**ANSSI - Agence nationale de la sécurité des systèmes d'information**

# Analyste des modes opératoires d’attaquants – menaces systémiques F/H

Paris 15e Arrondissement, 75, Paris, Île-de-France

| Type de contrat | Niveau d'études |
|---|---|
| Titulaire, contractuel, militaire | Diplôme d'ingénieur, Master 2 ou titre équivalent de niveau Bac + 5 |
| **Prise de fonction souhaitée** | **Date limite de candidature** |
| 09/09/2024 | - |
| **Domaine professionnel** | **Niveau d'expérience** |
| Analyste de la menace cybersécurité | Junior (1 à 5 ans d'expérience) |
| **Rémunération** | **Avantages liés au poste** |
| mensuel net<br>annuel brut (selon expérience) | - |
| **Contraintes particulières d'exercice** | **Télétravail** |
| - | Oui |

## Descriptif de l'organisation

Rejoindre l’Agence nationale de la sécurité des systèmes d’information (ANSSI), c’est mettre ses compétences au service de l’intérêt général en participant à une mission capitale, d’actualité et porteuse de grandes responsabilités dans un monde où la cybersécurité est devenue l’affaire de tous !

Au sein de la sous direction Opérations (SDO), la division connaissance et anticipation (DCA) est chargée d’acquérir, de développer, de capitaliser et de partager la connaissance sur la menace informatique (Cyber Threat Intelligence, CTI). Cette mission repose notamment sur le bureau d’Analyse des Menaces Systémiques (AMS), chargé du suivi des menaces faisant porter un risque

systémique à la Nation.

AMS étudie l'écosystème et les acteurs de la cybercriminalité et de la lutte informatique offensive privée, mène des investigations en source ouverte et développe des méthodes et outils de suivi et d'analyse automatisés des codes et de l'infrastructure utilisés par les attaquants.

## Descriptif des missions

En qualité d'analyste des modes opératoires des attaquants, vous aurez pour mission principale de construire et capitaliser la connaissance sur les menaces faisant porter un risque systémique à la Nation, comme la cybercriminalité et les services offensifs. Vos investigations ont pour objectif d'enrichir les capacités de détection souveraine, d'orienter les activités d'audit et réponse aux incidents dans les systèmes d'information nationaux à la recherche de compromissions ainsi que de diffuser cette connaissance auprès de différents écosystème-relais. Les analyses sont réalisées à partir des incidents traités par la SDO, d'investigations en sources ouvertes (OSINT) et des informations fournies par nos partenaires institutionnels et commerciaux.

Vos activités principales• analyser les tactiques et techniques d'attaques contemporaines (méthodes, infrastructures, outils, vulnérabilités, scénarios d'infection, moyens de latéralisation, etc.) à partir d'incidents traités par la SDO, d'éléments disponibles en sources ouvertes ou d'échanges avec les partenaires commerciaux et institutionnels à l'échelle nationale et internationale ;
• réaliser les investigations de découverte et de suivi des infrastructures d'attaques faisant porter un risque systémique à la Nation à partir des éléments techniques à disposition de la SDO ;
• qualifier et capitaliser les nouveaux éléments caractéristiques identifiés afin d'enrichir les capacités de détection souveraines ;
• partager les connaissances acquises pour sensibiliser et orienter les équipes de veille, de détection, d'audit, de recherche de compromission et de réponse à incidents ;
• participer aux échanges, coopérations et groupes de travail avec les partenaires nationaux et internationaux de l'ANSSI dans son domaine d'expertise ;
• contribuer aux spécifications, au développement et à la mise en œuvre de l'outillage nécessaire à l'analyse et à la capitalisation des informations sur les menaces étudiées.

## Profil recherché

Diplôme d'ingénieur reconnu par la commission des titres d'ingénieur, ou cursus universitaire de niveau BAC+5 minimum dans le domaine des technologies de l'information et de la communication. Une formation spécialisée en sécurité du numérique sera un atout important et une bonne expérience du domaine de la cyber sécurité est attendue. De solides connaissances et compétences techniques sont nécessaires notamment en matière de sécurité des réseaux et de programmation.

Savoir-faire
Connaissances dans les domaines suivants :• sécurité des réseaux et architecture d'Internet ;
• techniques et outils utilisées lors d'attaques informatiques et contre-mesures associées ;
• outils et méthodes d'analyses utilisés dans le domaine de la CTI ;
• langage de développement (bash, python) ;
• capitalisation et modélisation des données.

Savoir-être• Grande curiosité ;
• Autonomie ;
• Capacité à prendre des initiatives ;
• Rigueur intellectuelle ;
• Sens du contact humain et du service ;
• Esprit d'équipe ;
• Discrétion.

## Process de recrutement

• Si votre candidature est présélectionnée, vous serez contacté(e) pour apprécier vos attentes et vos motivations au cours d'un entretien téléphonique ou physique.
• Des tests techniques pourront vous être proposés.
• Vous ferez l'objet d'une procédure d'habilitation.