

CISC-19 - CBROPS - UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS V1.2

Categoria: **Cisco**

INFORMAZIONI SUL CORSO



Durata:
5 Giorni



Categoria:
Cisco



Qualifica Istruttore:
**Cisco Certified
Instructor**



Dedicato a:
Professionista IT



Produttore:
Cisco

OBIETTIVI

After completing this course you should be able to:

- Explain how a SOC operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective
- Explain the use of SOC metrics to measure the effectiveness of the SOC
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC
- Describe the Windows operating system features and functionality
- Provide an overview of the Linux operating system
- Understand common endpoint security technologies
- Explain the network security monitoring (NSM) tools that are available to the network security analyst
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts
- Explain the data that is available to the network security analyst
- Describe the basic concepts and uses of cryptography
- Understand the foundational cloud security practices, including deployment and service models, shared responsibilities, compliance frameworks, and identity and access management, to effectively secure cloud environments against cyberthreats
- Understand and implement advanced network security, data protection, secure application deployment, continuous monitoring, and effective disaster recovery strategies to secure cloud deployments
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors
- Identify the common attack vectors
- Identify malicious activities
- Identify patterns of suspicious behaviors
- Identify resources for hunting cyber threats
- Explain the need for event data normalization and event correlation
- Conduct security incident investigations
- Explain the use of a typical playbook in the SOC
- Describe a typical incident response plan and the functions of a typical computer security incident response team (CSIRT)

PREREQUISITI

Attendees should meet the following prerequisites:

- 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

Defining the Security Operations Center

- Types of Security Operations Centers
- SOC Analyst Tools
- Data Analytics
- Hybrid Installations: Automated Reports, Anomaly Alerts
- Staffing an Effective Incident Response Team
- Roles in a Security Operations Center
- Developing Key Relationships with External Resources

Understanding SOC Metrics

- Security Data Aggregation
- Time to Detection
- Security Controls Detection Effectiveness
- SOC Metrics

Understanding SOC Workflow and Automation

- SOC WMS Concepts
- Incident Response Workflow
- SOC WMS Integration
- DevSecOps in Cybersecurity
- Automate Security in CI/CD Pipelines
- DevSecOps for Cloud-Native and Containerized Environments
- SecOps Collaboration and DevSecOps Culture
- SOC Workflow Automation Example

Understanding Windows Operating System Basics (Self-Study)

- Windows Operating System History
- Windows Operating System Architecture
- Windows Processes, Threads and Handles
- Windows Virtual Memory Address Space
- Windows Services
- Windows File System Overview
- Windows File System Structure
- Windows Domains and Local user Accounts
- Windows GUI
- Run as Administrator
- Windows CLI

- Windows Powershell
- Windows net Command
- Controlling Startup Services and Executing System shutdown
- Controlling Services and Processes
- Monitoring System Resources
- Windows Boot Process
- Windows Networking
- Windows netstat Command
- Accessing Network Resources with Windows
- Windows Registry
- Windows Management Instrumentation
- Common Windows Server Functions
- Common Third-Party Tools
- Lab Set-up Video: Explore the Windows Operating System

Understanding Linux Operating System Basics (Self-Study)

- History and Benefits of Linux
- Linux Architecture
- Linux File System Overview
- Basic File System Navigation and Management Commands
- File Properties and Permissions
- Editing File Properties
- Root and Sudo
- Disks and File Systems
- System Initialization
- Emergency/Alternate Startup Options
- Shutting Down the System
- System Processes
- Interacting with Linux
- Linux Command Shell Concepts
- Piping Command Output
- Other Useful Command-Line Tools
- Overview of Secure Shell Protocol
- Networking
- Managing Services in SysV Environments
- Viewing Running Network Services
- Name Resolution: DNS
- Testing Name Resolution
- Viewing Network Traffic
- Configuring Remote Syslog
- Running Software on Linux
- Executables vs Interpreters
- Using Package Managers to Install Software in Linux
- System Applications
- Lightweight Directory Access Protocol
- Lab Set-Up Video: Explore the Linux Operating System

Understanding Endpoint Security Technologies

- Host-Based Personal Firewall
- Signature-Based and Rule-Based Monitoring
- Monitor Network Traffic and the Endpoint Level
- Predictive AI in Endpoint Security Monitoring
- AI-Driven Behavioral Analysis for Threat Detection
- Machine Learning Technologies in Host-Based Monitoring
- Cisco ML-and AI-Powered Security Solutions
- Host-Based Antivirus
- Host Intrusion Prevention System
- Application Allowed Lists and Blocked Lists
- Host-Based Malware Protection
- Sandboxing
- File Integrity Checking
- Lab Set-Up Video: Explore Endpoint Security
- Secure Virtualized Environments
- Container Security Fundamentals
- Monitor and Protect Container Workloads
- Best Security Practices for Hybrid Environments

Understanding Network Infrastructure and Network Security Monitoring Tools

- NAT Fundamentals
- Packet Filtering with ACLs
- ACLs with the Established Option
- Access Control Models
- Authentication, Authorization and Accounting
- Load Balancing
- Network-Based Malware Protection
- Network Security Monitoring Tools

Understanding Common TCP/IP Attacks

- Address Resolution Protocol
- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- ICMP Vulnerabilities
- TCP Vulnerabilities
- UDP Vulnerabilities
- Attack Surface and Attack Vectors
- Reconnaissance Attacks
- Access Attacks
- Man-in-the-Middle Attacks
- Denial of Service and Distributed Denial of Service
- Reflection and Amplification Attacks
- Spoofing Attacks
- DHCP Attacks

Exploring Data Type Categories

- Network Security Monitoring Data Types
- Security Onion Overview

- Full Packet Capture
- Packet Captures
- Packet Capture Using Tcpdump
- Session Data
- Transaction Data
- Alert data
- Other Data Types
- Correlating NSM Data
- Information Security Confidentiality, Integrity and Availability
- Personally Identifiable Information
- Regulatory Compliance
- Intellectual Property

Understanding Basic Cryptography Concepts

- Impact of Cryptography on Security Investigations
- Cryptography Overview
- Hash Algorithms
- Encryption Overview
- Cryptanalysis
- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithms
- Diffie-Helman Key Agreement
- Use Case: SSH
- Digital Signatures
- PKI Overview
- PKI Operations
- Use Case: SSL/TLS
- Cipher Suite
- Key Management
- NSA Suite B

Cloud Security Fundamentals

- Cloud Deployment and Service Models
- Shared Responsibility Model in Cloud Security
- Cloud Security Frameworks and Compliance
- Identity and Access Management in Cloud Environments

Securing Cloud Deployments

- Network Security in Cloud Environments
- Data Protection in the Cloud
- Secure Cloud Workload and Applications
- Cloud Monitoring, Logging and Incident Response
- Threat Detection and Vulnerability Management in the Cloud
- Disaster Recovery and Business Continuity in the Cloud

Understanding Incident Analysis in a Threat-Centric SOC

- Classic Kill Chain Model Overview
- Social Engineering Attack Vectors

- Generative AI in Social Engineering
- Detecting and Mitigating Social Engineering Threats
- Kill Chain Phase 1: Reconnaissance
- Kill Chain Phase 2: Weaponization
- Kill Chain Phase 3: Delivery
- Kill Chain Phase 4: Exploitation
- Kill Chain Phase 5: Installation
- Kill Chain Phase 6: Command-and-Control
- Kill Chain Phase 7: Actions on Objectives
- Applying the Kill Chain Model
- Diamond Model Overview
- Applying the Diamond Model
- MITRE ATTACK Framework

Identifying Common Attack Vectors

- DNS Operations
- Dynamic DNS
- Recursive DNS Query
- HTTP Operations
- HTTPS Operations
- HTTP/2 Operations
- SQL Operations
- SMTP Operations
- Web Scripting
- Obfuscated JavaScript
- Shellcode and Exploits
- Common Metasploit Payloads
- Directory Traversal
- SQL Injection
- Cross-Site Scripting
- Punycode
- DNS Tunneling
- Pivoting
- HTTP 302 Cushioning
- Gaining Access Via Web-Based Attacks
- Exploit Kits
- Emotet Advanced Persistent Threat

Identifying Malicious Activity

- Understanding the Network Design
- Zero Trust Model
- Identifying Possible Threat Actors
- Log Data Search
- System Logs
- Windows Event Viewer
- Firewall Log
- DNS Log
- Web Proxy Log

- Email Proxy Log
- AAA Server Log
- Next Generation Firewall Log
- Application Log
- NetFlow
- NetFlow as a Security Tool
- Network Behavior Anomaly Detection
- Data Loss Detection Using NetFlow example
- DNS Risk and Mitigation Tool
- IPS Evasion Techniques
- The Onion Router
- Gaining Access and Control
- Peer-to-Peer Networks
- Encapsulation
- Altered Disk Image

Identifying Patterns of Suspicious Behavior

- Network Baselineing
- Identifying Anomalies and Suspicious Behaviors
- PCAP Analysis
- Delivery

Identifying Resources for Hunting Cyber Threats

- Cyber-Threat Hunting Concepts
- Hunting Maturity Model
- Cyber Threat Hunting Cycle
- Common Vulnerability Scoring System
- CVSS v3.0 Scoring
- CVSS v3.0 Example
- Hot Threat Dashboard
- Publicly Available Threat Awareness Resources
- Other External Threat Intelligence Sources and Feed Reference
- Security Intelligence
- Threat Analytic Systems
- Security Tools Reference

Understanding Event Correlation and Normalization

- Event Sources
- Implementing SIEM Solutions for Effective Security Monitoring
- SOAR Platform Overview
- Cisco XDR Platform Overview
- Integrating XDR, SIEM, and SOAR for SOC Efficiency
- Evidence
- Chain of Custody
- Security Data Normalization
- Event Correlation
- Other Security Data Manipulation

Conducting Security Incident Investigations

- Security Incident Investigation Procedures
- Threat Investigation Example: China Chopper Remote Access Trojan

Using a Playbook Model to Organize Security Monitoring

- Security Analytics
- Playbook Definition
- What is a Play?
- Playbook Management System

Describing Incident Response

- Incident Response Planning
- Incident Response Life Cycle
- Incident Response Policy Elements
- Incident Attack Categories
- Reference US-CERT Incident Categories
- Regulatory Compliance Incident Response Requirements
- CSIRT Categories
- CSIRT Framework
- CSIRT Incident Handling Services

Labs

- Discovery Lab 1: Use NSM Tools to Analyze Data Categories
- Discovery Lab 2: Explore Cryptographic Technologies
- Discovery Lab 3: Explore TCP/IP Attacks
- Discovery Lab 4: Explore Endpoint Security
- Discovery Lab 5: Investigate Hacker Methodology
- Discovery Lab 6: Hunt Malicious Traffic
- Discovery Lab 7: Correlate Event Logs, PCAPs, and Alerts of an Attack
- Discovery Lab 8: Investigate Browser-Based Attacks
- Discovery Lab 9: Analyze Suspicious DNS Activity
- Discovery Lab 10: Explore Security Data for Analysis
- Discovery Lab 11: Investigate Suspicious Activity Using Security Onion
- Discovery Lab 12: Investigate Advanced Persistent Threats
- Discovery Lab 13: Explore SOC Playbooks
- Discovery Lab 14: Explore the Windows Operating System
- Discovery Lab 15: Explore the Linux Operating System

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)