



Offre n°2024-07619

Administrateur de solutions de sécurité

Niveau de diplôme exigé : Bac + 3 ou équivalent

Fonction : Personnel des fonctions support (IT)

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

Niveau d'expérience souhaité : De 3 à 5 ans

Contexte et atouts du poste

Le Centre des Opérations de Sécurité est composé de deux pôles :

- Un pôle dédié à la détection et la réponse à incident

Ce pôle a en charge la qualification des failles de sécurité pouvant porter atteinte au SI d'Inria, de la détection des failles avérées et de la coordination des actions de sécurisation. Il assure la détection des incidents de sécurité et le pilotage de leur résolution. Il est en charge de la coordination générale des détections et des résolutions, ainsi que du reporting au niveau RSSI et DSI.

- Un pôle dédié à l'administration des solutions de sécurité

Il a en charge l'administration et l'exploitation fonctionnelles des solutions de sécurité (SIEM, Scanner de vulnérabilités, laboratoire forensique, WAF, passerelles anti-spams, CTI, sondes, Firewall, ...), en collaboration étroite avec le Service Production, partageant les mêmes processus, environnements techniques et documentations.

Mission confiée

Vous contribuerez à la mise en place du nouveau pôle dédié à l'administration des solutions de sécurité en collaboration étroite avec les équipes de production.

En tant qu'administrateur de solutions de sécurité, vous aurez en charge l'administration et l'exploitation fonctionnelles des services numériques de sécurité. Vous participerez au bon fonctionnement de ces solutions de sécurité en garantissant leur maintien en conditions opérationnelles et en condition de sécurité.

Sous la responsabilité du responsable de service, vous participerez à la création et à la mise en place de ce nouveau pôle au sein du centre des opérations de sécurité qui vise à réunir des ressources spécialisées en production d'outils de sécurité.

Vous travaillerez en étroite collaboration avec les services owner des solutions et le service de production ainsi qu'avec les services impliqués dans les différents services de sécurité (SP, SA, CDS, SCI).

Principales activités

Au sein du Centre des Opérations de Sécurité et sur le périmètre des services numériques sécurité, vous serez amené à :

- Animer et suivre l'activité du pôle d'administration des solutions de sécurité,
- S'assurer du fonctionnement optimal des solutions de sécurité,
- Contribuer au paramétrage des solutions de sécurité, gérer les changements,
- Mettre en place la collecte des logs et des alertes issues des solutions vers un service de détection d'incidents,
- Rédiger et maintenir de la documentation, des procédures et des modes opératoires des processus d'administration fonctionnelle,
- Participer à la conception, au développement et à la maintenance des outils permettant

d'améliorer le fonctionnement du Centre des Opérations de Sécurité notamment en matière

d'outils de détection et d'investigation,

- Participer aux opérations relatives au traitement des incidents (verrouillage ou contrôle d'accès, archivage de logs, ...)
- Maintenir et faire évoluer les solutions de sécurité,
- 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 remontée des logs et des alertes,
- Animer l'activité d'administration fonctionnelle des services numériques de sécurité,
- Participer à l'élaboration des stratégies de détection des incidents de sécurité (incidents redoutés, scénarios de détection, règles de corrélation, collecte, notification),
- Participer à des projets de sécurisation du SI,
- Assurer une veille technologique permettant de conserver un haut niveau de technicité.

Compétences

Savoirs :

- Maîtrise des processus de production,
- Maîtrise de la sécurité des systèmes d'exploitation et de la sécurité des réseaux,
- Maîtrise de l'administration fonctionnelle d'un ou plusieurs outils de sécurité (WAF, Firewall, Sondes de détection, Antivirus, ...),
- Maîtrise des environnements Linux et/ou Windows,
- Maîtrise d'un langage de scripting (Python, PowerShell, Bash, ..),
- Connaissances des principes d'attaques et d'intrusions,
- Connaissance de l'environnement juridique lié aux contraintes SSI dans un établissement de recherche : PPST, RGS, RGPD, ...,
- Connaissance des processus ITIL.

Savoir-faire :

- Capacité à animer, à organiser et hiérarchiser les priorités,
- Capacité à travailler en équipe et à distance,
- Capacité à configurer des outils liés aux services numériques de sécurité,
- Capacité à écouter et dialoguer avec des experts techniques et des utilisateurs,
- Capacité à élaborer des procédures, consignes et documents techniques,
- Capacité à écouter et dialoguer avec des experts techniques et des utilisateurs,
- Capacité à analyser des journaux d'événements (systèmes, réseaux, applicatifs) et à corréler

les informations de nature différente.

Savoir-être :

- Rigueur et sens de l'organisation et de l'animation,
- Avoir le sens du service à l'utilisateur,
- Avoir le sens du collectif,
- Diplomatie et qualités relationnelles,

- Bonne gestion du stress.

Langues :

- Français : courant,
- Anglais : technique.

Avantages

- 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)

Informations générales

- Ville : Le Chesnay
- Centre Inria : [Siège](#)
- Date de prise de fonction souhaitée : 2024-09-01
- Durée de contrat : 3 ans
- Date limite pour postuler : 2024-05-31

Contacts

- Équipe Inria : DSI-SOC
- Recruteur :
Le Pendeven Laurent / Laurent.Le_Pendeven@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

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.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Un CV et une lettre de motivation sont obligatoires.

Sécurité défense :

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.