



Systems Security Certified Practitioner (SSCP)

Course Description

The Systems Security Certified Practitioner (SSCP) certification is a global IT security certification. The SSCP recognizes systems security practitioners who have the knowledge, skills. It shows you have the skills to implement, monitor and administer IT infrastructure using information security policies and procedures — ensuring the confidentiality, integrity and availability of data.

Course Duration:

5 days

Required Experience:

Candidates must have a minimum of one-year cumulative full-time work experience in one or more of the seven domains of the current ISC2 SSCP Exam Outline. Earning a post-secondary degree (bachelors or masters) in Computer Science, Information Technology (IT) or related fields may satisfy up to one year of the required experience. Part-time work and internships may also count towards the experience requirement.

Experience hours calculation:

- Full-Time Experience: Your work experience is accrued monthly. Experience must be accrued at a minimum of 35 hours/week for four weeks in order to achieve one month of work experience.
- Part-Time Experience: Your part-time experience cannot be less than 20 hours a week.
 - 1040 hours of part-time = 6 months of full-time experience
 - 2080 hours of part-time = 12 months full-time experience
- Internship: Internship, paid or unpaid, is acceptable for the certification experience requirement. You will need primary source documentation on company/organization/academic institution letterhead confirming your position and detailed experience.

Course Outline:

- Security Operations and Administration
- Access Controls
- Risk Identification, Monitoring and Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

Who Should Attend

The SSCP is designed for cybersecurity and IT/ICT professionals who have hands-on responsibility for designing, implementing and maintaining cyber, information, software and infrastructure security, whether in a cyber-dedicated role or as part of their day-to-day IT/ICT position. Roles include:

- Network Security Engineer
- IT/Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator
- Individuals operating in a security operations center (SOC) environment performing the role of incident handler, SIEM analyst, forensics specialist, threat intel researcher, etc.