Title

integrity check of installed files

Job Details Dashboard

jQuery Upgrade

Orphaned Scheduled Searches, Reports, and Alerts

Scheduled export is now available for Dashboard Studio

✓ Top Item Purchases

Panel Title

Optional

Visualization Type

Bar Chart

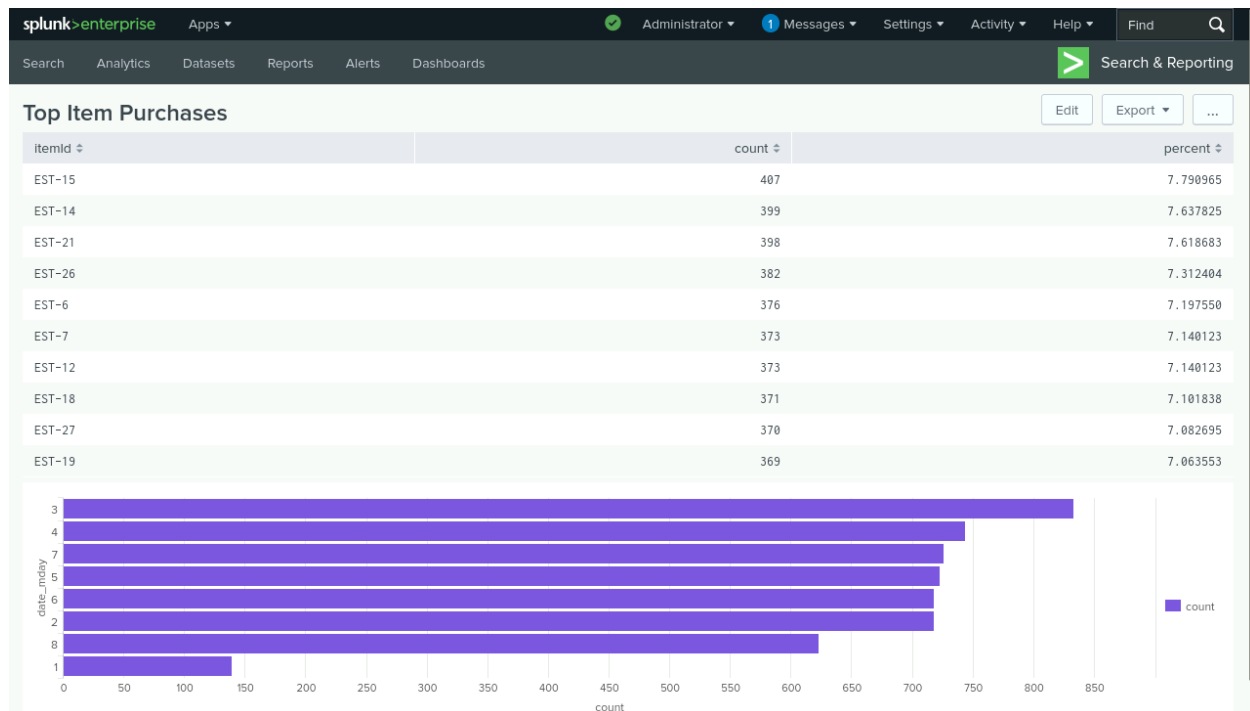
Statistics Table

> Advanced Panel Settings

Cancel

Save to Dashboard

Here is the Dashboard view:



Utilizing Learned Skills to Create Another Report & Dashboard

Failed purchase attempts by IP address:

sourcetype=access_* status=200 action=purchase error | top clientip

New Search

Save AsCreate Table ViewClose

sourcetype=access_* status=200 action=purchase error | top clientip

All time

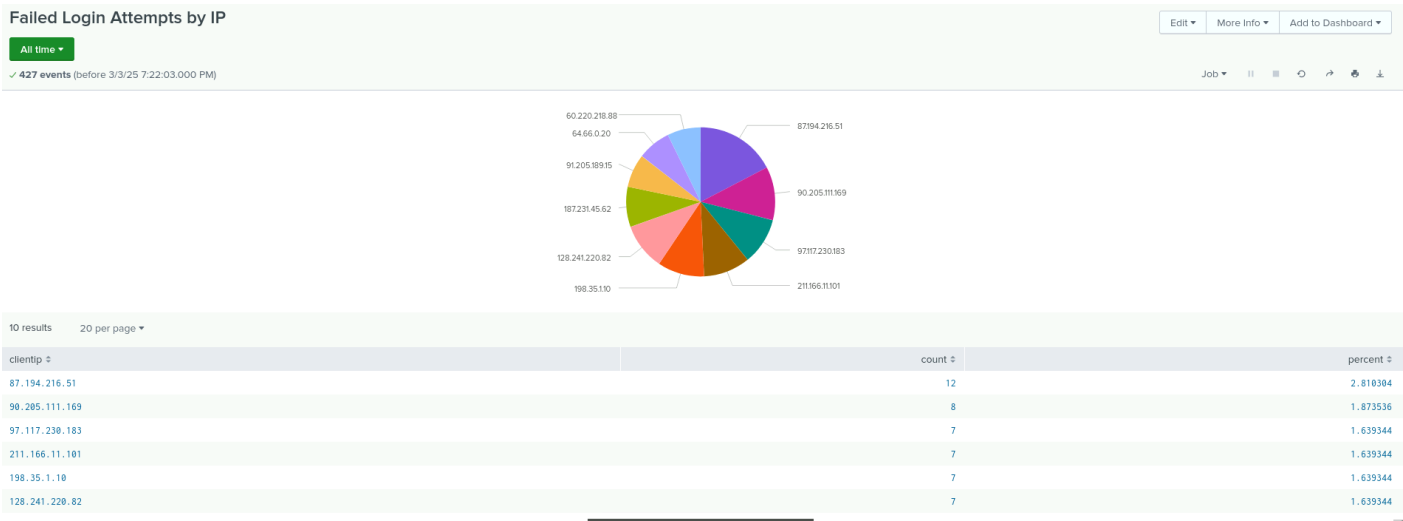
✓ 427 events (before 3/3/25 7:16:20.000 PM)No Event SamplingJob

EventsPatternsStatistics (10)Visualization

Show: 20 Per PageFormatPreview: On

clientip	count	percent
87.194.216.51	12	2.810304
90.205.111.169	8	1.873536
97.117.230.183	7	1.639344
211.166.11.101	7	1.639344
198.35.1.10	7	1.639344
128.241.220.82	7	1.639344
187.231.45.62	6	1.405152
91.205.189.15	5	1.170960
64.66.0.20	5	1.170960
60.220.218.88	5	1.170960

Report Below:



Dashboard Below:

