Concepteur Détection CyberSécurité F/H f/h

Pays de la Loire •Référence 2025-203426

2025-203426

Date de modification

10/22/2025

Contrat

CDI

Niveau d’études

Bac+5

Département

Loire-Atlantique - 44

Ville

Nantes

Entité

La Poste Groupe change, nos métiers évoluent. Etre toujours au plus près des Français, développer la confiance dans le numérique et être acteur de la transformation écologique, c'est aussi le sens de notre métier. Rejoindre La Poste Groupe, c'est rejoindre une entreprise responsable, riche de ses 232 000 collaborateurs ! Pour l'égalité des chances, La Poste fait vivre la diversité. Nos postes sont ouverts à toutes et à tous. Vous aussi, engagez-vous à nos côtés pour donner du sens à votre métier.

Filière Métier

Numérique/IT/SI

Mission

En rejoignant i-TEAM en tant que Concepteur de détection sécurité vous intégrerez la direction des services IT du Groupe La Poste à Nantes (44). i-TEAM, c’est 1000 collaborateurs au service des systèmes d’information du Groupe et de ses filiales. Au sein du CERT La Poste, aussi appelé Le Service de Lutte Contre la Cybercriminalité (SLCC), vous rejoindrez le pôle Détection des Incidents de Sécurité (DIS). Sa mission principale est de répondre aux enjeux de protection du Groupe La Poste et de ses Filiales face aux menaces cyber.

Vos missions si vous les acceptez :

–

Dans le pôle DIS, vous rejoindrez la division « Conception de la Détection », dont le rôle est de concevoir et faire évoluer les règles de détection au sein du SIEM, dans un but d’amélioration du niveau de protection global du Groupe. Vous ferez donc partie de la Blue Team !

Dans le cadre des projets de mise en détection sécurité, vous aurez la responsabilité de :

· Comprendre l’écosystème cible et ses enjeux sécurité, sur la base des analyses de risques, afin de proposer des mesures de détection adaptées

· Proposer, concevoir, mettre en œuvre des évolutions dans les environnements surveillés et dans le dispositif de détection

· En lien avec le chef de projet, communiquer avec les équipes opérationnelles des partenaires

· Rédiger la documentation de détection (fiches scénario, référentiels...)

· Ponctuellement, apporter soutien et accompagnement aux équipes d’analystes en cas d'incident

, editeur_offres

Profil

Nous recherchons une personne curieuse, tenace, rigoureuse et intègre, détenant de bonnes connaissances réseaux (IP, routage, DNS), système (Linux, Windows), et maîtrisant au moins une solution de SIEM (Splunk, Qradar...). La connaissance d’un langage de scripting est un plus.

L'activité s'inscrit dans un travail d'équipe :le partage d'informations objectives, la remise en question constructive et la participation de chacun·e jouent un rôle majeur. L’aptitude à intégrer une équipe experte et à contribuer dans un bon esprit est essentielle.

Diplômé·e d’un bac +5, vous avez une expérience de 2 ans à minima sur des missions similaires.

Possibilité de participer à des cycles d’astreinte. Certaines exigences réglementaires nécessite une habilitation à accéder à des informations couvertes par le secret défense.

Vous vous sentez à même de relever ce défi du Groupe La Poste, vous vous reconnaissez dans ces quelques lignes, alors n’hésitez plus et rejoignez-nous !

, editeur_offres

Formation et expérience

Votre environnement de travail : une équipe bienveillante qui saura vous chouchouter

· Possibilité de télétravailler jusqu’à 2 jours par semaine après la période d’essai

· 9 semaines de Congés et Repos

· Avantages sociaux : Famille, transport, vacances, logement

· Rémunération variable et intéressement

· Une entreprise à mission élue n°1 mondial de la RSE selon Moodie’s et labellisée Numérique Responsable

· Des locaux tout neufs au coeur de Nantes : La Maison de l'Innovation

, editeur_offres