HackerU
Experience Makes Experts

SOC Operation and Incident Response

Index: CS003

40
Hours

SOC Operation & Incident Response

Description

The Security Operations Center (SOC) lies at the front line of malicious attacks against the organization's 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. Starting from a broad understanding of the various functions in a SOC, and a thorough workout on its technologies, up to a real-time hands-on practice in a virtual simulation environment. The ultimate goal of this training is to develop a highly knowledgeable, practical and skilled security team inside the organization to handle cyber security incidents on a regular basis.

Target Audience

The course targets participants with a 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. Primarily:

- Tier-1 SOC analysts and operators
- Incident responders
- System/network administrators
- IT security personnel
- IT personnel migrating to IT security

Prerequisites

- Good knowledge of computer networking.
- CS002 provides a solid foundation of preliminary knowledge required for this course.

Technical Set-Up Information

- The course will use an open-source SIEM technology and utilize a virtual environment of a common organization to demonstrate the processes of a real SOC. In order to use and practice on the simulation environment, students require to install a virtualization platform on their PCs.
- For training on a specific SOC vendor that is available at your organization, some adaptations may be in place. Please refer to our sales consultants.

Objectives

- Provide studetns with a solid understanding of the SOC environment, its roles and functionalities.
- Gain practical capabilities of working inside a SOC as Tier-1 analysts and incident responders.
- Understanding the work of forensic investigators in a SOC, in order to ensure the tier-1 team properly supports the forensic procedures.
- Practicing the acquired knowledge in real-time through the simulation environment.
- Becoming familiar with differet attack scenarios affecting the system, recognizing the attacks as they happen & following with the right course of action to handle the incident.
- Mastering the proper documentation and reporting procedures for all activities inside the SOC.
- Preparing participants to function as security analysts and first responders, by knowing how to operate the different technologies in the SOC, and understanding the meaning of different artifcats.

Course Outline

01

Networking Fundamentals

4 Hours

The first module will introduce participants to the technical environment of a security-operations-center and deepen their understanding of network processes, protocols, firewalls, IDS/IPS and more. Finally, they will become familiar with the various stages of the investigation process, which they will practice and implement at a later stage of the course.

- Network protocols
  - Sniffing the network
  - Eliminating protocols
  - Analyzing protocols
  - "Studying" the network and its assets
- Firewall
  - Rules-based
  - Next generation
- Intrusion Detection System (IDS)
  - Network-based
  - Host-based
  - Exercise: configuring Snort and detecting attacks
- Intrusion Prevention System (IPS)
  - Network-based
  - Host-based
- The digital investigation process
  - Acquisition
  - Identification
  - Evaluation
  - Admittion

02

Monitoring the Systems

8 Hours

During this module, participants will gain a clear view of what is happening on the network and the PCs connected to it, and explore different types of attacks from inside the network and outside it. They will also understand the differentiation between an event and an incident. By the end of this module, students will be able to determine whether a computer on the network was compromised in real time.

- Attack scenarios
  - Attacks from inside the network
  - Attacks from outside the network
- Events vs. Incidents
  - Unsuccessful activity attempt (event)
  - Non-compliant activity (event)
  - Reconnaissance (event)
  - Investigating (event)
  - Explained anomaly (event)
  - Root Level intrusion (incident)
  - User Level intrusion (incident)
  - Denial-of-service (incident)
  - Malicious logic (incident)

03

Incident Response and Forensics

8 Hours

The primary role of incident response is to analyze the system after an attack to understand the changes or damages it suffered; forensics is an integral part of this process. This module will provide participants with some of the basics of cyber forensics, to give them a more comprehensive understanding of all the processes in a SOC, and insure proper correlation between the different roles in the SOC.

- Windows forensics
  - Collecting data
    - Dumping the memory
    - HDD
    - Logs
  - Creating a timeline
  - File recovery
  - Understanding the registry
  - Suspicious files
- Linux forensics
  - Live response
  - Analyzing file systems
  - Memory forensics
  - Volatility
- Identifying compromised hosts
  - Rapid data analysis
  - Cyber threat intelligence
  - Searching for indicators of compromise
  - Evidence of persistence
  - Packing/entropy/executableanomaly/density checks
  - System logs
  - Memory analysis
  - Malware identification

04

Setting Up the SOC Environment: Processes and Procedures

8 Hours

During this module participants will learn about the different roles and functions that make up the SOC environment, and more importantly, will experience the various processes that are regularly running in a SOC. This knowledge will help the SOC staff be better

correlated between themselves to ensure the correct flow of procedures. By the end of this module, participants will know to handle an incident from A to Z.

- SOC roles & responsibilities
- Preparing the framework
- Incident response tactics
- Awareness and communication
- Real-time monitoring
  - Aggregating logs
  - Aggregating data
  - Coordinating response and remediation
- Reporting methodology
- Post-incident analysis

05

Using the SIEM

8 Hours

This module will drill down to the nuts and bolts of operating the SIEM (Security Information and Event Management), the main 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-pre-pared virtual environment, mimicking an organization. The virtual environment will include: Firewall, WAF, a domain controller (Windows Server) and an anti-virus. During this part, students will have to demonstrate the various practical capabilities they acquired during the course and operate in a real-time environment. (Note: the simulation environment will naturally focus on attacks outside the organization).

- Setting-up an open source SIEM
  - Connecting devices to the SIEM
  - Running and configuring your SIEM
  - Upgrading your log filtering with bro
  - Setting your own methodology to cyber threats
- Monitoring using the virtual environment
  - SIEM monitoring and correlation
  - Antivirus monitoring and logging
  - Network and host IDS/IPS monitoring and logging
  - Network and host DLP monitoring and logging
  - Centralized logging platforms
  - Email and spam gateway and filtering
  - Web gateway and filtering
  - Threat monitoring and intelligence
  - Firewall monitoring and management
  - Application whitelisting or file integrity monitoring
  - Vulnerability assessment and monitoring
  - Notifications (email, mobile, home, chat, etc.)

06

Final Exercise

4 Hours

To wrap up the different capabilities and knowledge students gained during the training, they will be tasked with a final exercise to test their performance in real time. As the first step, participants will install the “organization virtual environment” on their virtualization platform. Then, the instructor will send out different attacks on the system, and students will be required to handle them, following all the necessary stages. By the end, they will file a detailed report of the incident, as a final assessment of the practical implementation of their knowledge.