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

Expert en investigation numérique F/H

Paris 15e Arrondissement, 75, Paris, Île-de-France

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**
01/01/2025	-
Domaine professionnel	**Niveau d'expérience**
Analyste réponse aux incidents de sécurité	Confirmé (5 à 10 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 Opération (SDO) et de la division Réponse (DR), le bureau Investigation Numérique (INM) est responsable des analyses techniques nécessaires au traitement d'incidents ou de signalements de sécurité.
A ce titre, le bureau est en charge de développer l'expertise de la sous-direction en investigation numérique sur les aspects système et réseau des technologies que la Division Réponse est amenée à rencontrer lors du traitement des signalements et incidents (Windows, Linux/Unix, MacOs,

équipements réseaux, téléphonie, SCADA, Cloud, etc…).

Descriptif des missions

En tant qu'expert technique, vous serez responsable des analyses techniques nécessaires au traitement d'incidents ou de signalement de sécurité, préalablement qualifié par le bureau incidents et signalements ou le bureau de coordination des analyses. Vous interviendrez également comme expert en investigation numérique au profit des équipes d'intervention des opérations de cyberdéfense.
Vous participerez au développement de l'expertise de la sous-direction en matière de traitement d'incident et d'analyse de systèmes d'information compromis : logiciels, parc informatique, matériels, équipement réseau, SCADA, téléphonie, etc…

Vous aurez comme activité principale l'analyse forensique de systèmes compromis : analyse de relevés techniques, d'images disques, d'images mémoires, de journaux d'événements et de traces système, réseau et applicatives, ainsi que l'analyse statique et dynamique de codes et documents malveillants. Vous participerez aussi aux opérations de cyberdéfense en base arrière ou dans des missions projetées.

En dehors des activités de traitement des incidents qui vous seront confiés, vous serez amener à :• entretenir et développer votre expertise en techniques et outils d'investigation numérique, exploitation de vulnérabilités, méthodes et outils d'analyse (veille, formation, conférences internationales…);
• concevoir et réaliser des outils pour améliorer les opérations d'investigation numérique ;
• transmettre vos compétences en interne via des sessions de formation et réalisations de documentations ;
• participer aux différentes publications de l'ANSSI.

Selon votre expérience et centres d'intérêts, vous serez amené à développer au profit du bureau une expertise sur des domaines spécifiques de l'investigation numérique (recherche de compromission à l'échelle d'un parc, équipement réseau, téléphone mobile, analyse matérielle, etc…).

Profil recherché

Vous êtes titulaire d'un diplôme de niveau 7 (universitaire ou ingénieur) et vous avez une expérience technique avancée dans le domaine de la sécurité informatique ou de très bonnes compétences en développement ou en administration des systèmes d'information et l'envie de vous spécialiser dans l'investigation numérique.

Des connaissances dans les domaines suivants seront recherchées :• systèmes d'exploitation
• applications et leurs vulnérabilités
• attaques et activités malveillantes
• outils d'investigation numérique
• protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation
• langages de programmation de bas niveau et langages de scripts

De plus, vous avez des connaissances dans les :• téléphones mobiles (systèmes d'exploitation, acquisition de données techniques, etc…)
• équipements réseaux (systèmes d'exploitation, configuration, etc…)
• analyse matérielle (JTAG, acquisition et analyse de firmware, etc…)
• SCADA (architecture, protocole réseau, etc…)

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.
• Télétravail possible sous certaines conditions.
• Vous ferez l'objet d'une procédure d'habilitation.