Visualizing and Alerting in Splunk Observability

Course Summary:

This blended course is for Devops/SREs and Developers.

The course describes ways to enhance dashboards and alerts to help with troubleshooting. You will also be able to find insights using analytics in charts and detectors and to create detectors for common use cases.

Note: A large portion of this course content was covered in the course Using Splunk Infrastructure Monitoring (retired course).

Course Duration:

4.5 Hours

Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Fundamentals of Metrics Monitoring in Splunk Observability Cloud

Course Outlines:

Module 1 – Create Efficient Dashboards and Alerts

- Add instructions to dashboards
- Create single-instance dashboards
- Add event feed charts
- Overlay event markers
- Configure data links
- Customize alert messages
- Troubleshoot charts and alerts

Module 2 – Find Insights and Refine Detectors Using Analytics

- Find total value across all sources
- Combine plots in charts
- View and alert on weekly, daily or hourly comparisons
- Use percentages and ratios to understand trends
- Apply analytic functions over moving and calendar time windows
- Apply analytic functions to a subset of MTS in a signal
- Create non-flapping detectors

Module 3 – Detectors for Common Use Cases (self-paced eLearning)

- Identify common issues with detectors
- Troubleshoot a detector
- Create detectors to monitor populations
- Create non-flapping detectors
- Monitor metrics with cyclic patterns

- Monitor large number of sources
- Monitor an ephemeral infrastructure

About Splunk Education:

- Devops/SREs
- Developers