Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Course Duration: 40 Hours **Course code: CBRFIR**

1. Course Overview

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (CBRFIR 300-215) is a 90-minute exam that is associated with the Cisco CyberOps Professional Certification. This exam tests a candidate's knowledge of forensic analysis and incident response fundamentals, techniques, and processes. The course Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps helps candidates to prepare for this exam.

2. What you'll learn?

Upon completing this course, you will be able to:

- Understand the digital forensic process and incident response lifecycle
- Perform host-based and network-based forensic analysis
- Identify indicators of compromise (IOCs) and attack patterns
- Use Cisco Secure technologies for endpoint, network, and cloud visibility
- Conduct log analysis and threat hunting
- Automate and orchestrate incident response actions
- Preserve and handle evidence for post-incident investigations

3. Target Audience

This course is designed for:

- Security Operations Center (SOC) analysts
- Incident response team members
- Cybersecurity investigators and threat hunters

- Network security engineers
- Cisco CyberOps Associate and Professional level learners

4. Pre-Requisites

Participants should have a basic understanding of:

- Networking concepts (TCP/IP, DNS, HTTP/S)
- Security operations and monitoring
- Cyber threat types and attack vectors
- Security event correlation and analysis

Recommended Prerequisites:

- CBROPS – Understanding Cisco Cybersecurity Operations Fundamentals
- SCOR – Implementing and Operating Cisco Security Core Technologies

5. Course content

1. Introduction to Forensics and Incident Response

Overview of Cybersecurity Threat Landscape
Incident Response and Forensics Defined
NIST and SANS IR Frameworks
Chain of Custody and Legal Considerations
Cisco Tools in the Forensic Workflow

2. Digital Forensics Fundamentals

Types of Digital Evidence
Host-Based vs. Network-Based Forensics
File System Structures and Artifacts
Data Acquisition and Imaging
Evidence Preservation and Validation

Forensic Tools and Open-Source Utilities

3. Network Forensics and Packet Analysis

Capturing and Analyzing Network Traffic
TCP/IP Session Reconstruction
Identifying Suspicious Traffic Patterns
Protocol Analysis (DNS, HTTP, SSL/TLS)
Using Cisco Secure Network Analytics (Stealthwatch)
Lateral Movement and Data Exfiltration Detection

4. Host-Based Forensics

Analyzing Windows and Linux Systems
Registry, Prefetch, Event Logs, and Memory Analysis
Identifying Malware Persistence Techniques
Cisco Secure Endpoint (AMP) for Host Insights
Endpoint IOC Hunting and Threat Score Interpretation

5. Cisco Incident Response Tools and Platforms

Cisco SecureX and Threat Response Integration
Cisco Secure Endpoint: Retrospective Analysis
Cisco Umbrella and DNS-based Detection
Cisco Talos Intelligence Utilization
Automating IR Workflows Using SecureX Playbooks
Threat Grid for Malware Sandboxing

6. Indicators of Compromise (IOCs) and Threat Hunting

Types and Sources of IOCs
IOC Collection and Enrichment
STIX, TAXII, and Threat Intelligence Feeds
Proactive Hunting with Behavioral Analytics
Building Threat Hunting Hypotheses

Tactics, Techniques, and Procedures (TTPs) – MITRE ATT&CK Mapping

7. Performing Log Analysis

Types of Logs: Syslog, NetFlow, Event Logs, Web Proxy Logs
Correlation Using SIEM Tools
Identifying Attack Patterns in Logs
Anomalous Behavior Detection
Pivoting Techniques and Timeline Analysis

8. Case-Based Investigation Scenarios

Ransomware Attack Investigation
Insider Threat and Data Exfiltration Case
Supply Chain Attack Response
Business Email Compromise (BEC) Response
Incident War Room Simulation

9. Incident Response Lifecycle and Documentation

Detection and Triage
Containment, Eradication, and Recovery
Lessons Learned and Post-Incident Review
Creating and Presenting Forensic Reports
Evidence Handover and Legal Collaboration
Playbook Creation and Continuous Improvement