SOC Essentials: Investigating and Threat Hunting

Category: Networking & Security | **Vendor:** Splunk

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

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 through best practices shared by our security champions, as well as practice some common analyst automation tasks using Splunk SOAR. You will also learn about the PEAK Threat Hunting framework and will apply its basic concepts in hypothesis-driven and baseline threat-hunting exercises.

About This Course

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 through best practices shared by our security champions, as well as practice some common analyst automation tasks using Splunk SOAR. You will also learn about the PEAK Threat Hunting framework and will apply its basic concepts in hypothesis-driven and baseline threat-hunting exercises.

Who Should Attend

- SOC Analysts
- Defense Engineers
- Splunk Admins who support these roles

Prerequisites & Entry Requirements

General 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 (SUF)
- Previous courses in the Defense Analyst learning path

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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.

Detailed 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

- 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

- Lab 3: Continue your investigation with RBA

Module 4 – Working with Splunk SOAR

- Lab 4: Splunk SOAR Practice

Module 5 – Threat Hunting Introduction

- Lab 5: Hunting with Windows Event Codes

Module 6 – Threat Hunting with PEAK: Hypothesis-based Hunt

- Lab 6: Hypothesis-based Threat Hunting Practice

Module 7 – Threat Hunting with PEAK: Baseline Hunt

- Lab 7: Baseline Threat Hunting Practice

This lab experience is using the following Splunk tools:

- Splunk Enterprise Version: 9.1.1

- Enterprise Security (ES) Version: 8.1.0

- Splunk SOAR Version: 6.4.1

Skills You Will Learn:

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.

Frequently Asked Questions

Q: What delivery options are available for SOC Essentials: Investigating and Threat Hunting?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day SOC Essentials: Investigating and Threat Hunting course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the SOC Essentials: Investigating and Threat Hunting training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for SOC Essentials: Investigating and Threat Hunting?

Yes, we provide corporate training, dedicated training, and closed classes for SOC Essentials: Investigating and Threat Hunting. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: SOC Essentials: Investigating and Threat Hunting, SOC Analyst (Enterprise Security), SEITH

Q: Why choose Nexus Human for SOC Essentials: Investigating and Threat Hunting?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your SOC Essentials: Investigating and Threat Hunting training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)