

Programme

Information Technology Specialist
Cybersecurity

CERTIFIER

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

La certification Information Technology Specialist : Cybersecurity prouve la maîtrise des principes fondamentaux de :

- la gestion des principes de sécurité ;
- la sécurisation du réseau ;
- la sécurisation des dispositifs de point d'accès ;
- l'évaluation des vulnérabilités et la gestion des risques ;
- la gestion des incidents.

L'examen évalue la compréhension des principes clés de la sécurité, des cadres de travail et de l'état d'esprit requis.

Une personne obtenant cette certification peut démontrer sa conscience aiguë de la manière dont les vulnérabilités exposent une entreprise à des incidents de sécurité, et de la façon dont le respect des principes de sécurité et la mise en œuvre de références peuvent aider à atténuer les risques d'attaque.

Durée : 50 minutes d'examen

Langues : français, anglais

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

1. GÉRER LES PRINCIPES DE SÉCURITÉ

- **Expliquer les principes de sécurité courants**

- Renforcement
- Défense en profondeur
- Confidentialité, intégrité et disponibilité (CIA)
- Code de déontologie
- Sécurité *Zero Trust*
- Confidentialité (y compris les cas d'utilisation de l'IA)
- Politiques de classification et de conservation des données
- Gouvernance de la sécurité

- **Expliquer les cadres de cybersécurité et les meilleures pratiques reconnues par l'industrie**

- Cadre de cybersécurité *NIST, ISO/IEC 2700*
- Contrôles de sécurité critiques *CIS*

- **Expliquer les vulnérabilités, les menaces et les attaques courantes**

- Vulnérabilités, menaces, exploits et risques
- Types d'attaquants
- Raisons des attaques
- Vecteurs d'attaque
- Types d'attaques : logiciels malveillants, attaque par force brute, attaques de sites web et d'applications (injection SQL et dépassement de mémoire tampon), élévation de privilèges, *ransomware*, déni de service/DDoS, *botnets*, attaques physiques, homme du milieu, vulnérabilités de l'IoT, menaces internes, menace persistante avancée (APT), usurpation d'identité

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

1. GÉRER LES PRINCIPES DE SÉCURITÉ

- **Reconnaître les attaques d'ingénierie sociale**
 - Intrusion par ruse et usurpation d'identité
 - Hameçonnage ciblé, hameçonnage, *vishing*, *smishing*, *whaling*, *watering holes*, *pharming*, etc.
 - Redirection malveillante (*QR codes*, URLs raccourcies et faux sites web)
 - Sophistication accrue des attaques due à l'utilisation de l'IA et des robots
- **Expliquer les principes et les procédures de gestion des accès**
 - Authentification, autorisation et comptabilité (AAA)
 - *RADIUS*
 - Méthodes d'authentification multifactorielle (*MFA*)
 - Politiques de mot de passe
 - Authentification biométrique
 - Partage de ressources basé sur le cloud
- **Expliquer comment le chiffrement protège la confidentialité et l'intégrité des données**
 - Chiffrement asymétrique et symétrique,
 - Hachage
 - Certificats
 - *Public key infrastructure* (PKI)
 - Algorithmes de chiffrement forts vs faibles
 - Chiffrement utilisé pour les données en transit, les données au repos et les données en cours d'utilisation

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

2. SÉCURISER LE RÉSEAU

- **Identifier les vulnérabilités associées aux protocoles couramment utilisés**

- TCP, ARP, ICMP, DHCP, DNS, SMTP, ND, CDP/LLDP, SNMP, syslog
- HTTP/HTTPS, FTP/SFTP, Telnet/SSH

- **Décrire le rôle de l'adressage dans la sécurité du réseau**

- Segmentation du réseau (DMZ, VLANs)
- NAT
- Réseaux publics vs privés
- Réseaux internes, externes et de confiance

- **Décrire l'objectif et la fonction des technologies de sécurité réseau**

- Honeypot, serveur proxy, IDS, IPS, portail captif, types de pare-feu (avec état, sans état), ACLs
- VPN, NAC, outils de bureau à distance
- Infrastructure de sécurité cloud (VPC et groupes de sécurité)

- **Valider la sécurité des réseaux sans fil**

- Filtrage des adresses MAC
- Normes et protocoles de chiffrement sans fil, SSID

- **Examiner les journaux de sécurité du réseau pour identifier les anomalies**

- Journaux de pare-feu
- Journaux IDS/IPS

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

3. SÉCURISER LES DISPOSITIFS DE POINT D'ACCÈS

- **Appliquer des paramètres de sécurité pour renforcer les systèmes d'exploitation**
 - Systèmes d'exploitation : *Windows, macOS* et *Linux*
 - *Windows Defender*
 - Autorisations de fichiers et de répertoires
 - Élévation de privilèges
 - Chiffrement de fichiers et de disques
 - Utilisation des références *CIS*
- **Utiliser les outils de point d'accès pour recueillir des informations d'évaluation de la sécurité**
 - *netstat, nslookup, nmap, zenmap, ss*
- **Utiliser les utilitaires de capture de paquets pour identifier les anomalies**
 - *Wireshark, tcpdump*
- **Démontrer une familiarité avec les politiques et les normes de sécurité des points d'accès**
 - Conformité réglementaire (*PCI DSS, HIPAA, RGPD*)
 - *BYOD*
 - Gestion des dispositifs (vérification du statut des mises à jour *Windows*, des mises à jour des applications, des pilotes de périphériques, du *firmware* et des correctifs)
 - Gestion de la configuration
- **Interpréter les journaux système pour identifier les anomalies**
 - *Event Viewer*, console, journaux d'audit, journaux de système et application, *syslog*
 - Serveur et dispositifs de l'utilisateur final

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

3. SÉCURISER LES DISPOSITIFS DE POINT D'ACCÈS

- **Effectuer la suppression des logiciels malveillants**
 - Analyse des systèmes
 - Examen des journaux d'analyse
 - Remédiation des logiciels malveillants
 - Compréhension que les logiciels malveillants peuvent infecter les points de restauration et les sauvegardes,
 - Réponse aux incidents de logiciels malveillants (confinement, mise en quarantaine, traitement et inoculation)

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

4. ÉVALUER LES VULNÉRABILITÉS ET GÉRER LES RISQUES

- **Utiliser les sources de renseignement sur les menaces pour identifier les vulnérabilités potentielles du réseau**

- Utilisations et limitations des bases de données de vulnérabilités
- Vulnérabilités et expositions communes (CVE),
- Rapports de cybersécurité
- Actualités de la cybersécurité
- Services d'abonnement et intelligence collective
- Renseignement sur les menaces ad hoc et automatisé
- Importance de la mise à jour proactive de la documentation et d'autres formes de communication avant, pendant et après les incidents de cybersécurité
- Comment sécuriser, partager et mettre à jour la documentation

- **Expliquer la gestion des risques**

- Vulnérabilité vs risque
- Approches de la gestion des risques, stratégies d'atténuation des risques, niveaux de gravité des risques (faible, moyen, élevé, extrêmement élevé),
- Probabilité de survenue
- Risques associés à des types de données et des classifications de données spécifiques
- Évaluations de la sécurité des systèmes informatiques (sécurité de l'information, gestion des changements, opérations informatiques, assurance de l'information)

- **Expliquer le processus de test de pénétration**

- Identification des vulnérabilités
- Rapport des résultats aux parties prenantes et formulation de recommandations pour l'atténuation
- Reconnaissance active et passive
- Tests (analyse de port et automatisation)

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

5. GÉRER LES INCIDENTS

- **Surveiller les événements de sécurité pour déterminer si une escalade est nécessaire**
 - Rôle du *SIEM* et du *SOAR*
 - Identification des événements suspects au fur et à mesure qu'ils se produisent
 - Différenciation entre un vrai ou faux positif
 - Différenciation entre un vrai ou faux négatif
- **Expliquer le processus de criminalistique numérique et les cadres d'attaque**
 - Sources de preuves (artefacts)
 - Gestion des preuves (préservation des preuves numériques, chaîne de possession)
 - *Cyber Kill Chain*, matrice *MITRE ATT&CK*, *Diamond Model*
 - Tactiques, techniques et procédures (*TTP*)
 - *Pyramid of Pain*
- **Expliquer les éléments de la réponse aux incidents de cybersécurité**
 - Éléments de politique, de plan et de procédure
 - Étapes du cycle de vie de la réponse aux incidents (publication spéciale *NIST 800-61* sections 2.3, 3.1-3.4)
 - Impact des cadres de conformité (*RGPD*, *HIPAA*, *PCI-DSS*, *FERPA*, *FISMA*) sur les exigences de notification et de rapport
- **Expliquer l'importance de la planification de la reprise après sinistre et de la continuité des activités**
 - Catastrophes naturelles et d'origine humaine
 - Caractéristiques des plans de reprise après sinistre (*DRP*) et des plans de continuité des activités (*BCP*)
 - Tous types de sauvegardes de données
 - Pièces de rechange à chaud et à froid
 - Contrôles de reprise après sinistre (*detective*, *preventive*, *corrective*)

IT SPECIALIST : CYBERSECURITY CERTIFICATION

Les objectifs de la certification

5. GÉRER LES INCIDENTS

- **Assister les utilisateurs dans la restauration des données après un incident**
 - Points de restauration
 - Restauration à partir du stockage sur le cloud

APPRENDRE

IT SPECIALIST : CYBERSECURITY CERTIFICATION

E-learning

La certification Information Technology Specialist Cybersecurity est idéale pour qui débute en cybersécurité et souhaite devenir spécialiste du domaine. Les objectifs couvrent les sujets essentiels du métier : principes fondamentaux, sécurité des réseaux, sécurité des terminaux, évaluation des vulnérabilités, gestion des risques et traitement des incidents. La maîtrise de ces fondamentaux constitue une base solide pour réussir l'examen et devenir professionnel de la cybersécurité. Animé par Michael Solomon, expert sécurité de LearnKey, le cours couvre les cinq domaines de l'examen. Un certificat de réussite est délivré à partir de 80 % de bonnes réponses à toutes les évaluations de fin de domaine ; un badge à partir de 90 %.

Le cours couvre :

- la gestion des principes de sécurité ;
- la gestion des concepts de base de la sécurité des réseaux ;
- la gestion des concepts de la sécurité des terminaux ;
- l'évaluation des vulnérabilités et la gestion des risques ;
- la gestion des incidents.

Les utilisateurs amélioreront leur employabilité générale tout en se préparant à l'examen Information Technology Specialist : Cybersecurity.

Ce cours est valable pendant un an en ligne sauf indication contraire, et est limité à l'utilisation par une seule personne. Les licences deviendront inactives si elles sont utilisées par plusieurs personnes.

Durée : 10h38 d'e-learning

Langue : anglais



TESTER

IT SPECIALIST : CYBERSECURITY CERTIFICATION

S'entraîner

Les tests pratiques ITS Cybersecurity sont alignés sur les objectifs de certification.

Les tests pratiques sont des évaluations basées sur la performance qui permettent aux candidats de se familiariser avec l'environnement de test et de gagner en confiance avant le jour de l'examen. Ils préparent les candidats à l'examen Information Technology Specialist : Cybersecurity.

Inclus :

- 1 examen blanc

Langues : français, anglais