CERTIFIED SECURITY OPERATIONS MANAGER

Course Syllabus

Built by experienced security leaders across military, finance, telecommunications, and managed security, CSOM provides established or aspiring security managers with the knowledge they need to develop a high-performing security operations team.

200+ Lessons, Tests and Labs // 6 Months Access to the content //
2 Years Relevant Experience Required to Take CSOM*

Syllabus

Content subject to change prior to release.
Approx 250 lessons, 15 labs

Introduction

1. Welcome to CSOM

Modern Security Operations

2. Domain Introduction
3. Business Objectives, Legal Enablers, and Considerations
4. Security Operations Teams

Building a Security Operations Centre

5. Domain Introduction
6. Threat Modelling
7. Building Your Team
8. SIEM & Detection Engineering
9. Case Management
10. Other Tooling & Administration
11. Processes and Policies

Capability Development

12. Domain Introduction
13. Incident Response
14. Threat Intelligence
15. Vulnerability Management
16. Digital Forensics
17. Malware Analysis
18. Threat Hunting

Metrics, Maturity, and Measuring Success

19. Domain Introduction
20. SOC Maturity Models
21. Operationalizing MITRE ATT&CK
22. Deception and Active Defense
23. Security Orchestration, Automation, and Response
24. Reporting and Metrics
25. Retaining Talent
26. Additional Activities

CSOM Exam Preparation

27. Theory Exam Format
28. Practical Exam Format
29. Preparation Tips

*To be eligible to take the CSOM exam, students must provide sufficient evidence of at least two years full-time experience working in a defensive cybersecurity role. Students are able to take and go through the course with any level of experience, however to become CSOM certified, this requirement must be met.