COMPUSEC (H/F)

STRASBOURG (67020)

Le COMPUSEC examine et analyse minutieusement les journaux de sécurité et les données d'événements afin d'identifier les problèmes de sécurité, les modèles et les tendances. Il collabore avec les membres de l'équipe pour élaborer des stratégies visant à améliorer la posture de sécurité sur la base de l'analyse des journaux. Il prépare des rapports d'incidents détaillés, y compris la portée, l'impact et les actions recommandées pour la remédiation et la prévention. Il surveille en permanence les tableaux de bord SIEM et d'autres outils de cybersécurité pour détecter les signes d'activité suspecte, les alertes de sécurité et les anomalies.
En outre, il communique efficacement avec les équipes interfonctionnelles, y compris les services informatiques, les services juridiques et la direction, afin de fournir des informations actualisées sur les incidents de sécurité et leur impact potentiel.
Il contribue aux programmes de sensibilisation et de formation à la cybersécurité destinés aux employés afin de renforcer la conscience de la sécurité et de promouvoir une culture de la sécurité au sein de l'organisation.

A. **Qualifications essentielles** :

1. **Expérience professionnelle** :

- 2 à 5 ans d'expérience dans un SOC (Security Operations Center) en tant que responsable technique principal ou 2 à 5 ans d'expérience dans une entreprise publique/privée en tant qu'enquêteur technique dans le domaine de la sécurité de l'information;
- Connaissance approfondie des outils de cybersécurité;
- Solides compétences en matière d'analyse et de résolution de problèmes, excellentes capacités de communication et de collaboration avec le personnel technique et non technique.

2. **Éducation/formation** :
   Diplôme en informatique ou dans un domaine connexe, de préférence en technologie des réseaux informatiques, compréhension des concepts de pare-feu, de proxis, de SIEM, d'antivirus et d'IDPS.

3. **Habilitation de sécurité** :
   Une habilitation de sécurité est obligatoire. Le Corps Européen effectuera les démarches nécessaires auprès des autorités nationales dont relève le candidat.

4. **Langue** :
   L'anglais est la langue de travail au sein du Corps Européen.

5. **Connaissances standard en matière de traitement automatisé des données (TAD)** :
   Traitement de texte : connaissance pratique - Tableur : connaissance pratique - Présentation graphique : connaissance pratique - Base de données : aucune connaissance

B. **Qualifications souhaitables** :

1. **Professionnelles** :
   Des certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP) ou Certified Incident Handler (GCIH), sont un atout.
2. **Éducation/formation** :
   Expérience avérée acquise par des qualifications d'un niveau professionnel équivalent.

—

The COMPUSEC scrutinizes and analyzes security logs and event data to identify security issues, patterns and trends. He works with team members to develop strategies to improve the security posture based on log analysis. He prepares detailed incident reports, including scope, impact and recommended actions for remediation and prevention. He constantly monitors SIEM dashboards and other cybersecurity tools for signs of suspicious activity, security alerts and anomalies.
In addition, he communicates effectively with cross-functional teams, including IT, legal and management, to provide up-to-date information on security incidents and their potential impact. He/she contributes to cybersecurity awareness and training programs for employees in order to strengthen security awareness and promote a security culture within the organization.

A. **Essential Qualifications** :

1. **Professional/Experience :**

- 2-5 years' experience in a SOC (Security Operations Center) as a senior technical lead OR 2-5 years' experience within a public/private company as a technical information security investigator.
- Extensive knowledge of cybersecurity tools.
- Strong analytical, problem-solving skills, excellent communication and collaboration abilities with both technical and non-technical personnel.

2. **Education/Training** :

Degree/Diploma in computer science or related field, preferably in IT network technology, understanding of firewalls, proxies, SIEM, antivirus, and IDPS concepts.

3. **Security Clearance** :

A security clearance is required. Eurocorps will make the necessary arrangements with the candidate's national authorities.

4. **Language** :

English is the day to day working language in Eurocorps.

5. **Standard Automated Data Processing (ADP) Knowledge** :

Word Processing : Working Knowledge - Spreadsheet : Working Knowledge - Graphics presentation : Working Knowledge - Database : No Knowledge.

B. **Desirable Qualifications** :

1. **Professional** :

Relevant certifications, such as Certified Information Systems Security Professional (CISSP) or Certified Incident Handler (GCIH), are a plus.

2. **Education/Training** :

Proven experience acquired by qualifications with an equivalent professional level.

Type de contrat

CDI tout public

Durée de travail

35h/semaine
Travail en journée

Salaire

Salaire brut : Mensuel de 2 900 € sur 12 mois
Mutuelle
Restauration

Profil souhaité

Expérience

• 2 An(s)	Cette durée minimale d'experience est indispensable

Langues

- Anglais Très Bon Cette langue est indispensable
- Français Très Bon Cette langue est indispensable

Informations complémentaires

- Secteur d'activité : Défense

Répondre à cette offre : humanresources@eurocorps.org