SPLUNK EDUCATION

Course Description

The Art of Investigation

Summary

This is the fifth 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, or anyone in security defensive roles that require investigative work. This interactive course takes place within the fictional Wonderland Security Operations Center (SOC). As an analyst-in-training with the Wonderland SOC, you will shadow other analysts to build skills and test yourself. During the experience, learners will "ride-along" with a Wonderland analyst during security investigations to build and hone critical thinking skills.

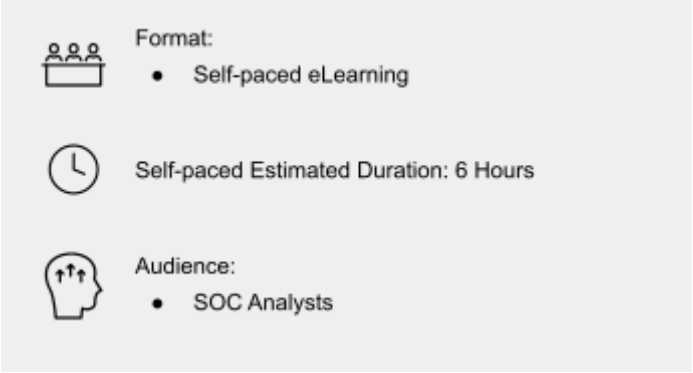
This is an e-learning course that combines videos with activities and knowledge checks. A quiz is available at the end and is required for course completion.

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

- Apply the five basic stages of investigation according to Splunk
- Understand how common SPL terms can be used during investigations
- Explain the use and function of interesting fields within Splunk with a focus on Security use cases.
- Identify common CIM fields that may be used in investigations.
- Distinguish common dispositions of events and correctly assign them.

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



Course Outline

Module 1 – Ground Zero - The Art of Investigation

- Introduction
- Put on your critical thinking cap
- The “art” of investigation
- Ride-alongs with our SOC Analysts

Module 2 – Ride-along 1

- **Skill level:** Beginner
- **Estimated time**: 60-75 minutes
- **Lessons:** 5
- **Short Description:** Join Robin in three mini-investigations looking for insider threats through anomalies.

Module 3 – Ride-along 2

- **Skill level:** Beginner/Intermediate
- **Estimated time**: 60-90 minutes
- **Lessons**: 6
- **Short Description**: There is a strange IP address lurking in the logs. Join Ashley on this investigation for the Splunk T-Shirt Company.

Module 4 – Ride-along 3

- **Skill level**: Intermediate/Advanced
- **Estimated time:** 80-120 minutes
- **Lessons:** 12
- **Short Description:** Join Robin for an in-depth investigation involving Frohtly, Windows workstations, and a Domain Controller. There's trouble bubbling up for Frothly's IT department.

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.

