Fiche de Mission – Alternant-e en Sécurité des Systèmes d'Information (SSI) et PCA/PRA Cyber

Intitulé du poste : Alternant·e en Sécurité des Systèmes d'Information (SSI) et PCA/PRA Cyber (H/F)

Durée : 2 ans (M1 + M2) – Contrat d'apprentissage ou de professionnalisation

Employeur : Direction Interdépartementale des Routes du Sud-Ouest (DIRSO)

Localisation : 155 avenue des Arènes Romaines - 31300 TOULOUSE (siège de la DIRSO)

Contexte

La Direction Interdépartementale des Routes Sud-Ouest (DIRSO) a récemment finalisé un audit sécurité de son Système d'Information (SI), identifiant 320 recommandations à traiter pour renforcer sa posture cybersécurité. Parallèlement, elle a aussi engagé la mise en place d'un Plan de Continuité d'Activité (PCA) et de Reprise d'Activité (PRA) Cyber, essentiel pour garantir la résilience face aux cybermenaces.

Dans ce cadre, elle recrute un alternant(e) qui sera positionné(e) au sein de la Division Appui au Management (DAM) comme acteur·rice clé de la remédiation des vulnérabilités relevées dans l'audit SSI et de l'accompagnement à l'élaboration du PCA/PRA Cyber, en collaboration avec les équipes techniques locales et nationales ainsi que les métiers impactés.

Composée de 8 agents dont un chargé de mission « système d'information » qui assure le pilotage des systèmes d'information et leur sécurité, la DAM a pour mission principale de faciliter l'amélioration de la performance des activités des services de la DIRSO.

Elle est rattachée au secrétariat général (SG) de la DIRSO chargé d'assurer la gestion des ressources humaines, la formation professionnelle, la sécurité et la prévention des risques professionnels, la gestion des moyens généraux, de l'immobilier et de l'informatique, la communication, l'animation du système de maîtrise de la qualité, le contrôle de gestion, la gestion des archives et le pilotage du système d'information et leur sécurité.

Missions Principales

1. Remédiation de l'audit SSI - Élaboration et suivi du plan d'action (70% du temps)

- **Hiérarchisation et priorisation** des 320 recommandations relevées dans l'audit SSI :
  - Analyse des risques (criticité, impact, faisabilité)
  - Construction d'un plan d'actions avec échéancier et responsables désignés.
  - Suivi des avancées via des tableaux de bord et des outils spécifiques à déterminer.
- **Accompagnement technique** :
  - Participation à la correction des vulnérabilités (ex : durcissement des configurations, partitionnement des réseaux, sensibilisation des utilisateurs, ...)
  - Rédaction de procédures et de documentations techniques.
- **Veille cybersécurité** :
  - Surveillance des alertes (ANSSI, CERT-FR) et adaptation des mesures.

2. Aide à l'élaboration du PCA/PRA Cyber (30% du temps)

- **Cartographie des processus critiques** :
  - Identification des services prioritaires et des dépendances (ex : hébergement, réseaux, données sensibles)
- **Rédaction des plans** :
  - Scénarios de crise (ex : ransomware, DDoS), procédures de reprise, et tests de simulation
  - Collaboration avec les métiers pour valider les RTO/RPO (objectifs de reprise)
- **Sensibilisation et formation** :
  - Organisation d'ateliers pour les équipes sur les bonnes pratiques PCA/PRA.

3. Transverses

- Participation aux réunions de suivi avec la direction et les prestataires.
- Rédaction de notes de synthèse et présentations pour la gouvernance.

Livrables Attendus

- **Année 1 (M1)** :
    - Plan d'actions remédiation audit (version initial + mises à jour trimestrielles)
    - Premier jet du PCA/PRA (cartographie des processus critiques)
- **Année 2 (M2)** :
    - Rapport final de remédiation (taux de couverture des recommandations)
    - PCA/PRA validé et testé (simulation de crise)
    - Mémoire de fin d'études sur un sujet lié (ex : "Méthodologie de priorisation des risques SSI dans un contexte public")

Compétences et Qualités Recherchées

Profil recherché :

- Master en Cybersécurité, Systèmes d'Information, ou équivalent
- Connaissances en normes ISO 27001, NIS 2, RGPD.

Compétences techniques :

- Bases en administration système/réseau (Windows/Linux, firewalls, Active Directory)
- Notions de gestion des risques
- Connaissance ou maîtrise des outils liés à la sécurité informatique comme Nessus, OpenVAS, ou Splunk ou d'outils pouvant faciliter la remédiation comme DefectDojo, Eramba ou OpenGRC (un plus)

Savoir-être :

- Rigueur et capacité à prioriser dans un environnement complexe
- Aisance relationnelle pour travailler avec des profils techniques et métiers variés
- Esprit d'analyse et rédaction claire (documents techniques et synthèses)

Eléments de candidature

Personne à contacter :

Alexandre DUMONT, Chargé de Mission Systèmes d'Information - 07 63 90 91 97 ou par email : Alexandre.Dumont@developpement-durable.gouv.fr

Environnement de Travail

- **Équipe** : Positionnement au sein de la DAM avec rattachement auprès du chargé de mission systèmes d'information qui assure le pilotage des systèmes d'information et leur sécurité (tuteur) et interactions régulières avec le RSSI et les services centraux de la Dnum
- **Outils** : suite bureautique LibreOffice, solutions de supervision LibreNMS, Bastion, serveurs de virtualisation, ….
- **Ce que l'on vous propose :** un tuteur expérimenté et une expérience dans la fonction publique de l'État

Qui sommes nous ?

La DIR-SO, certifiée ISO 9001 et 45001, gère, exploite et entretient environ 555 kilomètres de réseau routier national non concédé incluant 2 tunnels routiers, les voies structurantes de l'agglomération de Toulouse, des sections des autoroutes A64 et A68, et un secteur de haute montagne frontalier de l'Espagne et de l'Andorre. Elle conduit aussi des opérations d'ingénierie de modernisation, de sécurisation et de réparation du réseau, et de gestion du trafic. Ce service compte un peu moins de 400 agents répartis sur une vingtaine de sites sur 8 départements.