

Centre de ressources et de compétences régional, le GIP RECIA est un acteur public majeur de la communauté régionale numérique et un support d'expérimentations, de mutualisation et de prestation de services bénéficiant aujourd'hui à 1000 structures publiques de la région Centre-Val de Loire.

Dans le cadre de ses activités, le GIP RECIA recherche :

Analyse CSIRT

>>> PRÉSENTATION DU POSTE

- **Ingénieur ou niveau équivalent BAC+4/5 en Informatique / Ecole d'Ingénieur**
- **Poste ouvert aux contractuels et fonctionnaires de catégories A**
- **Date limite de candidature : 10 octobre 2024**

L'Etat, la Région Centre-Val de Loire, DEV'UP Centre-Val de Loire et le GIP RECIA se mobilisent pour lutter contre les cyberattaques afin de mieux protéger les entreprises et les collectivités de la région contre la menace cyber en forte croissance. Dans ce cadre, un centre régional de réponse à incident cyber dénommé CybeRéponse a été créé en 2023.

L'analyste CSIRT répond aux bénéficiaires, analyse les incidents de sécurité et apporte une réponse de premier niveau notamment, à l'aide de fiches reflexes. Il qualifie efficacement les incidents et est capable de réaliser le triage et de prioriser. Il escalade dans le respect de l'organigramme de réponse à incident, et relaie vers les prestataires référencés ou autres prestataires nationaux. Le traitement des incidents est soumis à des indicateurs de performance opérationnels. Dans le cadre de la mutualisation d'activités, l'analyste peut être amené à faire bénéficier les autres périmètres du centre de service de son expertise.

Dans ce cadre, voici la mission principale du chargé de mission :

L'ingénieur en cybersécurité sera chargé de suivre les incidents de sécurité et jouera un rôle de tiers de confiance technique. Il sera responsable de la gestion des crises cyber et de la communication avec les prestataires de remédiation, tout en garantissant des débats contradictoires sur les solutions proposées. En parallèle, il contribuera à la mise en place et à l'exploitation des outils techniques nécessaires au CSIRT pour la détection des signaux faibles et la supervision du périmètre de sécurité. Ce profil technique jouera également un rôle clé en tant que relais niveau III dans la réponse à incident, en apportant son expertise technique aux équipes du CSIRT ainsi qu'auprès des bénéficiaires du CSIRT.

>>> MISSIONS



Suivi des incidents de sécurité :

- Assurer le suivi continu des incidents de sécurité, en collaboration avec les différentes parties prenantes internes et externes

Tiers de confiance technique :

40%

- Agir en tant que médiateur technique entre les prestataires de remédiation et l'organisation, en menant des débats contradictoires sur les approches de résolution proposées

Mise en place d'outils techniques :

- Contribuer à la sélection, la mise en place et l'exploitation des outils de sécurité sous la supervision du responsable technique, y compris les sondes et autres dispositifs permettant de détecter les signaux faibles.

40%

Détection proactive :

- Participer à la surveillance proactive du réseau en détectant les tendances émergentes grâce à la mise en place outils et en identifiant les menaces potentielles dans le périmètre

Support niveau III :

- Intervenir en tant que relais technique de niveau III pour apporter son expertise lors de la réponse à incident et supporter les équipes techniques du CSIRT dans les cas complexes

20%

Management : Oui Non

Lieu d'exercice : Poste implanté au siège du GIP Recia à Orléans sud, sur le site du BRGM (Loiret), ou dans l'une de ses antennes à Ballan-Miré (Indre-et-Loire) ou à Bourges (Cher). Secteur d'activité sur l'ensemble de la région Centre-Val de Loire

Spécificités du poste : Permis B obligatoire / Déplacements sur tout le territoire régional / Assurer une permanence de service avec l'ensemble de l'équipe

Avantages : Télétravail possible avec équipement informatique personnel à disposition / véhicules de service / prestations sociales (association des personnels) / tickets restaurant / CESU / prise en charge partielle des trajets domicile-travail / forfait mutuelle / indemnité télétravail / cadre de travail agréable / accès aux infrastructures BRGM (restaurant d'entreprise, équipements sportifs...) / organisation de sorties à destination des personnels

>>> LES EXIGENCES DU POSTE

SAVOIRS	SAVOIRS-FAIRE
<ul style="list-style-type: none">• Expertise reconnue dans la gestion des incidents et la mise en place d'outils de sécurité.• Connaissance approfondie des processus et des technologies de détection d'intrusions, de surveillance réseau, et de gestion des incidents.• Connaissances solides des outils de détection d'intrusion (sondes, SIEM) et des technologies associées.• Bonnes pratiques et normes en matière de cybersécurité (ISO 27001, NIST, etc.).• Familiarisé avec les techniques de gestion de crise et la coordination avec des prestataires externes.	<ul style="list-style-type: none">• Expertise en gestion de crise et en réponse à incident dans le cadre de la cybersécurité.• Capacité à évaluer et implémenter des outils techniques de détection, sondes, et systèmes de surveillance.• Maîtrise des protocoles et des procédures de détection des signaux faibles dans les environnements de sécurité.• Compétences en gestion de projets techniques complexes, notamment dans la mise en œuvre de solutions de cybersécurité.• Aisance dans la communication avec des prestataires de remédiation pour mener des débats techniques contradictoires.• Connaissances approfondies des frameworks de cybersécurité et des outils spécialisés (SIEM, EDR, IDS, etc.).

Le champ des relations du poste :

- **Internes** : Directeur du GIP RECIA, Secrétaire Générale, Responsable CSIRT, Services numériques aux collectivités, Innovation.
- **Externes** : Conseil régional du Centre-Val de Loire, Agence DEVUP, Partenaires et entreprises spécialisés dans la cybersécurité, bénéficiaires du CSIRT, partenaires et prestataires des solutions déployées pour les bénéficiaires, Mouvement associatif.

Le champ d'autonomie, de responsabilité et de technicité du poste : Être autonome dans le cadre des responsabilités confiées.

Les difficultés, spécificités et les contraintes du poste : Déplacements chez les bénéficiaires du CSIRT, participation à des événements pouvant se tenir le week-end, représentation dans les instances locales. Continuité et stabilité des services mis en production.

>>> POSITIONNEMENT DANS L'ORGANIGRAMME



>>> MODALITES DE CANDIDATURE ET CONTACTS

Les candidats devront envoyer une lettre de motivation et un curriculum vitae à l'adresse mail : recrutement@recia.fr

Questions sur les missions du poste à pourvoir : M. Victor-Emmanuel de Sa, 06 64 16 36 49

Questions administratives ou sur les missions du poste à pourvoir : Mme Karen DESCHAMPS, 06 07 66 11 58