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

Ingénieur cyberdéfense en détection F/H

Rennes, 35, Ille-et-Vilaine, Bretagne

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**
07/10/2024	-
Domaine professionnel	**Niveau d'expérience**
Analyste de la menace cybersécurité	Junior (1 à 5 ans d'expérience)
Rémunération	**Avantages liés au poste**
A définir selon expérience mensuel net A définir selon expérience 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 détection (DD) pilote la définition et la mise en œuvre de la stratégie nationale de détection des attaques informatiques sur le périmètre défendu. A ce titre, elle est responsable de la conception de la capacité souveraine de détection et opère un service permanent de supervision de la sécurité (SOC) au profit des services de l'Etat. Dans leurs domaines de compétence respectifs, l'ensemble des bureaux qui composent la division peut également être associé à la mise en place de dispositifs de supervision de circonstance, dans

le cadre d’opérations de réponse à incident, le suivi de menaces, ou en préparation d’événements majeurs.

Descriptif des missions

L’agent est positionné dans une équipe opérationnelle chargée de mettre en œuvre une capacité de défense en profondeur des systèmes d’information de l’Etat. L’intéressé(e) sera placé(e) sous la responsabilité directe du chef de bureau.

En s’appuyant sur les connaissances internes issues de la cyber threat intelligence et du traitement des incidents, vous êtes responsable de l’analyse des comportements adverses afin de mettre en place des mécanismes de détection pertinents.
Pour ce faire, vous occupez un rôle hybride qui permet d’intervenir sur un large spectre de missions : • En tant qu’analyste, l’ingénieur en détection étudie les menaces afin d’identifier les traces caractérisant des comportements anormaux ou malveillants ;
• En tant que concepteur/rice, l’ingénieur conçoit et améliore des briques techniques armant une capacité opérationnelle souveraine.

Vos activités principales sont :

• Investiguer depuis des journaux d’événements systèmes (Windows Security, Sysmon, Auditd, etc.) ;
• Analyser des comportements suspects ou malveillants affectant les systèmes d’information supervisés ;
• Participer à la mise en œuvre de techniques de détection d'activités de cybercrime et d’activités APT ;
• Développer des scripts et outils dédiés à la cyberdéfense (Python, bash, etc.) ;
• Mettre en œuvre et piloter des opérations de supervision ponctuelles en appui des équipes de réponse à incidents ;
• Assurer une veille technologique et maintenir une base de connaissances des techniques et outils (wiki, présentations au reste de l’équipe, etc.) dans un environnement opérationnel sensible.

Profil recherché

Vous êtes issu(e) d’une formation de niveau 7, (école d’ingénieur ou équivalent), vous disposez idéalement d’une expérience sur des fonctions similaires.

Compétences attendues :• Connaissances du fonctionnement des systèmes d’exploitation (Windows, Linux) et des attaques les plus courantes ;
• Capacité à analyser des rapports et à en extraire des idées de détection ;
• Intérêt pour les sujets liés à la threat intelligence (veille ciblée, rejeu de vulnérabilités, MITRE Att&ck, etc.).

Serait un plus :• Connaissance des outils de supervision de type SIEM et EDR ;
• Attrait pour la sécurité offensive et l'investigation numérique ;
• Connaissance des APT et leurs techniques (TTP).

Savoir être : • Sens du service de l’État ;
• Autonomie, rigueur, capacité d'adaptation.

Avantages :• Équipe pluridisciplinaire, environnement technique riche et forte expertise ;

• Catalogue de formations techniques ;
• Possibilité d'assister à des conférences internationales ;
• 44 jours de congés et RTT par an ;
• Télétravail.

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.