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

Duration: 180 Days

The Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR) training builds your Digital Forensics and Incident Response (DFIR) and cybersecurity knowledge and skills. This training 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. This training also prepares you to take the 300-215 CBRFIR exam.

Skills You'll Learn:

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

Learning Path Objectives:

After taking this training, 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 responds 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)