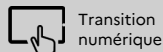


M1866**PENTESTEUR / PENTESTEUSE**Transition
numérique

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

Cet emploi est accessible avec une formation de 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
- Communiquer clairement les risques de sécurité aux parties prenantes
- Evaluer, prévenir, et gérer les risques et la sécurité

Transition numérique

Transition écologique

Communication, Création, Innovation, Nouvelles technologies

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

Transition numérique

Transition numérique

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
- Evaluer l'efficacité des mesures de sécurité en place
- Développer des stratégies de mitigation des risques
- Réaliser des audits de sécurité pour identifier les vulnérabilités
- Identifier les anomalies dans les résultats des tests

Transition numérique

Communication, Création, Innovation, Nouvelles technologies

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

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Coopération, Organisation et Développement de ses compétences

- Actualiser régulièrement ses connaissances

Management, Social, Soins

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

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Normes et procédés

- **Analyse de risques en sécurité informatique**
- Cryptographie appliquée
- Détection des intrusions réseau
- Normes de sécurité
- Protection des données personnelles

Transition numérique

Transition numérique

Transition numérique

Transition numérique

Techniques professionnelles

- Gestion des accès sécurisés
- Techniques de reporting efficace

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