Continuous Monitoring and Security Operations

Length: 6 Days

Course Objectives:

- Analyze modern hybrid enterprises for deficient protection/detection strategies
- Apply the principles learned in the course to design a defensible cloud, network, and endpoint security architecture and operations
- Understand the importance of detection-dominant security architecture and Security Operations Centers (SOC) for hybrid enterprises
- Identify the key components of cloud, network, and endpoint protection and monitoring across hybrid infrastructure
- Determine appropriate security monitoring needs for organizations of all sizes

COURSE CONTENT

Current State Assessment and Security Architecture

Exercises

- Detecting Traditional Attack Techniques with Security Onion and CyberChef
- Detecting Modern Attack Techniques with Security Onion
- Egress Analysis with Elastic Stack
- NetWars (Day 1): Immersive Cyber Challenges

Topics

- Traditional Security Architecture
  - Perimeter-focused
  - Addressed Layer 3/4
  - Centralized Information Systems
  - Prevention-Oriented
  - Device-driven
  - Traditional Attack Techniques
- Introducing Security Onion 2.X
  - Alerts Menu
  - Pivoting to the Hunt Menu
  - The PCAP Menu
- 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
  - MITRE ATTACK(R)
- Security Architecture - Key Techniques/Practices
  - Threat Vector Analysis
  - Data Exfiltration Analysis
  - Detection Dominant Design
  - Intrusion Kill Chain
  - Visibility Analysis
  - Lateral Movement Analysis
  - Data Ingress/Egress Mapping
  - Internal Segmentation
  - Network Security Monitoring
  - Continuous Security Monitoring

- Cloud Deployment Models
  - Cloud Shared Responsibilities
  - Infrastructure as Code (IaC)
  - Overexposed Cloud Services: Leaky Buckets
  - Cloud Network Visibility
- MITRE ATT&CK(R) & AWS Security Stack
  - AWS Security Hub
  - AWS Identity and Access Management (IAM)
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Firewall Manager
  - AWS WAF + AWS Shield
  - Amazon Virtual Private Cloud (VPC)
  - Amazon GuardDuty
  - Amazon Inspector
  - Amazon Macie

Network Security Architecture

Exercises

- ModSecurity
- Decrypting TLS with Wireshark
- Detecting Adversaries with Protocol Inspection
- HoneyTokens for Leak Detection
- NetWars (Day 2): Immersive Cyber Challenges

Topics

- 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/TLS Decryption
  - SIEMs, NIDS, Packet Captures, and DLP
  - Honeypots/Honeynets
  - Network Infrastructure - Routers, Switches, DHCP, DNS
  - Threat Intelligence
- Segmented Internal Networks
  - Routers
  - Internal SI Firewalls
  - VLANs
  - Detecting the Pivot
  - DNS architecture
  - Encrypted DNS including DNS over HTTPS (DoH) and DNS over TLS (DoT)
- Defensible Network Security Architecture Principles Applied
  - Internal Segmentation
  - Threat Vector Analysis
  - Data Exfiltration Analysis
  - Detection Dominant Design
  - Zero Trust Architecture (Kindervag)
  - Intrusion Kill Chain
  - Visibility Analysis
  - Data Visualization
  - Lateral Movement Analysis
  - Data Ingress/Egress Mapping

Network Security Monitoring

Exercises

- Pcap Carving with Zeek
- Security Onion Service-Side Attack Analysis
- Wireshark Merlin Analysis
- Detecting TLS Certificate and User-Agent Anomalies
- NetWars (Day 3): Immersive Cyber Challenges Labs

Topics

- 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
- Cloud NSM
- 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
- Detecting Malware via JA3

- Detecting Cobalt Strike
  - Criminal Usage of Cobalt Strike
  - Malleable C2
  - Cobalt Strikes x.509 Certificates

Endpoint Security Architecture

Exercises

- Sysmon
- Autoruns
- Application Control with AppLocker
- Merlin Sysmon Analysis
- NetWars Day 4: Immersive Cyber Challenges

Topics

- Endpoint Security Architecture
  - Endpoint Protection Platforms
  - Endpoint Detection Response
  - Authentication Protection/Detection
  - Configuration Management/Monitoring
- Endpoint Protection
  - TPM: Device Health Attestation
  - Host-based Firewall, Host-based IDS/IPS
  - Application Control, Application Virtualization
  - Virtualization Based Security
  - Microsoft Defender: Application Guard
  - Windows Defender: Credential Guard
  - Defender for Endpoint: Attack Surface Reduction
  - EMET and Defender Exploit Guard
- Cloud Configuration Management
- Endpoint Detection - Sysmon
  - FileDelete, ProcessTampering, and other recent additions
  - IMPHASH
  - DeepBlueHash
- Authentication Protection and Detection
  - Privileged Account Monitoring
  - Windows Hello
  - Dynamic Lock
  - PIN-Only Authentication
  - Passwordless
  - Azure Active Directory + MFA
  - Azure Authentication Methods
  - AAD Conditional Access
  - Hash/Ticket/Token Attacks
- Configuration Management/Monitoring
  - Cloud: Center for Internet Security (CIS) Hardened Images
  - Containers: CIS Hardened Images for Containers
  - Baseline Monitoring
  - Desired State Configuration (DSC)
  - Azure Automation State Configuration

Automation and Continuous Security Monitoring

Exercises

- Inventory
- Windows Event Logs
- DNS over HTTPS (DoH)
- Kansa Persistence and Pivoting
- NetWars (Day 5): Immersive Cyber Challenges

Topics

- 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 CIS Critical Security Controls
  - Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions
- Winning CSM Techniques
  - Long Tail Analysis
  - Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents
  - The ASD Essential Eight

- Maintaining Situational Awareness
- Host, Port, and Service Discovery
- Vulnerability Scanning
- Monitoring Patching
- Monitoring Applications
- Monitoring Service Logs
  - Detecting Malware via DNS logs
  - Detecting DNS Tunneling via Iodine and dnscat2
  - Domain_stats and Registration Data Access Protocol (RDAP)
- 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
  - DeepBlueCLI
- Security Operations Center (SOC)
  - Purpose of a SOC
  - Key SOC roles
  - Relationship to Defensible Security Architecture

Capstone: Design, Detect, Defend

Topics

- Security Architecture
- Continuous Security Monitoring
- Applied NSM and CSM
- Analyzing Malicious Traffic with Security Onion, Wireshark, and CyberChef
- Analzying Malicious Windows Event Logs
- Packet Analysis
- Log Analysis
- C2 Detection