Offer #2024-07619

Administrateur de solutions de sécurité

The offer description below is in French

Level of qualifications required : Bachelor's degree or equivalent

Fonction : Support functions

Corps d'accueil : Ingénieur d'Etudes (IE)

Level of experience : From 3 to 5 years

Context

Le Centre des Ope□rations de Se□curite□ est compose□ de deux po□les :

- Un po□le de□die□ a□ la de□tection et la re□ponse a□ incident

  Ce po□le a en charge la qualification des failles de se□curite□ pouvant porter atteinte au SI d'Inria, de la de□tection des failles ave□re□es et de la coordination des actions de se□curisation. Il assure la de□tection des incidents de se□curite□ et le pilotage de leur re□solution. Il est en charge de la coordination ge□ne□rale des de□tections et des re□solutions, ainsi que du reporting au niveau RSSI et DSI.

- Un po□le de□die□ a□ l'administration des solutions de se□curite□

  Il a en charge l'administration et l'exploitation fonctionnelles des solutions de se□curite□ (SIEM, Scanner de vulne□rabilite□s, laboratoire forensique, WAF, passerelles anti-spams, CTI, sondes, Firewall, ...), en collaboration e□troite avec le Service Production, partageant les me□mes processus, environnements techniques et documentations.

Assignment

Vous contribuerez a□ la mise en place du nouveau po□le de□die□ a□ l'administration des solutions de se□curite□ en collaboration e□troite avec les e□quipes de production.

En tant qu'administrateur de solutions de se□curite□, vous aurez en charge l'administration et l'exploitation fonctionnelles des services nume□riques de se□curite□. Vous participerez au bon fonctionnement de ces solutions de se□curite□ en garantissant leur maintien en conditions ope□rationnelles et en condition de se□curite□.

Sous la responsabilite□ du responsable de service, vous participerez a□ la cre□ation et a□ la mise en place de ce nouveau po□le au sein du centre des ope□rations de se□curite□ qui vise a□ re□unir des ressources spe□cialise□es en production d'outils de se□curite□.

Vous travaillerez en e□troite collaboration avec les services owner des solutions et le service de production ainsi qu'avec les services implique□s dans les diffe□rents services de se□curite□ (SP, SA, CDS, SCI).

Main activities

Au sein du Centre des Ope□rations de Se□curite□ et sur le pe□rime□tre des services nume□riques se□curite□, vous serez amene□ a□ :

- Animer et suivre l'activite□ du po□le d'administration des solutions de se□curite□,
- S'assurer du fonctionnement optimal des solutions de se□curite□,
- Contribuer au parame□trage des solutions de se□curite□, ge□rer les changements,
- Mettre en place la collecte des logs et des alertes issues des solutions vers un service de de□tection d'incidents,
- Re□diger et maintenir de la documentation, des proce□dures et des modes ope□ratoires des processus d'administration fonctionnelle,

- Participer a la conception, au developpement et a la maintenance des outils permettant d'ameliorer le fonctionnement du Centre des Operations de Securite notamment en matiere d'outils de detection et d'investigation,
- Participer aux operations relatives au traitement des incidents (verrouillage ou controle d'acces, archivage de logs, ...)
- Maintenir et faire evoluer les solutions de securite,
- Valider l'installation des outils dans l'environnement de production,
- Traiter les incidents ou anomalies ainsi que les exceptions,
- Veiller au bon fonctionnement de la remontee des logs et des alertes,
- Animer l'activite d'administration fonctionnelle des services numeriques de securite,
- Participer a l'elaboration des strategies de detection des incidents de securite (incidents redoutes, scenarios de detection, regles de correlation, collecte, notification),
- Participer a des projets de securisation du SI,
- Assurer une veille technologique permettant de conserver un haut niveau de technicite.

Skills

Savoirs :

- Maitrise des processus de production,
- Maitrise de la securite des systemes d'exploitation et de la securite des reseaux,
- Maitrise de l'administration fonctionnelle d'un ou plusieurs outils de securite (WAF, Firewall, Sondes de detection, Antivirus, ...),
- Maitrise des environnements Linux et/ou Windows,
- Maitrise d'un langage de scripting (Python, PowerShell, Bash, ..),
- Connaissances des principes d'attaques et d'intrusions,
- Connaissance de l'environnement juridique lie aux contraintes SSI dans un etablissement de recherche : PPST, RGS, RGPD, ...,
- Connaissance des processus ITIL.

Savoir-faire :

- Capacite a animer, a organiser et hierarchiser les priorites,
- Capacite a travailler en equipe et a distance,
- Capacite a configurer des outils lies aux services numeriques de securite,
- Capacite a ecouter et dialoguer avec des experts techniques et des utilisateurs,
- Capacite a elaborer des procedures, consignes et documents techniques,
- Capacite a ecouter et dialoguer avec des experts techniques et des utilisateurs,
- Capacite a analyser des journaux d'evenements (systemes, reseaux, applicatifs) et a correler les informations de nature differente.

Savoir-etre :

- Rigueur et sens de l'organisation et de l'animation,
- Avoir le sens du service a l'usager,
- Avoir le sens du collectif,

- Diplomatie et qualite□s relationnelles,
- Bonne gestion du stress.

Langues :

- Franc□ais : courant,
- Anglais : technique.

Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)

General Information

- **Town/city :** Le Chesnay
- **Inria Center :** Siège
- **Starting date :** 2024-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-07-31

Contacts

- **Inria Team :** DSI-SOC
- **Recruiter :**
  Le Pendeven Laurent / Laurent.Le_Pendeven@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

De formation Bac +3/5 en informatique, vous justifiez d'une expérience de cybersécurité acquise au sein d'un SOC ou d'un CERT ou vous avez acquis une expérience d'administration d'outils de sécurité .

Vous souhaitez participer à la création d'une nouvelle structure, vous appréciez le travail en équipe et vous souhaitez contribuer au partage et à l'acquisition de nouvelles compétences rejoignez-nous.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Un CV et une lettre de motivation sont obligatoires.

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.