CBRCOR

Performing CyberOps Using Cisco Security Technologies

40 horas | Security & Cybersecurity | Cisco

Cisco Continuing Education Credits

40 CE Credits

INTRODUÇÃO

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 select 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:

OBJETIVO DO CURSO

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.

PÚBLICO-ALVO

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

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)

CONTEÚDO PROGRAMÁTICO

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