CompTIA CySA+ (CS0-002)

Course Overview

The Cybersecurity Analyst course will teach students about IT security and security analysis. Topics covered include threats and vulnerabilities, infrastructure management, monitoring security options, incident response, compliance and assessment, and more.

Chapter 1 - Managing Threats and Vulnerabilities 2h 38m

Instructor Introduction
Course Introduction
Managing Threats and Vulnerabilities
Topic A: Threat Data and Intelligence
Importance of Threat Data
Open-Source Intelligence
Proprietary / Closed Source Intelligence
Intelligence Characteristics
Demo - Threat Data
Indicator Management
STIX Domain Objects
Trusted Automated Exchange of Indicator Information (TAXII)
OpenIoC
Threat Classification
Threat Actors
Intelligence Cycle
Information Sharing
Topic B: Utilizing Threat Intelligence
Threat Intelligence and Operational Security
Attack Frameworks
MITRE ATT&CK
MITRE ATT&CK (cont.)
The Diamond Model of Intrusion Analysis
Kill Chain
Threat Research
Threat Modeling
Threat Intelligence Sharing with Supported Functions
Topic C: Vulnerability Management
Introduction to Vulnerability Management
Vulnerability Identification
Validation Options
Remediation and Mitigation
Understanding Scanning
Additional Scanning Considerations
Inhibitors to Remediation
Topic D: Using Vulnerability Assessment Tools
Web Application Scanners

Infrastructure Scanners
Demo - Infrastructure Scanners
Software Assessments
Enumeration
Demo - Enumeration
Wireless Assessments
Cloud Assessment
Chapter 1 Review

Chapter 2 - Specialized Threats and Vulnerabilities 54m

Specialized Threats and Vulnerabilities
Topic A: Threats and Vulnerabilities with Specialized Technology
Common Vulnerabilities
App Vulnerabilities
Internet of Things (IoT)
Other Specialized Devices
Other Specialized Devices (cont.)
Topic B: Threats and Vulnerabilities for Cloud Environments
Cloud Services Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Cloud Deployment Models
Additional Cloud Concepts
Insecure Application Programming Interface (API)
Additional Cloud Vulnerabilities
Demo - Identifying Azure Security Vulnerabilities
Chapter 2 Review

Chapter 3 - Attacks and Software Vulnerability Mitigation 28m

Attacks and Software Vulnerability Mitigation
Topic A: Understanding Attack Types
Injection Attacks
Injection Attacks (cont.)
Directory Traversal
Buffer Overflow Attacks
Privilege Escalation
Authentication Attacks
Topic B: Software Vulnerabilities
Improper Error Handling
Dereferencing
Insecure Object Reference
Race Conditions
Sensitive Data Exposure
Additional Vulnerabilities
Chapter 3 Review

Chapter 4 - Infrastructure Management 1h 31m

Infrastructure Management
Topic A: Network Security Solutions
Network Architecture
Physical Network
Software-Defined Network
Virtual Private Cloud Network
Virtual Private Network
Virtualization Solutions
Network Segmentation
Demo - Virtual Network Segmentation
Demo - Data Collector Sets
Topic B: Identity and Access Management
IAM Concepts
Privilege Management
Multifactor Authentication
Demo - MFA Implementation
Identity Federation
Access Control Types
Demo - Access Control
Cloud Access Security Broker
Topic C: Additional Solutions
Monitoring and Logging
Cryptography
Demo - Encrypting File System and Certification Management
Chapter 4 Review

Chapter 5 - Hardware and Software Assurance 1h 1m

Hardware and Software Assurance
Topic A: Hardware Assurance Best Practices
Hardware Root of Trust
Trusted Platform Module
Demo - BitLocker Drive Encryption
Hardware Security Module
eFuse
Unified Extensible Firmware Interface (UEFI)
Measured Boot and Attestation
Additional Hardware Options
Topic B: Software Assurance Best Practices
Platforms and Software Architecture
Service-Oriented Architecture
Software Development Lifecycle
Software Assessment Methods
Secure Coding
Chapter 5 Review

Chapter 6 - Monitoring Security Options 49m

Monitoring Security Options
Topic A: Security Data Analytics
Monitoring Fundamentals
Aggregating Data
Data Analysis
Topic B: Endpoint and Network Analysis
Endpoint Security
Network Analysis
Log Review
Demo - Logging and Monitoring
Impact Analysis
Topic C: Email Analysis
Social Engineering
Anti-SPAM
Demo - Configuring Anti-Spam Options in Exchange Online
Chapter 6 Review

Chapter 7 - Implementing Security Changes 1h 5m

Implementing Security Changes
Topic A: Security Configuration Management
Fundamental Identity Configuration
Software Controls
Firewalls
Intrusion Detection Systems (IDS)
Data Loss Prevention
Endpoint Detection and Response
Network Access Control
Additional Techniques
Topic B: Threat Hunting
Understanding Threat Hunting
Threat Hunting Process
Establishing Hypothesis
Profiling Threat Actors
Threat Hunting Tactics
Attack Surface Reduction
Topic C: Automating Security
Security Automation Concepts
Workflow Orchestration
Orchestration Playbooks
Scripting
API Integration
REST Principles
Security Content Automation Protocol
Software Engineering
Chapter 7 Review

Chapter 8 - Incident Response 1h 55m

Incident Response
Topic A: Importance of Incident Response
Incident Response Process
Establishing Communications Processes
Internal Communications
External Communications
Identifying Critical Data
Topic B: Incident Response Procedures
Incident Response Cycle
Preparation Phase
Detection and Analysis
Containment
Containment Types
Eradication and Recovery
Eradication and Recovery (cont.)
Post-Incident Activities
Topic C: Analyzing Indicators of Compromise
Network-related Indicators
Host-related Indicators
Application-related Indicators
Demo - Analyzing IoCs
Topic D: Utilizing Digital Forensics Techniques
Digital Forensics
Using Network Tools
Demo - Using Wireshark
Capturing Endpoint Systems
Additional Forensics Situations
Building a Forensics Kit
Chapter 8 Review

Chapter 9 - Compliance and Assessment 1h 8m

Compliance and Assessment
Topic A: Data Privacy and Protection
Security vs. Privacy
Data Types
Legal Requirements
Nontechnical Controls
Data Retention Standards
Technical Controls
Data Loss Prevention
Demo - Implementing DLP
Topic B: Risk Mitigation
Business Impact Analysis
BIA Steps
Risk Assessment
Risk Identification Process
Risk Calculation
Risk Prioritization
Security Controls

Training and Exercises
Topic C: Policies and Procedures
Code of Conduct
Control Types
Audits and Assessment
Chapter 9 Review
Course Closure

Total Duration: 11h 29m