SSCP® – Systems Security Certified Practitioner (e-Learning)

ISC2

- **Nível:** Intermédio
- **Duração:** 35h

Sobre o curso

O curso Systems Security Certified Practitioner (SSCP®) proporciona uma visão geral e abrangente dos conhecimentos necessários para implementar, monitorizar e administrar infraestruturas de IT de acordo com políticas e procedimentos de segurança de informação que asseguram a confidencialidade, a integridade e a disponibilidade dos dados.

O presente curso de formação ajudará os participantes na revisão e na atualização dos seus conhecimentos, bem como na identificação da matéria e das áreas que devem estudar para o exame SSCP.

O conteúdo programático do curso encontra-se em total sintonia com os sete domínios do SSCP Common Body of Knowledge (CBK®) da ISC2, abrangendo-os na sua totalidade.

Todo o material didático empregue no curso é oficial e desenvolvido pela ISC2, a entidade criadora do SSCP CBK, assegurando, assim, que os conteúdos formativos se encontram atualizados e relevantes. Os nossos formadores são especialistas em segurança oficiais e acreditados como SSCP, que terão sido alvo de um período de treino e de formação intensivos a fim de estarem autorizados a lecionar os conteúdos da autoria da ISC2.

Destinatários

Este curso de formação destina-se a profissionais com pelo menos um ano de experiência remunerada em um, ou mais, dos sete domínios do SSCP CBK da ISC2, que pretendam ter formação como SSCP e obter a certificação correspondente. A obtenção da mesma facultar-lhes-á credibilidade e mobilidade para avançarem nas suas atuais carreiras no ramo da segurança da informação. Ainda que não se limite unicamente aos cargos listados abaixo, esta formação é ideal para aqueles com competências técnicas e conhecimentos práticos de segurança que desempenhem cargos na área das Operações de TI, tais como:

- Engenheiro de Segurança de Redes
- Administrador de Sistemas/Redes
- Analista de Segurança
- Engenheiro de Sistemas
- Consultor/Especialista de Segurança

- Administrador de Segurança
- Analista de Sistemas/Redes
- Administrador de Bases de Dados

Objetivos

- Descrever a segurança e o alinhamento da gestão de ativos com a gestão de riscos.
- Avaliar as opções de gestão de riscos e a utilização de controlos de acesso de maneira a conseguir proteger os ativos.
- Examinar o campo da criptografia de modo a proteger a informação e a comunicação.
- Criar uma postura de segurança através da proteção de software, de dados e de endpoints.
- Aplicar medidas de segurança de redes e comunicações com o intuito de estabelecer um ambiente em rede seguro.
- Avaliar a segurança na Cloud e na rede sem fios.
- Estar preparado para o processo de deteção e reposta a incidentes.
- Implementar medidas adequadas que contribuam para a maturidade da gestão de risco

---

Condições

Notas

O exame incluído no curso é presencial e realiza-se num centro Pearson VUE Select, como o da Rumos em Lisboa.

Para particulares
• 10% do valor total pago no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Formandos não residentes em Portugal: pagamento de 50% no ato da inscrição; restante valor até 7 dias antes do início do curso.
• Possibilidade de beneficiar do Cheque Formação+Digital até 750€ (conforme elegibilidade).
• Isenção de IVA para particulares.
Para empresas
• Empresas nacionais: pagamento a 30 dias, contra fatura (acresce IVA à taxa legal em vigor).
• Empresas da UE e fora da UE: valores isentos de IVA e pagamento a pronto.

Pré-requisitos

Ter pelo menos um ano de experiência remunerada em um, ou mais, dos sete domínios do SSCP CBK da ISC2.

Metodologia

A Formação Oficial ISC2 Online Self-Paced SSCP constitui uma forma inovadora de preparação para a certificação que utiliza inteligência artificial para personalizar o teu percurso de aprendizagem. Identifica as áreas que exigem foco adicional e orienta-te na preparação para o exame de forma verdadeiramente personalizada.

Estuda de forma mais inteligente com estas principais vantagens:

- **Instrução personalizada** – O conteúdo, o ritmo e a dificuldade adaptam-se ao teu nível de conhecimento, velocidade de aprendizagem e nível de confiança.
- **Maior envolvimento** – Feedback imediato e conteúdo dinâmico permitem-te aprender a um nível adequado.
- **Poupança de tempo** – O tempo de formação é otimizado ao focar-se nas áreas que exigem maior revisão.
- **Melhores resultados de aprendizagem** – A plataforma identifica as áreas que exigem revisão adicional e disponibiliza suporte direcionado para maximizar a tua compreensão do conteúdo.

A formação Systems Security Certified Practitioner (SSCP) tira partido do poder da inteligência artificial, orientando os formandos numa experiência de aprendizagem ao seu ritmo, adaptada às suas necessidades. Abrange conceitos de segurança da informação e boas práticas para implementar, monitorizar e administrar infraestruturas de IT com base em políticas e procedimentos de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade dos dados.

Programa

- Introdução à Segurança e o Alinhamento da Gestão de Ativos com a Gestão de Riscos
- As Opções da Gestão de Riscos e o Uso de Controlos de Acesso para Proteção dos Ativos
- Criptografia
- Proteção de Software, de Dados e de Endpoints
- Segurança de Redes e Comunicações
- Segurança na Cloud and na Rede Sem Fios
- Deteção e Resposta a Incidentes
- Maturidade da Gestão de Riscos

Introdução à Segurança e o Alinhamento da Gestão de Ativos com a Gestão de Riscos

- Classificar a segurança da informação e os conceitos de segurança.
- Resumir os componentes do ciclo de vida da gestão de ativos.
- Identificar os riscos e as vulnerabilidades mais comuns.
- Fornecer exemplos de medidas apropriadas de tratamento de riscos.

As Opções da Gestão de Riscos e o Uso de Controlos de Acesso para Proteção dos Ativos

- Fornecer exemplos de controlos e políticas de segurança funcionais para os cenários identificados.
- Classificar os diversos modelos de controlo de acesso existentes.
- Identificar os componentes do ciclo de vida da gestão de identidade.

- Estar a par dos métodos de controlo de acesso e de autenticação.

Criptografia

- Identificar os conceitos fundamentais de criptografia que determinam requisitos e vantagens.
- Estar a par dos métodos de encriptação simétrica.
- Utilizar métodos de encriptação assimétrica.
- Examinar os sistemas e os certificados da Infraestrutura de Chaves Públicas.
- Resumir termos e conceitos fundamentais da gestão de chaves.
- Saber como implementar protocolos seguros.
- Analisar os métodos de ataques criptoanalíticos.

Proteção de Software, de Dados e de Endpoints

- Discutir sistemas de software e segurança de aplicações.
- Reconhecer conceitos e competências associados à segurança de dados.
- Identificar código malicioso e contramedidas adequadas.
- Avaliar a Gestão de Dispositivos Móveis (MDM) e questões de segurança relacionadas com endpoints móveis e autónomos.
- Analisar ataques a máquinas virtuais e as contramedidas para os mesmos.

Segurança de Redes e Comunicações

- Reconhecer as camadas do modelo OSI, bem como as suas funções e os ataques presentes em cada uma das camadas.
- Identificar os protocolos e as portas mais usados.
- Selecionar as contramedidas adequadas a diferentes tipos de ataques a redes.
- Resumir as boas práticas para a criação de um ambiente em rede seguro.

Segurança na Cloud and na Rede Sem Fios

- Relembrar conceitos e configurações de segurança da cloud.
- Reconhecer tipos de virtualização e considerações de segurança da cloud.
- Resumir os tipos de telecomunicações e de controlos de acesso à rede.

Deteção e Resposta a Incidentes

- Rever os passos para a monitorização, a deteção de incidentes e a prevenção da perda de dados utilizando todas as fontes de informação.
- Identificar os elementos de uma política de resposta a incidentes e os membros da equipa de resposta a incidentes (IRT).
- Classificar o papel do SSCP no apoio a investigações forenses.

Maturidade da Gestão de Riscos

- Identificar aspetos operacionais da gestão da mudança.
- Resumir as considerações de segurança física.
- Traçar uma estratégia que promova o ensino e a consciencialização para a segurança.

- Conhecer as atividades de avaliação de segurança mais comuns.
- Classificar os componentes dos planos de continuidade do negócio e de recuperação de desastres.