

Mis à jour le 18/08/2025

S'inscrire

Formation Secure MFT Compliance

2 jours (14 heures)

Présentation

Secure MFT Compliance est une formation dédiée à la sécurisation et à la mise en conformité des transferts de fichiers critiques. Les solutions de Managed File Transfer (MFT) sont devenues incontournables pour garantir la confidentialité, l'intégrité et la traçabilité des données échangées, tout en respectant les exigences réglementaires (RGPD, ISO 27001, PCI DSS, HIPAA).

Notre formation vous permettra de comprendre les principes du MFT, de mettre en place des transferts sécurisés, de gérer les accès et de produire des rapports d'audit.

Vous apprendrez à intégrer une solution MFT dans votre écosystème IT (cloud, hybride, on-premises) et à automatiser les flux pour plus d'efficacité.

À l'issue, vous serez capable de piloter un projet MFT conforme aux standards de sécurité et de gouvernance, de préparer vos audits réglementaires et de sensibiliser vos équipes aux bonnes pratiques.

Comme toutes nos formations, celle-ci s'appuie sur les dernières solutions disponibles et leur version à jour.

Objectifs

- Sécuriser et automatiser vos transferts de fichiers
- Gérer les accès et produire des audits de conformité
- Répondre aux exigences RGPD, ISO 27001, PCI DSS, HIPAA
- Intégrer le MFT à vos systèmes IT
- Préparer vos audits réglementaires
- Appliquer les bonnes pratiques de gouvernance

Public visé

- Responsables sécurité et conformité IT
- Managers IT et responsables support
- Administrateurs systèmes & réseaux
- Auditeurs et consultants conformité
- Équipes de support et d'exploitation

Pré-requis

- Notions de sécurité IT
- Bases en conformité réglementaire

Programme de notre formation Secure MFT Compliance

Introduction au MFT et enjeux de conformité

- Définition du MFT et différences avec SFTP/FTPS
- Enjeux de sécurité et conformité (RGPD, PCI DSS, HIPAA)
- Rôle du MFT dans la gouvernance
- Cadres réglementaires à respecter
- Cartographie des flux sensibles
- Atelier : cartographier les flux de fichiers sensibles

Sécurisation des transferts et protocoles utilisés

- Protocoles : SFTP, FTPS, HTTPS, AS2
- Chiffrement (AES, RSA, TLS)
- Gestion certificats et clés
- Authentification : MFA, certificats, tokens
- Bonnes pratiques de sécurité
- Atelier : transfert sécurisé avec chiffrement

Gouvernance et contrôle des accès

- Gestion des rôles et identités (IAM, RBAC)
- Segmentation et moindre privilège
- Audit et traçabilité
- Supervision et alertes
- Réponse aux incidents
- Atelier : configurer rôles utilisateurs et audit

Intégration du MFT dans l'écosystème IT

- Déploiement on-prem, cloud, hybride
- Intégration AD, LDAP, SIEM

- Automatisation via scripts et API REST
- Connexion ERP & outils métiers
- Gestion multi-environnements
- Atelier : automatisation d'un flux de transfert

Conformité et audit des transferts

- Réglementations : RGPD, ISO 27001, PCI DSS, HIPAA
- Rapports et preuves de conformité
- Vérification d'intégrité
- Préparation audit externe
- Reporting et conservation
- Atelier : générer un rapport de conformité

Bonnes pratiques et roadmap MFT

- Critères de choix d'une solution MFT
- Plan de mise en conformité
- Plans PRA/PCA et résilience
- Sensibilisation des équipes
- Perspectives : MFT et Zero Trust
- Atelier : simulation d'un plan de mise en conformité

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.