https://latribunelibre.com/emploi/cybersecurite-conception-architecture-securite-f-h

Cybersécurité – Conception Architecture sécurité F/H

Organisme employeur
CORSAIR SYSTEM

Type de poste
Temps plein

Secteur
INGÉNIERIE, ÉTUDES TECHNIQUES

Lieu du poste
95127, CERGY, CERGY, France

Salaire de base
50000 € - **Salaire de base**
60000 €

Date de publication
2 octobre 2025 à 19:05

Valide jusqu'au
01.11.2025

Description

L'architecte SI se coordonne avec le responsable de la sécurité de l'unité commerciale pour :
 Analyser les exigences de sécurité de haut niveau et en déduire des exigences de sécurité détaillées pour les réseaux et les appliances de sécurité associées ; pour la prévention et la surveillance des menaces, pour la gestion et la surveillance des journaux ; pour la cryptographie, les certificats numériques et les infrastructures à clé publique (PKI), ainsi que les systèmes d'exploitation (Linux, Windows), les appliances et le renforcement des logiciels ; respectant les normes de l'industrie.
 Contribuer à l'appel d'offres
, y compris les estimations de coûts Proposer des contrôles de sécurité basés sur l'évaluation des technologies de sécurité ; Participer / Soutenir l'équipe projet dans la conception détaillée de la solution.
 Revoir l'architecture/les plateformes ; identifier les menaces/faiblesses possibles Préparer/compléter la documentation de sécurité pendant les phases de conception/développement/intégration/tests ; établir des directives/procédures de sécurité pour les systèmes opérationnels
 Mettre en œuvre ou gérer la mise en œuvre de solutions de sécurité ; la création, la transmission et la maintenance de clés et de certificats numériques ; Remplir la documentation
 Vérifier la solution de sécurité par le biais de tests de sécurité fonctionnels, gérer les tests dynamiques, l'analyse de code statique, les analyses de vulnérabilité et les tests d'intrusion ; analyser et valider les rapports d'essais ; détaillant les actions pour les autres membres de l'équipe.
 Maintenir la sécurité en surveillant et en assurant la conformité aux normes, politiques et procédures ; la réalisation d'analyses d'intervention en cas d'incident ; l'élaboration et la mise en œuvre de programmes de formation.
 Mettre à niveau les systèmes de sécurité en surveillant l'environnement ; l'identification des lacunes ; Évaluation et mise en œuvre des améliorations Préparer des rapports de sécurité du système en collectant, analysant et résumant les données et les tendances

Qualifications

 Fournir des conseils techniques et un soutien aux clients, partenaires et sous-traitants et aux membres
de l'équipe moins expérimentés Profil
 Baccalauréat en informatique ou dans une discipline pertinente. (Master de préférence)
 Min 5 ans d'expérience professionnelle dans au moins 2 des domaines suivants : Sécurité système (clé), Sécurité réseau (clé), Sécurité des données (clé), Section des applications, Section cloud
 Une expérience de travail sur des systèmes hautement sécurisés serait un atout
o Autonome, avec de bonnes compétences en communication pour interfacer et établir des relations (avec les clients, les partenaires et les équipes internes)

o Capacité à personnifier notre activité
de sécuritéo Habitué à travailler dans des équipes internationales (anglais courant, compétences interculturelles)
o Connaissance du cycle de vie du développement de projets / produits pour comprendre les contraintes de la solution déployée et des équipes
o Capacité à s'adapter rapidement aux exigences
du projet Compétences
techniques Expertise technique pratique en renforcement des systèmes d'exploitation, AD/LDAP, pare-feu, IDS/IPS, AV, IAM, PAM et SIEM de préférence. MDM (SOTI, ManageEngine) et SOAR exp
appréciés Sécurité des logiciels et des applications (SDLC, OWASP, tendances en matière de sécurité, normes, meilleures pratiques, concepts et solutions) ; Analyse de code statique et dynamique, gestion des vulnérabilités.
 Expérience de l'analyse des risques sur les petits systèmes (ISO27005, EBIOS)
 Production des systèmes de sécurité de l'information et des menaces associées (développement sécurisé, architecture, anonymisation, authentification, signatures, traces, réseau, environnement de
production, etc.).
 Sec Testing (une expérience en évaluation de vulnérabilité et en pentesting sera avantageuse).
 Formation
Sec connaissance/expérience des normes de sécurité appréciée :ISO/IEC 27001, ITIL, PCI DSS
 [Préféré] Un certificat sec professionnel internationalement reconnu, tel que CISSP, CREST, CEH, CISM. Preuve requise