SOC Essentials Program Information

Course Outline

Module 1: Computer Network and Security Fundamentals

Topics covered:

- Computer Network
- TCP/IP Model
- OSI Model
- Types of Networks
- Network Model
- Network Topologies
- TCP/IP Protocol Suite
- Network Security Controls
- Network Security Devices
- Windows Security
- Unix/Linux Security
- Web Application Fundamentals
- Information Security Standards, Laws, and Acts

Module 2: Fundamentals of Cyber Threats

Topics covered:

- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Vulnerability
- Threats & Attacks
- Example of Attacks
- Network-based Attacks
- Application-based
- Host Based Attacks
- Insider Attacks
- Malware (Viruses, Worms, Ransomware, etc.)
- Phishing and Social Engineering

Module 3: Introduction to Security Operations Center

Topics covered:

- What is a Security Operations Center (SOC)?
- Importance of SOC
- SOC Team Roles and Responsibilities
- SOC KPI
- SOC Metrics
- SOC Maturity Models
- SOC Workflow and Processes
- Challenges in Operating a SOC

Module 4: SOC Components and Architecture

Topics covered:

- Key Components of a SOC
- People in SOC
- Processes in SOC
- Technologies in SOC
- SOC Architecture and Infrastructure
- Different Types of SOC and Their Purposes
- Introduction to SIEM
- SIEM Architecture
- SIEM Deployment Models
- Data Sources in SIEM
- SIEM Logs
- Networking in SIEM
- Endpoint Data in SIEM

Module 5: Introduction to Log Management

Topics covered:

- Incident
- Event
- Log
- Typical Log Sources
- Need of Log
- Typical Log Format
- Local Log Management
- Centralized Log Management
- Logging Best Practices
- Logging/Log Management Tools

Module 6: Incident Detection and Analysis

Topics covered:

- SIEM Use Case Development
- Security Monitoring and Analysis
- Correlation Rules
- Dashboards
- Reports
- Alerting
- Triaging Alerts
- Dealing with False Positive Alerts
- Incident Escalation
- Communication Paths
- Ticketing Systems

Module 7: Threat Intelligence and Hunting

Topics covered:

- Introduction to Threat Intelligence
- Threat Intelligence Sources
- Threat Intelligence Types
- Threat Intelligence Lifecycle
- Role of Threat Intelligence in SOC Operations
- Threat Intelligence Feeds
- Threat Intelligence Sharing and Collaboration
- Threat Intelligence Tools/Platforms

- Introduction to Threat Hunting
- Threat Hunting Techniques
- Threat Hunting Methodologies
- Role of Threat Hunting in SOC Operations
- Leveraging Threat Intelligence for Hunting
- Threat Hunting Tools

Module 8: Incident Response and Handling

Topics covered:

- Incident Handling Process
- Incident Classification and Prioritization
- Incident Response Lifecycle
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Post-Incident Analysis and Reporting

What You'll Learn

- Learn the basics of computer networks
- Dive deep into the cyber threat concepts like threats, vulnerabilities, and attacks.
- Gain insights into the Security Operations Center (SOC) architecture and learn the importance, workflow, and processes of SOC.
- Understand advanced architectural concepts like SIEM architecture and deployment models.
- Learn what log management is and its key parts, like events, logs, and incidents.
- Learn how you can perform centralized management of logs.
- Gain knowledge on dashboards, reports, and incident escalation in terms of dealing with real positive and false alerts.
- Discover the sources, types, and lifecycle of threat intelligence and get introduced to threat hunting.
- Deep dive into the Incident response lifecycle.

Who Is it For

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity and is interested in SOC.
- This course is also helpful for IT professionals, SOC analysts, system security professionals, security engineers, threat management professionals, incident response teams, security administrators, vulnerability management professionals, and any cybersecurity professional.