carahsoft. splunk>

Splunk Tips and Tricks

This session will be going over some basic tips and tricks that make using Splunk easier!

In this section, we will go over the following:

- Customizing Dashboards
- Creating Your Own Dashboards
- Saving Searches
- Wildcards
- Indexes
- The Splunk Dashboard Examples App
- The Splunk Security Essentials App
- IT Essentials Work and Learn Apps

Indexes

If you want to have your data split into different use cases, categories, or by different teams you can separate them by indexes.

Security, Business Analytics, ITOps, Internet of Things, Networking, etc.

Security Operations Center, Network Operations Center, Sales, etc.

Wildcards

Trailing wild cards are the most efficient use for them; using wild cards alone should not be run in a search it could crash the system if you have a lot of data. Trailing wildcards make the search run better and also makes the search shorter and easier to read.

EX: status = fail* (This will return a fail, failed, or failure)

Save Searches

To save searches, hit the save as drop down button on the right hand side and click report. Fill out the name/description and your searches will be saved under the reports tab in the top left hand side.

Dashboard Customization

In windows, edit a visualization by clicking on the edit button on the top right side. Change the layout by dragging different panels, deleting irrelevant panels, or selecting difference visualizations. Use the source button to further customize the dashboards.

Create Your Own Dashboard

To create your own dashboard, have a search that you want to turn into a visualization. Click on the save as dropdown button and hit Dashboard Panel. Make sure the dashboard is a new dashboard and not an existing one. Fill out the required information and hit save.

Splunk Dashboard Examples App

This app aids in showing different kinds of dashboard examples that you could potentially benefit using, to make your data easier to view and analyze. There are many options to choose from that allow you to view your data in many different ways.

Splunk Security Essentials App

This unique app provides a library of different security based searches along with important information. You are able to see line by line what the search is doing and information about MITRE ATT&CK tactics and techniques, kill chain phases, and needed data sources. You can copy and paste the any of the searches in your Searching and Reporting App, so you don’t have to spend time learning the search language.

Splunk IT Essentials Learn

The IT Essentials Learn Application, it’s one of many free apps on Splunkbase. This app shows you different IT use cases and search strings that correspond to each use case. For each use case there is a library of different search strings available for you to easily copy and paste. It’s very similar to security essentials, but this targets regular IT data. The Welcome and Overview pages shows you a broad view on which available procedures there are, what you’ve viewed, and the procedures you’ve deployed. Pages regarding heat maps and your IT journey are provided here as well.

Splunk IT Essentials Work

IT Essentials Work is another free app that lets you monitor your IT infrastructure and is available on both cloud and on-prem. Here you are able to see an overview of your entire infrastructure. Entities will be shown with information about whether or not they are active, unstable, inactive, or N/A. Entities are normally hosts but they can also be other items like cloud or virtual resources, network devices, or applications. You’re able to look at alerts and episodes along with deep dives to see KPI search results overtime and correlate root causes to issues within your infrastructure.