Security Operations Center

EC-Council Accredited Training Center

SevenMentor PVT.LTD

SOC (Security Operations Center) ANALYST TRAINING

Module 1 : SOC Essential Concepts

- Basics of Networking and Security Concepts
- Types of IP address How Computer Communication.
- Transport Protocol IP Planning.
- DNS Server and Various types of DNS records.
- Understanding of OSI model and Reference layer devices.
- TCP/IP Packet Understanding. 3 Ways Handshake.
- Router, Switches And designing Corporate network etc.
- Understanding of Firewall. Web Application Firewall (WAF) Proxy
- Email Gateway (Email Security)
- Network ATTACK

Module 2 : Security Operations and Management

- Security Management
- Security Operations
- Security Operations Center (SOC)
- Need of SOC
- SOC Capabilities

SevenMentor PVT.LTD

- SOC Operations
- SOC report
- Kill Chain Deep Dive Scenario - Spear Phishing

Module 03: Understanding Cyber Threats and Attack Methodology

- Cyber Threats
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Network Level Attack
- Application Level Attacks
- SQL Injection Attacks
- Email Security Threats

Module 04 : Incidents, Events, and Logging

- What is the mean of Log
- What is incidents and event
- Local Logging : windows and linux logs
- How to get ROUTER AND WEB SERVER LOGS
- WHAT is Centralized Logging
- Why we need a logs
- Deeply log analysis
- Alerting and reporting

Module 05: Incident Detection with Security Information and Event Management (SIEM)

- Security Information and Event Management(SIEM)
- Need of SIEM
- Typical SIEM Capabilities
- SIEM Architecture and Its Components
- Splunk Enterprise Security
- Nessus
- SIEM Deployment
- Incident Detection with SIEM
- Handling Alert Triaging and Analysis

Module 6: Incident Detection with Threat Intelligence

- Understanding Cyber Threat Intelligence
- How can Threat Intelligence Help Organizations?
- Threat Intelligence Strategy
- Threat Intelligence Sources: OSINT

Module 07: Incident Response

- Incident Response (IR) Process Overview
- SOC and IRT collaboration
- Responding to Network Security Incident
- Responding to Application Security Incidents
- Responding to Email Security Incidents
- Responding to an Insider Incidents

WHAT YOU'LL BE LEARNING IN THIS COURSE?

SOC Team actually use SIEM tools to monitor the real-time threat activities so in this training we will cover SEIM tools This training is completely Realtime training, what experienced SOC Analyst people are actually doing in the companies all we will be covering here practically

EC-Council Valued By Leading Organizations Across The World

SevenMentor PVT.LTD