CCNP CyberOps Cisco Security Technologies CBRCOR

Course Overview:

- The Performing CyberOps Using Cisco Security Technologies (CBRCOR) v1.0 course covers 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 shows 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.
- Expand your knowledge in the following areas:
- Monitoring for cyberattacks
- Analyzing high volume of data using automation tools and platforms—both open source and commercial
- Accurately identifying the nature of attack and formulate a mitigation plan
- Scenario-based questions; for example, using a screenshot of output from a tool, you may be asked to interpret portions of output and establish conclusions

Why Learn CCNP CyberOps Cisco Security Technologies CBRCOR?

Earn your Cisco Certified CyberOps Professional certification.

Learn core cyber security operations including cyber security fundamentals, techniques, processes, and automation.

Use automation for security using cloud platforms and a SecDevOps methodology.

Learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

Audience Profile :

- Cybersecurity engineers and investigators
- Incident managers
- Incident responders
- Network engineers
- SOC analysts currently functioning at entry level with 2+ years of experience

Prerequisites:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS).
- Implementing and Administering Cisco Solutions (CCNA).
- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar

CCNP CyberOps Cisco Security Technologies CBRCOR Outline:

- Module 1: Fundamentals
- Interpret the components within a playbook
- Determine the tools needed based on a playbook scenario
- Apply the playbook for a common scenario (for example, unauthorized elevation of privilege, DoS and DDoS, website defacement)
- Infer the industry for various compliance standards (for example, PCI, FISMA, FedRAMP, SOC, SOX, PCI, GDPR, Data Privacy, and ISO 27101)
- Describe the concepts and limitations of cyber risk insurance
- Analyze elements of a risk analysis (combination asset, vulnerability, and threat)
- Module 2: Techniques
- Describe the use of hardening machine images for deployment
- Describe the process of evaluating the security posture of an asset
- Evaluate the security controls of an environment, diagnose gaps, and recommend improvement
- Determine resources for industry standards and recommendations for hardening of systems
- Determine SecDevOps recommendations (implications)
- Describe use and concepts related to using a Threat Intelligence Platform (TIP) to automate intelligence
- Describe the different mechanisms to detect and enforce data loss prevention techniques
- Module 3: Processes
- Prioritize components in a threat model
- Determine the steps to investigate the common types of cases
- Apply the concepts and sequence of steps in the malware analysis process:
- Interpret the sequence of events during an attack based on analysis of traffic patterns
- Determine the steps to investigate potential endpoint intrusion across a variety of platform types (for example, desktop, laptop, IoT, mobile devices)
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs), given a scenario
- Determine IOCs in a sandbox environment (includes generating complex indicators)
- Module 4: Automation
- Compare concepts, platforms, and mechanisms of orchestration and automation
- Modify a provided script to automate a security operations task
- Recognize common data formats (for example, JSON, HTML, CSV, XML)
- Determine opportunities for automation and orchestration
- Determine the constraints when consuming APIs (for example, rate limited, timeouts, and payload)
- Explain the common HTTP response codes associated with REST APIs
- Evaluate the parts of an HTTP response (response code, headers, body)
- Interpret API authentication mechanisms: basic, custom token, and API keys
- Utilize Bash commands (file management, directory navigation, and environmental variables)
- Describe components of a CI/CD pipeline
- Apply the principles of DevOps practices
- Describe the principles of Infrastructure as Code

Training Solutions:

√ Offline Classroom Instructor-Led Training in our labs or onsite Locations.

√ Virtual Instructor-Led Training Via Virtual Video Conferencing Tools.

Why Learners Prefer CLS as their Training Services provider ?

■ Premuim Training Services Accredited from Global Technology Vendors.

■ Best Rated Experts & Certified Trainers in Egypt.

■ Official Training Hours, Practice Labs, Hands-on Learning.

■ CLS Training Classrooms are designed with High Edge PCs and Training Facilities.

■ Return on Training Investment is Guaranteed to boost performance.