https://latribunelibre.com/emploi/ingenieur-cybersecurite-produits-f-h-2

Ingénieur Cybersécurité Produits F/H

Organisme employeur
XPERTZON

Type de poste
Temps plein

Secteur
ACTIVITÉS DES AGENCES DE PLACEMENT DE MAIN-D'OEUVRE

Lieu du poste
78646, VERSAILLES, VERSAILLES, France

Salaire de base
65000 € - **Salaire de base**
80000 €

Date de publication
12 janvier 2026 à 12:03

Valide jusqu'au
11.02.2026

Description

SOCIÉTÉ :

Notre client est une entreprise industrielle française à taille humaine, reconnue pour son expertise technologique et la fiabilité de ses solutions. Elle conçoit et développe des produits à haute valeur ajoutée, destinés à des environnements sensibles et critiques, en France et à l'international.

Dans un contexte de renforcement de son offre systèmes et d'exigences accrues en matière de cybersécurité et de conformité réglementaire, l'entreprise souhaite intégrer un référent cybersécurité produits senior.

OBJECTIF DU RECRUTEMENT :

L'Ingénieur **Cybersécurité Produits** senior est le référent sécurité des produits tout au long de leur cycle de vie. Il/elle intervient en amont des développements, sécurise les architectures, accompagne les équipes techniques et contribue activement aux démarches de certification.

Ce poste s'inscrit dans une logique produit, industrielle et long terme, et s'adresse à un profil expérimenté, capable d'apporter vision, méthode et structuration.

ORGANISATION :

L'Ingénieur Cybersécurité Produits travaille en étroite collaboration avec :

- les équipes systèmes et développement,
- la Direction Qualité,
- les interlocuteurs externes (organismes de certification, partenaires).

ACTIVITÉS PRINCIPALES :

Sécurité produits & analyses techniques

- Réaliser les analyses de risques (STRIDE, LINDDUN, etc.).
- Conduire des revues de code (C, JavaScript / TypeScript).
- Réaliser ou piloter des tests de sécurité (Linux embarqué, conteneurs).
- Mettre en œuvre et automatiser les tests SCA / SAST / DAST dans les chaînes CI/CD.

Secure-by-design & architectures

- Intégrer la sécurité dès les phases de spécification et de conception.
- Proposer des architectures durcies (hardening kernel, SELinux, AppArmor, seccomp).
- Accompagner les équipes de développement sur les bonnes pratiques de sécurité (OWASP, DevSecOps).

Certifications & conformité

- Contribuer aux démarches de certification et d'agrément (IEC 62443-4-1/4-2, CSPN, Common Criteria, FIPS, NIS2).
- Préparer les dossiers techniques à destination des organismes certificateurs (ex. ANSSI, BSI).
- Mettre en place et suivre les processus de gestion des vulnérabilités (ISO 30111, CVE / CVSS).

Veille, gouvernance et transmission

- Assurer une veille active sur les menaces et vulnérabilités (CERT-FR, CVE, MITRE ATT&CK).
- Participer à l'acculturation cybersécurité des équipes internes.
- Rédiger des guidelines et référentiels internes.

Qualifications

Compétences techniques

- Expérience confirmée en cybersécurité produits industriels ou embarqués.
- Solide maîtrise de Linux embarqué (kernel, boot sécurisé, TPM).
- Connaissance des environnements conteneurisés (Docker / OCI), images minimales, scans de vulnérabilités.
- Notions ou pratique du reverse engineering et de l'analyse firmware (ex. Ghidra, Binwalk).
- Cryptographie appliquée (TLS 1.3, PKI, HSM, secure element).
- Maîtrise des normes et référentiels : IEC 62443, ISO 27001/27034, OWASP ASVS, NIST 8259A.
- Connaissance des enjeux réglementaires et clients (dont NIS2).
- Une ou plusieurs certifications (CEH, OSCP, CISSP ou équivalent) constituent un plus.
- Connaissance CI/CD (GitLab, GitHub Actions) avec intégration SCA / SAST / DAST ; Kubernetes/Edge apprécié.

Compétences comportementales

- Capacité à travailler en environnement transverse et à coopérer avec des profils métiers diversifiés.
- Rigueur, méthode, sens de la structuration et de la confidentialité.
- Aisance relationnelle, sens du dialogue, capacité à convaincre et à embarquer les équipes.
- Capacité à transmettre, former et formaliser (rédaction de rapports et dossiers techniques).

Langues

- Français courant.
- Anglais professionnel (écrit et oral).

Formation et expérience

- Diplôme d'ingénieur ou équivalent (Bac +5).
- Expérience significative confirmée en **sécurité produit, systèmes embarqués** ou environnements critiques.
- Une expérience dans des secteurs sensibles (industrie, défense, sécurité, énergie, télécoms) est appréciée.