CCNP CyberOps Forensic Analysis & Incident Response CBRFIR

Course Overview:

- The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) v1.0 course helps build your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills.
- The course prepares you to identify and respond to cybersecurity threats, vulnerabilities, and incidents.
- Additionally, you will be introduced to digital forensics, including the collection and examination of digital evidence on electronic devices and learn to build the subsequent response threats and attacks.
- Students will also learn to proactively conduct audits to prevent future attacks.
- The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) v1.0 course also prepares you to take the 300-215 CBRFIR exam.
- This course will help you:
- Develop an understanding of various cybersecurity threat and vulnerabilities
- Establish a framework for proactively responding to cybersecurity threat and vulnerabilities

Why Learn CCNP CyberOps Forensic Analysis & Incident Response CBRFIR?

Be the first line of defense with Cisco CyberOps Professional Certification.

Protect, detect, and defend against cybersecurity threats

Meet that demand and confirm your abilities as an Information Security analyst in incident response roles, cloud security, and other active defense security roles.

Audience Profile :

- SOC analysts, Tiers 1–2
- Threat researchers
- Malware analysts
- Forensic analysts
- Computer telephony integration (CTI) analysts
- Incident response analysts
- Security operations center engineers
- Security engineers

Prerequisites:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS).
- Performing CyberOps Using Cisco Security Technologies (CBRCOR).
- 2–3 years' experience working in a security operations center (SOC) environment.

CCNP CyberOps Forensic Analysis & Incident Response CBRFIR Outline:

- Module 1: Fundamentals
- Analyze the components needed for a root cause analysis report
- Describe the process of performing forensics analysis of infrastructure network devices
- Describe antiforensic tactics, techniques, and procedures
- Recognize encoding and obfuscation techniques (such as, base 64 and hex encoding)
- Describe the use and characteristics of YARA rules (basics) for malware identification, classification, and documentation
- Module 2: Forensics Techniques
- Recognize the methods identified in the MITRE attack framework to perform fileless malware analysis
- Determine the files needed and their location on the host
- Evaluate output(s) to identify IOC on a host
- Determine the type of code based on a provided snippet
- Construct Python, PowerShell, and Bash scripts to parse and search logs or multiple data sources (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid)
- Module 3: Incident Response Techniques
- Interpret alert logs (such as, IDS/IPS and syslogs)
- Determine data to correlate based on incident type (host-based and network-based activities)
- Recommend mitigation techniques for evaluated alerts from firewalls, intrusion prevention systems (IPS), data analysis tools (such as, Cisco Umbrella Investigate, Cisco Stealthwatch, and Cisco SecureX), and other systems to responds to cyber incidents
- Recommend the Cisco security solution for detection and prevention, given a scenario
- Interpret threat intelligence data to determine IOC and IOA (internal and external sources)
- Evaluate artifacts from threat intelligence to determine the threat actor profile
- Describe capabilities of Cisco security solutions related to threat intelligence (such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, and AMP for Network)
- Module 4: Forensics Processes
- Describe antiforensic techniques (such as, debugging, Geo location, and obfuscation)
- Analyze network traffic associated with malicious activities using network monitoring tools (such as, NetFlow and display filtering in Wireshark)
- Interpret binaries using objdump and other CLI tools (such as, Linux, Python, and Bash)
- Module 5: Incident Response Processes
- Evaluate the relevant components from the ThreatGrid report
- Recommend next step(s) in the process of evaluating files from endpoints and performing ad-hoc scans in a given scenario
- Analyze threat intelligence provided in different formats (such as, STIX and TAXII)

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.