SPLUNK EDUCATION

Course Description

ES 8.0 Updates for the Splunk SOC

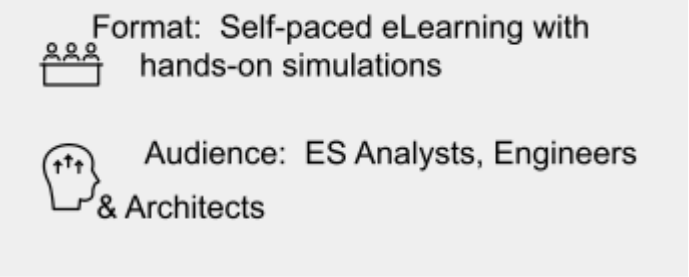
Summary

This self-paced eLearning course with hands-on simulations gives an overview of the new features and configuration of Enterprise Security (ES) 8.0 for the Splunk SOC.

This course does not include labs. This course takes approximately 1-3 hours to complete.

Prerequisites

- Using Splunk Enterprise Security
- Administering Splunk Enterprise Security



Course Outline

Lesson 1 – Introduction

- Review the similarities and differences between ES 8.0 and earlier versions of ES
- Give an overview of the new features of ES 8.0

Lesson 2 – Taxonomy & Terminology

- Review the OCSF taxonomy used in ES 8.0
- Review the updated ES 8.0 terminology

Lesson 3 – Exploring the Analyst Queue

- Give an overview of ES 8.0 navigation
- Explore the Analyst Queue
- Use the different filters to refine the results of the Analyst Queue

Lesson 4 – Customizing the Analyst Queue

- Explain how the look of the Analyst Queue can be changed from the Mission Control page
- Give an overview of the Analyst Queue settings and how they can customize the Analyst Queue

Lesson 5 – Working with Findings

- Give an overview of the Analyst Queue split view
- Explore the details of a finding
- Add notes to a finding

Lesson 6 – Case Management

- Create an investigation

- Add findings to an investigation
- Use a Response plan
- Run an Action on an investigation
- Run a SOAR Playbook

Lesson 7 – Working with Investigations

- Give an overview of the tools available for investigation
- Add a response plan to an investigation
- Explore response plan phases and tasks

Lesson 8 – Exploring Detections & Findings

- Give an overview of ES detections
- Explain the difference between Event-based and Finding-based detections
- Describe Intermediate Findings and Finding Groups
- Look at the Risk-Based Alerting (RBA) differences from ES 7.x to 8.0

Lesson 9 – Creating Detections & Detection Versioning

- Create an Event-based detection
- Create a Finding-based detection
- Discuss Detection Versioning

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit http://www.splunk.com/education.

To contact us, email education@splunk.com.