€TRAINING

Continuous Monitoring And Security Operations

Continuous Monitoring And Security Operations

Introduction

Continuous Monitoring and Security Operations will teach you how to strengthen your skills to undertake that proactive approach. Security monitoring is the automated process of collecting and analyzing indicators of potential security threats, then triaging these threats with the appropriate action.

Course Objectives

At the end of this course the participants will be able to:

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Centers SOC
- Identify the key components of Network Security Monitoring NSM/Continuous Diagnostics and Mitigation CDM/Continuous Monitoring CM
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring
- Determine requisite monitoring capabilities for a SOC environment

Targeted Audience

- IT professionals
- Security professionals
- Auditors
- Site administrators
- General management
- Anyone tasked with managing and protecting the integrity of the network infrastructure
- Anyone already familiar and involved with IT/cyber/digital security and seeking to build on their fundamental principles of security.

Course Outline

Unit 1: Current State Assessment, Security Operations Centers, and Security Architecture

- Perimeter-focused
- Addressed Layer 3/4
- Detection-oriented
- Post-Exploitation-focused
- Decentralized Information Systems/Data
- Risk-informed
- Layer 7 Aware
- Security Operations Centers

Unit 2: SOCs and Defensible Network Security Architecture

- Web Application Firewall
- Malware Detonation Devices
- HTTP Proxies, Web Content Filtering, and SSL/TLS Decryption
- Internal Segmentation
- Threat Vector Analysis
- Data Exfiltration Analysis

Unit 3: Network Security Monitoring

- Evolution of NSM
- The NSM Toolbox
- NIDS Design
- Cloud NSM
- Practical NSM Issues
- Cornerstone NSM

Unit 4: SOCs and Defensible Endpoint Security Architecture

- Endpoint Protection Platforms
- Endpoint Detection Response
- Authentication Protection/Detection
- TPM: Device Health Attestation
- Host-based Firewall, Host-based IDS/IPS
- Application Control, Application Virtualization
- Virtualization Based Security

Unit 5: Automation and Continuous Security Monitoring

- Continuous Security Monitoring CSM vs. Continuous Diagnostics and Mitigation CDM vs. Information Security Continuous Monitoring ISCM
- Cyberscope and SCAP
- Maintaining Situational Awareness
- Host, Port, and Service Discovery
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Applications