Manuals+ — User Manuals Simplified.

LUMIFY WORK 350-201 CBRCOR Performing CyberOps
Using Cisco Security Technologies

LUMIFY WORK 350-201 CBRCOR Performing CyberOps Using Cisco Security Technologies User Guide

LUMIFY WORK 350-201 CBRCOR Performing Cyber Ops Using Cisco Security Technologies

LUMIFY WORK 350-201 CBRCOR Performing CyberOps
Using Cisco Security Technologies

Contents

WHY STUDY THIS COURSE

The Performing Cyber Ops Using Cisco Security Technologies (CBRCOR) course guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this course 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 course teaches you how to use automation for security using cloud platforms and a Sec Dev Ops methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

This course will help you:

- Gain an advanced understanding of the tasks involved for senior-level roles in a security operations center
- Configure common tools and platforms used by security operation teams via practical application
- Prepare you to respond like a hacker in real-life attack scenarios and submit recommendations to senior management
- Prepare for the 350-201 CBRCOR core exam
- Earn 30 CE credits toward recertification

Digital courseware: Cisco provides students with electronic courseware for this course. Students who have a confirmed booking will be sent an email prior to the course start date, with a link to create an account via **learningspace.cisco.com** before they attend their first day of class. Please note that any electronic courseware or labs will not be available (visible) until the first day of the class.

CISCO AT LUMIFY WORK

Lumify Work is the largest provider of authorised Cisco training in Australia, offering a wider range of Cisco courses, run more often than any of our competitors. Lumify Work has won awards such as ANZ Learning Partner of the Year (twice!) and APJC Top Quality Learning Partner of the Year.

WHAT YOU'LL LEARN

- After taking this course, you should 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.
- Explain 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.
- Explain the common data formats, for example, JavaScript Object
- Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Describe API authentication mechanisms.
- Analyses 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 (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyses anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

" My instructor was great being able to put scenarios into real world instances that related to my specific situation.

I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.

I learnt a lot and felt it was important that my goals by attending this course were met.

Great job Lumify Work team.

AMANDA NICOL

IT SUPPORT SERVICES MANAGER – HEALTH WORLD LIMIT ED

Lumify Work Customized Training

- We can also deliver and customize this training course for larger groups saving your organisation time, money and resources.
- For more information, please contact us on 1 800 853 276.
- COURSE SUBJECTS
- Lab outline
- Understanding Risk Management and SOC Operations
- Understanding Analytical Processes and Playbooks
- Investigating Packet Captures, Logs, and Traffic Analysis
- Investigating Endpoint and Appliance Logs
- Understanding Cloud Service Model Security Responsibilities
- Understanding Enterprise Environment Assets
- Implementing Threat Tuning
- Threat Research and Threat Intelligence Practices
- Understanding APIs
- Understanding SOC Development and Deployment Models

- Performing Security Analytics and Reports in a SOC
- Malware Forensics Basics
- Threat Hunting Basics
- Performing Incident Investigation and Response
- Explore Cisco SecureX Orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Malicious File to Cisco Threat Grid for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Evaluate Assets in a Typical Enterprise Environment
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs from Cisco Talos Blog Using Cisco Secure X
- Explore the Threat Connect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Query Cisco Umbrella Using Postman API Client
- Fix a Python API Script
- Create Bash Basic Scripts
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response

WHO IS THE COURSE FOR?

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

We can also deliver and customize this training course for larger groups – saving your organisation time, money and resources. For more information, please contact us on 1800 U LEARN (1800 853 276)

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 offerings that may help you prepare for this course:

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

Recommended third-party resources:

- Splunk Fundamentals 1
- Blue Team Handbook: Incident Response Edition by Don Murdoch
- Threat Modeling – Designing for Security by Adam Shostack
- Red Team Field Manual by Ben Clark
- Blue Team Field Manual by Alan J White
- Purple Team Field Manual by Tim Bryant
- Applied Network Security and Monitoring by Chris Sanders and Jason Smith

The supply of this course by Lumify Work is governed by the booking terms and conditions . Pleas e read the terms and
conditions carefully before enrolling in this course, as enrolment in the course is conditional on acceptance of these terms and conditions .

https://www.lumifywork.com/en-au/courses/performing-cyberops-using-cisco-security-technologies-cbrcor/

- **LENGTH**
  5 days
- **PRICE (Incl. GST)**
  $6590
- **VERSION**
  1.0

Call 1800 853 276 and speak to a Lumify Work Consultant today!

✉ **training@lumifywork.com**

🌐 **https://www.lumifywork.com/**

f **https://www.facebook.com/LumifyWorkAU/**

in **https://www.linkedin.com/company/lumify-work/**

t **https://twitter.com/DDLSTraining**

▶ **https://www.youtube.com/@lumifywork**

Documents / Resources

LUMIFY WORK 350-201 CBRCOR Performing CyberOps Using Cisco Security Technologies [pdf] User Guide
350-201 CBRCOR, 350-201 CBRCOR Performing CyberOps Using Cisco Security Technologies, Performing CyberOps Using Cisco Security Technologies, CyberOps Using Cisco Security Technologies, Using Cisco Security Technologies, Security Technologies, Technologies

References

- **Lumify Work | Lumify Work AU**
- **Cisco Learning Network Space**
- **Lumify Work | Lumify Work AU**
- **Implementing and Administering Cisco Solutions (CCNA) | Lumify Work AU**
- **Performing CyberOps Using Cisco Security Technologies (CBRCOR) | Lumify Work AU**
- **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) | Lumify Work AU**
- **User Manual**