PROGRAMMA CompTIA Security + (SY0-601)

40 ore

Part I: Threats, Attacks, and Vulnerabilities

Social Engineering Techniques

The Social Engineer

Phishing and Related Attacks

Principles of Influence (Reasons for Effectiveness)

Attack Basics

Malware

Physical Attacks

Adversarial Artificial Intelligence (AI)

Password Attacks

Downgrade Attacks

Application Attacks

Race Conditions

Improper Software Handling

Resource Exhaustion

Overflows

Code Injections

Driver Manipulation

Request Forgeries

Directory Traversal

Replay Attack

Secure Sockets Layer (SSL) Stripping

Application Programming Interface (API) Attacks

Pass-the-Hash Attack

Network Attacks

Wireless

Man-in-the-Middle

Layer 2 Attacks

Domain Name System (DNS) Attacks

Denial of Service

Malicious Code and Script Execution

Threat Actors, Vectors, and Intelligence Sources

Threat Actor Attributes

Threat Actor Types

Vectors

Threat Intelligence and Research Sources

Vulnerabilities

Cloud-Based vs. On-Premises

Zero-Day

Weak Configurations

Third-Party Risks

Impacts

Security Assessment Techniques

Vulnerability Scans

Threat Assessment

Penetration Testing Techniques

Testing Methodology

Team Exercises

Part II: Architecture and Design

Enterprise Security Concepts

Configuration Management

Data Confidentiality

Deception and Disruption

Virtualization and Cloud Computing

Virtualization

On-Premises vs. Off-Premises

Cloud Models

Secure Application Development, Deployment, and Automation

Application Environment

Integrity Measurement

Change Management and Version Control

Secure Coding Techniques

Automation and Scripting

Scalability and Elasticity

Authentication and Authorization Design

Identification and Authentication, Authorization, and Accounting (AAA)

Multifactor Authentication

Single Sign-on

Authentication Technologies

Cybersecurity Resilience

Redundancy

Backups

Defense in Depth

Embedded and Specialized Systems

Embedded Systems

SCADA and ICS

Smart Devices and IoT

Physical Security Controls

Perimeter Security

Internal Security

Equipment Security

Environmental Controls

Secure Data Destruction

Cryptographic Concepts

Cryptosystems

Use of Proven Technologies and Implementation

Steganography

Cryptography Use Cases

Cryptography Constraints

Part III: Implementation

Secure Protocols

Secure Web Protocols

Secure File Transfer Protocols

Secure Email Protocols

Secure Internet Protocols

Secure Protocol Use Cases

Host and Application Security Solutions

Endpoint Protection

Application Security

Hardware and Firmware Security

Operating System Security

Secure Network Design

Network Devices and Segmentation

Security Devices and Boundaries

Wireless Security Settings

Access Methods

Wireless Cryptographic Protocols

Authentication Protocols

Wireless Access Installations

Secure Mobile Solutions

Communication Methods

Mobile Device Management Concepts

Enforcement and Monitoring

Deployment Models

Cloud Cybersecurity Solutions

Cloud Workloads

Third-Party Cloud Security Solutions

Identity and Account Management Controls

Account Types

Account Management

Account Policy Enforcement

Authentication and Authorization Solutions

Authentication

Access Control

Public Key Infrastructure

PKI Components

Part IV: Operations and Incident Response

Organizational Security

Shell and Script Environments

Network Reconnaissance and Discovery

Packet Capture and Replay

Password Crackers

Forensics and Data Sanitization

Incident Response

Attack Frameworks

Incident Response Plan

Incident Response Process

Continuity and Recovery Plans

Incident Investigation

SIEM Dashboards

Logging

Network Activity

Incident Mitigation

Containment and Eradication

Digital Forensics

Data Breach Notifications

Strategic Intelligence/Counterintelligence Gathering

Track Person-hours

Order of Volatility

Chain of Custody

Data Acquisition

Part V: Governance, Risk, and Compliance

Control Types

Nature of Controls

Functional Use of Controls

Compensating Controls

Regulations, Standards, and Frameworks

Industry-Standard Frameworks and Reference Architectures

Benchmarks and Secure Configuration Guides

Organizational Security Policies

Policy Framework

Human Resource Management Policies

Third-Party Risk Management

Risk Management

Risk Analysis

Risk Assessment

Business Impact Analysis

Sensitive Data and Privacy

Sensitive Data Protection

Privacy Impact Assessment