

# Analyste Forensics

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

- **Le traitement des incidents de sécurité**
- La réalisation d'une **veille opérationnelle** (#ThreatIntel)
- La **contribution à des développements technologiques**

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

- Réaliser des **investigations forensics**
- Définir la chronologie / timeline de l'attaque
- Rédiger des rapports de synthèse
- Comprendre le **mode opératoire des attaquants**
- Contribuer au développement de notre boîte à outils
- Participer à la production des publications du cabinet (Blog, ActuSecu)
- Capitaliser sur les interventions réalisées (maintien à jours des procédures / méthodologies / boîte à outils)
- Ponctuellement, intervenir sur des activités de **Reverse engineering**

## Profil recherché :

- Ingénieur, Master 2, Mastère spécialisé ou équivalent
- Curieux, motivé et passionné par la sécurité informatique (bonne compréhension de la sécurité « offensive »)
- 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
- Bonne qualité rédactionnelle (français et anglais)
- Connaissances techniques en sécurité (Techniques d'attaques)
- Connaissance des systèmes d'exploitation / de fichiers (Windows / Linux)
- Connaissance des principes d'Internet et des infrastructures réseau
- Maîtrise du Shell Unix et de Python (ou tout autre langage de Scripting)
- Rigueur et curiosité, esprit d'équipe
- Capacités relationnelles importantes
- Des certifications orientées DFIR seront un plus (SANS / GIAC, ...).