Cyber Security Institute

Incident Response and Network Forensics Training Boot Camp

Cyber Security Institute offers this hands-on Incident Response and Network Forensics course that covers the essential information you need to know in order to properly detect, contain and mitigate security incidents. Security incidents are a way of life in the modern world, and how organizations respond to them makes a massive difference in how much damage is ultimately done. In this five-day course, you learn the ins and outs of incident response, as well as the tools of the trade used by incident responders on a daily basis.

This course from Cyber Security Institute helps you fully understand how systems are compromised and what traces are left behind by attackers on the network, on disk and in volatile memory. The Incident Response and Network Forensics course addresses cutting edge attack vectors as well as tried and true methods for compromise. You leave the five-day course with the knowledge of how to prevent incidents and the skills to defend against a security incident if it does happen.

What You'll LEARN

- The Incident Response Process
- Event/Incident Detection
- Sources of Network Evidence
- TCP Reconstruction
- Flow Analysis
- NIDS/NIPS
- Log Analysis
- Firewall log Investigation
- Log Aggregation
- Network Artifact Discovery
- DNS Forensics and Artifacts
- NTP Forensics and Artifacts
- HTTP Forensics and Artifacts
- HTTPS and SSL Analysis
- FTP and SSH Forensics
- Email Protocol Artifacts
- Wireless Network Forensics

Course Objectives

The course focuses on the five key Incident Response tactics:

1. Plan – Preparing the right process, people and technology enables organizations to effectively respond to security incidents

2.Identify – Scoping the extent of the incident and determining which networks and systems have been compromised; includes assessing the extent to which systems have been compromised

3. Contain – Prevent the incident from further escalation using information gathered in Identify stage

4. Eradicate – Remove intruder access to internal and external company resources

5. Recover – Restore fully operational system capability and close out incident

Contact us:

What You'll DO

- Constructing your Live Incident Response Toolkit
- Perform Vulnerability Analysis
- The Incident Management Knowledgebase
- Timeline Analysis
- Triage & Analysis
- Volatile Data Sources and Collection
- Identify Rogue Processes
- Volatility Walkthrough
- Defensive review and recommendations
- Improving defenses
- Secure credential changing process and monitoring
- Increased monitoring period – when and how long
- Validate the system.
- Enable constituents to protect their assets and/or detect similar incidents.
- Report and coordinate incidents with appropriate external organizations
- CSIH Domains
- CSIH Practice Exam

What's Included?

- Five days of intense training with an expert instructor
- Pre-shipment of pre-study book
- Incident Response digital textbook (physical textbooks available to purchase)
- Incident Response toolkit
- Cyber Security Institute digital IR and Network Forensics lab guide
- CERT CSIH digital review guide
- Detailed reporting on exam readiness via your Flex Center (Flex Pro)
- CERT CSIH exam voucher
- 6 months access to virtual lab environment (Flex Pro)
- 100% Satisfaction Guarantee
- Exam Pass Guarantee (Flex Pro)
- Add-on: Video replays of daily lessons
- Add-on: Curated videos from other top-rated instructors