SPLUNK EDUCATION

Course Description

SOC Essentials: Introduction to Threat Hunting

Summary

This course is the last course in the Defense Analyst learning path and is intended for Cybersecurity Defense Analysts or SOC team members who perform threat hunts. This interactive course takes place within the fictional Wonderland SOC. As an analyst-in-training, learners will be guided through the stages of the PEAK Threat Hunting Framework as they practice how to prepare, plan, and gain tools to execute different types of threat hunts.

This eLearning combines videos with activities and includes a hands-on** portion with lab exercises that will challenge the student to practice what they learned. A passing score in the final quiz is required for completion.

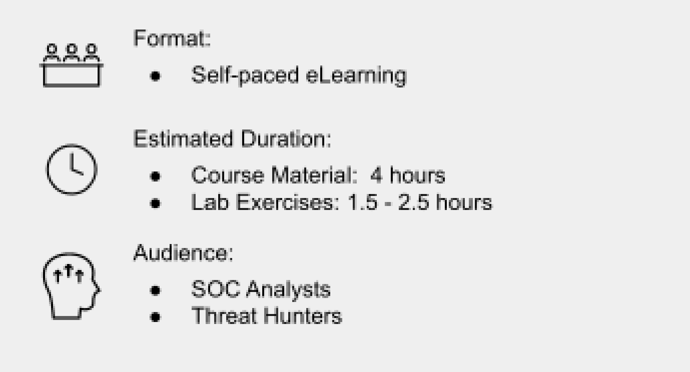
*****This course is available in two versions:** one includes labs, and the other does not. The hands-on experience is available only with the (paid) eLearning version.* ***The free version does not contain labs.***

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

- Describe the importance and impact of threat hunting in a security organization
- Summarize the main steps in the PEAK Threat Hunting Framework
- Determine the best threat hunting approach for a given scenario
- Follow best practices to plan for hypothesis-based or baseline threat hunts following the PEAK Framework
- Describe common methods to identify outliers in a data set
- Use Splunk for basic searches and to identify outliers in a data set
- Describe the high level steps for a Model-assisted Threat Hunting approach

Prerequisites

- To be successful students should 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
- The following Splunk courses are also highly recommended:
  - Intro to Splunk
  - Using fields
  - Previous courses in the Defense Analyst learning path



Format:

- Self-paced eLearning

Estimated Duration:

- Course Material: 4 hours
- Lab Exercises: 1.5 - 2.5 hours

Audience:

- SOC Analysts
- Threat Hunters

Course Outline

Module 1 – Threat Hunting

- Introduction
- The PEAK Threat Hunting Framework

Module 2 – Hypothesis-driven Hunting

- Overview
- Practice: Choose a Hypothesis

- Practice: Scope and Plan
- Execute and Act
- Threat Hunter Toolbox: Regex and Sorting Through Data 101

Module 3 – Baseline Threat Hunting

- Overview
- Threat Hunter Toolbox - The Power of Statistics
- Baseline Threat Hunting with Splunk

Module 4 – Model-Assisted Threat Hunting

- Overview

Module 5 – Course Wrap up

- Course Summary
- Course Quiz
- Next Steps and Resources

Hands-on Lab Activities**

- Prepare for a hunt in a new environment**
- Going on a hypothesis-based threat hunt **
- Hunting practice: Sorting through data with SPL**
- Practice hunting with Windows Event Codes **
- The Threat Hunter's Toolbox - Using Splunk Analytic Stories for hunting **

** ***For courses include labs, the experience uses the following Splunk tools:***

- Splunk Enterprise Version: 9.1.1
- Enterprise Security (ES) Version: 8.0.2

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:

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
6. SOC Essentials: Investigating with Splunk
7. 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 education@splunk.com.