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

Ingénieur développeur d'outils - analyse de la menace F/H

Type de contrat	Prise de fonction souhaitée	Localisation
Titulaire, contractuel, militaire	Poste à pourvoir immédiatement	Paris 15e Arrondissement, 75, Paris, Île-de-France
Niveau d'études	**Domaine professionnel**	**Niveau d'expérience**
Diplôme d'ingénieur, Master 2 ou titre équivalent de niveau Bac + 5	Analyste de la menace cybersécurité	Confirmé (5 à 10 ans d'expérience)
Rémunération	**Avantages liés au poste**	**Télétravail**
A définir selon expérience mensuel net A définir selon expérience	-	Oui

Descriptif de l'organisation

Le bureau Coordination des Analyses et Outillage (CAO) a pour objectif de parfaire la compréhension des intentions, des capacités et des opportunités des attaquants, et de renforcer les capacités de détection et d'identification de leurs victimes. En collaboration avec les bureaux en charge de l' Analyse de la Menace Ciblée (AMC) et de l'Analyse de la Menace Systémique (AMS), et plus largement, avec les autres divisions de la sous-direction opération, CAO est en charge de la coordination de travaux d'analyse au niveau technique ou stratégique ainsi que de la réalisation des projets capacitaires nécessaires à ses missions.

Le bureau est composé de coordinateurs assurant l'organisation et le suivi d'équipes pluridisciplinaires de travaux d'analyse (rétro-ingénierie, réseau, système, géopolitique, investigations en source ouverte) et d'ingénieurs pour le développement et la gestion des services / outils.

Descriptif des missions

Mission globale du poste

Afin de permettre aux bureaux d'analyse de la menace AMS et AMC d'accomplir leurs missions, le bureau CAO développe et maintien en condition opérationnelle plusieurs outils. Par exemple :

• des outils d'analyse de codes malveillants, y compris automatisés ;
• des services et applications de stockage et d'indexation de fichiers malveillants ;
• des outils de capitalisation de la connaissance sur les menaces ;
• des services d’exploration et d’exploitation des différentes bases de connaissances utiles aux investigations sur la menace ;
• des outils de gestion de marqueurs et de signatures, etc.

Missions et activités
Ainsi, vous aurez notamment pour mission de :

• maintenir et faire évoluer les services et applications ;
• améliorer les chaînes d’intégration et de déploiement continue des différents applicatifs ;
• sécuriser les infrastructures de déploiement ;
• industrialiser le système de monitoring et de remontée des alertes ;
• assurer la bonne montée en charge des différents outils ;
• formaliser auprès de la Division Infrastructures, Développements et Données (DID²) les besoins, notamment en matière d’infrastructure, de capacité de développement et d’accès aux données, nécessaires à la mise en œuvre des outils.

Compétences requises :

• Être expérimenté sur la mise en place de chaînes d’intégration automatisées (GitLab ou équivalent)
• Maîtriser des outils de déploiement automatique, de conteneurisation et d’orchestration (Ansible, Nomad, Swarm, Docker, Kubernetes) ;
• Savoir travailler avec une ou plusieurs typologies de bases de données courantes (ElasticSearch, Redis, PGSQL) et maîtriser leurs cadres d'emploi ;
• Connaissances sur les bus de gestion d'évènements (RabbitMQ, Apache Kafka, Redis)
• Connaitre les différents types d’architecture logicielle et leurs contraintes (redondance, distribution, haute disponibilité, notions de SLA etc.)
• Maîtriser le langage de programmation Python ;
• Être autonome sur la configuration et l’administration de systèmes GNU/Linux ;

Profil recherché

Vous êtes issu d’une formation d’ingénieur reconnue par la commission des titres d’ingénieur, ou vous avez suivi un cursus universitaire de niveau BAC+5 minimum. Vous avez une solide expérience dans le développement ou la mise en place opérationnelle d’applications. Une expérience de DevOps ou de SRE serait un plus.

En plus de celles requises (cf. ci-dessus), les compétences suivantes seront appréciées:

• Maîtrise d’autres langages selon différents paradigmes (par ex. C, C++, Rust, Golang, Java, JavaScript …) ;
• Maîtrise de la programmation système (Linux, Windows) ;
• Savoir-faire concernant la manipulation de grandes quantités de données ;
• Connaissances métiers dans le domaine de la CTI ;
• Notions de rétroconception de code.

Savoir être :

• curiosité, et ténacité ;

• agilité et recherche de l'échange avec les experts métiers ;
• autonomie et capacité à travailler en équipe ;
• esprit d’initiative et rigueur ;
• capacités rédactionnelles (spécification et documentation) ;
• sens du service.

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.