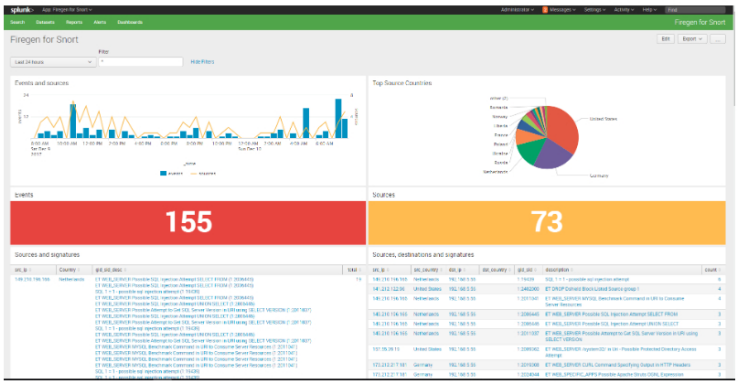
Splunk Crash Course – Creating Dashboards

Following the same format as the Alerts lesson, before we cover how to create your own dashboards, let's first cover what they are, and how they work within Splunk. A dashboard is a collection of panels, each displaying different data. We can use this to provide a "single pane of glass", where analysts can look at a single screen and see lots of different information in the form of graphs. Here's an example of a Splunk dashboard:



SIEMs will have dashboards to monitor information at a high level, but most Security Operations Centers will also have large screens that show information from multiple tools, such as case management systems, endpoint detection and response solutions, and SIEM. Obviously the information shown on SOC dashboards will vary depending on their focus areas, but the following information is typically valuable to analysts to have in one place:

- **Firewall graph** showing firewall denies and firewall allows (helps analysts spot spikes in firewall denies, that could represent a distributed denial-of-service attack, or a network issue)
- **Number of alerts/offences** showing how many alerts are currently under investigation or pending investigation
- **Number of alerts closed in the previous 24 hours** to show how efficiently the team is dealing with security events
- **Traffic flow going into each SIEM collector** which can help security teams identify if a collector stops responding so engineers can investigate the outage
- **An attack map** that correlates the source IP addresses from alerts, and plots them on a world map
- **Pie chart showing the event types per alert over the past 24 hours** which can help analysts to see which attacks have occurred more recently

Now that you have a basic understanding of what dashboards are, and why SOCs and SIEMs use them, let's move on to creating our own in Splunk!

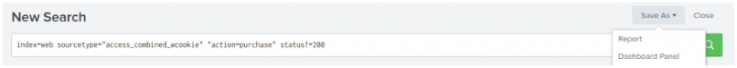
CREATING DASHBOARDS

Dashboards in Splunk are unique to Apps. So if we create a dashboard for the default Search and Reporting App, then the information will be associated with this application and it's functionality. This allows us to create different dashboards for different Apps, which makes sense because each of these has their own unique use case. For this walkthrough, we'll be using the Search and Reporting App. Once we've created our first dashboard, we'll show you

how to share and manage access with other users on the Splunk instance.

Splunk Reports

To create dashboards you need to first create a report, which are used to create panels on a dashboard. But how do I create a report? Whenever you perform a search you can select **'Save As'** and save it as a **'Report'**. For example here we are searching the web application data for each status code which is not equal to 200 (HTTP Status OK), we can create a report for it and quantify checkout failure on an E- commerce site.



Its always a good idea to decide a naming convention for reports, so that it's immediately obvious what the saved object is. Splunk's documentation recommended naming convention is as follows:

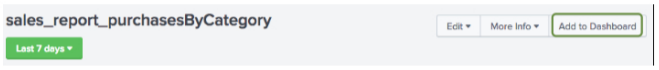
<group>_<object>_<description>

- **group**: the name of the group or department using the knowledge object such as sales, IT, finance, etc.
- **object**: report, dashboard, macro, etc.
- **description**: WeeklySales, FailedLogins, etc.

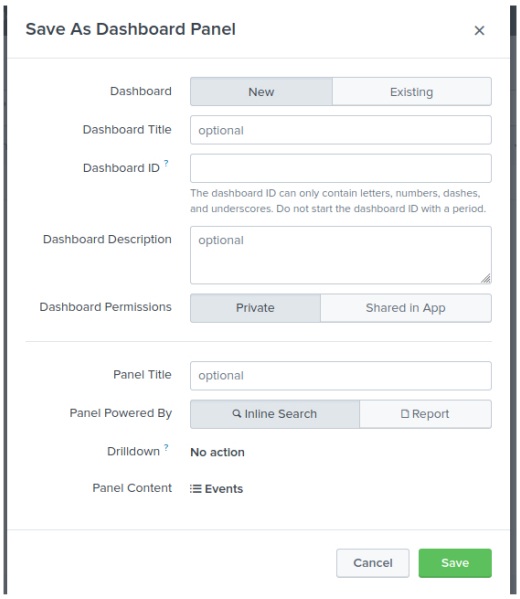
With the introduction to reports done, lets get started with creating a dashboard.

Splunk Dashboards

To use a report to create a dashboard, go to that particular report and click on **'Add to dashboard'**.



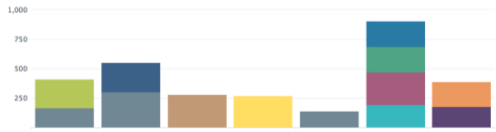
And a pop up should appear:



- **Dashboard Title –** Set an optional human-readable name for the dashboard.
- **Dashboard ID –** Set an identification number for the dashboard.
- **Dashboard Description –** Set an optional description of what the dashboard's intended purpose is.
- **Dashboard Permissions –** It's usually a good idea to keep the permissions set to Private until the dashboard has been tested.
- **Panel Title –** Set an optional name for the panel within a dashboard.

- **Panel Powered By** – Select the search query that powers the panel, either by writing a query in the 'Inline Search' box, or clicking on 'Report' and finding your saved report.

And here is our dashboard, you can set a dashboard to appear by default in the bottom panel of your home view. Click on your home app, select **Choose a home dashboard** and it will appear each time you login.



Obviously this is a very simple example – you should take some time to play around and create different panels for your own dashboard. Here are some suggestions:

- **Login Failures as a Line Chart** (Useful to show spikes in failure login attempts, which could represent a bruteforce attack)
- **HTTP response codes as a Line Chart** (Useful to show large spikes in connections to a website)

Previous Topic

Mark Complete

Back to Lesson