



Ingénieur cybersécurité datascience 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 spécialisés en systèmes de détection réseau. Actuellement, elle développe, améliore et renforce les capacités des sondes souveraines. Avant de prendre en compte

vosre mission, il faudra d'abord monter en connaissance et compétence sur les sondes du marché comme sur celles-ci, afin de connaître votre environnement. Ensuite, il vous faudra favoriser la lecture des données que nous collectons à ceux qui les analyses. Enfin, il vous faudra analyser les structures de données ou leur comportement pour conduire des investigations de haut niveau dans les incidents que nous détectons sur les réseaux bénéficiaires.

Vos activités principales :

- Mettre en forme, normaliser et corrélér les données collectées pour les rendre compréhensibles par les analystes ;
- Assurer des investigations de haut niveau en corrélant les différents types de données ;
- Porter un projet d'écriture de méthode d'investigation appliqué à nos données ;
- Assurer une montée en compétence des analystes selon vos modèles de traitement des données ou d'investigation ;
- Participer à la conception, au développement et à l'intégration des 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 ;
- Participer au développement des signatures de comportements malveillants connus sur les sondes de détection ;
- Aider à la maintenance opérationnelle des systèmes de détection d'intrusion déployés.

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 :

- Expertise en data-science ;
- Bonne connaissance du fonctionnement des suites protocolaires TCP/IP ;
- Appétence pour la détection réseau.

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.