CCNA CYBEROPS: IMPLEMENTING CYBERSECURITY OPERATIONS (SECOPS)

DATE: To be confirmed **CONTACT: academy@techlan.it** **PRICE: Request**

COURSE OBJECTIVE:

This course allows learners to understand how Cisco Security Operations Center (SOC) functions and the introductory-level skills and knowledge needed in this environment. It 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.

Upon completing this course, you will be able to:

- Define a SOC and the various job roles in a SOC
- Understand SOC infrastructure tools and systems
- Learn basic incident analysis for a threat centric SOC
- Explore resources available to assist with an investigation
- Explain basic event correlation and normalization
- Describe common attack vectors
- Learn how to identify malicious activity
- Understand the concept of a playbook
- Describe and explain an incident respond handbook
- Define types of SOC Metrics
- Understand SOC Workflow Management system and automation

PREREQUISIT:

It is recommended, but not required, that students have the following knowledge and skills:

Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1)

Working knowledge of the Windows operating system

Working knowledge of Cisco IOS networking and concepts

In relation to EXAM:

210-255 SECOPS

WHO SHOULD ATTEND

Security Operations Center – Security Analyst

Computer/Network Defense Analysts

Computer Network Defense Infrastructure Support Personnel

Future Incident Responders and Security Operations Center (SOC) personnel

Students beginning a career, entering the cybersecurity field

TECHLAN

ACADEMY

COURSE CONTENT:

Module 1: 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

Module 2: Security Incident Investigations
Understanding Event Correlation and Normalization
Identifying Common Attack Vectors
Identifying Malicious Activity
Identifying Patterns of Suspicious Behavior
Conducting Security Incident Investigations

Module 3: 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

LABS:

Lab 1: Explore Network Security Monitoring Tools
Lab 2: Investigate Hacker Methodology
Lab 3: Hunt Malicious Traffic
Lab 4: Investigate Browser –Based attacks
Lab 5: Analyse suspicious DNS Activity
Lab 6: Investigate Suspicious Activity Using Security Onion
Lab 7: Investigate Advanced Suspicious Threats
Lab 8: Explore SOC Playbooks