Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Course Duration: 40 Hours **Course code: CBRCOR**

1. Course Overview

You will learn foundational concepts and their application in real-world scenarios, and how to leverage playbooks in formulating an Incident Response (IR). The course teaches you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

2. What you'll learn?

Upon successful completion of this course, you should be able to:

- Describe the types of service coverage within a SOC and operational responsibilities associated with each.
- Compare security operations considerations of cloud platforms.
- Describe the general methodologies of SOC platforms development, management, and automation.
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, and approaches to each, as part of asset controls and protections.
- Describe Zero Trust and associated approaches, as part of asset controls and protections.
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC.
- Use different types of core security technology platforms for security monitoring, investigation, and response.

- Describe the DevOps and SecDevOps processes.
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Describe API authentication mechanisms.
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response.
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Interpret the sequence of events during an attack based on analysis of traffic patterns.
- Describe the different security tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyze anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

3. Target Audience

Cybersecurity analysts, engineers, investigators and incident responders.

4. Pre-Requisites

Attendees should meet the following pre-requisites:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands
- Familiarity with the Splunk search and navigation functions
- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar.

Recommended prerequisites:

- CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals v1.2

- CCNA - Implementing and Administering Cisco Solutions v2.1

5. Course content

Module 1: Understanding Risk Management and SOC Operations

Introduction to Risk Management in Cybersecurity

SOC Roles, Responsibilities, and Tiers

Threat Modeling and Risk Mitigation Techniques

Security Controls and Incident Handling Lifecycle

SOC Metrics, SLAs, and KPIs

Module 2: Understanding Analytical Processes and Playbooks

Cyber Kill Chain and MITRE ATT&CK Framework

Security Operations Workflows

Creating and Automating Playbooks

Event Triage and Escalation Models

Playbook Implementation in Cisco SecureX

Module 3: Investigating Packet Captures, Logs, and Traffic Analysis

Capturing and Analyzing Network Traffic

TCP/IP and Protocol Behavior Analysis

Using Wireshark and Cisco Secure Network Analytics (Stealthwatch)

Packet and Flow Correlation to Incidents

Identifying Malicious Patterns in Network Traffic

Module 4: Investigating Endpoint and Appliance Logs

Windows/Linux Log Structures and Analysis

Event Viewer, Syslog, and Sysmon Deep Dive

Cisco Secure Endpoint and AMP for Endpoints

Interpreting Firewall and IDS Logs

Detecting Privilege Escalation and Malware Activity

Module 5: Understanding Cloud Service Model Security Responsibilities

Security in IaaS, PaaS, and SaaS Models

Shared Responsibility Model

Cloud-native Threats and Vectors

Securing AWS, Azure, and Google Cloud Services

Cisco Cloud Security Portfolio Overview

Module 6: Understanding Enterprise Environment Assets

Identifying Critical Assets and Data Flow Mapping

IT vs. OT Assets and Their Risks

Asset Inventory and Classification

Business Impact Analysis

Integration of CMDB in SOC Workflows

Module 7: Implementing Threat Tuning

Alert Fatigue and Noise Reduction

Creating and Refining Detection Rules

Customizing Correlation Rules in SIEMs

Cisco SecureX Orchestration for Threat Tuning

Reducing False Positives and Increasing Visibility

Module 8: Threat Research and Threat Intelligence Practices

OSINT and Threat Research Techniques

Consuming and Enriching Threat Feeds

STIX, TAXII, and Threat Intelligence Sharing

Cisco Talos and Threat Grid

Building Threat Profiles and Indicators of Compromise (IOCs)

Module 9: Understanding APIs for SOC Automation

Role of APIs in SOC Automation

REST API Fundamentals
Integrating APIs with Cisco Security Tools
Creating Scripts for Automated Workflows
Securing API Usage and Access

Module 10: Understanding SOC Development and Deployment Models
In-House, MSSP, and Hybrid SOC Models
Building a SOC: Tools, Processes, and Personnel
Centralized vs. Distributed SOCs
Multi-Tenant Security Operations
SOC-as-a-Service and Future Trends

Module 11: Performing Security Analytics and Reports in a SOC
Data Aggregation and Correlation Techniques
Creating Dashboards and Executive Reports
KPIs and Metrics for Security Analytics
Using Cisco SecureX, Secure Analytics, and Splunk
Reporting Compliance and Risk Posture

Module 12: Malware Forensics Basics
Introduction to Malware Types and Behaviors
Static vs. Dynamic Analysis
Behavioral Indicators and IOC Extraction
Sandboxing with Cisco Threat Grid
Tools for Basic Forensic Investigation

Module 13: Threat Hunting Basics
Proactive Threat Hunting vs. Reactive Analysis
Hypothesis-Driven Investigations
Data Sources and Pivoting Techniques
Leveraging MITRE ATT&CK in Threat Hunts

Threat Hunting Lab Exercises

Module 14: Performing Incident Investigation and Response

Incident Detection and Verification

Scoping and Containment Strategies

Eradication, Recovery, and Lessons Learned

Post-Incident Reporting

Collaboration with Stakeholders and Law Enforcement