CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

SOC ANALYST

MAIN FEATURES

Labs

The labs hold questions and tasks to support the training.

Book

The coursebooks accompany the lecturers and students alike in cybersecurity studies.

Scenarios

Provide participants possible situations from cybersecurity or cyberterrorism to solve.

Project

Trainees must complete a practical built-in project, produce defense and assault tools.

CYBERIUM ARENA

— SIMULATOR —

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.

MODULES

Module 1: Windows Domain

Windows Server
Installing Windows Server
Configuring Windows Server
Managing Features
Windows Events
Events with PowerShell
Windows Domain
Subnetting
Installing AD DS
Configuring AD DS
Managing Domain Protocols
Working with Group Policy
Working with Wireshark

Module 2: SOC Environment

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

Module 3: Using the SIEM

Monitoring using the Virtual Environment
Firewall Monitoring and Management
Installing Firewall Packages
Web Gateway Filtering
Vulnerability Assessment and Monitoring
Setting your Rules for Cyber Threats

Module 4: Threat Hunting

Hunting in the Domain
Hardening Your Domain
Setting-Up an Open Source SIEM
Deploying OSSIM
Network and Host Monitoring and Logging