Performing CyberOps Using Cisco Security Technologies (CBRCOR) E-Learning

Cisco

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

Sobre o curso

The **Performing CyberOps Using Cisco Security Technologies (CBRCOR)** v1.0 course guides you through 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 teaches 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.

This course also earns you 40 Continuing Education (CE) credits towards recertification and prepares you for the **350-201 CBRCOR** core exam.

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

Certification

- Associated Certification: Cisco Certified CyberOps Professional
- Associated Exam: 350-201 CBRCOR

This course includes

- Access duration: 180 days
- Labs
- Self-paced training

This course is also available in an Instructor-Led Training (ILT) format. For more information, select this link: Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Destinatários

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

- Cybersecurity engineers and investigators
- Incident managers
- Incident responders
- Network engineers
- SOC analysts currently functioning at entry level with 2+ years of experience

Objetivos

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.

Pré-requisitos

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)