Conseil de l'Union européenne
Secrétariat général
Direction générale Développement organisationnel et services
Direction Ressources humaines
La directrice

Son Excellence Madame l'Ambassadrice ou Monsieur l'Ambassadeur
Représentant(e) permanent(e) des États membres auprès de
l'Union européenne

(par courriel)

Bruxelles, le 8 novembre 2023

Objet: **Détachement auprès du secrétariat général du Conseil d'un(e) expert(e) national(e) dans le domaine du cyber-renseignement**

Réf.: SNE/09/2023 (GSC.ORG.5.A.S1) - 1 poste (379229)

Madame l'Ambassadrice, Monsieur l'Ambassadeur,

La direction Prévention et sécurité recherche un(e) expert(e) en cyber-renseignement pour apporter un soutien à son équipe Enquêtes de sécurité et contre-espionnage.

La description de poste figure en pièce jointe.

La durée du détachement est de deux ans et peut faire l'objet d'une prorogation pour une durée totale n'excédant pas quatre ans. Veuillez noter qu'en application de l'article 5 de la décision (UE) 2015/1027 du Conseil, ce détachement pourrait, dans des cas exceptionnels, être prorogé pour une durée supplémentaire de deux ans.

L'expert(e) devrait prendre ses fonctions au secrétariat général du Conseil au plus tard le **1er mars 2024**.

Les qualifications et l'expérience requises sont précisées en annexe.

Les conditions du détachement, y compris les indemnités versées par le Conseil, sont fixées dans la décision du Conseil du 23 juin 2015 relative au régime applicable aux experts détachés auprès du secrétariat général du Conseil (décision (UE) 2015/1027 du Conseil, JO L 163 du 30.6.2015, abrogeant la décision 2007/829/CE). Conformément à l'article 2 de cette décision, les expertes et experts nationaux détachés doivent avoir la nationalité d'un État membre de l'UE. Les États membres sont

invités à proposer des candidat(e)s pour ce poste.

Le ou les noms du ou des points de contact nationaux responsables pour chaque candidature devront être indiqués dans les actes de candidature. Les actes de candidature devront être accompagnés d'un curriculum vitæ précisant toutes les fonctions exercées jusqu'à présent et les diplômes ou autres titres obtenus, ainsi que d'une lettre de motivation.

Les réponses à la présente lettre doivent être transmises par courrier électronique, au plus tard **le 30 novembre 2023 à 17 heures HEC**, à l'adresse suivante: sne.recruitment@consilium.europa.eu.

Le service compétent et la direction des ressources humaines examineront conjointement les candidatures reçues, décideront quels candidats et candidates seront retenus dans une première sélection et mèneront les entretiens. L'autorité investie du pouvoir de nomination prendra une décision de nomination sur la base du résultat de la procédure de sélection. Le secrétariat général du Conseil peut également décider d'utiliser la liste d'aptitude pour pourvoir, à l'avenir, d'éventuels postes vacants correspondant au même profil.

Si nécessaire, de plus amples informations peuvent être obtenues auprès du secrétariat général du Conseil en s'adressant à M. Philip Meulenberghs, chef du secteur Enquêtes et évaluation de la menace (tél.: +32 (0)2 281 8034, courriel: philip.meulenberghs@consilium.europa.eu).

Je vous prie de croire, Madame, Monsieur, à l'assurance de ma considération distinguée.

Nathalie Pensaert

Annexes

Annexe 1 – Description du poste

ANNEXE

Expert(e) national(e) détaché(e) (END)

auprès du secrétariat général du Conseil de l'Union européenne

Enquêtes et évaluation de la menace (ORG.5.A.S1) – expert(e) en cyber-renseignement

Réf.: SNE/09/2023 (GSC.ORG.5.A.S1) - 1 poste (379229)

Description du poste

A. Principales tâches et responsabilités

Sous l'autorité du directeur de la direction Prévention et sécurité et de la cheffe de l'unité Stratégie de sécurité et continuité des activités, l'expert(e) travaillera au sein de l'équipe "Enquêtes de sécurité et contre-espionnage" du secteur Enquêtes et évaluation de la menace de cette unité. L'expert(e) aura pour supérieur hiérarchique direct le chef du secteur ORG.5.A.S1 – Enquêtes et évaluation de la menace.

Le secteur exécute l'ensemble des tâches liées à la gestion des menaces et des risques en matière de sécurité: enquêtes de sécurité, renseignement de source ouverte et renseignement tiré des médias sociaux, gestion des risques de sécurité, évaluations de la menace, activités de contre-espionnage, tests de pénétration et activités de sensibilisation.

Le secteur fournit à l'encadrement supérieur une analyse des enquêtes de sécurité, des évaluations des risques et des menaces, des notes de sensibilisation et des conseils en matière de sécurité.

Le candidat ou la candidate sélectionné(e) devra s'acquitter des tâches suivantes:

- L'expert(e) travaillera dans une optique de résultats et fera preuve de pragmatisme et de souplesse. En fonction du dossier, l'expert(e) pourra être amené(e) à travailler pour la cheffe d'unité ou pour le directeur. L'expert(e) disposera d'une grande autonomie, mais devra travailler en étroite coopération et coordination avec les expert(e)s en contre-espionnage du secteur, avec le chef du bureau Enquêtes et l'équipe chargée des enquêtes de sécurité, avec les spécialistes du renseignement de source ouverte (RSO) et de la cybersécurité, ainsi qu'avec l'unité Cybersécurité de la direction Plateformes numériques.
- L'expert(e) contribuera à coordonner l'ensemble des activités liées aux enquêtes sur les incidents et risques de cybersécurité. L'expert(e) sera principalement chargé(e) des enquêtes de cybersécurité et du contre-espionnage.
- L'expert(e) fournira des conseils sur les cybermenaces mais aura, en particulier, un rôle opérationnel consistant à coordonner les cyberenquêtes et à y participer, à répertorier les incidents de cybersécurité ainsi qu'à contribuer aux tests de pénétration et autres tests et aux études en cybersécurité, s'il y a lieu.
- L'expert(e) sera invité(e) à fournir à l'encadrement supérieur des évaluations, des rapports et des avis dans son domaine d'expertise.

B. Qualifications et expérience

Les candidats et candidates devraient:

- avoir achevé un cycle universitaire, sanctionné par un diplôme, ou posséder une expérience professionnelle équivalente;
- avoir une expérience professionnelle d'au moins cinq ans – mais de préférence dix ans – dans le contre-espionnage au sein du service de sécurité d'un État membre, assortie d'une expérience récente d'expert(e) dans le domaine du cyber-renseignement;
- disposer d'une expertise dans le domaine des cyberattaques dirigées par des États, dans l'évaluation des acteurs de la menace et de leurs capacités et motivation, ainsi que dans l'évaluation de l'efficacité des mesures d'atténuation des menaces pour la sécurité contre ces acteurs;
- être en mesure de relier le cyber-renseignement à d'autres formes de renseignement, dont le renseignement d'origine électromagnétique (ROEM) et le renseignement d'origine humaine (ROHUM);
- être capable de traduire des concepts informatiques techniques complexes dans un langage compréhensible pour les collègues non spécialistes, les enquêteurs et enquêtrices et le personnel d'encadrement;
- être en mesure d'évaluer l'impact des cyberattaques et d'en rendre compte par écrit ou oralement;
- être en mesure de traiter et de coopérer avec les services de renseignement des États membres dans le domaine cyber, et d'interagir avec les parties prenantes d'autres services du SGC, y compris l'unité Cybersécurité, la direction Plateformes numériques, l'unité Protection des données et l'unité Sécurité de l'information;
- avoir une expérience de la présentation d'informations en matière de contre-espionnage cyber et de la formulation de conseils et de recommandations destinés à atténuer la menace de cyberespionnage, à sensibiliser à ces questions et à réduire les vulnérabilités;
- avoir une expérience des cyberenquêtes techniques et criminalistiques et être en mesure de mener de telles enquêtes, de donner des instructions compréhensibles aux équipes techniques et de rendre compte des résultats dans des rapports compréhensibles pour les collègues non spécialistes, les enquêteurs et enquêtrices et le personnel d'encadrement;
- avoir une connaissance des activités des institutions européennes ainsi que des structures de renseignement et des services de sécurité européens (la connaissance des politiques de l'UE dans le domaine cyber constituerait un atout);
- avoir une connaissance approfondie d'une langue de l'UE et une connaissance satisfaisante d'une deuxième langue de l'UE. En pratique, dans l'intérêt du service, il est nécessaire de disposer d'une maîtrise approfondie, à l'écrit et à l'oral, de l'anglais et/ou du français. Il est essentiel d'être capable de rédiger des rapports précis et analytiques en anglais ou en français.

C. Conditions et aptitudes requises

- Bonnes capacités rédactionnelles pour l'élaboration d'analyses, de rapports et d'exposés sur les questions liées à la cybersécurité
- Aptitude à exposer des informations à divers publics, y compris des cadres de haut niveau
- Discrétion dans le traitement des informations sensibles et confidentielles
- Solides qualités de jugement dans des situations critiques, et bonnes capacités à mener plusieurs tâches de front
- Faculté d'adaptation, sens de l'organisation et de la fixation des priorités, et esprit d'initiative
- Sens du travail en équipe
- Habilitation de sécurité nationale au niveau TRÈS SECRET UE/EU TOP SECRET. Cette habilitation de sécurité doit être obtenue par les candidat(e)s auprès de leurs autorités nationales compétentes avant leur détachement auprès du secrétariat général du Conseil. Sa validité doit couvrir toute la durée du détachement. À défaut, le secrétariat général du Conseil se réserve le droit de refuser le détachement.

D. Conditions générales

Les candidats et candidates doivent:

- avoir la nationalité de l'un des États membres de l'Union européenne et jouir de tous leurs droits civiques;
- avoir satisfait à toutes les obligations légales qui leur sont applicables en matière de service militaire.

Le secrétariat général du Conseil applique une politique de diversité et d'inclusion.

De plus amples informations sur la nature du poste peuvent être obtenues auprès de M. Philip Meulenberghs, chef du secteur Enquêtes et évaluation de la menace (tél.: +32 (0)2 281 8034, courriel: philip.meulenberghs@consilium.europa.eu).