Introduction to Splunk Security Essentials

This 45-minute eLearning course provides an overview of the security content available in Splunk Security Essentials (SSE) including use cases and analytic stories. You will learn how to filter the over 1000 pieces of content to find detections that are relevant to your security data. You will also discover the considerable amount of information provided for each use case including how the detection works and the data sources it is looking for.

Course Topics

- What is Splunk Security Essentials
- The Splunk Security Data Journey
- Finding security content in SSE
- Bookmarking security content
- Exploring security use cases and analytic stories
- Examining the Overview dashboard

Prerequisite Knowledge

To be successful, students should have a working understanding of the following:

- Splunk Enterprise or Splunk Cloud
- Splunk Enterprise Security

Course Format

This is a 45-minute eLearning course

Course Objectives

Topic 1 – Introduction

- What is Splunk Security Essentials
- Using the SSE Home page
- The benefits of using SSE

Topic 2 – The Security Data Journey

- What is the Splunk Security Data Journey
- Exploring the stages of the Security Data Journey
- How to use the Security Data Journey

Topic 3 – Finding Security Content

- The Security Content library
- Use case types
- Filtering the over 1000 security use cases
- Customizing the Security Content dashboard

Topic 4 – Bookmarking Security Content

- How to bookmark a use case
- Managing bookmarked content
- Exploring the Manage Bookmarks dashboard

Topic 5 – Uses Cases-Part 1

- Exploring the details of an SSE use case using a real-world scenario

Topic 6 – Uses Cases-Part 2

- Continued exploration of a use case using a real-world scenario

Topic 7 – The Overview Dashboard

- Using the Overview dashboard to review the security use cases available in SSE
- Installing the Splunk Sankey Diagram for custom visualization on various dashboard panels
- How to interpret a Sankey diagram

Topic 8 – Browsing Content by Framework

- Explore security content using the Ransomware Content Browser
- Browse use cases by MITRE ATT&CK technique
- Use the Risk-based Alerting Content Recommendation dashboard to find applicable use cases

Topic 9 – Analytic Stories

- What is an Analytic Story
- Examine the details of a story

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 Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/training

To contact us, email Education_AMER@splunk.com

Splunk, Inc.
270 Brannan St. San Francisco, CA 94107
+1 866.GET.SPLUNK (1 866.438.7758)
Contact sales