Performing Cybersecurity Using Cisco Security Technologies (CPLL-CBRCOR)

Duration: 180 Days

The Performing Cybersecurity Using Cisco Security Technologies (CBRCOR) training guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this training 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 training 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 training prepares you for the 350-201 CBRCOR v1.2 exam. If passed, you earn the Cisco Certified Specialist – Cybersecurity Core certification and satisfy the core exam requirement for the Cisco Certified Cybersecurity Professional certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

Skills You'll Learn:

- Detect, investigate, and respond to cyber threats using SIEM, SOAR, and industry-standard security tools
- Apply automation and scripting (Python, Bash) to improve security operations
- Perform threat hunting and leverage threat intelligence to identify and mitigate risks
- Analyze network traffic, logs, and endpoints to uncover indicators of compromise and attack
- Implement modern security frameworks such as Zero Trust, asset segmentation, and SecDevOps practices

Learning Path Objectives:

1. SOC Operations and Processes: Dive into an introduction to SOC operations and processes for the security analyst.
2. Threat Investigations: Explore threat investigations and security analytics practices.
3. Threat Hunting and Incident Response: Discuss threat hunting basics and performing incident investigation.