IT-SECOPS - Implementing Cisco Cybersecurity Operations

Cisco - CCNA Cyber Ops - Networking

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**Cisco Certified CyberOps Associate**

Descrizione del corso

The Implementing Cisco Cybersecurity Operations (SECOPS) v1.0 course gives you foundation-level knowledge of security incident analysis techniques used in a Security Operations Center (SOC). You will learn how to identify and analyze threats and malicious activity, correlate events, conduct security investigations, use incident playbooks, and learn SOC operations and procedures. This is the second of two courses that prepare you for the Cisco® CCNA® Cyber Ops certification. This certification validates your knowledge and hands-on skills to help handle cybersecurity events as an associate-level member of an SOC team. This course helps you prepare to take the 210-255 SECOPS exam, second of the two required exams to achieve the CCNA Cyber Ops certification. The 210-255 SECOPS exam will be available on February 24, 2020.

Programma

SOC Overview

- Defining the Security Operations Center
- Understanding NSM Tools and Data
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats

Security Incident Investigations

- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations

SOC Operations

- Describing the SOC Playbook
- Understanding the SOC Metrics
- Understanding the SOC WMS and Automation
- Describing the Incident Response Plan
- Appendix A – Describing the Computer Security Incident Response Team
- Appendix B – Understanding the use of VERIS

Lab outline

- Explore Network Security Monitoring Tools
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks