Autorité de la concurrence

La concurrence au service de tous

Administrateur systèmes et réseaux en charge de la cybersécurité (H/F)

Service des systèmes d'information

Publication le 16 janvier 2023

Autorité administrative indépendante, l'Autorité de la concurrence veille au bon fonctionnement concurrentiel de l'économie en France. Elle contribue à la régulation de la concurrence aux niveaux européen et international. Sa compétence transversale la conduit à intervenir dans tous les secteurs économiques.

Elle a en charge 4 grandes missions :

- **Lutter contre les pratiques anticoncurrentielles** (ententes et abus)
- **Contrôler les opérations de concentrations** (fusions et rachats)
- **Emettre des recommandations** (avis aux pouvoirs publics et acteurs économiques)
- **Réguler les professions réglementées**

Figurant parmi les meilleures autorités de concurrence au monde dans le classement de la Global Competition Review, l'Autorité est également en pointe sur les nouvelles problématiques liées à l'économie numérique et au développement durable.

ENVIRONNEMENT DU POSTE

Sous l'autorité du secrétaire général, le service des systèmes d'information est composé d'un chef de service, d'un chef de projet applicatif et numérique, de deux administrateurs systèmes et réseaux dont un en charge de la cybersécurité, d'un développeur applicatif et trois techniciens support.

Le service des systèmes d'information est chargé de mettre à disposition des utilisateurs, des ressources informatiques et audiovisuelles communes. Il offre une assistance personnalisée aux usagers et garantit la sécurité du système d'information de l'établissement.

DESCRIPTION DU POSTE

L'administrateur systèmes et réseaux en charge de la cybersécurité est responsable de la sécurité des systèmes informatiques et des réseaux. Il est chargé de protéger les données sensibles et les informations critiques contre les cyberattaques et les violations de la confidentialité. Pour ce faire, il met en place des procédures, des outils de sécurité et propose des politiques pour prévenir les intrusions et détecter les incidents.

Il est également responsable de l'administration et de la maintenance des systèmes de détection d'intrusion, des pare-feux, des VPN, des systèmes de détection de menaces, des logiciels de chiffrement et d'autres outils de cybersécurité. Il peut également être chargé de superviser les procédures de sauvegarde des données, de la récupération après sinistre, et de la gestion des accès utilisateur.

Il est enfin tenu de se tenir informé des menaces et des vulnérabilités les plus courantes, et de mettre en place des mécanismes pour les détecter et les corriger rapidement. Il doit également participer à la réalisation d'audits de sécurité réguliers et de tests d'intrusion pour évaluer la sécurité des réseaux et des systèmes informatiques. Il doit être en mesure de répondre rapidement aux incidents de sécurité et de coordonner les efforts de l'équipe pour remédier aux problèmes de sécurité.

L'administrateur systèmes et réseaux en charge de la cybersécurité sera chargé des activités suivantes :

- Installation, configuration et maintenance des systèmes d'exploitation et des logiciels réseau ; planification et mise en œuvre des mises à niveau et des mises à jour.
- Surveillance et gestion des performances des systèmes et des réseaux ; résolution des problèmes et des incidents.
- Conception et mise en place de solutions de stockage ; sauvegarde et restauration des données.
- Mise en place de politiques de sécurité et de contrôles d'accès ; gestion des utilisateurs et des autorisations d'accès.
- Communication avec les différents départements de l'institution ; documentation et suivi des activités liées aux systèmes et aux réseaux.
- Surveillance de la sécurité des systèmes et réseaux ; protection des systèmes et données contre les menaces extérieures.
- Audit de sécurité régulier et mise en place des politiques de sécurité ; mises à jour de sécurité pour les systèmes et applications.
- Gestion des incidents de sécurité ; planification de la récupération en cas d'incident.
- Sensibilisation des agents à la sécurité informatique.
- Gestion des relations avec les partenaires et fournisseurs de sécurité.

La fonction est éligible au télétravail.

PROFIL DU CANDIDAT

Le candidat doit justifier d'une formation supérieure en informatique, en particulier en architecture des systèmes et réseaux d'information et de communication et de connaissances avancées en sécurité des systèmes d'information et méthodes d'analyse des risques et d'audit.

Le candidat doit posséder une expérience professionnelle significative sur la fonction d'administrateur systèmes et réseaux. Une montée en compétence sur la partie cybersécurité pourra être proposée sous la forme d'un plan de formation qualifiante.

Les fonctions à exercer requièrent des capacités d'organisation, de méthode, d'analyse, de synthèse, de veille ainsi que des capacités d'écoute, de pédagogie et de persuasion. Elles nécessitent également de bonnes qualités rédactionnelles et d'une disponibilité et réactivité en cas de menaces ou d'incidents de sécurité.

Le candidat doit justifier des compétences et niveaux suivants :

SAVOIRS :

- Niveau expertise requis immédiatement : Administration des systèmes informatiques et de communication - Techniques de surveillance de l'exploitation des systèmes et des réseaux.
- Niveau maîtrise requis immédiatement : Analyser du système de cybersécurité et élaboration des plans d'action et de sécurité – Administration et supervision du Security Operating Center - Veille sur les menaces et prévention des potentielles attaques

SAVOIR-FAIRE :

- Niveau expertise requis immédiatement : VPN - Certificats PKI - VLAN - 802.1x - DHCP - DNS - DMZ - Fibre - LACP - Trunks - Spanning tree - Couches OSI - TOIP, VISIO - LDAP - Radius NPS - RSA - Microsoft Exchange

(2016, 2019, Load balancing) - Microsoft Server 2012, 2016, 2019 - Microsoft services (SQL server, WSUS, IIS, GPO, etc.) - VMWARE Vsphere (SDRS, DRS, HA, vMotion, DvSwitchs, etc.).

- Niveau maîtrise requis immédiatement : Linux - Debian - Ubuntu - Stratégies de sauvegarde - Stockage et réseaux fibres - Firewalls - WAF - EDR - Antivirus – SIEM – Antispam – Syslog - WIFI 6E - Chiffrement de postes.

Le candidat saura travailler en équipe et faire preuve d'autonomie et d'esprit d'initiative. Pour autant, il saura régulièrement rendre compte de l'évolution de son travail.

Réactif, rigoureux et discret il témoignera d'une capacité à déterminer les priorités, anticiper les échéances et respecter les délais avec souci du résultat et de l'efficacité.

MODALITES DE CANDIDATURE ET DE RECRUTEMENT

Ce poste est ouvert aux fonctionnaires de catégorie A des ministères économiques et financiers ou par voie de détachement, aux agents des fonctions publiques d'État, territoriale ou hospitalière.

Ce poste est également ouvert aux agents contractuels titulaires d'une formation supérieure en informatique. Le recrutement se fera par contrat à durée déterminée d'une durée de trois ans.

Les candidatures (curriculum vitae et lettre de motivation) sont à adresser, par courriel, au plus tard le **26 février 2023** à recrutement@autoritedelaconcurrence.fr

Merci de noter sur votre candidature la référence de l'offre : « **ASR.CYBERSECURITE.2023** »

Des renseignements peuvent être pris auprès de :
Noëmie Picand, chargée du recrutement au service des ressources humaines (01.55.04.01.06)
Cyrille Garnier, chef du service des systèmes d'information (01.55.04.00.17)

Autorité de la concurrence
11, rue de l'échelle, 75001 Paris
01 55 04 00 00
www.autoritedelaconcurrence.fr