CBROPS – Understanding Cisco Cybersecurity Operations Fundamentals

Days: *5*

Prerequisites: The knowledge and skills that the learner should have before attending this course are: Familiarity with Ethernet and TCP/IP networking, working knowledge of the Windows and Linux operating systems, and familiarity with basics of networking security concepts.

Audience: Associate-level cybersecurity analysts who are working in security operation centers.

Description: The Understanding Cybersecurity Operations Fundamentals (CBROPS) is a 5-day course that teaches participants about the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices, and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification.

Please note that this course is a combination of Instructor-Led and Self-Paced Study – 5 days in the classroom and approximately 1 day of self-study. The self-study content will be included in the digital courseware you receive at the beginning of the course and should be part of your exam preparation.

The course qualifies for 30 Cisco Continuing Education credits (CE) towards recertification.

Course Objectives: After taking this course, you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- 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.

CBROPS – Understanding Cisco Cybersecurity Operations Fundamentals

- Describe a typical incident response plan and the functions of a typical CSIRT.
- Explain the use of VERIS to document security incidents in a standard format.
- Describe the Windows operating system features and functionality.
- Describe the Linux operating system features and functionality.

OUTLINE:

- **Defining the Security Operations Center**
- **Understanding Network Infrastructure and Network Security Monitoring Tools**
- **Exploring Data Type Categories**
- **Understanding Basic Cryptography Concepts**
- **Understanding Common TCP/IP Attacks**
- **Understanding Endpoint Security Technologies**
- **Understanding Incident Analysis in a Threat-Centric SOC**
- **Identifying Resources for Hunting Cyber Threats**
- **Understanding Event Correlation and Normalization**
- **Identifying Common Attack Vectors**
- **Identifying Malicious Activity**
- **Identifying Patterns of Suspicious Behavior**
- **Conducting Security Incident Investigations**
- **Using a Playbook Model to Organize Security Monitoring**
- **Understanding SOC Metrics**
- **Understanding SOC Workflow and Automation**
- **Describing Incident Response**
- **Understanding the Use of VERIS**
- **Understanding Windows Operating System Basics**
- **Understanding Linux Operating System Basics**