SPLUNK EDUCATION

Course Description

SOC Essentials: Investigating with Splunk (eLearning)

Summary

This is the sixth course in the Defense Analyst learning path and is intended for learners who want to begin or advance a career as a Security Analyst within a SOC, as well as detection engineers and Splunk Enterprise Security or Splunk SOAR administrators who provide support to these roles.

This interactive course takes place within the fictional Wonderland SOC. As an analyst-in-training, learners will explore how to conduct investigations using Splunk Enterprise Security (ES) and Risk-based alerting, through best practices shared by our security champions. Learners will also perform some common analyst tasks using Splunk Enterprise Security and Splunk SOAR. This e-learning combines videos, activities and hands-on **+** labs that challenge learners to practice what they learned.

+ *This course is available in different modalities: one includes labs, and the other does not. The hands-on experience is available only with the (paid) eLearning version. The free version does not contain labs.*

At the end of this course you should be able to:

- Describe SIEM best practices and basic operation concepts of Splunk Enterprise Security, including the interaction between CIM, Data Models, and acceleration, and common CIM fields that may be used in investigations
- Describe the purpose of the Asset & Identity and Threat Intelligence frameworks in ES
- Explain what a Detection is and how Detections are used within Enterprise Security
- Define Splunk ES elements like Finding, Risk-Based or intermediate Finding, Adaptive Response Action, Entity, etc.
- Identify common built-in dashboards in Enterprise Security and the basic information they contain
- Explain the essentials of Risk-based Alerting and the Risk framework within Enterprise Security
- Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security
- Carry out event triage and an investigation using Splunk Enterprise Security**

Prerequisites

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

- Intro to Splunk
- Using fields
- Previous courses in the Defense Analyst learning path

Students should also have a basic understanding of common cyber technologies and concepts including:

- OSI Model
- Networking concepts and common security tools
- Common Operative Systems like Windows and Linux

Format: ELN

Duration: Content 2.5hrs, Lab 1.5-3 hrs based on expertise

Audience:

- SOC Analyst
- Detection Engineer
- Splunk admins who support these roles

Course Outline

Module 1 - Introduction

- The CyberSecurity Defense Analyst tasks
- CIM, Data Models and Correlation Refresh

Module 2 – Splunk Enterprise Security (ES) for Analysts

- What is SIEM again?
- Asset & Identity Framework
- Threat Intelligence Framework
- Notable Event Framework
- Adaptive Response Framework
- Incident Investigation Management in Splunk ES

Module 3 – Using Risk

- A Journey to Risk Based Alerting
- Risk Analysis Framework

Module 4 – Working with Splunk SOAR

- Introducing Splunk SOAR

Hands-on Lab Activities +

- Introducing the environment
- Investigating with Splunk ES
- Exploring Risk-Based Alerting
- Splunk SOAR practice
- Challenge Lab: Conduct your own investigation

+This lab experience uses the following Splunk tools:

- Enterprise 9.4.3
- Enterprise Security (ES) 8.1.0
- SOAR: 6.4.1*

The Cybersecurity Defense Analyst Learning Path

This course is part of a learning path that can help learners prepare for the role of a SOC Analyst and for the Splunk Certified Cybersecurity Defense Analyst exam.

The learning path includes the following courses:

- The Cybersecurity Landscape
- Understanding Threats and Attacks
- Security Operations and the Defense Analyst
- Data and tools for Defense
- The Art of Investigation
- SOC Essentials: Investigating with Splunk
- SOC Essentials: Introduction to Threat Hunting

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 splunk_training@cisco.com.