SOC Analyst Advanced

Course 71578 – 40 Hours

Overview

Nowadays, a Security Operation Centers (SOC) should have everything it needs to mount a competent defense of the constantly-changing IT enterprise. The SOC includes a vast array of sophisticated detection and prevention technologies, cyber intelligence reporting, and access to a rapidly expanding workforce of talented IT professionals. This SOC Operation course is designed for SOC organizations to implement a SOC solution and provide full guidance on the necessary skills and procedures to operate it. The training will provide participants with all aspects of a SOC team to keep the enterprise's adversary .

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

On completion, Delegates will be able to

- Provide participants with a solid understanding of the SOC environment, its roles, and functionalities
- Provide the participants the ability to 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

Who should attend

The course targets participants with foundation knowledge in computer networking, who wish to train SOC analysts and incident responders, or individuals who serve as corporate security analysts. Tier-1 SOC analysts and operators.

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

Prerequisites

- Linux
- SOC-Intermediate (Course 71577)

Course Contents:

Module Title	Description
Module 1: Intrusion Detection During this module, participants will further explore data packets' study on a deeper level, learn to identify network anomalies, and understand system alerts. Students will master the use of well-known command-line-interface (CLI) and graphic-user-interface (GUI) tools to further specialize in the field. Students will learn methodologies to approach investigations of incidents.	▪ **Basic Intrusion Detection Tools and Methods** ○ Sysmon ○ Advanced Wireshark ○ Uncovering User-Accounts ○ OS Fingerprinting ○ GeoIP Integration ○ Streams Analysis ○ Incident Investigation ○ Hashing Tables ○ Analyzing Cyber-Events ○ Web-Filtering ○ Network Events ○ TShark: Wireshark CLI Tool ▪ **Using Scapy Module** ○ Crafting and Analysing Packets ○ Working with PCAP Files ○ Replaying Packets for Investigating
Module 2: Using the SIEM This module will drill down to SIEM (Security Information and Event Management), the primary system used by SOC analysts for monitoring the network. Participants will install a freely-available open-source SIEM platform and simulate different scenarios through a pre-prepared virtual environment, mimicking an organization. The virtual environment will include: Firewall, WAF, a Domain Controller, and an Antivirus. Students will have to demonstrate the various practical capabilities they acquired during the course and operate in a real-time environment during this part.	▪ **Building SIEM Environment** ○ Installing AlienVault ○ Setting-up an Open Source SIEM ○ Deploying Security-Onion ○ Setting your Methodology to Cyber Threats ○ Network and Host DLP Monitoring and Logging ▪ **Monitoring using the Virtual Environment** ○ Firewall Monitoring and Management using Glasswire ○ Centralized Logging Platforms ○ Email and Spam Gateway and Web Gateway Filtering ○ Threat Monitoring and Intelligence ○ Application Whitelisting or File Integrity Monitoring ○ Vulnerability Assessment and Monitoring ○ Setting your Methodology to Cyber Threats
Module 3: Windows Management Instrumentation (WMI) This module will explain and expand on the use of Windows Management Instrumentation. Students will learn how the core management process is accomplished and use WMI to manage both local	▪ **WMI Architecture** ○ WMI Classes and Namespaces ○ Using WMI Methods ○ Associations ○ Working with Remote Computers ○ Access to the Registry

and remote computers on the LAN network to consolidate the acquired knowledge into building tools skills in PowerShell scripts and regular WMI usage.	○ Information Gathering ○ Storage Information ○ Command Execution ○ WMI Common Events ○ Detection with WMI
Module 4: SOC and IR This module will teach the student to manage an enterprise security incident while avoiding common errors, increasing both the effectiveness and efficiency of your incident response efforts.	▪ **Tools and Techniques for Digital Investigations** ○ Data Analysis of data formats analysis for investigative purposes ○ Behavior Analysis ○ Review of Data Collection Techniques ○ IR Essentials ○ Base Policy and Common Detection ○ Fingerprinting New Systems ○ Intro to Threat Hunting