INFOSECTRAIN

SSCP

Certification Training

Systems Security Certified Practitioner

INFOSECTRAIN

Course Highlights

- **40-Hour LIVE** Instructor-led Training
- Highly Interactive and Dynamic Sessions
- Career Guidance & Mentorship
- Hands-on Labs
- 98% Exam Pass Rate
- Extended Post Training Support
- Learn with Real-world Scenarios
- Learn from Industry Experts
- Access to Recorded Sessions

INFOSECTRAIN

About Course

The SSCP Certification Training course equips learners with the knowledge and skills required to implement, monitor, and administer IT infrastructure using cybersecurity best practices and policies.

Participants will learn to manage security operations, implement access controls, conduct risk assessments, respond to incidents, apply cryptography, secure networks, and protect systems and applications. The course also emphasizes hands-on experience through practical exercises, enabling learners to document and maintain security controls, manage identity lifecycles, operate security platforms, and respond to incidents effectively. By the end of the training, participants will be prepared to secure various IT environments and meet the SSCP certification requirements.

INFOSECTRAIN

Course Objectives

- Manage and administer security policies, procedures, and controls to protect information assets.
- Establish and manage access control mechanisms to ensure authorized access to sensitive information.
- Identify, assess, and monitor risks to information systems and develop mitigation strategies.
- Address and resolve security incidents efficiently to reduce damage and promptly restore services.
- Apply cryptographic principles to protect information confidentiality, integrity, and availability.
- Secure network infrastructure and communication channels against threats.
- Secure systems and applications by implementing best practices against vulnerabilities and attacks.

INFOSECTRAIN

Target Audience

- Database Administrators
- Network Security Engineers
- Security Administrators
- Security Analysts
- Security Consultants/Specialists
- Systems Administrators
- Systems Engineers
- Systems/Network Analysts
- Health Information Managers
- Practice Managers

Pre-requisites

- Basic IT Knowledge
- Having a degree or certification in fields like information security, computer science, or a related area is advantageous, though not strictly mandatory.
- At least one year of cumulative work experience in one or more of the seven domains of the SSCP Common Body of Knowledge (CBK).

INFOSECTRAIN

Exam Information

Exam Format	Multiple-choice Questions
Number of Questions	150 Questions
Exam Duration	4 Hours
Passing Score	700 out of 1000
Exam Language	English, Japanese, and Spanish
Testing Center	Pearson VUE

INFOSECTRAIN

Course Content

Domain 1. Security Operations and Administration (16%)

- 1.1 – Comply with codes of ethics
  - ISC2 Code of Ethics
  - Organizational code of ethics
- 1.2 – Understand security concepts
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Privacy
  - Non-repudiation
  - Least privilege
  - Segregation of Duties (SoD)
- 1.3 – Identify and implement security controls
  - Technical controls (e.g., session timeout, password aging)
  - Physical controls (e.g., mantraps, cameras, locks)
  - Administrative controls (e.g., security policies, standards, procedures, baselines)
  - Assessing compliance
  - Periodic audit and review

- 1.4 – Document and maintain functional security controls
  - Deterrent controls
  - Preventative controls
  - Detective controls
  - Corrective controls
  - Compensating controls
- 1.5 – Participate in asset management lifecycle (hardware, software and data)
  - Process, planning, design and initiation
  - Development/Acquisition
  - Inventory and licensing
  - Implementation/Assessment
  - Operation/Maintenance
  - Archiving and retention requirements
  - Disposal and destruction
- 1.6 – Participate in change management lifecycle
  - Change Management (e.g., roles, responsibilities, processes)
  - Security impact analysis
  - Configuration Management (CM)
- 1.7 – Participate in implementing security awareness and training (e.g., social engineering/phishing)
- 1.8 – Collaborate with physical security operations (e.g., data center assessment, badging)

Domain 2. Access Controls (15%)

- 2.1 – Implement and maintain authentication methods
  - Single/Multi-Factor Authentication (MFA)
  - Single Sign-On (SSO) (e.g., Active Directory Federation Services (ADFS), OpenID connect)
  - Device authentication
  - Federated access (e.g., Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))
- 2.2 – Support internetwork trust architectures
  - Trust relationships (e.g., 1-way, 2-way, transitive, zero)
  - Internet, intranet and extranet
  - Third-party connections
- 2.3 – Participate in the identity management lifecycle
  - Authorization
  - Proofing
  - Provisioning/De-provisioning
  - Maintenance
  - Entitlement
  - Identity and Access Management (IAM) systems
- 2.4 – Understand and apply access controls
  - Mandatory
  - Discretionary
  - Role-based (e.g., attribute-, subject-, object-based)
  - Rule-based

Domain 3. Risk Identification, Monitoring, and Analysis (15%)

- 3.1 – Understand the risk management process
  - Risk visibility and reporting (e.g., risk register, Common Vulnerability Scoring (CVSS), sharing threat intelligence/Indicators of Compromise (IOC))
  - Risk management concepts (e.g., threat modeling, impact assessments)
  - Risk management frameworks
  - Risk tolerance (e.g., appetite)
  - Risk treatment (e.g., acceptance, transference, mitigation, or avoidance)
- 3.2 – Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
- 3.3 – Participate in security assessment and vulnerability management activities
  - Security testing
  - Risk review (e.g., internal, supplier, architecture)
  - Vulnerability management lifecycle
- 3.4 – Operate and monitor security platforms (e.g., continuous monitoring)
  - Source systems (e.g., applications, security appliances, network devices, and hosts)
  - Events of interest (e.g., anomalies, intrusions, unauthorized changes, compliance monitoring)
  - Log management
  - Event aggregation and correlation
- 3.5 – Analyze monitoring results
  - Security baselines and anomalies
  - Visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)
  - Event data analysis
  - Document and communicate findings (e.g., escalation)

Domain 4. Incident Response and Recovery (14%)

- 4.1 – Support incident lifecycle, e.g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO)
  - Preparation
  - Detection, analysis and escalation
  - Containment
  - Eradication
  - Recovery
  - Lessons learned/implementation of new countermeasure
- 4.2 – Understand and support forensic investigations
  - Legal (e.g., civil, criminal, administrative) and ethical principles
  - Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)
  - Reporting of analysis
- 4.3 – Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
  - Emergency response plans and procedures (e.g., pandemic, natural disaster, information system contingency, crisis management)
  - Interim or alternate processing strategies
  - Restoration planning
  - Backup and redundancy implementation
  - Testing and drills

Domain 5. Cryptography (9%)

- 5.1 – Understand cryptography
  - Confidentiality
  - Integrity and authenticity
  - Data sensitivity (e.g., Personally Identifiable Information (PII), Intellectual Property (IP), Protected Health Information (PHI))
  - Regulatory and industry best practices (e.g., International Organization for Standardization (ISO), Payment Card Industry Data Security Standards (PCI-DSS))
- 5.2 – Apply cryptography concepts
  - Hashing
  - Salting
  - Symmetric/Asymmetric encryption/Elliptic Curve Cryptography (ECC)
  - Non-repudiation (e.g., digital signatures/certificates, Hash-based Message Authentication Code (HMAC), audit trails)
  - Strength of encryption algorithms and keys (e.g., Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA), 256-, 512-, 1024-, 2048-bit keys)
  - Cryptographic attacks, cryptanalysis, and countermeasures (e.g., quantum computing)

- 5.3 – Understand and implement secure protocols
  - Services and protocols
  - Common use cases
  - Limitations and vulnerabilities
- 5.4 – Understand Public Key Infrastructure (PKI)
  - Fundamental key management concepts (e.g., storage, rotation, composition, generation, destruction, exchange, revocation, escrow)
  - Web of Trust (WOT)

Domain 6. Network and Communications Security (16%)

- 6.1 – Understand and apply fundamental concepts of networking
  - Open Systems Interconnection (OSI) and Transmission Control
  - Protocol/Internet Protocol (TCP/IP) models
  - Network topologies
  - Network relationships (e.g., Peer-to-Peer (P2P), client server)
  - Transmission media types (e.g., wired, wireless)
  - Software-Defined Networking (SDN) (e.g., Software-Defined Wide Area Network (SD-WAN), network virtualization, automation)
  - Commonly used ports and protocols
- 6.2 – Understand network attacks
  - Distributed Denial of Service (DDoS)
  - Man-in-the-Middle (MITM)
  - Domain Name System (DNS) poisoning
  - Countermeasures (e.g., Content Delivery Networks (CDN)
- 6.3 – Manage network access controls
  - Network access controls, standards and protocols (e.g., Remote Authentication Dial-In User Service (RADIUS), Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Terminal Access Controller Access-Control System Plus (TACACS+))
  - Remote access operation and configuration (e.g., thin client, Virtual Private Network (VPN))

- 6.4 – Manage network security
  - Logical and physical network devices placement (e.g., passive, inline, virtual)
  - Segmentation (e.g., data/control plane, physical/logical, Virtual Local Area Network (VLAN), Access Control List (ACL), firewall zones, micro-segmentation)
  - Secure device management
- 6.5 – Operate and configure network-based security devices
  - Firewalls and proxies (e.g., filtering methods, Web Application Firewalls (WAF))
  - Network intrusion detection/prevention systems
  - Routers and switches
  - Traffic-shaping devices (e.g., Wide Area Network (WAN) optimization, load balancing)
- 6.6 – Secure wireless communications
  - Technologies (e.g., cellular network, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
  - Authentication and encryption protocols (e.g., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP))
  - Internet of Things (IoT)

Domain 7. Systems and Application Security (15%)

- 7.1 – Identify and analyze malicious code and activity
  - Malware (e.g., spyware, scareware, ransomware, trojans, viruses, worms, rootkits, trapdoors, backdoors, fileless)
  - Malware countermeasures (e.g., scanners, anti-malware, code signing)
  - Malicious activity (e.g., data theft, Distributed Denial of Service (DDoS), insider threat, botnet, zero-day exploits, web-based attacks, Advanced Persistent Threat (APT))
  - Malicious activity countermeasures (e.g., user awareness, patching, sandboxing, system hardening, isolation, Data Loss Prevention (DLP))
- 7.2 – Implement and operate endpoint device security
  - Host-based firewalls
  - Application whitelisting
  - Host-based Intrusion Prevention System (HIPS)
  - Endpoint encryption (e.g., whole disk encryption)
  - Trusted Platform Module (TPM)
  - Secure browsing
  - Endpoint Detection and Response (EDR)
- 7.3 – Administer Mobile Device Management (MDM)
  - Provisioning techniques (e.g., Corporate-Owned Personally Enabled (COPE), Bring Your Own Device (BYOD))
  - Containerization
  - Encryption
  - Mobile application management (MAM)

- 7.4 – Understand and configure cloud security
  - Deployment models (e.g., private, public, hybrid, community)
  - Service models (e.g., Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS))
  - Virtualization
  - Legal and regulatory concerns (e.g., privacy, jurisdiction, surveillance, data ownership, eDiscovery)
  - Data storage, processing, and transmission (e.g., recovery, resilience, archiving)
  - Third-party/outsourcing requirements (e.g., data portability, Service-Level Agreement (SLA), data destruction, auditing)
  - Shared responsibility model
- 7.5 – Operate and maintain secure virtual environments
  - Containers
  - Hypervisor
  - Virtual appliances
  - Continuity and resilience
  - Attacks and countermeasures
  - Shared storage

INFOSECTRAIN
Educate. Excel. Empower.

www.infosectrain.com | sales@infosectrain.com