



Secrétariat général (SG)

Genève, le 2 octobre 2026

Courriel: HRerecruit@itu.int

A l'attention de la Direction générale

Lettre circulaire N° 26/43

Sujet: **AVIS DE VACANCE No. 2416P-2026/SG-ISD/EXTERNE/P4 « Responsable des opérations de cybersécurité »**

Madame, Monsieur,

L'emploi décrit en annexe doit être pourvu au siège de l'UIT.

La description d'emploi correspondante, les aptitudes requises des candidats, ainsi que toutes indications utiles, figurent en annexe à la présente lettre.

Les Administrations sont priées de diffuser les avis de vacance à toutes les sources potentielles de recrutement : universités, instituts, associations d'ingénieurs et le secteur privé selon le cas.

Je serais reconnaissant à votre Administration de bien vouloir inciter les candidats et notamment les candidates qualifié(e)s à soumettre leur candidature pour l'emploi mentionné ci-dessus, au plus tard le 02/12/2026 sur notre site carrière :

[Responsable des opérations de cybersécurité](#)

La Conférence de plénipotentiaires a adopté la Résolution 48 (Rev. Dubaï 2018), décidant que :
« ... lorsque des emplois vacants sont pourvus par recrutement international, lors du choix entre plusieurs candidats ayant les qualifications requises pour l'emploi, la préférence doit être donnée aux candidats des régions du monde qui sont sous-représentées dans les effectifs de l'Union, compte tenu de l'équilibre entre le personnel féminin et le personnel masculin prescrit dans le régime commun des Nations Unies ; ».

Veuillez agréer, Madame, Monsieur, l'assurance de ma haute considération.

Doreen Bogdan-Martin
Secrétaire générale

Annexes : AVIS DE VACANCE No. 2416P-2026/SG-ISD/EXTERNE/P4 « Responsable des opérations de cybersécurité »

Titre du poste: Responsable des opérations de cybersécurité

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

L'UIT - principale institution des Nations Unies pour les technologies de l'information et de la communication - a pour tâche de connecter le monde. A cette fin, elle gère sur le plan international le spectre des fréquences radioélectriques et les orbites de satellites, s'emploie à renforcer l'infrastructure des communications dans les pays en développement et élabore des normes mondiales qui garantissent la parfaite interconnexion de systèmes de communication très divers.

L'UIT applique une politique de tolérance zéro à l'égard de toute forme de harcèlement. L'UIT s'est engagée en faveur de la diversité et de l'intégration au sein de son effectif, et encourage tous les candidats quels que soient leur sexe, leur nationalité, leurs origines religieuses et ethniques, y compris les personnes handicapées, à postuler pour faire partie de l'organisation. La parité des genres est d'une grande importance pour l'UIT.

Responsable des opérations de cybersécurité

Numéro de l'avis de vacance: 2416

Secteur: SG

Département: ISD

Pays du contrat: Suisse

Lieu d'affectation: Genève

Numéro de poste: IS12/P4/328

Grade: P4

Type de contrat: Durée déterminée

Durée du contrat: 2 ans avec possibilité de prolongation

Type de publication: Externe

Date limite de candidature (Minuit heure de Genève) 2 décembre 2026

UNITE ORGANISATIONNELLE

Le Secrétariat général dirige les ressources administratives, humaines et financières et des activités de l'Union, y compris la mise en œuvre des normes administratives relatives aux questions de fonctionnement et la diffusion d'informations sur les questions de télécommunication/TIC à des fins opérationnelles et autres, de formuler des avis juridiques à l'ensemble de l'Union. Le Secrétariat général coordonne la mise en œuvre du Plan stratégique, surveille l'environnement des télécommunications/TIC et recommande, si nécessaire, des mesures concernant les politiques et la stratégie futures de l'Union. Le Secrétariat général assure la coordination et la coopération intersectorielles pour faire progresser l'approche globale de l'UIT (One-ITU) au siège et sur le terrain. Le Secrétariat général fournit un appui logistique et de technologie de l'information aux activités de l'Union, notamment aux conférences et forums mondiaux ; la coordination des travaux de l'Union avec le système des Nations Unies et d'autres organisations internationales ; et l'engagement des États Membres, Membres des Secteurs et les établissements universitaires. Le Secrétariat général gère la gouvernance de l'organisation et la communication stratégique et les relations avec les médias, les différents groupes de parties prenantes ainsi que le grand public.

Au sein du Secrétariat général, le Département des services informatiques (IS) coordonne les services de technologies de l'information de l'UIT et gère les applications ERP et CRM, les services liés aux documents, les systèmes et l'infrastructure informatiques, le service d'assistance aux utilisateurs, les services de gestion de la bibliothèque, des archives et de l'information, la sûreté et la sécurité (physique et logique), en vue de fournir un appui aux fonctionnaires au siège et sur le terrain, ainsi qu'aux délégués assistant aux conférences, aux réunions et aux manifestations partout dans le monde. Il encourage en outre la collaboration, les partenariats et l'échange d'informations dans le domaine des TIC et représente l'UIT dans

les commissions et les réunions inter organisations concernant la gestion des technologies de l'information et de la sécurité.

CONTEXTE ORGANISATIONNEL

Sous la supervision du Chef de l'Unité de la sécurité des TIC et dans les limites des pouvoirs qui lui seront délégués, au sein du Département des services informatiques (ISD), le/la responsable des opérations de cybersécurité est chargé(e) de la gestion opérationnelle pratique de l'infrastructure de cybersécurité, des services de sécurité et des projets relatifs à la sécurité de l'UIT. Le/la titulaire est un(e) responsable particulièrement qualifié(e) sur le plan technique, qui possède des compétences pratiques approfondies dans le domaine des technologies de cybersécurité tout en ayant la capacité de gérer des sous-traitants, des fournisseurs et des prestataires de services de sécurité extérieurs.

Le/la titulaire est responsable du fonctionnement courant de l'infrastructure de sécurité et du Centre des opérations de sécurité 24 heures sur 24 et 7 jours sur 7, qui est géré par l'intermédiaire d'un fournisseur extérieur de services de sécurité gérés (MSSP). Le responsable des opérations de cybersécurité remplit également les fonctions de chef de programme/projet pour les principales initiatives en matière de sécurité, notamment l'achat et la mise en œuvre de nouveaux produits et services de sécurité, la modernisation du centre des opérations de sécurité et l'amélioration de l'architecture de sécurité. Le/la titulaire assure la supervision opérationnelle des risques de sécurité liés aux technologies émergentes, notamment l'intelligence artificielle (IA)/l'apprentissage automatique (ML), les grands modèles de langage (LLM) et les systèmes d'IA agentique, et veille à ce que les opérations de sécurité soient alignées sur la stratégie de transformation numérique de l'UIT et les cadres internationaux de cybersécurité applicables.

TÂCHES ET RESPONSABILITES

1. Gère l'intégralité du cycle de vie des projets complexes relatifs à la cybersécurité et à l'infrastructure de sécurité, des études de faisabilité et de la conception de l'architecture jusqu'à l'achat, la mise en œuvre, les tests et la mise en service des technologies de sécurité, y compris les plates-formes de gestion des informations et des événements de sécurité (SIEM), les systèmes de prévention des intrusions/systèmes de détection des intrusions (IPS/IDS), les pare-feux de prochaine génération (NGFW), les passerelles web sécurisées et les plates-formes de protection aux points d'extrémité/détection aux points d'extrémité et d'intervention aux points d'extrémité (EPP/EDR). Supervise les solutions de sécurité de réseau dans les environnements LAN/WAN, physiques, virtuels, hybrides et multi-nuages, ainsi que dans les locaux, en assurant l'intégration dans les environnements d'exploitation Unix, Windows et Linux au siège de l'UIT, dans les bureaux hors siège, lors des manifestations et lors des conférences. Prépare des documents techniques, des évaluations de la sécurité et des évaluations des offres, et apporte un appui au Chef de la sécurité des TIC concernant l'administration des contrats, y compris les appels d'offres, les accords de niveau de service (SLA), le suivi des performances des fournisseurs et l'établissement de rapports sur le rapport coût-efficacité.
2. Assure la fonction d'interlocuteur principal de l'UIT assurant la liaison avec le fournisseur MSSP extérieur assurant le fonctionnement du centre des opérations de sécurité 24 heures sur 24 et 7 jours sur 7 et la détection des menaces. S'occupe de la validation des accords SLA et gère les travaux visant à remédier aux lacunes en matière de détection. Dirige la définition et l'amélioration des cas d'utilisation SIEM, en garantissant des règles de corrélation en fonction du contexte pour les serveurs d'importance critique, les applications et les utilisateurs. Encadre la modernisation du centre des opérations de sécurité grâce à des chaînes d'automatisation et une couverture de détection étendue, la détection des menaces fondée sur l'IA/ML, l'analyse comportementale, la protection des points d'extrémité de prochaine génération et des identités. Gère le flux de travail des interventions en cas d'incident interne à l'UIT, y compris l'évaluation des incidences, l'escalade, l'endiguement, l'éradication et l'examen après incident, en étroite coordination avec le fournisseur MSSP. Élabore et simule des situations de crise pour tester les manuels d'intervention en cas d'incident, des procédures de rétablissement après une catastrophe et les scénarios de cyberexercices pour garantir la résilience de l'organisation.
3. Assure le bon fonctionnement et la maintenance de l'infrastructure de sécurité et de la sécurité du nuage, tout en encourageant des améliorations efficaces en termes de coûts. Assure la supervision pratique de la pile de sécurité, y compris les systèmes NGFW, IPS/IDS, EPP/EDR, ainsi que les systèmes

de gestion d'identité et d'accès (IAM), de sécurité du courrier électronique, de stockage et de gestion de l'information. Surveille en permanence les événements et résout directement des problèmes complexes dans les réseaux, les systèmes et les applications. Gère la sécurité multi-nuage dans un environnement de logiciel en tant que service (SaaS), d'infrastructure en tant que service (IaaS) et de plate-forme en tant que service (PaaS) en appliquant des contrôles de sécurité particuliers à l'architecture, à la gouvernance et aux fournisseurs. Supervise le cycle de vie des identités, y compris l'authentification sans mot de passe, l'authentification à plusieurs facteurs (MFA), la biométrie et la gestion des accès privilégiés (PAM).

4. Dirige les activités de sensibilisation et de formation à la cybersécurité à l'échelle de l'organisation, tant au siège de l'UIT que dans les bureaux hors siège. Met à jour le contenu pour faire face à l'évolution des menaces, notamment l'ingénierie sociale, l'hameçonnage, les rançongiciels et les attaques utilisant l'IA. Conçoit et exécute des simulations d'hameçonnage, puis analyse les résultats pour cibler les efforts de correction. Coordonne les exercices de simulation et les cyberexercices. Suit l'efficacité au moyen de critères de mesure et de retours d'information et rend compte des résultats à la haute direction.

5. Évalue les risques de sécurité liés aux technologies de rupture. Ces technologies sont notamment les systèmes d'IA/ML, avec l'évaluation de la sécurité des systèmes IA, la protection des données d'entraînement, la sécurité de l'inférence des modèles et la défense contre les attaques par exemples contradictoires. Ce point couvre également la sécurité des modèles (LLM), y compris la prévention des infiltrations de requête, la protection contre les fuites de données, les contrôles d'accès et l'architecture de déploiement sécurisé du LLM. En outre, s'occupe de la sécurité de l'IA agentique en appliquant des stratégies de surveillance et de confinement du comportement pour les agents IA autonomes. Met en place des outils de collaboration, des systèmes de chiffrement avancé et solutions de mobilité. Met en œuvre des contrôles techniques de sécurité pour l'IA et le langage LLM, conseille les unités opérationnelles sur l'intégration sécurisée et supervise des cadres de gouvernance responsables pour l'IA.

6. Supervise l'identification des vulnérabilités, le tri des alertes de sécurité et les programmes d'analyse des menaces, en veillant à la mise en place sans délai de mesures correctives dans les environnements d'entreprise. Met concrètement à profit les renseignements sur les menaces en tenant compte des flux automatisés sur les menaces et des rapports de veille dans les règles de détection, les priorités de correction et les informations communiquées aux parties prenantes. Déploie des capacités de détection des menaces et de réponse automatisée fondées sur l'IA/ML pour réduire les délais de détection et de réponse. Dirige les initiatives d'échange de renseignements sur les menaces avec les partenaires du système des Nations Unies et les équipes nationales d'intervention en cas d'urgence informatique (CERT) concernées. Présente sans délai des rapports destinés à l'adoption de mesures concrètes sur les incidences des menaces au Secrétariat général, aux Bureaux et aux bureaux hors siège.

7. Fournit un appui au Chef de la sécurité des TIC concernant la gestion du programme de gestion des risques de cybersécurité de l'entreprise. Identifie, évalue et planifie les mesures d'atténuation des risques visant le siège, les bureaux hors siège, les manifestations et les conférences. Intégrer les risques liés à l'IA, aux langages LLM et à l'IA agentique dans le registre des risques pour de l'organisation. Suit les plans de traitement des risques et fait remonter les risques émergents à la haute direction.

8. Gère la mise en œuvre technique des politiques, normes et exigences réglementaires en matière de cybersécurité. Met en œuvre les recommandations du Comité consultatif interne pour les questions de gestion (CCIG), du Corps commun d'inspection (CCI), ainsi que du vérificateur extérieur des comptes et des auditeurs internes, et suit les progrès accomplis en ce qui concerne les corrections. Définit des indicateurs fondamentaux de performance (IFP), élabore des tableaux de bord de la conformité et établit des rapports à l'intention du Conseil de l'UIT et de ses Groupes de travail. Gère les contrôles techniques en matière de protection des données, y compris le chiffrement (au repos et en transit), la classification des données, la prévention de la perte de données (DLP) et les politiques de traitement des données propres à l'IA/aux langages LLM. Fait appliquer les principes de sécurité de base dans les cadres de gouvernance des données et de classification des données et fournit un appui au Comité de gouvernance de la cybersécurité.

COMPETENCES ESSENTIELLES

Application des connaissances spécialisées; Aptitude à communiquer efficacement; Formation et échange de connaissances; Engagement à l'égard de l'organisation; Approche axée sur les résultats; et, Esprit d'équipe et collaboration.

COMPETENCES FONCTIONNELLES

Analyse, sûreté de jugement et aptitude à décider
 Souci du client et de la prestation de services
 Ouverture à l'innovation et au changement
 Qualités de chef
 Etablissement de réseaux et de partenariats
 Aptitude à planifier et à organiser
 Gestion efficace

COMPETENCES TECHNIQUES

- Connaissance solide des pare-feux NGFW, des systèmes IPS/IDS, de la segmentation, de la confiance zéro et des règles de corrélation SIEM (Splunk/Sentinel/QRadar). Connaissance des services EDR pour les points d'extrémité, la gestion IAM, l'authentification MFA, la gestion PAM, les modèles de confiance zéro et la sécurité du courrier électronique (DMARC/DKIM/SPF).
- Capacité à diriger les interventions en cas d'incident, les activités d'informatique légale et la gestion des vulnérabilités. Connaissance de la mise en œuvre des renseignements sur les menaces, des accords SLA pour les centres SOC/MSSP, du cadre CSF du NIST et de la norme ISO 27001.
- Solide connaissance de la sécurité multi-nuage (AWS/Azure/GCP), de la sécurité de l'IA/ML (données d'entraînement, inférence de modèle, défense contre les attaques par exemples contradictoires) et des risques liés aux langages LLM (infiltration de requête, fuite de données). Connaissance de la sécurité de l'IA agentique, du chiffrement et de la prévention DLP.
- Aptitude à mener à bien des projets dans le domaine de la cybersécurité (passation de marchés, appels d'offres). Solide connaissance de la gestion de la performance des fournisseurs/SLA/contrats.

QUALIFICATIONS REQUISES

Education:

Diplôme universitaire supérieur en informatique, sécurité de l'information, cybersécurité, systèmes d'information ou dans un domaine connexe OU formation reçue dans un établissement d'enseignement supérieur de réputation établie, sanctionnée par un diplôme de niveau équivalent à un diplôme universitaire supérieur dans l'un des domaines précités. Pour les candidats internes, un titre universitaire de premier cycle dans l'un des domaines précités, associé à dix années d'expérience professionnelle pertinente, peut remplacer le titre universitaire supérieur à des fins de promotion ou de rotation.

Les certifications Certified Information Systems Security Professional (*Professionnel certifié en sécurité des systèmes d'information, CISSP*) et Certified Information Security Manager (*Responsable certifié de la sécurité de l'information, CISM*) constitueraient un avantage.

Les certifications GIAC Certified Incident Handler (*Gestionnaire des incidents certifié GIAC, GCIH*), GIAC Certified Forensic Analyst (*Analyste d'informatique légale certifié GIAC, GCFA*), Certified Ethical Hacker (*Hacker éthique certifié, CEH*), GIAC Security Essentials (*Fondamentaux de la sécurité GIAC, GSEC*) et Certified Information Systems Auditor (*Auditeur certifié des systèmes d'information, CISA*) sont souhaitables.

Les certifications Certified Cloud Security Professional (*Professionnel certifié en sécurité du nuage, CCSP*), Amazon Web Services (AWS) Certified Security Specialty (*Certification spécialisée en sécurité d'Amazon Web Services*), Microsoft Certified: Azure Security Engineer Associate (*Ingénieur associé*

certifié en sécurité Azure de Microsoft) et Google Professional Cloud Security Engineer (*Ingénieur professionnel certifié en sécurité du nuage Google*) sont souhaitables.

Expérience:

Au moins sept années d'expérience à des postes à responsabilité croissante dans le domaine des opérations de cybersécurité et de la gestion de la sécurité, dont au moins trois ans au niveau international. Un doctorat dans un domaine connexe peut être considéré comme équivalent à trois années d'expérience professionnelle.

Expérience des plates-formes SIEM, des systèmes IPS/IDS, des pare-feux NGFW, des points EPP/EDR, de la sécurité des réseaux; supervision du Centre SOC/MSSP avec la gestion des accords SLA.

Expérience des interventions en cas d'incident, des activités d'informatique légale, de la sécurité TIC à grande échelle (rétablissement en cas d'incident, continuité des activités).

Expérience de la sécurité multi-nuages (SaaS/IaaS/PaaS) et évaluations de la sécurité des systèmes d'IA/ML et LLM.

Expérience de la gestion des vulnérabilités, des renseignements sur les menaces et de la fourniture de projets de cybersécurité (achat, mise en œuvre, gestion des fournisseurs).

Langues:

Connaissance de l'une des six langues officielles de l'Union (anglais, arabe, chinois, espagnol, français, russe) au niveau avancé et connaissance d'une deuxième langue officielle au niveau intermédiaire. La connaissance d'une troisième langue officielle serait un avantage. (Selon les dispositions de la Résolution 626 du Conseil, l'assouplissement des conditions requises en matière de connaissances linguistiques peut être autorisé pour les candidats ressortissants de pays en développement: lorsque les candidats de ces pays possèdent une connaissance approfondie de l'une des langues officielles de l'Union, leur candidature pourra être prise en considération.)

DROITS ET PRESTATIONS

Salaire:

Le traitement annuel total se compose d'un traitement annuel net (net d'impôts et avant déduction des contributions à l'assurance maladie et à la Caisse des pensions) en dollars USD et d'une indemnité de poste (indemnité de cherté de la vie). L'indemnité de poste est variable et peut être modifiée sans préavis, conformément aux taux fixés dans le régime commun des Nations Unies pour les traitements et les prestations.

Salaire annuel à partir de **\$ 86,027** + indemnité de poste **\$ 72,004**

Les autres indemnités et prestations sont soumises aux conditions particulières de l'engagement, merci de vous référer à: [Ce que nous offrons](#)

INFORMATION SUR LE PROCESSUS DE RECRUTEMENT

Veuillez noter que tous les candidats doivent remplir une demande en ligne et fournir des informations complètes et exactes. Pour postuler, veuillez visiter le site Web de l'UIT [Carrières](#). L'évaluation des candidats est basée sur les critères de l'avis de vacance et peut inclure des tests et/ou des évaluations, ainsi qu'un entretien basé sur les compétences. L'UIT utilise des technologies de communication telles que la vidéo ou la téléconférence, la correspondance par e-mail, etc. pour l'évaluation des candidats. Veuillez noter que seuls les

candidats sélectionnés seront contactés et que les candidats à l'étape de sélection finale seront soumis à une vérification des références sur la base des informations fournies. Les messages émanant d'adresses email différentes de celles de l'UIT - @itu.int - ne doivent en aucun cas être considérées. L'UIT ne facture aucun frais à aucun moment au cours du processus de recrutement.