SEC 551 - Leading Effective Security Operations Centers

- 5 Days
- Lecture and Hands-on Labs

Course Overview

This course is the functional equivilant of the LDR551 and prepares students to build or improve the Security Operations Center (SOC) and the leadership thereof. Students will learn to how to build the SOC, perform threat modeling and defense theory, understand threat detection, build response incident plans, and learn to understand and appreciate metrics to improve operations and the team. The course also prepares students for the GIAC Security Operations Manager Certification (GSOM). ## Who Should Attend

- Cyber security professionals
- Business leaders seeking cyber security insights
- Developers expanding knowledge of threats and trends
- Managers building secure programs and policies
- Specifically those building or improving a Security Operations Center (SOC)

What You'll Learn

- Prepare for the GSOM certification
- Learn mechanisms for improving the SOC and the supporting team
- Get hands on with tools like pcaps, Wireshark, TCPDump, ATT&CK Navigator and many more
- Proactive threat scanning
- Response incident planning
- Building a better SOC through metric analysis
- SOC building and design

Outline

Day 01 - Foundations of SOC Leadership and Strategic Planning

- 💬 Lecture: Course Overview

What Business Are You In?

- 💬 Lecture: Vision vs Mission
- 💬 Lecture: Identifying Stakeholders
- 💬 Lecture: Understanding History
- 💬 Lecture: Assets
- 💬 Lecture: Business and Security Goals

What are Cybersecurity Threats?

- 💬 Lecture: CyberSecurity History
- 💬 Lecture: Threat Actors

- 💻 Lecture + Lab: Attack Paths with Attack Flow

- 💬 Lecture: MITRE ATT&CK Framework
- 💻 Lecture + Lab: MITRE ATT&CK Navigator
- 💬 Lecture: Intrusion Kill Chain
- 💬 Lecture: Identifying Unique Attack Surfaces

Overview of SOC Operations

- 💬 Lecture: SOC Role in Cyber Defense
- 💻 Lecture + Lab: Decoding Operations Reports
- 💬 Lecture: SOC Design and Planning

Day 02 - Core SOC Functions and Tools

- 💬 Lecture: Current Trends #### Cyber Defense Industry Trends
- 💬 Lecture: Threat Intelligence
- 💬 Lecture: Defensible Architecture #### Building SOC Types
- 💬 Lecture: Building a Lean SOC
- 💬 Lecture: Building a Virtual SOC

Mapping the Core SOC Functions

- 💬 Lecture: Data Collection
- 💬 Lecture: Detection
- 💬 Lecture: Triage
- 💻 Lecture + Lab: Attack Path and Data Source
- 💬 Lecture: Incident Response and Reporting
- 💻 Lecture + Lab: Incident Response and Reporting
- 💬 Lecture: SOC Workflows
- 💻 Lecture + Lab: Mapping Core SOC Functions

SOC Tools & Tech Overview

- 💬 Lecture: SOC Tools and Technology Overview
- 💬 Lecture: Automation for the SOC Team
- 💬 Lecture: Analytic Frameworks and Tools

Day 03 - Build and Maintain SOC

- 💬 Lecture: Team Creation, Hiring, and Training Overview
- 💻 Lecture + Lab: Lab Roles
- 💬 Lecture: Effective Alerting
- 💻 Lecture + Lab: Investigations and Improvements
- 💬 Lecture: Staff Retention and Burnout Mitigation

SOC Network Tracing Tools

- 💻 Lecture + Lab: Introduction to Using Wireshark
- 💬 Lecture: Starting and Stopping Captures with Wireshark
- 💻 Lecture + Lab: Using TCPdump to make pcap Files for Wireshark
- 💻 Lecture + Lab: Introduction to Termshark
- 💻 Lecture + Lab: Find packet
- 💻 Lecture + Lab: Flow and IO Graphs

SOC Scripting and Data Tools

- 💻 Lecture + Lab: Introduction to Jupyter Notebook
- 💻 Lecture + Lab: Using VSCode

Day 04 - Incident Response and Improvement

- 💬 Lecture: Planning and Preparation
- 💬 Lecture: Playbooks and Protocols
- 💬 Lecture: Cloud Based Environments
- 💬 Lecture: Incident Response Execution
- 💬 Lecture: Investigations and Response Phases
- 💬 Lecture: Containing and Eradicating Threats
- 💻 Lecture + Lab: Building Playbooks
- 💬 Lecture: Post Incident Analysis and Continuous Improvement
- 💬 Lecture: Identifying Gaps and Optimization of SOC Ops
- 💬 Lecture: Analytic Testing and Adversarial Emulation
- 💻 Lecture + Lab: Designing an Exercise
- 💬 Lecture: Proactive Detection and Threat Hunting
- 💻 Lecture + Lab: Threat Hunting
- 💬 Lecture: Active Defense Techniques

Day 05 - Metrics, Performance, and Strategic Leadership

- 💬 Lecture: SOC Metrics and KPIs
- 💻 Lecture + Lab: Defining and Measuring Metrics
- 💬 Lecture: SOC Effectiveness
- 💬 Lecture: Metrics
- 💻 Lecture + Lab: Organizing Use Cases
- 💬 Lecture: Metrics Goals and Effective Execution
- 💻 Lecture + Lab: Improvements for the SOC
- 💬 Lecture: Designing a Strategic SOC Plan

Appendix

- References and Additional Reading
- Glossary

Prerequisites

There are no pre-requisites for this class.

Next Courses

- Alta3 Research TCP IP (3 days) (https://alta3.com/courses/tcp-ip)
- Alta3 Research Security Leadership - Strategy, Policy and Planning (5 days) (https://alta3.com/courses/leading-security)