CYBERIUM ARENA

Description

This SOC Operation module is designed for SOC organizations to implement a SOC solution and provide full guidance on the necessary skills and procedures to operate it. The program provides participants with all aspects of a SOC team to keep the enterprise's adversary.

SOC ANALYST

Module 1: Windows Domain

This focused module centers on Sysmon, a powerful Windows system monitoring tool. It teaches learners how to use Sysmon for comprehensive event logging, contributing to a deeper understanding of Windows domain operations.

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

This module includes the Firewalls configuration and management using pfSense, including the creation of firewall and NAT rules. It involves real-time system monitoring and explores Intrusion Detection and Prevention Systems (IDS/IPS). Participants gain hands-on experience with Snort, understanding rule structures, configuration, and advanced traffic analysis using the NAT feature.

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

This module guides participants through the essential components of Security Information and Event Management (SIEM). It initiates with the exploration of ELK stack, covering event monitoring, search methods, custom queries, and alert settings. The latter part delves into Splunk, teaching how to monitor events, the fundamentals of Search Processing Language (SPL).

ELK
Monitoring Events
Different Search Methods
Custom Queries
Setting Alerts
Splunk
Monitoring with Splunk
Splunk Alerts

Module 4: Threat Hunting

This module immerses participants into advanced aspects of cybersecurity. It begins with comprehensive log analysis, incorporating advanced filtering and threat hunting via events and MITRE ATT&CK. Participants work with Sysmon and its configuration, followed by exploring YARA for rule creation and 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
IR Playbooks
Investigating Files

NX Defense | LEVEL: 3 | DURATION: 10-12 weeks (self-paced) / 40h (trainer-led)