Rumos valorizamos profissionais!

Implementing Cisco Cybersecurity Operations (SECOPS)

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Porto
- **Data:** 13 Mai. 2019 a 17 Mai. 2019
- **Preço:** 2750€
- **Horário:** Laboral - das 09h00 às 17h00
- **Duração:** 35 horas

This is the second course in Cisco's CCNA Cyber Ops Curriculum and is designed to provide students with an understanding of how a Security Operations Center (SOC) functions and the knowledge required in this environment.

This course focuses on the introductory-level skills needed for a SOC Analyst at the associate level. Specifically, understanding basic threat analysis, event correlation, identifying malicious activity and how to use a playbook for incident response.

This course will help you:

- Learn the fundamental skills that a cybersecurity analyst in a security operations center uses, including threat analysis, event correlation, identifying malicious activity, and how to use a playbook for incident response
- Prepare for the Cisco Certified CyberOps Associate certification with hands-on practice using real-life security analysis tools, such as those found in a Linux distribution
- Qualify for entry-level job roles in the high-demand area of cybersecurity

Destinatários

- IT professionals
- Any learner interested in entering associate-level cybersecurity roles such as:
    - SOC cybersecurity analysts
    - Computer or network defense analysts
    - Computer network defense infrastructure support personnel
    - Future incident responders and SOC personnel
    - Cisco integrators or partners

Pré-requisitos

To fully benefit from this course, you should first complete the following course or obtain the equivalent knowledge and skills:

- **Understanding Cisco Cybersecurity Fundamentals (SECFND)**

Objectivos

After taking this course, you should be able to:

- Describe the three common SOC types, tools used by SOC analysts, job roles within the SOC, and incident analysis within a threat-centric SOC
- Explain security incident investigations, including event correlation and normalization and common attack vectors, and be able to identify malicious and suspicious activities
- Explain the use of an SOC playbook to assist with investigations, the use of metrics to measure the effectiveness of the SOC, the use of an SOC workflow management system and automation to improve SOC efficiency, and the concepts of an incident response plan

---

Programa

- **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