SPRINTZEAL
Empowering Professionals

SSCP – SYSTEMS SECURITY CERTIFIED PRACTITIONER

Course Agenda

Course Overview:

Program Overview

Sprintzeal provides training for individuals to become Systems Security Certified Practitioner (SSCP) certified, preparing them for the exam and identifying areas for improvement. SSCP certifications can increase earning potential, with professionals earning between $40,000 and $88,000 per year. They also meet Department of Defense security certification requirements and are required by private sector organizations. SSCP certification demonstrates advanced technical skills and knowledge in IT infrastructure, advancing career prospects, and joining a supportive community.

This course is ideal for

SSCP is suitable for IT administrators, managers, directors, and network security professionals in charge of the hands-on operational security of their organization's key assets, including those in the following positions:

- Systems Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator
- Health Information Manager
- Practice Manager

Key Learning

- Understanding the principles and frameworks of GRC.
- Proficiency in risk identification and assessment.
- Developing and implementing effective compliance programs.
- Establishing robust governance structures.
- Conducting internal and external audits.
- Integrating risk management into decision-making processes.
- Navigating complex regulatory environments.
- Enhancing communication skills for GRC reporting

Skills You Will Acquire:

- Systems Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator
- Health Information Manager
- Practice Manager

SPRINTZEAL
Empowering Professionals

Module 1: Security Operations and Administration

Module 1.1 - Comply with codes of ethics

- ISC2 Code of Ethics
- Organizational code of ethics

Module 1.2 - Understand security concepts

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy
- Non-repudiation
- Least privilege
- Segregation of duties (SoD)

Module 1.3 - Identify and implement security controls

- Technical controls (e.j., 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

Module 1.4 - Document and maintain functional security controls

- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Compensating controls

Module 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

Module 1.6 - Participate in change management lifecycle

- Change management (e.g., roles, responsibilities, processes)
- Security impact analysis
- Configuration management (CM)

Module 1.7 - Participate in implementing security awareness and training (e.g., social engineering/phishing)

Module 1.8 - Collaborate with physical security operations (e.g., data center assessment, badging)

SPRINTZEAL
Empowering Professionals

Module 2: Access Controls

Module 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))

Module 2.2 - Support internetwork trust architectures

- Trust relationships (e.g., 1-way, 2-way, transitive, zero)
- Internet, intranet and extranet
- Third-party connections

Module 2.3 - Participate in the identity management lifecycle

- Authorization
- Proofing
- Provisioning/De-provisioning
- Maintenance
- Entitlement
- Identity and access management (IAM) systems

Module 2.4 - Understand and apply access controls

- Mandatory
- Discretionary
- Role-based (e.g., attribute-, subject-, object-based)
- Rule-based

Module 3: Risk Identification, Monitoring and Analysis

Module 3.1 - Understand the risk management process

- Risk visibility and reporting (e.g., risk register, sharing threat intelligence/Indicators of Compromise (IOC), Common Vulnerability Scoring (CVSS))
- Risk management concepts (e.g., impact assessments, threat modelling)
- Risk management frameworks
- Risk tolerance (e.g., appetite)
- Risk treatment (e.g., accept, transfer, mitigate, avoid)

Module 3.2 - Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)

Module 3.3 - Participate in security assessment and vulnerability management activities

- ·Security testing
- ·Risk review (e.g., internal, supplier, architecture)
- ·Vulnerability management lifecycle

Module 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

Module 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)

Module 4: Incident Response and Recovery

Module 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

Module 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

Module 4.3 - Understand and support business continuity plan (BCP) and disaster recovery plan (DRP)

- Emergency response plans and procedures (e.g., information system contingency, pandemic, natural disaster, crisis management)
- Interim or alternate processing strategies
- Restoration planning
- Backup and redundancy implementation
- Testing and drills

Module 5: Cryptography

Module 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 practice (e.g., Payment Card Industry Data Security Standards (PCI-DSS), International Organization for Standardization (ISO))

Module 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)

Module 5.3 - Understand and implement secure protocols

- Services and protocols
- Common use cases
- Limitations and vulnerabilities

Module 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)

SPRINTZEAL
Empowering Professionals

Module 6: Network and Communication Security

Module 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

Module 6.2 - Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name System (DNS) poisoning) and countermeasures (e.g., content delivery networks (CDN))

Module 6.3 - Manage network access controls

- Network access controls, standards and protocols (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+))
- Remote access operation and configuration (e.g., thin client, virtual private network (VPN))

Module 6.4 - Manage network security

- Logical and physical placement of network devices (e.g., inline, passive, virtual)
- Segmentation (e.g., physical/logical, data/control plane, virtual local area network (VLAN), access control list (ACL), firewall zones, micro-segmentation)
- Secure device management

Module 6.5 - Operate and configure network-based security devices

- Firewalls and proxies (e.g., filtering methods, web application firewalls (WAF)) Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Network intrusion detection/prevention systems
- Routers and switches
- Traffic-shaping devices (e.g., wide area network (WAN) optimization, load balancing)

Module 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)

Module 7: Systems and Application Security

Module 7.1 - Identify and analyze malicious code and activity

- Malware (e.g., rootkits, spyware, scareware, ransomware, trojans, virus, worms, trapdoors, backdoors, fileless)
- Malware countermeasures (e.g., scanners, anti-malware, code signing)
- Malicious activity (e.g., insider threat, data theft, distributed denial of service (DDoS), botnet, zero-day exploits, web-based attacks, advanced persistent threat (APT))
- Malicious activity countermeasures (e.g., user awareness, system hardening, patching, sandboxing, isolation, data loss prevention (DLP))

Module 7.2 - Implement and operate endpoint device security

- Host-based intrusion prevention system (HIPS)
- Host-based firewalls
- Application white listing
- Endpoint encryption (e.g., whole disk encryption)
- Trusted Platform Module (TPM)
- Secure browsing
- Endpoint Detection and Response (EDR)

Module 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)

Module 7.4 - Understand and configure cloud security

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

Module 7.5 - Operate and maintain secure virtual environments

- Hypervisor
- Virtual appliances
- Containers
- Continuity and resilience
- Attacks and countermeasures
- Shared storage

About Sprintzeal's Systems Security Certified Practitioner (SSCP)

·Sprintzeal provides SSCP certification training, which can boost earning potential and meet Department of Defense security requirements. This certification is highly valued by private-sector organizations and showcases advanced IT infrastructure skills. The course covers topics like security operations, access controls, risk identification, incident response, cryptography, network security, and systems and application security.