Faysal Aziz

Mastering Advanced Security Operations Center (SOC) Techniques

FA-0460 · 5-Days

DevOps, Cloud & Infrastructure · Cybersecurity · Automation, RPA & Power Platform

---

Introduction

5-Days

In today's rapidly evolving cybersecurity landscape, Security Operations Centers (SOCs) serve as the frontline defense for organizations against a multitude of cyber threats. As these threats become more sophisticated, it is imperative for SOC professionals to advance their skills and knowledge to stay ahead of potential attackers. This advanced SOC training course is designed to empower security professionals with cutting-edge techniques, tools, and methodologies necessary for operating an effective and resilient SOC. With over 30 years of industry experience, the course instructor will share real-world insights and practices that are highly demanded by the industry, ensuring that the content is practical, relevant, and immediately applicable.

Learning outcomes

By the end of this course, participants will be able to:

- Implement advanced threat detection and analysis techniques.
- Utilize cutting-edge tools and technologies to enhance SOC operations.
- Perform in-depth incident response and forensic investigations.
- Develop and optimize SOC processes, including automation and orchestration.
- Apply threat intelligence to strengthen proactive defense mechanisms.
- Conduct red team/blue team exercises for continuous improvement of SOC capabilities.
- Manage and mitigate complex security incidents with confidence.

Prerequisites

Participants should have:

- A solid understanding of basic SOC operations and cybersecurity principles.
- Prior experience with security monitoring, incident detection, and response.
- Familiarity with security tools such as SIEM, IDS/IPS, and firewalls.
- Basic knowledge of network protocols, operating systems, and cybersecurity frameworks.
- Eagerness to learn advanced techniques and apply them in real-world scenarios.

Training outline

1. 1. Advanced Threat Detection and Analysis

Enhanced Threat Hunting Techniques

- Understanding threat hunting methodologies.
- Leveraging advanced SIEM capabilities for proactive threat detection.
- Utilizing machine learning and AI in threat hunting.
- Practical threat hunting exercises.

Behavioral Analysis and Anomaly Detection

- Analyzing user and entity behavior analytics (UEBA).
- Implementing behavioral baselines and anomaly detection.
- Case studies on identifying sophisticated threats through behavior analysis.

2. 2. Cutting-Edge SOC Tools and Technologies

Advanced Security Information and Event Management (SIEM)

- Customizing SIEM for advanced threat detection.
- Creating and optimizing complex correlation rules.
- SIEM use cases and real-world applications.

Next-Generation Endpoint Detection and Response (EDR)

- Deep dive into EDR capabilities and integrations.
- Advanced techniques for detecting and responding to endpoint threats.
- Hands-on with leading EDR tools.

Network Traffic Analysis and Monitoring

- Leveraging network analysis tools for advanced threat detection.
- Deep packet inspection and analysis.

- Identifying and mitigating network-based threats.

3. 3. Incident Response and Forensic Investigation

Advanced Incident Response Techniques

- Incident response lifecycle and advanced methodologies.
- Utilizing playbooks for effective incident management.
- Real-world incident response scenarios and case studies.

Digital Forensics and Evidence Handling

- In-depth analysis of digital evidence and forensic techniques.
- Handling and preserving evidence in complex environments.
- Forensic tools and their applications in SOC.

Malware Analysis and Reverse Engineering

- Introduction to reverse engineering malware.
- Static and dynamic analysis techniques.
- Tools and techniques for malware analysis.

4. 4. SOC Process Optimization and Automation

Security Orchestration, Automation, and Response (SOAR)

- Introduction to SOAR platforms and their role in SOC.
- Automating repetitive tasks and incident response processes.
- Developing and deploying playbooks within SOAR.

SOC Metrics and Performance Management

- Key performance indicators (KPIs) for SOC efficiency.
- Continuous improvement through metrics and feedback loops.
- Benchmarking SOC performance against industry standards.

Process Improvement and SOC Maturity Models

- Assessing and improving SOC maturity.
- Implementing best practices for process optimization.
- Case studies on successful SOC transformation.

5. 5. Proactive Defense and Threat Intelligence

Integrating Threat Intelligence into SOC Operations

- Types of threat intelligence and their applications.
- Automating threat intelligence gathering and dissemination.

- Utilizing threat intelligence for proactive defense.

Red Team/Blue Team Exercises

- Understanding the roles and objectives of red and blue teams.
- Conducting and analyzing red team/blue team exercises.
- Using results to enhance SOC capabilities and defenses.

Proactive Threat Mitigation Strategies

- Developing proactive defense mechanisms.
- Implementing advanced deception techniques and honeypots.
- Case studies on proactive threat mitigation in action.

This advanced SOC training will not only refine your existing skills but also equip you with the expertise needed to tackle the ever-growing challenges in the cybersecurity realm. Whether you are looking to upgrade your current SOC practices or prepare for the next wave of cyber threats, this course offers the comprehensive knowledge and practical skills necessary to excel.

© 2026 Faysal Aziz · Kuala Lumpur