SSCP-Systems Security Certified Practitioner - Préparation à la Certification sécurité

Durée: 5 Jours **Réf de cours: GK1642**

Résumé:

Le Systems Security Certified Practitioner (SSCP) est la certification idéale pour les personnes ayant des compétences techniques avérées et des connaissances pratiques en matière de sécurité dans des rôles informatiques opérationnels. Elle confirme la capacité d'un praticien à mettre en œuvre, surveiller et administrer une infrastructure informatique conformément aux politiques et procédures de sécurité de l'information qui garantissent la confidentialité, l'intégrité et la disponibilité des données. Le large éventail de sujets inclus dans le SSCP Common Body of Knowledge (CBK) garantit sa pertinence dans toutes les disciplines du domaine de la sécurité de l'information.

Les candidats retenus sont compétents dans les sept domaines suivants : Opérations et administration de la sécuritéContrôles d'accèsIdentification, surveillance et analyse des risques Réponse aux incidents et récupération Cryptographie Sécurité des réseaux et des communications Sécurité des systèmes et des applications

Veuillez noter :Pour vous inscrire au nouvel examen (ISC)2, vous aurez besoin d'un voucher Pearson VUE. Ce voucher n'est pas inclus dans le prix du cours.

Public visé:

Le SSCP est idéal pour les administrateurs, gestionnaires et directeurs informatiques, ainsi que pour les professionnels de la sécurité des réseaux responsables de la sécurité opérationnelle pratique des actifs critiques de leur organisation, notamment ceux qui occupent les postes suivants :Ingénieur en sécurité réseauAdministrateur de systèmesAnalyste de la sécuritéIngénieur systèmeConsultant/spécialiste en sécuritéAdministrateur de sécuritéAnalyste systèmes/réseauxAdministrateur de bases de données

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Comprendre les différents systèmes de contrôle d'accès et comment ils doivent être mis en œuvre pour protéger le système et les données en utilisant les différents niveaux de confidentialité, d'intégrité et de disponibilité.
- Comprendre les processus nécessaires pour travailler avec la direction et les propriétaires, gardiens et utilisateurs de l'information afin de définir les classifications de données appropriées. Cela garantira le traitement approprié de toutes les informations sur papier et électroniques lorsqu'elles sont appliquées par les Opérations et l'Administration de la sécurité.
- Le domaine Identification, surveillance et analyse des risques indique comment identifier, mesurer et contrôler les pertes associées aux événements indésirables. Vous examinerez, analyserez, sélectionnerez et évaluerez les mesures de protection pour atténuer les risques.
- Identifier comment gérer la réponse aux incidents et la récupération en utilisant des approches cohérentes et appliquées, y compris l'utilisation des concepts de plan de continuité des activités (BCP) et de plan de récupération après sinistre (DRP) afin d'atténuer les dommages, de récupérer les opérations commerciales et d'éviter une interruption critique des activités, ainsi que la réponse d'urgence et la récupération après sinistre.
- Identifier et différencier les concepts cryptographiques clés et la manière de les appliquer, mettre en œuvre des protocoles sécurisés, les concepts de gestion des clés, l'administration et la validation des clés, et l'infrastructure à clé publique dans le cadre de la sécurisation des communications en présence de tiers.
- Définir et identifier la sécurité des réseaux et des communications nécessaire pour sécuriser la structure du réseau, les méthodes de transmission des données, les formats de transport et les mesures de sécurité utilisées pour maintenir l'intégrité, la disponibilité, l'authentification et la confidentialité des informations transmises.
- La section Sécurité des systèmes et des applications identifie et définit les attaques techniques et non techniques et la manière dont une organisation peut se protéger de ces attaques, y compris les concepts de sécurité des dispositifs d'extrémité, de sécurité de l'infrastructure du cloud, de sécurisation des systèmes de big data et de sécurisation des environnements virtuels.

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Une année de travail dans le domaine de la sécurité de l'information, couvrant au moins un des domaines du SSCP CBK.
- G005 - Préparation à la certification Network+ - Compétences support

Test et certification

- Durée de l'examen : 3 heures
- Nombre de questions : 125
- Format des questions : Choix multiple
- Note de passage : 700 sur 1000 points
- Langues disponibles : anglais, japonais et portugais brésilien
- Centre d'examen : Pearson VUE Testing Center

Pondération de l'examen : SSCP

- Opérations et administration de la sécurité 16 %
- Contrôles d'accès 15 %
- Identification, surveillance et analyse des risques 15 %
- Réponse aux incidents et récupération 14 %.
- Cryptographie 9 %
- Sécurité des réseaux et des communications 16 %.
- Sécurité des systèmes et des applications 15 %
- Total 100%

Contenu:

1. Opérations et administration de la sécurité

1.1 Se conformer aux codes d'éthique

- Code d'éthique de l'ISC
- Code d'éthique de l'organisation

1.2 Comprendre les concepts de sécurité

- Confidentialité
- Intégrité
- la disponibilité
- Responsabilité
- Confidentialité
- Non-répudiation
- Le moindre privilège
- Séparation des tâches (SoD)

1.3 Identifier et mettre en œuvre des contrôles de sécurité

- Contrôles techniques (par exemple, expiration de la session, vieillissement du mot de passe)
- Contrôles physiques (par exemple, mantras, caméras, serrures)
- Contrôles administratifs (par exemple, politiques de sécurité, normes, procédures, lignes de base)
- Évaluation de la conformité
- Audit et révision périodiques

1.4 Documenter et maintenir des contrôles de sécurité fonctionnels

- Contrôles dissuasifs
- Contrôles préventifs
- Contrôles de détection
- Contrôles correctifs
- Contrôles compensatoires

1.5 Participer au cycle de vie de la gestion des actifs (matériel, logiciel et données)

- Processus, planification, conception et initiation
- Développement/Acquisition
- Inventaire et licences
- Mise en œuvre/évaluation
- Exploitation/Maintenance
- Exigences d'archivage et de conservation
- Elimination et destruction

1.6 Participer au cycle de vie de la gestion du changement

- Gestion du changement (par exemple, rôles, responsabilités, processus)
- Analyse de l'impact sur la sécurité
- Gestion de la configuration (CM)

1.7 Participer à la mise en œuvre de la

3. Identification, surveillance et analyse des risques

3.1 Comprendre le processus de gestion des risques

- Visibilité des risques et établissement de rapports (par exemple, registre des risques, partage des renseignements sur les menaces/indicateurs de compromission (IOC), notation commune des vulnérabilités (CVSS)).
- Concepts de gestion des risques (par exemple, évaluations d'impact, modélisation des menaces)
- Cadres de gestion des risques
- Tolérance au risque (p. ex., appétit)
- Traitement du risque (par exemple, accepter, transférer, atténuer, éviter).

3.2 Comprendre les préoccupations d'ordre juridique et réglementaire (p. ex., juridiction, limites, confidentialité

3.3 Participer aux activités d'évaluation de la sécurité et de gestion des vulnérabilités

- Tests de sécurité
- Examen des risques (p. ex., interne, fournisseur, architecture)
- Cycle de vie de la gestion des vulnérabilités

3.4 Exploiter et surveiller les plateformes de sécurité (p. ex., surveillance continue)

- Systèmes sources (p. ex., applications, dispositifs de sécurité, périphériques réseau et hôtes)
- Événements d'intérêt (p. ex., anomalies, intrusions, modifications non autorisées, surveillance de la conformité)
- Gestion des journaux
- Agrégation et corrélation des événements

3.5 Analyser les résultats de la surveillance

- Lignes de base et anomalies de sécurité
- Visualisations, mesures et tendances (par exemple, notifications, tableaux de bord, chronologies)
- Analyse des données d'événements
- Documenter et communiquer les résultats (par exemple, escalade)

4. Réponse aux incidents et récupération

4.1 Prise en charge du cycle de vie des incidents (par exemple, National Institute of

5.4 Comprendre l'infrastructure à clé publique (ICP)

- Concepts fondamentaux de la gestion des clés (par exemple, stockage, rotation, composition, génération, destruction, échange, révocation, séquestre).
- Web of Trust (WOT)

6. Sécurité des réseaux et des communications

6.1 Comprendre et appliquer les concepts fondamentaux de la mise en réseau

- Modèles d'interconnexion des systèmes ouverts (OSI) et de protocole de contrôle de transmission/protocole Internet (TCP/IP).
- Topologies de réseau
- Relations entre réseaux (par exemple, peer-to-peer (P2P), client-serveur)
- Types de supports de transmission (par exemple, filaire, sans fil).
- Réseaux définis par logiciel (SDN) (par exemple, réseau étendu défini par logiciel (SD-WAN), virtualisation du réseau, automatisation).
- Ports et protocoles couramment utilisés

6.2 Comprendre les attaques réseau (par exemple, déni de service distribué (DDoS), man-in-the-middle (MITM), empoisonnement du système de nom de domaine (DNS)) et les contre-mesures (par exemple, réseaux de diffusion de contenu (CDN)) 6.3 Gérer les contrôles d'accès au réseau

- Contrôles d'accès au réseau, normes et protocoles (par exemple, Institute of Electrical and Electronics Engineers (IEEE) 802.1X, Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+)).
- Fonctionnement et configuration de l'accès à distance (par exemple, client léger, réseau privé virtuel (VPN))

6.4 Gérer la sécurité du réseau

- Placement logique et physique des dispositifs du réseau (par exemple, en ligne, passif, virtuel)
- Segmentation (par exemple, physique/logique, données/plan de contrôle, réseau local virtuel (VLAN), liste de contrôle d'accès (ACL), zones de pare-feu, micro-segmentation).
- Gestion des dispositifs sécurisés

6.5. Exploiter et configurer les dispositifs de

sensibilisation et de la formation à la sécurité (par exemple, ingénierie sociale/hameçonnage)

1.8 Collaborer aux opérations de sécurité physique (par exemple, évaluation du centre de données, badgeage)

2. Contrôles d'accès

2.1 Mettre en place et maintenir des méthodes d'authentification

- Authentification simple/multi-facteurs (MFA)
- Authentification unique (SSO) (par exemple, Active Directory Federation Services (ADFS), OpenID Connect)
- Authentification du dispositif
- Accès fédéré (par exemple, Open Authorization 2 (OAuth2), Security Assertion Markup Language (SAML))

2.2 Prendre en charge les architectures de confiance des réseaux Internet

- Relations de confiance (par exemple, 1 voie, 2 voies, transitive, zéro)
- Internet, intranet et extranet
- Connexions de tiers

2.3 Participer au cycle de vie de la gestion des identités

- Autorisation
- Vérification
- Approvisionnement/déprovisionnement
- Maintenance
- Habilitation
- Systèmes de gestion des identités et des accès (IAM)

2.4 Comprendre et appliquer les contrôles d'accès

- Obligatoire
- Discrétionnaire
- Basé sur le rôle (par exemple, basé sur l'attribut, le sujet, l'objet)
- Basé sur des règles

Standards and Technology (NIST), International Organization for Standardization (ISO))

- Préparation
- Détection, analyse et escalade
- Confinement
- Eradication
- Récupération
- Enseignements tirés/mise en œuvre de nouvelles contre-mesures.

4.2 Comprendre et soutenir les enquêtes médico-légales

- Principes juridiques (par exemple, civils, criminels, administratifs) et éthiques.
- Traitement des preuves (par exemple, premier intervenant, triage, chaîne de possession, préservation de la scène)
- Rapport d'analyse

4.3 Comprendre et soutenir le plan de continuité des activités (PCA) et le plan de reprise après sinistre (PRS)

- Plans et procédures d'intervention en cas d'urgence (par exemple, contingence du système d'information, pandémie, catastrophe naturelle, gestion de crise).
- Stratégies de traitement provisoire ou alternatif
- Planification de la restauration
- Mise en place de sauvegardes et de redondances
- Tests et exercices

5. Cryptographie

5.1 Comprendre la cryptographie

- La confidentialité
- Intégrité et authenticité
- Sensibilité des données (par exemple, informations personnelles identifiables (PII), propriété intellectuelle (IP), informations de santé protégées (PHI))
- Les meilleures pratiques réglementaires et industrielles (par exemple, les normes de sécurité des données de l'industrie des cartes de paiement (PCI-DSS), l'Organisation internationale de normalisation (ISO)).

5.2 Appliquer les concepts de cryptographie

- Hachage
- Salage
- Cryptage symétrique/symétrique/cryptographie à courbe elliptique (ECC)
- Non-répudiation (par exemple, signatures/certificats numériques, code d'authentification de message basé sur le

sécurité basés sur le réseau

- Pare-feu et proxies (par exemple, méthodes de filtrage, pare-feu d'application web (WAF)) Systèmes de détection des intrusions (IDS) et systèmes de prévention des intrusions (IPS)
- Systèmes de détection/prévention des intrusions dans le réseau
- Routeurs et commutateurs
- Dispositifs de mise en forme du trafic (par exemple, optimisation du réseau étendu (WAN), équilibrage de la charge).

6.6 Communications sans fil sécurisées

- Technologies (par exemple, réseau cellulaire, Wi-Fi, Bluetooth, Near-Field Communication (NFC))
- Protocoles d'authentification et de cryptage (par exemple, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), EAP (Extensible Authentication Protocol))
- Internet des objets (IoT)

7. Sécurité des systèmes et des applications

7.1 Identifier et analyser les codes et activités malveillants

- Malware (par exemple, rootkits, spyware, scareware, ransomware, trojans, virus, vers, trappes, backdoors, fileless)
- Contre-mesures aux logiciels malveillants (par exemple, scanners, anti-malware, signature de code)
- Activités malveillantes (menace d'initié, vol de données, déni de service distribué (DDoS), botnet, exploits du jour zéro, attaques sur Internet, menaces persistantes avancées (APT), etc.)
- Contre-mesures en cas d'activité malveillante (par exemple, sensibilisation des utilisateurs, renforcement du système, correctifs, sandboxing, isolation, prévention des pertes de données (DLP)).

7.2 Mettre en œuvre et exploiter la sécurité des dispositifs d'extrémité

- Système de prévention des intrusions basé sur l'hôte (HIPS)
- Pare-feu basés sur l'hôte
- Liste blanche des applications
- Chiffrement des points d'extrémité (par exemple, chiffrement du disque entier)
- Module de plateforme de confiance (TPM)
- Navigation sécurisée
- Détection et réponse aux points d'extrémité (EDR)

7.3 Administrer la gestion des dispositifs mobiles (MDM)

hachage (HMAC), pistes d'audit).
- Force des algorithmes et des clés de chiffrement (par exemple, Advanced Encryption Standards (AES), Rivest-Shamir-Adleman (RSA), clés de 256, 512, 1024 et 2048 bits).
- Attaques cryptographiques, cryptanalyse et contre-mesures (par exemple, informatique quantique).

5.3 Comprendre et mettre en œuvre des protocoles sécurisés

- Services et protocoles
- Cas d'utilisation courants
- Limites et vulnérabilités

- Techniques d'approvisionnement (par exemple, propriété de l'entreprise, capacité personnelle (COPE), Bring Your Own Device (BYOD))
- Conteneurisation
- Chiffrement
- Gestion des applications mobiles (MAM)

7.4 Comprendre et configurer la sécurité du cloud computing

- Modèles de déploiement (par exemple, public, privé, hybride, communautaire)
- Modèles de service (par exemple, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) et Software as a Service (SaaS))
- Virtualisation (par ex., hyperviseur)
- Préoccupations juridiques et réglementaires (par exemple, vie privée, surveillance, propriété des données, juridiction, eDiscovery)
- Stockage, traitement et transmission des données (par exemple, archivage, récupération, résilience)
- Exigences relatives aux tiers/à l'externalisation (par exemple, accord de niveau de service (SLA), portabilité des données, destruction des données, audit).
- Modèle de responsabilité partagée

7.5 Exploiter et maintenir des environnements virtuels sécurisés

- Hyperviseur
- Appareils virtuels
- Conteneurs
- Continuité et résilience
- Attaques et contre-mesures
- Stockage partagé

Méthodes pédagogiques :

Support de cours remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.