

SSCP

Systems Security
Certified Practitioner



Systems Security Certified Practitioner

SSCP or the 'Systems Security Certified Practitioner from (ISC)2 shows that you have the advanced technical skills and knowledge to implement, monitor, and administer IT infrastructure using best practices, policies, and procedures laid out by (ISC)2



Overview

The SSCP certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. It provides industry-leading confirmation of a practitioner's ability to implement, monitor, and administer IT infrastructure by information security policies and procedures that ensure data confidentiality, integrity, and availability.

The SSCP indicates a practitioner's technical ability to tackle the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more.

SSCP complies with the stringent requirements of ANSI/ISO/IEC Standard 17024.

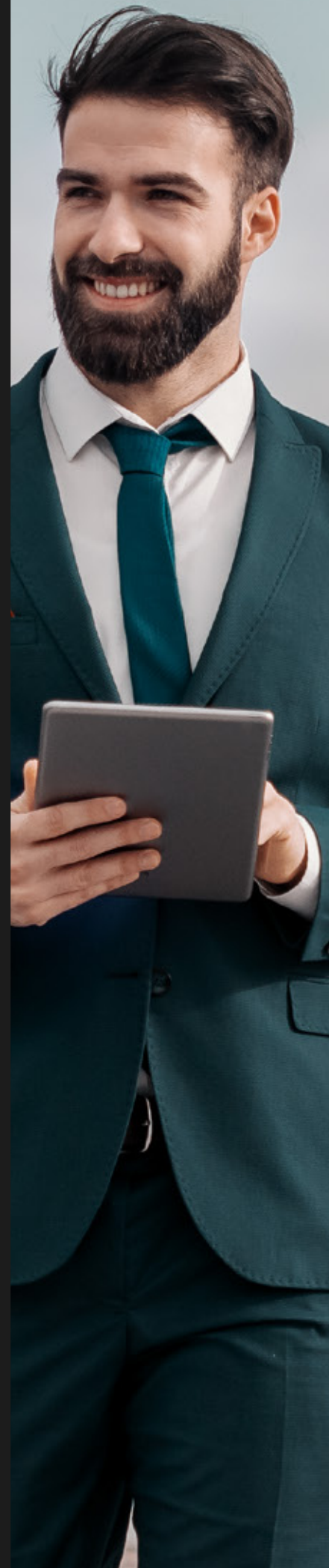
Why attend the **SSCP** certification training with InfoSec Train?

Here are some compelling reasons as to why you should choose the 'SSCP Online Certification Training Course' from InfoSec Train:

- Experienced and certified instructors
- Good course content
- Seamlessly delivery of course content
- Understanding instructors
- Small class size to focus on each student's strengths and weaknesses
- We are motivated to help you pass the exam!

Target Audience

- Database Administrator
- Network Security Engineer
- Security Administrator
- Security Analyst
- Security Consultant/Specialist
- Systems Administrator
- Systems Engineer
- Systems/Network Analyst



Pre- Requisite

To be SSCP certified, a candidate should pass the exam and have a minimum of 1 year of cumulative paid full-time work experience in one or more of the seven domains of the SSCP CBK.

Exam Information

Duration	3 hours
Number of Questions	125
Question format	Multiple Choice
Passing grade	700 out of 1000
Languages available	English, Japanese, and Brazilian Portuguese

Why Infosec Train?



Certified &
Experienced Instructor



Flexible Schedule



Access to the
recorded
sessions



Post Training
Support



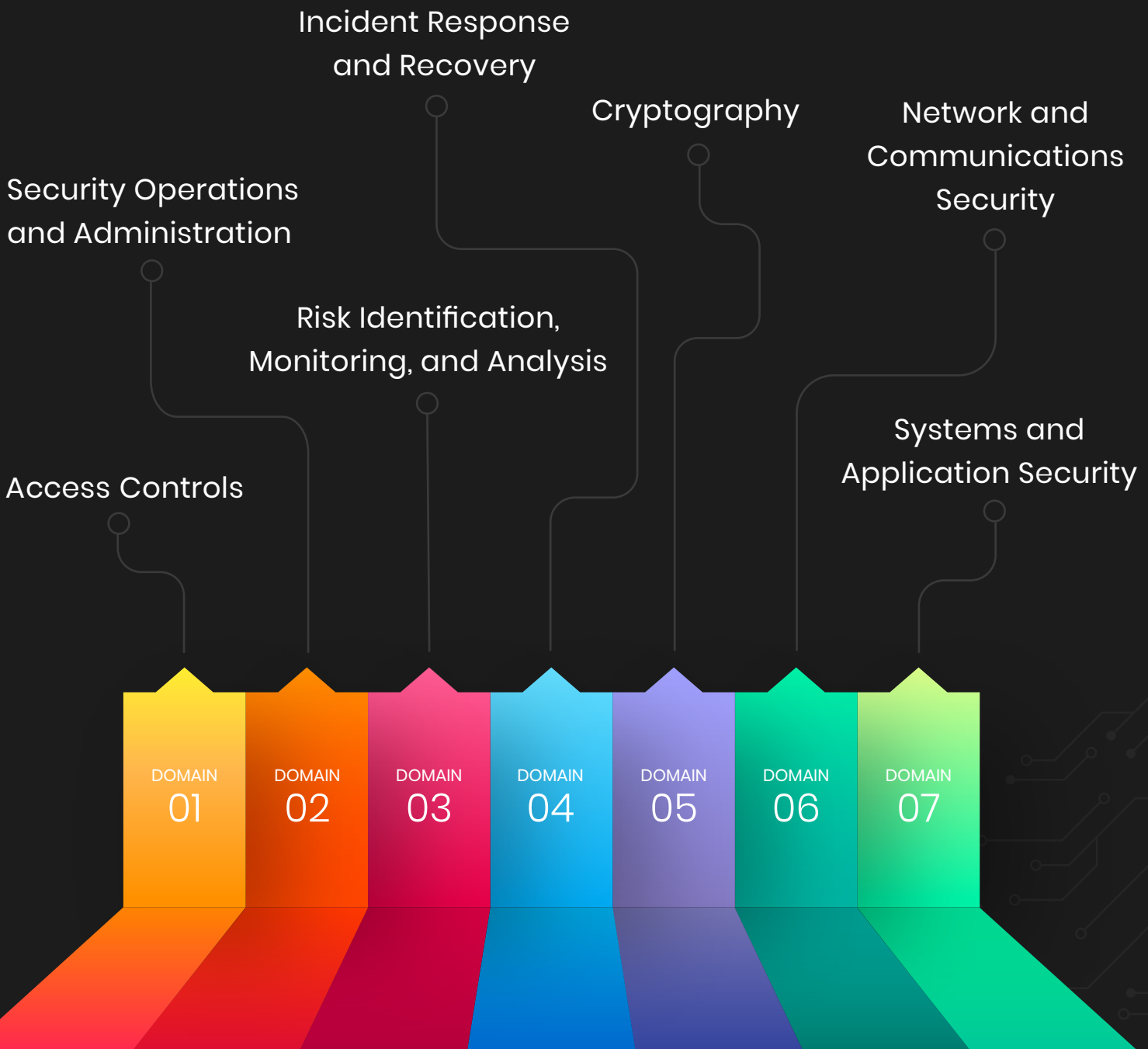
Tailor Made Training



Telegram
Discussion
Group

SSCP Domains

The seven domains in SSCP include



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)² Code of Ethics
- Organizational code of ethics

2.2 Understand security concepts

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

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

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

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

7.3 Operate and configure cloud security

7.4 Operate and secure virtual environments



www.infosectrain.com | sales@infosectrain.com