M1866
PENTESTEUR / PENTESTEUSE

Transition numérique

Autres emplois décrits

- Expert / Experte en tests d'intrusion - sécurité des systèmes d'information

Définition

Le Pentesteur ou testeur d'intrusion, est un spécialiste dans la sécurité des systèmes informatiques et des réseaux d'une organisation en simulant des attaques malveillantes.

- Évalue la sécurité des systèmes informatiques par des tests d'intrusion ciblés
- Identifie les vulnérabilités et propose des solutions pour les corriger
- Réalise des audits de sécurité pour prévenir les risques potentiels
- Forme le personnel à la sécurité informatique
- Collabore avec les équipes de développement pour renforcer la sécurité des applications
- Documente et rapporte les résultats des tests d'intrusion après analyse des risques de corruption à la direction technique

Accès à l'emploi

Ce métier est accessible avec un niveau Bac + 3 à Bac + 5 en programmation, systèmes et réseaux, spécialisation en sécurité informatique, avec des cours spécialisés en test d'intrusion, cryptographie.
Des certifications spécialisées seraient un plus telles OSCP (reconnaissance en test d'intrusion) ou CISSP (certification en sécurité de l'information)

Certifications et diplômes :

- Expert en cybersécurité des systèmes d'information
- Spécialiste en cybersécurité
- Licence pro mention métiers de l'informatique : administration et sécurité des systèmes et des réseaux
- Expert de la sécurité des données, des réseaux et des systèmes
- Expert en cybersécurité et sécurité informatique
- Expert en cybersécurité (MS)
- Licence pro mention métiers de l'informatique : systèmes d'information et gestion de données
- Licence pro mention métiers des réseaux informatiques et télécommunications
- Expert en sécurité digitale
- Expert en sécurité des développements informatiques
- Expert en cybersécurité
- Expert en développement de solutions de cybersécurité
- Spécialiste en cybersécurité (MS)

Compétences

Savoir-faire

Savoir-faire principaux

Production, Construction, Qualité, Logistique

- Analyser les risques de sécurité pour les systèmes informatiques — Transition numérique
- Communiquer clairement les risques de sécurité aux parties prenantes
- Evaluer, prévenir, et gérer les risques et la sécurité

Communication, Création, Innovation, Nouvelles technologies

- Concevoir des scénarios de test d'intrusion adaptés — Transition numérique
- Tester un logiciel, un système d'informations, une application — Transition numérique
- Utiliser des outils de cryptographie pour sécuriser les données — Transition numérique

Coopération, Organisation et Développement de ses compétences

- Communiquer, lire et rédiger des documents techniques, des rapports, des notes en anglais
- Documenter les interventions et les anomalies rencontrées

Savoir-faire secondaires

Production, Construction, Qualité, Logistique

- Mener un processus de test en cybersécurité — Transition numérique
- Evaluer l'efficacité des mesures de sécurité en place
- Développer des stratégies de gestion des risques
- Réaliser des audits de sécurité périodiques
- Identifier les anomalies dans les résultats des tests

Communication, Création, Innovation, Nouvelles technologies

- Analyser les logs pour identifier les tentatives d'intrusion — Transition numérique
- Collaborer avec des équipes de développement pour intégrer la sécurité — Transition numérique
- Développer ses compétences en cybersécurité — Transition numérique
- Piloter les fonctionnalités des équipements et systèmes de sécurité informatique — Transition numérique
- Mettre à jour un dossier, une base de données — Transition numérique
- Réaliser une veille technique ou technologique pour anticiper les évolutions — Transition numérique

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

Coopération, Organisation et Développement de ses compétences

- Actualiser régulièrement ses connaissances

Management, Social, Soin

- Evaluer les besoins en formation sécurité du personnel

Savoir-être professionnels

- Faire preuve d'autonomie
- Faire preuve de rigueur et de précision
- Etre ouvert aux changements

Savoirs

Domaines d'expertise

- Analyse forensique numérique — Transition numérique
- Conseil en sécurité informatique — Transition numérique
- Evaluation de la sécurité des réseaux — Transition numérique
- Gestion des accès et des identités — Transition numérique
- Protection contre les malwares — Transition numérique
- Réseaux informatiques et télécoms — Transition numérique
- Sécurité des transactions électroniques — Transition numérique
- Surveillance de la sécurité des systèmes — Transition numérique

Normes et procédés

- **Analyse de risques en sécurité informatique** — Transition numérique
- Cryptographie appliquée — Transition numérique
- Détection des intrusions réseau — Transition numérique
- Normes de sécurité
- Protection des données personnelles — Transition numérique
- Gestion des menaces et des vulnérabilités — Transition numérique

Techniques professionnelles

- Gestion des accès sécurisés
- Techniques de reporting — 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
- En milieu nucléaire
- Possibilité de télétravail

Horaires et durée du travail

- Travail en horaires décalés
- 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)
- 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