

## Analyste Threat Intelligence

Au sein d'une équipe jeune, dynamique et riche en compétences, vous partagerez votre temps entre quatre 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** via la fourniture de renseignements fiables et contextualisés ;
- La **réalisation d'investigation** sur le **Darkweb** ;
- La **recherche et l'évaluation de nouveaux outils** permettant d'améliorer notre service.

Concrètement, votre quotidien sera rythmé par les activités suivantes :

### Recherches OSINT & investigations

- **Qualifier les menaces, évaluer leurs impacts** et leur criticité, et synthétiser ces analyses afin d'alerter nos clients en cas de risques ;
- **Analyser les événements remontés** par notre service de Cyber-surveillance, et faire des recherches manuelles ciblées pour aider nos clients à anticiper des attaques ;
- **Rédiger des notes d'analyses stratégiques** sur les cybermenaces à destination de nos clients ;
- **Établir une présence** sur les principaux espaces d'échanges du Darkweb (forum, marketplace, ...)

### Veille et publication de contenu

- Opérer **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 ;
- **Participer activement** à la production des publications du cabinet (Blog, ActuSecu).

### Amélioration de nos outils

- **Développer** nos capacités d'investigations (identification de nouvelles sources et de nouvelles méthodes de recherche) ;
- **Imaginer les pistes d'amélioration** de nos différents services et outils ;
- **Enrichir** notre réseau de capteurs techniques et notre boîte à outils (test des nouveaux outils, etc.).

#### Profil recherché :

- Master 2, Mastère spécialisé ou équivalent (formation en intelligence économique, sciences politiques, géopolitiques, etc.) ;
- Curieux, motivé et passionné par la Cyber Threat Intelligence et le Darkweb ;
- 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 ;
- Très bonne qualité rédactionnelle en anglais et en français indispensable ;
- La connaissance des outils et techniques d'investigation OSINT (type Maltego, RiskIQ) est un plus ;
- La maîtrise d'une langue comme le russe, le chinois, l'arabe, etc. est également un plus.