



Responsable des activités industrielles pour la cyberdéfense F/H

Type de contrat	Prise de fonction souhaitée	Localisation
Titulaire, contractuel, militaire	Poste à pourvoir immédiatement	Paris 15e Arrondissement, 75, Paris, Île-de-France
Niveau d'études	Domaine professionnel	Niveau d'expérience
Diplôme d'ingénieur, Master 2 ou titre équivalent de niveau Bac + 5	Coordinateur sécurité	Confirmé (5 à 10 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 des Opérations, la Division Ecosystèmes, Services et Coordination (DESC) a pour mission de coordonner la fourniture à l'extérieur des services portés par la sous-direction Opérations sous la marque CERT-FR.

Au sein de la Sous Direction Expertise et de la Division Industrie et Technologies (DIT), le bureau « environnement industriel » (BEI) identifie et accompagne les entreprises et offres portant des enjeux de cybersécurité. Le bureau développe et maintient la relation avec les fournisseurs de produits et services, anime les communautés d'offres, analyse le marché et gère les projets visant à favoriser le développement de solutions de confiance.

Descriptif des missions

Sous l'autorité du chef du bureau environnement industriel, vous serez rattaché à la Division Ecosystèmes, Services et Coordination (DESC) pour agir en immersion au sein de la Sous Direction des Opérations (SDO) et y apporter votre expertise en matière de coopération avec l'industrie de la

cyber.

Vous aurez pour missions de :

- Assurer la liaison, faire circuler l'information et coordonner l'action sur les sujets relatifs au secteur industriel entre les deux sous-directions concernées ;
- Identifier les acteurs clés de l'industrie du domaine de la cybersécurité, ou dont les solutions répondent aux besoins opérationnels, en coordination avec les pilotes de partenariats (notamment : éditeurs, prestataires en détection, CTI, réponse, audit, etc.) et recueillir l'information à usage opérationnel ;
- Participer à la construction des partenariats avec l'industrie utiles à la mission de cybersécurité notamment en lien avec les visas de sécurité, afin d'orienter la feuille de route des partenaires et répondre aux besoins à moyens et courts termes de la Sous Direction des Opérations et des écosystèmes opérationnels nationaux;
- Identifier et rendre compte des constats d'insuffisance de l'offre privée au regard des besoins de cybersécurité ;
- Contribuer aux travaux d'accompagnement des offreurs pour faire émerger des solutions adaptées aux besoins opérationnels (roadmap produits, maturité offre, conformité) ;
- Participer à l'animation de communautés d'offeurs pour faciliter le partage de connaissances d'intérêt opérationnel avec l'écosystème ;
- Contribuer à la mise en œuvre de projets financés par le Centre National de Coordination Cyber pour favoriser l'émergence de solutions de confiance ;
- Participer au recueil des besoins des écosystèmes relais du CERT-FR afin de capitaliser les offres disponibles.

Nécessités du poste :

- Double rattachement nécessitant de grandes qualités de compte-rendu et des facultés d'adaptation ;
- Travail en multisites (Campus Cyber - Puteaux et Paris 15e).

Profil recherché

Vous êtes détenteur d'un diplôme ou d'un titre de niveau BAC+5, ou pouvez justifier d'acquis équivalents et, disposez de connaissances et expériences solides des technologies de l'information et de la communication, en particulier dans le domaine de la sécurité des systèmes d'information.

Savoir-faire

- Sens avéré de la diplomatie et de la négociation ;
- Bonne connaissance du marché de la cybersécurité et des enjeux de confiance du numérique ;
- Connaissance générale sur les différents métiers associés à la lutte informatique défensive (détection, investigation numérique, audit, traitement d'incidents, analyse de logiciels malveillants, etc.) ;
- Connaissance de la réglementation, de l'organisation de la SSI et des acteurs du domaine cyber ;
- Une maîtrise de l'anglais à l'écrit et à l'oral est nécessaire.

Savoir-être

- Rigueur et sens des responsabilités ;
- Qualités relationnelles ;

- Autonomie et esprit d'initiative ;
- Esprit de synthèse ;
- Sens du service de l'État.

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.