Leader Technique Cybersécurité - Pôle Protection F/H f/h

Ile-de-France •Référence 2024-186205

2024-186205

Date de modification

06/07/2025

Contrat

CDI

Niveau d’études

Bac+5

Département

Val-de-Marne - 94

Ville

Ivry-sur-Seine

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. Filiale de La Poste Groupe, Docaposte compte 6 400 collaborateurs et 70 sites. Référent de la confiance numérique en France, Docaposte permet aux entreprises et institutions publiques d'accélérer leur transformation avec une des offres les plus larges du marché alliant numérique et physique. Docaposte se porte garant de la souveraineté des données clients hébergées dans ses propres infrastructures, avec un haut niveau de sécurité et de conformité. www.docaposte.com

Filière Métier

Numérique/IT/SI

Mission

Sous la responsabilité du Responsable du COSC, le Tech Lead Cyber est spécialisé dans l'Identification des Menaces.

Vous jouerez un rôle central dans la définition, la mise en œuvre et la supervision des initiatives visant à renforcer la posture de sécurité de Docaposte. Vous piloterez une équipe dynamique de professionnels de la cybersécurité et collaborerez étroitement avec d'autres départements pour identifier et anticiper les menaces potentielles.

Vos principales missions s'articulent sur :

•Leadership technique du pôle (pilotage des équipes du pôle protection et défense, expertise et accompagnement des équipes du pôle autour des sujets de cryptographie, IAM, PAM, NetSec)
•Gestion des solutions (administrer et maintenir en condition opérationnelle les solutions du périmètre, industrialiser et automatiser les processus autour des solutions, proposer des évolutions et améliorations continues autour des plate-formes et services)
•IAM / PAM (consolider, industrialiser et automatiser les solutions d'accès privilégiés, mettre en place une stratégie IAM au sein du groupe)
•Vulnérabilités, durcissement des systèmes et obsolescence (surveillance accrue des nouvelles vulnérabilités, assurer la mesure et coordination de l'état des vulnérabilités des systèmes au sein de Docaposte)
•Reporting et Présentation des KPI
•Participation aux Audits SSI

, editeur_offres Télétravail : 1
Temps de travail hebdomadaire : 39 heures

Profil

Vos compétences techniques:

oConnaissances:

-Réseaux et ses techniques d'attaques
-Systèmes Linux/Windows
-Tactiques et Techniques d'attaques (pentest/red teaming)
oScripting Bash/Python
oMaitrise CyberWatch/Rapid7/MISP/QRadar
oAnalyses de trace réseaux
oGestion d'incidents et de crises cyber

Certification technique CyberWatch, Rapid7 ou Qradar requis.

Motivé, réactif, dynamique, autonome et doté d'excellentes capacités d'analyse et de rédaction, vous avez le sens du service et du relationnel.
« Team spirit », vous êtes capable d'évoluer dans un environnement critique et sous contrainte.

Enfin, votre leadership est source d'inspiration.

Vous êtes disposés à faire des astreintes et votre niveau d'anglais est opérationnel.

, editeur_offres

Formation et expérience

De formation minimum BAC +5, vous justifiez d'une expérience professionnelle solide (dix ans) dans le domaine de la Cybersécurité et dans la mise en place d'outils de réponse à incident / amélioration continue des processus

de sécurité.

, editeur_offres