



**Offre n°2025-08867**

## **Apprenti(e) : Ingénieur(e) Cybersécurité – Outillage et automatisation SOC (H/F)**

**Type de contrat :** Apprenticeship contract

**Niveau de diplôme exigé :** Master's or equivalent

**Fonction :** Apprenticeship Support functions

**Niveau d'expérience souhaité :** Recently graduated

### **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 composée de huit services :

- deux services de conception :
  - le Service applications (DSI-SA) ;
  - le Service de conception d'infrastructure (DSI-SCI).
- le Centre de services (DSI-CDS) ;
- le Service des équipements informatiques et du budget (DSI-SEIB) ;
- le Centre d'opérations de sécurité (DSI-SOC) ;
- le Service de production (DSI-SP) ;
- le Service des référents SI (DSI-SRSI) ;
- le Service d'urbanisation et appui aux projets (DSI-SUAP).

Elle est en charge de la conception et du développement du Système d'Information, de l'offre globale 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 de l'ensemble de l'institut.

## 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 incidents

Ce pôle a 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 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.

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

Il a en charge l'administration et l'exploitation fonctionnelle 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 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).

Durant cette alternance, une partie de l'activité sera consacrée à l'administration des solutions de sécurité et l'autre partie sera en lien avec la détection et la réponse à incident afin de mettre en place les outils nécessaires à l'orchestration, l'automatisation et la réponse à incident (SOAR).

## Principales activités

- Participer aux tâches quotidiennes d'exploitation fonctionnelle en opérant les solutions de sécurité (SIEM, passerelles anti-spams, CTI, ... )
- Contribuer à l'automatisation des activités de prévention, de détection et de réponse aux incidents (gestion des non conformités et des vulnérabilités, traitement des phishings, ...) en développant l'outillage du SOC,

- Contribuer au développement de l’outillage d’administration fonctionnelle (traitement des demandes liés aux outils de sécurité telles que des actions de remédiation, d’administration des outils, ... ),
- Mettre en œuvre et maintenir les règles de détection du SIEM en collaboration avec le pôle détection,
- Mener des actions de sécurisation en collaboration avec le pôle détection.

### **Activités complémentaires :**

- Rédiger et maintenir des documents, procédures et des guides liés à la 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 :**

- Connaissances générales dans le domaine de la sécurité des systèmes d’information,
- Connaissances des outils de détection et d’analyse de sécurité (SIEM, Scanners de vulnérabilités, distribution de sécurité ),
- Maîtriser un système d’exploitation et avoir des connaissances de Linux et/ou Windows,
- Connaissance des protocoles réseaux,
- Connaissance d’un langage de scripting (Python, Bash, PowerShell, ...),
- Capacité à rédiger,
- Capacité à écouter et dialoguer avec des experts techniques et des utilisateurs,

### **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.
- Éthique personnelle.

### **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 (après 6 mois d'ancienneté) 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)
- Accès à la formation professionnelle
- 5 jours de révision apprentis

## **Informations générales**

- **Ville :** Paris 13e
- **Centre Inria :** [Siège](#)
- **Date de prise de fonction souhaitée :** 2025-09-01
- **Durée de contrat :** 2 years
- **Date limite pour postuler :** 2025-07-31

## **Contacts**

- **Équipe Inria :** DSI-SOC (DSI)

- **Recruteur :**  
Arunraja Emilie / [emilie.arunraja@inria.fr](mailto:emilie.arunraja@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

- Volonté d'apprentissage et de progression.
- Réactivité et disponibilité.
- Rigueur et esprit d'analyse.
- Avoir mené un ou des projets en informatique.

**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

### 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.