digital Point IT Consulting Training IT Infrastructure Support Cloud Migration

http://training.digitalpoint.tech

Cyber Security – SOC Analyst

SOC Analyst Market Scope:

Cybersecurity jobs are in high demand. According to the US Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022 that's much faster than the average for all other occupations. Obtaining work in this industry can mean a great income, job security, and advancement potential. There are many business opportunities, including company management positions, available for professional hackers in today's workforce.

The Highest-Paid Cybersecurity Jobs:

- **SOC Analyst:** The Penetration Tester role nets an average salary between $80,000 and $130,000.
- **IS Security Engineer:** This role nets an average salary range of $90,000 to $150,000.

Prerequisites:

- A bachelor's degree in any background (You don't need any IT background)
- You must have good presentation skills

Course Duration (40 Hours)

Class Schedule: SAT & SUN 9:00AM to 2:00PM EST | Tue & Thu 7:00 P.M – 10 P.M EST

Training Methodology:

- Digital point is a global classroom. All classes are featured online (No recorded version). Students around world can join this online live class
- Each class will be recorded, and students will get access to watch video for practice.
- Real-world scenario labs.
- VPN access to digital Point's Lab that is accessible from anywhere 24/7
- Class Notes and Labs for each class

Course Fee: $999

Why choose us?

- Real-world industry experienced instructor
- We help you with Resume preparation, Interview preparation, before and after job support
- Student can repeat the same program two times with no extra cost.

Benefit of the course:

- Completion of this course, you can apply as a Penetration Tester
- Job Support – We will provide you job support
- Interview Preparation
- Mock Interview
- Resume Writing

Course Curriculum

Module 1 Computer Network Fundamentals
Module 2 TCP/IP and OSI Model
Module 3 Networking, Active Directory and DNS
Module 4 Network Security controls and devices
Module 5 Windows OS Security
Module 6 Unix OS Security
Module 7

- **Identifying Security Fundamentals**
  - Identify Information Security Concepts
  - Identify Basic Security Controls
  - Identify Basic Authentication and Authorization Concepts
  - Identify Basic Cryptography Concepts

Module 8

- **Analyzing Risk**
  - Analyze Organizational Risk
  - Analyze the Business Impact of Risk

Module 9

- **Security Management**
  - Identify Social Engineering Attacks
  - Security Operations
  - Security Operations Center (SOC)
  - SOC Capabilities
  - SOC Operations
  - SOC Workflow
  - Components of SOC: People, Process and Technology
  - Types of SOC Models
  - SOC Maturity Models
  - SOC Generations
  - SOC Implementation
  - SOC Key Performance Indicators
  - Challenges in Implementation of SOC
  - Best Practices for Running SOC
  - SOC vs NOC

Module 10

- **Security Logging and Monitoring**
  - Typical Log Sources

- Need of Log
- Logging Requirements
- Typical Log Format
- Logging Approaches
- Local Logging
- Centralized Logging

Module 11

- **Security Information and Event Management (SIEM)**
  - Security Analytics
  - Need of SIEM
  - Typical SIEM Capabilities
  - SIEM Architecture and Its Components
  - SIEM Solutions
  - SIEM Deployment
  - Incident Detection with SIEM
  - Examples of Commonly Used Use Cases Across all SIEM deployments
  - Handling Alert Triaging and Analysis
  - Enhanced Incident Detection with Threat Intelligence

Module 12

- **Incident Response**
  - Incident Response Team (IRT)
  - Where does IRT Fit in the Organisation
  - SOC and IRT Collaboraton
  - Incident Response (IR) Process Overview
  - Step 1: Preparation for Incident Response
  - Step 2: Incident Recording and Assignment
  - Step 3: Incident Triage
  - Step 4: Notification
  - Step 5: Containment
  - Step 6: Evidence Gathering and Forensic Analysis
  - Step 7: Eradication
  - Step 8: Recovery
  - Step 9: Post-Incident Activities
  - Responding to Network Security Incidents
  - Responding to Application Security Incidents
  - Responding to Email Security Incidents
  - Responding to Insider Incidents

- Responding to Malware Incidents

Module 13

- **Network Penetration Test**
  - Plan for Network Penetration Testing
  - External Network Penetration Testing
  - Internal Network Penetration Testing
  - Wireless Network Penetration Testing
  - Footprinting
  - Scanning and Enumeration
  - System Hacking
  - Malware
  - Sniffing
  - Social Engineering
  - Denial of Service
  - Session Hijacking

Module 14

- **Boot Camp – SOC Analyst**
  - Real-World SOC best practices

Module 15 Job Support

- Resume Writing
- Project Analysis
- Interview Preparation
- Mock Interview
- Job Support

Contact Us

Phone: 1-703-652-9640 | 226-972-1877

Web: http://training.digitalpoint.tech Email: admin@digitalpoint.tech