Cisco Certified CyberOps Professional

Introduction

This certification gives you knowledge and skills beyond simple firewalls and antivirus software and enables you to become a skilled CyberOps professional. This program is designed for mid-career professionals.

This certification programs will equip you with the skills and knowledge for the following job roles:

- Sr. Information Security Analyst
- Incident manager
- Security Architect
- Security analyst/Senior SOC analyst (Tier 2 and 3)

This certification is an investment that repays itself in improving your marketability and enhancing your ability to respond to more sophisticated cyberattacks and protect your organization's data.

Required exam

350-201 CBRCOR: Performing CyberOps Using Cisco Security Technologies

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0 course covers cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this course will prepare you for the role of Information Security Analyst on a Security Operations Center (SOC) team. You will learn foundational concepts and their application in real-world scenarios, and how to leverage playbooks in formulating an Incident Response (IR). The course shows you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

Duration

5 Days

Course Objectives

- Describe the types of service coverage within a SOC and operational responsibilities associated with each.
- Compare security operations considerations of cloud platforms.
- Describe the general methodologies of SOC platforms development, management, and automation.
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, and approaches to each, as part of asset controls and protections.
- Describe Zero Trust and associated approaches, as part of asset controls and protections.
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC.
- Use different types of core security technology platforms for security monitoring, investigation, and response.
- Describe the DevOps and SecDevOps processes.
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML,

Comma-Separated Values (CSV).
- Describe API authentication mechanisms.
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response.
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Interpret the sequence of events during an attack based on analysis of traffic patterns.
- Describe the different security tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyze anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

Prerequisites

Although there are no mandatory prerequisites, to fully benefit from this course, you should have the following knowledge:

- Good grasp of the content covered in the CyberOps Associate level course (CBROPS).
- Familiarity with UNIX/Linux shells (bash, csh) and shell commands.
- Conceptual understanding of the topics covered in the CCNA® course.
- Basic understanding of scripting using one or more of Python, JavaScript, PHP, or similar.

Target Audience

Although there are no mandatory prerequisites, the course is particularly suited for the following audiences:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC analysts currently functioning at entry-level with 2+ years of experience

Course Outline

- Understanding Risk Management and SOC Operations
- Understanding Analytical Processes and Playbooks
- Investigating Packet Captures, Logs, and Traffic Analysis
- Investigating Endpoint and Appliance Logs
- Understanding Cloud Service Model Security Responsibilities
- Understanding Enterprise Environment Assets
- Threat Tuning
- Threat Researching and Threat Intelligence Practices
- Understanding APIs
- Understanding SOC Development and Deployment Models
- Performing Security Analytics and Reports in a SOC
- Malware Forensics Basics
- Threat Hunting Basics

Concentration Exams

300-215 CBRFIR: Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps

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.

Course Outline

- **Fundamentals**
  - Analyze the components needed for a root cause analysis report
  - Describe the process of performing forensics analysis of infrastructure network devices
  - Describe antiforensic tactics, techniques, and procedures
  - Recognize encoding and obfuscation techniques (such as base 64 and hex encoding)
  - Describe the use and characteristics of YARA rules (basics) for malware identification, classification, and documentation
  - Describe the role of:
    - hex editors (HxD, Hiew, and Hexfiend) in DFIR investigations
    - disassemblers and debuggers (such as Ghidra, Radare, and Evans Debugger) to perform basic malware analysis
    - deobfuscation tools (such as XORBruteForces, or tool, and unpacker)
  - Describe the issues related to gathering evidence from virtualized environments (major cloud vendors)

- **Forensics Techniques**
  - Recognize the methods identified in the MITRE attack framework to perform fileless malware analysis
  - Determine the files needed and their location on the host
  - Evaluate output(s) to identify IOC on a host
    - process analysis
    - log analysis
  - Determine the type of code based on a provided snippet
  - Construct Python, PowerShell, and Bash scripts to parse and search logs or multiple data sources (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid)
  - Recognize the purpose, use, and functionality of libraries and tools (such as Volatility, Systernals, SIFT tools, and TCPdump)

- **Incident Response Techniques**
  - Interpret alert logs (such as, IDS/IPS and Syslog)
  - Determine data to correlate based on incident type (host-based and network-based activities)
  - Determine attack vectors or attack surface and recommend mitigation in a given scenario
  - Recommend actions based on post-incident analysis
  - Recommend mitigation techniques for evaluated alerts from 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
  - Recommend a response to 0-day exploitations (vulnerability management)
  - Recommend a response based on intelligence artifacts
  - Recommend the Cisco security solution for detection and prevention, given a scenario
  - Interpret threat intelligence data to determine IOC and IOA (internal and external sources)
  - Evaluate artifacts from threat intelligence to determine the threat actor profile
  - Describe capabilities of Cisco security solutions related to threat intelligence (such as Cisco

Umbrella, Sourcefire IPS, AMP for Endpoints, and AMP for Network)

- **Forensics Processes**
  - Describe anti-forensic techniques (such as, debugging, Geolocation, and obfuscation)
  - Analyze logs from modern web applications and servers (Apache and NGINX)
  - Analyze network traffic associated with malicious activities using network monitoring tools (such as NetFlow and display filtering in Wireshark)
  - Recommend next step(s) in the process of evaluating files based on distinguishing characteristics of files in a given scenario
  - Interpret binaries using objdump and other CLI tools (such as Linux, Python, and Bash)

- **Incident Response Processes**
  - Describe the goals of incident response
  - Evaluate elements required in an incident response playbook
  - Evaluate the relevant components from the ThreatGrid report
  - Recommend next step(s) in the process of evaluating files from endpoints and performing ad-hoc scans in a given scenario
  - Analyze threat intelligence provided in different formats (such as STIX and TAXII)