Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0

What you'll learn in this course

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.

The official release date for this course is April 2021, but the first three sections are available now and we will release more sections over the coming months. If you purchase the course before its official release, you'll receive:

- A discounted purchase price of $700 (full list price is $1,000)
- Sections as they become available
- Access to the content for one year from the date of purchase.
- If you purchase the complete course after the release date, you'll have access to the content for 6 months from the date of purchase.

Course duration

- E-learning: 5 days with hands-on practice, plus equivalent of 3 days of content with practice, and challenges

How you'll benefit

This course will help you:

- Gain an advanced understanding of the tasks involved for senior-level roles in a security operations center
- Configure common tools and platforms used by security operation teams via practical application
- Prepare you to respond like a hacker in real-life attack scenarios and submit recommendations to senior management
- Prepare for the **350-201 CBRCOR** core exam

What to expect in the exam

350-201 Performing CyberOps Using Cisco Security Technologies (CBRCOR) is a 120-minute exam associated with the Cisco CyberOps Professional Certification. The multiple-choice format tests knowledge of core cybersecurity operations including cybersecurity fundamentals, techniques, policies, processes, and automation. The exam will test for knowledge in the following areas:

- Monitoring for cyberattacks
- Analyzing high volume of data using automation tools and platforms—both open source and commercial

- Accurately identifying the nature of attack and formulate a mitigation plan
- Scenario-based questions; for example, using a screenshot of output from a tool, you may be asked to interpret portions of output and establish conclusions

Who should enroll

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

How to enroll

E-learning

- To buy a single e-learning license, visit the Cisco Learning Network Store.
- For more than one license, or a learning library subscription, contact us at learning-bdm@cisco.com.

Technology areas

- Cybersecurity

Course details

Objectives

After taking this course, you should be able to:

- 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.

Recommended Cisco offering that may help you prepare for this course:

- **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.