cert xmco
we deliver security expertise since 2002

Analyste Threat Intelligence

Au sein d'une équipe jeune, dynamique et riche en compétences, vous partagerez votre temps entre trois activités complémentaires :

- La **veille opérationnelle** sur les menaces (identification des IoC, surveillance de l'évolution des modes opératoires des attaquants, ...).
- La **protection de nos clients** au travers de renseignements fiables et contextualisés leur permettant d'adapter et d'améliorer leurs moyens de détection.
- Le **développement de nouveaux outils** permettant de développer le service (R&D).

En pratique, votre quotidien sera rythmé par les activités suivantes :

- **Effectuer une veille opérationnelle** afin de :
  - capitaliser et d'alimenter notre base de connaissances CTI ;
  - suivre les groupes d'attaquants (TTPs) ;
  - produire des indicateurs techniques fiables et contextualisés ;
- Développer nos **capacités d'investigations** (identification de nouvelles sources et de nouvelles méthodes de recherche) ;
- Enrichir notre réseau de **capteurs techniques** ;
- **Enrichir notre boîte à outils** (développement de scripts, développement de modules Serenety pour notre service de Cyber-surveillance, test des nouveaux outils open source)
- **Rédiger des rapports d'analyse sur les cybermenaces** (aspects techniques et stratégiques) à destination de nos clients et participer à la production des publications du cabinet (Blog, ActuSecu)

Profil recherché :

- Ingénieur, Master 2, Mastère spécialisé ou équivalent (formation en informatique, en sciences politiques, en langues, en géopolitiques, en intelligence économique, juridique, etc.)
- Curieux, motivé et passionné par la sécurité informatique
- Envie d'apprendre, d'évoluer et de partager ses connaissances au sein d'une équipe de consultants experts dans leur domaine

Compétences requises :

- Forte capacité d'analyse et de synthèse
- Maîtrise des techniques d'investigation en Cyber Threat Intelligence
- Bonne qualité rédactionnelle (français et anglais)
- Rigueur et curiosité, esprit d'équipe
- Capacités relationnelles importantes
- La maîtrise du Shell Unix et de Python (ou tout autre langage de Scripting) sera un plus
- La maîtrise d'une langue comme le russe, le chinois, l'arabe, etc. sera un plus.