Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Category: Networking & Security | **Vendor:** Cisco

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Cisco Certified Cybersecurity Associate, Cisco Certified CyberOps Associate
Related Exam:	200-201

Course Overview

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this training, you will have the basic knowledge that is required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center (SOC).

This training prepares you for the 200-201 CBROPS v1.2 exam. If passed, you earn the Cisco Certified Cybersecurity Associate certification and the role of a junior or entry-level cybersecurity operations analyst in a SOC.

How You'll Benefit

This training will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 CBROPS v1.2 exam
- Earn 30 CE credits toward recertification

What to Expect in the Exam

The 200-201 CBROPS exam is a 120-minute assessment for the Cisco Certified CyberOps Associate certification and is aligned with the associate-level cybersecurity operations analyst job role. The CBROPS exam tests a candidate’s knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

About This Course

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this training, you will have the basic knowledge that is required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center (SOC).

This training prepares you for the 200-201 CBROPS v1.2 exam. If passed, you earn the Cisco Certified Cybersecurity Associate certification and the role of a junior or entry-level cybersecurity operations analyst in a SOC.

How You'll Benefit

This training will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 CBROPS v1.2 exam
- Earn 30 CE credits toward recertification

What to Expect in the Exam

The 200-201 CBROPS exam is a 120-minute assessment for the Cisco Certified CyberOps Associate certification and is aligned with the associate-level cybersecurity operations analyst job role. The CBROPS exam tests a candidate’s knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

Who Should Attend

This training 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

Prerequisites & Entry Requirements

General Prerequisites:

Before taking this training, 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

The following Cisco course can help you gain the knowledge you need to prepare for this course:

Implementing and Administering Cisco Solutions (CCNA)

Learning Outcomes

Upon successful completion of this course, participants will be able to:

After taking this training, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective
- Explain the use of SOC metrics to measure the effectiveness of the SOC
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC
- Describe the Windows operating system features and functionality
- Provide an overview of the Linux operating system
- Understand common endpoint security technologies
- Explain the network security monitoring (NSM) tools that are available to the network security analyst
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts
- Explain the data that is available to the network security analyst
- Describe the basic concepts and uses of cryptography
- Understand the foundational cloud security practices, including deployment and service models, shared responsibilities, compliance frameworks, and identity and access management, to effectively secure cloud environments against cyberthreats
- Understand and implement advanced network security, data protection, secure application deployment, continuous monitoring, and effective disaster recovery strategies to secure cloud deployments
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors
- Identify the common attack vectors
- Identify malicious activities
- Identify patterns of suspicious behaviors
- Identify resources for hunting cyber threats
- Explain the need for event data normalization and event correlation
- Conduct security incident investigations
- Explain the use of a typical playbook in the SOC

- Describe a typical incident response plan and the functions of a typical computer security incident response team (CSIRT)

Detailed Course Outline

- Defining the Security Operations Center
- Understanding SOC Metrics
- Understanding SOC Workflow and Automation
- Understanding Windows Operating System Basics
- Understanding Linux Operating System Basics
- Understanding Endpoint Security Technologies
- Understanding Network Infrastructure and Network Security Monitoring Tools
- Understanding Common TCP/IP Attacks
- Exploring Data Type Categories
- Understanding Basic Cryptography Concepts
- Cloud Security Fundamentals
- Securing Cloud Deployments
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Conducting Security Incident Investigations
- Using a Playbook Model to Organize Security Monitoring
- Describing Incident Respons

e

□□ Certification Path

Cisco Certified Cybersecurity Associate, Cisco Certified CyberOps Associate

Exam: 200-201

Skills You Will Learn:

After taking this training, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective
- Explain the use of SOC metrics to measure the effectiveness of the SOC
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC
- Describe the Windows operating system features and functionality
- Provide an overview of the Linux operating system
- Understand common endpoint security technologies
- Explain the network security monitoring (NSM) tools that are available to the network security analyst
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts
- Explain the data that is available to the network security analyst
- Describe the basic concepts and uses of cryptography
- Understand the foundational cloud security practices, including deployment and service models, shared responsibilities, compliance frameworks, and identity and access management, to effectively secure cloud environments against cyberthreats
- Understand and implement advanced network security, data protection, secure application deployment, continuous monitoring, and effective disaster recovery strategies to secure cloud deployments
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors
- Identify the common attack vectors
- Identify malicious activities
- Identify patterns of suspicious behaviors
- Identify resources for hunting cyber threats
- Explain the need for event data normalization and event correlation
- Conduct security incident investigations
- Explain the use of a typical playbook in the SOC
- Describe a typical incident response plan and the functions of a typical computer security incident response team (CSIRT)

Frequently Asked Questions

Q: What delivery options are available for Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course helps prepare you for the Cisco Certified Cybersecurity Associate, Cisco Certified CyberOps Associate certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 200-201 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)?

Yes, we provide corporate training, dedicated training, and closed classes for Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Understanding Cisco Cybersecurity Operations Fundamentals, Cisco Associate Level Cybersecurity - CCNA Cybersecurity, CBROPS

Q: Why choose Nexus Human for Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)