Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

Course Duration

5 Days

Course Price

$4,295.00
43 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.1 training teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This training teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities.

This training helps you prepare for the Cisco® Certified CyberOps 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 towards recertification.

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

How you will benefit

This class will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam which earns the Cisco Certified CyberOps Associate certification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Students pursuing a technical degree
- Current IT professionals
- Recent college graduates with a technical degree

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

Objectives

After taking this course, you should be able to:

- Explain how a Security Operations Center (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.
- Describe a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT).
- Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

Course Outline

Module 1: Defining the Security Operations Center

Module 2: Understanding Network Infrastructure and Network Security Monitoring Tools

Module 3: Exploring Data Type Categories

Module 4: Understanding Basic Cryptography Concepts

Module 5: Understanding Common TCP/IP Attacks

Module 6: Understanding Endpoint Security Technologies

Module 7: Understanding Incident Analysis in a Threat-Centric SOC

Module 8: Identifying Resources for Hunting Cyber Threats

Module 9: Understanding Event Correlation and Normalization

Module 10: Identifying Common Attack Vectors

Module 11: Identifying Malicious Activity

Module 12: Identifying Patterns of Suspicious Behavior

Module 13: Conducting Security Incident Investigations

Module 14: Using a Playbook Model to Organize Security Monitoring

Module 15: Understanding SOC Metrics

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

Course Outline

Module 16: Understanding SOC Workflow and Automation

Module 17: Describing Incident Response

Module 18: Understanding the Use of VERIS

Module 19: Understanding Windows Operating System Basics

Module 20: Understanding Linux Operating System Basics

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) V1.0

Lab Outline

- **Lab 1:** Use NSM Tools to Analyze Data Categories
- **Lab 2:** Explore Cryptographic Technologies
- **Lab 3:** Explore TCP/IP Attacks
- **Lab 4:** Explore Endpoint Security
- **Lab 5:** Investigate Hacker Methodology
- **Lab 6:** Hunt Malicious Traffic
- **Lab 7:** Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack
- **Lab 8:** Investigate Browser-Based Attacks
- **Lab 9:** Analyze Suspicious Domain Name System (DNS) Activity
- **Lab 10:** Explore Security Data for Analysis
- **Lab 11:** Investigate Suspicious Activity Using Security Onion
- **Lab 12:** Investigate Advanced Persistent Threats
- **Lab 13:** Explore SOC Playbooks
- **Lab 14:** Explore the Windows Operating System
- **Lab 15:** Explore the Linux Operating System