SOC Essentials: Investigating and Threat Hunting (ILT)

In this course you will learn and practice how to conduct investigations using Splunk Enterprise Security features, including Risk Based Alerting, through best practices shared by our security champions, and practice some common tasks using Splunk SOAR.

You will also learn about the PEAK Threat Hunting framework and will apply its basic concepts in a hypothesis-driven threat-hunting exercise.

Course Topics

- Introduction
  - The CyberSecurity Defense Analyst
  - CIM, Data Models and Correlation Refresh
  - Lab 1: Introducing the environment
- Splunk Enterprise Security (ES) for Analysts
  - What is SIEM again?
  - Asset & Identity Framework
  - Threat Intelligence Framework
  - Notable Event FrameworkAdaptive Response Framework
  - Incident Investigation Management in Splunk ES
  - Lab 2: Pick up an Investigation
- Risk Analysis Framework
  - Overview
  - Lab 3: Continue your investigation with RBA
- Working with Splunk SOAR
  - Introducing Splunk SOAR
  - Lab 4: Splunk SOAR practice
- Threat Hunting with PEAK
  - PEAK Overview
  - Lab 5: Threat Hunting Hands-on
- Challenge Lab
  - Lab 6: Run your own investigation

Course Format

This is an instructor-led course with lab exercises that will challenge the student to practice what they learned.

This lab experience is using the following Splunk tools:

- Splunk Enterprise Version: 9.1.1
- Enterprise Security (ES) Version: 7.3.1
- Splunk SOAR Version: 6.2.0.355

Estimated completion time:

- 9 hours

Prerequisite Knowledge

To be successful, students should have a working understanding of the topics covered in the **Intro to Splunk** course as well as a basic understanding of common cyber technologies and concepts including:

- Networking concepts and common security tools
- Common Operating Systems like Windows and Linux

Course Objectives

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
- Carry out a typical triage and investigation process using Splunk Enterprise Security
- Describe the purpose of the Asset and Identity, and Threat Intelligence frameworks in ES
- Define Splunk ES elements like Notable Event, Risk Notable, Adaptive Response Action, Risk Object, and Contributing Events.
- Identify common built-in dashboards in Enterprise Security and the basic information they contain.
- Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security
- Explain the essentials of Risk-based Alerting and the Risk framework
- List the common high-level steps of threat hunting using the PEAK framework and practice some common steps of hypothesis hunting with Splunk.

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.

Explore other courses in this learning path:

1. The Cybersecurity Landscape
2. Understanding Threats and Attacks
3. Security Operations and the Defense Analyst
4. Data and tools for Defense
5. The Art of Investigation

It is recommended that you review the full exam blueprint when preparing for the exam.

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