SEC511.1: Current State Assessment, Security Operations Centers, and Security Architecture

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

- Overview
  - Traditional Security Architecture
  - Perimeter-focused
  - Addressed Layer 3/4
  - Centralized Information Systems
  - Prevention-Oriented
  - Device-driven
  - Traditional Attack Techniques
- Modern Security Architecture Principles
  - Detection-oriented
  - Post-Exploitation-focused
  - Decentralized Information Systems/Data
  - Risk-informed
  - Layer 7 Aware
  - Security Operations Centers
  - Network Security Monitoring
  - Continuous Security Monitoring
  - Modern Attack Techniques
  - Adversarial Dominance
- Frameworks and Enterprise Security Architecture
  - Enterprise Security Architecture
  - Security Frameworks
- Security Architecture - Key Techniques/Practices
  - Threat Vector Analysis
  - Data Exfiltration Analysis
  - Detection Dominant Design
  - Zero Trust Model (Kindervag)
  - Intrusion Kill Chain
  - Visibility Analysis
  - Data Visualization
  - Lateral Movement Analysis
  - Data Ingress/Egress Mapping
  - Internal Segmentation
  - Network Security Monitoring
  - Continuous Security Monitoring
- Security Operations Center (SOC)
  - Purpose of a SOC
  - Key SOC roles
  - Relationship to Defensible Security Architecture

SEC511.2: Network Security Architecture

Day 2: SOCs and Defensible Network Security Architecture

- SOCs/Security Architecture - Key Infrastructure Devices
    - Traditional and Next Generation Firewalls, and NIPS
    - Web Application Firewall
    - Malware Detonation Devices
    - HTTP Proxies, Web Content Filtering, and SSL Decryption
    - SIMs, NIDS, Packet Captures, and DLP
    - Honeypots/Honeynets
    - Network Infrastructure - Routers, Switches, DHCP, DNS
    - Mobile Devices and Wireless Access Points
    - Threat Intelligence
- Segmented Internal Networks
    - Routers
    - Internal SI Firewalls
    - VLANs
    - Detecting the Pivot
- Defensible Network Security Architecture Principles Applied
    - Internal Segmentation
    - Threat Vector Analysis
    - Data Exfiltration Analysis
    - Detection Dominant Design
    - Zero Trust Model (Kindervag)
    - Intrusion Kill Chain
    - Visibility Analysis
    - Data Visualization
    - Lateral Movement Analysis
    - Data Ingress/Egress Mapping

SEC511.3: Network Security Monitoring

Day 3: Network Security Monitoring

- Continuous Monitoring Overview
    - Defined
    - Network Security Monitoring (NSM)
    - Continuous Security Monitoring (CSM)
    - Continuous Monitoring and the 20 Critical Security Controls
- Network Security Monitoring (NSM)
    - Evolution of NSM
    - The NSM Toolbox
    - NIDS Design
    - Analysis Methodology
    - Understanding Data Sources
        - Full Packet Capture

        - Extracted Data
        - String Data
        - Flow Data
        - Transaction Data
        - Statistical Data
        - Alert Data
        - Tagged Data
        - Correlated Data
    - Practical NSM Issues
    - Cornerstone NSM
        - 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

SEC511.4: Endpoint Security Architecture

Day 4: SOCs and Defensible Endpoint Security Architecture

- Security Architecture - Endpoint Protection
    - Anti-Malware
    - Host-based Firewall, Host-based IDS/IPS
    - Application Whitelisting, Application Virtualization
    - Privileged Accounts, Authentication, Monitoring, and UAC
    - Whole Disk Encryption
    - Virtual Desktop Infrastructure
    - Browser Security
    - EMET
- Dangerous Endpoint Applications
    - Java
    - Adobe Reader
    - Flash
    - Microsoft Office
    - Browsers
- Patching
    - Process
    - To Test or Not to Test
    - Microsoft
    - Third Party

SEC511.5: Automation and Continuous Security Monitoring

Day 5: Automation and Continuous Security Monitoring

- Overview
    - Continuous Security Monitoring (CSM) vs. Continuous Diagnostics and Mitigation (CDM) vs. Information Security Continuous Monitoring (ISCM)
    - Cyberscope and SCAP
- Industry Best Practices
    - Continuous Monitoring and the 20 Critical Security Controls
    - Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions
- Winning CSM Techniques
- Maintaining Situational Awareness
- Host, Port, and Service Discovery
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Applications
- Monitoring Service Logs
    - Detecting Malware via DNS logs
- Monitoring Change to Devices and Appliances
- Leveraging Proxy and Firewall Data
- Configuring Centralized Windows Event Log Collection
- Monitoring Critical Windows Events
    - Hands on: Detecting Malware via Windows Event Logs
- Scripting and Automation
    - Importance of Automation
    - PowerShell
    - Hands-on: Detecting Malicious Registry Run Keys with PowerShell

SEC511.6: Capstone: Design, Detect, Defend

Day 6: Capstone - Design/Detect/Defend

- Security Architecture
- Assess Provided Architecture
- Continuous Security Monitoring
- Using Tools/Scripts to Assess the Initial State
- Quickly/Thoroughly Find All Changes Made