CompTIA Advanced Security Practitioner
Exam CAS-003

Overview
CASP+ covers the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise.

Prerequisites
A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience.

Course Objectives
Upon successful completion of this course, students will be able to:

- Identify enterprise security fundamentals.
- Apply enterprise security technology solutions.
- Identify enterprise resource technologies and the potential security implications for these resources.
- Design security solutions.
- Identify application security design issues such as best practices for development and testing as well as threat mitigation techniques.
- Manage risk, security policies, and security procedures within an enterprise.
- Integrate security solutions within an enterprise.
- Conduct security research and analysis.

Course Contents

- Risk Management
- Summarize business and industry influences and associated security risks.
  - Risk management of new products
  - New or changing business
  - Security concerns of integrating
  - Internal and external influences
  - Impact of de-perimeterization (e.g. constantly changing network boundary)
- Compare and contrast security, privacy polices and procedures based on organizational requirements

- Policy and process life cycle management
- Support legal compliance and advocacy by partering with human resources, legal, management and other entitles
- Understand common business documents to support security
- Research security requirements for contracts
- Understand general privacy principles for sensitive information
- Support the development of polices containing standard security practices

- Given a scenario, execute risk mitigation strategies and controls
  - Cate gorize data types by impact levels based on CIA
  - Incorporate stakeholder input into CIA impact-level decisions
  - Determine minimum-required security controls based on aggregate score
  - Extreme scenario planning/worst-case scenario
  - Conduct system-specific risk analysis
  - Make risk determination based upon know metrics
  - Translate technical risk in business terms
  - Recommend which strategy should be applied based o risk appetite
  - Risk management processes
  - Continuous improvement/monitoring
  - Business continuity planning
  - IT governance
  - Enterprise resilience
- Analyze risk metric scenarios to secure the enterprise
  - Review effectiveness of existing security controls
  - Reverse engineer/deconstruct
  - Create benchmarks and compare to baselines
  - Analyze and interpret data to anticipate cyber defense needs
  - Analyze security solution metrics and attributes to ensure they meet business needs
- Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements
  - Physical and virtual network and security devices
  - Application and protocol-aware technologies
  - Advanced network design (wired/wireless)
  - Complex network security solutions for data flow

- Secure configuration and baselining of networking and security components
  - Software-defined networkin
  - Network management and tools
  - Advanced configuration of routers, switches and other network devices
  - Security zones
  - Network access control
  - Network-enabled devices
  - Critical Infrastructure
- Analyze a scenario to integrate security controls for host devices to meet security requirements.
  - Trusted OS (e.g., how and when to use it)
  - Endpoint security software
  - Host hardening
  - Boot loader protections
  - Vulnerabilities associated with hardware
  - Terminal services/application delivery services
- Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements
  - Enterprise mobility management
  - Security implications/privacy concerns
  - Wearable technology
- Given software vulnerability scenarios, select appropriate security controls
  - Aplication security design considerations
  - Specific application issues
  - Application sandboxing
  - Secure encrypted enclaves
  - Database activity monitor
  - Web application firewalls
  - Client-side processing vs. server-side processing
  - Operating system vulnerabilities
  - Firmware vulnerabilities
- Enterprise Security Operations
- Given a scenario, conduct a security assessment using the appropriate methods

- Methods
- Types

- Analyze a scenario or output, and select the appropriate tool for a security assessment
  - Network tool types
  - Host tool types
  - Physical security tolos
- Given a scenario, implement incident response and recovery procedures
  - E-discovery
  - Data breach
  - Facilitate incident detection and response
  - Incident and emergency response
  - Incident response support tolos
  - Severity of incident or breach
  - Post-incident response
- Technical Integration of Enterprise Security
- Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.
  - Adapt data flow security to meet changing business needs
  - Standards
  - Interoperability issues
  - Resilience issues
  - Data security considerations
  - Resources provisioning and deprovisioning
  - Design considerations during mergers, acquisitions and demergers/divestitures
  - Network secure segmentation and delegation
  - Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
  - Security and privacy considerations of storage integration
  - Security implications of integrating enterprise applications
- Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.
  - Technical deployment models (outsourcing/insourcing/managed services/partnership)

- Security advantages and disadvantages of virtualization
- Cloud augmented security services
- Vulnerabilities associated with comingling of hosts with different security requirements
- Data security considerations
- Resources provisioning and deprovisioning

- Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.
  - Authentication
  - Authentication
  - Attestation
  - Identity proofing
  - Identity propagation
  - Federation
  - Trust models
- Given a scenario, implement cryptographic techniques.
  - Techniques
  - Implementations
- Given a scenario, select the appropriate control to secure communications and collaboration solutions.
  - Remote Access
  - Unified collaboration tolos
- Research, Development and Collaboration
- Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.
  - Perform ongoing research
  - Threat intelligence
  - Research security implications of emerging business tools
  - Global IA industry/community
- Given a scenario, implement security activities across the technology life cycle.
  - Systems development life cycle
  - Software development life cycle
  - Adapt solutions to address:

- Asset management (inventory control)
- Explain the importance of interaction across diverse business units to achieve security goals.
  - Interpreting security requirements and goals to communicate with stakeholders from other disciplines
  - Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls
  - Establish effective collaboration within teams to implement secure solutions
  - Governance, risk and compliance committee.

Certification Information

- CAS-003