Performing CyberOps Using Cisco Security Technologies (CBRCOR)

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 Specialist – Cybersecurity Core, Cisco Certified Cybersecurity Professional
Related Exam:	350-201

Course Overview

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 ProfessionalCCNP CYBERSECURITY

How You'll Benefit

This training will help you:

- Develop essential cybersecurity skills in SOC operations, threat detection, and incident response through real-world labs and scenarios
- Gain hands-on experience with leading security tools such as Cisco XDR, Splunk Phantom, and Firepower NGFW
- Learn automation and SecDevOps practices to improve efficiency and effectiveness in security operations
- Prepare for the 350-201 CBRCOR v1.2 exam
- Earn 40 CE credits toward recertification

What to Expect in the Exam

Performing Cybersecurity Using Cisco Security Technologies (350-201 CBRCOR) v1.2 is a 120-minute exam associated with the Cisco Certified Specialist – Cybersecurity Core certification and satisfies the core exam requirement for the Cisco Certified Cybersecurity Professional certification.

This exam tests your knowledge of core cybersecurity operations, including:

- Cybersecurity fundamentals
- Techniques
- Processes
- Automation

About This Course

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 ProfessionalCCNP CYBERSECURITY

How You'll Benefit

This training will help you:

- Develop essential cybersecurity skills in SOC operations, threat detection, and incident response through real-world labs and scenarios
- Gain hands-on experience with leading security tools such as Cisco XDR, Splunk Phantom, and Firepower NGFW
- Learn automation and SecDevOps practices to improve efficiency and effectiveness in security operations
- Prepare for the 350-201 CBRCOR v1.2 exam
- Earn 40 CE credits toward recertification

What to Expect in the Exam

Performing Cybersecurity Using Cisco Security Technologies (350-201 CBRCOR) v1.2 is a 120-minute exam associated with the Cisco Certified Specialist – Cybersecurity Core certification and satisfies the core exam requirement for the Cisco Certified Cybersecurity Professional certification.

This exam tests your knowledge of core cybersecurity operations, including:

- Cybersecurity fundamentals
- Techniques
- Processes
- Automation

Who Should Attend

Although there are no mandatory prerequisites, the course is particularly suited for the following audiences:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC analysts currently functioning at entry level with a minimum of 1 year of experience

Prerequisites & Entry Requirements

General Prerequisites:

Although there are no mandatory prerequisites, to fully benefit from this course, you should have the following knowledge:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands
- Familiarity with the Splunk search and navigation functions
- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar.

Recommended Cisco offering that may help you prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA)
- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Learning Outcomes

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

- Describe the types of service coverage within a SOC and operational responsibilities associated with each
- Compare security operations considerations of cloud platforms
- Describe the general methodologies of SOC platforms development, management, and automation
- Describe asset segmentation, segregation, network segmentation, microsegmentation, and approaches to each, as part of asset controls and protections
- Describe Zero Trust and associated approaches, as part of asset controls and protections
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC
- Use different types of core security technology platforms for security monitoring, investigation, and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats (e.g., JavaScript Object Notation (JSON), HTML, XML, and Comma-Separated Values (CSV))
- Describe API authentication mechanisms
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
- Interpret the sequence of events during an attack based on analysis of traffic patterns
- Describe the different security tools and their limitations for network analysis (e.g., packet capture tools, traffic analysis tools, and network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

Detailed Course Outline

- Understanding Risk Management and SOC Operations
- Understanding Analytical Processes and Playbooks
- Understanding Cloud Service Model Security Responsibilities
- Understanding Enterprise Environment Assets

- Understanding APIs
- Understanding SOC Development and Deployment Models
- Investigating Packet Captures, Logs, and Traffic Analysis
- Investigating Endpoint and Appliance Logs
- Implementing Threat Tuning
- Threat Research and Threat Intelligence Practices
- Performing Security Analytics and Reports in a SOC
- Malware Forensics Basics
- Threat Hunting Basics
- Performing Incident Investigation and Response

□□ Certification Path

Cisco Certified Specialist – Cybersecurity Core, Cisco Certified Cybersecurity Professional

Exam: 350-201

Skills You Will Learn:

- Describe the types of service coverage within a SOC and operational responsibilities associated with each
- Compare security operations considerations of cloud platforms
- Describe the general methodologies of SOC platforms development, management, and automation
- Describe asset segmentation, segregation, network segmentation, microsegmentation, and approaches to each, as part of asset controls and protections
- Describe Zero Trust and associated approaches, as part of asset controls and protections
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC
- Use different types of core security technology platforms for security monitoring, investigation, and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats (e.g., JavaScript Object Notation (JSON), HTML, XML, and Comma-Separated Values (CSV))
- Describe API authentication mechanisms
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
- Interpret the sequence of events during an attack based on analysis of traffic patterns
- Describe the different security tools and their limitations for network analysis (e.g., packet capture tools, traffic analysis tools, and network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

Frequently Asked Questions

Q: What delivery options are available for Performing CyberOps Using Cisco Security Technologies (CBRCOR)?

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 Performing CyberOps Using Cisco Security Technologies (CBRCOR) course helps prepare you for the Cisco Certified Specialist – Cybersecurity Core, Cisco Certified Cybersecurity Professional certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 350-201 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 Performing CyberOps Using Cisco Security Technologies (CBRCOR) 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 Performing CyberOps Using Cisco Security Technologies (CBRCOR) 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 Performing CyberOps Using Cisco Security Technologies (CBRCOR)?

Yes, we provide corporate training, dedicated training, and closed classes for Performing CyberOps Using Cisco Security Technologies (CBRCOR). 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: Performing CyberOps Using Cisco Security Technologies, Cisco Professional Level Cybersecurity - CCNP Cybersecurity, CBRCOR

Q: Why choose Nexus Human for Performing CyberOps Using Cisco Security Technologies (CBRCOR)?

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 Performing CyberOps Using Cisco Security Technologies (CBRCOR) 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)