Understanding Cisco Cybersecurity Operations Fundamentals (CPLL-CBROPS)

Duration: 180 Days

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training provides an understanding of the network infrastructure devices, operations, and vulnerabilities of the TCP/IP protocol suite, and basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents. After completing this training, you will have the basic knowledge that is required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center (SOC).

This training prepares you for the 200-201 CBROPS v1.2 exam. If passed, you earn the Cisco Certified Cybersecurity Associate certification and the role of a junior or entry-level cybersecurity operations analyst in a SOC. This training also earns you 30 Continuing Education (CE) credits toward recertification.

Skills You'll Learn:

- Gain an understanding and follow established security procedures for response to alerts converted to incidents
- Learn about different models for incident investigations and response
- Discover how to identify common attack vectors, malicious activities, and suspicious behaviors

Learning Path Objectives:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective
- Explain the use of SOC metrics to measure the effectiveness of the SOC
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC
- Describe the Windows operating system features and functionality
- Provide an overview of the Linux operating system
- Understand common endpoint security technologies
- Explain the network security monitoring (NSM) tools that are available to the network security analyst
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts

- Explain the data that is available to the network security analyst
- Describe the basic concepts and uses of cryptography
- Understand the foundational cloud security practices, including deployment and service models, shared responsibilities, compliance frameworks, and identity and access management, to effectively secure cloud environments against cyberthreats
- Understand and implement advanced network security, data protection, secure application deployment, continuous monitoring, and effective disaster recovery strategies to secure cloud deployments
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors
- Identify the common attack vectors
- Identify malicious activities
- Identify patterns of suspicious behaviors
- Identify resources for hunting cyber threats
- Explain the need for event data normalization and event correlation
- Conduct security incident investigations
- Explain the use of a typical playbook in the SOC
- Describe a typical incident response plan and the functions of a typical computer security incident response team (CSIRT)