

KOENIG SOLUTIONS • COURSE OUTLINE

Systems Security Certified Practitioner (SSCP)

Learn to implement, monitor and administer IT security controls across access, networks, cryptography and incident response.

5 Days

40 HOURS

7

MODULES

133

TOPICS

COURSE OVERVIEW

The SSCP course is a foundational training program designed for IT professionals seeking to showcase their knowledge in the field of security. This course equips learners with the skills needed to implement, monitor, and administer IT infrastructure in accordance with established cybersecurity policies and procedures that ensure data confidentiality, integrity, and availability. The training covers various aspects of security operations, including Access controls, Risk identification, incident response, Cryptography, network security, and Systems and application security. By completing the SSCP Certification, individuals demonstrate their technical ability to tackle operational security challenges and adhere to best practices. It is an excellent stepping stone for those aspiring to build a career in cybersecurity and provides a comprehensive understanding necessary to protect organizations against cyber threats.

Who Should Attend

The Systems Security Certified Practitioner (SSCP) course is designed for IT professionals seeking to enhance their cybersecurity skills and knowledge.

IT Security Analysts

Network Security Engineers

Systems Administrators

Security Administrators

Security Consultants/Specialists

IT Auditors

Information Security Officers

IT/Security Practitioners

Systems Analysts

Database Administrators

Government or military IT professionals and contractors

Incident Response Handlers

Risk/Threat/Vulnerability Analysts

Security Operations Center (SOC) staff

Compliance Personnel dealing with information security requirements

Professionals aiming for a career transition into cybersecurity

Technical Support Engineers looking to specialize in security

Professionals preparing for the ISC² SSCP certification exam

LEARNING OBJECTIVES

- Implement authentication methods and identity management lifecycles
- Apply access control models including mandatory and role-based
- Document and maintain security controls and asset management processes
- Analyse risk management frameworks and security assessment results
- Operate monitoring systems and interpret event data
- Support incident response, forensic investigation and recovery planning
- Explain cryptographic concepts, protocols and key management
- Configure network security devices and wireless technologies

7 Modules, 133 Topics

01

Access Controls

IMPLEMENT AND MAINTAIN AUTHENTICATION METHODS

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

SUPPORT INTERNETWORK TRUST ARCHITECTURES

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

PARTICIPATE IN THE IDENTITY MANAGEMENT LIFECYCLE

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

IMPLEMENT ACCESS CONTROLS

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

02

Security Operations and Administration

COMPLY WITH CODES OF ETHICS

- (ISC)² Code of Ethics
- Organizational code of ethics

UNDERSTAND SECURITY CONCEPTS

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

DOCUMENT, IMPLEMENT, AND MAINTAIN FUNCTIONAL SECURITY CONTROLS

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

PARTICIPATE IN ASSET MANAGEMENT

- Lifecycle (hardware, software, and data)
- Hardware inventory
- Software inventory and licensing
- Data storage

Security Operations and Administration (continued)

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

PARTICIPATE IN CHANGE MANAGEMENT

- Execute change management process
- Identify security impact
- Testing/implementing patches, fixes, and updates (e.g., operating system, applications, SDLC)
- Participate in security awareness and training

03

Risk Identification, Monitoring, and Analysis

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)

PERFORM SECURITY ASSESSMENT ACTIVITIES

- Participate in security testing
- Interpretation and reporting of scanning and testing results
- Remediation validation
- Audit finding remediation

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)

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)

04

Incident Response and Recovery

SUPPORT INCIDENT LIFECYCLE

- Preparation
- Detection, analysis, and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/implementation of new countermeasure

UNDERSTAND AND SUPPORT FORENSIC INVESTIGATIONS

- Legal and ethical principles
- Evidence handling (e.g., first responder, triage, chain of custody, preservation of scene)

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

05

Cryptography

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

UNDERSTAND REASONS AND REQUIREMENTS FOR CRYPTOGRAPHY

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

UNDERSTAND AND SUPPORT SECURE PROTOCOLS

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

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)

Network and Communications Security

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

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)

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

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)

OPERATE AND CONFIGURE WIRELESS TECHNOLOGIES (E.G., BLUETOOTH, NFC, WIFI)

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

Systems and Application Security

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)

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)

Systems and Application Security (continued)

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

OPERATE AND SECURE VIRTUAL ENVIRONMENTS

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

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Hands-on exercises throughout the course
- Delivery by certified instructors and subject matter experts
- Course completion certificate from Koenig

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com