CERTIFIED SECURITY OPERATIONS MANAGER

Course Syllabus

Built by experienced security leaders across military, finance, telecommunications, healthcare, and managed security industries, CSOM has been designed to provide 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
5. Operational Environments
6. Cyber Threat Hunting

Building a Security Operations Centre

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

Capability Development

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

Metrics, Maturity, and Measuring Success

21. Domain Introduction
22. SOC Maturity Models
23. Operationalizing MITRE ATT&CK
24. Purple Team Engagements
25. Deception and Active Defense
26. Security Orchestration, Automation, and Response
27. Reporting and Metrics
28. Security Research and Presentation
29. Retaining Talent
30. Additional Activities

CSOM Exam Preparation

31. Theory Exam Format
32. Practical Exam Format
33. 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.