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

Description

The **Conducting Forensic Analysis and Incident Response Using Cisco Technologies for Cybersecurity (CBRFIR)** training builds your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills. This training prepares you to identify and respond to cybersecurity threats, vulnerabilities, and incidents. Additionally, you will be introduced to digital forensics, including the collection and examination of digital evidence on electronic devices and learn to build the subsequent response threats and attacks. You will also learn to proactively conduct audits to prevent future attacks.

This training prepares you for the 300-215 CBRFIR v1.2 exam. If passed, you earn the Cisco Certified Cybersecurity Specialist – Cybersecurity Forensic Analysis and Incident Response certification and satisfy the concentration requirement for the Cisco Certified Cybersecurity Professional certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How you'll benefit

This training 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 v1.2 exam
- Earn 40 CE credits toward recertification

Who should enroll

- 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

Technology areas

- Network Security
- Security Analysis

Objectives

- 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 responds 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)

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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 of experience working in a Security Operations Center (SOC) environment (experience Tier 1, or new Tier 2)

These skills can be found in the following Cisco Learning Offerings:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Outline

- Introduction to Incident Response

- Preparing for Incident Response
- Gathering and Examining Digital Intelligence
- Describing Detection, Analysis, and Investigation Forensics

What to expect on the exam

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for Cybersecurity (300-215 CBRFIR) v1.2 is a 90-minute exam associated with the Cisco Certified Cybersecurity Specialist – Cybersecurity Forensic Analysis and Incident Response certification and satisfies the concentration exam requirement for the Cisco Certified Cybersecurity Professional certification.

This exam tests your knowledge of forensic analysis and incident response components, including:

- Fundamentals
- Techniques
- Processes

Links

- Cisco U. Learning Path
- Cisco Learning Network Store