Using Splunk Mission Control

Splunk Mission Control is a cloud-based, unified security operations platform. It brings together security data, analytics, and operations so that security teams can manage incidents across the entire event lifecycle. This 1-day hands-on course introduces Mission Control and illustrates its benefits to security teams. You will learn how to triage, investigate, and respond to security incidents. You will also learn how to create new response plans and build customized dashboards to gain further insights into your data.

Course Topics

- Mission Control overview and architecture
- Features, capabilities, and benefits
- Triage notables in the analyst queue
- Start a notable investigation
- Use and create new response templates
- Analyze security data using dashboards

Course Prerequisites

Required:

- Using Splunk Enterprise Security

Class Format

Virtual instructor-led lecture with hands-on labs.

Course Modules

Module 1 – Splunk Mission Control Overview

- Introduce Splunk Mission Control
- Discuss features and capabilities
- Identify benefits to security teams
- Review the overall architecture

Module 2 – Triage, Investigate, & Respond

- Review the analyst queue
- Search for notables and filter the analyst queue
- Use response templates in a notable investigation
- Add notes, files, artifacts, and critical evidence to a notable

Module 3 – Response Templates

- Select and apply a response template for a particular use case
- Modify the template to fit the notable investigation use case
- Edit and delete the phases and tasks of the template
- Create a new response template

Module 4 – Dashboards

- Review how to manage and create dashboards
- Configure ad-hoc and on-premises searches
- Build visualizations and utilize user inputs
- Save and export dashboards

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education
To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
270 Brannan
San Francisco, CA
94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com