CYBER AWARENESS AND DOCUMENTATION (H/F)

STRASBOURG (67020)

Responsable de la sensibilisation au cyberespace et de la documentation du Corps Européen (CE), il développe et organise le plan de sensibilisation au cyberespace pour le personnel du CE, en organisant différentes conférences et journées de sensibilisation et élabore la documentation du bureau des Systèmes d'Information et de Communication (SIC), conformément aux orientations données. Il doit aider les autres membres du bureau Cyber à créer des lignes directrices en matière de sécurité, un concept et un état de la sécurité de l'information. Il analyse les documents de sécurité, développe et soumet des directives, collabore aux règlements en ce qui concerne les questions de sécurité des SIC et maintient une bibliothèque de publications et d'instructions de sécurité à jour.

A. **Qualifications essentielles** :

1. **Expérience professionnelle** :

   Compétences en matière d'organisation de conférences et d'explications.
   Initier et coordonner des sessions de formation et de sensibilisation à la sécurité de l'information.
   Expérience significative des logiciels d'application utilisateur tels que Windows et MS Office.
   Connaissance des lois, des politiques, des procédures ou de la gouvernance relatives à la cybersécurité des infrastructures critiques et à la protection de la vie privée.
   Connaissance des cybertechnologies actuelles et émergentes.
   Connaissance des principes de cybersécurité et de protection de la vie privée.
   Connaissance des cybermenaces et des vulnérabilités.
   Capacité à exploiter les meilleures pratiques et les enseignements tirés de l'expérience.

2. **Éducation/formation** :
   Master en informatique, Cyber sécurité ou equivalent.

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** :
   Connaissance des procédures et des orientations de l'OTAN.
   Connaissance des différentes classes d'attaques (passives, actives, internes, rapprochées, de distribution).

Connaissance des cyberattaquants (script kiddies, menace interne, attaques non parrainées par un État-nation…).
Connaissance des étapes d'une cyberattaque.
Connaissance des protocoles de réseau.
Expérience et connaissances en matière de sécurité de l'information et de technologies de l'information.
Compétences analytiques et réflexion axée sur les processus.

2. **Éducation/formation** :
Diplôme universitaire de niveau Master en informatique.

—

HQ EC Cyber Awareness and Documentation Manager develops and organizes the cyber awareness plan for the personnel of the HQ, with different conferences and awareness pills, as well as elaborates the memory and documentation, according to the guidance. He should support other members of Cyber Office with the creation of security guidelines, concept and the status of information security. He works in close coordination with the other members of the CIS chain. He analyzes CIS security documents and translates them in EC documents and maintains a library of up-to-date CIS Security publications and instructions.

A. **Essential Qualifications** :

1. **Professional/Experience :**

Conference and explanation skills.
Initiating and coordinating information security awareness and training sessions.
Must have significant experience in user application software such as Windows and MS Office.
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures and privacy.
Knowledge of current and emerging cyber technologies.
Knowledge of cybersecurity and privacy principles.
Knowledge of cyber threats and vulnerabilities.
Ability to leverage best practices and lessons.

2. **Education/Training** :
Master's degree in IT, Cyber Defence, or equivalent.

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** :
   Knowledge about procedures and NATO guidance.
   Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
   Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored…).
   Knowledge of cyber-attack stages.
   Knowledge of network protocols.
   Experience and knowledge in information security and IT.
   Analytical skills and process-oriented thinking.
   Awareness: sense of risks and their magnitude.

2. **Education/Training** :
   Completed university degree in information technology.

Type de contrat
CDI tout public
Durée de travail
35h/semaine
Travail en journée
Salaire
Salaire brut : Selon grille de salaire propre au Corps Européen
Mutuelle
Restauration

Profil souhaité

Formation

- Bac+5 ou équivalents

Langues

• Anglais	Niveau Très Bon	Cette langue est indispensable
• Français	Niveau Très Bon	Cette langue est indispensable

Savoirs-être professionnels

Capacité à travailler en équipe.
Sensibilité : sens des risques et de leur ampleur.

Informations complémentaires

- Secteur d'activité : Défense

Répondre à cette offre : humanresources@eurocorps.org