ZOOM TECHNOLOGIES

CYBEREYE™ The Science of Security BY US-COUNCIL
www.us-council.com

Cybersecurity Associate - SOC Analyst

(Includes Cybersecurity Fundamentals)

The Cybersecurity Associate - SOC Analyst course is designed to provide a comprehensive understanding of the fundamental concepts and practical skills required to start a career in Cybersecurity. This program is ideal for individuals aspiring to become SOC Analyst , equipping them with the knowledge and hands-on experience required to monitor a network in the Security Operations Center and to further pursue Cybersecurity Professional course.

Key Topics:

- IP Addressing, Network Devices, and Packet Analysis
- Operating Systems (Windows, Unix/Linux)
- Troubleshooting network problems
- SOC Operations
- Network Monitoring

Cybersecurity Associate - SOC Analyst

CYBEREYE The Science of Security BY US-COUNCIL

Module 1: Introduction to Cybersecurity

- What is Cybersecurity
- Understanding the Cybersecurity terminology
- Components of Cybersecurity
  - Networking
  - Server administration
  - Security Operations Center

Module 2: Fundamentals of Networking

- Introduction to Networking
- Understanding Networks and Networking
- Types of Networks: LAN, MAN, WAN, and Internet
- Network Topologies: Bus, Ring, Star, and Mesh
- Essential Network Components: NIC Cards, MAC Addresses, Media, and Devices (Hubs, Switches, Routers, Firewalls)
- OSI Reference Model and TCP/IP Model

Module 3: Basics of Operating Systems

- Introduction to Operating Systems
- Overview of Windows, Linux, and Mac OS
- Server vs. Client Operating Systems
- Installation Processes for Windows Server 2022, Windows 11, Ubuntu Server, and Ubuntu Client

Module 4: Fundamentals of Networking

- Understanding LAN Networks
- Setting up a LAN: Components and Functions
- Working with Hubs, Switches: Broadcast Traffic, Flooding, MAC Tables, Unicast

Module 5: Principles of IP Addressing

- Understanding IP Addresses
- Types of IP Addressing: IPv4 and IPv6
- Subnetting Techniques

Module 6: Configuring, Administering, and Managing Windows Server

- Active Directory Setup and Management
- Domain and Workgroup Models
- User and Group Policies
- File and Printer Sharing
- DHCP and DNS Services
- Internet Information System (IIS)

Module 7: Configuring, Administering, and Managing Linux Server

- Linux Operating System Basics
- Linux Filesystem and User Accounts
- File Permissions and Package Management
- Setting up Web and FTP Servers

Module 8: Implementing WAN Connectivity between Multiple Organization Locations

- Introduction to Routers and Their Functions
- Configuring Cisco Routers
- WAN Connectivity and Routing Principles
- Types of Routing: Static, Dynamic, and Default

Module 9: Implementing Internet Connectivity

- Network Address Translation (NAT) and Port Address Translation (PAT)

- Static NAT
- Configuring Organization Routers
- Configuring Home WiFi Routers
- WiFi Security for Home Users

Module 10: System and Network Troubleshooting Techniques

- Troubleshooting System, LAN, and WAN Connectivity Issues

Module 11: Introduction to Cloud Technologies

- Understanding Cloud Computing
- Types of Cloud Technologies: SAAS, PAAS, IAAS
- Overview of Cloud Service Providers: AWS, Azure, GCP
- Creating Cloud Machines on AWS, Azure, and GCP

Module 12: Commonly used Protocols & Ports

- ARP Protocol
- DHCP Protocol
- DNS Protocol
- HTTP Protocol
- FTP Protocol
- SMTP Protocol
- SSH Protocol
- Telnet Protocol

Module 13: Cyber Threats and Incident Response

- Common Cyber Threats
- Host discovery
- Service enumeration
- Vulnerability scanning
- Web application attacks
  - Directory traversal
  - Cross-site scripting
  - SQL Injection
- Password cracking
  - Brute force attack
  - Dictionary attack
  - Phishing attack
- Man-in-the-middle attack
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Malware types
  - Virus
  - Worms
  - Trojans
  - Ransomware
- Incident Response

Module 14: Security Operations Centre (SOC)

- What is SOC
- Roles and responsibilities of SOC
- Tools & Technologies in SOC
  - Firewall
  - IDS
  - IPS
  - Next gen. Firewall
  - UTM
  - SIEM
  - Endpoint Detection and Response (EDR)
- Security Information and Event Management (SIEM)
  - What is SIEM
  - Functions of SIEM
  - SIEM dashboard and alerts

Module 15: Best Practices in Cybersecurity