BLACK BEAR
ACADEMY

Certified Digital Forensic and Incident Responder

This course is focused on professionals who wish to acquire skillsets in conducting digital forensics and Incident response after a breach plus counter measures by acquiring cyber threat intelligence related to the tactics, techniques and procedures (TTPs) attributed to the potential threat actors. This covers the investigative methods and standards for the acquisition, extraction, preservation, analysis, and deposition of digital evidence from devices.

Agenda: To equip participants with the skills and knowledge required to effectively conduct digital forensic investigations and manage incident response. The training will focus on enhancing forensic analysis capabilities, improving incident response strategies, understanding legal and ethical considerations, and applying best practices in real-world scenarios.

Audience:

- Digital Forensic Analysts
- Incident Responders
- Security Operations Center (SOC) Analysts
- IT Security Professionals
- Law Enforcement Officers
- Legal and Compliance Teams

Qualifications for This Course:

- Basic Understanding of IT Systems: Participants should have a basic knowledge of computer systems, networking, and information security concepts.
- Experience in IT or Cybersecurity Roles: Prior experience working in IT, system administration, or information security is recommended.
- Familiarity with Cybersecurity Tools and Practices: Experience with security monitoring tools, network traffic analysis, or incident response practices is beneficial, but not mandatory.
- Enthusiasm for Problem-Solving and Investigations: Individuals with an analytical mindset who enjoy investigating and solving complex problems will excel in this

Career Level Advancement:

This certification course is designed for individuals looking to:

- Transition into Forensics and Incident Response Roles: Those working in general IT or cybersecurity roles can use this course to specialize in digital forensics and incident response.

- Get Promoted to Mid-Level or Senior Cybersecurity Roles: Upon completing this course, participants will be qualified for mid-level roles such as Digital Forensic Analyst, Incident Response Specialist, or SOC Analyst.
- Pursue Leadership Roles: With further experience, certified participants can advance to leadership positions such as Incident Response Manager, SOC Manager, or Cybersecurity Team Lead.
- Leverage the Certification for Job Opportunities: The certification is valuable for roles in cybersecurity firms, law enforcement agencies, and government bodies that require digital forensics expertise.

Benefits of Certification:

1. Enhanced Career Opportunities:
   - Certified professionals are in high demand due to the increasing frequency of cyber incidents.
   - Certification can open doors to specialized roles in forensics and incident response, making you a valuable asset to organizations facing cyber threats.
2. Recognition as an Expert:
   - The certification demonstrates that you possess the skills and knowledge needed to handle complex digital forensic investigations and lead incident response efforts.
   - It positions you as an expert in handling and mitigating cyber incidents, increasing your credibility in the field.
3. Competitive Edge in the Job Market:
   - Employers seek certified professionals who can immediately contribute to defending against cyberattacks and managing incidents.
   - This certification differentiates you from peers, highlighting your commitment to mastering digital forensics and incident response.
4. Higher Earning Potential:
   - Certified individuals typically earn higher salaries than their non-certified counterparts due to their specialized skills.
   - Employers recognize the value of certification and are willing to compensate accordingly for expertise in protecting critical assets and responding to cyber threats.
5. Broader Professional Network:

- Participating in this course and certification allows you to connect with other professionals in the field, opening opportunities for collaboration and career growth.
- It helps you stay updated with the latest trends, tools, and techniques in digital forensics and incident response.

6. Contribution to Organizational Security:
   - Certified professionals play a key role in safeguarding organizations from cyberattacks by improving detection, investigation, and remediation processes.
   - You will be able to identify, analyze, and mitigate security incidents, reducing the risk and impact of future cyber threats.

Day 1

Session 1 (Morning) - Introduction to Digital Forensics and Incident Response Objectives: This session will help participants to:

· Understand the basics of digital forensics and incident response.

· Identify the role of digital forensics in incident response.

· Recognize different types of digital evidence and their importance.

Topics:

1. Introduction to Digital Forensics

· Definition, Importance, and Overview

· Types of Digital Evidence (Files, Emails, Logs, etc.)

· Forensic Readiness and Its Importance

2. Introduction to Incident Response

· Incident Response Life Cycle (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned)

· The Role of Incident Response in Cybersecurity

· Key Components of an Effective Incident Response Plan

3. Legal and Ethical Considerations

· Legal Frameworks and Compliance (GDPR, HIPAA, etc.)

· Ethical Issues in Digital Forensics and Incident Response

· Chain of Custody and Maintaining Evidence Integrity

Exercise: Digital Evidence Identification and Handling (1hr and 30 mins)

· Participants will engage in an exercise to identify, preserve, and document digital evidence in a simulated scenario.

Session 2 (Afternoon) - Tools and Techniques for Digital Forensics Objectives: This session will help participants to:

· Familiarize with common digital forensic tools and their applications.

· Understand the techniques for acquiring and analyzing digital evidence.

· Recognize the importance of documentation and reporting in digital forensics.

Topics:

1. Digital Forensic Tools

· Overview of Popular Tools (FTK, EnCase, Magnet AXIOM, etc.)

· Selecting the Right Tool for the Task

· Open Source vs. Commercial Tools

2. Evidence Acquisition

· Imaging and Cloning of Digital Devices

· Memory Forensics and Volatile Data Collection

· Network Forensics and Traffic Analysis

3. Evidence Analysis

· File System Forensics

· Email and Browser Forensics

· Malware Analysis and Reverse Engineering

Interactive Workshop: Using Forensic Tools for Evidence Acquisition (1hr)

· Requirements: Participants will practice acquiring evidence from different digital devices using forensic tools and techniques.

INJECT - Table-Top Exercise: Simulating a Forensic Investigation (30 mins)

· A simulated forensic investigation will be presented, and participants will work through the process of acquiring, analyzing, and reporting on digital evidence.

Reflection:

- What were the challenges faced during the evidence acquisition process?
- What areas require further improvement or practice?
- How can these tools and techniques be applied in real-world investigations?

Day 2

Session 3 (Morning) - Advanced Forensic Analysis Techniques Objectives: This session will help participants to:

· Dive deeper into advanced forensic analysis techniques.

· Understand the forensic analysis of complex data types.

· Learn to correlate data from multiple sources to build a comprehensive case.

Topics:

1. Advanced File System Forensics

· NTFS, FAT32, and Ext File Systems

· Hidden and Alternate Data Streams (ADS)

· Recovering Deleted Files and Partitions

2. Network Forensics

· Capturing and Analyzing Network Traffic

· Identifying Indicators of Compromise (IoCs)

· Forensic Analysis of Network Devices (Routers, Firewalls)

3. Mobile Device Forensics

· Acquisition and Analysis of Mobile Devices (iOS, Android)

· Extracting Data from Apps, SMS, and Call Logs

· Analyzing GPS and Location Data

Exercise: Advanced Data Recovery and Analysis (1hr and 30 mins)

· Participants will perform advanced recovery techniques on corrupted or deleted data and analyze the recovered information.

Session 4 (Afternoon) - Incident Response in Action Objectives: This session will help participants to:

· Apply incident response methodologies in various scenarios.

· Coordinate incident response activities with different teams.

· Develop and implement effective containment and eradication strategies.

Topics:

1. Incident Detection and Triage

· Early Detection Techniques (SIEM, IDS/IPS)

· Prioritizing Incidents Based on Impact and Urgency

· Initial Response Steps and Quick Containment

2. Containment and Eradication

· Short-term vs. Long-term Containment Strategies

· Eradication of Threats and Remediation of Systems

· Ensuring a Clean and Secure Environment Post-Incident

3. Post-Incident Activities

· Lessons Learned and After-Action Reporting

· Implementing Improvements in Security Posture

· Communication with Stakeholders and Regulatory Bodies

Interactive Workshop: Simulated Incident Response Exercise (1hr)

· Requirements: Participants will work in teams to respond to a simulated cybersecurity incident, coordinating their actions and documenting the response process.

INJECT - Table-Top Exercise: Handling a Complex Cyber Incident (30 mins)

· Participants will be presented with a complex incident scenario and will need to plan and execute a response, focusing on coordination and communication.

Reflection:

1. What were the key challenges in managing the incident?

2. How effective were the containment and eradication strategies?

3. What lessons can be applied to improve future incident responses?

Day 3

Session 5 (Morning) - Reporting and Presenting Forensic Findings Objectives: This session will help participants to:

· Understand the importance of clear and concise reporting in digital forensics.

· Learn best practices for documenting and presenting forensic findings.

· Develop skills in communicating complex technical information to non-technical audiences.

Topics:

1. Forensic Report Writing

· Structure and Content of a Forensic Report

· Ensuring Accuracy and Completeness

· Presenting Findings in a Clear and Understandable Manner

2. Presenting Forensic Evidence

· Preparing for Legal Proceedings (Testimony, Depositions)

· Creating Visualizations and Demonstrations of Findings

· Communicating with Legal and Management Teams

3. Peer Review and Quality Assurance

· Importance of Peer Review in Forensic Analysis

· Quality Assurance Processes in Digital Forensics

· Continuous Improvement of Forensic Practices

Exercise: Forensic Report Writing and Presentation (1hr and 30 mins)

· Participants will create a forensic report based on a case study and present their findings to the group, simulating a courtroom or boardroom scenario.

Session 6 (Afternoon) - Certification Exam and Wrap-Up Objectives: This session will help participants to:

· Validate their knowledge and skills through a certification exam.

· Review key concepts and techniques covered during the training.

· Reflect on the training and plan for applying new skills in their roles.

Topics:

1. Certification Exam Preparation

· Review of Key Concepts

· Sample Questions and Exam Strategy

· Addressing Participant Questions and Concerns

2. Certification Exam

· A written exam to test participants on the material covered over the 3 days.

· Practical scenarios and case studies to assess hands-on skills.

3. Wrap-Up and Final Reflection

· Review of Training Objectives and Key Takeaways

· Group Discussion on Applying Skills in Real-World Scenarios

· Planning for Continuous Learning and Professional Development

Reflection:

1. How well did the training prepare you for real-world digital forensics and incident response?

2. What areas do you feel confident in, and where do you need further practice?

3. What are your next steps in developing your expertise in digital forensics and incident response?

Lesson to be Learned:

Over the course of 3 days, participants will have developed a strong foundation in digital forensics and incident response, with practical skills they can immediately apply in their roles. Continuous learning and adaptation to new challenges are key to staying effective in this field.