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 **Développeur Perl et Sysadmin FreeBSD.**

Votre mission : Développer le moteur de scan Internet et les API backend, et assurer le maintien en conditions opérationnelles et de sécurité de la plateforme de stockage et de scan.

Vos responsabilités clés :

- Assurer les évolutions logicielles de la solution ;
- Ajouter des nouvelles fonctionnalités logicielles ;
- Développer des API (Mojolicious) ;
- Assurer le maintien en conditions opérationnelles et de sécurité de l'infra de stockage (FreeBSD, Elastic Stack).

Les langages et technologies à maitriser :

- Perl, Mojolicious
- Mercurial
- FreeBSD
- Elastic Stack
- Expertise en big data serait un plus.

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).