

NOTRE HISTOIRE :

 Rejoignez Scaleway et façonnez le cloud souverain de demain !

Depuis 1999, nous concevons des infrastructures sécurisées, durables et pensées pour accompagner les entreprises les plus ambitieuses.

Historiquement reconnus pour nos serveurs dédiés Dedibox, nous avons pris en 2015 un virage stratégique vers le cloud computing. En restant fidèles à nos principes de simplicité, flexibilité et d'excellence technique, nous avons su trouver notre place parmi les leaders européens du secteur.

Avec l'essor de l'intelligence artificielle, nous avons choisi de renforcer notre engagement en bénéficiant du soutien du groupe Iliad, qui investit aujourd'hui 3 milliards d'euros pour développer une alternative IA souveraine et sérieuse aux géants américains et asiatiques.

Chaque jour et grâce à notre riche catalogue de produits et services (bare metal, conteneurisation, serverless, IA etc.), Scaleway sert fièrement 38 000 clients privés et du secteur public, de Photoroom à Mistral AI en passant par Golem.AI ou l'ADEME.

 Nos bureaux se trouvent à Paris, Lille, Rouen, Rennes, Toulouse, Bordeaux et Lyon.

POURQUOI AVONS-NOUS BESOIN DE VOUS ?

Notre croissance nous pousse à renforcer la **partie engineering de notre équipe CSIRT** afin de soutenir le développement des outils et services internes.

Votre mission sera de **concevoir, développer et maintenir des outils fiables et sécurisés**, tout en contribuant à la **réponse aux incidents**, afin d'améliorer notre visibilité interne sur les risques d'attaque et de répondre à nos obligations légales.

VOTRE FUTUR ÉQUIPE :

Nous évoluons dans un environnement **collaboratif**, où la diversité des Scalers, combinée à un esprit de partage, permet de concrétiser de nouveaux projets chaque jour et de faire avancer nos ambitions ensemble.

Vous ferez partie d'une **équipe agile de 5 personnes**, incluant un Tech Lead et un Manager. Vous collaborerez étroitement avec l'équipe **Trust & Safety** ainsi qu'avec d'autres départements de Scaleway. L'équipe est actuellement concentrée sur la finalisation de sa **stack interne**.

VOTRE QUOTIDIEN :

- Développer et maintenir des **outils de sécurité internes** pour le CSIRT et l'équipe Trust & Safety
 - Créer des outils et approches pour **atténuer les risques**
 - Contribuer à améliorer la **visibilité sur les surfaces d'attaque potentielles** en créant de nouveaux outils pour l'équipe SOC
 - Collaborer avec les autres équipes pour **assurer des pratiques secure-by-design**
 - Intégrer des outils open source (OpenCTI, Shodan, Shadowserver) dans notre stack interne pour permettre un travail efficace de l'équipe SOC
 - Automatiser les **capacités de détection et d'alerte** en fonction des retours de l'équipe SOC
 - Participer à la **planification des sprints** et aux workflows de développement agile
 - Fournir des **programmes de formation et de sensibilisation** aux bonnes pratiques de sécurité au sein de l'organisation
-

À PROPOS DE VOUS :



HARD SKILLS

- Minimum **3 ans d'expérience** avec des outils SIEM, EDR, SOAR et UEBA
- Expérience dans le **développement de vos propres outils de sécurité**
- Maîtrise du développement en **Golang et/ou Python**
- Bonne compréhension des **principes de sécurité** et des workflows de **réponse aux incidents**
- Expérience en **CTI (Cyber Threat Intelligence)** et solutions de surveillance de surfaces d'attaque comme OpenCTI, Shodan et Shadowserver
- Familiarité avec des services IT comme GitLab, Vault, etc.
- À l'aise dans un environnement **Unix/Linux**
- Certifications sécurité pertinentes (CISSP, GCIA, GCIH, GCFA, GCFE) un plus

- Compétences en **automatisation, configuration et intégration continue** : Ansible, Terraform, CI/CD (pipelines et déploiement automatisé)
- Maîtrise du **français** et bon niveau en anglais

SOFTSKILLS

- Esprit **collaboratif et orienté équipe**
 - Créatif et **proactif dans la résolution de problèmes**
 - Capacité à **s'adapter rapidement** et à gérer le stress
 - Curieux et désireux **d'apprendre**
 - **Esprit analytique et critique**
-

CE QUE VOUS TROUVEREZ CHEZ SCALEWAY ++++

- **Travail hybride** : jusqu'à 3 jours de télétravail par semaine
- **Locaux** : espaces de travail spacieux, dynamiques et au design audacieux, proches des transports. La plupart offrent des espaces extérieurs (terrasses) et des stationnements vélos.
- **Restauration** : service de repas équilibrés assuré par notre chef au siège, petit-déjeuner offert sur tous les sites toute l'année. Carte Swile pour les équipes en régions.
- **Engagements QVT** : salle de sport, berceaux d'entreprise, tarifs préférentiels pour services à la personne... Scaleway s'engage pour une vie équilibrée.
- **Environnement international** : plusieurs dizaines de nationalités, un cadre stimulant où l'anglais est aussi utilisé que le français.
- **Carrières & mobilités** : culture forte de mobilité interne, avec des passerelles possibles vers d'autres entités du groupe Iliad.

 **Pourquoi rejoindre l'aventure Scaleway ?**

- ✓ Une offre produit riche et diversifiée : plus de 100 produits cloud public sur le IaaS, PaaS et IA
 - ✓ Un environnement technique de pointe : infrastructures modernes, serveurs bare metal haute performance, défis techniques stimulants
 - ✓ Un engagement pour un cloud responsable : datacenters alimentés uniquement par de l'énergie renouvelable depuis 2017, empreinte écologique réduite, certification au plus haut niveau
-

 **LA SUITE ...**

- **Entretien découverte** avec un recruteur (30 min)
- **Entretien technique** pour évaluer vos compétences en sécurité et engineering (45 min)
- **Entretien avec le manager** pour comprendre votre approche du poste (45 min)

Chez Scaleway, nous nous engageons à construire un environnement inclusif et respectueux où chacun a une juste opportunité de s'épanouir.

Toutes les candidatures sont étudiées avec soin, sans distinction d'âge, de genre, d'orientation sexuelle, d'origine ethnique ou sociale, de religion, de handicap ou de toute autre caractéristique.

Nous croyons que les grandes idées viennent de partout et de chacun — c'est pourquoi vous devriez absolument postuler.