MFE-IT

Formation CompTIA Security+

Cybersécurité fondamentale — examen officiel inclus

CompTIA Security+ (SY0-701)

Référence : SM-CS+

Durée : 4 jours • **Volume horaire : 28 h**

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

Cette formation « CompTIA Security+ : cybersécurité fondamentale & examen officiel inclus » vous prépare à obtenir la certification internationale CompTIA Security+ (SY0-701), reconnaissant des compétences de base en sécurité informatique. Les cours couvrent les concepts clés comme la sécurité réseau, la cryptographie, la gestion des accès, les menaces et les opérations de sécurité.

Entraînements pratiques, simulations d'examen et QCM vous aideront à maîtriser les objectifs de l'examen. À l'issue, vous serez prêt à passer l'examen officiel et à valider votre expertise. Obtenir cette certification renforce votre crédibilité dans les métiers IT et cybersécurité.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les principes fondamentaux de la sécurité de l'information : confidentialité, intégrité et disponibilité.
- Identifier les menaces, les vulnérabilités et les types d'attaques courants (malware, phishing, rançongiciels, etc.).
- Sécuriser les réseaux et les communications (pare-feu, VPN, segmentation).
- Appliquer la cryptographie et la gestion des clés (chiffrement, PKI, HSM, certificats).
- Mettre en œuvre la gestion des identités et des accès (MFA, politiques d'accès, comptes à privilèges).
- Mener des opérations de sécurité et répondre aux incidents (détection, surveillance, analyse forensique).
- Se préparer efficacement et réussir l'examen officiel CompTIA Security+ (SY0-701).

PRÉREQUIS

- Connaissances de base en administration IT, systèmes et réseaux (souhaitées mais pas obligatoires).
- Une expérience d'environ deux ans en administration système / réseau est recommandée pour maximiser les chances de succès à l'examen.
- La certification CompTIA Network+ est un plus mais non obligatoire.
- Parce que chaque participant est unique, un entretien personnalisé avec notre expert nous permet de concevoir une formation parfaitement alignée avec ses objectifs, son niveau et ses enjeux professionnels.

PUBLIC VISÉ

- Professionnels IT souhaitant se spécialiser en cybersécurité ou valider leurs compétences par une certification reconnue.
- Administrateurs systèmes, ingénieurs réseau ou support technique souhaitant approfondir leurs connaissances de la sécurité.
- Techniciens, analystes sécurité, consultants, et toute personne visant un rôle de cybersécurité de niveau débutant/intermédiaire.

PROGRAMME DÉTAILLÉ

Module 1 — Introduction à la cybersécurité et objectifs de certification

- Vue d'ensemble de la certification CompTIA Security+ (SY0-701) et de son importance professionnelle.
- Structure de l'examen, formats de questions (QCM et performance-based).

Module 2 — Concepts fondamentaux de sécurité

- Principes de confidentialité, intégrité, disponibilité (CIA).
- Modèles de contrôle d'accès, authentification, autorisation, Zero Trust.

Module 3 — Menaces, vulnérabilités et attaques

- Types de menaces (malware, phishing, ransomware, etc.).
- Techniques de reconnaissance, vecteurs d'attaque, mitigation.

Module 4 — Sécurité réseau et communications

- Sécurisation des réseaux (firewalls, VPN, segmentation).
- Protocoles sécurisés, déploiement sécurisé des services.

Module 5 — Cryptographie et gestion des clés

- Concepts de cryptage, clés, PKI, HSM, certificats.
- Mise en œuvre pratique des méthodes cryptographiques.

Module 6 — Gestion des identités et des accès (IAM)

- MFA, politiques d'accès, comptes privilégiés, IAM dans les environnements hybrides.

Module 7 — Opérations de sécurité et réponse aux incidents

- Détection, surveillance, analyse forensique de base.
- Stratégies de réponse, frameworks de gestion des incidents.

Module 8 — Préparation à l'examen CompTIA Security+

- Simulations d'examen, QCM, questions performance-based basées sur les objectifs officiels.
- Conseils pour la réussite, gestion du temps, checklist de révision.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

MFE-IT privilégie un format en mini-groupe (1 à 3 participants), garanti dès un seul inscrit (sauf cas de force majeure). La formation se déroule en distanciel (classe virtuelle synchrone, sessions également enregistrées) ou en présentiel dans vos locaux. Le programme alterne apports théoriques, entraînements pratiques et simulations d'examen.

Format ultra-personnalisé

Un entretien préalable est organisé avec le participant et/ou un représentant de l'entreprise afin d'adapter le contenu à son niveau, à ses besoins et à ses enjeux professionnels.

Moyens techniques

Un support pédagogique complet est remis à chaque participant. Les sessions s'appuient sur des labs, des QCM et des simulations d'examen. Une connexion internet et un poste de travail sont requis pour les sessions à distance.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au moyen de quiz, de mises en situation et de simulations d'examen. Une attestation de fin de formation est remise à l'issue du parcours.

Accessibilité et handicap

Nos formations peuvent être adaptées aux personnes en situation de handicap. Merci de nous contacter en amont afin d'étudier ensemble les modalités d'accueil et d'aménagement (référent handicap : contact@mfe-it.com).

Assistance post-formation

Chaque participant bénéficie d'un accompagnement de 30 jours après la formation pour toute question relative au contenu abordé.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT s'engage à étudier toute demande d'aménagement. Un échange avec notre référent handicap permet d'adapter les conditions d'accueil et de déroulement de la formation.

Modalités pédagogiques et techniques

Formation en distanciel (classe virtuelle synchrone) ou en présentiel dans vos locaux, en mini-groupe. Alternance de théorie, d'entraînements pratiques et de simulations d'examen.

Moyens du formateur

Formateur expert certifié, support de cours complet, labs et simulations d'examen.

Validation et sanction

Attestation de fin de formation. Cette formation inclut le passage de l'examen officiel CompTIA Security+ (SY0-701).

Type de formation

Action de formation professionnelle continue : acquisition et perfectionnement de compétences.

Suivi de l'exécution

Feuilles de présence signées, évaluations en cours de formation et attestation de fin de formation.

Modalités d'évaluation

Quiz, mises en situation, QCM et simulations d'examen tout au long de la formation.

Aide à l'orientation

La CompTIA Security+ s'inscrit dans un parcours cybersécurité (CompTIA Network+, CySA+, PenTest+).