

# SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP)

## COURSE CONTENT

### Domain 1:

#### Access Controls

##### 1.1 Implement and maintain authentication methods

- » Single/multifactor authentication
- » Single sign-on
- » Device authentication
- » Federated access

##### 1.2 Support internetwork trust architectures

- » Trust relationships (e.g., 1-way, 2-way, transitive)
- » Extranet
- » Third party connections

##### 1.3 Participate in the identity management lifecycle

- » Authorization
- » Proofing
- » Provisioning/de-provisioning
- » Maintenance
- » Entitlement
- » Identity and Access Management (IAM) systems

##### 1.4 Implement access controls

- » Mandatory
- » Non-discretionary
- » Discretionary
- » Role-based
- » Attribute-based
- » Subject-based
- » Object-based

### Domain 2:

#### Security Operations and Administration

##### 2.1 Comply with codes of ethics

- » (ISC)<sup>2</sup> Code of Ethics
- » Organizational code of ethics

##### 2.2 Understand security concepts

- » Confidentiality
- » Integrity
- » Availability
- » Accountability
- » Privacy
- » Non-repudiation
- » Least privilege
- » Separation of duties

##### 2.3 Document, implement, and maintain functional security controls

- » Deterrent controls
- » Preventative controls
- » Detective controls

- » Corrective controls
- » Compensating controls
- 2.4 Participate in asset management**
  - » Lifecycle (hardware, software, and data)
  - » Hardware inventory
  - » Software inventory and licensing
  - » Data storage
- 2.5 Implement security controls and assess compliance**
  - » Technical controls (e.g., session timeout, password aging)
  - » Physical controls (e.g., mantrap, cameras, locks)
  - » Administrative controls (e.g., security policies and standards, procedures, baselines)
  - » Periodic audit and review
- 2.6 Participate in change management**
  - » Execute change management process
  - » Identify security impact
  - » Testing /implementing patches, fixes, and updates (e.g., operating system, applications, SDLC)
- 2.7 Participate in security awareness and training**
- 2.8 Participate in physical security operations (e.g., data center assessment, badging)**

## Domain 3:

### Risk Identification, Monitoring, and Analysis

- 3.1 Understand the risk management process**
  - » Risk visibility and reporting (e.g., risk register, sharing threat intelligence, Common Vulnerability Scoring System (CVSS))
  - » Risk management concepts (e.g., impact assessments, threat modelling, Business Impact Analysis (BIA))
  - » Risk management frameworks (e.g., ISO, NIST)
  - » Risk treatment (e.g., accept, transfer, mitigate, avoid, recast)
- 3.2 Perform security assessment activities**
  - » Participate in security testing
  - » Interpretation and reporting of scanning and testing results
  - » Remediation validation
  - » Audit finding remediation
- 3.3 Operate and maintain monitoring systems (e.g., continuous monitoring)**
  - » Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring)
  - » Logging
  - » Source systems
  - » Legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
- 3.4 Analyze monitoring results**
  - » Security baselines and anomalies
  - » Visualizations, metrics, and trends (e.g., dashboards, timelines)
  - » Event data analysis
  - » Document and communicate findings (e.g., escalation)

## Domain 4:

### Incident Response and Recovery

- 4.1 Support incident lifecycle**
  - » Preparation
  - » Detection, analysis, and escalation
  - » Containment
  - » Eradication

- » Recovery
- » Lessons learned/implementation of new countermeasure
- 4.2 Understand and support forensic investigations
  - » Legal and ethical principles
  - » Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
- 4.3 Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) activities
  - » Emergency response plans and procedures (e.g., information system contingency plan)
  - » Interim or alternate processing strategies
  - » Restoration planning
  - » Backup and redundancy implementation
  - » Testing and drills

## Domain 5: Cryptography

### 5.1 Understand fundamental concepts of cryptography

- » Hashing
- » Salting
- » Symmetric/asymmetric encryption/Elliptic Curve Cryptography (ECC)
- » Non-repudiation (e.g., digital signatures/ certificates, HMAC, audit trail)
- » Encryption algorithms (e.g., AES, RSA)
- » Key strength (e.g., 256, 512, 1024, 2048-bit keys)
- » Cryptographic attacks, cryptanalysis, and counter measures

### 5.2 Understand reasons and requirements for cryptography

- »» Confidentiality
- »» Integrity and authenticity
- »» Data sensitivity (e.g., PII, intellectual property, PHI)
- »» Regulatory

### 5.3 Understand and support secure protocols

- »» Services and protocols (e.g., IPSec, TLS, S/MIME, DKIM)
- »» Common use cases
- »» Limitations and vulnerabilities

### 5.4 Understand Public Key Infrastructure (PKI) systems

- » Fundamental key management concepts (e.g., key rotation, key composition, key creation, exchange, revocation, escrow)
- » Web of Trust (WOT) (e.g., PGP, GPG)

## Domain 6: Network and Communications Security

### 6.1 Understand and apply fundamental concepts of networking

- » OSI and TCP/IP models
- » Network topographies (e.g., ring, star, bus, mesh, tree)
- » Network relationships (e.g., peer to peer, client server)
- » Transmission media types (e.g., fiber, wired, wireless)
- » Commonly used ports and protocols

6.2 Understand network attacks and countermeasures (e.g., DDoS, man-in-the-middle, DNSpoisoning)

6.3 Manage network access controls

- » Network access control and monitoring (e.g., remediation, quarantine, admission)
- » Network access control standards and protocols (e.g., IEEE 802.1X, Radius, TACACS)
- » Remote access operation and configuration (e.g., thin client, SSL VPN, IPSec VPN, telework)

6.4 Manage network security

- » Logical and physical placement of network devices (e.g., inline, passive)
- » Segmentation (e.g., physical/logical, data/control plane, VLAN, ACLs)
- » Secure device management

6.5 Operate and configure network-based security devices

- » Firewalls and proxies (e.g., filtering methods)
- » Network intrusion detection/prevention systems
- » Routers and switches
- » Traffic-shaping devices (e.g., WAN optimization, load balancing)

6.6 Operate and configure wireless technologies (e.g., bluetooth, NFC, WiFi)

- » Transmission security
- » Wireless security devices (e.g., WIPS, WIDS)

## Domain 7:

# Systems and Application Security

7.1 Identify and analyze malicious code and activity

- » Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, and remote access trojans)
- » Malicious code countermeasures (e.g., scanners, anti-malware, code signing, sandboxing)
- » Malicious activity (e.g., insider threat, data theft, DDoS, botnet)
- » Malicious activity countermeasures (e.g., user awareness, system hardening, patching, sandboxing, isolation)

7.2 Implement and operate endpoint device security

- » HIDS
- » Host-based firewalls
- » Application white listing
- » Endpoint encryption
- » Trusted Platform Module (TPM)
- » Mobile Device Management (MDM) (e.g., COPE, BYOD)
- » Secure browsing (e.g., sandbox)

7.3 Operate and configure cloud security

- » Deployment models (e.g., public, private, hybrid, community)
- » Service models (e.g., IaaS, PaaS and SaaS)
- » Virtualization (e.g., hypervisor)
- » Legal and regulatory concerns (e.g., privacy, surveillance, data ownership, jurisdiction, eDiscovery)
- » Data storage and transmission (e.g., archiving, recovery, resilience)
- » Third party/outsourcing requirements (e.g., SLA, data portability, data destruction, auditing)
- » Shared responsibility model

7.4 Operate and secure virtual environments

- » Software-defined networking
- » Hypervisor
- » Virtual appliances
- » Continuity and resilience
- » Attacks and countermeasures
- » Shared storage