Understanding Cisco Cybersecurity Operations Fundamentals Training (CBROPS)

Course: **00113**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Systems & Network Security**
Price: **1200,00 €**

About Course

The Understanding Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

What you'll learn

- 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.

Targeted audience

- Recommended as preparation for the following exams: 200-201 - CBROPS Understanding Cisco Cybersecurity Operations Fundamentals.

Pre-requisites

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions
- (CCNA) course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

Curriculum

Module 1: Defining the knowledge areas and process groups

-

Module 2: Defining the Security Operations Center

-

Module 3: Understanding Network Infrastructure and Network Security Monitoring Tools

-

Module 4: Exploring Data Type Categories

-

Module 5: Understanding Basic Cryptography Concepts

-

Module 6: Understanding Common TCP/IP Attacks

-

Module 7: Understanding Endpoint Security Technologies

-

Module 8: Understanding Incident Analysis in a Threat-Centric SOC

-

Module 9: Identifying Resources for Hunting Cyber Threats

-

Module 10: Understanding Event Correlation and Normalization

-

Module 11: Identifying Common Attack Vectors

-

Module 12: Identifying Malicious Activity

-

Module 13: Identifying Patterns of Suspicious Behavior

-

Module 14: Conducting Security Incident Investigations

-

Module 15: Using a Playbook Model to Organize Security Monitoring

-

Module 16: Understanding SOC Metrics

-

Module 17: Understanding SOC Workflow and Automation

-

Module 18: Describing Incident Response

-

Module 19: Understanding the Use of VERIS

-

Module 20: Understanding Windows Operating System Basics

-

Module 21: Understanding Linux Operating System Basics

-