Understanding Cisco Cybersecurity Operations Fundamentals

Duration: 5 Days **Course Code: CBROPS** **Version: 1.1**

Overview:

The **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)** course teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This training teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities. This course prepares you for the Cisco Certified Cybersecurity Associate certification.

Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx 1 day of self study. The self-study content will be provided as part of the digital courseware that you will recieve at the beginning of the course and should be part of your preparation for the exam.

This course is worth 30 Continuing Education (CE) Credits towards recertification.

Target Audience:

This course is designed for an associate-level cybersecurity analyst working in a security operation center (SOC).

Objectives:

- **After completing this course you should be able to:**
- Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- 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 a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT).
- Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Prerequisites:

Attendees should meet the following prerequisites:

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

Testing and Certification

Recommended as preparation for the following exams:

- **200-201** - CBROPS Understanding Cisco Cybersecurity Operations Fundamentals

- Familiarity with basics of networking security concepts
- CCNA - Implementing and Administering Cisco Solutions

Content:

Defining the Security Operations Center

- Types of Security Operations Centers
- SOC Analyst Tools
- Data Analytics

Understanding Network Infrastructure and Network Security Monitoring Tools

- NAT Fundamentals
- Packet Filtering with ACLs
- Hybrid Installations: Automated Reports, Anomaly Alerts
- Staffing an Effective Incident Response Team
- Rules in a Security Operations Center
- Developing Key Relationships with External Resources
- ACLs with the Established Option
- Access Control Models
- Authentication, Authorization and Accounting
- Load Balancing
- Network-Based Malware Protection
- Network Security Monitoring Tools

Exploring Data Type Categories

- Network Security Monitoring Data Types
- Security Information and Event Management Systems
- Security Orchestration, Automation and Response
- 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

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
- Evidence
- Chain of Custody
- Security Data Normalization
- Event Correlation
- Other Security Data Manipulation

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 Persistant 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

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
- SOC Workflow Automation Example

Describing Incident Response

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

Understanding the Use of VERIS (Self-Study)

- VERIS Overview
- VERIS Incidents Structure
- VERIS 4 A's
- VERIS Records
- VERIS Community Database
- Verizon Data Breach Investigation Report and Cisco Annual Security Report

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

- Use Case: SSL/TLS
- Cipher Suite
- Key Management
- NSA Suite B

Understanding Common TCP/IP Attacks

- Address Resolution Protocol
- Legacy TCP/IP Vulnerabilties
- 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

Understanding Endpoint Security Technologies

- Host-Based Personal Firewall
- 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

Understanding Incident Analysis in a Threat-Centric SOC

- Classic Kill Chain Model Overview
- 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

- 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 Baselining
- Identifying Anomalies and Suspicious Behaviors
- PCAP Analysis
- Delivery

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

- 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 Opertaing System

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

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/