Training Course on Building a Security Operations Center (SOC) for IR

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s digital age, organizations face increasingly complex and persistent cybersecurity threats. Building a robust Security Operations Center (SOC) is critical to detect, monitor, analyze, and respond to incidents in real time. Training Course on Building a Security Operations Center (SOC) for Incident Response (IR) provides professionals with the hands-on skills and strategic insights required to establish and manage an efficient SOC tailored for Incident Response (IR). Participants will explore SOC frameworks, operational procedures, threat intelligence integration, and automation techniques.

This intensive training combines theoretical knowledge with real-world applications, preparing cybersecurity personnel to mitigate risks and secure enterprise assets. Emphasizing real-time threat detection, SIEM architecture, and SOC team structuring, this course is designed for IT leaders, cybersecurity analysts, and response teams. Through practical labs, case studies, and simulation exercises, attendees will gain critical decision-making skills and proficiency in cyber threat hunting, incident triage, and attack surface monitoring.

Programme Curriculum

Training Course on Building a Security Operations Center (SOC) for Incident Response (IR)

Introduction

In today’s digital age, organizations face increasingly complex and persistent cybersecurity threats. Building a robust Security Operations Center (SOC) is critical to detect, monitor, analyze, and respond to incidents in real time. Training Course on Building a Security Operations Center (SOC) for Incident Response (IR) provides professionals with the hands-on skills and strategic insights required to establish and manage an efficient SOC tailored for Incident Response (IR). Participants will explore SOC frameworks, operational procedures, threat intelligence integration, and automation techniques.

This intensive training combines theoretical knowledge with real-world applications, preparing cybersecurity personnel to mitigate risks and secure enterprise assets. Emphasizing real-time threat detection, SIEM architecture, and SOC team structuring, this course is designed for IT leaders, cybersecurity analysts, and response teams. Through practical labs, case studies, and simulation exercises, attendees will gain critical decision-making skills and proficiency in cyber threat hunting, incident triage, and attack surface monitoring.

Course Objectives

1. Understand the architecture and core components of a modern Security Operations Center (SOC).
2. Learn advanced cyber threat detection and prevention strategies.
3. Master the configuration and optimization of SIEM tools.
4. Develop and implement incident response playbooks.
5. Design effective SOC workflows and escalation matrices.
6. Analyze real-world SOC breach case studies.
7. Identify and mitigate false positives and alert fatigue.
8. Utilize threat intelligence feeds for proactive defense.
9. Automate SOC operations using SOAR platforms.
10. Build and scale a SOC team with defined roles.
11. Ensure compliance with NIST, ISO 27001, and GDPR frameworks.
12. Integrate endpoint detection and response (EDR) tools into SOC.
13. Conduct post-incident forensics and recovery planning.

Target Audience:

1. Cybersecurity Analysts
2. SOC Managers
3. Incident Response Teams
4. IT Security Engineers
5. Risk & Compliance Officers
6. Network Security Architects
7. Cybersecurity Consultants
8. CISO & Security Leaders

Course Duration: 5 days

Course Modules

Module 1: Introduction to SOC & Threat Landscape

- Overview of SOC functions and value
- Evolution of cyber threats and attack vectors
- Types of SOC (in-house, hybrid, MSSP)
- Key SOC KPIs and success metrics
- SOC maturity models and global standards
- **Case Study:** Evolution of SOC at a Global Bank

Module 2: SOC Infrastructure and Architecture

- Network design for security monitoring
- SIEM setup and data ingestion pipelines
- Endpoint, cloud, and perimeter integration
- Log collection, normalization, and storage
- SOC toolchain: IDS, EDR, firewalls, UEBA
- **Case Study:** SOC Deployment in a Hybrid Cloud Environment

Module 3: Incident Detection and Triage

- Event correlation and alert management
- Threat hunting and IOC identification
- Detection logic development
- Alert prioritization and triage frameworks
- Use of MITRE ATT&CK for classification
- **Case Study:** Detecting a Nation-State Attack

Module 4: SIEM and Threat Intelligence

- SIEM rule creation and tuning
- Use of open-source vs commercial SIEMs
- Integration of threat intelligence feeds
- STIX/TAXII protocols for threat sharing
- Threat actor profiling and tracking
- **Case Study:** SIEM-Driven Threat Intelligence Use in E-commerce

Module 5: Incident Response Frameworks

- IR process stages: detect, contain, eradicate, recover
- Response playbook development
- Escalation matrices and communication protocols
- Legal and regulatory considerations
- Post-incident analysis and documentation
- **Case Study:** Ransomware Response Playbook in Action

Module 6: Automation and Orchestration (SOAR)

- SOAR capabilities and benefits
- Automated incident triage workflows
- Use of Python/PowerShell for playbooks
- Integration with SIEM and ticketing systems
- Metrics for automation success
- **Case Study:** Reducing MTTR with SOAR at a Tech Enterprise

Module 7: Team Structure and Skill Development

- Defining roles: L1, L2, L3 analysts
- Hiring and skill gap identification
- Training and simulation tools
- Shift scheduling and analyst fatigue
- Continuous learning programs
- **Case Study:** Building a SOC Team from Scratch at a Fintech Startup

Module 8: Compliance, Risk & Future Trends

- Compliance frameworks: NIST, GDPR, ISO 27001
- Risk assessments and SOC audit readiness
- Metrics and continuous improvement
- Future trends: AI in SOC, XDR, SASE
- Building a threat-resilient SOC roadmap
- **Case Study:** Preparing for a SOC 2 Type II Audit

Training Methodology

- Interactive instructor-led training (ILT)

- Hands-on labs using real-world SOC tools
- Group exercises and threat detection simulations
- Live case study walkthroughs
- Scenario-based assessments and quizzes
- Post-training certification exam

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com