800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

# Security Blue Team Certified Security Operations Manager Training

**Centri Authorized Training · Applied Technology Academy**

Learn to build, staff, and mature security operations, covering metrics, threat modeling, and MITRE ATT&CK strategy.

| LEVEL | DURATION | EXPERIENCE | AVERAGE SALARY | LABS |
|---|---|---|---|---|
| **Advanced** | **4 Days** | **2+ year: SOC Manager** | **$140,000** | **Yes** |

## Course Overview

This Security Operations Management training is designed for leaders, focusing on how to plan, build, and mature security operations teams within an enterprise. You will gain the strategic and managerial knowledge required to effectively lead functions like Incident Response, Threat Hunting, and SIEM. The course emphasizes governance, metrics, and managing people and processes to mature the entire security operations capability.

## Course Outline

- **Module 1: Modern Security Operations**
  - Business Objectives, Legal Enablers, and Considerations (Aligning SOC with Governance)
  - Security Operations Team (Roles, Structure, and Collaboration Models)
- **Module 2: Building a Security Operations Team**
  - Threat Modelling (Techniques and methodologies for identifying organizational threats)
  - Building Your Team (Staffing, Training, and Organizational Placement)
  - SIEM & Detection Engineering (Strategic planning and selection of detection technologies)
  - Case Management (Process, standardization, and tooling)
  - Other Tooling & Administration (Vulnerability Scanners, Endpoint tools, etc.)
  - Processes and Documentation (Playbooks, Runbooks, SOPs)
- **Module 3: Capability Development**
  - Incident Response (Building the full lifecycle capability)
  - Threat Intelligence (Integration into SOC workflows and strategic decision-making)
  - Vulnerability Management (Process ownership and cross-functional remediation)
  - Digital Forensics (Establishing forensic readiness and collection capabilities)
  - Malware Analysis (Integrating analysis output into detection)
  - Threat Hunting (Establishing a hunting program and team structure)
- **Module 4: Metrics, Maturity, and Measuring Success**

- Maturity Models (Using frameworks to assess and advance SOC capability)
- Operationalizing MITRE ATT&CK (Mapping detections and controls to adversary tactics)
- Cyber Deception (Implementing deception techniques like honeypots)
- Security Orchestration, Automation, and Response (SOAR) (Strategy and implementation)
- Reporting and Metrics (KPIs, KRIs, Executive Reporting, and Dashboards)
- Security Research & Presentation (Staying current and communicating risk to leadership)
- Retaining Talent (Strategies for team morale and skill development)

## Intended Audience

- Security Managers
- SOC Managers
- Heads of Security Operations
- Directors of Security Operations
- Consultants

## Prerequisites

2+ years security management experience

## Follow-On Courses

- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CGEIT (Certified in the Governance of Enterprise IT)

**Ready to enroll?** Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.