SPLUNK EDUCATION

Course Description

Data and Tools for Defense Analysts

Summary

This course is intended for anyone who wants to begin or advance a career as a Security Analyst within a SOC. This is the fourth course in the Defense Analyst learning path and marks the beginning of a more focused learning experience, introducing learners to the tools and data used by analysts in a SOC. This course is presented as an interactive experience, featuring the fictional Wonderland SOC and its staff. The course builds on general security knowledge from previous courses to emphasize the specific sources of security data, tools and resources that a cyber defense analyst needs to successfully investigate security events.

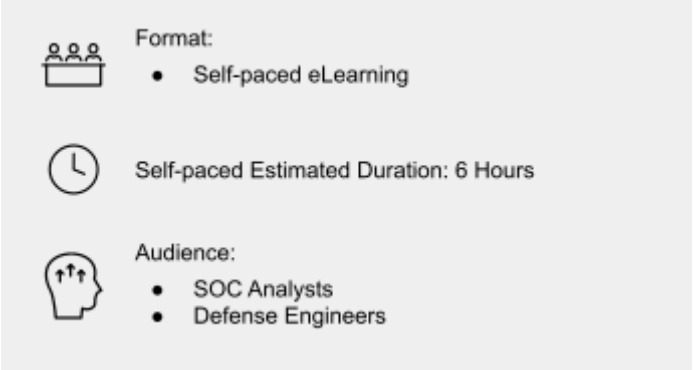
This is an e-learning course that combines videos with activities and knowledge checks. A quiz is available at the end and is required for course completion.

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

- Identify common types of cyber defense systems, analysis tools, and useful data sources for threat analysis for both on-premises and cloud security.
- Identify the common tiers of Threat Intelligence and how they might be applied to threat analysis.
- Search Intelligence sources for information on potential Indicators of Compromise.
- Describe SIEM best practices and basic operation concepts of Splunk Enterprise Security, like CIM, Data Models, and acceleration.
- Explain and use common SPL commands, including TSTATS, TRANSACTION, FIRST/LAST, REX, EVAL, and LOOKUP.
- Provide examples of Splunk best practices for composing efficient searches.
- Identify SPL resources including Splunk Security Essentials and Splunk Lantern.
- Describe how Splunk Security Essentials can be used to assess data sources or content for a given sourcetype.
- Analyze information concerning a security event, and determine which sources of data may best guide an investigation.

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 – Introducing the Wonderland SOC

- SOC Operations
- Tools for Analysts

- Data for Defense
- Frothly's Architecture
- Find Frothly's Data

Module 2 – Putting data into context

- Cyber Threat Intelligence
- Using Cyber Threat Intelligence
- Final thoughts

Module 3 – Diving into the wire

- Working with Data in splunk
- The Splunk Common Information Model (CIM)
- Splunk Data Models
- Splunk Search Processing Language (SPL)
- Transforming your Results
- Searching with Data Models
- Better Searching

Module 4 – Putting it all to work

- Activity 1: Evidence in the Cloud
- Activity 2: Through the looking glass
- Activity 3: Infected
- Wrap up

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.