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

Analyste en outils et codes malveillants – menaces systémiques F/H

Type de contrat	Prise de fonction souhaitée	Localisation
Titulaire, contractuel, militaire	Poste à pourvoir immédiatement	Rennes, 35, Ille-et-Vilaine, Bretagne
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	Junior (1 à 5 ans d'expérience)
Rémunération	**Avantages liés au poste**	**Télétravail**
A définir selon expérience mensuel net A définir selon expérience	-	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, 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 en outils génériques et codes malveillants vous aurez pour mission principale de suivre et d'analyser les outils génériques utilisés dans le cadre d'attaques, les codes malveillants liés aux menaces systémiques, notamment la cybercriminalité et les services de lutte informatique

privée et de proposer des méthodes de détection et de protection contres ces menaces.

Vos activités principales : • analyser des codes malveillants de la cybercriminalité et ceux de la lutte informatique offensive privée recensés ainsi que les outils génériques utilisés à large échelle ;
• contribuer au développement des outils et méthodes d'analyse de codes malveillants utilisés par le bureau notamment à des fins de traitement automatisé ;
• synthétiser et capitaliser l'information (réalisation de rapports techniques d'analyse, de synthèses, présentation de fonctionnement de codes malveillants, moyen de detection, etc.) ;
• fournir un appui et développer des connaissances sur les incidents traités par la sous-direction ;
• alimenter et contribuer au développement des bases de connaissances internes de capitalisation des menaces, codes malveillants et de leurs moyens de détection (signatures) et de neutralisation
• participer aux échanges, coopérations et groupes de travail avec les partenaires nationaux et internationaux de l'ANSSI dans votre domaine d'expertise ;
• assurer une veille sur les menaces systémiques à partir de sources d'information variées (rapports d'éditeurs, publications d'experts, etc.), et capitaliser l'information notamment de manière automatisée.

Profil recherché

Diplôme d'ingénieur reconnue par la commission des titres d'ingénieur ou cursus universitaire de niveau BAC+3 dans le domaine des technologies de l'information et de la communication. Une expérience dans le domaine de la rétro-ingénierie (reverse) de codes malveillants est attendue.

Savoir-Faire• Fonctionnement des codes malveillants : installation, exécution, communication, protection (cryptographie, packing) ;
• Principaux outils d'analyse dynamique (x64dbg, windbg), comportementale (bac à sable) et statique (IDA Pro, Ghidra, etc.) de code et leur utilisation ;
• Assembleur x86/64 ;
• Au moins un langage de programmation de bas niveau et un langage de scripts (C, C++, Rust, Python, etc.) ;
• Fonctionnement interne d'un ou plusieurs systèmes d'exploitation ;
• Les types d'attaques informatiques et activités malveillantes.

Savoir-être• curiosité
• rigueur
• discrétion
• autonomie et esprit d'initiative
• capacité à travailler en équipe
• capacité à gérer simultanément plusieurs tâches
• 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.