

Security Operations and the Defense Analyst

Summary

Security Operations and the Defense Analyst is the last 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. The course includes important perspectives and experiences of professionals that have had successful careers within a SOC. The course includes interviews with Splunk Security champions who provide depth and insight into the role of an analyst, and life in the SOC.

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

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

- Describe a typical Security Operations organization
- Summarize the organization of a typical SOC
- Explain the role of the Cyber Analyst and the tasks belonging to Analyst, Engineer and Architect roles
- Describe common performance measurements for Analysts like dwell time, MTTD, MTTR, and how analysts can help define which metrics will be used.

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 also recommended to have completed the Cybersecurity Landscape and Understanding Threats and Attacks courses.



Format:

- Self-paced eLearning



Self-paced Estimated Duration: 2 Hours



Audience:

- SOC Analysts
- Detection Engineers

Course Outline

Module 1 – Cybersecurity Operations

- Introduction
- Interview with Splunk Advanced Response Team Manager, Tony Iacobelli

Module 2 – The Security Operations Center (SOC)

- Introduction
- Common Technologies
- Roles and Responsibilities
- Interview with Security Strategist, Haylee Mills

Module 3 – The Cybersecurity Defense Analyst

- Who is the Defense Analyst?
- Interview with Director of Splunk Security Interlock, Katie Brown

Module 4 – Measuring Success

- Common SOC Metrics
- Interview with Tony I. and Katie B.

Module 5 – Course Wrap up

- Words of advice from Splunk Security champions

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.

