Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • IT Specialist – Network Security

IT Specialist – Network Security

Cette formation prépare à la certification IT Specialist – Network Security et couvre les bases de la cybersécurité réseau, incluant la défense en profondeur, la sécurisation des systèmes et équipements, la protection des utilisateurs et les bonnes pratiques de navigation.

Durée	Examen
32 h (recommandé)	IT Specialist – Network Security
Modalité	**Niveau**
Distanciel	Fondamental / Junior

Distributeur officiel Certiport

Centre d'examen Certiport

Learn • Practice • Certify

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : Bases de la sécurité réseau : CIA, menaces, vulnérabilités et politiques.
- **Practice** : Exercices pratiques sur Windows et Linux : pare-feu, sécurité des postes, outils réseau et analyse d'incidents.
- **Certify** : préparation structurée aux domaines d'objectifs de l'examen IT Specialist – Network Security et passage de l'examen dans notre centre.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les principes de base de la sécurité et les risques liés aux menaces et vulnérabilités.
- Sécuriser les systèmes d'exploitation via durcissement, mises à jour et gestion des droits.
- Protéger les équipements réseau avec pare-feu, VPN et protocoles sécurisés.
- Assurer la sécurité des utilisateurs et se préparer à l'examen IT Specialist – Network Security.

PUBLIC CIBLE

- Pour étudiants et débutants en informatique avec des notions en réseaux et systèmes.
- Pour techniciens IT juniors et support souhaitant renforcer leurs compétences en cybersécurité.
- Pour les personnes en reconversion vers les métiers de la sécurité informatique.

PRÉREQUIS

- Lecture au niveau collège avec bonne compréhension écrite et connaissances de base en systèmes d'exploitation et réseaux.
- Capacités de réflexion critique et de résolution de problèmes requises.

© 2026 Smartfuture — IT Specialist – Network Security

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Défense en profondeur

Identifier les principes fondamentaux de la sécurité

- Confidentialité, intégrité, disponibilité, non-répudiation, menace, risque, vulnérabilité, principe du moindre privilège, surfaces d'attaque (y compris IoT).

Définir et appliquer la sécurité physique

- Sécurisation des locaux et des sites.
- Sécurisation physique des ordinateurs et postes de travail.
- Gestion sécurisée des périphériques et supports amovibles.
- Contrôles physiques : sas (mantraps), accès contrôlés, etc.

Identifier les types de politiques de sécurité

- Contrôles administratifs (procédures, règles internes, conformité).
- Contrôles techniques (mécanismes techniques de protection).

Identifier les types d'attaques

- Débordement de mémoire (buffer overflow).
- Virus, virus polymorphes, vers, chevaux de Troie.
- Spyware, ransomware, adware.
- Rootkits, portes dérobées (backdoors).
- Vulnérabilités et attaques de type zero-day.
- Attaques par déni de service (DoS).
- Méthodes d'attaque courantes et types de vulnérabilités.
- Cross-site scripting (XSS), injection SQL.
- Attaques par force brute.
- Attaques de type homme-du-milieu (MITM) et homme-dans-le-navigateur (MITB).
- Ingénierie sociale.
- Keyloggers (logiciels et matériels), bombes logiques.

Identifier les types de sauvegardes et de restaurations

- Sauvegarde complète.
- Sauvegarde incrémentielle.
- Sauvegarde différentielle.

© 2026 Smartfuture — IT Specialist – Network Security

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Sécurité des systèmes d'exploitation

Identifier les protections côté client et côté serveur

- Séparation des rôles et des services.
- Durcissement des systèmes (hardening).
- Gestion des correctifs (patch management).
- Réduction de la surface d'attaque.
- Stratégies de groupe (gpupdate, gpresult).
- Mises à jour DNS sécurisées.
- Contrôle de compte utilisateur (UAC).
- Maintien à jour du système d'exploitation et des logiciels côté client.
- Chiffrement des dossiers hors ligne.
- Politiques de restriction logicielle.

Configurer l'authentification des utilisateurs

- Authentification multi-facteur (MFA).
- Application de politiques de mot de passe.
- Accès distant sécurisé.
- Utilisation de comptes secondaires pour les tâches administratives (Run As, sudo).
- Création de comptes et groupes locaux et de domaine.
- Notions de Kerberos.

Gérer les permissions sous Windows et Linux

- Permissions sur fichiers et dossiers.
- Permissions de partage.
- Héritage des permissions.
- Effets des déplacements ou copies de fichiers sur le même disque ou un autre.
- Gestion de plusieurs groupes avec des niveaux de permissions différents.
- Prise de possession (take ownership).
- Délégation d'administration.

© 2026 Smartfuture — IT Specialist – Network Security

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Faciliter la non-répudiation via les stratégies d'audit et les journaux

- Types d'événements auditables.
- Configuration de l'audit et choix des éléments à auditer.
- Choix de l'emplacement de stockage des logs.
- Analyse et revue des journaux.

Démontrer la compréhension du chiffrement

- Chiffrement de fichiers et dossiers et impact sur les copies/déplacements.
- Chiffrement de disque, TPM.
- Processus de communication sécurisée (email, messagerie, réseaux sociaux).
- Chiffrement VPN et méthodes associées.
- Clé publique / clé privée, certificats et services de certificats.
- BitLocker.

Sécurité des équipements réseau

Mettre en œuvre la sécurité sans fil

- Identifier les types de sécurité Wi-Fi et la robustesse des différents modes de chiffrement.
- Configuration et gestion des SSID.
- Filtrage par adresse MAC.
- Paramètres par défaut et configuration initiale (OOBE).

Identifier le rôle des dispositifs de protection réseau

- Objectif d'un pare-feu.
- Pare-feu matériel vs logiciel, pare-feu réseau vs hôte.
- Inspection avec état (stateful) vs sans état (stateless).
- Notion de référentiels et baselines de sécurité.
- Systèmes de détection d'intrusion (IDS) et de prévention (IPS).
- SIEM (Security Information and Event Management).
- Filtrage de contenu, listes noires et listes blanches.

© 2026 Smartfuture — IT Specialist – Network Security

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Identifier les méthodes d'isolation réseau

- Routage et segmentation.
- Honeynet.
- Réseaux périmétriques (DMZ).
- NAT et PAT.
- VPN et IPsec.
- Air-gap network.
- DirectAccess.
- VLAN (Virtual LAN).

Identifier les concepts de sécurité des protocoles

- Tunneling.
- DNSSEC.
- Sniffing réseau et analyse de trafic.
- Ports applicatifs courants : FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP.

Poste de travail et usage sécurisé

Mettre en œuvre la protection du courrier électronique

- Mécanismes antispam.
- Lutte contre le spoofing, phishing et pharming.
- Protection côté client (filtrage, règles, signalement).
- Formation et sensibilisation des utilisateurs.

Gérer la sécurité du navigateur

- Paramètres de sécurité du navigateur.
- Gestion du cache et suppression des données de navigation.
- Navigation privée et limites associées.

© 2026 Smartfuture — IT Specialist – Network Security

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Installer et configurer des solutions anti-malware et antivirus

- Installation, désinstallation et réinstallation.
- Mise à jour des signatures et du moteur.
- Planification de scans réguliers.
- Remédiation et actions après détection.
- Analyse et investigation des alertes.

© 2026 Smartfuture — IT Specialist – Network Security