CISC-17 - SECOPS - IMPLEMENTING CISCO CYBERSECURITY OPERATIONS

Categoria: **Cisco**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	Cisco	Cisco Certified Network Associate	Professionista IT	Cisco

OBIETTIVI

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 a SOC playbook to assist with investigations, the use of metrics to measure the effectiveness of the SOC, the use of a SOC workflow management system and automation to improve SOC efficiency, and the concepts of an incident response plan

PREREQUISITI

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)
- -The following Cisco learning offering can help you meet this prerequisite:
  CCNA Cyber Ops SECFND #210-250 Official Cert Guide, by Omar Santos, Joseph Muniz, and Stefano De Crescenzo

CONTENUTI

Content Outline

- -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

INFO

Esame: 210-255 - Implementing Cisco Cybersecurity Operations
Manuale: Student Kit Ufficiale Cisco
Prezzo manuale: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)