SOC Essentials: Investigating and Threat Hunting

(SP-SOCEITH)

COURSE OVERVIEW

This course is part of 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 defense engineers and Splunk Enterprise Security or Splunk SOAR administrators who provide support to these roles.

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, as well as practice some common tasks using SOAR. You will also learn about the PEAK Threat Hunting framework and will apply its basic concepts in a hypothesis-driven threat-hunting exercise.

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, 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.

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

SOC Essentials: Investigating and Threat Hunting (SP-SOCEITH)

COURSE OUTLINE

Module 1 - Introduction

- The CyberSecurity Defense Analyst
- CIM, Data Models and Correlation Refresh
- Lab 1: Introducing the environment

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
- Lab 2: Pick up an investigation

Module 3 - Risk Analysis Framework

- Overview
- Lab 3: Continue your investigation with RBA

Module 4 - Working with Splunk SOAR

- Introducing Splunk SOAR
- Lab 4: Splunk SOAR Practice

Module 5 - Threat Hunting with PEAK

- PEAK Framework overview
- Lab 5: Hypothesis-based Threat Hunting Practice

Module 6 - Challenge Lab

- Lab 6: Run your own investigation