CyberlyUSA

Delivering Efficiency, Driving IT Excellency

SOC ANALYST

SOC Analyst Course Outline

Module 01:
Security Operations Center Concepts

- CIA Triad • Types of Hackers • What is SOC?

- Why is it required? (Objectives)
- NOC Vs. SOC
- SOC Infrastructure
- SOC Models and types
- Concept of Logging
  - Local Logging vs Centralized Logging
- Log management
  - Computer Security Log Management
  - Log Management Infrastructure
  - Log Management Planning
  - Log Management Operational Process
- Incidents vs Events
- True vs False Incident Categories
- Common Attacks
  - DOS and DDOS
  - Ransomware
  - Malwares
  - Phishing
  - Brute-force

Module 02:
Fundamentals Networking and Data Communications

- **OSI Model and TCP/IP Networking Model**
- **Basic Networking and Network Devices Concepts**
  Firewall
  IDS
  IPS
  VPN
  Switches and Routers

- **Network Security and Authentication Concepts**
- **Ports, Protocols and Services in Networking**
- **Conducting a Port Scan with Nmap – Practical**

Module 03:
Anatomy of Cyber Attacks and Unauthorized Access

- **Common Windows Operating System Threats**
- **Common Linux Operating System Threats**
- **Common Network Attacks and Network Security Threats**
- **Common Network Port and Network Protocol-based Attacks**

Module 04:
Blue Team Vulnerability Assessment Exercises

- What is a Vulnerability?
- What is Vulnerability Analysis?
- Overview of Vulnerability Assessment
- Different types of Vulnerability Issues?
- What are the different types of vulnerability Issues?
- Importance of Vulnerability Assessment

Module 05:
Blue Team Vulnerability Assessment Exercises -Practicals

- Well-known Advantageous Vulnerability Assessment tools
- Windows Operating System Vulnerability Analysis
- Linux Operating System Vulnerability Analysis
- Web Application Vulnerability Analysis
- Major Vulnerabilities Analysis using CVE ID
- Vulnerability Classification and Severity levels Analysis
- Threat and Vulnerability Assessment Report Writing

Module 06:
SIEM (Security Information and Event Management) System of SOC

- Introduction to SIEM
- SIEM Vs. SEM Vs. EDR Vs. XDR Vs. MDR Vs. SOAR
- SIEM Architecture
- Logs and Events
- Understanding Windows logs
- Understanding Linux logs
- Log Baselining
- SIEM Capabilities: Aggregation, Reporting, Storage, Alerts
- Event Collection and Event Correlation
- Correlation Rules
- SOC Workflows and Playbooks

Module 07:
Introduction to Microsoft Sentinel

- Introduction to Security Information and Event Management (SIEM)
- Explanation of Microsoft Sentinel as a SIEM tool
- • Understanding the key features and benefits of Microsoft Sentinel
  • Comparison of Microsoft Sentinel with other SIEM tools

Module 08:
Key KQL Fundamentals for Sentinel and Security

- Most Used Operators
- Analysing Query Results
- Building Multi-Table Statements Using KQL
- Working with String Data Using KQL

Module 09:
Using Microsoft Sentinel

- Understanding the Sentinel dashboard and workspace
- Creating custom queries and alerts in Sentinel
- Analysing and investigating incidents using Sentinel
- Responding to incidents using automated playbooks in Sentinel

Module 10:
Introduction to Collecting Logs with Sentinel

- What is Log Analytics Workspace (LAW)
- How to Collect Logs
- Start Using the Connector • What is Sentinel Workbook

Module 11:
Introduction to Detecting Suspicious Activity with Sentinel

- What are Analytic Rules
- How to Detect Suspicious Activity • Generating an Incident

Module 12:
Introduction to Managing and Investigating Incidents with Sentinel

- What are Incidents • Incident Management Lifecycle • Managing and Investigating Incidents with Sentinel
- • Threat Hunting with Sentinel
- • Start Working with Sentinel- Respond