Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Course Duration: 40 Hours **Course code: CBROPS**

1. Course 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.

2. What you'll learn?

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)

3. Target Audience

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

4. Pre-Requisites

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

5. Course content

Module 1: Defining the Security Operations Center (SOC)

- Role of SOC in Enterprise Security
- SOC Analyst Responsibilities
- Collaboration with IT and Incident Response Teams
- SOC Tools and Platforms Overview

Module 2: Understanding Network Infrastructure and Network Security Monitoring Tools

- Components of Network Infrastructure
- Firewalls, IDS/IPS, and Proxy Servers
- Network Monitoring Tools (SIEM, NetFlow, Packet Capture Tools)
- Network Topologies and Data Flow in Security Monitoring

Module 3: Exploring Data Type Categories

- Host-Based Data (Logs, Process Information)
- Network-Based Data (Packets, Flows)
- Threat Intelligence Data
- Data Sources for Analysis in SOC

Module 4: Understanding Basic Cryptography Concepts

- Importance of Cryptography in Security
- Symmetric vs. Asymmetric Encryption
- Hashing, Digital Signatures, and Certificates
- Cryptographic Protocols (SSL/TLS, IPSec)

Module 5: Understanding Common TCP/IP Attacks

- Denial-of-Service (DoS) and Distributed DoS
- IP Spoofing, Man-in-the-Middle (MitM), and Sniffing
- TCP SYN Floods and Fragmentation Attacks
- Attack Signatures in Packet Analysis

Module 6: Understanding Endpoint Security Technologies

- Antivirus and EDR Solutions
- Sandboxing and Application Control
- Host-Based Firewalls and HIPS
- Logging and Monitoring Endpoint Activity

Module 7: Understanding Incident Analysis in a Threat-Centric SOC

- Incident Detection and Categorization
- Analyzing Alerts from SIEM and IDS
- Identifying Attack Patterns and Indicators
- Coordinating with Response Teams

Module 8: Identifying Resources for Hunting Cyber Threats

- Threat Intelligence Platforms
- Open Source and Commercial Resources
- Utilizing STIX, TAXII, and MITRE ATT&CK Framework
- Threat Hunting Methodologies

Module 9: Understanding Event Correlation and Normalization

- Correlation Rules in SIEM Systems
- Normalization of Log Data
- Cross-Device Event Linking
- Reducing False Positives

Module 10: Identifying Common Attack Vectors

- Email and Phishing Attacks
- Web-Based Exploits
- Drive-By Downloads and Malicious Ads
- Removable Media and Physical Attacks

Module 11: Identifying Malicious Activity

- Behavioral Indicators of Malware
- Identifying C2 (Command and Control) Communication
- Data Exfiltration Techniques
- Persistence Mechanisms

Module 12: Identifying Patterns of Suspicious Behavior

- Login Anomalies and Credential Abuse
- File Integrity and Registry Changes
- Suspicious Scripting Activity
- Heuristics and Machine Learning in Detection

Module 13: Conducting Security Incident Investigations

- Steps in Security Investigation Process
- Collecting and Preserving Evidence
- Documentation and Reporting
- Case Studies of Real-World Incidents

Module 14: Using a Playbook Model to Organize Security Monitoring

- What is a Security Playbook?
- Playbook Development and Automation
- Example Playbooks for Common Incidents
- Integration with SOAR Tools

Module 15: Understanding SOC Metrics

- Key Performance Indicators (KPIs) for SOCs
- MTTR, Detection Time, Escalation Rates
- Metrics for Process and Analyst Performance
- Reporting and Continuous Improvement

Module 16: Understanding SOC Workflow and Automation

- Alert Triage and Ticketing Systems
- Escalation Procedures and Analyst Roles
- Workflow Automation with SOAR
- Runbooks and Response Templates

Module 17: Describing Incident Response

- NIST Incident Response Lifecycle
- Phases: Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned
- Roles and Responsibilities during IR
- Communication and Legal Considerations

Module 18: Understanding the Use of VERIS

- What is VERIS (Vocabulary for Event Recording and Incident Sharing)?
- VERIS Framework Structure and Use Cases
- Mapping Incidents to VERIS Categories
- Integration with DBIR (Data Breach Investigations Report)

Module 19: Understanding Windows Operating System Basics

- Windows File System and Registry
- Task Manager, Event Viewer, and Windows Logs
- User Profiles and System Services
- Command-Line Tools for Troubleshooting

Module 20: Understanding Linux Operating System Basics

- File System Hierarchy and Permissions
- System Logs and Log Files (/var/log)
- Common Linux Commands for Security Monitoring
- Process and Service Management

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com