CBROPS (UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS) 1.0

Objetivo

After taking this course, you should be able to: â¢ Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analystâs perspective; â¢ Explain Network Security Monitoring (NSM) tools that are available to the network security analyst; â¢ Explain the data that is available to the network security analyst; â¢ Describe the basic concepts and uses of cryptography; â¢ Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts; â¢ Understand common endpoint security technologies. â¢ Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors; â¢ Identify resources for hunting cyber threats; â¢ Explain the need for event data normalization and event correlation; â¢ Identify the common attack vectors; â¢ Identify malicious activities; â¢ Identify patterns of suspicious behaviors; â¢ Conduct security incident investigations; â¢ Explain the use of a typical playbook in the SOC; â¢ Explain the use of SOC metrics to measure the effectiveness of the SOC;Ã§ â¢ Explain the use of a workflow management system and automation to improve the effectiveness of the SOC; â¢ Describe a typical incident response plan; â¢ Describe functions of a typical Computer Security Incident Response Team (CSIRT); â¢ Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

PÃºblico Alvo

This course is designed for individuals seeking a role as an associate-level cybersecurity analyst and IT professionals desiring knowledge in Cybersecurity operations or those in pursuit of the Cisco Certified CyberOps Associate certification.

PrÃ©-Requisitos

Before taking this course, you should have the following knowledge and skills: â¢ Familiarity with Ethernet and TCP/IP networking; â¢ Working knowledge of the Windows and Linux operating systems; â¢ Familiarity with basics of networking security concepts. The following Cisco course can help you gain the knowledge you need to prepare for this course: â¢ Implementing and Administering Cisco Solutions (CCNAÂ®)

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Course Introduction
Course Outline
Course Goals & Objectiveds

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

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