carahsoft splunk>

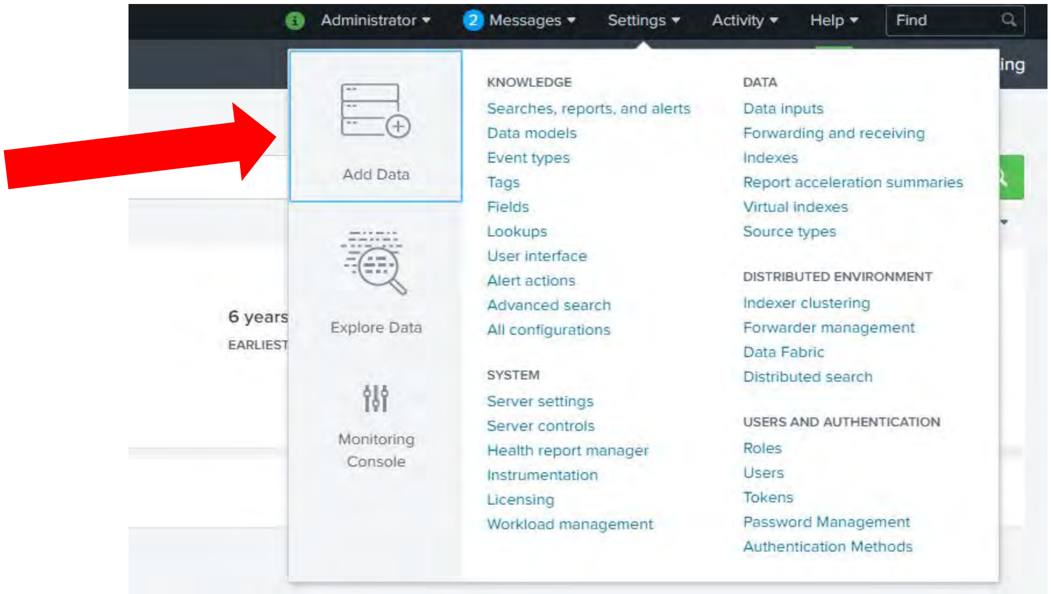
Windows IT Operations Instructions

This session will be focusing on manipulating data dealing with IT Operations within Windows data. This can also be relevant to any IT operations data within your environment but we want to show you the variety of different dashboards and visualizations you can create and customize.

*** Before we get started, make sure you received the email we sent out with the **WindowsITOps.csv** file included. If you did not, let us know and we will send you this file.***

Adding Data

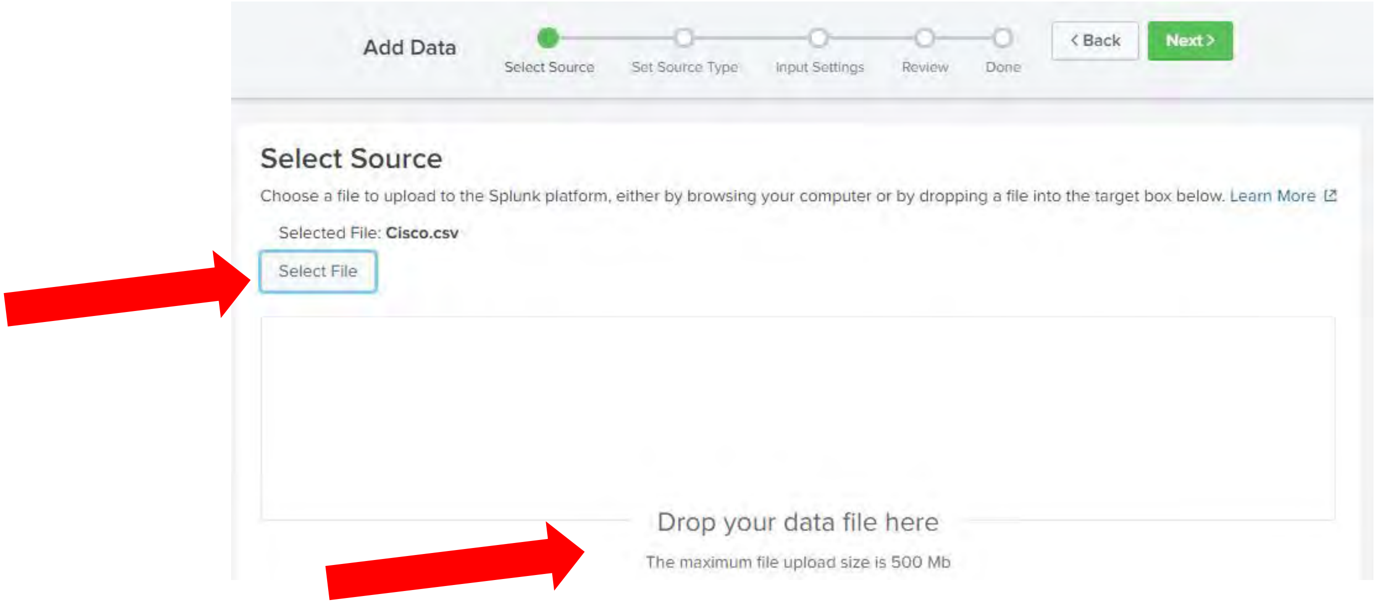
1. In your Splunk instance, make sure you are in the default **Searching & Reporting App**. In the top right corner, Select **Settings,** and from there Click on the "**Add Data**" as shown below:



2. From there, you will see a screen asking which method you would like to get data in by.
    a. Select the **Upload** option

The first part of uploading data is '*Select the Source*'.

3. Here we can either select the "**Select File"** option or we can simply drag the **WindowsITOps.csv** file directly into the box. If you select the **"Select File"** option, it will prompt you to find the current location of this file.



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 More

Selected File: **Cisco.csv**

Drop your data file here

The maximum file upload size is 500 Mb

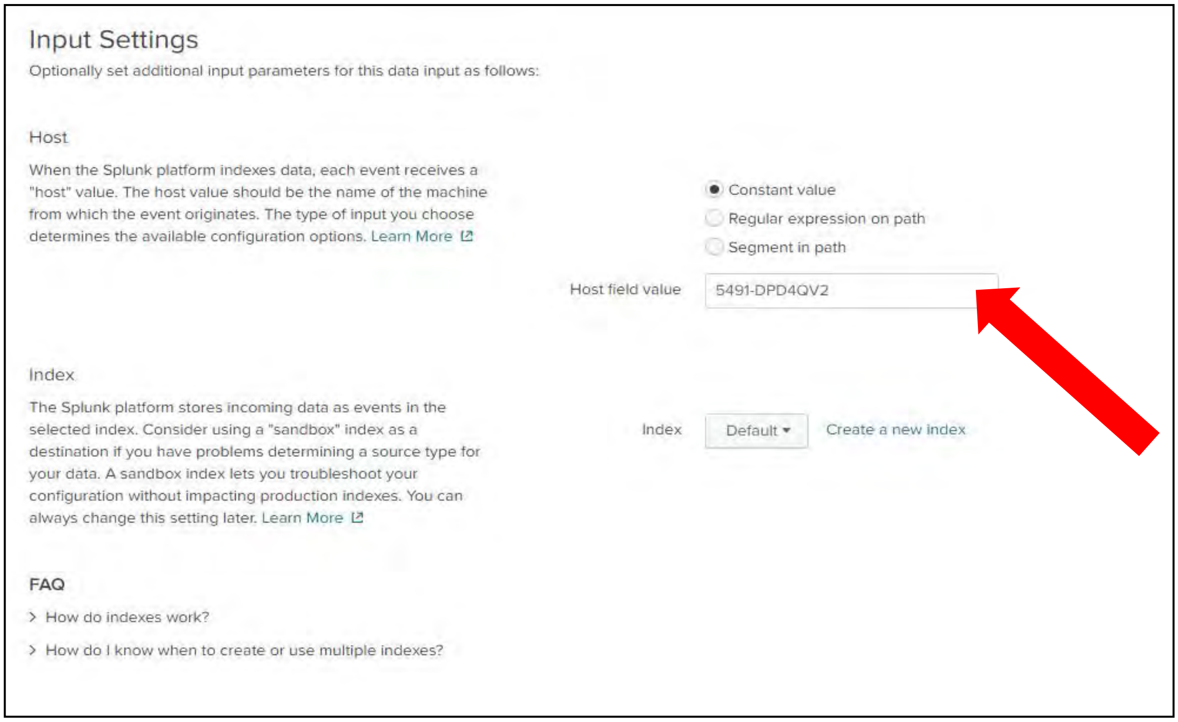
4. Select "**Next"** when file is completely done uploading.
5. In this next stage, **Select Source Type**, Splunk will automatically determine the source type of the data that is being uploaded. If the type is not known, you can manually tell Splunk what it is. But for now, **we will keep it as-is**
    a. You can also edit the **Timestamp, Delimited Settings, and Advanced** settings here
        i. Splunk will usually be able to extract fields automatically but sometimes it cannot do that. When you look at the **Timestamp** setting, you can change how Splunk extracts this field from the incoming data. You can use a current time of ingest, an advanced setting for extracting, you can configure another file to tell you this information, or lastly have splunk automatically extract it.

ii. Next is the **Delimited Setting.** Splunk again can usually automatically find when one event ends and another begins. With this setting, we can

help Splunk in telling which character is the determining factor or event breaks.

iii. Lastly we have the **Advanced** settings. This is where we can add addition event characteristic needed to properly extract your data. For example, if we know for a fact that events should merge over multiple lines. We can set **SHOULD_LINEMERGE** to **true** to merge the lines into a single event.

6. Select **"Next"** again.
7. Now you should be in the **Input Settings**
   a. We are going to keep the Host field as it is
   b. For **Index,** we are going to **Create a new index**
      iv. *This is a best practice for separating your data. You can later set different privileges for different indexes, meaning certain people can, or cannot, have access to certain indexes*



Input Settings

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

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

Host field value: 5491-DPD4QV2

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾ Create a new index

FAQ

> How do indexes work?

> How do I know when to create or use multiple indexes?

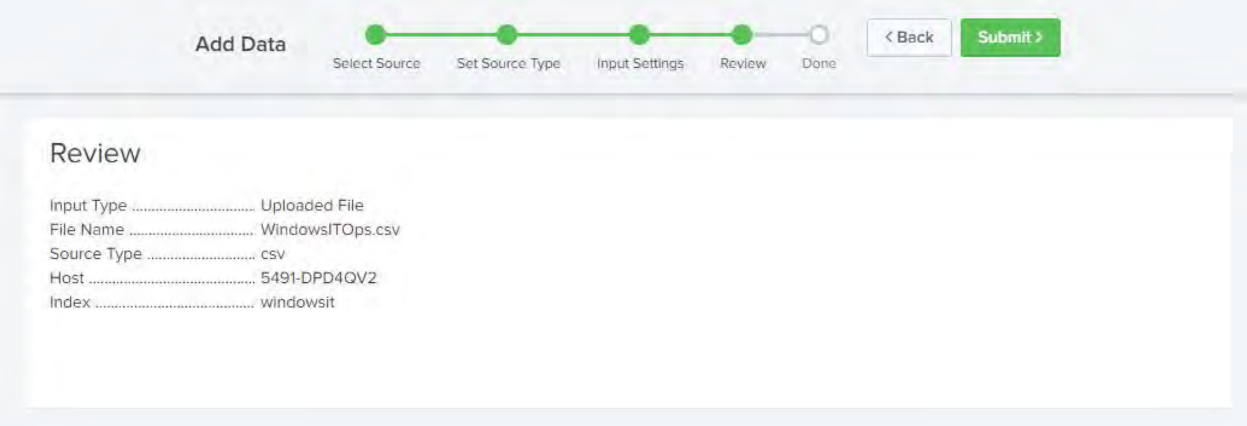
c. **Index Name:** WindowsIT

d. **Make sure the **App** is set to **Search and Report**

e. **Save**

f. Make sure that *Index* is now selected in the **Input Settings** page

8. Lastly, the **Review** Page. It should match the below capture (other than the Host

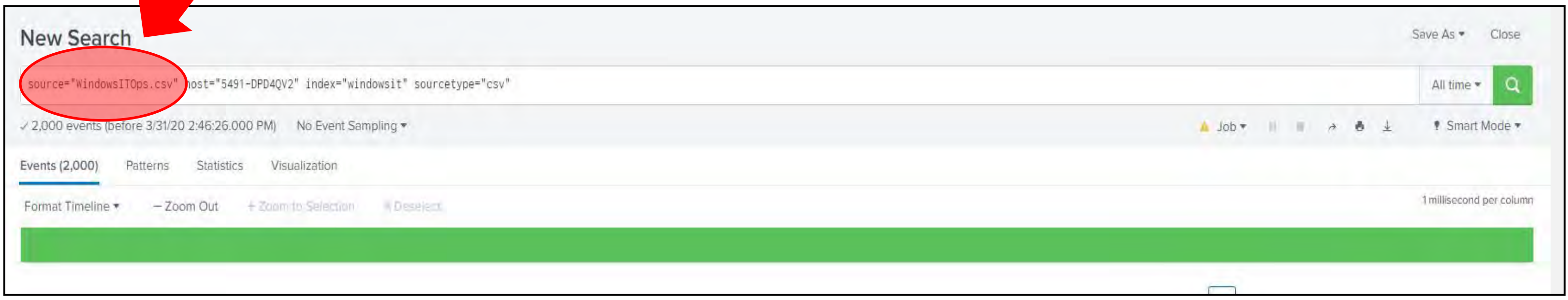


Review

Input Type .... Uploaded File
File Name .... WindowsITOps.csv
Source Type .... csv
Host 5491-DPD4QV2
Index .... windowsit

value)

9. Select “**Submit**” and now we want to make sure we did everything right by selecting **Start Searching**.
    a. Splunk should automatically populate a search for you and you should find **2,000 Events** populated



New Search

```
source="WindowsITOps.csv" host="5491-DPD4QV2" index="windowsit" sourcetype="csv"
```

✓ 2,000 events (before 3/31/20 2:46:26.000 PM)

Now that we have uploaded our data, we are going to want to make this data easier to look at. From here, we are going to create a dashboard with different visualizations to show you what Splunk can do with your data. We are only going to get into a very small portion of what Splunk is able to do with your data but some more examples include:

- App Uptime
- Reduce Downtime
- Continuous Threat Remediation
- More…

Let’s look at the different fields that we have on the left-hand side (Interesting Fields). Splunk has automatically detected and extracted these fields so that you can easily reference them in queries. In order for a field to be considered an “Interesting Field”, it

must show up in your

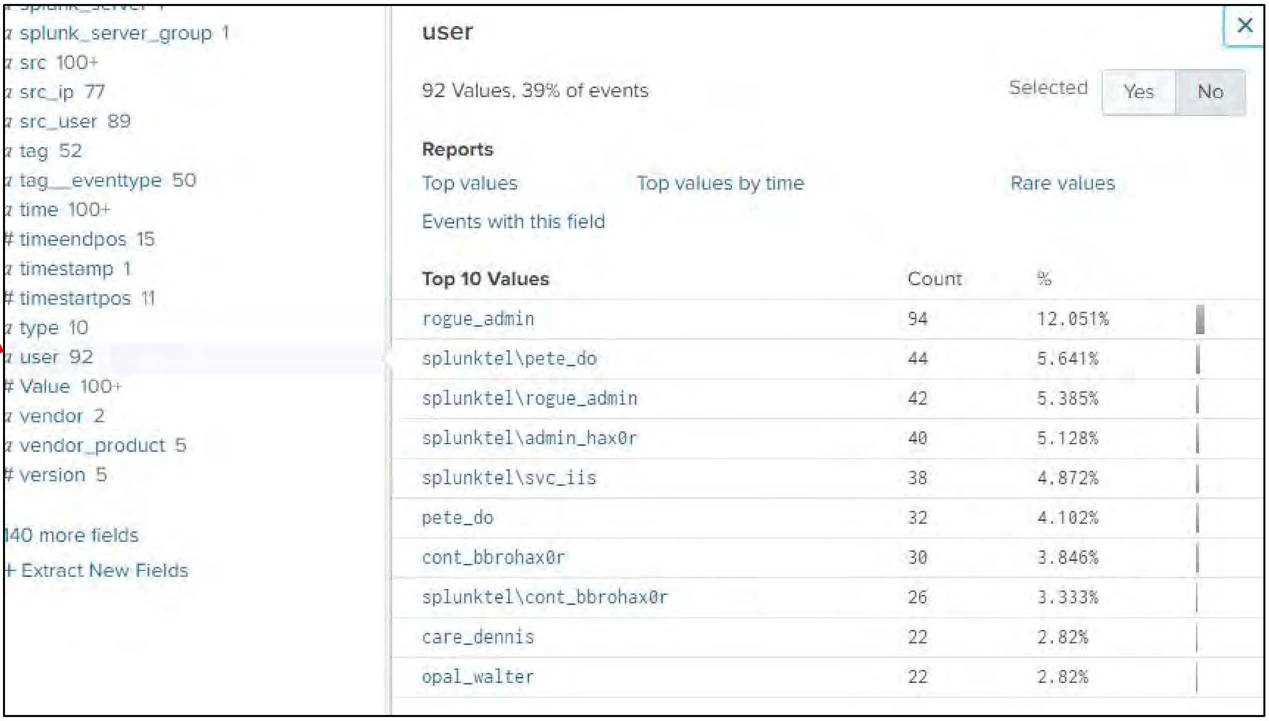
data 20% if the time. For example, there is anything from action, to product, to source.

What we want to do it make all of this information useful to us by finding correlations.

Rogue Admin Actions

First, let’s look at the different **Users**. This fields tells us which users are active within this

dataset. The values should show as followed:



a splunk_server_group	1
a src	100+
a src_ip	77
a src_user	89
a tag	52
a tag__eventtype	50
a time	100+
# timeendpos	15
a timestamp	1
# timestartpos	11
a type	10
a user	92
# Value	100+
a vendor	2
a vendor_product	5
# version	5

140 more fields

+ Extract New Fields

user

92 Values, 39% of events

Selected: Yes [✓ No]

Reports

Top values   Top values by time   Rare values

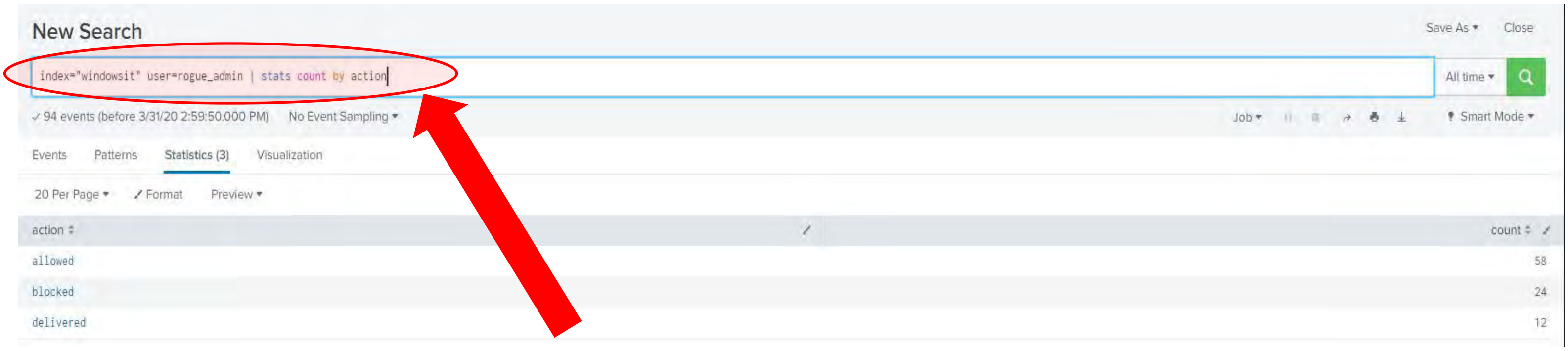
Events with this field

Top 10 Values	Count	%
rogue_admin	94	12.051%
splunktel\pete_do	44	5.641%
splunktel\rogue_admin	42	5.385%
splunktel\admin_hax0r	40	5.128%
splunktel\svc_iis	38	4.872%
pete_do	32	4.102%
cont_bbrohax0r	30	3.846%
splunktel\cont_bbrohax0r	26	3.333%
care_dennis	22	2.82%
opal_walter	22	2.82%

Here we can see we have a ‘**rogue_admin’** as our most active user (sorry for the name

being so blunt). Obviously in your data, a rogue user will not have that exact name but this is just an example of how Splunk can automatically extract the different fields and values which allows us to create dashboards or alerts from these values.

1. In the search bar, enter **<u>index="windowsit" user=rogue_admin | stats count by action</u>**
    a. You should see results similar to the below:

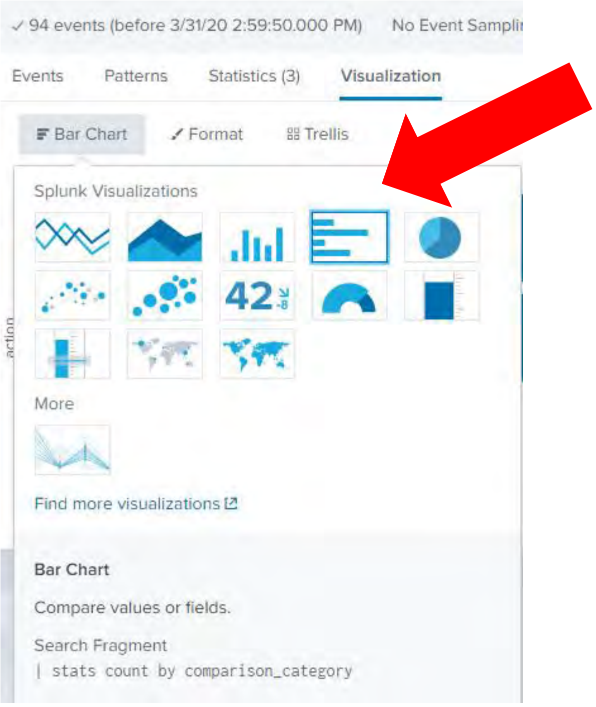


```
index="windowsit" user=rogue_admin | stats count by action
```

✓ 94 events (before 3/31/20 2:59:50.000 PM)

action	count
allowed	58
blocked	24
delivered	12

2. Select **Visualization**
    a. Here we can see some of the visualizations you can use with your data. You can add more visualizations with the ‘Find more visualizations’ which we will do later. For this we are going to use a **Bar Chart** for this specific search



✓ 94 events (before 3/31/20 2:59:50.000 PM) No Event Sampli

Events Patterns Statistics (3) Visualization

Bar Chart ✓ Format Trellis

Splunk Visualizations

42

More

Find more visualizations

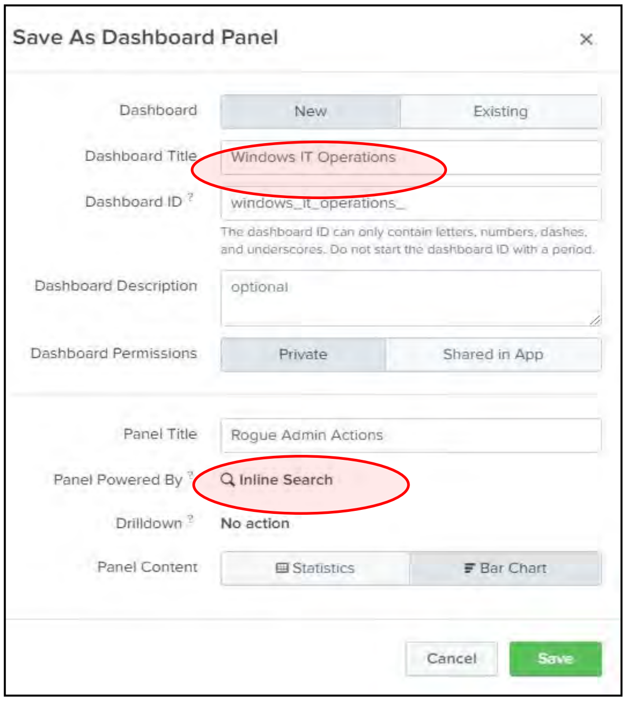
Bar Chart

Compare values or fields.

Search Fragment

```
| stats count by comparison_category
```

3. Now we want to save this as a Dashboard Panel. In the top right corner, near the search icon, Select **Save As** dropdown
   a. Select **Dashboard Panel**
   b. Keep **"New"** Selected
   c. **Dashboard Title** is **Windows IT Operations**
   d. Keep Dashboard ID, Dashboard Description, and Dashboard Permissions as-is
   e. **Panel Title** is going to be **Rogue Admin Actions**



Save As Dashboard Panel ×

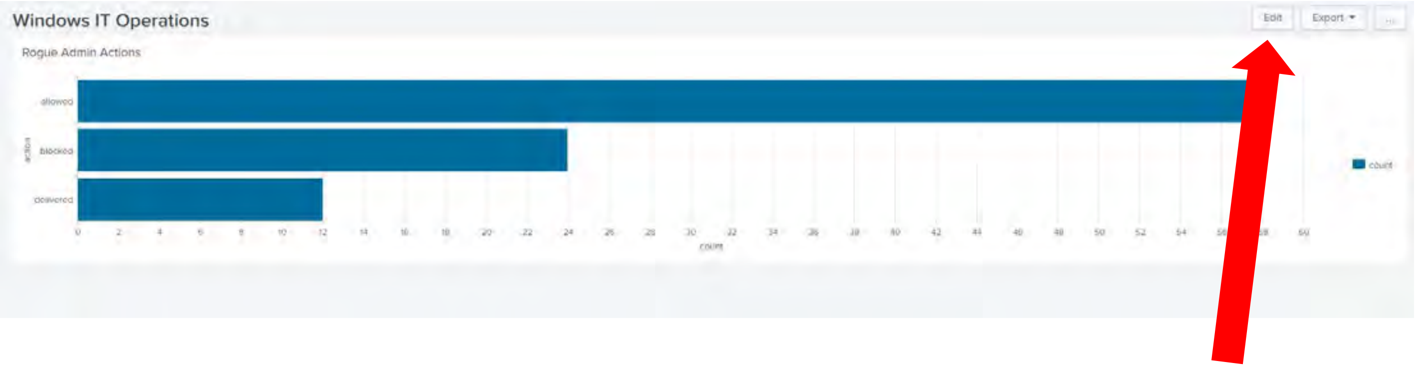
Dashboard	New / Existing
Dashboard Title	Windows IT Operations
Dashboard ID ?	windows_it_operations_
	The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.
Dashboard Description	optional
Dashboard Permissions	Private / Shared in App
Panel Title	Rogue Admin Actions
Panel Powered By ?	Inline Search
Drilldown ?	No action
Panel Content	Statistics / Bar Chart

Cancel Save

f. Finally, select **Save**

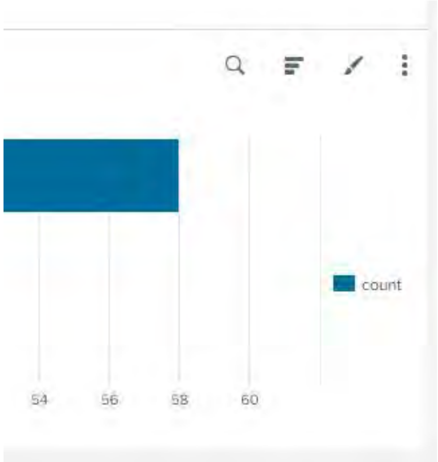
4. Let's View this Dashboard to see what we created.

   a. It should look as seen below:



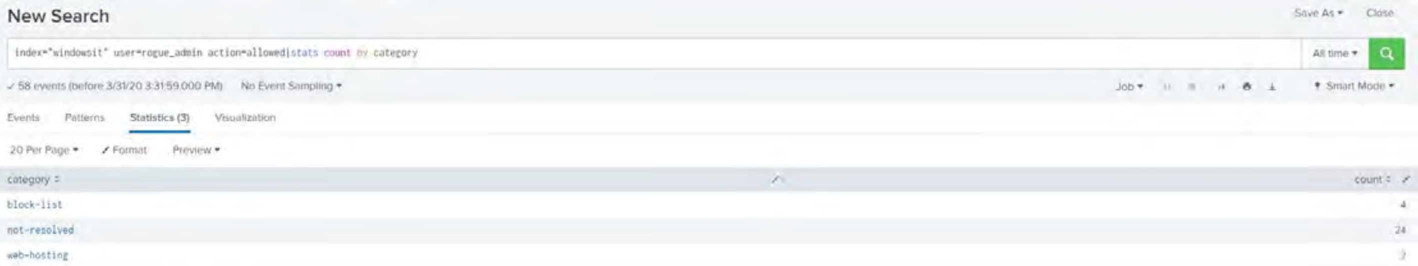
5. We are now going to edit the drilldown for this chart now. A drilldown is a tool used to share additional data insight when a user clocks on a data point, or table row, or other visualization element. So first we are going to select **Edit** on the top right of the dashboard

6. Now select the Three Vertical Dots on the right side of the chart we created



7. Select **Edit Drilldown.**
8. "**On Click**" we are going to change the value of **No action** to **Link to search**
9. Select **Custom**
10. Erase the Search String and replace it with:
    a. *index="windowsit" user=rogue_admin action=$row.action$ | stats count by category*

11. Make sure the **Time Range** is at **All time**
12. Now if we click on one of the bars on the graph, it should send us to a new search which should look like the following:



```
index="windowsit" user=rogue_admin action=allowed|stats count by category
```

✓ 58 events (before 3/31/20 3:31:59.000 PM) No Event Sampling ▾

category	count
block-list	4
not-resolved	24
web-hosting	2

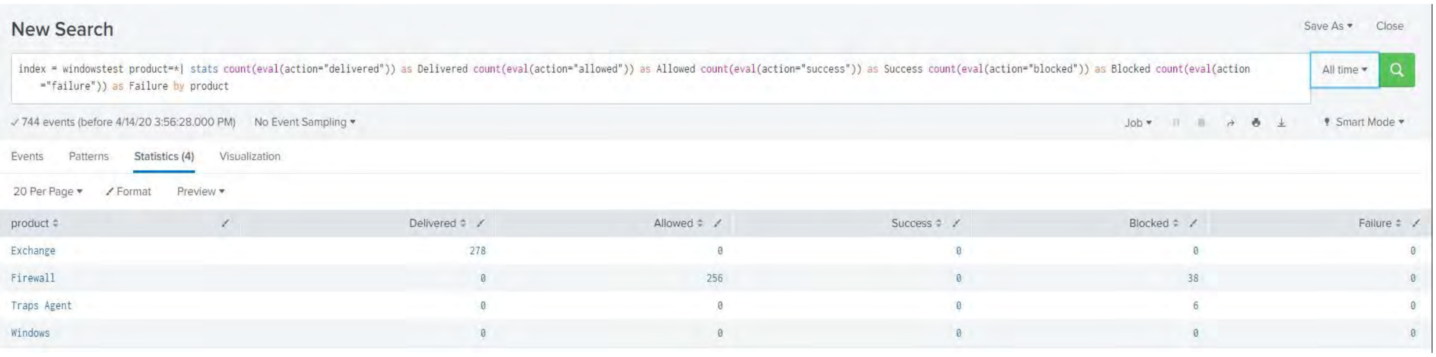
Action by Product

Now let's looks take a look at the different actions that are taking place within our Windows data and sort it out by the different Windows products. This could be useful to see if one product is not allowing any access or is allowing too much access.

1. In the search bar, enter:

index = windowsit product=*| stats count(eval(action="delivered")) as Delivered count(eval(action="allowed")) as Allowed count(eval(action="success")) as Success count(eval(action="blocked")) as Blocked count(eval(action="failure")) as Failure by product

** The ‘as’ field is for renaming purposes and the ‘eval’ field is showing Splunk which aspect of the product field to specifically look at**



```
index = windowstest product=*| stats count(eval(action="delivered")) as Delivered count(eval(action="allowed")) as Allowed count(eval(action="success")) as Success count(eval(action="blocked")) as Blocked count(eval(action
    ="failure")) as Failure by product
```

✓ 744 events (before 4/14/20 3:56:28.000 PM) No Event Sampling ▾

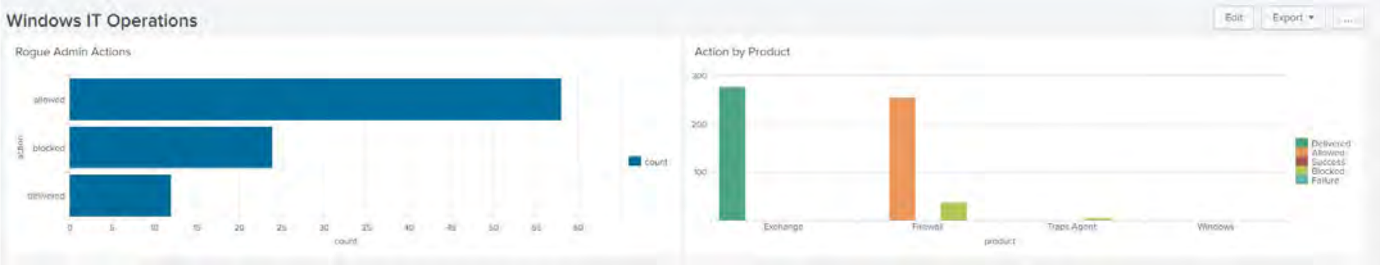
product	Delivered	Allowed	Success	Blocked	Failure
Exchange	278	0	0	0	0
Firewall	0	256	0	38	0
Traps Agent	0	0	0	6	0
Windows	0	0	0	0	0

2. Select **Visualization**
    a. Select *Column Chart*
3. **Save as**
    a. **Dashboard Panel**

   i. **Existing → Windows IT Operations**

   ii. Panel Title → **Action by Product**

4. Now you should have two charts with the Rogue Admin Actions on the top. Select **Edit** on the top right of the dashboard and re-arrange the charts to be side-by-side (Click and drag the dotted lines to make the charts side-by-side). Below is what the result to be:



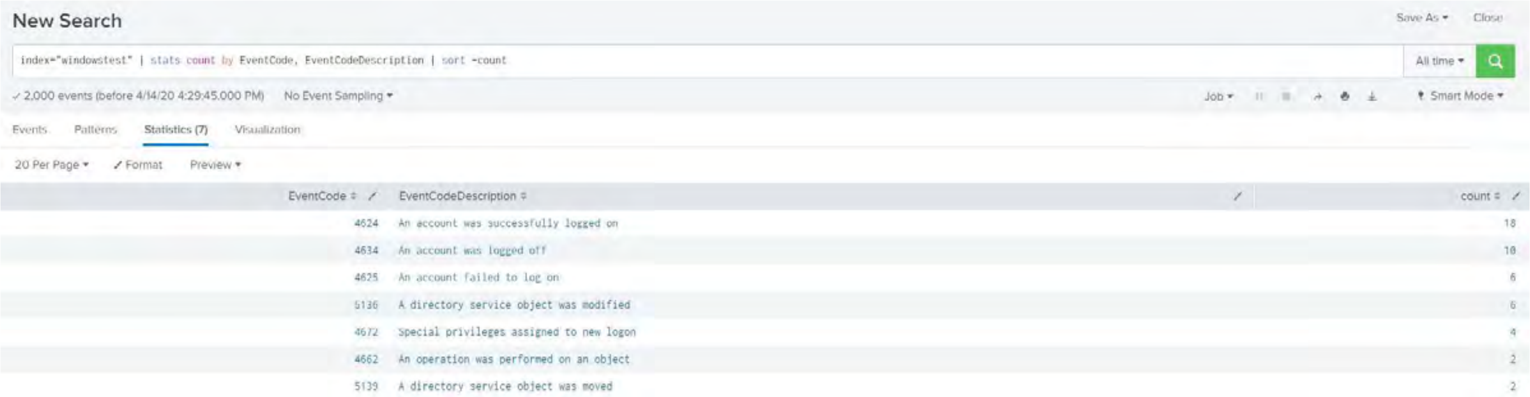
Event Code Descriptions

This chart is going to show you how splunk can help you see correlations within your data which will help you better understand exactly what your data is trying to tell you. Splunk is able to automatically extract fields with most sourcetypes and find correlated information within your data. In this chart, we are going to show you how you can add this aspect to a dashboard.

1. In your search bar, enter:

index="windowsit" | stats count by EventCode, EventCodeDescription | sort – count

a. What this search is doing is extracting all the Event Codes and telling us exactly what they are and how many times they appear. This could be extremely useful and can save you the time of looking up what every Event Code means.



New Search

```
index="windowstest" | stats count by EventCode, EventCodeDescription | sort -count
```

✓ 2,000 events (before 4/14/20 4:29:45.000 PM) No Event Sampling ▾

EventCode	EventCodeDescription	count
4624	An account was successfully logged on	18
4634	An account was logged off	10
4625	An account failed to log on	6
5136	A directory service object was modified	6
4672	Special privileges assigned to new logon	4
4662	An operation was performed on an object	2
5139	A directory service object was moved	2

2. For this search, we are actually going to leave it as-is, without a visualization. This is because this chart is already showing exactly what we need to see and we do not want to over-complicate this.
3. Select **Save As** and save it to our **Windows IT Operations** with the Panel Title of **Event Code Description**

Available Mbytes

For this chart, we are going to look at the available memory space we have. This is obviously something that is very important when trying to be proactive with your data.

1. In your search bar, enter:

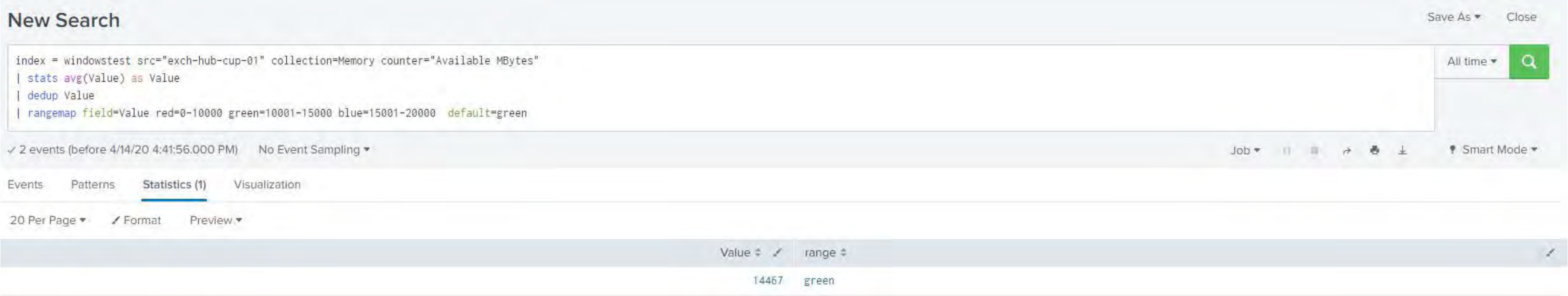
<u>index = windowstest src="exch-hub-cup-01" collection=Memory counter="Available MBytes"</u>

<u>| stats avg(Value) as Value</u>

<u>| dedup Value</u>

<u>| rangemap field=Value red=0-10000 green=10001-15000 blue=15001-20000 default=green</u>

** ‘dedup’ command is deleting any duplicate values



```
index = windowstest src="exch-hub-cup-01" collection=Memory counter="Available MBytes"
| stats avg(Value) as Value
| dedup Value
| rangemap field=Value red=0-10000 green=10001-15000 blue=15001-20000  default=green
```

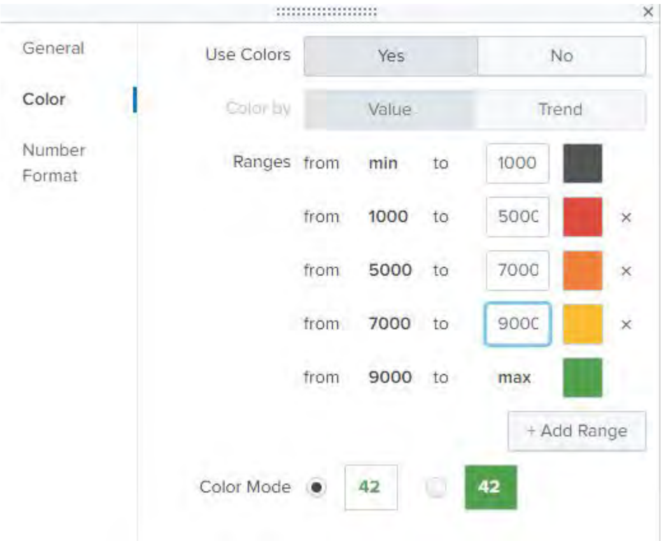
✓ 2 events (before 4/14/20 4:41:56.000 PM)   No Event Sampling ▾

Value	range
14467	green

- As you can see there is a ‘range = green’. We defined this in the search at the very bottom in the ‘rangemap’ command. You can customize this to whatever values seem fit.

2. Select **Visualization → Single Value**

3. Here we can add colors to the number (or single value) itself based on either the ‘range’ you can set or the actual value of the number. Select **Format** and fill in the information as shown below:



Use Colors: Yes [✓] | No

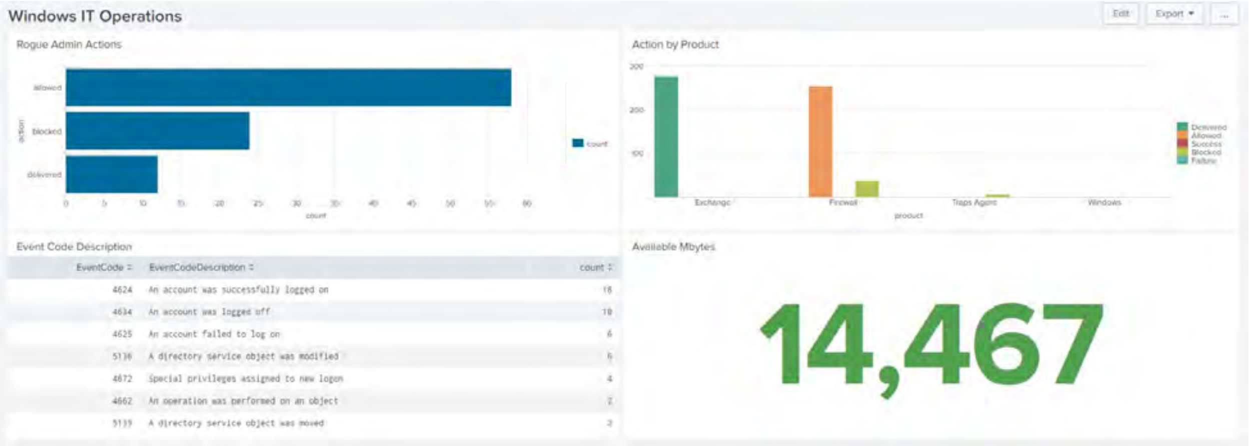
Color by: Value [✓] | Trend

Ranges					
from	min	to	1000	⬛	
from	1000	to	5000	🟥	×
from	5000	to	7000	🟧	×
from	7000	to	9000	🟨	×
from	9000	to	max	🟩	

Color Mode ● 42 ○ 42

4. Now you can save this to our existing dashboard with the Panel Title **Available Mbytes**

5. **Edit** your dashboard to look like the following:



Event Code Description

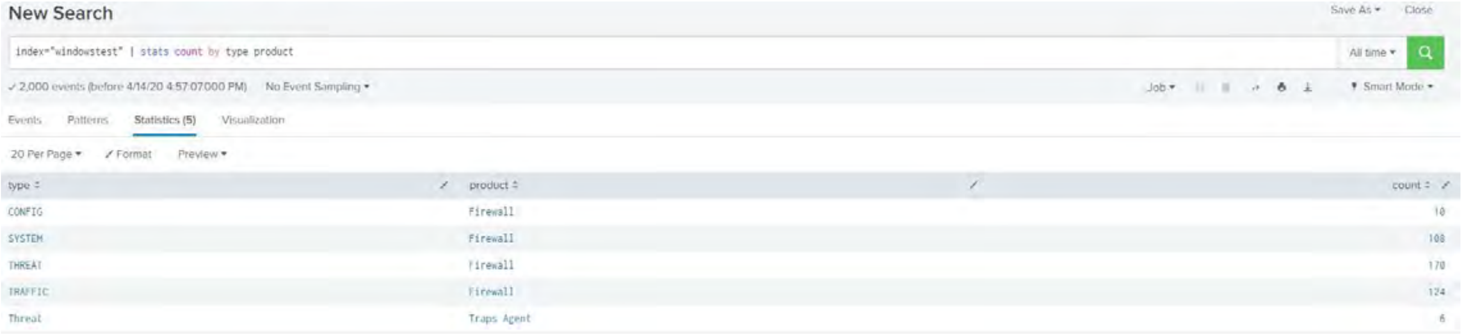
EventCode	EventCodeDescription	count
4624	An account was successfully logged on	18
4634	An account was logged off	10
4625	An account failed to log on	6
5136	A directory service object was modified	6
4672	Special privileges assigned to new logon	4
4662	An operation was performed on an object	2
5139	A directory service object was moved	2

Type of Action by Product

The next chart we are going to create is one of the more unique and visually-pleasing charts within Splunk. The Parallel Coordinates visualization is great for finding correlations, root-cases, and many more use-cases within your data. For this workshop, we are going to look at the types of actions by product with the count of each.

1. In your search bar, enter:

<u>**index="windowsit" | stats count by type product**</u>



```
index="windowstest" | stats count by type product
```

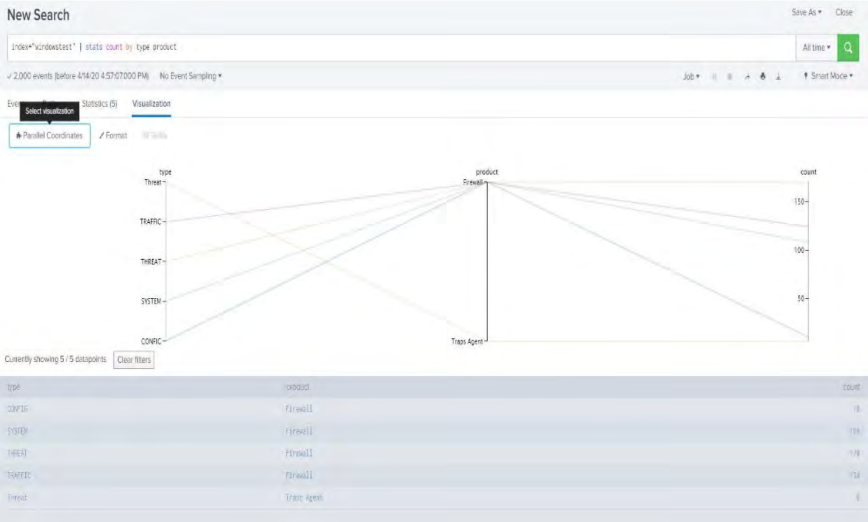
✓ 2,000 events (before 4/14/20 4:57:07.000 PM) No Event Sampling ▾

type	product	count
CONFIG	Firewall	10
SYSTEM	Firewall	108
THREAT	Firewall	170
TRAFFIC	Firewall	124
Threat	Traps Agent	6

2. **Visualization → find more visualizations**
3. In the Search bar in the top left corner, enter **Parallel Coordinates**
    a. **Download this apps**

i. **This may prompt you to enter your Splunk credentials

4. Now in our original search, Select the visualization you just downloaded



New Search

```
index="windowstest" | stats count by type product
```

✓ 2,000 events (before 4/14/20 4:57:07.000 PM) No Event Sampling ▾

Currently showing 5 / 5 datapoints

type	product	count
CONFIG	Firewall	10
SYSTEM	Firewall	108
THREAT	Firewall	178
TRAFFIC	Firewall	124
Threat	Traps Agent	6

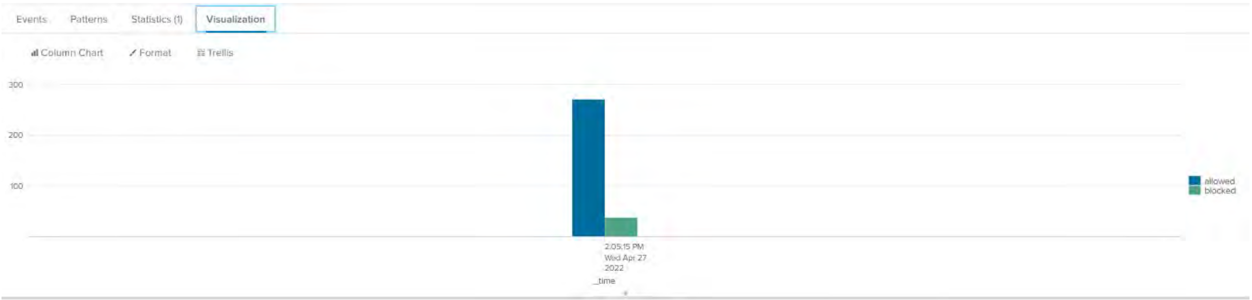
5. Save this to our Dashboard with the Panel Name **Type of Action by Product**

Utilizing Splunkbase

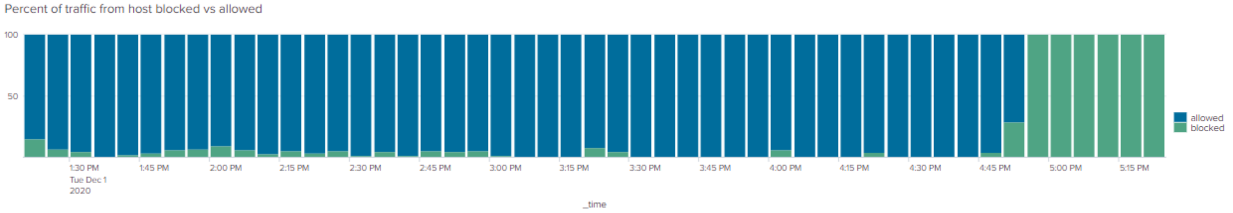
Splunk has thousands of applications available on Splunkbase, where you can find predefined searches, visualizations, and dashboards. This last visualization will be using a search from IT Essentials Learn. This is a free app containing searches for a variety of different IT use cases.

This search is for detecting blocked traffic from a host. It can determine if outbound traffic from a host is being dropped at the firewall and easily determine when the traffic blocking began.

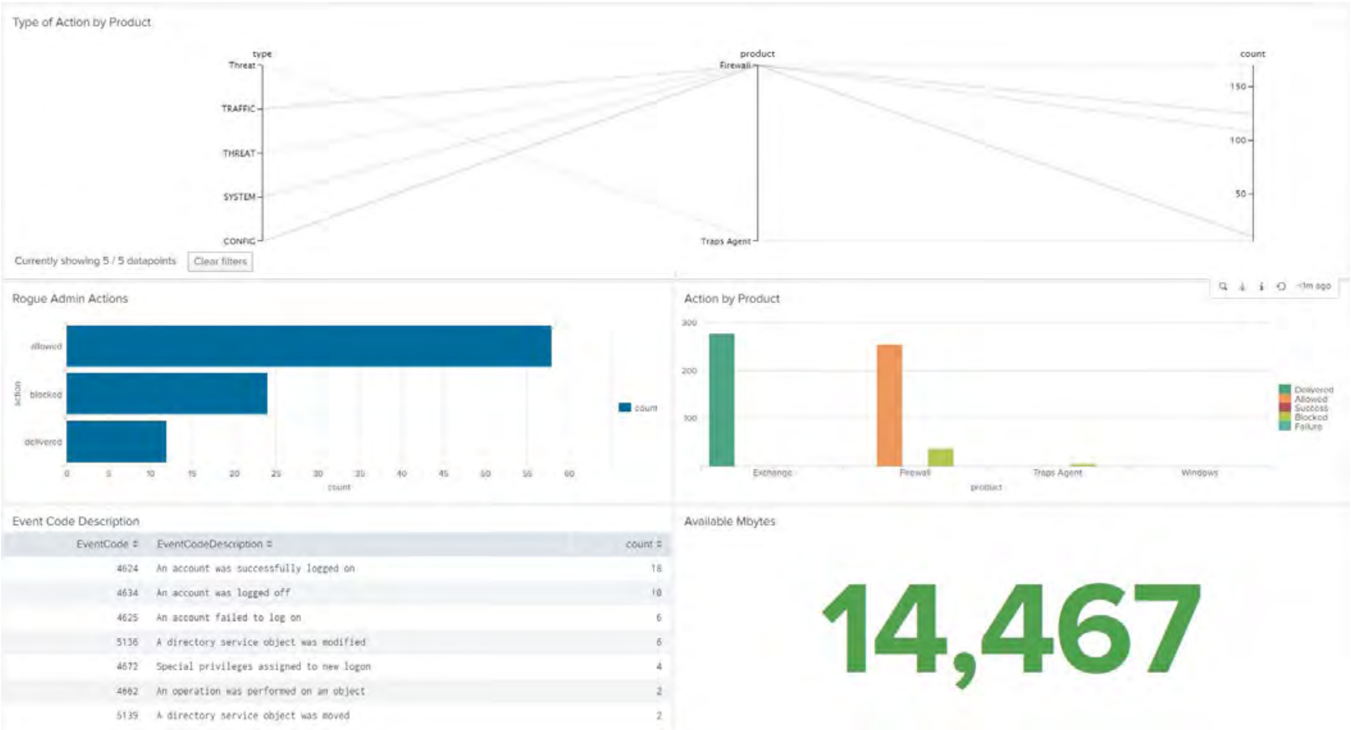
1. This is the original search found within the IT Essentials Learn app:
   a. **Index=* tag=network tag=communicate src_ip="<IP Address of host>" action IN (allowed, blocked) | timechart count by action**
2. Now we will edit the search to fit our demo data:
   a. **Index = windowsit src_ip="192.168.0.2" action IN (allowed, blocked) | timechart count by action**
   b. Here we have edited our search to fit our demo data, which is static meaning we only have events for one specific time and date.
   c. This is what the result should look like:



d. Here is an example of what the result would look like with non-static data:



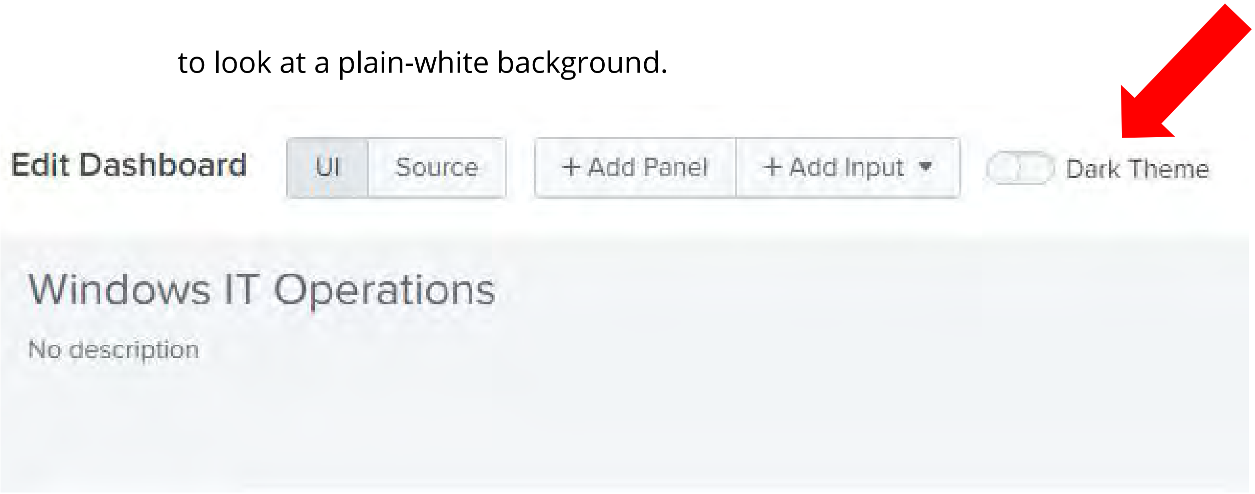
6. Edit the Dashboard around to make it look like the following:



Event Code Description

EventCode	EventCodeDescription	count
4624	An account was successfully logged on	18
4634	An account was logged off	10
4625	An account failed to log on	6
5136	A directory service object was modified	6
4672	Special privileges assigned to new logon	4
4662	An operation was performed on an object	2
5139	A directory service object was moved	2

7. Another unique aspect of Splunk is the ability to make the background into **Dark Theme.**
    a. In the dashboard, Select **Edit** and then Select **Dark Theme**
    b. After you select this, you can press **Save** and refresh the dashboard
        i. This just makes the dashboard look, in my opinion, cool. No one likes to look at a plain-white background.



Conclusion/Recap

The first step of this workshop was to upload a CSV of Windows data, determine a splunk index, and set a sourcetype. With this information alone you will be able to start a PoC or begin to instrument some of the Windows data you will be funneling into Splunk. Taking these steps for different source types in a test environment will also allow you to expand the scope of information you could forward into splunk. Instead of uploading a CSV, you will be using the a Splunk Universal Forwarder placed a syslog server that is collecting this firewall and other network traffic data to populate dashboards such as the Cisco Security

Suite, Juniper, Windows, and other Application that had been built already by Splunk engineers to help visualize this

data. These different apps are found on **Splunkbase** and they will tell you what is needed to implement them into your environment.

The first two visualizations we created included a column and bar chart showing us actions by both a Rogue User and by Product. These charts can help you visualize a wide variety of data other than what we used today.

The next chart we created did not have a visualization with it. With the Event Codes, all we wanted to see if what the description of that specific event code was and how many times this code happened. Some of the visualizations you may create in the future may be best left as-is. As mentioned in the workshop, Splunk can find correlations between Event Codes and the description of what the code is very easy for you, which in-turn can save you time in the future.

The next visualization we created was a Parallel Coordinates visualization. This is most useful when you want to find correlations between multiple different fields in your environment. For us, we wanted to see the correlation between Action and product with the count included. This was a very simple example of this type of visualization, but it shows you how powerful this visualization can be.

The last visualization we created used a search from the free IT Essentials Learn app. Thousands of apps are available on Splunkbase where you can find predefined searches, visualizations, and dashboards.

Moving on from here, you now know how to correctly upload your data into Splunk and how to make use of your data. You can also forward data into your instance and get apps on Splunkbase with pre-existing dashboards already built for you. You also know the roots of making use of your data. I only went into a few very simple searches and made them into visualizations based on what we were looking at. This is something that is very important when

creating your own visualizations. Knowing which visualizations capture which aspects of your data is something that is very important. Say, for example, you want to see which user is sending the most email. Using a Parallel Coordinates visualization will not help you capture this as well as a pie chart.