

## Formation CompTIA S+, Les bases de la cybersécurité

### Présentation

Ce programme de formation en cybersécurité couvre les concepts de base, la sécurité des réseaux, et la gestion des identités et des accès. Il inclut également la sécurité des systèmes et des applications, la cryptographie, et la réponse aux incidents. Le programme aborde la conformité et les bonnes pratiques, propose des cas pratiques et simulations, et prépare à la certification CompTIA Security+.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

### Objectifs de la formation

- Comprendre les concepts de base de la cybersécurité.
- Identifier et atténuer les risques de sécurité.
- Mettre en œuvre des solutions pour protéger les systèmes et les réseaux.
- Répondre aux incidents de sécurité et appliquer les bonnes pratiques.
- Se préparer à la certification CompTIA Security+.

### Prérequis

- Connaissances de base en réseaux et systèmes d'exploitation.
- Aucune expérience préalable en cybersécurité n'est requise, mais une compréhension des concepts informatiques est recommandée.

### Public

- Débutants en cybersécurité.
- Administrateurs système et réseau.
- Techniciens en support informatique.
- Professionnels souhaitant valider leurs compétences en sécurité.

### Programme de la formation



**Module 1 : Concepts de base de la cybersécurité**

- Introduction à la cybersécurité et aux concepts de confidentialité, intégrité et disponibilité (CIA).
- Présentation des menaces, vulnérabilités et risques.
- Principes de gestion des risques et de conformité.

**Module 2 : Sécurité des réseaux**

- Concepts de sécurisation des réseaux (pare-feu, VPN, IDS/IPS).
- Détection et prévention des attaques réseau (DDoS, spoofing, etc.).
- Sécurisation des protocoles réseau (TCP/IP, DNS, DHCP).

**Module 3 : Gestion des identités et des accès**

- Authentification multifacteur (MFA) et gestion des identités (IAM).
- Sécurisation des services d'annuaire (LDAP, Active Directory).
- Gestion des certificats numériques et des clés.

**Module 4 : Sécurité des systèmes et des applications**

- Sécurisation des systèmes d'exploitation (Windows, Linux).
- Protection contre les vulnérabilités courantes (OWASP Top 10).
- Meilleures pratiques de développement sécurisé (SDLC).

**Module 5 : Cryptographie**

- Principes de base de la cryptographie (chiffrement symétrique et asymétrique).
- Utilisation des certificats numériques et des infrastructures à clé publique (PKI).
- Applications pratiques de la cryptographie (SSL/TLS, chiffrement des données).

**Module 6 : Réponse aux incidents**

- Étapes de la réponse aux incidents (préparation, détection, analyse, confinement, éradication, récupération).
- Utilisation des outils de forensic et d'analyse post-incident.
- Rédaction de rapports d'incidents et communication avec les parties prenantes.

**Module 7 : Conformité et bonnes pratiques**

- Présentation des réglementations et normes (GDPR, ISO 27001, NIST).
- Mise en œuvre des politiques de sécurité et des contrôles d'accès.
- Gestion des audits de sécurité et des évaluations de risques.

**Module 8 : Cas pratiques et simulations**

- Scénarios de détection et de réponse aux menaces.
- Simulation de tests d'intrusion et de scans de vulnérabilités.
- Exercices pratiques de sécurisation de réseaux et d'applications.

**Module 9 : Préparation à la certification**

- Revue des objectifs de l'examen CompTIA Security+.
- Examen blanc et analyse des résultats.
- Conseils et stratégies pour réussir la certification.

## Organisation

**Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

**Moyens pédagogiques et techniques**

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.

- Supports de cours, ressources documentaires et références mis à disposition par le formateur

## **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

### **En amont de la formation** *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

### **Tout au long de la formation**

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

### **À l'issue de la formation** *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

## **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.