Training Course on Incident Response Team Leadership and Management

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 hyper-connected digital era, cyber threats have become increasingly sophisticated and relentless. The effectiveness of an organization’s Incident Response Team (IRT) lies not just in its technical capabilities but in its leadership, management, and crisis response strategy. Training Course on Incident Response Team Leadership and Management is designed for professionals aiming to lead high-performing incident response teams that can rapidly mitigate cyber threats, protect organizational assets, and uphold public trust.

This hands-on, leadership-focused training program equips participants with the practical skills and decision-making frameworks necessary to build, manage, and optimize incident response teams in high-pressure environments. Using real-world scenarios, attendees will learn to coordinate, communicate, and lead through cyber crises with confidence and resilience.

Programme Curriculum

Training Course on Incident Response Team Leadership and Management

Introduction

In today’s hyper-connected digital era, cyber threats have become increasingly sophisticated and relentless. The effectiveness of an organization’s Incident Response Team (IRT) lies not just in its technical capabilities but in its leadership, management, and crisis response strategy. Training Course on Incident Response Team Leadership and Management is designed for professionals aiming to lead high-performing incident response teams that can rapidly mitigate cyber threats, protect organizational assets, and uphold public trust.

This hands-on, leadership-focused training program equips participants with the practical skills and decision-making frameworks necessary to build, manage, and optimize incident response teams in high-pressure environments. Using real-world scenarios, attendees will learn to coordinate, communicate, and lead through cyber crises with confidence and resilience.

Course Objectives

1. Develop cyber crisis leadership skills for fast-paced threat environments.
2. Understand the lifecycle of an incident response plan (IRP) from initiation to recovery.
3. Create scalable and resilient cybersecurity frameworks.
4. Master cyber threat intelligence integration into incident response.
5. Establish clear communication protocols across technical and non-technical stakeholders.
6. Analyze and apply cyber risk management strategies in team leadership.
7. Execute tabletop exercises and live simulations for team preparedness.
8. Lead with compliance and regulatory awareness (e.g., GDPR, HIPAA, NIST).
9. Manage cross-functional cybersecurity teams effectively.
10. Identify and mitigate insider threats and human error vectors.
11. Implement post-incident review strategies for continuous improvement.
12. Leverage automation and AI tools in incident response operations.
13. Align cybersecurity governance with organizational goals and values.

Target Audience

1. CISOs & CIOs
2. IT Security Managers
3. SOC Team Leaders
4. Cybersecurity Consultants
5. IT Risk & Compliance Officers
6. Network & System Administrators
7. Emergency Response Coordinators
8. Government & Military Cybersecurity Personnel

Course Duration: 5 days

Course Modules

Module 1: Foundations of Incident Response Team Leadership

- Define roles and responsibilities within an IRT.
- Establish team mission and escalation procedures.
- Develop leadership presence during crises.
- Analyze leadership styles under stress.
- Integrate leadership in the NIST IR lifecycle.
- **Case Study**: Leadership decisions during the SolarWinds breach.

Module 2: Strategic Planning and Cyber Resilience

- Design an incident response strategy aligned with business goals.
- Build resilient IT architecture for rapid recovery.
- Identify and document critical assets and risk areas.
- Create budget-friendly IR strategies.
- Balance proactive and reactive measures.
- **Case Study**: Strategic planning failures in the Equifax incident.

Module 3: Communication and Coordination in Cyber Crises

- Implement real-time incident reporting protocols.
- Coordinate across internal departments and vendors.
- Manage stakeholder expectations during breaches.
- Leverage secure communication tools.

- Conduct effective post-mortem communication.
- **Case Study**: Crisis communication lessons from the Marriott data breach.

Module 4: Team Building and Performance Management

- Recruit and retain top cyber talent.
- Establish clear KPIs and performance metrics.
- Foster a high-performance team culture.
- Implement continuous feedback systems.
- Design team onboarding and skill development programs.
- **Case Study**: How Google's security teams maintain high performance under pressure.

Module 5: Legal, Compliance, and Governance

- Review legal implications of incident response.
- Understand GDPR, HIPAA, CCPA, and other compliance frameworks.
- Implement governance and audit processes.
- Align policies with industry standards (ISO, NIST).
- Report incidents to regulators and legal authorities.
- **Case Study**: Legal fallout of the Uber data breach cover-up.

Module 6: Advanced Threat Management and AI Integration

- Identify advanced persistent threats (APTs).
- Integrate AI tools in threat detection.
- Respond to zero-day vulnerabilities effectively.
- Monitor emerging threat landscapes.
- Analyze malware using AI-driven platforms.
- **Case Study**: Using AI to detect ransomware in Colonial Pipeline attack.

Module 7: Post-Incident Review and Continuous Improvement

- Conduct root-cause analysis.
- Measure response time and effectiveness.
- Facilitate team debriefs and retrospectives.
- Update response plans based on lessons learned.
- Build institutional memory for future responses.
- **Case Study**: Microsoft's detailed post-incident playbook for cyberattacks.

Module 8: Real-Time Simulation and Tabletop Exercises

- Plan and execute live response simulations.
- Evaluate leadership under pressure.
- Use gamification to assess team readiness.
- Record and analyze simulation outcomes.
- Adjust training programs based on gaps identified.
- **Case Study**: DHS Cyber Storm exercise evaluation.

Training Methodology

- Instructor-led virtual or in-person sessions
- Hands-on lab simulations and role-play exercises
- Case study evaluations and group debriefs
- Live tabletop exercises with real-world attack scenarios
- Team-based assignments and scenario planning
- Interactive leadership coaching and feedback sessions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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