Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • IT Specialist

IT Specialist – Cybersecurity

Formation d'initiation à la cybersécurité centrée sur les principes essentiels, la sécurité réseau, la protection des postes de travail, la gestion des vulnérabilités et la réponse aux incidents, pour préparer et réussir la certification IT Specialist – Cybersecurity.

Distributeur officiel Certiport | Centre d'examen Certiport | Learn • Practice • Certify

Durée 23 h (recommandé)	**Examen** ITS–Cybersecurity
Modalité Distanciel	**Niveau** Fondamental / Entry-level

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : Comprendre les principes clés de la cybersécurité, les menaces actuelles et les bonnes pratiques pour protéger l'entreprise.
- **Practice** : Pratique sur cas concrets avec outils de sécurité et exercices alignés sur l'examen IT Specialist.
- **Certify** : passage de l'examen officiel IT Specialist – Cybersecurity dans notre centre Certiport (voucher inclus selon formule).

OBJECTIFS PÉDAGOGIQUES

- Comprendre les bases de la cybersécurité et de la défense en profondeur.
- Identifier les menaces majeures et adopter les bons réflexes.
- Maîtriser les notions essentielles de sécurité réseau et d'accès sécurisés.
- Appliquer les bonnes pratiques des postes et gérer vulnérabilités et incidents.

PUBLIC CIBLE

- Débutants et étudiants souhaitant acquérir une base solide en cybersécurité.
- Techniciens IT et administrateurs juniors visant des rôles en sécurité.
- Toute personne voulant structurer ses connaissances en protection des systèmes d'information.

PRÉREQUIS

- Lecture niveau 8e année avec bonnes capacités de raisonnement et pensée critique.
- Notions d'algèbre de base et connaissances générales en systèmes d'exploitation et réseaux simples.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Principes essentiels de sécurité (Essential Security Principles)

Définir les principes essentiels de sécurité

- Vulnérabilités, menaces, exploits et risques ; vecteurs d'attaque ; durcissement (hardening) ; défense en profondeur (defense-in-depth) ; confidentialité, intégrité et disponibilité (CIA) ; types d'attaquants ; motifs d'attaque ; code d'éthique.

Expliquer les menaces et vulnérabilités courantes

- Malware, ransomware, attaques par déni de service (DoS), botnets, attaques d'ingénierie sociale (tailgating, spear phishing, phishing, vishing, smishing, etc.), attaques physiques, attaques de type man-in-the-middle, vulnérabilités IoT, menaces internes (insider threats), menaces persistantes avancées (APT).

Expliquer les principes de gestion des accès

- Authentication, authorization et accounting (AAA) ; RADIUS ; authentification multifactorielle (MFA) ; politiques de mots de passe.

Expliquer les méthodes de chiffrement et leurs applications

- Types de chiffrement ; hachage (hashing) ; certificats ; infrastructure à clés publiques (PKI) ; algorithmes forts vs faibles ; états des données et chiffrement approprié (données en transit, au repos, en cours d'utilisation) ; protocoles utilisant le chiffrement.

Concepts de base de la sécurité réseau (Basic Network Security Concepts)

Décrire les vulnérabilités des protocoles TCP/IP

- Vulnérabilités associées aux protocoles TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS.

Expliquer l'impact des adresses réseau sur la sécurité

- Adresses IPv4 et IPv6, adresses MAC, segmentation réseau, notation CIDR, NAT, différence entre réseaux publics et privés.

Décrire l'infrastructure réseau et les technologies associées

- Architecture de sécurité réseau, DMZ, virtualisation, cloud, honeypot, serveur proxy, systèmes de détection et de prévention d'intrusion (IDS/IPS).

Configurer un réseau sans fil SoHo sécurisé

- Filtrage d'adresses MAC, standards et protocoles de chiffrement Wi-Fi, paramètres SSID.

2.5 Mettre en œuvre des technologies d'accès sécurisé

- Listes de contrôle d'accès (ACL), pare-feu, VPN, Network Access Control (NAC).

Concepts de sécurité des endpoints (Endpoint Security Concepts)

Décrire les concepts de sécurité des systèmes d'exploitation

- Windows, macOS et Linux ; fonctionnalités de sécurité, y compris Windows Defender et les pare-feux locaux ; utilisation de la ligne de commande (CLI) et de PowerShell ; permissions de fichiers et répertoires ; escalade de privilèges.

Utiliser les outils appropriés de sécurité des endpoints

- Familiarisation avec des outils tels que netstat, nslookup, tcpdump pour collecter des informations de sécurité et diagnostiquer les communications réseau.

Vérifier que les endpoints respectent les politiques de sécurité

- Gestion des inventaires matériels et logiciels (asset management), déploiement de programmes, sauvegarde des données, conformité réglementaire (PCI DSS, HIPAA, GDPR), gestion des appareils personnels (BYOD : chiffrement des données, distribution d'applications, gestion de la configuration).

Mettre en œuvre les mises à jour logicielles et matérielles

- Windows Update, mises à jour applicatives, pilotes de périphériques, firmware, patch management.

Interpréter les journaux système

- Utilisation de l'Observateur d'événements (Event Viewer), journaux d'audit, journaux système et applicatifs, syslog, identification des anomalies dans les logs.

Connaître les principes de base de la suppression de malware

- Analyse des systèmes, examen des journaux d'analyse, processus de remédiation après détection de malware.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Analyse des vulnérabilités et gestion des risques (Vulnerability Assessment and Risk Management)

Expliquer la gestion des vulnérabilités

- Identification, gestion et atténuation des vulnérabilités ; reconnaissance active et passive ; tests (scan de ports, automatisation des analyses).

Utiliser le renseignement sur les menaces (threat intelligence)

- Utilisation et limites des bases de vulnérabilités ; outils standards pour évaluer les vulnérabilités et formuler des recommandations, politiques et rapports ; Common Vulnerabilities and Exposures (CVEs), rapports de cybersécurité, actualités, services d'abonnement et intelligence collective ; renseignement ad hoc et automatisé ; importance de la mise à jour de la documentation et de la communication avant, pendant et après les incidents ; sécurisation, partage et mise à jour de la documentation.

Expliquer la gestion des risques

- Différence entre vulnérabilité et risque ; hiérarchisation des risques ; approches de gestion ; stratégies d'atténuation ; niveaux de risque (faible, moyen, élevé, extrêmement élevé) ; risques associés aux types de données et à leur classification ; évaluations de sécurité des systèmes informatiques (sécurité de l'information, gestion des changements, opérations informatiques, assurance de l'information).

Expliquer l'importance du plan de reprise après sinistre et de continuité d'activité

- Catégories de sinistres (catastrophes naturelles et d'origine humaine), caractéristiques des plans de reprise d'activité (DRP) et de continuité d'activité (BCP), sauvegardes, contrôles de reprise après sinistre (détectifs, préventifs et correctifs).

Gestion des incidents (Incident Handling)

Surveiller les événements de sécurité et savoir quand escalader

- Rôle des solutions SIEM et SOAR ; surveillance des données réseau pour identifier les incidents (captures de paquets, entrées de journaux, etc.) ; identification d'événements suspects en temps réel.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Expliquer la recherche de preuves numériques et l'attribution des attaques

- Cyber Kill Chain, matrice MITRE ATT&CK, Diamond Model ; tactiques, techniques et procédures (TTP) ; sources de preuves (artifacts) ; gestion des preuves (préservation des preuves numériques, chaîne de conservation/chain of custody).

Expliquer l'impact des cadres de conformité sur la gestion des incidents

- Cadres de conformité (GDPR, HIPAA, PCI-DSS, FERPA, FISMA) ; exigences en matière de rapports et de notifications après incidents.

Décrire les éléments de la réponse aux incidents de cybersécurité

- Politiques, plans et procédures de réponse aux incidents ; étapes du cycle de vie de la réponse aux incidents selon le NIST SP 800-61 (préparation, détection et analyse, confinement, éradication, récupération, retour d'expérience).