CBRFIR - CONDUCTING FORENSIC ANALYSIS AND INCIDENT RESPONSE USING CISCO TECHNOLOGIES FOR CYBEROPS V1.0

Course Code: 860001

The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) course helps build your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills. The course prepares you to identify and respond to cybersecurity threats, vulnerabilities, and incidents.

The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) course helps build your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills. The course prepares you to identify and respond to cybersecurity threats, vulnerabilities, and incidents.

Gain an understanding of digital forensics, including the collection and examination of digital evidence on electronic devices. Learn how to build the subsequent response to threats and attacks and how to proactively conduct audits to prevent future attacks.

This course will help you:

- Develop an understanding of various cybersecurity threat and vulnerabilities
- Establish a framework for proactively responding to cybersecurity threat and vulnerabilities
- Prepare for the 300-215 CBRFIR Professional Level exam.

What You'll Learn

After completing this course, you should be able to:

- Analyze the components needed for a root cause analysis report
- Apply tools such as YARA for malware identification
- Recognize the methods identified in the MITRE attack framework
- Leverage scripting to parse and search logs or multiple data sources such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid
- Recommend actions based on post-incident analysis

- Determine data to correlate based on incident type (host-based and network-based activities)
- Evaluate alerts from sources such as firewalls, intrusion prevention systems (IPS), data analysis tools (such as, Cisco Umbrella Investigate, Cisco Stealthwatch, and Cisco SecureX), and other systems to respond to cyber incidents and recommend mitigation
- Evaluate elements required in an incident response playbook and the relevant components from the ThreatGrid report
- Analyze threat intelligence provided in different formats (such as, STIX and TAXII)

Who Needs to Attend

This training is designed for the following roles:

- SOC analysts, Tiers 1–2
- Threat researchers
- Malware analysts
- Forensic analysts
- Computer Telephony Integration (CTI) analysts
- Incident response analysts
- Security operations center engineers
- Security engineers

Prerequisites

Attendees should meet the following pre-requisites:

- Familiarity with network and endpoint security concepts and monitoring
- Experience with network intrusion analysis
- An understanding of security policies and procedures
- Experience with risk management
- Experience with traffic and logs analysis
- Familiarity with APIs
- 2–3 years' experience working in a Security Operations Center (SOC) environment (experience Tier 1, or new Tier 2)

CBRFIR - CONDUCTING FORENSIC ANALYSIS AND INCIDENT RESPONSE USING CISCO TECHNOLOGIES FOR CYBEROPS V1.0

Course Code: 860001

ON-DEMAND	$800 USD

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 8/30/2025 8:08:17 PM