DEF 111:
Security Architecture, Analysis, and Operations

A 30-Hour Training Course

Description

This course is designed for cybersecurity professionals looking to become competent security analysts or SOC engineers. Cyber defense is switching from preventive to detective, and this means security analysts need to be proactive threat hunters. As a participant, you will learn in-depth Security Architecture for both networks and endpoints; this will cover not only the technologies, solutions, and devices, but also the principles, techniques, and methods. In addition, you will learn how to implement Network Security Monitoring (NSM) and Continuous Security Monitoring (CSM). Those are applied frameworks comprising tools and methodologies that no security analysis is effective without them.

You will gain hands-on experience using Security Onion Linux distribution, particularly on tools like Sguil (a collection of free software components for Network Security Monitoring), Snort (and open-source IDS), Wireshark (an open-source packet capture and analysis tool), OSSIM (an open-source Security Information & Event Management), Suricata (an open-source IDS/IPS) and others. Finally, we will cover the architecture and components of the Security Operations Center (SOC), and how incident response can be automated using Security Orchestration, Automation, and Response (SOAR) technology.

Audience

- SOC Analysts
- Security Engineers
- Blue-Team Professionals

Prerequisites

- Basic knowledge in Cybersecurity [*Course CYB101*]
- Good knowledge in Networking
- Good knowledge in Operating Systems

Outline

MODULE 01: THE EVOLUTION OF CYBER-ATTACKS

- From Hobbyist to Professional Attackers
- From Server-Side to Client-Side Exploitation
- From Network to Web Application Attacks
- From Botnets to Advanced Post-Exploitation
- The Introduction of Layer 8 – Social Engineering

MODULE 02: THE EVOLUTION OF CYBER DEFENSE

- From Prevention to Detection
- From Perimeter to Post-Exploitation
- From Centralized to Decentralized Systems
- From Layer 3-4 to Layer 7
- Security Operations Center (SOC)

MODULE 03: TECHNOLOGIES FOR NETWORK SECURITY ARCHITECTURE

- Traditional and Next Generation Firewall
- Network Intrusion Detection/Prevention Systems
- Web Application Firewall
- Forward Proxies
- Deception Technology
- Security Information and Event Management
- Malware Sandboxing Technology

MODULE 04: PRINCIPLES OF NETWORK SECURITY ARCHITECTURE

- Internal Segmentation
- Network Traffic Analysis
- Detection-Oriented Design
- Defense in Depth
- Visibility and Data Visualization
- Intrusion Kill Chain
- Zero-Trust Network Design

MODULE 05: NETWORK SECURITY MONITORING

- Benefits and Values of NSM
- The Tools Needed for NSM
- The NSM Cycle: Collection, Detection, and Analysis
- The Applied Collection Framework (ACF)
- Installation and Deployment of NSM Tools
- Maximum Visibility with Data Sources
- Types and Mechanisms of Detection

MODULE 06: NSM: SECURITY ANALYSIS CASE STUDIES

- Service-Side and Client-Side Exploits
- Identifying High-Entropy Strings
- Tracking EXE Transfers
- Identifying Command and Control (C2) Traffic
- Tracking User Agents
- C2 via HTTPS
- Tracking Encryption Certificates

MODULE 07: TECHNOLOGIES FOR ENDPOINT SECURITY ARCHITECTURE

- Anti-Malware
- Endpoint Protection Platform (EPP)
- Endpoint Detection and Response (EDR)
- Host-based Firewall
- Host-Based IDS/IPS
- Physical and BIOS/MBR Security

MODULE 08: PRINCIPLES FOR ENDPOINT SECURITY ARCHITECTURE

- Authentication, Authorization, and Accounting
- Privileges and User Access Control (UAC)
- Whole-Disk Encryption
- Browser Security
- EMET
- Patching Process

MODULE 09: CONTINUOUS SECURITY MONITORING (CSM)

- Best Practices in CSM
- Network Mapping
- Vulnerability Scanning
- Patch Management
- Monitoring Applications
- Monitoring Service Logs
- Monitoring Changes

MODULE 10: SECURITY OPERATIONS CENTER (SOC)

- People, Processes, and Technologies
- Threat Detection
- Incident Response
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)