



Ingénieur cybersécurité en détection d'intrusion réseau F/H

Type de contrat	Prise de fonction souhaitée	Localisation
Titulaire, contractuel, militaire	Poste à pourvoir immédiatement	Paris 15e Arrondissement, Paris, Île-de-France, France
Niveau d'études	Domaine professionnel	Niveau d'expérience
Diplôme d'ingénieur, Master 2 ou titre équivalent de niveau Bac + 5	Développeur de solutions de sécurité	De junior à confirmé (3 à 10 ans d'expérience)
Rémunération	Avantages liés au poste	Télétravail
mensuel net annuel brut (selon expérience)	-	Non

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 Division Détection de la Sous-direction Opérations (SDO), le bureau Dispositifs de Détection Réseau (DDR) assure une expertise de haut niveau. Il développe, maintient et exploite des dispositifs de détection d'intrusions dans le but d'identifier des attaques ciblant les systèmes d'information d'intérêt pour l'Etat.

L'équipe compte actuellement 6 ingénieurs en conception de systèmes de détection d'intrusion réseau, un data-scientist et un ingénieur administrateur système. Pour les travaux de fond, chacun est autonome, et rend compte de son travail à ses pairs quotidiennement. De grands travaux de rationalisation sont prévus qui nécessiteront un travail en équipe.

Descriptif des missions

En un mot :

L'équipe est composée d'ingénieurs qui comme vous sont spécialisés en systèmes de détection réseau. Actuellement, elle développe, améliore et renforce les capacités des sondes souveraines.

Votre mission sera d'abord de monter en connaissance et compétence sur les sondes du marché comme sur celles-ci. Ensuite, il vous faudra analyser des comportements malveillants pour écrire des protocoles qui nous permettront de les détecter sur les réseaux bénéficiaires et de favoriser la lecture des données que nous collectons à ceux qui les analyses.

Vos activités principales :

- Concevoir, développer et intégrer les composants des dispositifs de détection d'intrusions réseau tels que des moteurs d'inspection de paquets (DPI), des moteurs de règles et des dissecteurs protocolaires ;
- Maintenir une expertise technique sur la détection d'intrusion réseau ;
- Assurer le développement des signatures de comportements malveillants connus sur les sondes de détection ;
- Participer à la maintenance opérationnelle des systèmes de détection d'intrusion déployés ;
- Mettre en forme les données collectées pour les rendre compréhensibles par les analystes.

Avantages :

- Equipe jeune et dynamique ;
- 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 partiel à négocier.

Profil recherché

Compétences attendues :

- Bonne connaissance du fonctionnement des suites protocolaires TCP/IP ;
- Appétence pour la détection réseau ;
- Très bonne connaissance en développement logiciel, tests unitaire, documentation ;
- Maîtrise d'un langage de développement de bas niveau de type C/C++ ;
- Connaissance de l'architecture des systèmes d'exploitation de type Unix.

Compétences bonus :

- Connaissance en développement de systèmes d'inspection de paquets (DPI) ;
- Connaissance d'un système de détection d'intrusion et son implémentation ;
- Expertise réseau (protocoles réseau, analyse de trames, etc) ;
- Connaissance des modes opératoires des attaquants (Kill chain, MITRE ATT&CK).

Appétences appréciées :

- Autonomie ;
- Curiosité ;
- Rigueur ;
- Capacité à travailler seul et en équipe ;
- Goût pour transmettre son savoir.

Process de recrutement

- Si votre candidature est présélectionnée, vous serez contacté(e) pour apprécier vos attentes, vos

motivations et évaluer vos compétences via des tests techniques ;

- Les entretiens de sélection pourront être menés en visio-conférence ou en présentiel par l'employeur accompagné par la division des ressources humaines ;
- Vous serez informé(e) des suites données à votre candidature ;
- Le poste proposé nécessitant d'avoir accès à des informations relevant du secret de la défense nationale, vous ferez l'objet d'une procédure d'habilitation.