CertNexus CyberSAFE 2019 Exam CBS-310 Exam Information

Admissibilité des candidats:

Les informations d'identification CyberSAFE 2019 ne nécessitent aucun frais, aucune documentation justificative ou autre éligibilité
des mesures de vérification pour vous permettre de terminer le processus d'identification. Achetez simplement une clé d'accès pour
Cours CyberSAFE 2019 du CertNexus Store ici. Ce cours comprend l'accès aux informations d'identification
processus directement via la plateforme CHOICE.

Conditions préalables à l'examen

Bien qu'il n'y ait pas de conditions préalables formelles pour terminer le processus d'accréditation CyberSAFE, il est
recommandé d'avoir une expérience de l'utilisation de base de la technologie conventionnelle pour l'utilisateur final,
comme ordinateurs de bureau, portables et tablettes; appareils mobiles; et les fonctions Internet de base, comme le Web
navigation et e-mail.
Une fois que vous avez obtenu ce niveau de compétences et de connaissances, ou si vous le possédez déjà, CertNexus également
vous recommande vivement de vous préparer à l'accréditation CyberSAFE en prenant le CyberSAFE de CertNexus
2019: Cours d'examen CBS-310.

Spécifications d'examen

Nombre d'articles : 10
Note de passage : 8 sur 10 (80%)

Durée : Il n'y a pas de limite de temps formelle pour obtenir les informations d'identification CyberSAFE. Cependant, vous devez vous attendre
être en mesure de terminer l'évaluation en 15 à 30 minutes environ.

Options d'examen : en ligne via le CHOICE LMS - l'évaluation est à livre ouvert

Formats d'élément : Choix multiple / Réponse multiple / Vrai-Faux

Description de l'examen

Candidat cible :
Ces informations d'identification sont conçues pour tous les utilisateurs finaux d'ordinateurs, d'appareils mobiles, de réseaux et d'Internet pour
s'assurer qu'ils peuvent utiliser la technologie en toute sécurité pour minimiser les risques de sécurité.

Énoncé de l'objectif de l'examen :

L'évaluation certifiera que le candidat retenu possède les connaissances, les compétences et les capacités requises
pour identifier les risques courants associés à l'utilisation de la technologie conventionnelle des utilisateurs finaux et protéger en toute sécurité

eux-mêmes et leurs organisations contre les risques de sécurité.

Pour s'assurer que les candidats possèdent les connaissances, compétences et capacités susmentionnées, le CyberSAFE
Les informations d'identification 2019 les testeront sur les domaines suivants avec les pondérations suivantes:

Domaine.	%d'examen
1.0 Conformité	12%
2.0 Ingénierie sociale	20%
3.0 Protection des appareils et des données	37%
4.0 Sécurité en ligne	31%
Total	100%

Les informations qui suivent sont destinées à vous aider à vous préparer à votre évaluation des titres CertNexus.
Ces informations ne représentent pas une liste exhaustive de tous les concepts et compétences que vous pourriez être
testé lors de l'évaluation. Les domaines, identifiés précédemment et inclus dans les objectifs
liste, représentent les grandes zones de contenu couvertes par le test. Les objectifs dans ces domaines représentent les tâches spécifiques associées à l'utilisation en toute sécurité des appareils informatiques sur lesquels vous serez testé.
Les informations au-delà des domaines et des objectifs visent à fournir des exemples des types de concepts, outils, compétences et capacités liés aux domaines et objectifs correspondants. Celles-ci
les exemples ne sont pas nécessairement en corrélation individuelle avec le contenu couvert dans votre programme de formation
ou sur votre test. CertNexus vous recommande fortement d'étudier indépendamment pour vous familiariser
avec tout concept identifié ici avec lequel vous n'êtes pas familier avant de passer l'évaluation.

Objectifs :

Conformité du domaine 1.0

Objectif 1.1 Identifier les exigences de conformité en matière de sécurité organisationnelle

- Sources des exigences de conformité organisationnelles
    - o Politique de mot de passe
    - o Politique d'utilisation d'Internet
    - o Confidentialité des données
    - o Informations personnellement identifiables (PII)
    - o AUP
        - ▪ Sur site vs à distance
        - ▪ Équipement
        - ▪ Ressources partagées (mots de passe, boîtes aux lettres, etc.)
        - ▪ Exceptions et dérogations

        Chemins d'escalade / rapport d'incident
    - o Politiques des installations
        - ▪ Accès des employés / visiteurs
        - ▪ Exigences relatives aux badges
        - ▪ Politiques clés
    - o Ramifications du non-respect

Objectif 1.2 Identifier les exigences de conformité légale

- Sources des exigences de conformité légale

- Règlement / loi
  - HIPAA
  - SOX
  - PCI DSS
  - Ordonnances locales
- Conséquences juridiques du non-respect

Objectif 1.3 Identifier les ressources de sécurité et de conformité

- Ressources de conformité organisationnelle et juridique
  - Manuels d'organisation / sites Web
  - Documentation AUP
    - Mises à jour
    - Localisation / accès
  - Départements organisationnels
    - Juridique
    - RH
    - Gestion des informations sur la santé
    - informatique
  - Associations industrielles / groupes professionnels
  - Sites Web gouvernementaux

Domaine 2.0 Ingénierie sociale

Objectif 2.1 Reconnaître les attaques d'ingénierie sociale

- Vecteurs d'attaque
  - Nom d'utilisateur / mot de passe
  - Informations organisationnelles / personnelles
  - Accès physique
  - Informations personnelles de l'utilisateur final
- Objectifs d'attaque
  - Destruction des données
  - Vol de données
  - Gain financier
  - Gain politique
  - Réputation
  - Vengeance / Réplique ?
- Cibles de grande valeur
  - C-suite
  - Personnel comptable
  - Personnel RH
  - Personnel informatique
- Types d'attaques
  - Phishing
    - Chasse à la baleine
    - Hameçonnage
  - Vishing
  - Pharming
  - Appâtage
  - Prétexte
  - Usurpation d'identité

- Quid pro quo
- Tailgating / ferroutage
- Surf à l'épaule ?

Objectif 2.2 Se défendre contre les attaques d'ingénierie sociale

- Ressources à défendre
  - Matériel / appareils organisationnels
  - Données organisationnelles
  - Accès réseau
  - Accès aux locaux
  - Informations d'identification de l'utilisateur
- Techniques d'atténuation
  - Conscience situationnelle
  - Systèmes de badges / contrôles de sécurité
  - Serrures de porte
  - Vérification des demandes
  - Élimination / suppression appropriée des informations sensibles
  - Éducation / communication

Domaine 3.0 Protection des appareils et des données

Objectif 3.1 Maintenir la sécurité physique des appareils
- Appareils contenant des données potentiellement sensibles
  - Ordinateurs portables / ordinateurs
  - Téléphones mobiles
  - Tablettes
  - Stockage amovible
- Exigences organisationnelles en matière de sécurité des appareils
  - Limiter les appareils ayant accès aux données sensibles
  - Appareils acceptables pour le stockage des données
  - Exigences d'élimination / suppression
- Présence numérique
  - Journaux de l'appareil
  - Fichiers temporaires
  - Historique du navigateur
  - Identifiants mis en cache / enregistrés
- Techniques de sécurité physique des appareils
  - Stockage / élimination / recyclage appropriés
  - Rapports de perte / vol
  - Verrouillage des machines / appareils sans surveillance

Objectif 3.2 Utiliser les mots de passe en toute sécurité

- Mots de passe / NIP
  - Changement fréquent
  - Complexité
  - Interdire la réutilisation / le partage
  - Mémorisation vs enregistrement / documentation
- Biométrie
- Authentification multifacteur vs authentification en deux étapes
- Gestionnaires de mots de passe
- Techniques de sécurité par mot de passe / PIN
  - Entrée secrète (assurez-vous que personne ne peut vous regarder entrer)
  - Changer immédiatement après une violation / un incident
  - Stockage sécurisé des mots de passe

- Importance critique de la protection des mots de passe de messagerie
- Utilisation de l'authentification multifacteur lorsque cela est possible
- Complexité par rapport à la sensibilité des données
- Mots de passe uniques pour tous les sites et systèmes
- Éviter d'utiliser des mots de passe faciles à deviner

Objectif 3.3 Adhérer aux bonnes pratiques de protection des données et des données sensibles

- Sauvegardes de données / emplacements de stockage
- Considérations relatives aux appareils mobiles
  - Fuite d'informations grâce à la fonctionnalité d'application permanente
  - Enregistrement accidentel ou intentionnel de données sensibles
    - Caméra
    - Microphone
- Techniques de sécurité des données
  - Interdictions de copier / imprimer
  - Élimination appropriée des données imprimées
  - Interdictions contre les périphériques de stockage amovibles
  - Interdiction des appareils mobiles lors des réunions

Objectif 3.4 Identifier les sources potentielles de logiciels malveillants et prévenir les infections

- Effets de logiciels malveillants
  - Corruption du système
  - Espionnage / logging
  - Distrayant / ennuyeux
  - Dégradation des performances de l'appareil
  - Détournement / rançon de données
  - Destruction des données
  - Chantage
  - Publicité
- Types de logiciels malveillants
  - Enregistreur de frappe
  - Ransomware
  - Adware / spyware
  - cheval de Troie
  - Virus
  - Ver
  - Pirate de navigateur
- Sources de logiciels malveillants
  - Offres astuces
  - Antivirus non autorisé
  - Escroqueries de logiciels gratuits
  - ferroutage logiciel
  - Options confuses ou obscurcies (installations personnalisées)
  - Sites de téléchargement inconnus / non approuvés
  - Pièces jointes aux e-mails
  - Liens
  - Scripts dans les fichiers de données / logiciels
  - Matériel infecté
    - Clé USB
    - Disques durs externes
- Techniques de prévention des logiciels malveillants
  - Lecture attentive des emails / boîtes de dialogue / offres / pop-ups / etc.
  - Approbation informatique pour l'installation du logiciel
  - Inspection des liens avant de sélectionner

- Analyse des avantages / risques lors de l'installation du logiciel
- Conscience générale du comportement du système
- Utilisation uniquement de fournisseurs et d'appareils connus
  - Éditeurs vérifiés

Objectif 3.5 Utiliser les appareils sans fil en toute sécurité

- Risques courants de réseau sans fil
  - Écoute
  - Réseaux non sécurisés
    - Privé
    - Publique
    - Ouvert
  - Points d'accès non fiables
  - Jumeaux maléfiques
  - «Se souvenir» des réseaux sans fil
- Techniques d'utilisation sécurisée des appareils sans fil
  - Interdictions d'utilisation du réseau public
  - Chiffrement
    - WEP / WPA / WPA2
    - Sécurisation des mots de passe Wi-Fi
  - Réseau sans fil «oubliant»
  - Évitement des jumeaux maléfiques
    - Noms de réseau mal orthographiés
    - Manque d'exigences de mot de passe au moment prévu
    - Plusieurs réseaux avec des noms similaires

Domaine 4.0 Sécurité en ligne

Objectif 4.1 Naviguer sur le Web en toute sécurité
- Navigateurs bien connus
  - Chrome
  - Internet Explorer
  - Bord
  - Firefox
  - Safari
- Construction d'URL
  - HTTP contre HTTPS
    - Non cryptage vs cryptage
  - Domaines de premier niveau
  - Noms de domaine
  - URL suspectes / falsifiées
    - Fermer les orthographes / fautes d'orthographe
- Techniques de navigation Web sécurisées
  - Utilisation actuelle et mise à jour du navigateur Web
  - Déchiffrer les adresses Web
  - Complément inconnu, plug-in, évitement de la barre d'outils
  - Ne pas cliquer / appuyer sur les publicités et les pop-ups
  - Vérification du protocole
  - Vérification d'URL lors de l'utilisation de liens
  - Taper vs cliquer
  - Bookmarking des sites communs
  - Attention lors de l'utilisation d'appareils mobiles (les URL ne sont pas toujours visibles)

Objectif 4.2 Utiliser le courrier électronique en toute sécurité

- Risques courants d'utilisation des e-mails
    - Attaques d'ingénierie sociale fréquentes
        - Alertes de problème de sécurité
        - Demandes d'informations d'identification utilisateur
        - Offres de suppression de logiciels malveillants / d'assistance informatique
        - Offres gratuites
        - Escroqueries monétaires / d'héritage
        - Demandes d'informations
    - Pièces jointes malveillantes
        - Types de fichiers à haut risque
        - Conformité à la politique / réglementation des pièces jointes
- Techniques d'utilisation sécurisée des e-mails
    - Identification de l'imposteur
        - Nom de l'expéditeur et adresse e-mail
        - Thèmes de la ligne d'objet
        - Tonalité / voix / grammaire de l'expéditeur
        - Lignes de signature
        - Demandes inhabituelles / atypiques provenant de sources apparemment valides
- «Banque» demandant le mot de passe par e-mail
- «IT» demandant des informations personnelles par e-mail
    - Vérification de l'expéditeur
        - Rappelez / rencontrez en personne avant de répondre / de cliquer
    - Envoyez-nous un e-mail sur la conformité à la politique
    - Considérations relatives aux pièces jointes

Objectif 4.3 Utiliser les réseaux sociaux en toute sécurité

- Considérations relatives à la sécurité des réseaux sociaux
    - Partage accidentel d'informations sensibles
    - Commentaires désobligeants
        - Se représenter par rapport à l'organisation
    - Manque de contrôle sur les données et le partage
        - Confidentialité
        - Une fois publié, toujours en ligne
    - Paramètres de sécurité déroutants
    - Opportunités d'ingénierie sociale
    - Comptes falsifiés
- Techniques de réseautage social sûres
    - Alignement sur l'utilisation et les politiques des réseaux sociaux de l'organisation
    - Recherche approfondie et configuration des paramètres de sécurité et de confidentialité
    - Attention au partage de tout élément potentiellement sensible ou préjudiciable à la réputation
information
    - Sécurité des informations d'identification d'administrateur
    - Sensibilisation à l'ingénierie sociale

Objectif 4.4 Utiliser les services cloud en toute sécurité

- Risques liés au service cloud
    - Usurpation de service cloud
    - Changements de fournisseur
        - Acquisitions / fusions
        - En faillite
    - Mélange de comptes professionnels et privés (emplacement de stockage numérique)

- Considérations relatives aux appareils IoT
- Techniques d’utilisation sécurisée des services cloud
    - Approbation organisationnelle pour tout le stockage basé sur le cloud
    - Sauvegardes locales
    - Vigilance supplémentaire des informations d'identification

Exigences en matière de formation continue

Les informations d'identification CyberSAFE 2019 sont valides pendant 1 an à compter de la délivrance du certificat.
Vous devez prendre
le certificat de recertification pour CyberSAFE ou utilisez la version la plus à jour de CyberSAFE identifiant avant la fin de la période d'un an pour maintenir une certification en permanence valide.