



FICHE DE POSTE SOC Analyst

En intégrant Aramys, vous ferez partie d'une entreprise familiale de 85 personnes en constante croissance. Nos collaborateurs sont notre principale richesse et nous investissons massivement dans la formation afin de faire évoluer les compétences. Nous gagnons en performance et en compétitivité et vous facilitons l'évolution vers d'autres métiers.

Nous nous soucions de votre bien-être et de votre équilibre, aussi nous avons mis en place une charte de télétravail de 2 jours/ semaine. Nous proposons également un véhicule de fonction que nous choisirons ensemble. Vous pourrez également bénéficier des offres de notre comité d'entreprise, ...

Aramys s'engage en matière de non-discrimination et dans la promotion de la diversité au sein de ses équipes. Nos postes sont ouverts à tous les profils.

Que proposons-nous ?

Rattaché(e) au service Cybersécurité, à l'équipe SOC (Security Operations Center) vous aurez la charge de l'identification précoce des cyberattaques, de faire des réponses adaptées face aux incidents de cybersécurité, définir d'une défense proactive pour limiter des risques liés aux vulnérabilités de nos clients

Vos principales missions et responsabilités :

- Contextualiser et qualifier de manière précise les incidents de sécurités
- Rédiger des rapports d'incidents de sécurité
- Améliorer les capacités de détection du service SOC
- Déployer, administrer et faire évoluer les différentes solutions au catalogue
- Fournir des recommandations sur les incidents de sécurité aux clients en vue d'assurer la gestion de l'incident
- Participer aux activités récurrentes du CSIRT Aramys
- Comprendre les techniques d'attaques informatiques, les analyser, et les expliquer.

Qui êtes-vous ?

Passionné par la Cyberdéfense et la sécurité informatique, vous possédez des connaissances dans les solutions Microsoft, Trend Micro, Palo Alto Networks, CISCO. Une bonne connaissance des outils big data (Kafka, Elastic, Hadoop, Splunk, Ossim, etc.) et des langages de scripting serait un vrai plus

Vous effectuez la veille permanente sur les menaces, les failles et la bonne utilisation du hardware et software, vous maîtrisez les méthodes d'analyse des flux et des outils de corrélation. Vous effectuez des tests d'intrusion en boîte noire, grise ou blanche pour les

systèmes, les applications Web et les réseaux afin de détecter les vulnérabilités et fournir des recommandations, votre anglais est opérationnel... alors ce poste est fait pour vous !

Niveau d'expérience : Master 2 / Diplôme d'ingénieur ou équivalent.

Référence de l'offre : 646358.

Localisation : Arras (62000), Lens (62300), Hénin-Beaumont (62110)

Type de contrat : CDI

Date de début : dès que possible.

Salaire : à définir.

