SPLUNK EDUCATION

Course Description

Understanding Threats and Attacks

Summary

Understanding Threats and Attacks is the second of three courses in the Defense Analyst learning path that serve as an introduction to the world of cybersecurity. These courses are intended for learners who want to begin or advance a career as a Security Analyst within a SOC. This course includes important concepts, tools and resources to help learners understand the most common threats and attacks organizations are faced with today. It includes episodes of the "Once Upon an Attack (OUAA)" web series to complement the course experience.

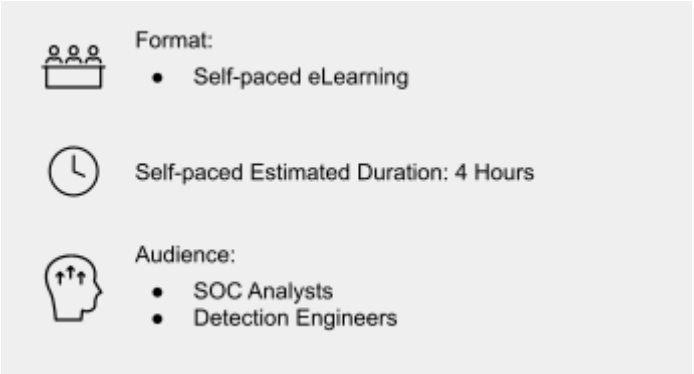
This is an e-learning course that combines videos with activities and knowledge checks. A quiz is available at the end and is required for course completion.

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

- Identify common motivations for attacks
- Describe the basics of advanced persistent threats
- Recognize common types of attacks and attack vectors
- Recognize commonly seen tactics, techniques and procedures
- Navigate the MITRE ATT&CK® matrices and frameworks
- Recognize common analytic frameworks
- Understand how the Pyramid of Pain classifies Indicators of Compromise

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
- It is recommended to have completed the Cybersecurity Landscape course or have equivalent knowledge



Course Outline

Module 1 – The Attackers

- What are we defending against?
- Threat Spotlight: Phishing Campaigns and Credential Compromise
- Common Vulnerabilities and Exposures
- Threat Spotlight: Denial of Service and Botnets

Module 2 – Tactics, Techniques and Procedures

- Introduction
- Threat Spotlight: Exploiting Cloud and Web Vulnerabilities
- Navigating the MITRE ATT&CK™ Enterprise Matrix
- Threat Spotlight: Malware
- The Pyramid of Pain

Module 3 – Analytic Frameworks

- MITRE ATT&CK™ Enterprise Matrix, The Lockheed Martin Cyber Kill Chain ® and the Diamond Model of Intrusion Analysis
- Threat Spotlight: Insider Threats
- Threat Spotlight: Supply Chain Attacks

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.