RIASEC : Ic

M1882
ARCHITECTE SÉCURITÉ INFORMATIQUE

Emploi cadre

Transition numérique

Autres emplois décrits

- Architecte cybersécurité
- Security architect

Définition

L'architecte sécurité informatique conçoit et supervise la stratégie de sécurité des systèmes d'information.

- Évalue et analyse les risques et vulnérabilités de sécurité des données informatiques face aux menaces extérieures et cyberattaques
- Conçoit des mesures de sécurité adaptées pour répondre aux besoins de toute entreprise informatique
- Supervise des procédures de récupération après sinistre en s'assurant de la conformité et réglementation en vigueur
- Implémente des solutions de sécurité et applique les processus de vérification
- Forme le personnel aux protocoles de sécurité et aux meilleures pratiques
- Assure une veille technologique constante pour anticiper les menaces potentielles
- Garant de la confidentialité, l'intégrité et la disponibilité des données

Accès à l'emploi

Ce métier est accessible avec un Bac + 5 Master, un diplôme d'ingénieur en informatique, sécurité des systèmes d'information. Une certification professionnelle en cybersécurité serait un atout.

Certifications et diplômes :

- Expert en architectures systèmes, réseaux et sécurité informatique
- Master mention cybersécurité
- Ingénieur spécialisé en sécurité pour les systèmes informatiques et les communications, diplômé d'Eurecom
- Expert en architectures systèmes-réseaux et en sécurité informatique
- Master mention informatique

Compétences

Savoir-faire

Savoir-faire principaux

Communication, Création, Innovation, Nouvelles technologies

- Concevoir des architectures de sécurité — Transition numérique
- Collaborer avec des équipes de développement pour intégrer la sécurité — Transition numérique
- Documenter les procédures de sécurité — Transition numérique

Production, Construction, Qualité, Logistique

- Analyser les risques de sécurité pour les systèmes informatiques — Transition numérique
- Implémenter des solutions de sécurité informatique — Transition numérique

Pilotage, Gestion, Cadre réglementaire

- Assurer la conformité réglementaire en matière de sécurité

Management, Social, Soin

- Former les utilisateurs aux bonnes pratiques de sécurité informatique — Transition numérique

Savoir-faire secondaires

Communication, Création, Innovation, Nouvelles technologies

- Piloter les fonctionnalités des équipements et systèmes de sécurité informatique — Transition numérique
- Mener des recherches sur les menaces émergentes — Transition numérique

Production, Construction, Qualité, Logistique

- Evaluer l'impact des nouvelles technologies sur la sécurité — Transition numérique
- S'assurer du respect des règles de cybersécurité — Transition numérique
- Savoir reconnaître les données sensibles pour la cybersécurité — Transition numérique
- Configurer des pare-feu et des systèmes de détection d'intrusions — Transition numérique

Coopération, Organisation et Développement de ses compétences

- Respecter les normes de sécurité informatique dans l'assistance — Transition numérique
- Respecter les normes de sécurité informatique dans le développement — Transition numérique
- Développer ses compétences en continu, notamment dans les technologies émergentes — Transition numérique

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

Pilotage, Gestion, Cadre réglementaire

- Suivre les évolutions juridiques du marché en termes de sécurité informatique afin de garantir la conformité du SI au droit individuel et collectif
- Négocier avec les fournisseurs de solutions IT et de sécurité — Transition numérique

Développement économique

- Optimiser les processus de sécurité pour réduire les coûts — Transition numérique

Savoir-être professionnels

- Organiser son travail selon les priorités et les objectifs
- Faire preuve de rigueur et de précision
- Etre force de proposition

Savoirs

Domaines d'expertise

- **Audit de sécurité informatique** — Transition numérique
- **Veille technologique en sécurité informatique** — Transition numérique
- Conseil en sécurité informatique — Transition numérique
- Analyse de la vulnérabilité des systèmes informatiques — Transition numérique
- Intégration de systèmes de détection d'intrusions — Transition numérique
- Optimisation des processus de sécurité informatique — Transition numérique
- Utilisation de logiciels de gestion de la sécurité — Transition numérique
- Formation en sécurité informatique — Transition numérique
- **Formation des utilisateurs sur les pratiques de sécurité** — Transition numérique

Normes et procédés

- **Gestion de la sécurité des réseaux** — Transition numérique
- Analyse de risques en sécurité informatique — Transition numérique

Techniques professionnelles

- Gestion des incidents de sécurité — Transition numérique
- Mise à jour de sécurité informatique — Transition numérique

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail

Contextes de travail

Conditions de travail et risques professionnels

- Déplacements professionnels
- Possibilité de télétravail
- Travail en mode projet

Horaires et durée du travail

- Travail en journée
- Travail selon un rythme irrégulier et des pics d'activité

Publics spécifiques

- Clientèle d'entreprises

Statut d'emploi

- Salarié secteur privé (CDI, CDD)
- Salarié secteur public
- Travailleur indépendant

Types de structures

- Entreprises et milieux professionnels

Secteurs d'activité

- Informatique et télécommunication

© Copyright octobre 2026 France Travail - Reproduction et diffusion interdites sans l'accord de France Travail