Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CBROPS - Cisco Certified Cybersecurity Associate

Cisco recently renamed its CyberOps certification track to Cisco Cybersecurity certifications. The CyberOps exam numbers and acronyms remain the same, but the exam names and version numbers have changed. CyberOps Associate 200-201 CBROPS v1.1 is now Cybersecurity Associate 200-201 CBROPS v1.2

Course Description & Overview

SecureNinja’s Cisco Certified Cybersecurity Associate (CBROPS) v1.2 certification training provides the essential skills and knowledge required to monitor, detect, and respond to cybersecurity incidents in Security Operations Center (SOC) environments. This associate-level course is designed for those beginning their career in cybersecurity and covers the core principles and practical tools used in enterprise security operations.

Aligned with Cisco's updated 200-201 CBROPS exam objectives, this training is built around five critical domains: Security Concepts, Security Monitoring, Host-Based Analysis, Network Intrusion Analysis, and Security Policies and Procedures. Learners will gain practical experience analyzing logs, investigating threats, and applying security policies, while using tools such as SIEM, Wireshark, endpoint monitoring platforms, and intrusion detection systems.

Why Choose Cisco Certified Cybersecurity Associate (CBROPS)

- SOC-Ready Skills: Designed for Security Operations Center roles, including incident response and threat monitoring.
- Vendor-Recognized Certification: Globally respected Cisco credential aligned with modern cybersecurity demands.
- Real-World Application: Training incorporates real tools and scenarios used in blue team environments.
- AI and Threat Intelligence Updates: Reflects current cybersecurity operations, including SOAR, threat modeling, and AI-powered analysis.

Topics Covered

- Security Concepts: CIA triad, threat modeling, DevSecOps, access control models, and CVSS scoring.
- Security Monitoring: SIEM usage, log interpretation, event correlation, and anomaly detection.
- Host-Based Analysis: Windows and Linux log analysis, malware behavior, and file system artifacts.
- Network Intrusion Analysis: Network packet capture, flow analysis, and detection of attacks like DDoS, SQL injection, and phishing.
- Security Policies and Procedures: Risk assessment, compliance, response plans, and chain of custody principles.

Who is it for

- SOC Analysts: Entry-level professionals monitoring and triaging security alerts.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Cybersecurity Analysts: Individuals investigating and responding to cyber threats.
- IT Support Technicians: Transitioning into security operations roles.
- Network Support Professionals: Expanding into incident response and threat analysis.

Who Would Benefit

- Career Starters in Cybersecurity: Individuals beginning their journey in SOC, blue team, or cybersecurity analysis roles.
- Help Desk Technicians: Gaining exposure to real-time security operations.
- Technical Project Leads: Overseeing security monitoring or compliance teams.

Prerequisites

No formal prerequisites are required. A basic understanding of computer networks, operating systems, and general cybersecurity concepts is recommended.

Course Outline

1. Security Concepts

- CIA triad, threat intelligence, malware analysis, DevSecOps, risk and access control models.
- Understanding CVSS metrics and defense-in-depth strategies.

2. Security Monitoring

- Log sources and types, SIEM/SOAR platforms, and interpreting alerts.
- Application and network log analysis for anomalies.

3. Host-Based Analysis

- Understanding Windows/Linux logs, file system monitoring, malware behavior, and host-based indicators.

4. Network Intrusion Analysis

- PCAP interpretation, protocol analysis, and attack signature detection.
- Analyzing DNS, HTTP, TCP/IP for suspicious behavior.

5. Security Policies and Procedures

- Cybersecurity frameworks (e.g., NIST), response workflows, forensic procedures, and privacy principles.
- Documentation, chain of custody, and data handling guidelines.

Course Length

- 5 Days
- 40 Hours

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Exam Details

- Exam Code: 200-201 CBROPS v1.2
- Number of Questions: 95–105
- Duration: 120 minutes
- Question Types: Multiple-choice
- Passing Score: 820 (out of 1000)

The Cisco Certified Cybersecurity Associate (CBROPS) certification is an ideal entry point into cybersecurity operations. This training equips learners with the foundational skills necessary to detect, analyze, and respond to security threats, and sets the stage for advancement into roles in SOCs, threat intelligence, or incident response teams.