Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Description

A key training to master CyberOps security

The “Performing CyberOps Using Cisco Security Technologies (CBRCOR)” course offers you a unique opportunity to deepen your cybersecurity knowledge. Through this course, you will learn to manage and automate security operations in a SOC environment. This training prepares you for the CBRCOR exam and gives you access to Cisco’s latest security technologies. With practical scenarios, you will be trained to become a true expert in incident response and cyber threat management.

Expertise tailored to your cybersecurity career

With this training, you will develop the skills necessary to analyze complex threats and propose solutions adapted to modern enterprise environments. By focusing on tools like Cisco Firepower and Cisco SecureX, this course allows you to better understand and respond to cyberattacks. A comprehensive program that will help you excel as a SOC analyst. Don’t wait, take the step toward a promising future in cybersecurity.

Niveau
Intermédiaire
Course Content
Module 1: Risk management and SOC operations

- Understand analytical processes and playbooks
- Analyze packet captures and traffic analysis
- Evaluate security risks and threats in a SOC

Module 2: Log analysis of terminals and appliances

- Understand cloud security responsibilities
- Analyze terminal and appliance logs
- Monitor assets in the enterprise environment

Module 3: Threat Tuning and threat intelligence

- Implement Threat Tuning in a SOC environment
- Advanced threat research and intelligence practices
- Understand and use APIs for cybersecurity

Module 4: SOC security and analytical reporting

- Analyze network security and produce reports
- Basic malware forensics
- Perform proactive threat hunting

Module 5: Incident investigation and response

- Investigate incidents using SIEM and SOAR tools
- Respond to incidents following SOC best practices
- Determine Indicators of Compromise (IOC) and Indicators of Attack (IOA)

Lab / Exercises

- Explore Cisco SecureX orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower packet captures and PCAP analysis
- Validate an attack and determine the incident response
- Submit a malicious file to Cisco Threat Grid for analysis
- Explore Cisco Firepower NGFW access control policies and Snort rules
- Follow successful attack TTPs using a TIP
- Query Cisco Umbrella using the Postman API client
- Correct an API Python script
- Create basic Bash scripts
- Reverse engineering of malware

Documentation

- Digital course materials included

Exam

- This course prepares you to the 350-201 CBRCOR Cisco Security Technologies exam. If you wish to take this exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- Basic knowledge of UNIX/Linux environments
- Familiarity with Splunk and its search functions
- Knowledge of scripting languages such as Python or JavaScript
- Understanding of cybersecurity concepts
- Experience analyzing logs and network logs

Prerequisites

- Configure SOC tools and platforms
- Use playbooks for incident response
- Analyze threats with Cisco Firepower

- Understand SecDevOps deployment models
- Apply automation with Cisco SecureX
- Interpret and analyze network logs

Objectives

- Configure SOC tools and platforms
- Use playbooks for incident response
- Analyze threats with Cisco Firepower
- Understand SecDevOps deployment models
- Apply automation with Cisco SecureX
- Interpret and analyze network logs

Description
Performing CyberOps Using Cisco Security Technologies (CBRCOR) training
Classroom Registration Price (CHF)
4350
Virtual Classroom Registration Price (CHF)
4350
Duration (in Days)
5
Reference
CBRCOR