Blue Team or Cyber Defense Package (Level2) Syllabus

Package Duration : 120 H

SEC511,SEC530,SEC555

SEC511: Continuous Monitoring and Security Operations

SEC511.1 : Current State Assessment , Security Operations Center ,and Security

- 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
  - 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

- 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
    - Mobile Devices and Wireless Access Points
    - 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 Model (Kindervag)
    - Intrusion Kill Chain
    - Visibility Analysis
    - Data Visualization
    - Lateral Movement Analysis
    - Data Ingress/Egress Mapping

SEC511.3 : 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
    - 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

SEC511.4 : Endpoint Security Architecture

- Security Architecture - Endpoint Protection
    - Anti-Malware
    - Host-based Firewall, Host-based IDS/IPS
    - Application Control, Application Virtualization
    - Privileged Accounts, Authentication, Monitoring, and UAC
    - Virtual Desktop Infrastructure
    - Browser Security
    - EMET and Defender Exploit Guard
- Patching
    - Process
    - To Test or Not to Test
    - Microsoft
    - Third-Party

SEC511.5 : 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 CIS 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
    - DeepBlueCLI
    - Hands-on: Detecting Malicious Registry Run Keys with PowerShell

SEC530: Defensible Security Architecture and Engineering

SEC530.1 : Defensible Security Architecture and Engineering

- Traditional Security Architecture Deficiencies
    - Emphasis on Perimeter/Exploitation
    - Lack of a True Perimeter ("De-perimeterization" as a Result of Cloud/Mobile)
    - The Internet of Things
    - Predominantly Network-centric
- Defensible Security Architecture
    - Mindset
        - Presumption of Compromise
        - De-perimeterization
        - Predominantly Network-centric
    - Models
        - Zero-Trust Model (Kindervag - Forrester)
        - Intrusion Kill Chain
        - Diamond Model of Intrusion Analysis

    - Software-defined Networking and Virtual Networking
    - Micro-Segmentation
- Threat, Vulnerability, and Data Flow Analysis
    - Threat Vector Analysis
        - Data Ingress Mapping
    - Data Exfiltration Analysis
        - Data Egress Mapping
    - Detection Dominant Design
    - Attack Surface Analysis
    - Visibility Analysis
- Layer 1 Best Practices
    - Network Closets
    - Penetration Testing Dropboxes
    - USB Keyboard Attacks (Rubber Ducky)
- Layer 2 Best Practices
    - VLANs
        - Hardening
        - Private VLANs
    - Layer 2 Attacks and Mitigation
- NetFlow
    - Layer 2 and 3 NetFlow
    - NetFlow, Sflow, Jflow, VPC Flow, Suricata and Endpoint Flow

SEC530.2 : Network Security Architecture and Engineering

- Layer 3: Router Best Practices
    - CIDR and Subnetting
- Layer 3 Attacks and Mitigation
    - IP Source Routing
    - ICMP Attacks
    - Unauthorized Routing Updates
    - Securing Routing Protocols
    - Unauthorized Tunneling (Wormhole Attack)
- Layer 2 and 3 Benchmarks and Auditing Tools
    - Baselines
        - CISecurity
        - Cisco's Best Practices
        - Cisco Autosecure
        - DISA STIGs
        - Nipper-ng
    - Securing SNMP
        - SNMP Community String Guessing
        - Downloading the Cisco IOS Config via SNMP
        - Hardening SNMP
        - SNMPv3
    - Securing NTP

        - NTP Authentication
        - NTP Amplification Attacks
    - Bogon Filtering, Blackholes, and Darknets
        - Bogon Filtering
        - Monitoring Darknet Traffic
        - Building an IP Blackhole Packet Vacuum
    - IPv6
        - Dual-Stack Systems and Happy Eyeballs
        - IPv6 Extension Headers
        - IPv6 Addressing and Address Assignment
    - Securing IPv6
        - IPv6 Firewall Support
        - Scanning IPv6
        - IPv6 Tunneling
        - IPv6 Router Advertisement Attacks and Mitigation
    - VPN
        - Path MTU Issues
        - Fragmentation Issues Commonly Caused by VPN
    - Layer 3/4 Stateful Firewalls
        - Router ACLs
        - Linux and BSD Firewalls
        - pfSense
        - Stateful
    - Proxy
        - Web Proxy
        - SMTP Proxy
            - Augmenting with Phishing Protection and Detection Mechanisms
        - Explicit vs. Transparent
        - Forward vs. Reverse

SEC530.3 : Network-Centric Security

- NGFW
    - Application Filtering
    - Implementation Strategies
- NIDS/NIPS
    - IDS/IPS Rule Writing
    - Snort
    - Suricata
    - Bro
- Network Security Monitoring
    - Power of Network Metadata
    - Know Thy Network
- Sandboxing
    - Beyond Inline
    - Integration with Endpoint

    - Feeding the Sandbox Potential Specimens
    - Malware Detonation Devices
- Encryption
    - The "Encrypt Everything" Mindset
        - Internal and External
    - Free SSL/TLS Certificate Providers
    - SSL/SSH Inspection
    - SSL/SSH Decrypt Dumps
    - SSL Decrypt Mirroring
    - Certificate Pinning
        - Malware Pins
    - HSTS
    - Crypto Suite Support
        - Qualys SSL Labs
    - Secure Remote Access
        - Access into Organization
        - Dual Factor for All Remote Access (and More)
            - Google Authenticator/TOTP: Open Authentication
        - IPSec VPNs
        - SSH VPNs
        - SSL/TLS VPN
        - Jump Boxes
    - Distributed Denial-of-Service
        - Impact of Internet of Things
        - Types of Attacks
        - Mitigation Techniques

SEC530.4 : Data-Centric Security

- Application (Reverse) Proxies
- Full Stack Security Design
    - Web Server
    - App Server
    - DB Server
- Web Application Firewalls
    - Whitelisting and Blacklisting
    - WAF Bypass
    - Normalization
    - Dynamic Content Routing
- Database Firewalls/Database Activity Monitoring
    - Data Masking
    - Advanced Access Controls
    - Exfiltration Monitoring
- File Classification
    - Data Discovery
        - Scripts vs. Software Solutions

        - Find Sensitive Data in Databases or Files/Folders
        - Advanced Discovery Techniques such as Optical Character Recognition Scanning of Pictures and Saved Scan Files
    - Methods of Classification
    - Dynamic Access Control
- Data Loss Prevention (DLP)
    - Network-based
    - Endpoint-based
    - Cloud Application Implementations
- Data Governance
    - Policy Implementation and Enforcement
    - Access Controls vs. Application Enforcement and Encryption
    - Auditing and Restrictions
- Mobile Device Management (MDM) and Mobile Application Management (MAM)
    - Security Policies
    - Methods for Enforcement
    - End-user Experience and Impact
- Private Cloud Security
    - Securing On-premises Hypervisors (vSphere, Xen, Hyper-V)
    - Network Segmentation (Logical and Physical)
    - VM Escape
    - Surface Reduction
    - Visibility Advantages
- Public Cloud Security
    - SaaS vs. PaaS vs. IaaS
    - Shared Responsibility Implications
    - Cloud Strengths and Weaknesses
    - Data Remanence and Lack of Network Visibility
- Container Security
    - Impact of Containers on On-premises or Cloud Architectures
    - Security Concerns
    - Protecting against Container Escape

SEC530.5 : Zero-Trust Architecture : Addressing the Adversaries Already in our Networks

- Zero Trust Architecture
    - Why Perimeter Security Is Insufficient
    - What Zero Trust Architecture Means
    - "Trust but Verify" vs. "Verify then Trust"
    - Implementing Variable Access
    - Logging and Inspection
    - Network Agent-based Identity Controls
- Credential Rotation
    - Certificates
    - Passwords and Impact of Rotation
    - Endpoints

- Compromised Internal Assets
    - Pivoting Adversaries
    - Insider Threat
- Securing the Network
    - Authenticating and Encrypting Endpoint Traffic
    - Domain Isolation (Making Endpoint Invisible to Unauthorized Parties)
    - Mutual TLS
    - Single Packet Authorization
- Tripwire and Red Herring Defenses
    - Honeynets, Honeypots, and Honeytokens
    - Single Access Detection Techniques
    - Proactive Defenses to Change Attacker Tool Behaviors
    - Increasing Prevention Capabilities while Adding Solid Detection
- Patching
    - Automation via Scripts
- Deputizing Endpoints as Hardened Security Sensors
    - End-user Privilege Reduction
    - Application Whitelisting
    - Host Hardening
        - EMET
    - Host-based IDS/IPS
        - As Tripwires
    - Endpoint Firewalls
        - Pivot Detection
    - Scaling Endpoint Log Collection/Storage/Analysis
        - How to Enable Logs that Matter
        - Designing for Analysis Rather than Log Collection

SEC555: SIEM with Tactical Analytics

SEC555.1 : SIEM Architecture

- State of the SOC/SIEM
    - Industry statistics
    - Industry problems
- Log Monitoring
    - Assets
        - Windows/Linux
        - Network devices
        - Security devices
    - Data gathering strategies
    - Pre-planning
- Logging architecture
    - Log inconsistencies

    - Log collection and normalization
    - Log retention strategies
    - Correlation and gaining context
    - Reporting and analytics
    - Alerting
- SIEM platforms
    - Commercial solutions
    - Home-grown solutions
- Planning a SIEM
    - Ingestion control
    - What to collect
    - Mission
- SIEM Architecture
- Ingestion techniques and nodes
- Acceptance and manipulation for value
- Augmentation of logs for detection
- Data queuing and resiliency
- Storage and speed
- Analytical reporting
    - Visualizations
    - Detection Dashboards

SEC555.2 : Service Profiling with SIEM

- Detection methods and relevance to log analysis
    - Attacker patterns
    - Attacker behaviors
    - Abnormalities
- Analyzing common application logs that generate tremendous amounts of data
    - DNS
        - Finding new domains being accessed
        - Pulling in addition information such as domain age
        - Finding randomly named domains
        - Discover domain shadowing techniques
        - Identifying recon
        - Find DNS C2 channels
    - HTTP
        - Use large datasets to find attacks
        - Identify bot traffic hiding in the clear
        - Discover requests that users do not make
            - Find ways to filter out legitimate noise
        - Use attacker randomness against them
        - Identify automated activity vs user activity
        - Filter approved web clients vs unauthorized
        - Find HTTP C2 channels
    - HTTPS

        - Alter information for large scale analysis
        - Analyze certificate fields to identify attack vectors
        - Track certificate validity
        - Apply techniques that overlap with standard HTTP
        - Find HTTPS C2 channels
    - SMTP
        - Identify where unauthorized email is coming from
        - Find compromised mail services
        - Fuzzy matching likely phishing domains
        - Data exfiltration detection
    - Apply threat intelligence to generic network logs
    - Active Dashboards and Visualizations
        - Correlate network datasets
        - Build frequency analysis tables
        - Establish network baseline activity

SEC555.3 : Advanced Endpoint Analytics

- Endpoint logs
    - Understanding value
    - Methods of collection
        - Agents
        - Agentless
        - Scripting
    - Adding additional logging
        - EMET
        - Sysmon
        - Group Policy
    - Windows filtering and tuning
    - Analyze critical events based on attacker patterns
        - Finding signs of exploitation
        - Find signs of internal reconnaissance
        - Finding persistence
        - Privilege escalation
        - Establishing a foothold
        - Cleaning up tracks
    - Host-based firewall logs
        - Discover internal pivoting
        - Identify unauthorized listening executables
        - See scan activity
    - Credential theft and reuse
        - Multiple failed logons
        - Unauthorized account use
    - Monitor PowerShell
        - Configure PowerShell logging
        - Identify obfuscation

        - Identify modern attacks
    - Containers
        - Logging methods
        - Monitoring

SEC555.4 : Baselining and User Behavior Monitoring

- Identify authorized and unauthorized assets
    - Active asset discovery
        - Scanners
        - Network Access Control
    - Passive asset discovery
        - DHCP
        - Network listeners such as p0f, bro, and prads
        - NetFlow
        - Switch CAM tables
    - Combining asset inventory into a master list
    - Adding contextual information
        - Vulnerability data
        - Authenticated device vs unauthenticated device
    - Identify authorized and unauthorized software
        - Source collection
            - Asset inventory systems
            - Patching management
            - Whitelisting solutions
            - Process monitoring
        - Discovering unauthorized software
    - Baseline data
        - Network data (from netflow, firewalls, etc)
            - Use outbound flows to discover unauthorized use or assets
            - Compare expected inbound/outbound protocol
            - Find persistence and beaconing
            - Utilize geolocation and reverse dns lookups
            - Establish device-to-device relationships
            - Identify lateral movement
            - Configure outbound communication thresholds
        - Monitor logons based on patterns
            - Time-based
            - Concurrency of logons
                - # logons by user
                - # logons by source device
                - Multiple geo locations
            - Endpoint baseline monitoring
                - Configure enterprise wide baseline collection
                - Large scale persistence monitoring
                - Finding abnormal local user accounts

        - Discover dual-homed devices
    - Cloud baselining (Example in class uses Amazon AWS)

SEC555.5 : Tactical SIEM Detection and Post-Mortem Analysis

- Centralize NIDS and HIDS alerts
- Analyze endpoint security logs
    - Provide alternative analysis methods
    - Configure tagging to facilitate better reporting
- Augment intrusion detection alerts
    - Extract CVE, OSVDB, etc for further context
    - Pull in rule info and other info such as geo
- Analyze vulnerability information
    - Setup vulnerability reports
    - Correlate CVE, OSVDB, and other unique IDs with IDS alerts
    - Prioritize IDS alerts based on vulnerability context
- Correlate malware sandbox logs with other systems to identify victims across enterprise
- Monitor Firewall Activity
    - Identify scanning activity on inbound denies
    - Apply auto response based on alerts
    - Find unexpected outbound traffic
    - Baseline allow/denies to identify unexpected changes
    - Apply techniques to filter out noise in denied traffic
- SIEM tripwires
    - Configure systems to generate early log alerts after compromise
        - Identify file and folder scan activity
        - Identify user token stealing
        - Operationalize virtual honeypots with central logging
        - Allow phone home tracking
    - Post mortem analysis
        - Re-analyze network traffic
            - Identify malicious domains and IPs
            - Look for beaconing activity
        - Identify unusual time-based activity
        - Use threat intel to reassess previous data fields such as user-agents
        - Utilize hashes in log to constantly re-evaluate for known bad files