SOC Analyst Intermediate

Course 71577 – 40 Hours

Overview

The Security Operations Center (SOC) lies at the front line of malicious attacks against its network. Those responsible for the initial triage of an incident are the SOC analysts and incident responders. This course covers the necessary skills and practices to train such SOC personnel and successfully operate a modern-day SOC. The training starts from a broad understanding of the various SOC functions and a thorough workout on its technologies, up to a real-time hands-on practice in a virtual simulation environment. This training aims to develop a highly knowledgeable, practical, and skilled security team inside the organization to handle cybersecurity incidents regularly.

The course helps prepare for the certification exams CISM (ISACA) and GSEC (SANS).

On completion, Delegates will be able to

- Provide students with an understanding of the SOC environment, roles, and functionalities
- Gain practical capabilities of working inside a SOC as Tier-1 analysts and incident responders
- Understand the work of forensic investigators in a SOC
- Practice the acquired knowledge in real-time through the simulation environment
- Become familiar with different attack scenarios

Who should attend

The course targets participants with foundation knowledge in computer networking, who wish to operate a SOC on the analyst and incident responder levels, or individuals who serve as corporate security analysts.

- Incident responders
- System/network administrators
- IT security personnel

Course Contents:

Module 1: Windows Domain

Windows Server

- Installing Windows Server
- Configuring Windows Server
- Managing Features
- Windows Events
- Sysmon

Windows Domain

- Installing AD DS
- Configuring AD DS
- Managing Domain Protocols
- Working with Group Policy
- Working with Wireshark

Module 2: SOC Environment

Firewalls

- pfSense Installation
- Configuring FW Rules
- Configuring NAT Rules
- Installing and Managing Packages
- Real-Time Monitoring

IDS/IPS

- Working with Snort
- Snort Rules Structure
- Setting and Configuring Rules
- Passing Traffic using the NAT Feature
- Analyzing Advanced Rules

Module 3: Using the SIEM

ELK

- Monitoring Events
- Different Search Methods
- Custom Queries
- Setting Alerts

Splunk

- Monitoring with Splunk
- SPL Basics
- Splunk Alerts
-

Module 4: Threat Hunting

Log Analysis

- Analyzing Logs
- Advanced Filtering

MITRE ATT&CK

- Hunting via Events
- Creating Hunting Rules

Sysmon

- Configuring XML Settings
- Analyzing Sysmon Events

YARA

- Rules Structure
- Hunting with YARA

Incident Response

- Network Analysis
- IR Playbooks
- Investigating Files