ONYPHE, leader européen du scan d'Internet, est fournisseur de données techniques à destination des équipes de cybersécurité (CSIRT/CERT, SOC, CTI, Red Team, ...) en France et à l'international. Nos solutions d'ASD (Attack Surface Discovery), d'ASM (Attack Surface Management) et de CTI (Cyber Threat Intelligence) permettent à nos clients de défendre leurs périmètres à l'échelle d'un pays entier, et de suivre l'évolution de la menace sur Internet. Basée sur notre technologie propriétaire, l'expertise d'ONYPHE dans notre domaine d'activité est reconnue par nos pairs et nos clients. En priorisant la valeur de nos données et une proximité technique avec nos clients, nous sommes devenus un partenaire de confiance pour de grandes entreprises, des administrations et des gouvernements.

Nos enjeux concrets :

- ASD : Créer un inventaire des actifs d'une entité en partant de son nom de domaine ;
- ASM : Identifier les menaces sur les actifs exposés sur Internet pour éliminer les points d'entrée exploités par les cybercriminels (ex. : ransomware) ;
- CTI/Threat Hunting : Devenir la référence européenne des données de scan Internet, en rivalisant avec le leader mondial, et en élargissant sans cesse notre couverture (ports, protocoles, vhosts etc.) ainsi que la fréquence de rafraichissement.

Nous recherchons un **Analyste CTI – Cyber Threat Intelligence & Communication Technique.**

Votre mission : Valoriser nos données et notre expertise CTI

Vous rejoindrez une équipe technique pour donner du sens à nos données et renforcer notre visibilité auprès des clients, de nos prospects et de la communauté cyber. Votre rôle sera à la fois analytique (investigations, patterns) et communicationnel (contenu, conférences, réseaux sociaux).

Vos responsabilités clés :

- Réalisation d'investigations concernant la menace sur Internet ;
- Identification de patterns dans nos données pour enrichir la qualification des données ;
- Rédaction de contenu CTI sur le blog de l'entreprise ;
- Présentation lors de conférences afin de faire connaitre l'expertise ONYPHE dans ce domaine ;
- Participation à des conférences CTI ;
- Animation des réseaux sociaux d'un point de vue découvertes techniques ;
- Proposition d'évolutions de la techno dans le domaine de la CTI.

Profil recherché :
Vous aimez traquer les infrastructures des acteurs malveillants ? Vous avez un œil pour repérer les schémas suspects dans des jeux de données massifs et une plume pour en raconter l'histoire en français et en anglais ?

Chez ONYPHE, vous aurez :

- Un accès unique à des données de scan Internet pour identifier, cartographier et analyser les infrastructures ;
- La liberté d'investiguer : corrélation de données, détection d'anomalies, et qualification des menaces potentielles ;
- Un espace pour écrire : rédiger des analyses techniques, des rapports synthétiques ou des articles en français et en anglais pour transformer des données en récits utiles pour nos clients et la communauté cyber.

Ce qui nous intéresse :

- Un profil technique : vous maîtrisez les bases réseau (protocoles, analyse de trafic) ou système (comportements, logs). Ces connaissances sont essentielles pour exploiter nos données et identifier des infrastructures suspectes ;
- Un profil de chasseur : vous savez exploiter des données pour repérer des comportements anormaux ou des tendances émergentes ;
- Un talent pour la narration technique : vous aimez expliquer vos découvertes, que ce soit sous forme de rapports, de threads ou de présentations, y compris en anglais ;
- De la rigueur analytique : vous savez distinguer un faux positif d'une réelle piste et creuser pour comprendre en profondeur.

Bonus (mais pas obligatoire) :

- Expérience en analyse OSINT, ou détection de patterns dans des données massives ;
- Curiosité pour les méthodologies et outillages de Threat Hunting, ou pour tester de nouveaux outils d'analyse.

Rejoindre ONYPHE c'est :

- Rejoindre le leader Européen du scan Internet ;
- Travailler dans le vrai big data (bientôt en Peta Octets) ;
- Du 100% télétravail sans contraintes de localisation géographique (mais France préférée) ;
- Travailler sur du concret en ayant un réel impact dans le cyber ;
- Lutter réellement contre le cyber crime ;
- Scanner Internet sur le temps de travail ;
- Avoir une vue à 360 sur le fonctionnement et la stratégie de l'entreprise ;
- PEE + tickets restaurants ;
- Pas de couches hiérarchiques (mais il n'y a qu'un boss).