# Performing CyberOps Using Cisco Security Technologies

**Varighed: 5 Days** **Kursus Kode: CBRCOR** **Version: 1.1** **Leveringsmetode: Virtuel deltagelse**

## Beskrivelse:

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 Professional certification.
**This training also earns you 40 Continuing Education (CE) credits toward recertification.**

*Updated November 2026*

## Målgruppe:

This class is intended for the following participants:
- Cybersecurity Engineers
- Cybersecurity Investigators
- Incident Managers
- Incident Responders
- Network Engineers
- SOC Analysts currently functioning at entry level with a minimum of 1 year of experience

## Agenda:

- After this course participants 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
- 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

## Forudsætninger:

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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

These skills can be found in the following Cisco Learning Offerings:

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

## Test og certificering

**Recommended as preparation for the following exam:**

- **350-201 CBRCOR** - Performing CyberOps Using Cisco Security Technologies Exam

## Indhold:

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

Lab Outline

- Explore Cisco XDR
- Explore Splunk Phantom Playbooks
- Evaluate Assets in a Typical Enterprise Environment
- Fix a Python API Script
- Create Bash Basic Scripts
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Sample to Cisco Secure Malware Analytics for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK®
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs using Cisco XDR
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response

## Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre