Syllabus

SOC Analyst

CYBERIUM ARENA

-SIMULATOR-

Description

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).

Target Audience

The course targets participants with foundation knowledge in computer networking.

Pre-requisites

Linux

Objectives

- 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
- Practice the acquired knowledge in real-time through the simulation environment

Module 1: Intrusion Detection

During this module, participants will further explore data packets' and 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.

Networking

- Network Protocols
- The OSI Model
- Analyzing Packets

Basic Intrusion Detection Tools and Methods

- Wireshark
- GeolP Integration
- TShark
- Sysmon

Using the Scapy Module

- Crafting and Analysing Packets
- Working with PCAP Files
- Replaying Packets for Investigating

Module 2: Setting Up the SOC Environment

Companies regularly deploy various security technologies designed to prevent and detect threats and strengthen and protect assets. During this module, we will detail SOC environments and how they work. The student will know to build and properly configure his SOC environment and correlate it with other security products/assets. Having a SOC allows you to have dynamic security that acts as a real bastion of analysis, monitoring, prevention, and remediation.

Preparing the Framework

- Introduction to ELK
- Deploying Beats
- Identifying Threats
- Aggregating Data
- Real-Time Monitoring

Hands-on PfSense

- Setting and Configuring Rules
- Passing Traffic using the NAT Feature
- Configuring Firewall Rules
- Managing Network Security
- Snort

Module 3: Using the SIEM

Learning about the 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.

Building SIEM Environment

- Configuring Your Domain
- Setting-Up an Open Source
- SIEM Deploying Security-Onion
- Network and Host OLP Monitoring and Logging

Monitoring using the Virtual Environment

- Firewall Monitoring and Management
- Email and Spam Gateway and Web Gateway Filtering
- Vulnerability Assessment and Monitoring
- Setting your Rules for Cyber Threats

Module 4: Windows Management Instrumentation (WMI)

In this module, students will learn to use the Windows Management Instrumentation. Students will learn how the core management process is accomplished and use WMI to manage both local and remote computers on the LAN network to consolidate the acquired knowledge into building tools skills in PowerShell scripts and regular WMI usage.

WMI Architecture

- Using WMI Methods
- Working with Remote Computers
- Access to the Registry
- Information Gathering
- Storage Information
- Command Execution
- Common Events
- Detection with WMI