carahsoft.

splunk>

Part 4 | Carahsoft + Splunk Workshop Series

Dashboarding Cisco Security Data

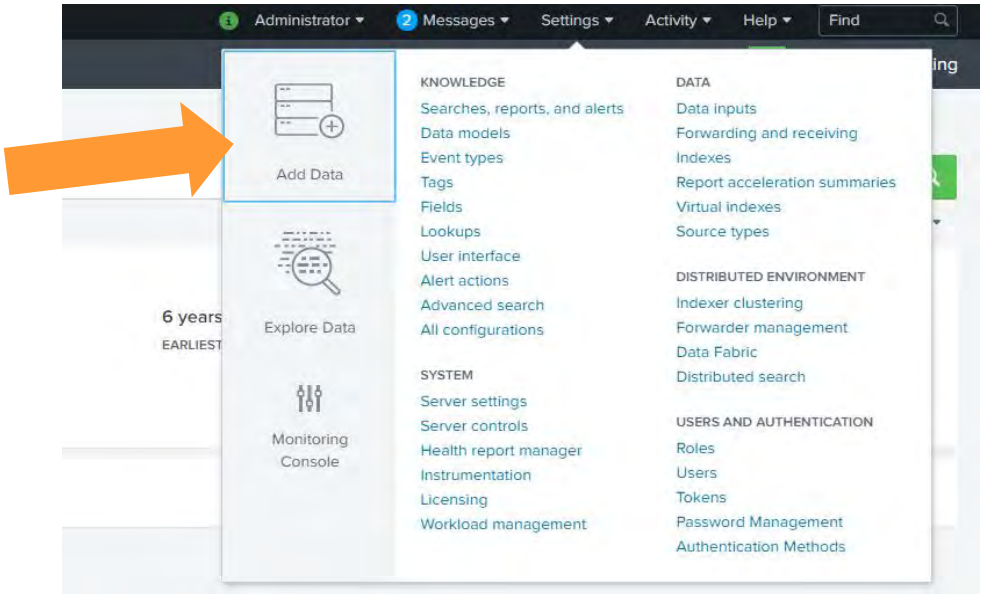
Welcome to week 4 of Carahsoft + Splunk Workshop Series! Today we will be focusing on manipulating data dealing with Cisco Events. This can also be relevant to any security data within your environment but we just want to show you the variety of different dashboards and visualizations you can create and customize.

In this section, we will go over the following:

- Adding Data
- Running Searches
- Creating Dashboards
- Customizing Dashboards

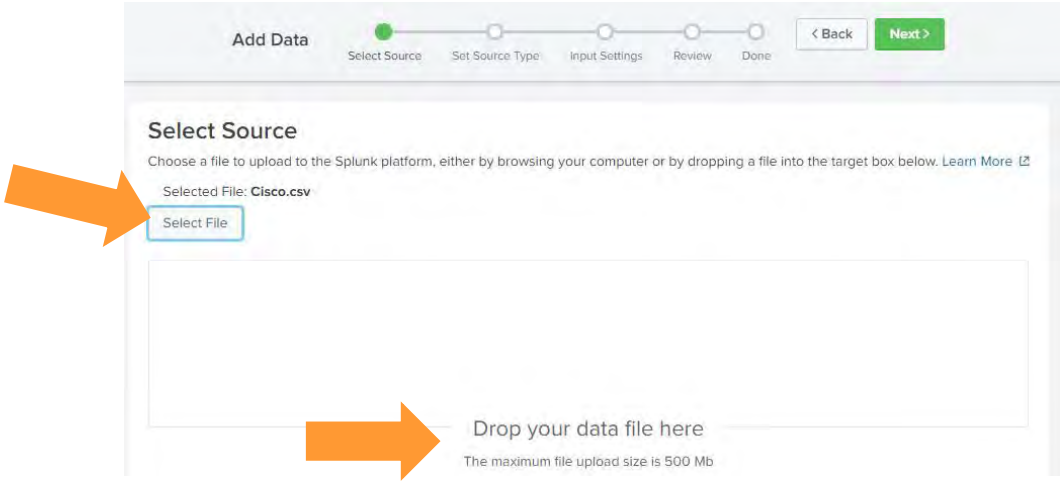
Adding Data

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



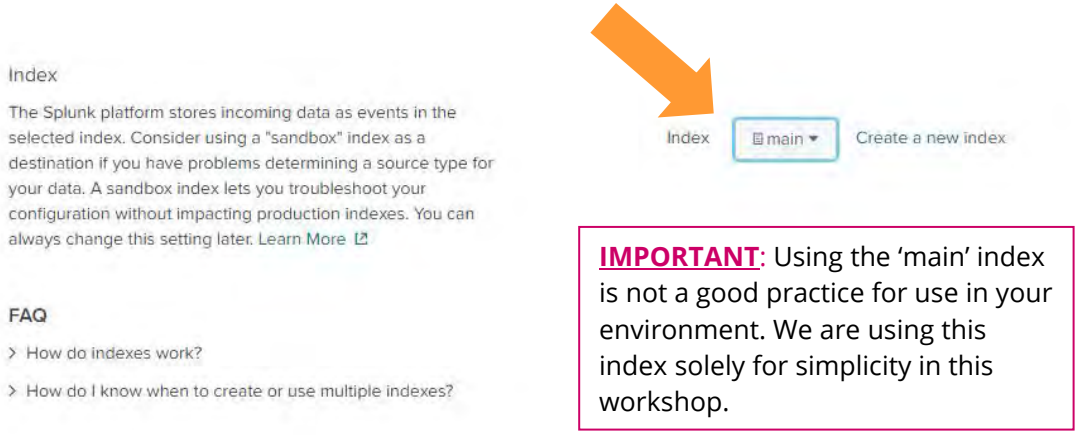
2. From there, you will see a screen asking which method you would like to get data in by.
    a. Select the **Upload** option

   The first part of uploading data is to select the Source.
3. Here we can either select the "**Select File**" option or we can simply drag the **Cisco.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.



4. Select "**Next**" when file is completely done uploading.
5. In this next stage, **Select Source Type**, Splunk will automatically determine the data that is being uploaded. If the type is not known, you can manually tell Splunk what it is. For now, **we will keep it as-is**.
    a. You can also the 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, 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 sends and another begins. With this setting, we can help Splunk by telling it which character is the determining factor or event breaks.
        iii. Lastly we have the **Advanced** settings. This is where we can add additional event characteristics 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.

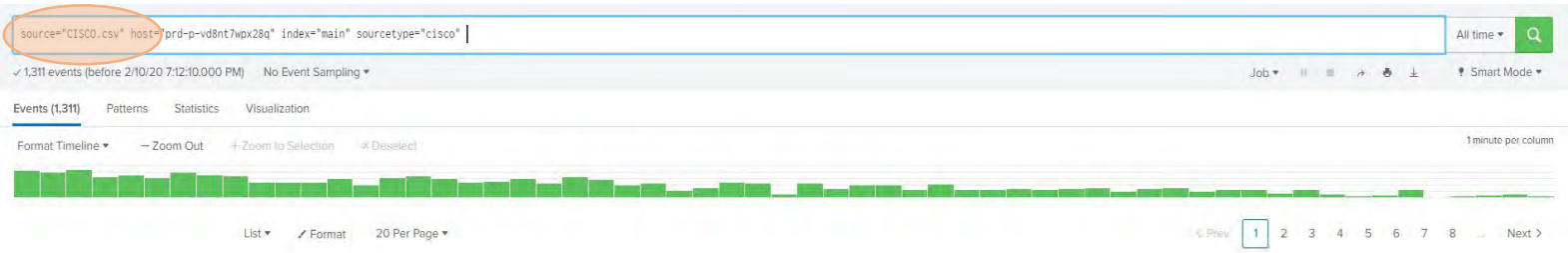
6. Select "**Next**" again.
7. **Input Settings** is where we can set any additional input parameters, like **Host Field Value** and **Index**
    a. We are going to use the Index **Main**.



IMPORTANT: Using the 'main' index is not a good practice for use in your environment. We are using this index solely for simplicity in this workshop.

8. Lastly, you should see a **Review** page. Make sure your values match up with the following:

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 **1,311 Events** populated.



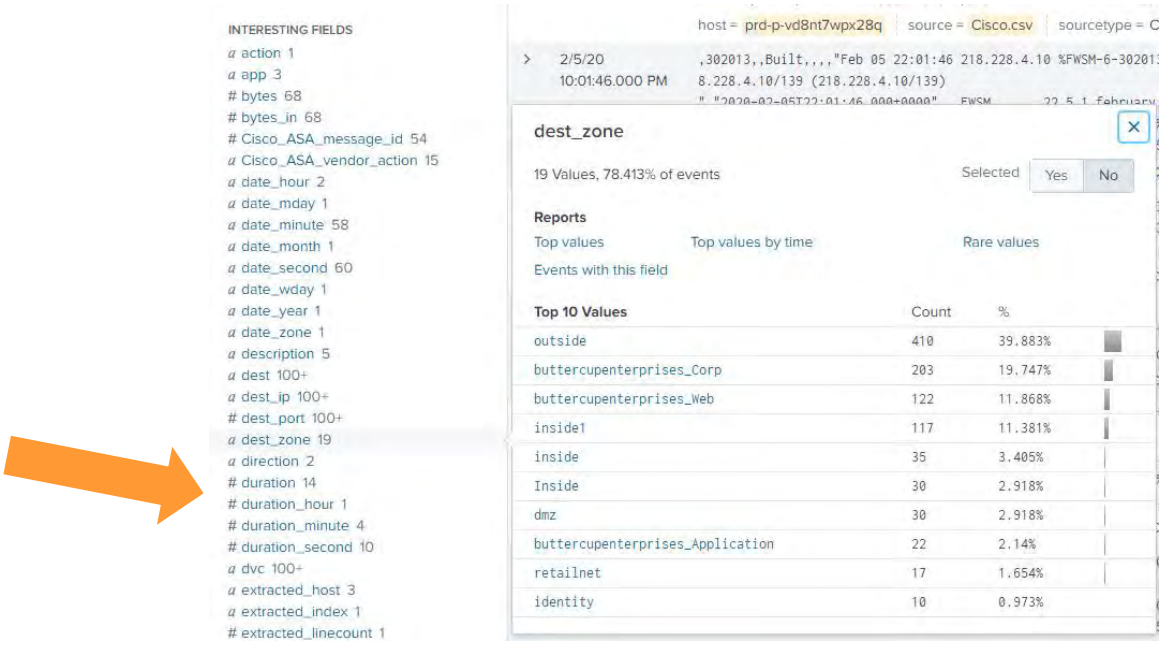
Now that we have uploaded our data, we are going to want to make this data easier to look at. From here, we are going to create a dashboard with different visualizations to show you what Splunk can do with your data. We are only going to get in into a very small portion of what Splunk is able to do with 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. 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% of the time. For example, there is anything from action, to direction, to message_id. What we want to do is make all of this information useful to us by finding correlations.

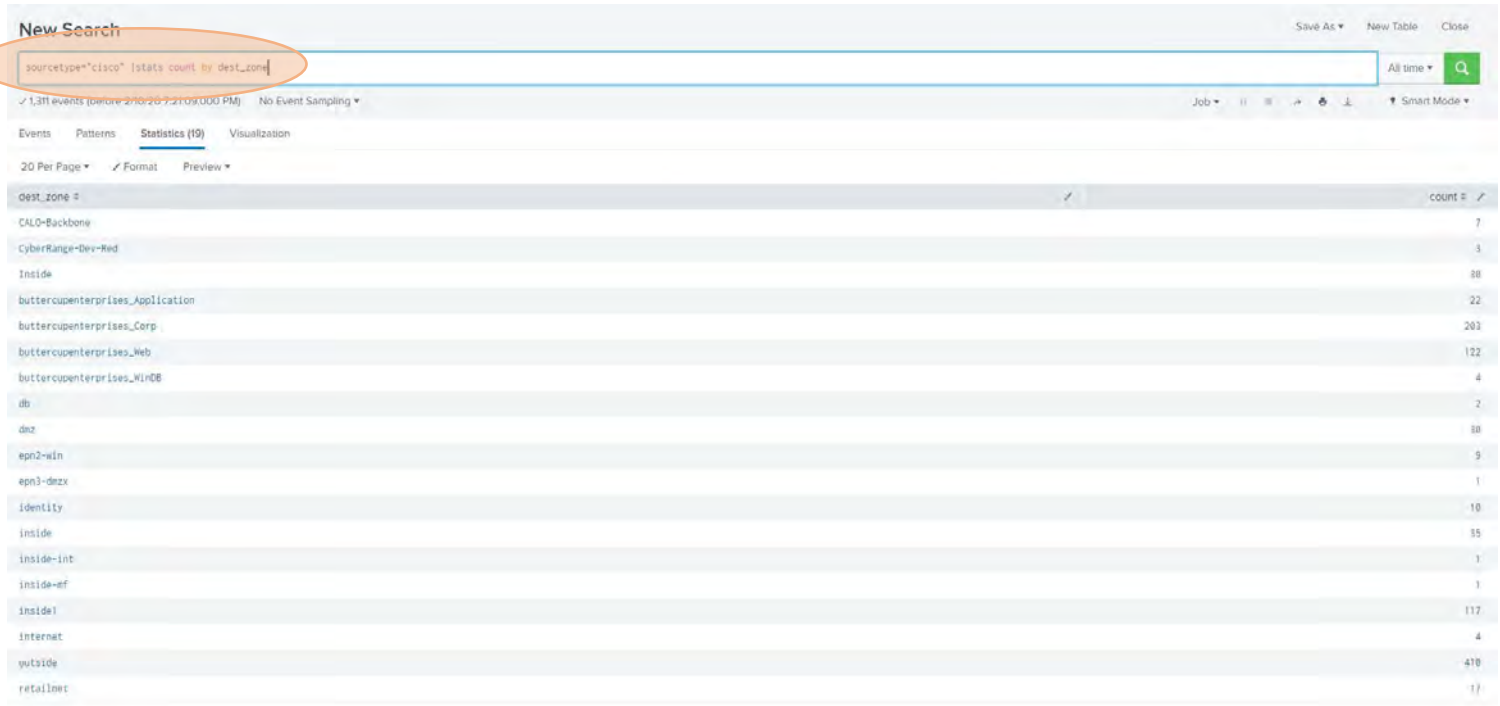
Destination Zone

First, let's look at the different **dest_zone**. This field tells us where data is being sent to and allows us to see not only where most of our data is going, but to identify and investigate any suspicious destinations. The values should show up as following:

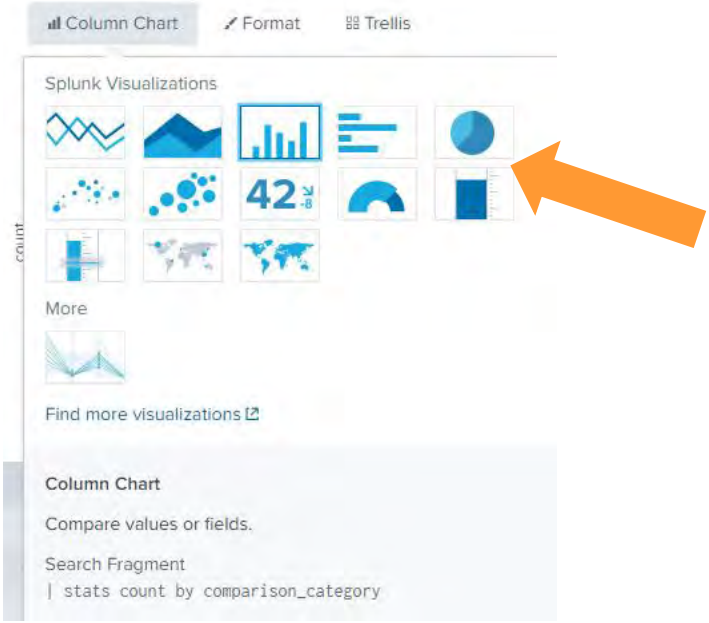


Now we want to identify trends and create visualizations that allow us to easily see the value in this data.

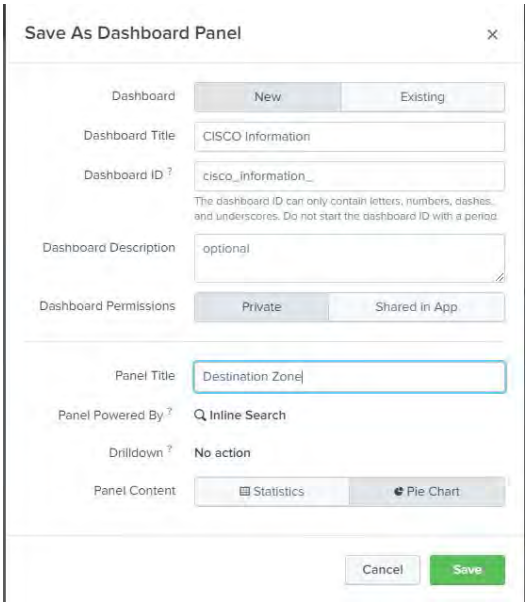
1. In the search bar, enter **sourcetype="csv" | stats count by dest_zone**
    a. You should see a result similar to the image below:



2. Select “Visualization” and then we want to change it from a Column Chart to a **Pie Chart.**



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

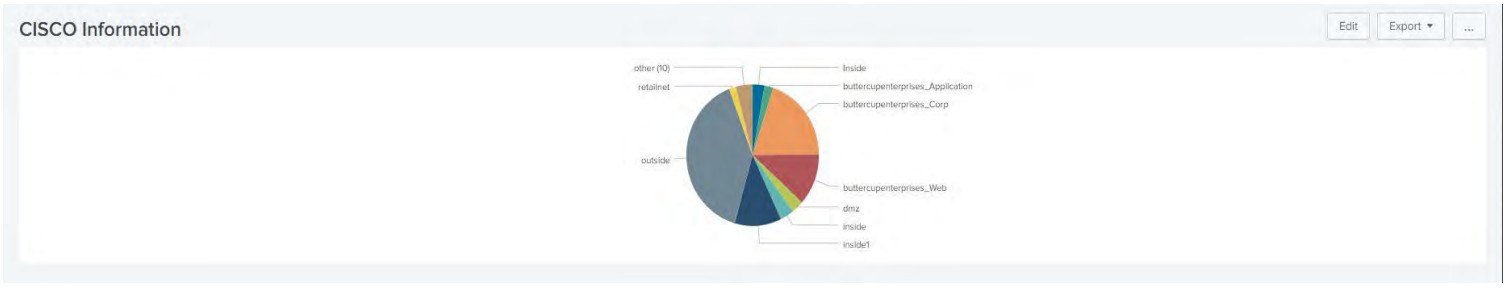
   c. **Dashboard Title** is **CISCO Information**

   d. Keep Dashboard ID, Dashboard Description, and Dashboard Permissions as-is

   e. **Panel Title** will be **Destination Zone**

   f. Finally, Select **Save**

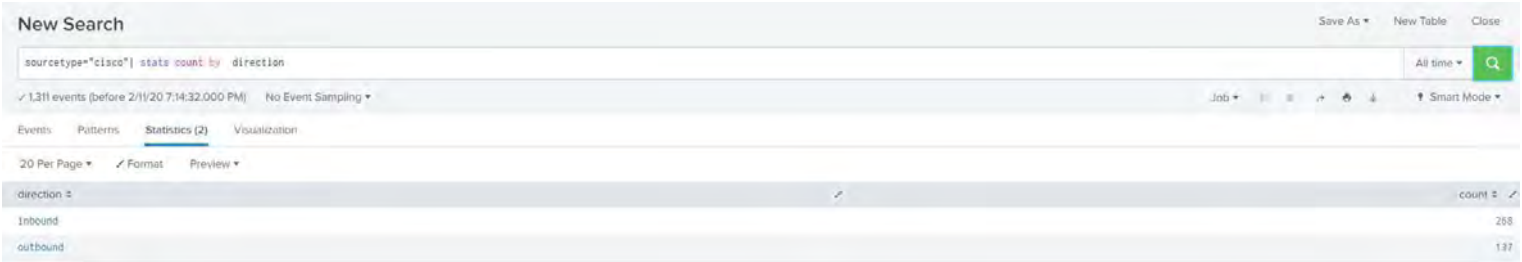
Now if we view this dashboard, you should see that Pie Chart. This allows us to easily see the most common destinations our traffic is being routed to.



Direction

Now let's go back to the searching screen and create one more pie chart. This one will be dealing with the direction of traffic within our CISCO environment. This one is a simple pie chart because there are only two results within it, but it's still important information we want to keep track of. For example, a dramatic shift in inbound to outbound traffic could be indicative of a DoS attack. A rise in either could be at the root cause of dropped packets, etc. Sometimes even basic visualizations can give us a lot of insight.

1. Search **sourcetype="csv" | stats count by direction**
    a. You should get two results, Inbound and Outbound followed by a count of each.



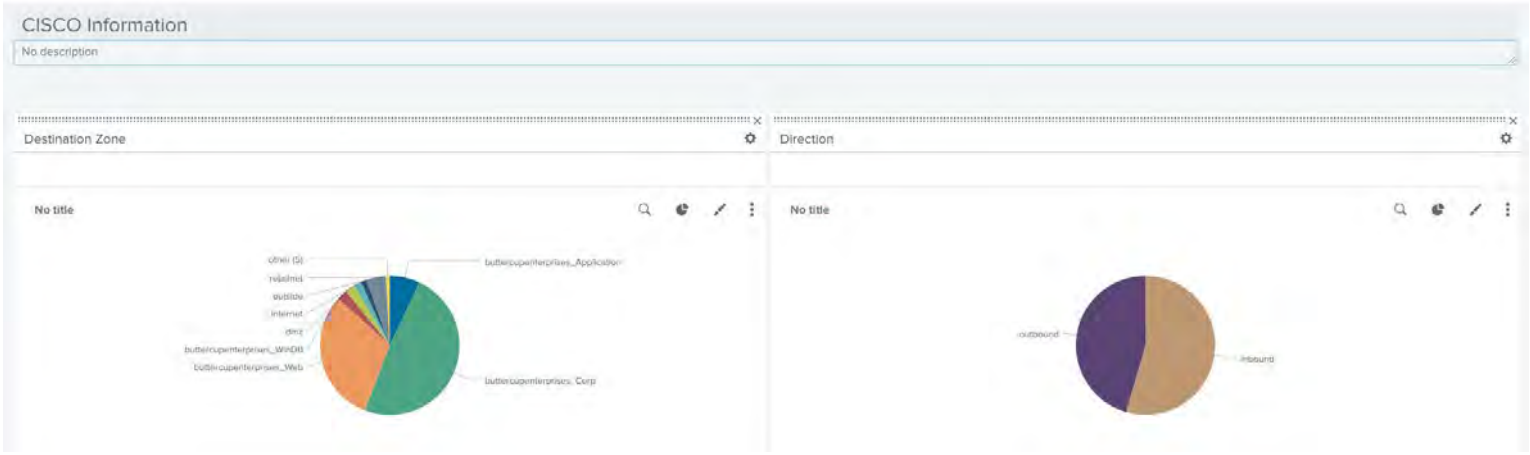
2. From here we can select Visualizations again. Like before select **Pie Chart**.
3. Select **Save As**
    a. **Dashboard Panel**
    b. **Existing**
        i. **Cisco Information**
        ii. **Panel Title** is **Direction**

iii. **Save**

4. Now we have two Pie charts stacked on top of each other. We can change how these are arranged so that they are side-by-side.
    a. On the top-right, select **Edit**
    b. Now you should see each visualization separated from one another. We want to now select the **dotted line** (visualization a) at the top of the **Destination Zone** Pie Chart and drag it next to the other Pie Chart (visualization b).

(a)

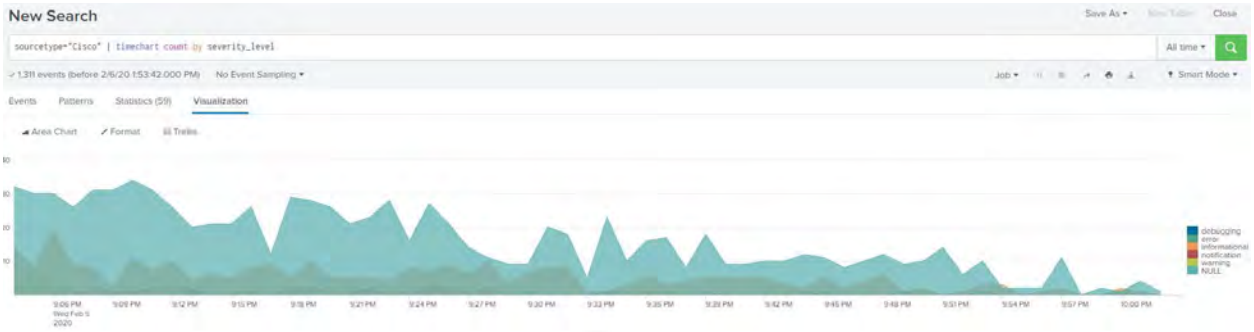
(b)



Security Levels

Many Cisco tools conveniently convey the severity level of a log along with the message, status code, and more. This can be very useful, but larger networks create more logs, and it can be difficult to understand when and where our attention should be focused. Here we are going to create a Timechart based on the different severity levels of the Cisco logs generated within our environment.

1. In the Search bar, Enter **sourcetype="csv" | timechart count by severity_level**
2. For this visualization, we want to use an **Area Chart**



3. Select Save As
    a. **Dashboard Panel**
    b. **Existing**
        i. **CISCO Information**
    c. **Panel Title**
        i. **Severity Levels**
    d. **Save**

4. 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 clicks on a data point, table row, or other visualization element. So first we are going to select Edit on the top right dashboard.

    a. Go to the Severity Levels chart and select the Three Vertical Dots on the right side of the chart.
    b. Select Edit Drilldown

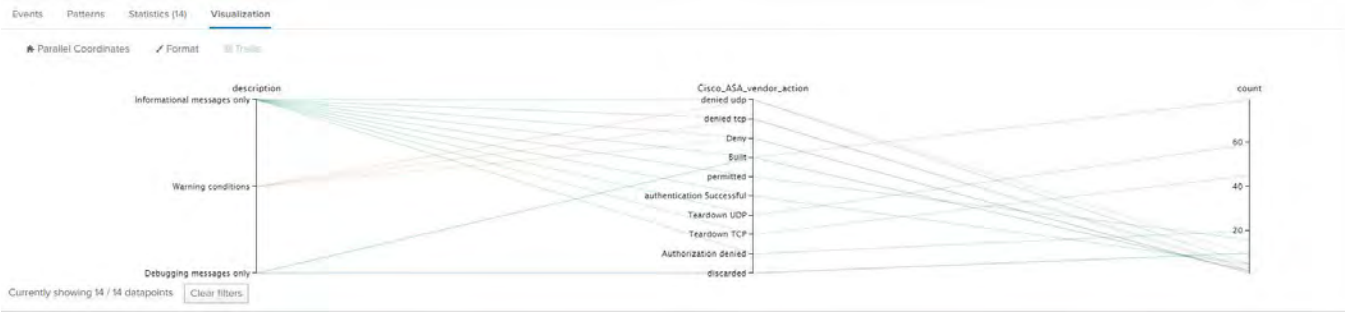
c. "On Click" change the "No action" to Link to Search
d. Change "Auto" to Custom
e. Erase the current Search String and replace it to:
    i. **sourcetype=csv | stats count by severity_level**
    ii. Make sure the "Time Range" is set to **Presets, All Time**
f. Now when we click on the graphic, it should send us to a New Search which looks like this:

CISCO Actions

Next we are going to look at correlations between actions, descriptions of those actions, and the count.

1. In the default search, enter:
    a. **sourcetype=csv | stats count by description Cisco_ASA_vendor_action**
    b. This is what the result should look like:

c. This time we are going to change the Visualization to **Parallel Coordinates**. The results should look like the following:



d. Just like before, we are going to save this to our **CISCO Information Dashboard** and save this panel as **Cisco Actions**.

i. This visualization helps see different correlations between the different fields being used. So here we can see the amount of vendor actions and the descriptions to go along with them. Another example of this could be the count of different users along with the specific applications being used by those users.

Trendlines

Trendlines in Splunk are used to show the occurrence of events over a customized time frame. Among other things, they can be used to easily identify spikes in activity that might indicate compromise or instability in our infrastructure. These next two visualizations are going to be trendlines, showing us when events happen and if there are any trends in activity.

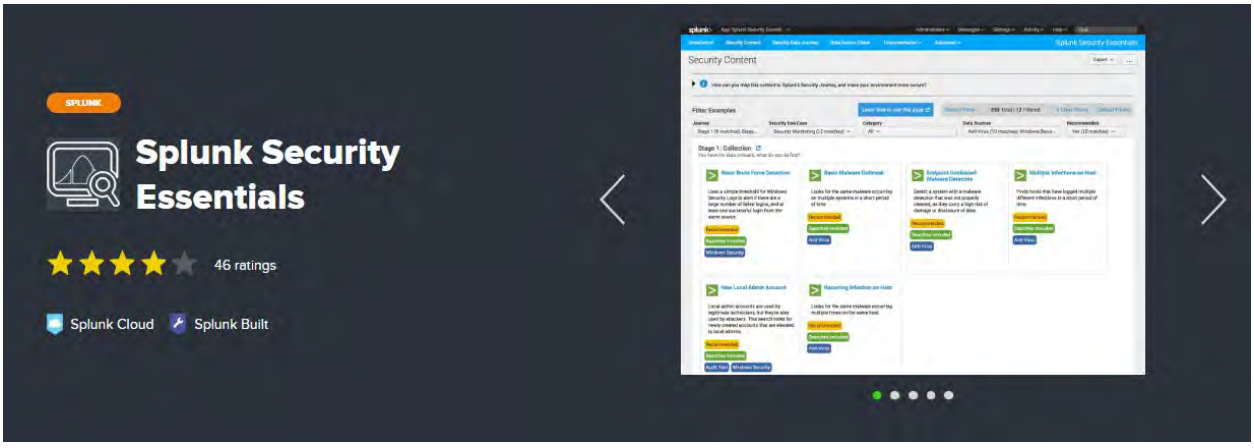
The first trendline we are going to create is going to show us the different hosts that are within our Cisco environment. This is important to see if there are any irregular activities by specific hosts or even if a specific host is not working at all.

1. Enter the following search:
    a. **sourcetype=csv | chart count,sparkline(count) as "Trend" by extracted_host | sort –count**
    b. As you can see, using the command “sparkline”, it show us what we are calling “Trend” with the specific host in search.
    c. Save this search to the **Cisco Information** Dashboard and name the panel **Security Event Stats by Host**

2. Start a new Search with the string:
    a. **sourcetype=csv | chart count,sparkline(count) as "Trend" by transport | sort –count**
    b. Again, save this to our **Cisco Information** Dasboard with the Panel name, **Transport Type**.

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 Security Essentials. This is a free app containing searches for hundreds of different security use cases.



This search is for basic scanning. The search looks for hosts that reach out to more than 1000 hosts, or more than 1000 ports in a short period of time, indicating scanning.

1. This is the original search found within the Security Essentials app:
    a. **index=* ((tag=network tag=communicate) OR sourcetype=zscalernss-fw OR sourcetype=pan*traffic OR sourcetype=opsec OR sourcetype=cisco:asa) earliest=-1h**
    | stats dc(dest_port) as num_dest_port dc(dest_ip) as num_dest_ip by src_ip
    | where num_dest_port > 1000 OR num_dest_ip > 1000

2. Now we will edit the search to fit our demo data:
    a. **index=wstest**
    | stats dc(dest_port) as num_dest_port dc(dest_ip) as num_dest_ip by src_ip
    | where num_dest_port > 0 OR num_dest_ip > 0
    b. Here we have edited our search to fit our demo data, which does not have any hosts that would indicate scanning
    c. This is what the result should look like:

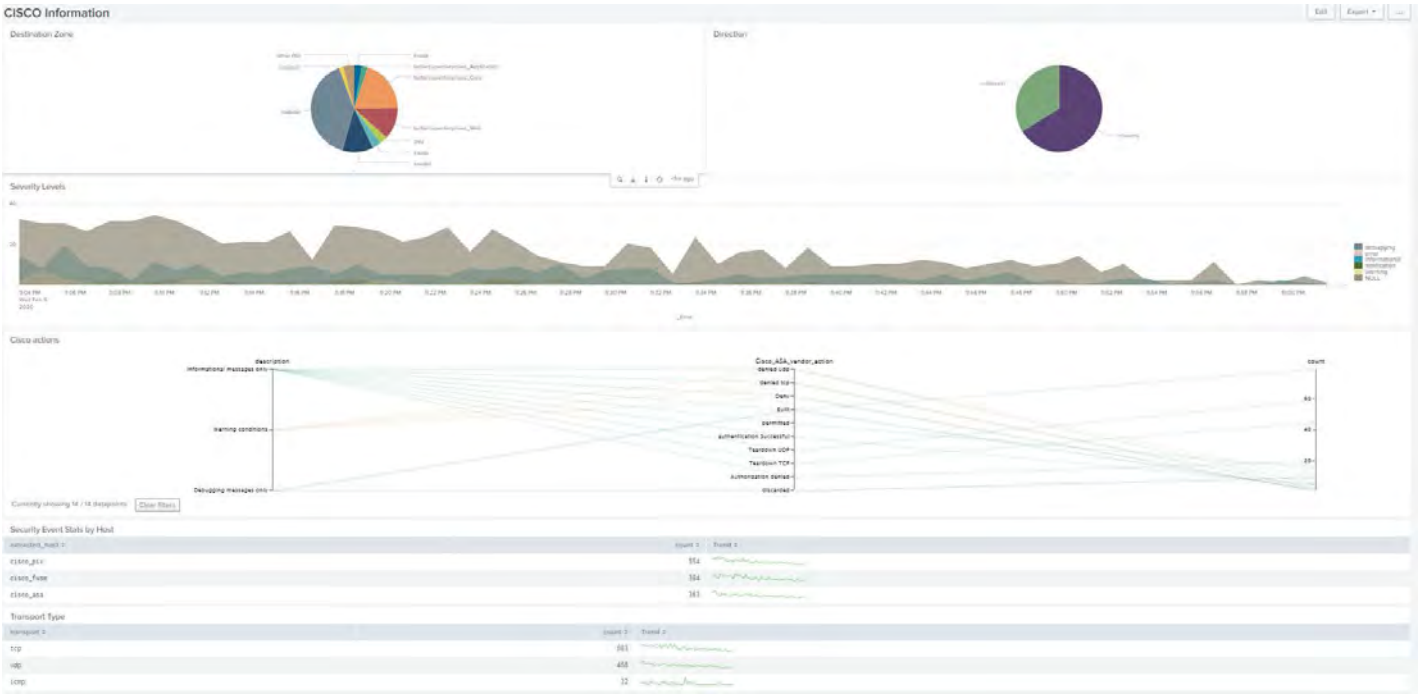
src_ip	num_dest_port	num_dest_ip
0.154.41.22	1	1
0.37.28.242	1	1
0.4.148.53	1	1
0.49.231.212	1	1
0.89.152.201	1	1
1.10.77.127	1	1
1.155.252.153	1	1
1.23.87.4	1	1
1.53.61.38	1	1
1.6.34.132	1	1
1.87.130.211	1	1
10.180.230.33	1	1
10.206.236.223	0	1
10.240.196.200	1	1
10.44.246.59	1	1
100.1.96.168	1	1
100.120.82.39	1	1
100.234.28.92	1	1
101.123.2.120	1	1
101.126.125.152	1	1

d. Here is an example of what the result would look like with hosts indicating scanning:

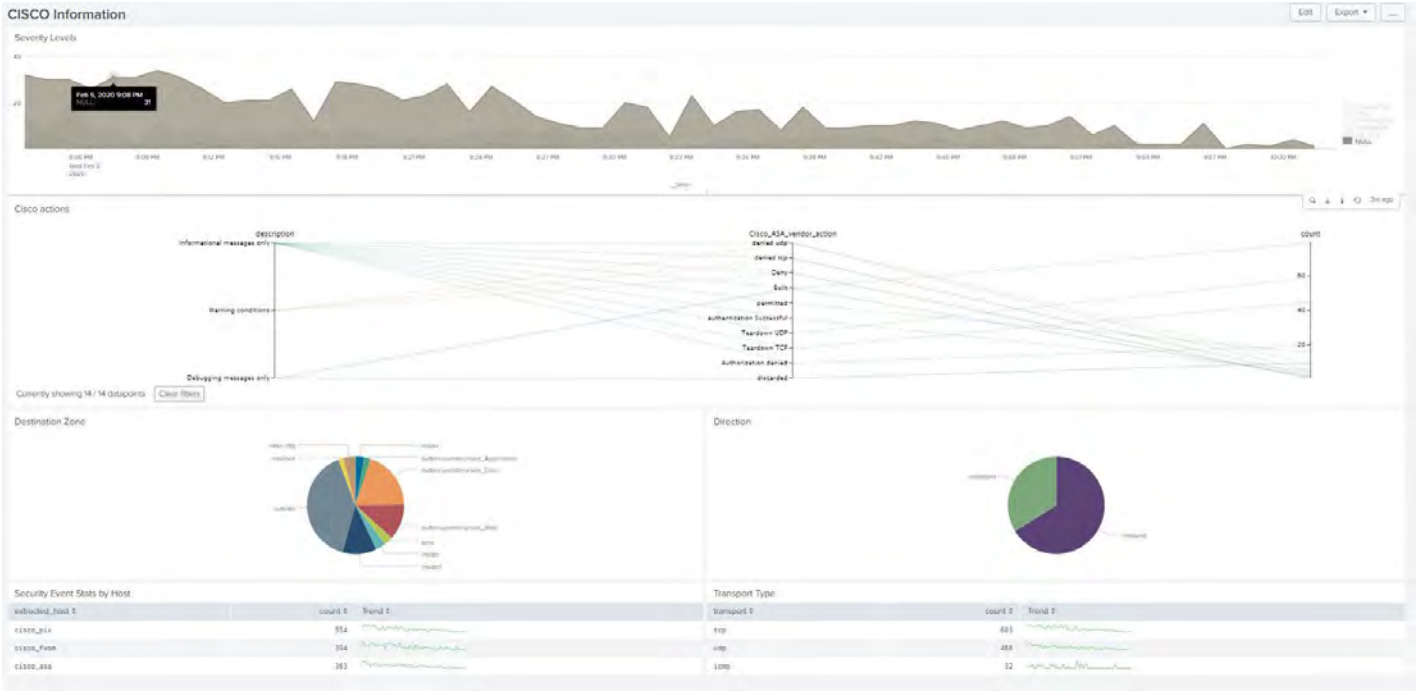
src_ip	_time	num_dest_port	num_dest_ip
10.174.30.199	2016-03-06 15:00	2	6001
10.174.30.199	2016-03-07 15:00	6001	1

3. Now let’s go to the dashboard and re-arrange a few things.

4. The following is what we have so far:

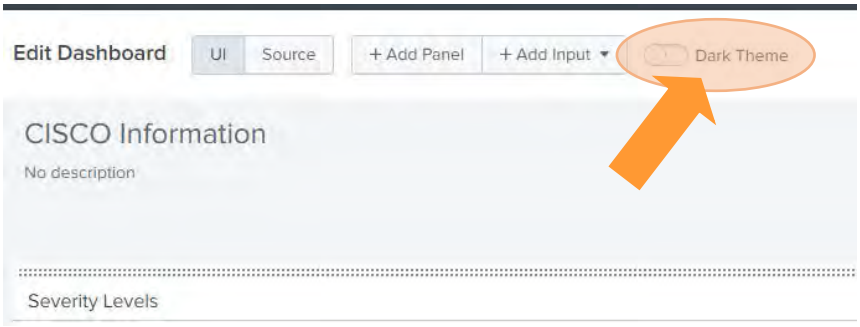


5. Now, re-arrange it to look like the following:



6. 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, unique and different. Some people don't like looking at a plain-white background.



Conclusion/Recap

The first step we did was upload a CSV of Firewall security 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 security 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 in to Splunk.

Instead of uploading a CSV, you will be using the **Splunk Universal Forwarder** placed on a syslog server that is collecting the firewall and other network traffic data to populate dashboards such as the Cisco Security Suite, Juniper, Windows, and other Applications that have been already built 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 were pie charts. This was used because we wanted to see what major actions were being performed. In the **Destination Zone** we wanted to see where we were sending the majority of our data, and in **Direction** we wanted to see if there was more data coming in our going out.

The next chart we built was looking **vendor actions** by description. This type of chart can be used multiple other ways; I wanted to show you how to create this so if you have disparate events from different solutions or hardware you can create a correlation chart to aid in understanding the trends on how they are interacting within your environment.

The next two visualizations created were **Trendlines**. They are the most useful when you want to see the “trends” within your data. Whether there is a spike in that specific field or a dip, this visualization can help you stay proactive with how these fields are performing.

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