Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Price: 800

Duration 365 Days

Delivery Methods eLearning

URL Enroll Buy Now

Overview

The duration of this course is 12 hours, and it is eligible for 40 CE credits towards recertification.

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.

How You'll Benefit

This training will help you:

- Develop an understanding of various cybersecurity threat and vulnerabilities
- Establish a framework for proactively responding to cybersecurity threat and vulnerabilities

Who Should Enroll

This course is designed for the following roles:

- 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

Learning Path Objectives

After taking this course, you should be able to:

- Analyze the components needed for a root cause analysis report
- Apply tools such as YARA for malware identification
- Recognize the methods identified in the MITRE attack framework
- Leverage scripting to parse and search logs or multiple data sources such as, Cisco Umbrella, Sourcefire IPS, AMP for Endpoints, AMP for Network, and PX Grid
- Recommend actions based on post-incident analysis
- Determine data to correlate based on incident type (host-based and network-based activities)
- Evaluate alerts from sources such as firewalls, intrusion prevention systems (IPS), data analysis tools (such as, Cisco Umbrella Investigate, Cisco Stealthwatch, and Cisco SecureX), and other systems to respond to cyber incidents and recommend mitigation
- Evaluate elements required in an incident response playbook and the relevant components from the ThreatGrid report
- Analyze threat intelligence provided in different formats (such as, STIX and TAXII)

Learning Path Prerequisites

Before taking this course, you should have:

- Familiarity with network and endpoint security concepts and monitoring
- Experience with network intrusion analysis
- An understanding of security policies and procedures
- Experience with risk management
- Experience with traffic and logs analysis
- Familiarity with APIs
- 2–3 years’ experience working in a security operations center (SOC) environment (experience Tier 1, or new Tier 2)

These recommended Cisco learning offerings may help students meet these prerequisites:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Performing CyberOps Using Cisco Security Technologies (CBRCOR)
- Splunk Fundamentals 1

Learning Path Outline

- Introduction to Incident Response
- Preparing for Incident Response
- Gathering and Examining Digital Intelligence
- Describing Detection, Analysis, and Investigation Forensics

Why Professional Choose TOPTALENT?

Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

Certified Industry Instructor

Learn from professionaly certified experts with real world experience and a proven commitment to learner success.

For questions

call:

(469) 721-6100

Email:

info@toptalentlearning.com

Find More Training

FAQ

What if I have to reschedule my class due to conflict?

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to info@toptalentlearning.com to avoid rescheduling penalties.

How do I enroll for this class?

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

What happens once I purchase a class?

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

What is your late policy?

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

What happens when I finish my class?

You will receive a 'Certificate of Completion' once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.