SOC Essentials

Course Duration: 40 Hrs. **Course code: 112-56**

Course Overview

The SOC Essentials course provides foundational knowledge in Security Operations Center (SOC) concepts, equipping learners with the skills needed to monitor, detect, and respond to security threats, particularly beneficial for those new to cybersecurity.

What you'll learn?

- **Computer Networks & Security:**
  Learn about TCP/IP, OSI models, and fundamental security concepts.
- **Cyber Threats, Vulnerabilities, and Attacks:**
  Understand various cyber threats, vulnerabilities, and attack patterns.
- **SOC Architecture & Operations:**
  Explore the structure, workflow, and processes of a Security Operations Center (SOC).
- **Security Tools & Technologies:**
  Gain familiarity with essential tools like SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), and EDR (Endpoint Detection and Response).
- **Incident Response:**
  Understand the incident response lifecycle and processes.
- **Threat Intelligence:**
  Learn about sources, types, and the lifecycle of threat intelligence.

V25031

Target Audience

- **Cybersecurity Professionals:**
  The course is designed for individuals looking to enter the cybersecurity field, providing a solid foundation in SOC operations.
- **Graduates:**
  Students and recent graduates can use this course to gain practical skills and knowledge in cybersecurity, preparing them for entry-level roles.
- **Career Switchers:**
  Individuals from non-IT backgrounds who want to transition into cybersecurity can benefit from this course, which provides a comprehensive overview of SOC fundamentals.

Pre-Requisites

- **No Prior Experience Required:**
  Many courses, like the EC-Council SOC Essentials Series, are designed for complete beginners, including those looking to switch careers into cybersecurity.
- **Basic IT Knowledge:**
  A fundamental understanding of IT concepts, networking, and operating systems (Windows and Linux) is helpful, but not always mandatory.
- **Curiosity and Willingness to Learn:**
  The most important prerequisite is a genuine interest in cybersecurity and a willingness to learn new skills.

Course content

Module 1: Computer Network and Security Fundamentals

A. Computer Network
B. TCP/IP Model
C. OSI Model
D. Types of Networks
E. Network Model

F. Network Topologies
G. TCP/IP Protocol Suite
H. Network Security Controls
I. Network Security Devices
J. Windows Security
K. Unix/Linux Security
L. Web Application Fundamentals
M. Information Security Standards, Laws, and Acts

Module 2: Fundamentals of Cyber Threats

A. Cyber Threats
B. Intent-Motive-Goal
C. Tactics-Techniques-Procedures (TTPs)
D. Opportunity-Vulnerability-Weakness
E. Vulnerability
F. Threats & Attacks
G. Example of Attacks
H. Network-based Attacks.
I. Application-based
J. Host Based Attacks
K. Insider Attacks
L. Malware (Viruses, Worms, Ransomware, etc.)
M. Phishing and Social Engineering

Module 3: Introduction to Security Operations Center

A. What is a Security Operations Center (SOC)?
B. Importance of SOC
C. SOC Team Roles and Responsibilities
D. SOC KPI
E. SOC Metrics
F. SOC Maturity Models
G. SOC Workflow and Processes
H. Challenges in Operating a SOC

Module 4: SOC Components and Architecture

A. Key Components of a SOC
B. People in SOC
C. Processes in SOC
D. Technologies in SOC
E. SOC Architecture and Infrastructure
F. Different Types of SOCS and Their Purposes
G. Introduction to SIEM
H. SIEM Architecture
I. SIEM Deployment Models
J. Data Sources in SIEM
K. SIEM Logs
L. Networking in SIEM
M. Endpoint Data in SIEM

Module 5: Introduction to Log Management

A. Incident
B. Event
C. Log
D. Typical Log Sources
E. Need of Log
F. Typical Log Format
G. Local Log Management
H. Centralized Log Management
I. Logging Best Practices
J. Logging/Log Management Tools

Module 6: Incident Detection and Analysis

A. SIEM Use Case Development
B. Security Monitoring and Analysis
C. Correlation Rules
D. Dashboards

E. Reports
F. Alerting
G. Triaging Alerts
H. Dealing with False Positive Alerts
I. Incident Escalation
J. Communication Paths
K. Ticketing Systems

Module 7: Threat Intelligence and Hunting

A. Introduction to Threat Intelligence
B. Threat Intelligence Sources
C. Threat Intelligence Types
D. Threat Intelligence Lifecycle
E. Role of Threat Intelligence in SOC Operations
F. Threat Intelligence Feeds
G. Threat Intelligence Sharing and Collaboration
H. Threat Intelligence Tools/Platforms
I. Introduction to Threat Hunting
J. Threat Hunting Techniques
K. Threat Hunting Methodologies
L. Role of Threat Hunting in SOC Operations
M. Leveraging Threat Intelligence for Hunting
N. Threat Hunting Tools

Module 8: Incident Response and Handling

A. Incident Handling Process
B. Incident Classification and Prioritization
C. Incident Response Lifecycle
D. Preparation
E. Identification
F. Containment
G. Eradication
H. Recovery
I. Post-Incident Analysis and Reporting

Exam Preference

Exam Code	112-56
Number Of Questions	75
Length Of Test	120 Minutes
Passing Score	75%