CertKit: Cisco 200-201: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) CertKit teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. You will learn the essential skills, concepts, and technologies to be a contributing member of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities. This course helps you prepare for the Cisco Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC.

Prerequisites:
To fully benefit from this course, you should have the following knowledge and skills:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

Course outcome:

- Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure the effectiveness of the SOC.

Who should attend:
This course is designed for individuals seeking a role as an associate-level cybersecurity analyst and IT professionals desiring knowledge in Cybersecurity operations or those in pursuit of the Cisco Certified CyberOps Associate certification including:

- Students pursuing a technical degree
- Current IT professionals
- Recent college graduates with a technical degree

CertKit content:

- E-learning courses:
  - CBROPS: The CIA Triad & Security Approaches
  - CBROPS: Threat Actors, Security, & Risk Management
  - CBROPS: CVSS, Deployments, Access Control, & Data Visibility
  - CBROPS: Data Loss, Host Isolation, & Detection Methods
  - CBROPS: Attack Surfaces, Vulnerability, & Analysis Tools
  - CBROPS: Firewall, Filtering, Visibility, & Control Data
  - CBROPS: Data & Attack Types
  - CBROPS: Social Engineering, Evasion, Obfuscation, & Certificates
  - CBROPS: Host-based Analysis & the Role of Attribution
  - CBROPS: Log Evidence, Disk Images, & Malware Analysis Output
  - CBROPS: File Extraction, Event Artifacts, & Regular Expressions
  - CBROPS: Incident Response, Security Management, & Analysis
  - CBROPS: Protected Data, Profiling, Forensics, & IRP
- MeasureUp Exam simulation
  - 220+ questions
- Tips & Tricks