Enterprise Security Operations Center Management Training Course



14 - 18 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CYB9014_88791

Course Introduction / Overview:

In today's hyper-connected digital landscape, the effective management of a Security Operations Center (SOC) is no longer a luxury but a fundamental necessity for enterprise survival. This course provides a comprehensive, A-to-Z exploration of building, managing, and optimizing a modern enterprise SOC. We delve beyond basic monitoring to cover strategic planning, technology integration, process maturity, and leadership excellence. As discussed by cybersecurity expert Richard Bejtlich in works like "The Practice of Network Security Monitoring," a proactive and intelligence-driven approach is paramount. This program is designed to equip participants with the advanced skills needed to transform their SOC from a reactive cost center into a proactive, value-driving security powerhouse. At BIG BEN Training Center, we focus on a holistic framework that integrates people, processes, and technology to create a resilient and adaptive security posture, capable of defending against the sophisticated cyber threats of today and tomorrow. This training course is meticulously structured to provide actionable insights and practical strategies that can be immediately applied to enhance your organization's security operations and overall cyber defense capabilities.

Target Audience / This training course is suitable for:

- SOC Managers and Team Leads.
- Senior Security Analysts and Engineers.
- Cybersecurity Directors and Managers.
- IT Security and Information Security Professionals.
- Incident Response Team Members.
- Cybersecurity Consultants and Advisors.
- Individuals aspiring to a leadership role in cybersecurity operations.
- Risk and Compliance Managers.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical.
- Government and Public Sector Agencies.
- Technology and Telecommunications.
- Energy, Oil, and Gas.
- Retail and E-commerce.
- Critical Infrastructure and Utilities.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology Department.
- Cybersecurity and Information Security Department.
- Risk Management and Compliance.
- Internal Audit and Governance.
- Network Operations.
- Incident Response Teams.
- Security Operations Center (SOC).

Course Offerings:

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

- Develop a strategic vision and roadmap for an enterprise-level SOC.
- Master the complete incident response lifecycle from detection to post-incident analysis.
- Evaluate, select, and optimize core SOC technologies like SIEM and SOAR.
- Build, train, and lead high-performing cybersecurity teams.
- Implement a metrics-driven approach to measure SOC effectiveness using KPIs.
- Integrate threat intelligence into daily security operations for proactive defense.
- Design and implement effective security monitoring and threat hunting strategies.
- Ensure SOC operations align with business objectives and regulatory compliance.
- Manage stakeholder communication and reporting during security incidents.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical, ensuring participants gain skills they can apply immediately in their professional roles. We move beyond traditional lecture-based formats to create a dynamic learning environment. The course heavily relies on real-world case studies of major security incidents, allowing participants to analyze complex scenarios and develop strategic responses. Interactive group discussions and collaborative workshops encourage the sharing of diverse experiences and perspectives, fostering a deeper understanding of SOC management challenges. Practical exercises and simulation-based activities will challenge participants to apply concepts related to incident handling, playbook development, and technology evaluation. Our expert instructors facilitate sessions that are rich with practical examples, best-practice frameworks, and actionable insights. Continuous feedback and Q&A sessions are integrated throughout the course to address specific queries and ensure a clear grasp of all topics, creating a comprehensive and engaging educational experience.

Course Agenda (Course Units):

Unit One: Foundations of Modern SOC Strategy and Governance

- Defining the mission and vision of the enterprise SOC.
- Exploring different SOC models (in-house, outsourced, hybrid).
- Developing a comprehensive SOC governance framework.
- Aligning SOC strategy with overall business objectives.
- Understanding key legal, regulatory, and compliance requirements.
- Budgeting and resource planning for SOC operations.
- Establishing the SOC charter and stakeholder engagement plan.

Unit Two: Core Technologies and Infrastructure

- Deep dive into Security Information and Event Management (SIEM) architecture.
- Leveraging Security Orchestration, Automation, and Response (SOAR).
- Integrating Threat Intelligence Platforms (TIPs) effectively.
- Utilizing Endpoint Detection and Response (EDR) and Network Detection and Response (NDR).
- Managing log sources and developing a data collection strategy.
- Technology evaluation, procurement, and lifecycle management.
- Optimizing the SOC technology stack for maximum efficiency.

Unit Three: Mastering SOC Processes and Operations

- Designing the incident response lifecycle and procedures.
- Developing and implementing effective SOC playbooks.
- Establishing a proactive threat hunting program.
- Managing vulnerability assessment and remediation processes.
- Conducting digital forensics and malware analysis basics.
- Implementing continuous security monitoring and alerting triage.
- Workflow optimization and process automation within the SOC.

Unit Four: Leadership, Team Management, and Performance Metrics

- Building and structuring a high-performance SOC team.
- Defining roles, responsibilities, and career paths for SOC analysts.
- Effective leadership, communication, and decision-making in a crisis.
- Developing and managing a continuous training and skills development program.
- Defining and tracking Key Performance Indicators (KPIs) and metrics.
- Creating effective dashboards and reports for different stakeholders.
- Managing analyst burnout and maintaining team morale.

Unit Five: Advanced SOC Strategies and Future Trends

- Managing security operations in cloud and hybrid environments.
- Leveraging Artificial Intelligence (AI) and Machine Learning (ML) in the SOC.
- Participating in threat intelligence sharing communities (ISACs).
- Conducting red team, blue team, and purple team exercises.
- Developing a SOC maturity model and continuous improvement plan.
- Communicating risk and SOC value to executive leadership.
- Preparing for future threats and the evolution of cybersecurity.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As automation and AI become more integrated into SOC operations, what is the evolving role of human intuition and expertise in threat detection and response?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, strategic management perspective on Security Operations Center leadership, rather than focusing narrowly on specific tools or vendor platforms. While technical proficiency is essential, we emphasize the integration of people, processes, and technology under a unified governance framework. Our curriculum is built around real-world case studies and strategic decision-making scenarios, compelling participants to think like cybersecurity leaders who must align security initiatives with business objectives and manage risk effectively. Unlike other programs that may concentrate solely on the analyst's role, this course is designed for current and future managers, focusing on team building, performance metrics, stakeholder communication, and continuous process improvement. The content moves beyond reactive incident response to instill a proactive mindset, covering advanced topics like threat hunting, intelligence integration, and preparing for the future cyber landscape. It provides a comprehensive blueprint for building and maturing a SOC that not only defends the enterprise but also delivers demonstrable value and resilience.