



Data Analyst – Traitement et intégration des données de Cyber Threat Intelligence [CDI] [START-UP] [CYBER] [DATA] [DEV] [CTI]

Notre entreprise

Co-fondée fin 2017 par deux spécialistes de Threat Intelligence issus du centre opérationnel de l'ANSSI (autorité française de cyberdéfense), **Citalid** a développé une nouvelle approche de gestion et de simulation du risque cyber à destination de grands comptes et d'entreprises stratégiques. Notre approche technologique, doublement primée aux Assises de la Sécurité 2018, puis lors du FIC 2020, répond directement aux exigences des RSSI, Risk Managers et assureurs. En 2021, nous avons été sélectionnés par le gouvernement français dans le cadre du Grand Défi Cyber, grâce au projet MATRICE qui a pour but d'unifier l'ensemble de la chaîne de pilotage des risques cyber dans un seul outil.

Notre plateforme est un outil d'évaluation et de pilotage des risques cyber unique qui permet d'évaluer financièrement les risques en prenant en compte les cybermenaces susceptibles de cibler l'entreprise, son niveau de défense et son contexte géopolitique. L'approche financière inédite adoptée par la plateforme permet de remonter l'information, dans un langage adapté, au plus haut niveau stratégique.

Notre équipe composée de passionnés de Cyber et de Géopolitique est actuellement à la recherche d'un ingénieur Data Analyst souhaitant mettre ses compétences au service de la cybersécurité pour un CDI !

Plus d'infos > <https://citalid.com/>

Vos principales missions

Les algorithmes prédictifs de Citalid se reposent sur des données de Cyber Threat Intelligence (CTI), collectées et analysées par l'équipe CTI constituée d'experts et d'analystes. Ces données décrivent les groupes d'attaquant, leur mode opératoire, leur victimologie, leurs objectifs et motivations, ...

Votre mission principale sera de mettre en place et de maintenir les processus et outils permettant de faire la jonction entre l'équipe CTI et les produits Citalid. A ce titre, votre travail servira aussi bien aux experts CTI qu'aux développeurs des produits de Citalid :

- **Mise en place et maintenance des outils de collecte et d'analyse de la donnée CTI** : l'équipe CTI utilise divers outils de collecte et d'analyse, qui doivent à la fois faciliter leur travail, et également permettre une exploitation des données par les produits de Citalid. Il s'agit donc de faire évoluer ces outils pour satisfaire ces deux besoins, notamment en garantissant la "propreté" des données (structure et validité des données), afin de permettre une utilisation automatisée.
- **Automatisation du process d'intégration des données CTI dans les produits Citalid** : en collaboration avec l'équipe CTI et l'équipe de développement, vous automatisez le déploiement des bases de données CTI dans les différents produits de Citalid. Vous privilégiez des formats standards (bundles STIX, ...) et gardez le bon déroulement de ces opérations.



- **Analyse et validation des données CTI** : vous facilitez l'analyse des données CTI et des résultats obtenus par leur exploitation dans les algorithmes Citalid, en mettant en place des outils de visualisation et d'analyse à destination des personnes en charge de la validation de ces données : l'équipe CTI, l'équipe Produit et l'équipe UX exploiteront ces outils pour réaliser les validations fonctionnelles.

Votre profil

Indispensable :

- École d'ingénieur ou équivalent
- Maîtrise du langage Python et de bibliothèques de traitement de données (Numpy, Pandas, ...)
- Fort intérêt pour la Cybersécurité et en particulier la donnée de Cyber Threat Intelligence
- Connaissance des méthodes et outils de collecte et d'analyse de données
- Rigueur, esprit d'initiative et autonomie
- Bonne communication et sens du travail en équipe
- Bon niveau d'anglais technique

Fortement apprécié :

- Expérience en traitement de données de Cyber Threat Intelligence (format STIX, MITRE ATT&CK, ...)
- Maîtrise des méthodes et outils de développement en équipe (Git, Gitlab, tests unitaires, revues de code, intégration continue, sprints, ...)

Nice to have :

- Expérience avec le framework backend Django
- Notion de modélisation de la donnée (UML)
- Bonnes compétences algorithmiques (algorithmes classiques, résolution de problèmes, complexité algorithmique, ...)

Ce que nous vous offrons

- Travailler sur un projet innovant mettant en œuvre des technologies variées et à l'état de l'art
- Une mutuelle d'entreprise de choc (Alan Blue) + une prise en charge des titres de transport à hauteur de 50% sur présentation de justificatif + des tickets restaurant d'une valeur faciale de 10 euros pris en charge à 50%
- Un cycle de formations internes dispensées par des experts du domaine dès votre arrivée
- Télétravail (hors Covid) flexible : possibilité de passer 1 à 2 jours par semaine en télétravail
- Rejoindre une équipe d'experts pluridisciplinaires passionnés évoluant dans une ambiance de travail dynamique et bienveillante.
- Faire partie d'une success story française de la cyber, secteur hautement stratégique et en plein essor !

Process de recrutement

CV et lettre de motivation obligatoires par mail à :

recrutement@citalid.com

copie à :

olivier.hamon@citalid.com

Informations complémentaires

Type de contrat : CDI

Période d'essai : 4 mois renouvelable

Date de début : ASAP

Lieu : Paris