Description de poste

Ingénieur Cybersécurité — VOC et gestion des vulnérabilités (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 cybersécurité définit spécialisé en gestion des vulnérabilité, déploie et améliore les mesures de durcissement des systèmes d'information. Il ou elle supporte nos clients pour la détection, l'analyse, la priorisation et le traitement des vulnérabilités, et mène des activités de threat hunting afin de rechercher de manière proactive des comportements suspects ou des signes d'activité malveillante.

Activités principales

1. Hardening et sécurisation des systèmes

- Définir et maintenir les standards de durcissement des systèmes d'exploitation, serveurs, postes de travail, équipements réseau, environnements cloud et solutions de sécurité.
- Établir des configurations de référence conformes aux bonnes pratiques et référentiels applicables, notamment CIS Benchmarks, ANSSI et exigences internes.
- Évaluer les écarts entre les configurations en place et les configurations attendues.
- Accompagner les équipes techniques dans la mise en œuvre des recommandations de durcissement.
- Vérifier l'efficacité des mesures déployées et contribuer à leur automatisation lorsque cela est pertinent.
- Documenter les procédures, dérogations et plans de remédiation.

2. Gestion des vulnérabilités

- Organiser les campagnes de détection sur les environnements concernés à l'aide d'outils de scan et de contrôles complémentaires.
- Qualifier les résultats et distinguer les vulnérabilités avérées des faux positifs.
- Évaluer les risques selon la criticité technique, l'exposition, l'exploitabilité et l'importance des actifs concernés.
- Prioriser les corrections et proposer des délais de traitement adaptés au niveau de risque.

3. Threat hunting et analyse de sécurité

- Formuler des hypothèses de chasse à partir des alertes, du contexte de l'organisation, des renseignements sur les menaces et des comportements observés.
- Assurer une veille sur les nouvelles menaces de cyber sécurité au travers de Plateforme de renseignement sur les menaces.

- Collaborer avec les équipes SOC, IT, réseau et systèmes pour approfondir les investigations et contribuer au traitement des découvertes.
- Documenter les hypothèses, démarches, constats et recommandations.
- Contribuer à l'amélioration des règles de détection, des tableaux de bord et des procédures à partir des résultats des chasses.

Profil et compétences requises

Formation et expérience

- Formation ingénieur en cybersécurité, informatique, systèmes et réseaux, ou expérience équivalente.
- Expérience entre 2 et 4 ans en sécurité des infrastructures, gestion des vulnérabilités, durcissement des systèmes ou opérations de sécurité.

Compétences Techniques :

- Bonne connaissance des environnements Windows et Linux, des infrastructures réseau et des environnements virtualisés.
- Maîtrise des principes de hardening et des référentiels de configuration sécurisée.
- Expérience des outils de gestion des vulnérabilités et de conformité, par exemple Tenable, Qualys, Rapid7 ou solutions équivalentes.
- Compréhension des CVE, CVSS, des publications CERT-FR et des bases de connaissances des éditeurs.
- Connaissance des outils SIEM et EDR/XDR, ainsi que des pratiques d'analyse de journaux et de corrélation d'événements.
- Capacité à interpréter des rapports de scan, des alertes et des données de sécurité, puis à formuler des recommandations concrètes.
- Connaissance des environnements cloud, de la gestion des correctifs et des processus de changement.
- Connaissance des tactiques et techniques d'attaque et des méthodes d'investigation en threat hunting.

Compétences complémentaires appréciées :

- Sécurité des réseaux : IDS/IPS, protection contre les attaques DDoS, NAC, proxy, pare-feu et concentrateurs VPN (IPsec, SSL).
- Protocoles et infrastructures d'authentification : Active Directory, LDAP, RADIUS, PKI et accès distants (Citrix, DirectAccess, VPN).
- Certifications en cybersécurité, notamment OSCP ou CEH.

Aptitudes relationnelles et comportementales :

- Rigueur, curiosité et sens de l'analyse.
- Capacité à formuler et vérifier des hypothèses, à interpréter les résultats et à prioriser les risques.
- Prise en compte des contraintes opérationnelles et recherche de solutions pragmatiques.
- Communication et pédagogie auprès d'interlocuteurs techniques et non techniques.
- Aptitude à coordonner des actions impliquant plusieurs équipes.
- Esprit de synthèse et capacité à produire une documentation claire.
- 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.