Course Introduction
Course Introduction

Lesson 01 - Assessing Information Security Risk
Lesson 01 - Assessing Information Security Risk

Topic A: Identify the Importance of Risk Management

Elements of Cybersecurity (Perimeter Model)
Elements of Cybersecurity (Endpoint Model)
The Risk Equation
Risk Management
The Importance of Risk Management

ERM
Reasons to Implement ERM
Risk Exposure
Risk Analysis Methods
Risks Facing an Enterprise

Topic B: Assess Risk

ESA Frameworks
ESA Framework Assessment Process
New and Changing Business Models
De-perimeterization
New Products and Technologies
Internal and External Influences
System-Specific Risk Analysis
Risk Determinations
Documentation of Assessment Results
Guidelines for Assessing Risk

Topic C: Mitigate Risk

Classes of Information
Classification of Information Types into CIA Levels
Security Control Categories
Technical Controls (Template)
Technical Controls (Example Answer)
Aggregate CIA Score
Common Vulnerability Scoring System
Common Vulnerabilities and Exposures
Demo - Common Vulnerability Scoring System
Extreme Scenario Planning and Worst Case Scenarios

Risk Response Techniques
Additional Risk Management Strategies
Continuous Monitoring and Improvement

IT Governance
Guidelines for Mitigating Risk

Topic D: Integrate Documentation into Risk Management

From Policy to Procedures
Policy Development
Process and Procedure Development
Lesson 02 - Analyzing the Threat Landscape
Topic A: Classify Threats and Threat Profiles
Threat Actors
Threat Motives
Threat Intentions
Attack Vectors
Attack Technique Criteria
Qualitative Threat and Impact Analysis
Guidelines for Classifying Threats and Threat Profiles
Topic B: Perform Ongoing Threat Research
Ongoing Research
Situational Awareness
Commonly Targeted Assets
The Latest Vulnerabilities
The Latest Threats and Exploits
The Latest Security Technologies
Resources Aiding in Research
Demo - Resources that Aid in Research of Threats
The Global Cybersecurity Industry and Community
Trend Data
Trend Data and Qualifying Threats
Guidelines for Performing Ongoing Threat Research
Lesson 02 Review

Lesson 03 - Analyzing Reconnaissance Threats to Computing and Network Environments
Topic A: Implement Threat Modeling
The Diverse Nature of Threats
The Anatomy of a Cyber Attack
Threat Modeling
Reasons to Implement Threat Modeling
Threat Modeling Process
Attack Tree
Threat Modeling Tools
Threat Categories
Topic B: Assess the Impact of Reconnaissance Incidents
Footprinting, Scanning, and Enumeration
Footprinting Methods
Network and System Scanning Methods
Enumeration Methods
Evasion Techniques for Reconnaissance
Reconnaissance Tools
Packet Trace Analysis with Wireshark
Demo - Performing Reconnaissance on a Network
Demo - Examining Reconnaissance Incidents
Topic C: Assess the Impact of Social Engineering

Social Engineering
Types of Social Engineering
Phishing and Delivery Media
Phishing and Common Components
Social Engineering for Reconnaissance
Demo - Assessing the Impact of Social Engineering
Demo - Assessing the Impact of Phishing
Lesson 03 Review

Lesson 04 - Analyzing Attacks on Computing and Network Environments 1h 36m
Topic A: Assess the Impact of System Hacking Attacks
System Hacking
Password Sniffing
Password Cracking
Demo - Cracking Passwords Using a Password File
Privilege Escalation
Social Engineering for Systems Hacking
System Hacking Tools and Exploitation Frameworks
Topic B: Assess the Impact of Web-Based Attacks
Client-Side vs. Server-Side Attacks
XSS
XSRF
SQL Injection
Directory Traversal
File Inclusion
Additional Web Application Vulnerabilities and Exploits
Web Services Exploits
Web-Based Attack Tools
Demo - Assessing the Impact of Web-Based Threats
Topic C: Assess the Impact of Malware
Malware Categories
Trojan Horse
Polymorphic Virus
Spyware
Supply Chain Attack
Malware Tools
Demo - Malware Detection and Removal
Topic D: Assess the Impact of Hijacking and Impersonation Attacks
Spoofing, Impersonation, and Hijacking
ARP Spoofing
DNS Poisoning
ICMP Redirect
DHCP Spoofing
NBNS Spoofing
Session Hijacking
Hijacking and Spoofing Tools
Topic E: Assess the Impact of DoS Incidents
DoS Attacks
Lesson 05 - Analyzing Post-Attack Techniques  1h 3m

Topic A: Assess Command and Control Techniques
Command and Control
IRC
HTTP/S
DNS
ICMP
Additional Channels
Demo - Assessing Command and Control Techniques
Topic B: Assess Persistence Techniques
Advanced Persistent Threat
Rootkits
Backdoors
Logic Bomb
Demo - Detecting Rootkits
Rogue Accounts
Topic C: Assess Lateral Movement and Pivoting Techniques
Lateral Movement
Pass the Hash
Golden Ticket
Remote Access Services
WMIC
PsExec
Port Forwarding
VPN Pivoting
SSH Pivoting
Routing Tables and Pivoting
Topic D: Assess Data Exfiltration Techniques
Data Exfiltration
Covert Channels
Steganography
Demo - Steganography
File Sharing Services
Topic E: Assess Anti-Forensics Techniques
Anti-Forensics
Golden Ticket and Anti-Forensics
Demo - Assessing Anti-Forensics
Buffer Overflows
Memory Residents
Program Packers
VM and Sandbox Detection
ADS
Covering Tracks
Lesson 05 Review

Lesson 06 - Evaluating the Organization's Security Posture
54m
Topic A: Conduct Vulnerability Assessments
Vulnerability Assessment
Penetration Testing
Vulnerability Assessment vs. Penetration Testing
Vulnerability Assessment Implementation
Vulnerability Assessment Tools
Specific Assessment Tools
Port Scanning and Fingerprinting
Sources of Vulnerability Information
Operating System and Software Patching
Systemic Security Issues
Demo - Perform a Vulnerability Scan with Nessus
Demo - Perform a Vulnerability Scan with MBSA
Topic B: Conduct Penetration Tests on Network Assets
ROE
Pen Test Phases
Pen Test Scope
External vs. Internal Pen Testing
Pen Testing Techniques
Pen Testing Tools of the Trade
Kali Linux
Data Mining
Attack Surface Scanning and Mapping
Packet Manipulation for Enumeration
Simulated Attacks
Password Attacks
Penetration Test Considerations
Topic C: Follow Up on Penetration Testing
Effective Reporting and Documentation
Target Audiences
Information Collection Methods
Penetration Test Follow-Up
Report Classification and Distribution
Lesson 06 Review
Lesson 07 - Collecting Cybersecurity Intelligence

Topic A: Deploy a Security Intelligence Collection and Analysis Platform

Security Intelligence

The Challenge of Security Intelligence Collection

Security Intelligence Collection Lifecycle

Security Intelligence Collection Plan

CSM

What to Monitor

Security Monitoring Tools

Data Collection

Potential Sources of Security Intelligence

Guidelines for Determining Which Data to Collect for Security Intelligence

Guidelines for Determining Which Fields You Should Log

Guidelines for Configuring Logging Systems Based on Their Impact

Guidelines for Determining Which Events Should Prompt an Alert

Information Processing

External Data Sources

Publicly Available Information

Collection and Reporting Automation

Data Retention

Topic B: Collect Data from Network-Based Intelligence Sources

Network Device Configuration Files

Network Device State Data

Switch and Router Logs

Wireless Device Logs

Firewall Logs

WAF Logs

IDS/IPS Logs

Proxy Logs

Carrier Provider Logs

Software-Defined Networking

Network Traffic and Flow Data

Log Tuning

Demo - Collecting Network-Based Security Intelligence

Topic C: Collect Data from Host-Based Intelligence Sources

Operating System Log Data

Windows Event Logs

Syslog Data

Application Logs

DNS Event Logs

SMTP Logs

HTTP Logs

FTP Logs

SSH Logs

SQL Logs

Demo - Collecting Host-Based Security Intelligence

Demo - Parsing Log Files

Lesson 07 Review
Lesson 08 - Analyzing Log Data

Topic A: Use Common Tools to Analyze Logs
- Preparation for Analysis
- Guidelines for Preparing Data for Analysis
- Log Analysis Tools
  - The grep Command
  - The cut Command
  - The diff Command
  - The find Command
- WMIC for Log Analysis
- Event Viewer
- Bash
- Windows PowerShell
- Additional Log Analysis Tools
- Guidelines for Using Windows- and Linux-Based Tools for Log Analysis
- Demo - Analyzing Linux Logs for Security Intelligence

Topic B: Use SIEM Tools for Analysis
- Security Intelligence Correlation
- SIEM
  - The Realities of SIEM
  - SIEM and the Intelligence Lifecycle
- Guidelines for Using SIEMs for Security Intelligence Analysis
- Demo - Incorporating SIEMs into Security Intelligence Analysis

Topic C: Parse Log Files with Regular Expressions
- Regular Expressions
  - Quantification Operators
  - Anchor Operators
  - Character Set Operators
  - Miscellaneous Search Operators
  - Special Operators
  - Build an Expression
  - Keyword Searches
  - Special Character Searches
  - IP Address Searches
- Guidelines for Writing Regular Expressions

Lesson 08 Review

Lesson 09 - Performing Active Asset and Network Analysis

Topic A: Analyze Incidents with Windows-Based Tools
- Registry Editor (regedit)
- Analysis with Registry Editor
- File System Analysis Tools for Windows
- Process Explorer
- Process Monitor
- Service Analysis Tools for Windows
- Volatile Memory Analysis Tools for Windows
- Active Directory Analysis Tools
- Network Analysis Tools for Windows
- Demo - Windows-Based Incident Analysis Tools

Topic B: Analyze Incidents with Linux-Based Tools
File System Analysis Tools for Linux
Process Analysis Tools for Linux
Volatile Memory Analysis Tools for Linux
Session Analysis Tools for Linux
Network Analysis Tools for Linux
Demo - Linux-Based Incident Analysis Tools
Topic C: Analyze Malware
Malware Sandboxing
Crowd-Sources Signature Detection
VirusTotal Malware Entry
Reverse Engineering
Disassemblers
Disassembly of Malware in IDA
Malware Strings
Anti-Malware Solutions
MAEC
Guidelines for Analyzing Malware
Demo - Analyzing Malware
Topic D: Analyze Indicators of Compromise
IOCs
Unauthorized Software and Files
Suspicious Emails
Suspicious Registry Entries
Unknown Port and Protocol Usage
Excessive Bandwidth Usage
Service Disruption and Defacement
Rogue Hardware
Suspicious or Unauthorized Account Usage
Guidelines for Analyzing Indicators of Compromise
Demo - Analyzing Indicators of Compromise
Lesson 09 Review

Lesson 10 - Responding to Cybersecurity Incidents
Lesson 10 - Responding to Cybersecurity Incidents
1h 13m
Topic A: Deploy an Incident Handling and Response Architecture
Incident Handling and Response Planning
Site Book
Incident Response Process
SOCs
CSIRT Organization
CSIRT Roles
A Day in the Life of a CSIRT
CSIRT Communication Process
Incident Indicator Sources
The Impact and Scope of Incidents
Incident Evaluation and Analysis
Incident Containment
Incident Mitigation and Eradication
Incident Recovery
Lessons Learned
Incident Handling Tools
Lesson 11 - Investigating Cybersecurity Incidents

1. **Topic A: Apply a Forensic Investigation Plan**
   - A Day in the Life of a Forensic Analyst
   - Forensic Investigation Models
   - Forensic Investigation Preparation
   - Investigation Scope
   - Timeline Generation and Analysis
   - Authentication of Evidence
   - Chain of Custody
   - Communication and Interaction with Third Parties
   - Forensic Toolkits
   - Guidelines for Preparing for a Forensic Investigation

2. **Topic B: Securely Collect and Analyze Electronic Evidence**
   - Order of Volatility
   - File Systems
   - File Carving and Data Extraction
   - Persistent Data
   - Data Preservation for Forensics
   - Forensic Analysis of Compromised Systems
   - Demo - Securely Collecting Electronic Evidence
   - Demo - Analyzing Forensic Evidence

3. **Topic C: Follow Up on the Results of an Investigation**
   - Cyber Law
   - Technical Experts and Law Enforcement Liaisons
   - Documentation of Investigation Results

**Lesson 11 Review**

**Next Steps**

**Course Closure**

**Total Duration:** 12h 7m