CISC-19 - CCNACBR - UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS V2.0

Categoria: **Cisco**

INFORMAZIONI SUL CORSO

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

OBIETTIVI

After completing this course you should be able to:

- Explain the foundational aspects of SOCs, including their types, key roles, and essential metrics for measuring effectiveness
- Apply foundational security principles and risk management concepts to assess and protect organizational assets
- Compare and apply various access control models to secure network resources and enforce organizational policies
- Differentiate between various cloud deployment and service models and explain the shared responsibility for security in cloud environments
- Explain the fundamental concepts of cryptography, differentiate between various cryptographic algorithms, and explain how cryptographic principles are applied in real-world protocols and systems, including key exchange, digital signatures, and SSL/TLS
- Identify and describe the fundamental components and operational aspects of the Windows operating system for security analysis
- Identify and describe the fundamental components and operational aspects of the Linux operating system for security analysis
- Utilize Command Line Interfaces (CLIs) for basic system interaction, file management, and security-related tasks in both Windows and Linux environments
- Explain the operations and identify the security implications of foundational network protocols
- Describe and differentiate various network security controls and their application in protecting network infrastructure
- Differentiate between various Intrusion Detection and Prevention Systems (IDS/IPS) and interpret their output for security monitoring
- Describe and compare various endpoint security solutions and their effectiveness against common threats
- Identify and categorize various cyber threat actors based on their motivations, capabilities, and common tactics
- Explain the phases of the Classic Cyber Kill Chain model and identify adversary actions within each phase
- Apply the MITRE ATT&CK Framework to analyze and map cyber threats, explain its structure and application, and leverage it to enhance threat detection, incident response, and communication within a security operations environment
- Identify and describe various social engineering attack vectors, including those enhanced by generative AI
- Describe fundamental network attack techniques that exploit protocol vulnerabilities
- Describe advanced attack vectors and emerging threats in the current cybersecurity landscape

- Identify and explain various types of Network Security Monitoring (NSM) data and their role in incident investigation
- Identify and interpret various log data sources from operating systems, network devices, and security tools
- Explain NetFlow operations and its application as a security tool for network monitoring and anomaly detection
- Describe common web application attacks and their exploitation methods
- Apply advanced log analysis techniques to interpret security data and identify patterns of suspicious behavior
- Perform packet capture analysis and apply digital forensics processes to investigate security incidents. Focus on the 5-tuple and timestamps to correlate with other logs, as this is your primary tool for network forensics
- Explain malware analysis outputs and apply threat intelligence frameworks for security investigations
- Explain the architecture, core functions, and best practices for implementing SIEM solutions for effective security monitoring
- Explain the features and common use cases of SOAR platforms for automating and streamlining incident response
- Explain the Cisco XDR platform, its core functions, features, and components for unified threat detection and response
- Differentiate between the legacy and modern NIST incident response guidance (NIST SP 800-61 Rev 2 and NIST SP 800-61 Rev 3 special publications), describe core IR components aligned with the NIST CSF 2.0 framework, and identify how these practices satisfy CMMC requirements for the Defense Industrial Base (DIB)
- Describe the roles, categories, and operational services of Computer Security Incident Response Teams (CSIRTs)
- Explain the concept of security monitoring playbooks and their components for standardizing incident response
- Apply various threat hunting methodologies to proactively identify and mitigate hidden threats within a network

PREREQUISITI

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

Recommended prerequisites:

- CCNA - Implementing and Administering Cisco Solutions

CONTENUTI

Course Outline

- Security Operations
- Security Principles
- Access Control Models
- Cloud Security Models
- Cryptography for Security Operations
- Windows OS Basics
- Linux OS Basics
- CLIs in Security
- Network Protocols
- Network Security Controls
- IDS and IPS

-Endpoint Security
-Threat Actors
-Cyber Kill Chain Model
-MITRE Attack Framework
-Social Engineering Attacks
-Network Attack Fundamentals
-Advanced Threat Landscape
-Network Security Monitoring (NSM) Data
-Log Data Sources
-NetFlow for Security Monitoring
-Web Application Attacks
-Advanced Log Analysis
-Packet Capture and Forensics
-Malware and Threat Intelligence
-Security Information and Event Management (SIEM)
-Security Orchestration, Automation, and Response (SOAR)
-Extended Detection and Response (XDR)
-Incident Response Planning
-CSIRT Roles and Operations
-Security Monitoring Playbooks
-Threat Hunting Methodologies

Lab Outline

-Explore Cryptographic Technologies
-Explore the Windows Operating System
-Explore the Linux Operating System
-Explore Endpoint Security
-Investigate Hacker Methodology
-Explore TCP/IP Attacks
-Investigate Advanced Persistent Threats
-Use NSM Tools to Analyze Data Categories
-Analyze Suspicious DNS Activity
-Investigate Browser-based Attacks
-Correlate Event Logs, PCAPs, and Alerts of an Attack
-Explore SOC Playbooks
-Hunt Malicious Traffic

INFO

Esame: 200-201 - Understanding Cisco Cybersecurity Operations Fundamentals
Materiale didattico: Materiale didattico ufficiale Cisco in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)