

CBRFIR (CONDUCTING FORENSIC ANALYSIS AND INCIDENT RESPONSE USING CISCO TECHNOLOGIES FOR CYBEROPS) 1.0

Objetivo

After taking 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)

Público Alvo

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

Pré-Requisitos

After taking this course, you should be able to:

- 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

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Introducing Incident Response and Forensic Analysis
Describing Digital Forensics and Incident Response (DFIR) Guidelines and Associations

Examining Threats and Vulnerability Frameworks
Describing the Analytical Mindset
Preparing for Incident Response and Responding to Threats
Identifying Sources of Evidence
Gathering Intelligence
Examining Digital Forensics and Incident Response Tools
Describing Detection and Analysis
Describing Investigation and Detection
Describing Digital Forensics
Describing Breach Containment and Eradication
Describing Post-Incident Activities

Demo Videos

Explore Adversarial Techniques, Tactics, and Common Knowledge (ATT&CK), Common Attack Pattern Enumeration and Classification (CAPEC), and National Institute of Standards and Technology (NIST) Common Weakness Enumeration Specification (CWE), and Common Vulnerabilities and Exposures (CVE) Frameworks
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