Cybersecurity Defense and Protection Training System

Wealth Horizons Academy | $1997

THE COMPREHENSIVE CYBERSECURITY TRAINING SYSTEM FOR PROFESSIONALS

This advanced program provides the technical knowledge and practical skills to build, defend, and manage enterprise-level cybersecurity capabilities.

UNIT 1: NETWORK SECURITY ARCHITECTURE

Understanding Network Fundamentals

The OSI Model (7 Layers): 1. Physical: Hardware, cables, wireless signals 2. Data Link: MAC addresses, switches 3. Network: IP addresses, routing 4. Transport: TCP/UDP, ports 5. Session: Connection management 6. Presentation: Encryption, encoding 7. Application: HTTP, DNS, email protocols

Security attacks and defenses map to specific OSI layers. Understanding the model is fundamental to understanding attacks.

Network Segmentation

Divide your network into security zones to contain breaches: - DMZ (Demilitarized Zone): Internet-facing systems - Internal Network: General user workstations - Secure Zone: Financial systems, HR, executives - Industrial/OT Network: Manufacturing and operational systems (if applicable) - Management Network: IT administration

Firewalls and Next-Generation Firewalls (NGFW): Traditional firewalls: Allow/deny based on IP and port NGFW: Deep packet inspection, application awareness, IPS, SSL inspection

Intrusion Detection and Prevention

IDS (Intrusion Detection System): Monitors and alerts on suspicious activity **IPS (Intrusion Prevention System):** Monitors and actively blocks suspicious activity

Detection methods: - Signature-based: Matches known attack patterns (fast but misses unknown attacks) - Anomaly-based: Detects deviations from normal (catches unknown attacks but more false positives) - Behavior-based: AI/ML analysis of behavior patterns (most sophisticated)

UNIT 2: ENDPOINT SECURITY

Endpoint Detection and Response (EDR)

Modern EDR platforms provide: - Real-time monitoring of endpoint activity - Behavioral detection of unknown threats - Automated response and containment - Forensic investigation capabilities - Threat hunting tools

Leading EDR Solutions: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint

Vulnerability Management Program

1. Asset inventory: Know every device on your network
2. Vulnerability scanning: Regular automated scanning
3. Risk-based prioritization: Not all vulnerabilities are equal
4. Remediation tracking: Ensure patches are applied
5. Reporting: Document and measure progress over time

Key Vulnerability Databases: - CVE (Common Vulnerabilities and Exposures) - NVD (National Vulnerability Database) - CISA Known Exploited Vulnerabilities Catalog

UNIT 3: IDENTITY AND ACCESS MANAGEMENT

Privileged Access Management (PAM)

Privileged accounts (administrators, service accounts) are the most targeted accounts in any environment.

PAM Best Practices: - Just-in-time access (elevate only when needed) - Credential vaulting (no one knows the password) - Session recording for all privileged access - Separate privileged accounts from daily-use accounts

Single Sign-On (SSO) and Federation

SSO allows users to authenticate once and access multiple applications.

Benefits: - Improved user experience (fewer passwords) - Centralized access control - Easier deprovisioning when employees leave

Standards: SAML, OAuth 2.0, OpenID Connect

UNIT 4: SECURITY OPERATIONS

Security Operations Center (SOC) Functions

A SOC is the team responsible for monitoring and defending an organization's security.

SOC Capabilities: - 24x7 monitoring of security events - Alert triage and investigation - Incident response - Threat hunting - Vulnerability management - Threat intelligence consumption

SIEM (Security Information and Event Management): Collects and correlates log data from across the environment to identify threats.

Key SIEM Use Cases: - Failed login detection - Lateral movement detection - Data exfiltration alerts - Malware execution detection - Privilege escalation detection

Threat Intelligence

Types of Threat Intelligence: - Strategic: High-level trends, nation-state activities, industry threats - Tactical: TTPs (Tactics, Techniques, Procedures) of threat actors - Operational: Specific, actionable intelligence on active threats - Technical: IOCs (Indicators of Compromise) — IPs, domains, file hashes

MITRE ATT&CK Framework: A globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Use it to:

- Understand how attackers operate - Identify detection gaps in your defenses - Prioritize security investments

UNIT 5: SECURITY GOVERNANCE AND RISK

Information Security Policy Framework

Every organization needs documented security policies: - Information Security Policy (master policy) - Acceptable Use Policy - Access Control Policy - Incident Response Policy - Data Classification Policy - Business Continuity/ Disaster Recovery Plan

Risk Assessment Process

1. Identify assets (data, systems, processes)
2. Identify threats (who/what could harm assets)
3. Identify vulnerabilities (weaknesses that could be exploited)
4. Calculate risk (likelihood × impact)
5. Evaluate controls (what is already in place)
6. Determine residual risk (risk after controls)
7. Treat risk (accept, mitigate, transfer, avoid)

Risk Treatment Options: - Accept: Risk is within acceptable tolerance - Mitigate: Implement controls to reduce risk - Transfer: Insurance or contractual shift of risk - Avoid: Stop the activity that creates the risk

Cyber Insurance

Cyber insurance has become essential: - Average claim: $350,000+ - Covers: Incident response costs, business interruption, notification costs, regulatory fines, third-party liability

Insurers now require specific security controls to qualify. Minimum requirements typically include MFA on email, regular backups, and security awareness training.
