CBRCOR - PERFORMING CYBERSECURITY USING CISCO SECURITY TECHNOLOGIES V1.1

Course Code: 821350

The Performing Cybersecurity Using Cisco Security Technologies v1.1 (CBRCOR) course 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 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.

What You'll Learn

Upon successful completion of 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
- 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

Who Needs to Attend

- 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

Prerequisites

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:

CBRCOR - PERFORMING CYBERSECURITY USING CISCO SECURITY TECHNOLOGIES V1.1

Course Code: 821350

CLASSROOM LIVE	$3,995 USD	5 Day

Classroom Live Outline

Section 1: Understanding Risk Management and SOC Operations

- Governance, Risk, and Compliance
- Security Regulatory Requirements
- Security Policy
- Protected Information
- Risk Analysis and Insurance
- SOC Services, Operations, and Automation
- SOC Service Models

Section 2: Understanding Analytical Processes and Playbooks

- Security Analytics
- SOC Playbook
- SOC Automation and Workflow
- Incident Response Concepts, Metrics, and Workflow
- Documenting Security Incidents in Cases
- Security Orchestration, Automation, and Response
- Cisco XDR
- Splunk Enterprise and Phantom Overview

Section 3: Understanding Cloud Service Model Security Responsibilities

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the laaS Service Model
- Security Responsibilities in the PaaS Service Model
- Security Responsibilities in the SaaS Service Model
- Cloud Deployment Models
- Key Security Controls in SaaS
- Cloud Access Security Broker

- Cisco Cloudlock
- Cloud Security Regulations and References

Section 4: Understanding Enterprise Environment Assets

- Asset Management
- Remediating Vulnerabilities and the SOC
- Assessing Vulnerabilities
- Patch Management
- Data Storage and Protecting Data Privacy
- Multi-Factor Authentication
- Zero Trust Model

Section 5: Understanding APIs

- API Overview
- CSV, HTML, and XML Data Encoding
- JSON Data Encoding
- YAML Data Serialization Standard
- HTTP-Based APIs
- RESTful APIs vs. Non-RESTful APIs
- Cisco pxGrid
- HTTP-Based Authentication
- Postman
- NETCONF
- Data Modeling with YANG
- RESTCONF
- Google RPC
- STIX and TAXII Specifications
- Role of APIs in Cisco Security Solutions
- Python Fundamentals
- Python Virtual Elements

Section 6: Understanding SOC Development and Deployment Models

- Agile Methodology
- DevOps Practices and Principles
- Components of a CI/CD Pipeline
- Essential Windows and Linux CLI for Development and Operations
- Infrastructure as Code
- SOC Platform Development, Engineering, Operation, and Maintenance

Section 7: Investigating Packet Captures, Logs, and Traffic Analysis

- Identity Access Management Logs
- Artifacts and Traffic Streams in a Packet Capture
- Nextgen Firewall and IPS Logs
- Dissecting Suspicious Requests
- Network Traffic Analysis Using NetFlow Analytics
- Detecting and Enforcing DLP On-the-Wire
- Cisco AMP Architecture

- Cisco Web Security Appliance
- Network DNS Logs
- Cisco Email Security Appliance
- Email Security Logs (Not Detection-Based)
- Cisco Umbrella

Section 8: Investigating Endpoint and Appliance Logs

- Cisco ISE Monitoring, Reporting, and Alerting
- Cisco Advanced Malware Protection
- Cisco Threat Grid
- Endpoint Logs from Non-Detection Sources
- Server DNS Logs
- Internet of Things
- Web Security Logs
- Endpoint Data Loss Prevention

Section 9: Implementing Threat Tuning

- Security Tuning Governance Policy
- Tuning Security Controls Rules, Filters, and Policies
- Determining If a Rule Is Defective
- Anatomy of a Snort Rule
- Troubleshooting Detection Rules
- Recommending Scenarios for Tuning

Section 10: Threat Research and Threat Intelligence Practices

- Cyber Threat Intelligence Overview
- Cyber Threat Intelligence Lifecycle
- Cyber Threat Intelligence Data Sources
- Indicators of Compromise and Indicators of Attack
- Security Intelligence Reports
- Cyber Attribution
- Cyber Threat Intelligence Tools
- Security Intelligence in a TIP Platform
- Using Indicator Analysis to Reveal Hidden Infections

Section 11: Performing Security Analytics and Reports in a SOC

- Security Data and Log Analytic Techniques
- Security Data Management Users
- Security Data with Log Management and Retention
- Security Data and Log Aggregations
- Security Information and Event Management
- Security Data and Log Analytics Automation
- Dashboards and Reports

Section 12: Malware Forensics Basics

- Malware Detection Tools
- Static Malware Analysis from Detection Tools
- Dynamic Malware Analysis from Sandbox Logs

- File Fingerprinting for Attribution
- Evading Detection
- File Forensics

Section 13: Threat Hunting Basics

- Proactive Threat Hunting Concepts
- Using MITRE ATTACK@ Framework for Threat Hunting
- Using CAPEC to Hunt for Weaknesses in Applications
- Evaluating Security Posture and Gaps in Controls Using MITRE ATTACK®
- Threat Hunting Case Study

Section 14: Performing Incident Investigation and Response

- Threat Modeling
- Attack Campaigns, Tactics, Techniques, and Procedures
- Steps to Investigate Potential Data Loss

Classroom Live Labs

- 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

CBRCOR - PERFORMING CYBERSECURITY USING CISCO SECURITY TECHNOLOGIES V1.1

Course Code: 821350

VIRTUAL CLASSROOM LIVE	$3,995 USD	5 Day

Virtual Classroom Live Outline

Section 1: Understanding Risk Management and SOC Operations

- Governance, Risk, and Compliance
- Security Regulatory Requirements
- Security Policy
- Protected Information
- Risk Analysis and Insurance
- SOC Services, Operations, and Automation
- SOC Service Models

Section 2: Understanding Analytical Processes and Playbooks

- Security Analytics
- SOC Playbook
- SOC Automation and Workflow
- Incident Response Concepts, Metrics, and Workflow
- Documenting Security Incidents in Cases
- Security Orchestration, Automation, and Response
- Cisco XDR
- Splunk Enterprise and Phantom Overview

Section 3: Understanding Cloud Service Model Security Responsibilities

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the laaS Service Model
- Security Responsibilities in the PaaS Service Model
- Security Responsibilities in the SaaS Service Model
- Cloud Deployment Models
- Key Security Controls in SaaS
- Cloud Access Security Broker

- Cisco Cloudlock
- Cloud Security Regulations and References

Section 4: Understanding Enterprise Environment Assets

- Asset Management
- Remediating Vulnerabilities and the SOC
- Assessing Vulnerabilities
- Patch Management
- Data Storage and Protecting Data Privacy
- Multi-Factor Authentication
- Zero Trust Model

Section 5: Understanding APIs

- API Overview
- CSV, HTML, and XML Data Encoding
- JSON Data Encoding
- YAML Data Serialization Standard
- HTTP-Based APIs
- RESTful APIs vs. Non-RESTful APIs
- Cisco pxGrid
- HTTP-Based Authentication
- Postman
- NETCONF
- Data Modeling with YANG
- RESTCONF
- Google RPC
- STIX and TAXII Specifications
- Role of APIs in Cisco Security Solutions
- Python Fundamentals
- Python Virtual Elements

Section 6: Understanding SOC Development and Deployment Models

- Agile Methodology
- DevOps Practices and Principles
- Components of a CI/CD Pipeline
- Essential Windows and Linux CLI for Development and Operations
- Infrastructure as Code
- SOC Platform Development, Engineering, Operation, and Maintenance

Section 7: Investigating Packet Captures, Logs, and Traffic Analysis

- Identity Access Management Logs
- Artifacts and Traffic Streams in a Packet Capture
- Nextgen Firewall and IPS Logs
- Dissecting Suspicious Requests
- Network Traffic Analysis Using NetFlow Analytics
- Detecting and Enforcing DLP On-the-Wire
- Cisco AMP Architecture

- Cisco Web Security Appliance
- Network DNS Logs
- Cisco Email Security Appliance
- Email Security Logs (Not Detection-Based)
- Cisco Umbrella

Section 8: Investigating Endpoint and Appliance Logs

- Cisco ISE Monitoring, Reporting, and Alerting
- Cisco Advanced Malware Protection
- Cisco Threat Grid
- Endpoint Logs from Non-Detection Sources
- Server DNS Logs
- Internet of Things
- Web Security Logs
- Endpoint Data Loss Prevention

Section 9: Implementing Threat Tuning

- Security Tuning Governance Policy
- Tuning Security Controls Rules, Filters, and Policies
- Determining If a Rule Is Defective
- Anatomy of a Snort Rule
- Troubleshooting Detection Rules
- Recommending Scenarios for Tuning

Section 10: Threat Research and Threat Intelligence Practices

- Cyber Threat Intelligence Overview
- Cyber Threat Intelligence Lifecycle
- Cyber Threat Intelligence Data Sources
- Indicators of Compromise and Indicators of Attack
- Security Intelligence Reports
- Cyber Attribution
- Cyber Threat Intelligence Tools
- Security Intelligence in a TIP Platform
- Using Indicator Analysis to Reveal Hidden Infections

Section 11: Performing Security Analytics and Reports in a SOC

- Security Data and Log Analytic Techniques
- Security Data Management Users
- Security Data with Log Management and Retention
- Security Data and Log Aggregations
- Security Information and Event Management
- Security Data and Log Analytics Automation
- Dashboards and Reports

Section 12: Malware Forensics Basics

- Malware Detection Tools
- Static Malware Analysis from Detection Tools
- Dynamic Malware Analysis from Sandbox Logs

- File Fingerprinting for Attribution
- Evading Detection
- File Forensics

Section 13: Threat Hunting Basics

- Proactive Threat Hunting Concepts
- Using MITRE ATTACK@ Framework for Threat Hunting
- Using CAPEC to Hunt for Weaknesses in Applications
- Evaluating Security Posture and Gaps in Controls Using MITRE ATTACK®
- Threat Hunting Case Study

Section 14: Performing Incident Investigation and Response

- Threat Modeling
- Attack Campaigns, Tactics, Techniques, and Procedures
- Steps to Investigate Potential Data Loss

Virtual Classroom Live Labs

- 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

Aug 10 - 14, 2026 | 8:30 AM - 4:30 PM EDT

Oct 5 - 9, 2026 | 8:30 AM - 4:30 PM EDT

Dec 7 - 11, 2026 | 8:30 AM - 4:30 PM EST

Feb 1 - 5, 2027 | 8:30 AM - 4:30 PM EST

Apr 5 - 9, 2027 | 8:30 AM - 4:30 PM EDT

CBRCOR - PERFORMING CYBERSECURITY USING CISCO SECURITY TECHNOLOGIES V1.1

Course Code: 821350

ON-DEMAND	$1,000 USD

On-Demand Outline

Section 1: Understanding Risk Management and SOC Operations

- Governance, Risk, and Compliance
- Security Regulatory Requirements
- Security Policy
- Protected Information
- Risk Analysis and Insurance
- SOC Services, Operations, and Automation
- SOC Service Models

Section 2: Understanding Analytical Processes and Playbooks

- Security Analytics
- SOC Playbook
- SOC Automation and Workflow
- Incident Response Concepts, Metrics, and Workflow
- Documenting Security Incidents in Cases
- Security Orchestration, Automation, and Response
- Cisco XDR
- Splunk Enterprise and Phantom Overview

Section 3: Understanding Cloud Service Model Security Responsibilities

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the laaS Service Model
- Security Responsibilities in the PaaS Service Model
- Security Responsibilities in the SaaS Service Model
- Cloud Deployment Models
- Key Security Controls in SaaS
- Cloud Access Security Broker

- Cisco Cloudlock
- Cloud Security Regulations and References

Section 4: Understanding Enterprise Environment Assets

- Asset Management
- Remediating Vulnerabilities and the SOC
- Assessing Vulnerabilities
- Patch Management
- Data Storage and Protecting Data Privacy
- Multi-Factor Authentication
- Zero Trust Model

Section 5: Understanding APIs

- API Overview
- CSV, HTML, and XML Data Encoding
- JSON Data Encoding
- YAML Data Serialization Standard
- HTTP-Based APIs
- RESTful APIs vs. Non-RESTful APIs
- Cisco pxGrid
- HTTP-Based Authentication
- Postman
- NETCONF
- Data Modeling with YANG
- RESTCONF
- Google RPC
- STIX and TAXII Specifications
- Role of APIs in Cisco Security Solutions
- Python Fundamentals
- Python Virtual Elements

Section 6: Understanding SOC Development and Deployment Models

- Agile Methodology
- DevOps Practices and Principles
- Components of a CI/CD Pipeline
- Essential Windows and Linux CLI for Development and Operations
- Infrastructure as Code
- SOC Platform Development, Engineering, Operation, and Maintenance

Section 7: Investigating Packet Captures, Logs, and Traffic Analysis

- Identity Access Management Logs
- Artifacts and Traffic Streams in a Packet Capture
- Nextgen Firewall and IPS Logs
- Dissecting Suspicious Requests
- Network Traffic Analysis Using NetFlow Analytics
- Detecting and Enforcing DLP On-the-Wire
- Cisco AMP Architecture

- Cisco Web Security Appliance
- Network DNS Logs
- Cisco Email Security Appliance
- Email Security Logs (Not Detection-Based)
- Cisco Umbrella

Section 8: Investigating Endpoint and Appliance Logs

- Cisco ISE Monitoring, Reporting, and Alerting
- Cisco Advanced Malware Protection
- Cisco Threat Grid
- Endpoint Logs from Non-Detection Sources
- Server DNS Logs
- Internet of Things
- Web Security Logs
- Endpoint Data Loss Prevention

Section 9: Implementing Threat Tuning

- Security Tuning Governance Policy
- Tuning Security Controls Rules, Filters, and Policies
- Determining If a Rule Is Defective
- Anatomy of a Snort Rule
- Troubleshooting Detection Rules
- Recommending Scenarios for Tuning

Section 10: Threat Research and Threat Intelligence Practices

- Cyber Threat Intelligence Overview
- Cyber Threat Intelligence Lifecycle
- Cyber Threat Intelligence Data Sources
- Indicators of Compromise and Indicators of Attack
- Security Intelligence Reports
- Cyber Attribution
- Cyber Threat Intelligence Tools
- Security Intelligence in a TIP Platform
- Using Indicator Analysis to Reveal Hidden Infections

Section 11: Performing Security Analytics and Reports in a SOC

- Security Data and Log Analytic Techniques
- Security Data Management Users
- Security Data with Log Management and Retention
- Security Data and Log Aggregations
- Security Information and Event Management
- Security Data and Log Analytics Automation
- Dashboards and Reports

Section 12: Malware Forensics Basics

- Malware Detection Tools
- Static Malware Analysis from Detection Tools
- Dynamic Malware Analysis from Sandbox Logs

- File Fingerprinting for Attribution
- Evading Detection
- File Forensics

Section 13: Threat Hunting Basics

- Proactive Threat Hunting Concepts
- Using MITRE ATTACK@ Framework for Threat Hunting
- Using CAPEC to Hunt for Weaknesses in Applications
- Evaluating Security Posture and Gaps in Controls Using MITRE ATTACK®
- Threat Hunting Case Study

Section 14: Performing Incident Investigation and Response

- Threat Modeling
- Attack Campaigns, Tactics, Techniques, and Procedures
- Steps to Investigate Potential Data Loss

On-Demand Labs

- 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

CBRCOR - PERFORMING CYBERSECURITY USING CISCO SECURITY TECHNOLOGIES V1.1

Course Code: 821350

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 6/15/2026 8:58:02 AM