



Offre n°2020-02905

Analyste SOC (H/F)

Type de contrat : Mobilité ou CDD

Contrat renouvelable : Oui

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

A propos du centre ou de la direction fonctionnelle

La Direction des systèmes d'information (DSI) coordonne la mise en œuvre de la politique informatique d'Inria. Elle fait partie du siège de l'Institut et est implantée sur tous les sites Inria du territoire national. Elle est en charge de la conception et du développement du Système d'Information, de la mutualisation des services numériques ainsi que de la mise en œuvre de la sécurité informatique ; de l'administration et du maintien en condition opérationnelle des différents services numériques communs à Inria ; du maintien du catalogue de services numériques ; de l'achat et de la maintenance des équipements, logiciels et prestations informatiques.

Elle est composée de huit services :

- le Centre de services (DSI-CDS),
- le Service de production (DSI-SP),
- le Centre d'opérations de sécurité (DSI-SOC),
- le Service des référents SI (DSI-SRSI),
- le Service d'urbanisation et appui aux projets (DSI-SUAP),
- le Service de conception d'infrastructure (DSI-SCI),
- le Service applications (DSI-SA),
- le Service commandes et budgets (DSI-SCB).

Contexte et atouts du poste

Le Centre des opérations de sécurité (SOC) est en charge de 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 la coordination de leur résolution. Le SOC est en charge de la coordination générale des détections et des résolutions, ainsi que du reporting au niveau RSSI. Il assure la rédaction et la maintenance et guides liés à la sécurisation du SI.

Le Centre des opérations de sécurité recherche pour le 1er octobre 2020 son Ingénieur sécurité- Analyste SOC.

Le poste est localisé au sein des Centres Inria de Grenoble, Rocquencourt ou Paris.

Mission confiée

Vous contribuerez à la sécurisation des infrastructures et des services numériques de l'Institut. Vous interviendrez en appui mais aussi en conseils et expertise sur le domaine de la sécurité des systèmes d'information (SSI) auprès des concepteurs et exploitants informatiques et du Responsable de la Sécurité des Systèmes d'Information (RSSI).

Principales activités

Au sein du Centre des Opérations de Sécurité (SOC) vous serez amené à :

- Qualifier des failles de sécurité pouvant porter atteinte au SI Inria,
- Détecter des anomalies avérées et coordonner des actions de sécurisation,
- Détecter des incidents de sécurité et coordonner leur résolution,
- Identifier et opérer les outils de détection utiles au contexte Inria (Splunk, Nessus, SIEM...),
- Auditer les systèmes pour assurer une prévention continue,
- Élaborer des stratégies de détection des incidents de sécurité (incidents redoutés, scénarios de détection, règles de corrélation, collecte, notification...),
- Effectuer le reporting sécurité auprès du RSSI et du DSI,

- Rédiger et maintenir des documents, procédures et des guides liées à la sécurisation du SI,
- Participer à des projets de sécurisation du SI,
- Assurer une veille technologique permettant de conserver un haut niveau de technicité,
- Mener des actions de sensibilisation et de formation.

Compétences

Compétences techniques et opérationnelles :

- Maîtrise des règles d'administration système et réseau,
- Maîtrise des environnements Linux et/ou Windows
- Capacité à analyser des protocoles réseaux,
- Connaissance des outils de monitoring et de détection permettant de tracer les menaces et tentatives d'intrusion,
- Capacité à analyser des journaux d'événements (systèmes, réseaux, applicatifs),
- Connaissance de langages de scripting (Python, Bash, PowerShell, ...),
- Connaissance en architecture des SI et en architecture applicative,
- Capacité à évaluer et analyser une solution en fonction des besoins,
- Connaissance de l'environnement juridique lié aux contraintes SSI dans un établissement de recherche : PPST, RGS, RGPD, ...,
- Capacité à élaborer des procédures, consignes et documents techniques,
- Capacité à écouter et dialoguer avec des experts techniques et des utilisateurs,
- Connaissance des processus ITIL,

Compétences personnelles :

- Avoir le sens du service à l'utilisateur.
- Être capable de travailler en équipe et à distance.
- Avoir le sens du collectif.
- Être rigoureux et autonome.
- Savoir organiser et hiérarchiser les priorités.

Langues :

- Français : courant
- Anglais : technique

Avantages

- Restaurant d'entreprise subventionné
- Congés : 7 semaines de congés annuels + 10 jours de RTT
- Possibilité de télétravail (après 6 mois d'ancienneté) et d'aménagement du temps de travail
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)

Rémunération

Selon profil et expérience

Informations générales

- **Ville** : Rocquencourt, Grenoble, Paris
- **Centre Inria** : [Siège](#)
- **Date de prise de fonction souhaitée** : 2020-09-01
- **Durée de contrat** : 3 ans, 1 mois
- **Date limite pour postuler** : 2020-09-30

Contacts

- **Équipe Inria** : DSI-SOC (DSI)
- **Recruteur** :
Lacouture Noemie / noemie.lacouture@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

Les compétences et qualités suivantes seraient particulièrement appréciées :

- Très bonne connaissance des principes d'attaque et de défense des SI,
- Expériences dans l'administration des systèmes Unix et Windows dans des environnements réseaux Ethernet et TCP/IP et des problématiques de sécurité associées,
- Savoir traiter de sujets sensibles en un temps contraint,
- Réactivité et disponibilité selon le contexte,
- Rigueur et esprit d'analyse, Volonté d'apprentissage et de progression.

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

Ce poste est à pouvoir par voie de mobilité inter-fonction publique ou contractuelle (CDD 3 ans).

Nous vous remercions de candidater en ligne, en joignant votre CV et une lettre de motivation.

Les candidatures seront étudiées à partir du 24 août 2020.

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.