SSCP®

Systems Security
Certified Practitioner

Esboço do Exame de Certificação

Data efetiva: Novembro de 2018

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

Sobre SSCP

A Systems Security Certified Practitioner (SSCP) é a certificação ideal para aqueles com habilidades técnicas comprovadas, que tem conhecimentos em segurança na prática em funções operacionais de TI. Ela provê a confirmação de habilidades práticas para implementar, monitorar e administrar a infraestrutura de TI de acordo com as políticas e procedimentos de segurança que asseguram a confidencialidade, integridade e disponibilidade dos dados.

O amplo espectro de tópicos incluído no Corpo Comum de Conhecimento (CBK) assegura sua relevância através de todas as disciplinas no campo de segurança da informação. Candidatos bem-sucedidos são competentes nos 7 domínios a seguir:

- Controles de acesso
- Operações e Administração de Segurança
- Identificação, Monitoramento e Análise de Riscos
- Recuperação e Resposta a Incidentes
- Criptografia
- Segurança de Redes e Comunicações
- Segurança em Sistemas e Aplicações

Requisitos de Experiência

Os candidatos devem ter no mínimo 1 ano acumulado de experiência de trabalho em 1 ou mais dos 7 domínios do SSCP CBK. Será concedido 1 ano do caminho de pré-requisito aos candidatos que tenham recebido um diploma (graduação ou pós graduação) em um programa de cibersegurança.

Um candidato que não tem a experiência requerida para tornar-se um SSCP pode se tornar um Associado do (ISC)² ao passar com sucesso no exame SSCP. O Associado do (ISC)² terá então 2 anos para ganhar o ano da experiência requerida.

Credenciamento

SSCP está em conformidade com os requisites rigorosos do ANSI/ISO/IEC Standard 17024.

Análise de Tarefa de Trabalho (JTA)

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

Informações sobre o exame SSCP

Duração do Exame	3 horas
Número de Questões	125
Formato das Questões	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

Domínios	Peso
1. Controles de acesso	16%
2. Operações e Administração de Segurança	15%
3. Identificação, Monitoramento e Análise de Riscos	15%
4. Recuperação e Resposta a Incidentes	13%
5. Criptografia	10%
6. Segurança de Rede e Comunicações	16%
7. Segurança de Sistemas e Aplicações	15%
Total:	**100%**

Domínio 1: Controles de Acesso

1.1 Implementar e manter métodos de autenticação

» Autenticação única/multifatorial
» Logon Único
» Autenticação de Dispositivos
» Acessos federados

1.2 Suportar arquiteturas de confiança entre redes

» Relações de Confiança (por exemplo, 1-way, 2-way, transitivo)
» Extranet
» Conexões com terceiros

1.3 Participar no ciclo de vida do gerenciamento de identidade

» Autorização
» Verificação
» Provisionamento/desprovisionamento
» Manutenção
» Direito
» Sistemas de Gerenciamento de Identidade e Acessos (IAM)

1.4 Implementar controles de acesso

» Mandatório
» Não discricionário
» Discricionário
» Baseado em Regras
» Baseado em Atributos
» Baseado em Assuntos
» Baseado em Objetos

Domínio 2:
Operações e Administração de Segurança

2.1 Cumprir o código de ética

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

2.2 Comprender os conceitos de Segurança

» Confidencialidade
» Integridade
» Disponibilidade
» Auditoria
» Privacidade
» Não-repúdio
» Menor privilégio
» Segregação de tarefas

2.3 Documentar, implementar, e manter controles de segurança funcionais

» Controles Desencorajadores
» Controles Preventivos
» Controles Detectivos
» Controles Corretivos
» Controles Compensatórios

2.4 Participar do Gerenciamento de Ativos

» Ciclo de vida (hardware, software, e dados)
» Inventário de Hardware
» Inventário de Software e licenciamento
» Armazenamento de Dados

2.5 Implementar controles de segurança e avaliar a conformidade

» Controles Técnicos (por exemplo, tempo de expiração de sessão, tempo de expiração de senha)
» Controles Físicos (por exemplo, jaulas, câmeras, fechaduras)
» Controles Administrativos (por exemplo, padrões e políticas de segurança procedimentos, baselines)
» Auditoria e Revisão periódica

2.6 Participar do Gerenciamento de Mudanças

» Executar o processo de gerenciamento de mudanças

» Identificar o impacto na segurança

» Testar /implementar patches, correções e atualizações (por exemplo, sistemas operacionais, aplicações, SDLC)

2.7 Participar no treinamento e conscientização de segurança

2.8 Participar de operações de segurança (por exemplo, Avaliação do Datacenter, Crachá)

Domínio 3:
Identificação, Monitoramento e Análise de Riscos

3.1 Compreender o processo de gerenciamento de risco

» Visibilidade de Risco e relatórios (por exemplo, registro do risco, compartilhamento de inteligência de ameaças, Sistema Comum de Pontuação de Vulnerabilidade (CVSS))

» Conceitos de Gerenciamento de Risco (por exemplo, avaliação de impacto, modelagem de ameaças, Análise de Impactos no Negócio(BIA))

» Frameworks de Gerenciamento de Risco (por exemplo, ISO, NIST)

» Tratamento de Risco (por exemplo, aceitar, transferir, mitigar, evitar, reformular)

3.2 Realizar atividades de avaliação de segurança

» Participar dos testes de segurança

» Interpretação e relatórios de varredura e resultados de testes

» Validação das remediações

» Auditoria para encontrar remediação

3.3 Operar e manter sistemas de monitoramento (por exemplo, monitoramento contínuo)

» Eventos de interesse (por exemplo, anomalias, intrusões, mudanças não autorizadas, monitoramento de conformidade)

» Logging

» Sistemas de Origem

» Preocupações legais e regulatórias (por exemplo, jurisdição, limitações, privacidade)

3.4 Analizar os resultados do monitoramento

» Baselines de Segurança e anomalias

» Visualizações, métricas e tendências (por exemplo, painéis, linhas do tempo)

» Análise de dados de eventos

» Documentar e comunicar descobertas (por exemplo, escalação)

Domínio 4:
Recuperação e Resposta a Incidentes

4.1 Ciclo de vida do incidente de suporte

» Preparação
» Detecção, Análise e escalação
» Contenção
» Erradicação
» Recuperação
» Lições aprendidas/implementação de novas contramedidas

4.2 Compreender e apoiar investigações forenses

» Princípios éticos e legais
» Tratamento de evidências (por exemplo, primeiro respondedor, triagem, cadeia de custódia, preservação da cena)

4.3 Compreender e apoiar as atividades do Plano de Continuidade dos Negócios (PCN) e do Plano de Recuperação de Desastres (PRD)

» Planos e procedimentos de resposta a emergências (por exemplo, plano de contingência do sistema de informações)
» Estratégias de processamento intermediárias ou alternativas
» Planejamento de restauração
» Backup e implementação de redundância
» Testes e exercícios

Domínio 5: Criptografia

5.1 Compreender os conceitos fundamentais de criptografia

- Hashing
- Salting
- Criptografia Simétrica/Assimétrica / Criptografia de Curva Elíptica (ECC)
- Não-repúdio(por exemplo, assinaturas digitais/ certificados, HMAC, trilha de auditoria)
- Algoritmos de Criptografia (por exemplo, AES, RSA)
- Força da chave (por exemplo, chaves de 256, 512, 1024, 2048 bits)
- Ataques criptográficos, criptoanálise e contramedidas

5.2 Compreender razões e requisitos para criptografia

- Confidencialidade
- Integridade e autenticidade
- Sensibilidade dos dados (por exemplo, PII, propriedade intelectual, PHI)
- Regulamentar

5.3 Compreender e suportar protocolos seguros

- Serviços e protocolos (por exemplo, IPSec, TLS, S/MIME, DKIM)
- Casos de uso comuns
- Limitações e vulnerabilidades

5.4 Compreender os sistemas de Infraestrutura de Chave Pública (PKI)

- Conceitos fundamentais de gerenciamento de chaves (por exemplo, rotação de chaves, composição das chaves, criação das chaves, troca, revogação, custódia)
- Teia de Confiança (WOT) (por exemplo, PGP, GPG)

Domínio 6:
Segurança de Rede e Comunicações

6.1 Compreender e aplicar conceitos fundamentais de rede

» modelos OSI e TCP/IP

» topografias de rede (por exemplo, anel, estrela, barramento, mesh, árvore)

» Relações de rede (por exemplo, par a par, cliente e servidor)

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

» » Portas e protocolos comumente usados

6.2 Compreender ataques de rede e contramedidas (exemplos, DDoS, man-in-the-middle, envenenamento de DNS)

6.3 Gerenciar controles de acesso à rede

» Controle de acesso à rede e monitoramento (por exemplo, remediação, quarentena, ingresso)

» Padrões e protocolos de controle de acesso à rede (por exemplo, IEEE 802.1X, Radius, TACACS)

» Operação de acesso remoto e configuração (por exemplo, thin client, SSL VPN, IPSec VPN, teletrabalho)

6.4 Gerenciar segurança de rede

» Colocação lógica e física de dispositivos de rede (por exemplo, inline, passive)

» Segmentação (por exemplo, físico/lógico, plano de dados/controle, VLAN, ACLs)

» Gerenciamento seguro de dispositivos

6.5 Operar e configurar dispositivos de segurança baseados em rede

» Firewalls e proxies (por exemplo, métodos de filtragem)

» Sistemas de detecção / prevenção de intrusão de rede

» Roteadores e switches

» Dispositivos de Traffic-shaping (por exemplo, otimização de WAN, balanceamento de carga)

6.6 Operar e configurar tecnologias sem fio (por exemplo, bluetooth, NFC, WiFi)

» Segurança de transmissão

» Dispositivos de segurança sem fio (por exemplo, WIPS, WIDS)

Domínio 7:
Segurança de Sistemas e Aplicações

7.1 Identificar e analisar código e atividade maliciosa

» Malware (por exemplo, rootkits, spyware, scareware, ransomware, trojans, vírus, worms, trapdoors, backdoors, e Trojans de acesso remoto)

» Contramedidas de códigos maliciosos (por exemplo, scanners, anti-malware, assinatura de código, sandboxing)

» Atividade maliciosa (por exemplo, ameaça interna, roubo de dados, DDoS, botnet)

» Contramedidas de atividade maliciosa (por exemplo, conscientização de usuários, hardening de sistemas, patching, sandboxing, isolamento)

7.2 Implementar e operar a segurança de endpoint

» HIDS

» Firewalls baseados em Host

» white listing de Aplicações

» Criptografia de Endpoint

» Trusted Platform Module (TPM)

» Gerenciamento de Dispositivos Móveis (MDM) (por exemplo, COPE, BYOD)

» Navegação segura (por exemplo, sandbox)

7.3 Operar e configurar segurança em nuvem

» Modelos de Implantação (por exemplo, pública, privada, hibrida, compartilhada)

» Modelos de serviço (por exemplo, IaaS, PaaS e SaaS)

» Virtualização (por exemplo, hypervisor)

» Preocupações legais e regulatórias (por exemplo, privacidade, vigilância, propriedade dos dados, jurisdição, eDiscovery)

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

» Requisitos de Terceirização (por exemplo, SLA, portabilidade dos dados, destruição dos dados, auditoria)

» Modelo de responsabilidade compartilhada

7.4 Operar e proteger ambientes virtuais

» Rede definida por Software

» Hypervisor

» Appliances virtuais

» Continuidade e resiliência

» Ataques e contramedidas

» Armazenamento compartilhado

Informações adicionais sobre exames

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.

Veja a lista completa de referências complementares em
www.isc2.org/certifications/References.

Políticas e Procedimentos de Exame

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

Informação Legal

Para quaisquer questões relacionadas às politicas legais do (ISC)², favor entrar em contato com Departamento Legal (ISC)2 através do e-mail legal@isc2.org.

Alguma pergunta ?

Serviços aos candidatos (ISC)²
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

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

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

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

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