Description de poste

Ingénieur(e) cybersécurité — Sécurité applicative (F/H)

Sofrecom, filiale du groupe Orange, a développé depuis plus de 45 ans un savoir-faire unique dans les métiers de l'opérateur, qui en fait aujourd'hui l'un des leaders mondiaux du conseil et de l'ingénierie. Ces dernières années, plus de 200 acteurs majeurs, dans plus de 100 pays, ont confié à Sofrecom la conduite de leurs projets stratégiques et opérationnels : transformation et optimisation, modernisation technologique, innovation et développement. Son accès privilégié aux expertises et à l'innovation du Groupe Orange permet à Sofrecom de proposer à ses clients des solutions d'avant-garde qui ont fait leurs preuves.

Sofrecom est une entreprise internationale riche de sa diversité, avec plus de 1500 consultants et experts répartis dans 11 implantations à travers le monde et issus de plus de 30 nationalités. Sofrecom est avant tout un réseau d'hommes et de femmes, un puissant réseau de savoir-faire et d'expertises qui relie ses clients, les experts Orange, ses partenaires industriels et locaux.

Lancée en novembre 2011, Sofrecom Tunisie compte aujourd'hui plus de 700 ingénieurs et étend la présence de Sofrecom sur la zone Afrique du Nord et Moyen-Orient afin de répondre à une demande croissante de solutions dédiées et compétitives. Centre de développement et d'expertise pour les plates-formes de services et du système d'information, Sofrecom Tunisie s'inscrit en complémentarité des domaines d'activité des autres implantations de Sofrecom dans la région et permettra aux clients du groupe Sofrecom de bénéficier des synergies entre nos filiales.

Sofrecom, the Know-How Network.

Missions

Au sein du pôle Sécurité, l'ingénieur(e) cybersécurité spécialisé(e) en sécurité applicative contribue à la protection des applications tout au long de leur cycle de vie, de la conception au déploiement et à la maintenance.

Il ou elle accompagne les équipes de développement et les métiers dans l'intégration des exigences de sécurité, identifie les vulnérabilités applicatives et conseille sur les mesures de correction adaptées.

Activités principales

1. Intégration de la sécurité dans le cycle de développement

- Accompagner les équipes projet et développement dans l'application des principes de sécurité dès la conception (Security by Design).
- Contribuer à la définition des exigences de sécurité et à leur intégration dans les spécifications, l'architecture et les critères de validation.
- Participer aux revues d'architecture et aux analyses de risques applicatifs.
- Contribuer à l'intégration des contrôles de sécurité dans les pipelines CI/CD et les démarches DevSecOps.

2. Évaluation et tests de sécurité

- Réaliser ou coordonner des évaluations de sécurité applicative, notamment des analyses de code et des tests de sécurité.
- Exploiter les résultats des outils SAST, DAST, SCA et des tests manuels afin d'identifier et de qualifier les vulnérabilités.
- Analyser les risques associés aux défauts détectés en tenant compte de leur exploitabilité, de leur exposition et du contexte métier.
- Accompagner les équipes dans la priorisation et la correction des vulnérabilités.
- Vérifier la mise en œuvre des corrections et contribuer au suivi des plans de remédiation.
- Documenter les constats, les risques et les recommandations dans des rapports compréhensibles par les équipes techniques et les responsables concernés.

3. Expertise et accompagnement technique

- Participer à l'analyse de vulnérabilités applicatives, notamment celles décrites dans les référentiels OWASP.
- Accompagner le traitement des incidents de sécurité liés aux applications, en coordination avec les équipes concernées.

4. Pilotage et amélioration continue

- Suivre les vulnérabilités applicatives, les plans de correction et les indicateurs associés.
- Participer à la définition et à l'amélioration des processus de sécurité applicative et DevSecOps.
- Assurer une veille sur les vulnérabilités, les menaces, les outils et les pratiques de développement sécurisé.
- Sensibiliser et former les équipes de développement aux risques applicatifs et aux méthodes de prévention.
- Contribuer aux audits, aux revues de sécurité et aux démarches de conformité applicables.

Profil et compétences requises

Formation et expérience

- Formation d'ingénieur en cybersécurité, informatique, développement logiciel ou systèmes d'information, ou expérience équivalente.
- Expérience entre deux et 4 ans en sécurité applicative, développement sécurisé, tests de sécurité ou accompagnement d'équipes de développement.

Compétences Techniques :

- Bonne compréhension du cycle de développement logiciel et des architectures applicatives.
- Connaissance des vulnérabilités web et des recommandations OWASP, notamment OWASP Top 10 et OWASP ASVS.
- Compréhension des mécanismes d'authentification, d'autorisation, de gestion des sessions et de protection des données.
- Connaissance des protocoles et technologies web, notamment HTTP/HTTPS, REST et API.
- Pratique ou connaissance des outils d'analyse SAST, DAST et SCA ; la familiarité avec des solutions telles que Checkmarx, Fortify, SonarQube, Burp Suite, OWASP ZAP, Snyk ou des outils équivalents est appréciée.
- Notions de sécurité des composants tiers, des dépendances logicielles et de la gestion des secrets.
- Connaissance des environnements cloud et des pratiques DevSecOps.
- Capacité à analyser les résultats de tests et à proposer des mesures de correction concrètes.
- La connaissance d'un ou plusieurs langages de programmation et de scripting constitue un atout.

Compétences complémentaires appréciées :

- Expérience des pipelines CI/CD et des outils d'automatisation.
- Connaissance des référentiels et normes de sécurité applicative, tels que ISO 27001, NIST ou les recommandations OWASP.
- Certifications en cybersécurité applicative, développement sécurisé ou tests de sécurité appréciées.

Aptitudes relationnelles et comportementales :

- Rigueur, curiosité et sens de l'analyse.
- Capacité à expliquer les risques et les mesures de sécurité de manière claire et pragmatique.
- Aptitude à collaborer avec des équipes de développement, d'architecture, d'exploitation et des interlocuteurs métiers.
- Sens de la pédagogie et capacité à accompagner les équipes dans la mise en œuvre des recommandations.
- Esprit de synthèse, autonomie et sens du service.

Langues

La maîtrise du français et de l'anglais, à l'écrit comme à l'oral, est nécessaire dans l'environnement international de Sofrecom.