Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps

Cisco

- **Nível:** Avançado
- **Duração:** h

Sobre o curso

The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) v1.0 training is a 5-day training consisting of a series of lectures and videos that build your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills. The 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. Students will also learn to proactively conduct audits to prevent future attacks.

The **Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)** v1.0 training also prepares you to take the **300-215 CBRFIR** exam.

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

CERTIFICATION

- Associated Certification: CyberOps Professional
- Associated Exam: 300-215 CBRFIR

THIS COURSE INCLUDES

- Access duration: 180 days
- Labs
- Self-paced training
- Continuing Education Credits: 40

Destinatários

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

Objetivos

After taking this training, 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 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)

Pré-requisitos

Before taking this training, you should have:

- 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)

These recommended Cisco learning offerings may help students meet these prerequisites:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)
- Splunk Fundamentals 1

Programa

- Explore Adversarial Techniques, Tactics, and Common...
- Explore Available Incident-Related Information
- Examine Network Diagrams
- Examine Logs

- Examine Response Data Formats
- Discover Sources of Evidence in the Network
- Discover Sources of Evidence at Endpoints
- Discover Sources of Evidence in the Cloud
- Discover Syslog Facilities and Severity Levels
- Explore Gathered Intelligence
- Explore AccessData Forensic Toolkit (FTK) and Autopsy
- Explore Hex Encoding
- Explore Disassemblers and Debuggers
- Explore Deobfuscation Tools
- Explore Native Windows Tools Used in Digital Forensics and Incident Response
- Explore Native Linux Tools
- Explore Wireshark
- Create and Use a Yet Another Recursive Acronym (YARA) Rule
- Examine the Threat-Hunting Process
- Perform Data Acquisition
- Acquire Data from the Cloud
- Acquire Data Acquisition from Files, Disk, and Drive
- Analyze RAM and Fileless Malware Data
- Analyze Network Data
- Correlate Data from Different Sources
- Use Scripting for Forensics

- Analyze Web Application Logs
- Contain the Attack
- Remediate an Incident
- Analyze the Evidence and Propose the Solution