Description de poste

Spécialiste Risque Cyber, BCCM & Résilience Opérationnelle — 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 1000 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 d'une équipe dédiée aux risques cyber, à la continuité d'activité, à la gestion de crise et à la résilience opérationnelle, le Spécialiste risque cyber contribue au pilotage opérationnel de projets transverses liés aux dispositifs BCCM, gestion de crise cyber et résilience.

Il intervient sous la supervision d'un chef de projet senior ou d'un manager, avec pour rôle de structurer, coordonner, suivre et sécuriser l'avancement des chantiers confiés : campagnes d'évaluation, plans de remédiation, exercices de crise, plans de continuité, plans de reprise et actions d'amélioration de la maturité cyber/résilience.

Activités principales

- Participer au cadrage des projets BCCM, risque cyber et résilience opérationnelle : objectifs, périmètre, parties prenantes, planning, livrables et jalons.
- Contribuer au pilotage opérationnel des chantiers liés à la continuité d'activité, à la gestion de crise cyber, à la reprise après incident et à la résilience opérationnelle.
- Construire et suivre les plannings projet, les plans d'action, les échéances, les dépendances et les points de blocage.
- Coordonner les échanges avec les parties prenantes internes et externes : équipes sécurité, IT, réseau, métiers, conformité, risques, filiales ou clients.
- Organiser et préparer les réunions projet : ordre du jour, supports, comptes rendus, décisions, actions à suivre et relances.
- Assurer le suivi de l'avancement des plans de remédiation issus des évaluations de maturité, audits, exercices de crise ou analyses d'écarts.
- Contribuer à la préparation et à l'organisation des exercices de crise cyber ou de continuité : chronogramme, participants, supports, scénarios, injects, suivi post-exercice.

- Participer à la formalisation des livrables projet : roadmap, tableaux de bord, supports de comité, synthèses d'avancement, reporting risques/actions/décisions.
- Identifier les retards, risques projet, dépendances critiques et points nécessitant arbitrage.
- Contribuer à l'amélioration continue des méthodes, modèles de suivi, supports de pilotage et rituels projet.
- Assurer une communication claire et régulière auprès du chef de projet senior, du management et des parties prenantes concernées.

Compétences requises

De formation Bac+5 en cybersécurité, informatique, télécoms, gestion de projet, gouvernance SI, management des risques, continuité d'activité, résilience opérationnelle ou équivalent.

Expérience souhaitée : 2 à 3 ans dans la gestion de projet, la cybersécurité, le conseil, le GRC, le BCCM, la continuité d'activité, la gestion des risques ou la coordination de projets IT/cyber.

Une expérience en cabinet de conseil, environnement international, programme cyber ou projet transverse serait appréciée.

Compétences Techniques exigées :

- Bonne compréhension des fondamentaux de la gestion de projet : planning, jalons, risques, actions, dépendances, reporting et gouvernance projet.
- Connaissance générale des sujets risque cyber, BCCM, continuité d'activité, gestion de crise, PRA/PCA et résilience opérationnelle.
- Capacité à piloter plusieurs actions en parallèle avec rigueur et méthode.
- Capacité à suivre un plan de remédiation et à challenger l'avancement réel des actions.
- Bonne maîtrise d'Excel, PowerPoint et des outils collaboratifs.
- Capacité à produire des supports de pilotage clairs, synthétiques et orientés décision.
- Bonne qualité rédactionnelle pour comptes rendus, synthèses projet et supports de comité.
- Connaissance de base des référentiels ISO 27001, ISO 22301, ISO 27005, NIST ou équivalents.
- Une première exposition à un outil GRC, outil de gestion projet, outil de ticketing ou outil de reporting serait un plus.

Compétences souhaitées

- Certification ou formation en gestion de projet : PMP, Prince2, Agile/Scrum, CAPM ou équivalent est un plus.
- Certification ou sensibilisation ISO 27001, ISO 22301, ITIL ou équivalent.
- Première expérience dans les campagnes de maturité cyber, audits, plans de remédiation ou projets de résilience.

- Connaissance des environnements IT, réseau, infrastructure, cloud, sauvegarde, IAM ou sécurité opérationnelle.

Aptitudes relationnelles et comportementales :

- Leadership junior : capacité à faire avancer les sujets sans autorité hiérarchique directe.
- Rigueur, organisation et sens des priorités.
- Capacité à relancer avec tact, clarté et fermeté.
- Esprit de synthèse et orientation résultat.
- Bonne communication avec des interlocuteurs techniques, fonctionnels et management.
- Capacité à travailler dans un contexte international et multiculturel.
- Réactivité, autonomie progressive et fiabilité.
- Bon niveau en français et en anglais, à l'écrit comme à l'oral.

L'environnent international dans lequel évolue Sofrecom, implique la parfaite maitrise du français et de l'anglais tant à l'écrit qu'à l'oral.