S|CE
SOC Essentials

EC-Council
Building A Culture Of Security

SOC Essentials

COURSE OUTLINE

EC-Council Official Curricula

SOC Essentials Outline

Module 01: Computer Network and Security Fundamentals

- Computer Network
- TCP/IP Model
- OSI Model
- Types of Networks
- Network Model
  - Types of a Network
    - Types of a Network (PAN)
    - Types of a Network (LAN)
    - Types of a Network (WLAN)
    - Types of a Network (MAN)
    - Types of a Network (WAN)
    - Types of a Network (SAN)
- Network Topologies
  - Network Hardware Components
- TCP/IP Protocol Suite
- Network Security Controls
  - Key Network Security Controls
- Network Security Devices
- Windows Security
- Unix/Linux Security
- Web Application Fundamentals
- Information Security Standards, Laws and Acts

Module 02: Fundamentals of Cyber Threats

- Cyber Threats
  - Classification of Cyber Threats
  - Impact of Cyber Threats
  - Vulnerability in Cybersecurity
  - Cybersecurity Best Practices
  - Emerging Threats and Future challenges
  - Ransomware
  - Impact of Ransomware
- Intent-Motive-Goal
  - Cybercrime Performed
  - Email compromise Attack
- Tactics-Techniques-Procedures (TTPs)
  - Example -Data Exfiltration
  - Practical Example – Data Exfiltration
  - Key Steps for Lateral Movement
  - APT - Example
- Opportunity-Vulnerability-Weakness
  - Opportunity
  - Vulnerability
  - Weakness
  - Practical Example- E-Commerce Website
  - Practical Example- Online Banking System
- Vulnerability
  - Type of vulnerabilities
  - Source of Vulnerabilities
  - Lifecycle of Vulnerabilities
  - Practical Example - Vulnerability
- Threats & Attack
  - Types of Threat & Attack

- Cyber Threat
- Mitigation strategies for Cyber Threats

- Example of Attacks
  - Example of Attack – Blended Cyber Attack
  - Example of Attack -Man-in-the-Middle Attack for Credentials Harvesting
- Network-based attacks
- Application-based
  - Cross-site Scripting
  - Types of Cross-site Scripting
  - Attack Process
  - Application Based Attack
- Host Based Attacks
  - Host Based Attack - Impact
- Insider Attacks
  - Types of Insider Attacks
  - Prevention and Mitigation
  - Examples
- Malware (viruses, worms, ransomware, etc.)
  - Types of Malware
  - Distribution Method
  - Prevention And Mitigations
- Phishing and social engineering
  - Common Characteristics
  - Examples
  - Prevention
  - Social Engineering Common Characteristics
  - Example
  - Prevention
  - Key Difference

Module 03: Introduction to Security Operations Center (SOC)

- What is a Security Operations Center (SOC)?
- Importance of SOC
  - Importance of SOC in Cybersecurity
- SOC Team Roles & Responsibilities
- SOC KPI
- SOC Metrics
- SOC Maturity Models
  - Typical Stages in the SOC Maturity Model
  - Benefits of the SOC Maturity Model
- SOC Workflow and Processes
- Challenges in Operating a SOC

Module 04: SOC Components and Architecture

- Key Components of a SOC
  - Security Operation Center
  - Breakdown of the Key Components of the SOC
- People in SOC
- Processes in SOC
  - Key Processes in SOC
  - Example of Processes in SOC
- Technologies in SOC
  - Key Technology in SOC
- SOC Architecture and Infrastructure
  - Key Components of SOC Architecture and Infrastructure
- Different Types of SOC and Their Purpose
- Introduction to SIEM
  - Key components of SIEM
  - Benefits of SIEM
  - Challenges of SIEM
  - Use Cases of SIEM

- SIEM Architecture
  - Key Components of SIEM Architecture
  - SIEM Architecture
- SIEM Deployment Model
- Data Sources in SIEM
- SIEM Logs
  - Overview of Logs in SIEM Environment
- Networking in SIEM
- Endpoint Data in SIEM

Module 05: Introduction to Log Management

- Incident
  - Example of Cybersecurity Incidents
- Event
  - Example of Cybersecurity Events
- Log
  - Key points of Logs
  - Example of Log Types
- Typical Log Sources
  - Typical Log Sources with Example
- Need of Log
- Typical Log Format
- Local Log management
  - Benefits of Local Log Management
- Centralized Log Management
  - Key Components of Centralized Log Management
- Logging Best Practices
- Logging/Log Management Tools

Module 06: Incident Detection and Analysis

- SIEM Use Cases Development
- Security Monitoring and analysis
  - Basic Concept of Security Monitoring
  - Basic Concept of Security Analysis
  - Security Monitoring and Analysis Process
  - Practical Example – Malware Detection and Analysis
  - Practical Example – Abnormal or non-typical user Behavior Detection
  - Practical Example – Phishing Attack Detection and Response
- Correlation Rules
  - Overview of Correlation Rules
  - Use cases: Detection of a Distributed Denial of Service (DDoS) Attack
- Dashboards
  - Overview of Dashboards
- Reports
  - Key Components of Reports
  - Types of Reports
  - Benefits of Reports
- Alerting
  - Purpose of Alerting
  - Key components of Alerting
  - Type of Alerts
  - Alerting Workflow
  - Benefits of Alert
- Triaging alerts
  - Purpose of Triaging alerts
  - Key components of Triaging alerts
  - Triage Process
  - Benefits of Triaging alerts
- Dealing with False Positive Alerts

- Mitigation strategies
- Final step in Dealing with False positive Alerts

- Incident Escalation
  - Purpose of Incident Escalation
  - Key Components of Incident Escalation
  - Escalation Process
  - Benefits of Incident Escalation
- Communication Paths
  - Common Communication paths in cybersecurity
- Ticketing Systems
  - Example of Ticketing Systems

Module 07: Threat Intelligence and Hunting

- Introduction to Threat Intelligence
  - Breakdown of Threat Intelligence
- Threat Intelligence Sources
- Threat Intelligence Types
- Threat Intelligence Lifecycle
- Role of Threat Intelligence in SOC operations
- Threat Intelligence Feeds
  - Types of Threat Intelligence Feeds
  - Content and Format
  - Integration and consumption
  - Evaluation and Selection
- Threat Intelligence Sharing and Collaboration
  - Types of Threat Intelligence Sharing
  - Benefits of Threat Intelligence sharing
  - Challenges and Considerations
- Threat Intelligence Tools/Platforms
  - Malware Analysis Platform

- Open-Source Intelligence Tools
- Vulnerability Management Tools
- Threat Intelligence Feeds and APIs
- Dark Web Monitoring Tools
- Adversary Emulation Platforms

- Introduction to threat Hunting
- Threat Hunting Techniques
  - Common Threat threat-hunting techniques
- Threat Hunting Methodologies
  - Common Threat Hunting Methodologies
- Role of Threat Hunting In SOC Operations
- Leveraging Threat Intelligence for Hunting
- Threat Hunting Tools

Module 08: Incident Response and Handling

- Incident Handling Process
  - Steps in the Incident Handling Process
- Incident classification and prioritization
  - Breakdown of Incident Classification
- Incident response lifecycle
  - Preparation
  - Detection & Analysis
  - Containment, Eradication & Recovery
  - Post-Incident Analysis
  - Continuous Improvement
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Post-Incident Analysis and Reporting