


Course Name	Cisco Certified CyberOps Associate (200-201 CBROPS)	
About the Course	With a CyberOps Associate certification, you'll prove your expertise in essential cybersecurity skills, concepts, and technologies, including understanding IT infrastructure, operations, and vulnerabilities	
Key Skills You Will Learn	Security concepts, Security monitoring, Host-based analysis, Network intrusion analysis	
Course Pre-Requisite	No formal prerequisites,	
Target Audience	New or aspiring IT professionals who want to specialize in cybersecurity, Experienced IT professionals who want to prove their skills with Cisco and Cisco-adjacent cybersecurity technologies	
Job prospects with this role	Network security engineer, Security operations center (SOC) analyst, IT security operations specialist, CyberOps engineer, CyberOps analyst	
Course Duration	~ 12 Hrs	
Course Customisation	Not applicable	
Certification	READYBELL CISCO CyberOps Associate Certificate	
Mode of Training	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner	
Course Fees	Please contact us	
Refund Policy	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don't give refunds	
Job Assistance	Will assist candidate in securing a suitable job	
Contact	<p>READYBELL SOFTWARE SERVICES PVT. LIMITED AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091 E-MAIL: contact@readybellsoftware.com PH: +91 - 9147708045/9674552097, +91 - 33-79642872</p>	

CURRICULUM		
Topic	Sub-Topic	Duration (Hrs)
Cisco Certified CyberOps Associate (200-201 CBROPS)	Module 1: Security Concepts	12 Hrs
	Overview	
	Comparing Security Deployments Part 1	
	Comparing Security Deployments Part 2	
	Describing Security Terms Part 1	
	Describing Security Terms Part 2	
	Comparing Security Concepts	
	Comparing Access Control Models	
	Common Vulnerability Scoring System	
	The 5 Tuple Isolation Approach and Data Visibility	
	Module 2: Social Engineering Techniques	
	Overview	
	Introduction to Social Engineering	
	Phishing and Related Attacks	
	Low Tech Attacks	
	Identifying a Phishing Email	
	Social Engineering Toolkit	
	Module 3: Vulnerability and Attack Surfaces	
	Overview	
	Intro to Vulnerability and Attack Surfaces	
	On-Prem and Cloud-Based Vulnerabilities	
	Lack of Patch Management	
	Module 4: Cyber Attack Techniques	
	Overview	
	Introduction to Cyber Attack Techniques	
	Malware	
	Password Attacks	
	Password Attack Example	
	Cyber Physical Components	
	Adversarial AI	
Supply Chain Security		
Cryptographic Attacks		

Module 5: Data Types for Security Monitoring
Overview
Intro to Data Types for Security Monitoring
TCPdump Data
NetFlow Data
Data from Stateful Firewalls
Data from Next-gen Firewalls
IPS and IDS Data
Data from Security Appliances
Module 6: Application Attacks
Overview
Introduction to Application Attacks
Injection Attacks
Cross Site Scripting
Poorly Written Apps
Overflow Attack Demo
Poorly Written App Attack
Impersonation
Error Handling Attack
Additional Application Attacks
Password Recovery Fail
Module 7: Data Obfuscation and Hiding
Overview
Intro to Data Obfuscation and Hiding
Installing Tails
Steganography
HTTPS
NAT-PAT
Module 8: Network Attacks
Overview
Introduction to Network Attacks
In-line / On-path Attacks
Layer 2 attacks
Domain name system (DNS)
Distributed denial-of-service (DDoS)
Malicious code or script execution
Remediation Options

Module 9: Certificates and the PKI
Overview
Intro to Digital Certificates and the PKI
Symmetrical vs Asymmetrical Encryption
Digital Certificates Overview
Digital Signatures
Creating an HTTPS Session Key
Public Key Infrastructure
Module 10: Host Based Analysis
Overview
Endpoint Security Monitoring Technologies
Identifying the Role of Attribution
Comparing Disk Images
Interpreting Logs
Analyzing Sandbox Reports
Module 11: Operating System Fundamentals
Overview
Exploring the Windows Registry
Exploring Linux Processes
Linux File Permissions
Linux Sudo and Networking
Module 12: Network Intrusion Analysis
Overview
Introduction to Network Intrusion Analysis
Data Sources
Event Severity
PCAP analysis
Extract files from PCAP
Regular Expressions
Module 13: Incident Response and Forensic Evidence Collection
Overview
Information Security Management Concepts
Discussing Elements of an Incident Response (IR) Plan
Defining the Incident Response Process
Mapping Stakeholders to Incident Response (IR) Categories
Exploring the Forensic Evidence Collection Process

	Module 14: Security Policies and Procedures	
	Overview	
	Server Profiling	
	Network Profiling	
	Identifying Protected Network Data	
	SOC Metrics And Scope Analysis	
To register for this course please e-mail/call us		