Numérique

Administrateur plateformes Cloud Native H/F

Levallois-Perret (92)

La DGSI est un service de renseignement français relevant du Ministère de l'Intérieur. Travailler à la DGSI, c'est être au cœur des enjeux du XXIème siècle et participer à la protection des français en mettant ses compétences au service de l'Etat, à travers des missions telles que :

Contre-terrorisme et extrémismes violents | Contre-espionnage | Protection économique et contre-prolifération | Cyberdéfense

LES MISSIONS

En tant qu'administrateur.rice des plateformes Cloud Native, vous êtes intégré.e dans l'entité des systèmes, des middlewares, des services Linux et de l'écosystème Cloud Native (Landscape CNCF).

En collaboration avec le.la chef.fe de section/Tech Lead : Vous maintenez en condition opérationnelle et de sécurité les solutions afférantes à l'écosystème CNCF (orchestrateurs de conteneurs, conteneur engine, Images registry, opérateur de déploiement...)

- Vous définissez les rôles et droits RBAC des utilisateurs ;
- Vous préparez les modèles pour les objets liés à l'orchestrateur ;
- Vous construisez les templates de descripteurs de déploiement ;
- Vous déployez et maintenez en condition opérationnelle et de sécurité la chaîne de déploiement continue selon les principes GitOps en coordination avec les équipes en charge de la forge CI ;
- Vous contribuez à l'implémentation des bonnes pratiques dans un environnement technique vairié et impulsez les processus et les outils associés au déploiement auprès des équipes de développement ;
- Vous participez également au bon fonctionnement et à la sécurisation (DICT) des solutions déployées en conformité avec la politique de sécurité de la direction ;
- Vous assurez le support N2 sur incident excaladé. Le cas échéant, vous assurez le suivi auprès des fournisseurs/éditeurs ou du support N3 ;
- Vous assurez le suivi, le monitoring et le reporting des composants mis en place et participez à la fourniture des indicateurs de consommation et de performance pour la construction du capacity planning ;
- Vous assurez la remontée des logs vers le SOC ;
- Vous mettez à disposition les éléments de configuration à externaliser sur des supports de sauvegarde ;
- Vous participez aux tests périodiques sur votre périmètre dans le cadre du PRI/PCI ;
- Vous rédigez la documentation associée à votre périmètre d'action (DIN,DEX, fiches réflexes,...) ;
- Vous automatisez les moyens de provisionnement et de configuration sur votre périmètre ;
- Vous assurez une veille technologique sur votre périmètre et documentez l'usage de nouveaux produits ou de nouveaux processus.

En complément, vous serez amené.e à intervenir sur les systèmes et services Linux « legacy » pour assurer la continuité de service.
Au-delà des compétences techniques, nous recherchons un.e collaborateur.rice ayant le sens de l'intérêt général, prêt.e à relever des défis technologiques variés, force de proposition et capable d'émuler les bonnes pratiques selon les principes GitOps, SRE, et DevSecOps auprès de ses collaborateurs.

PROFIL RECHERCHÉ

Titulaire d'un diplôme en informatique vous possédez les compétences techniques suivantes :

- Maîtrise des OS et services Linux de la famille Red Hat (KickStart, web, réseaux, repo yum/dnf, lvm, systemd,...) ;
- Maîtrise sur les protocoles de stockage (NFS, CIFS,...) et éventuellement sur le protocole S3 (bucket S3 et IAM associé)
- Maîtrise de scripting (Bash, Python,...) et d'un repostiory (Git, Nexus,...) ;
- Maîtrise d'au moins une technologie permettant l'automatisation et l'industrialisation des déploiements et/ou de la gestion des configurations (Ansible, Chef, Puppet,...) ;
- Maîtrise des protocoles et services réseaux de niveaux 2 et 3 dans le périmètre LAN Datacenter ;
- Maîtrise des mécanismes de sécurité des systèmes d'information (règle iptables ou équivalent, syslog, reverse proxy, RBAC, mécanismes d'authentification, chiffrement at rest, chiffrement en transit, ...) ;
- Maîtrise d'un outil de gestion de conformité (Katello/Foreman,...) serait un plus ;
- Maîtrise de conteneurisation (construction d'images OCI, utilisation d'un registry,...) ;
- Connaissances générales sur les principes GitOps, DevSecOps, SRE et des pipelines, Cintegration/Cdelivery/Cdeplyment ;
- Connaissances générales sur l'architecture applicative, fonctionnelle et techniques des systèmes d'information;
- Connaissances générales sur les méthodes de mise en production, ITIL-ISO 200000 ;

Protéger, Veiller... dans l'ombre

CONTACTS

recrutement-dgsi@interieur.gouv.fr

DGSI – Direction Générale de la Sécurité Intérieure

www.dgsi.interieur.gouv.fr

Nationalité française requise

- Poste catégorie A/B
- Habilitation « Très Secret »
- CDD jusqu'à 3 ans, renouvelable et évoluant vers un CDI
- 54 jours de repos (25 jours de congés annuels + 29 ARTT au régime de 40h30 hebdomadaires)
- Restauration sur place / Actions sociales