https://latribunelibre.com/emploi/expert-cybersecurite-iam-f-h

Expert Cybersécurité IAM F/H

Organisme employeur
DEXTON CONSULTING

Type de poste
Temps plein

Secteur
CONSEIL POUR LES AFFAIRES ET AUTRES CONSEILS DE GESTION

Lieu du poste
France

Date de publication
28 août 2024 à 21:01

Valide jusqu'au
27.09.2024

Description

L'ingénieur expert en cybersécurité est chargé de protéger les systèmes, réseaux et données de l'entreprise contre les cybermenaces.

Missions :

Analyse des Risques :

Évaluer les vulnérabilités des systèmes et réseaux informatiques.

Effectuer des analyses de risques et proposer des mesures correctives.

Gestion des Identités et des Accès :

Mettre en place et maintenir les procédures de gestion des identités (IAM) et des accès (IAM).

Superviser les processus d'authentification, d'autorisation et de gestion des droits.

Surveillance et détection des menaces :

Mettre en place des systèmes de surveillance et de détection des intrusions.

Réagir aux incidents de sécurité et coordonner les actions correctives.

Mettre en place un reporting de suivi à construire en fonction des besoins qui seront identifiés

Sécurité des Réseaux :

Configurer et maintenir les équipements de sécurité réseau (pare-feu, VPN, IDS/IPS, etc.).

Assurer la sécurité des communications et des flux de données.

Piloter ou effectuer des audits opérationnels et des tests d'intrusion internes.

Contribuer au pilotage de la gestion des incidents et des crises de sécurité.

Définir et contrôler le niveau de durcissement des éléments techniques de protection.

Améliorer les mesures de sécurité pour la protection des données, applications et infrastructures.

Veille :

Une activité de veille importante doit permettre de maintenir le SI à un niveau de sécurité très élevé.

Participe à différents séminaires, état de l'art, WebEx pour maintenir une vigilance pro-active sur la sécurité

Objectifs et livrables

Analyse des Risques :

Évaluer les vulnérabilités des systèmes et réseaux informatiques.

Effectuer des analyses de risques et proposer des mesures correctives.

Gestion des identités et des accès :

Mettre en place et maintenir les procédures de gestion des identités (IAM) et des accès (IAM).

Superviser les processus d'authentification, d'autorisation et de gestion des droits.

Surveillance et détection des Menaces :

Mettre en place des systèmes de surveillance et de détection des intrusions.

Réagir aux incidents de sécurité et coordonner les actions correctives.

Mettre en place d'un reporting de suivi à construire en fonction des besoins qui seront identifiés

Sécurité des Réseaux :

Configurer et maintenir les équipements de sécurité réseau (pare-feu, VPN, IDS/IPS, etc.).

Assurer la sécurité des communications et des flux de données.

Piloter ou effectuer des audits opérationnels et des tests d'intrusion internes.

Contribuer au pilotage de la gestion des incidents et des crises de sécurité.

Définir et contrôler le niveau de durcissement des éléments techniques de protection.

Améliorer les mesures de sécurité pour la protection des données, applications et infrastructures.

Veille :

Une activité de veille importante doit permettre de maintenir le SI à un niveau de sécurité très élevé.

Participe à différents séminaires, état de l'art, WebEx pour maintenir une vigilance pro-active sur la sécurité

Qualifications

Expérience dans la dématérialisation serait appréciée

Avancé

Compétences en gestion des risques, en cybersécurité et en SMSI

Confirmé

Connaissances approfondies en protocoles réseau, systèmes d'exploitation et technologies de sécurité.

Confirmé

Connaissance des normes et standards de sécurité (ISO 2700X, PCI-DSS, etc.)

Confirmé

Connaissance des environnements cloud (IaaS, PaaS, SaaS, etc.)

Confirmé

Compétences en programmation (Python, PowerShell, etc.) et en scripting sont un plus

Avancé

Maîtrise des outils de sécurité (chiffrement, firewalling, IAM, SIEM, etc.)

Confirmé