Cyber Training Arena

TRAINING MODULES FOR ENTRY LEVEL

Advanced SOC Specialist

In modern organizations SOC operation becomes increasingly complex, requiring advanced integration of diverse systems. Today's SOC analysts need both to handle the modern SIEM (Security Information & Management) systems, and have broad vision and capabilities in the general field of cyber-security. CYBERGYM's "Zero to Hero for SOC Analyst" program allows organization's high-quality personnel without prior cyber-related background, to gradually develop the knowledge, understanding and practical experience required to become a SOC analyst - learning, understanding and trying various tools, concepts and methods in the field.

Target Audience

- IT Personnel
- Technical personnel in the fields of computing and/or networking
- Graduate of the "Cyber Guardian" training program OR
- IT personnel with good understanding of systems architecture, interoperability and interfaces development concepts
- Programmers and/or sysadmins with knowledge in scripting, interfaces development and data parsing
- Beginner SOC analyst
- IT personnel re-qualifying as SOC analysts

Expected Outcomes

- Undergo high-intensity hands-on experience, executing actual APT scenarios in the Cyber warfare Arena environment.
- Acquire the experience, knowledge and skills required for advanced SIEM/SOC management and operation
- Get familiar with the advanced tools, skills and work methods utilized by modern SIEM systems operators
- Acquire the fundamental experience, knowledge and skills required for SIEM/SOC management and operation
- Get familiar with the advanced capabilities of a modern SIEM systems

Reverse Analysis - Level 1 [Phishing Mail]

Objectives

The trainees will analyze, detect and offer action to restore the system back to action mode

Target Audience

- Tier 1 Security Analyst
- Tier 2+3 Security Analyst
- IT/OT Professional
- CISO - Chief Information Security Officer
- SOC Analyst

Mandatory Prerequisites

- IT background
- IR advanced Tactics training
- IR principal Tactics training

Expected Outcomes

Ability to analyze a hacked system and restore it back