SSCP®

Systems Security Certified Practitioner

Descrição do Exame de Certificação

Data efetiva: Novembro de 2021

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

Sobre o SSCP

A Systems Security Certified Practitioner (SSCP) é a certificação ideal para aqueles com habilidades técnicas comprovadas e conhecimento prático e útil de segurança em funções operacionais de TI. Fornece a confirmação da capacidade de um profissional de implementar, monitorar e administrar a infraestrutura de TI de acordo com as políticas e procedimentos de segurança da informação que garantem a confidencialidade, integridade e disponibilidade dos dados.

O amplo espectro de tópicos incluídos no Corpo Comum de Conhecimento do SSCP (CBK®) garante sua relevância em todas as disciplinas no campo da segurança da informação. Os candidatos aprovados são competentes nos seguintes sete domínios:

- Operações e Administração de Segurança
- Controles de Acesso
- Identificação, Monitoramento e Análise de Risco
- Recuperação e Resposta de Incidentes
- Criptografia
- Segurança de Rede e Comunicações
- Segurança de Sistemas e Aplicações

Requisitos de Experiência

Os candidatos devem ter um mínimo de 1 ano de experiência profissional acumulada em 1 ou mais dos 7 domínios do CBK do SSCP. Um caminho de um ano de pré-requisito será concedido para candidatos que receberam um diploma (bacharelado ou mestrado) em um programa de segurança cibernética.

Um candidato que não tem a experiência necessária para tornar-se um SSCP pode se tornar um Associado do (ISC)² passando com sucesso no exame SSCP. O Associado do (ISC)² terá então 2 anos para obter a experiência necessária de um ano. Você pode aprender mais sobre os requerimentos de experiência do SSCP e como contabilizar trabalho de meio período e estágios em www.isc2.org/Certifications/SSCP/experience-requirements.

Acreditação

O SSCP está em conformidade com os requerimentos rigorosos da norma ANSI/ISO/IEC 17024.

Análise de Tarefa de Trabalho (JTA)

(ISC)² tem a obrigação para com seus membros de manter a relevância do SSCP. Realizado em intervalos regulares, a Análise da Tarefa de Trabalho (JTA) é um processo metódico e crítico para determinar as tarefas que são executadas por profissionais de segurança que estão engajados na profissão definida pelo SSCP. Os resultados da JTA são usados para atualizar o exame. Este processo garante que os candidatos sejam testados nas áreas de tópico relevantes para as funções e responsabilidades dos atuais profissionais de segurança da informação.

Informações do Exame SSCP

Duração do Exame	3 horas
Número de itens	125
Formato do item	Múltipla escolha
Nota de aprovação	700 de 1000 pontos
Disponibilidade do exame	Inglês, Japonês e Português Brasileiro
Centro de Testes	Centro de testes Pearson VUE

Pesos do exame SSCP

Domínios	Peso
1. Operações e Administração de Segurança	16%
2. Controles de Acesso	15%
3. Identificação, Monitoramento e Análise de Riscos	15%
4. Recuperação e Resposta de Incidentes	14%
5. Criptografia	9%
6. Segurança de Rede e Comunicações	16%
7. Segurança de sistemas e aplicativos	15%
Total:	**100%**

Domínio 1:
Operações e Administração de Segurança

1.1 Cumprir o código de ética

» Código de Ética (ISC)²
» Código de Ética Organizacional

1.2 Comprender os conceitos de Segurança

» Confidencialidade
» Integridade
» Disponibilidade
» Prestação de contas
» Privacidade
» Não repúdio
» Menor privilégio
» Segregação de funções (SoD)

1.3 Identificar e implementar controles de segurança

» Controles técnicos (por exemplo, tempo limite da sessão, expiração de senha)
» Controles físicos (por exemplo, clausuras, câmeras, fechaduras)
» Controles administrativos (por exemplo, políticas de segurança, padrões, procedimentos, referências)
» Avaliando conformidade
» Auditoria e revisão periódica

1.4 Documentar e manter controles de segurança funcionais

» Controles de dissuasão
» Controles preventivos
» Controles detectivos
» Controles corretivos
» Controles de compensação

1.5 Participar do ciclo de vida do gerenciamento de ativos (hardware, software e dados)

» Processo, planejamento, desenho e iniciação
» Desenvolvimento/Aquisição
» Inventário e licenciamento
» Implementação/Avaliação
» Operação/Manutenção
» Requerimentos de arquivamento e retenção
» Eliminação e destruição

1.6 Participação no ciclo de vida do gerenciamento de mudanças

» Gerenciamento de mudança (por exemplo, funções, responsabilidades, processos)
» Análise de impacto de segurança
» Gerenciamento de configuração (CM)

1.7 Participar da implementação de conscientização e treinamento de segurança (por exemplo, engenharia social/phishing)

1.8 Colaborar com as operações de segurança física (p. ex., avaliação do centro de dados, crachá)

Domínio 2:
Controles de Acesso

2.1 Implementar e manter métodos de autenticação

» Autenticação de Fator Único/Multifator (MFA)

» Logon Único (SSO) (por exemplo, Serviços de Federação do Active Directory (ADFS), OpenID Connect)

» Autenticação de dispositivo

» Acesso federado (por exemplo, Autorização Aberta 2 (OAuth2),Linguagem de Marcação para Asserções de Segurança (SAML))

2.2 Suporte às arquiteturas de confiança entre redes

» Relações de confiança (p. ex., unilateral, bidirecional, transitivo, zero)

» Internet, intranet e extranet

» Conexões de terceiros

2.3 Participar do ciclo de vida do gerenciamento de identidade

» Autorização

» Verificação

» Provisionamento / Desprovisionamento

» Manutenção

» Direito

» Sistemas de gerenciamento de identidade e acesso (IAM)

2.4 Compreender e aplicar controles de acesso

» Mandatório

» Discricionário

» Com base na função (por exemplo, com base em atributo, sujeito, objeto)

» Com base na função

Domínio 3:
Identificação, Monitoramento e Análise de Risco

3.1 Compreender o processo de gerenciamento de risco

» Visibilidade e relatórios de risco (p. ex., registro de risco, compartilhamento de inteligência de ameaças/indicadores de compromisso (IOC), Sistema de pontuação de vulnerabilidade comum (CVSS))

» Conceitos de gerenciamento de risco (por exemplo, avaliações de impacto, modelagem de ameaças)

» Estruturas de gerenciamento de risco (por exemplo, Organização Internacional de Padronização (ISO), Instituto Nacional de Padrões e Tecnologia (NIST))

» Tolerância ao risco (por exemplo, apetite)

» Tratamento do risco (por exemplo, aceitar, transferir, mitigar, evitar, ignorar)

3.2 Compreender questões legais e regulatórias (p. ex., jurisdição, limitações, privacidade)

3.3 Participar de atividades de avaliação de segurança e gerenciamento de vulnerabilidade

» Testes de segurança

» Revisão de risco (p. ex., interno, fornecedor, arquitetura)

» Ciclo de vida de gerenciamento de vulnerabilidade

3.4 Operar e monitorar plataformas de segurança (p. ex., monitoramento contínuo)

» Sistemas de origem (p. ex., aplicações, dispositivos de segurança, dispositivos de rede e hospedagem)

» Eventos de interesse (p. ex., anomalias, intrusões, alterações não autorizadas, monitoramento de conformidade)

» Gerenciamento de log

» Agregação e correlação de eventos

3.5 Analisar os resultados do monitoramento

» Referências de segurança e anomalias

» Visualizações, métricas e tendências (p. ex., notificações, dashboards, cronogramas)

» Análise de dados de eventos

» Documentar e comunicar as descobertas (p. ex., escalação)

Domínio 4:
Recuperação e Resposta de Incidentes

4.1 Suporte ao ciclo de vida do incidente (por exemplo, Instituto Nacional de Padrões e Tecnologia (NIST), Organização Internacional de Padronização (ISO))

» Preparação

» Detecção, análise e escalonamento

» Contenção

» Erradicação

» Recuperação

» Lições aprendidas/Implementação de nova contramedida

4.2 Compreender e apoiar investigações forenses

» Princípios legais (p. ex., civil, criminal, administrativo) e éticos

» Tratamento de evidências (por exemplo, primeiro atendente, triagem, cadeia de custódia, preservação da cena)

» Relatório de análise

4.3 Compreender e apoiar as atividades do plano de continuidade de negócios (BCP) e do plano de recuperação de desastres (DRP)

» Planos e procedimentos de resposta a emergências (por exemplo, contingência de sistemas de informação, pandemia, desastre natural, gerenciamento de crise)

» Estratégias de processamento provisórias ou alternativas

» Planejamento de restauração

» Implementação de backup e redundância

» Testes e simulações

Domínio 5: Criptografia

5.1 Compreender as razões e requerimentos para criptografia

» Confidencialidade

» Integridade e autenticidade

» Sensibilidade de dados (por exemplo, informações de identificação pessoal (PII), propriedade intelectual (IP), informações protegidas de saúde (PHI))

» Práticas recomendadas regulatórias e da indústria (por exemplo, Padrões de segurança de dados da indústria de cartões de pagamento (PCI-DSS), Organização Internacional de Padronização (ISO))

5.2 Aplicar conceitos de criptografia

» Hashing

» Salting

» Criptografia Simétrica/Assimétrica/ Criptografia de curva elíptica (ECC)

» Não repúdio (p. ex., assinaturas/certificados digitais, código de autenticação de mensagens baseado em Hash (HMAC), trilhas de auditoria)

» Força dos algoritmos de criptografia e de chaves (p. ex., Padrões de criptografia Avançada (AES), Rivest-Shamir-Adleman (RSA), chaves de 256-, 512-, 1024-, 2048 bits)

» Ataques criptográficos, criptoanálise e contramedidas (p. ex., computação quântica)

5.3 Compreender e implementar protocolos seguros

» Serviços e protocolos (por exemplo, Segurança do Protocolo de Internet (IPsec), Segurança da Camada de Transporte (TLS), Extensões Seguras/Multifuncionais de Correio da Internet (S/MIME), Chaves de Domínio para Correio Identificado (DKIM))

» Casos de uso comuns

» Limitações e vulnerabilidades

5.4 Compreender e oferecer suporte a sistemas de infraestrutura de chave pública (PKI)

» Conceitos básicos de gerenciamento de chaves (por exemplo, armazenamento, rotação, composição, geração, destruição, troca, revogação, garantia)

» Web of Trust (WOT) (p. ex., Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), blockchain)

Domínio 6:
Segurança de Rede e Comunicações

6.1 Compreender e aplicar os conceitos fundamentais de rede

» Modelos de Interconexão de Sistemas Abertos (OSI) e Protocolo de Controle de Transmissão/ Protocolo de Internet (TCP/IP)

» Topologias de rede

» Relações de rede (p. ex., ponto a ponto (P2P), servidor cliente)

» Tipos de mídia de transmissão (por exemplo, com fio, sem fio)

» Rede definida por software (SDN) (por exemplo, Rede de longa distância definida por software (SD-WAN), virtualização de rede, automação)

» Portas e protocolos comumente usados

6.2 Compreender ataques de rede (por exemplo, negação de serviço distribuída (DDoS), man-in-the-middle (MITM), envenenamento do Sistema de Nomes de Domínio (DNS)) e contramedidas (por exemplo, redes de entrega de conteúdo (CDN))

6.3 Gerenciar controles de acesso à rede

» Controles, padrões e protocolos de acesso à rede (p. ex., Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS +))

» Operação e configuração de acesso remoto (p. ex., thin client, rede privada virtual (VPN))

6.4 Gerenciar a segurança da rede

» Posicionamento lógico e físico de dispositivos de rede (p. ex., em linha, passivo, virtual)

» Segmentação (p. ex., plano físico/lógico, plano de dados/controle, rede local virtual (VLAN), lista de controle de acesso (ACL), zonas de firewall, microssegmentação)

» Gerenciamento seguro de dispositivos

6.5 Operar e configurar dispositivos de segurança baseados em rede

» Firewalls e proxies (p. ex., métodos de filtragem, firewall de aplicações web (WAF))

» Sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS)

» Roteadores e switches

» Dispositivos de modelagem de tráfego (p. ex., otimização de rede de longa distância (WAN), balanceamento de carga)

6.6 Comunicações sem fio seguras

» Tecnologias (p. ex., rede celular, Wi-Fi, Bluetooth, Near-Field Communication (NFC))

» Protocolos de autenticação e criptografia (p. ex., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP))

» Internet das Coisas (IoT)

Domínio 7:
Segurança de Sistemas e Aplicações

7.1 Identificar e analisar código e atividade maliciosa

» Malware (p. ex., rootkits, spyware, scareware, ransomware, trojans, vírus, worms, trapdoors, backdoors, sem arquivo)

» Contramedidas de malware (p. ex., scanners, antimalware, assinatura de código)

» Atividade maliciosa (p. ex., ameaça interna, roubo de dados, negação de serviço distribuída (DDoS), botnet, exploits de dia zero, ataques baseados na web, ameaça persistente avançada (APT))

» Contramedidas de atividades maliciosas (p. ex., conscientização do usuário, fortalecimento do sistema, patching, isolamento, prevenção contra perda de dados (DLP))

» Engenharia social (p. ex., phishing, falsificação de identidade)

» Análise de comportamento (p. ex., aprendizado de máquina, inteligência artificial (IA), análise de dados)

7.2 Implementar e operar a segurança de endpoint

» Sistema de prevenção de intrusão baseado em host (HIPS)

» Firewalls baseados em host

» Lista de permissões de aplicações

» Criptografia de endpoint (p. ex., criptografia de disco inteiro)

» Módulo de plataforma confiável (TPM)

» Navegação segura

» Detecção e Resposta de Endpoint (EDR)

7.3 Administrar Gerenciamento de Dispositivos Móveis (MDM)

» Técnicas de provisionamento (p. ex., propriedade corporativa, habilitado pessoalmente (COPE), Traga seu Próprio Dispositivo (BYOD))

» Containerização

» Criptografia

» Gerenciamento de aplicativos móveis (MAM)

7.4 Compreenda e configure a segurança na nuvem

» Modelos de implantação (p. ex., público, privado, híbrido, comunidade)

» Modelos de serviço (por exemplo, Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS))

» Virtualização (p. ex., Hypervisor)

» Questões legais e regulatórias (p. ex., privacidade, vigilância, propriedade de dados, jurisdição, eDiscovery)

» Armazenamento, processamento e transmissão de dados (por exemplo, arquivamento, recuperação, resiliência)

» Requerimentos de terceiros/terceirização (por exemplo, acordo de nível de serviço (SLA), portabilidade de dados, destruição de dados, auditoria)

» Modelo de responsabilidade compartilhada

7.5 Operar e manter ambientes virtuais seguros

» Hipervisor
» Aplicativos virtuais
» Recipientes
» Continuidade e resiliência
» Ataques e contra-medidas
» Armazenamento compartilhado

Informações Adicionais do Exame

Referências Suplementares

Os candidatos são incentivados a complementar sua educação e experiência revisando os recursos relevantes que pertencem ao CBK e identificando áreas de estudo que podem precisar de atenção adicional.

Consulte a lista completa de referências suplementares em www.isc2.org/certifications/References.

Políticas e Procedimentos do Exame

(ISC)² recomenda que os candidatos do SSCP revejam as políticas e procedimentos do exame antes de se inscreverem para o exame. Leia a análise detalhada desta informação importante em www.isc2.org/Register-for-Exam.

Informações Legais

Para quaisquer questões relacionadas com politicas legais do (ISC)², entre em contato com o Departamento Legal do legal@isc2.org.

Alguma pergunta ?

(ISC)² Americas
Tel: +1.866.331.ISC2 (4722)
Email: info@isc2.org

(ISC)² Asia Pacífico
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org