



General Secretariat (GS)

Geneva, 2 October 2026

E-mail: HRerecruit@itu.int

To the Director-General

Circular letter No. 26/43

Subject: **VACANCY NOTICE No. 2416P-2026/SG-ISD/EXTERNAL/P4 “Cybersecurity Operations Manager”**

Dear Madam, Dear Sir,

The post described in the Annex is to be filled at ITU Headquarters.

The relevant job description with the qualifications required, as well as all other useful information, is annexed hereto.

Administrations are requested to circulate vacancy notices to all potential sources of recruitment including universities, institutes, associations of engineers and the private sector as the case may be.

I would be grateful if Administrations would invite qualified candidates and especially women candidates to apply for the above position not later than 02/12/2026 on ITU career website:

[Cybersecurity Operations Manager](#)

The Plenipotentiary Conference adopted the Resolution 48 (Rev. Dubai 2018), affirming that: “...when filling vacant posts by international recruitment, in choosing between candidates who meet the qualification requirements for a post, preference shall be given to candidates from regions of the world which are under-represented in the staffing of the Union, taking into account the balance between female and male staff mandated by the United Nations common system;”.

Yours faithfully,

Doreen Bogdan-Martin

Secretary-General

Annexes: **VACANCY NOTICE No. 2416P-2026/SG-ISD/EXTERNAL/P4 “Cybersecurity Operations Manager”**

Job Title: Cybersecurity Operations Manager

INTERNATIONAL TELECOMMUNICATION UNION

ITU is the leading United Nations agency for information and communication technologies, with the mission to connect the world. To achieve this, ITU manages the radio-frequency spectrum and satellite orbits at the international level, works to improve communication infrastructure in the developing world, and establishes global standards that foster seamless interconnection of a vast range of communication systems.

ITU applies a zero-tolerance policy against all forms of harassment. ITU is committed to diversity and inclusion within its workforce, and encourages all candidates, irrespective of gender, nationality, religious and ethnic backgrounds, including persons with disabilities, to apply to become a part of the organization. Achieving gender balance is a high priority for ITU.

Cybersecurity Operations Manager

Vacancy notice no: 2416

Sector: SG

Department: ISD

Country of contract: Switzerland

Duty station: Geneva

Position number: IS12/P4/328

Grade: P4

Type of contract: Fixed-term

Duration of contract: 2 years with possibility of renewal

Recruitment open to: External

Application deadline (Midnight Geneva Time): 02 December 2026

ORGANIZATIONAL UNIT

The General Secretariat directs administrative, human and financial resources and activities of the Union, including the implementation of the provisions of the administrative regulations on operational questions, the dissemination of information on telecommunication/ICT matters for operational and other purposes, and the provision of legal advice to the whole of the Union. The General Secretariat coordinates the implementation of the Strategic Plan, monitors the telecommunication/ICT environment and recommends as needed action relating to the Union's future policies and strategy. The General Secretariat ensures inter-sectoral coordination and cooperation to advance a whole of ITU approach (One-ITU) in headquarters and the field. The General Secretariat provides logistical and information technology support to the Union's activities including conferences and global forums; the coordination of the work of the Union with the United Nations system, and other international organizations; and the engagement of the Member States, Sector Members, and Academia. The General Secretariat manages corporate governance, and strategic communications and relations with the media, different stakeholder groups as well as the general public.

Within the General Secretariat, the Information Services Department (IS) is the focal point for the ITU information technology services, managing ERP, CRM, documents, information systems and infrastructure, service-desk, library, archives and information management services, safety and security (both physical and logical), to support staff both at Headquarters and in the Field, as well as delegates attending conferences, meetings and events world-wide. It also promotes ICT collaboration, partnerships and information-sharing and represents ITU in inter-organization meetings and committees related to information technology and security management.

ORGANIZATIONAL CONTEXT

Under the supervision and delegated authority of the Head of the ICT Security Unit, Information Services Department, the Cybersecurity Operations Manager leads the hands-on operational management of ITU's cybersecurity infrastructure, security services, and security projects. The incumbent is a technically competent manager who combines deep practical expertise in cybersecurity technologies with the ability to manage contractors, vendors, and external security service providers.

The role is accountable for the day-to-day operation of security infrastructure and the 24/7 Security Operations Center (SOC), managed through an external MSSP. The Cybersecurity Operations Manager also serves as Program/Project Manager for major security initiatives including acquisition and implementation of new security products and services, SOC modernization, and security architecture improvements. The incumbent provides operational oversight of emerging technology security risks, including AI/ML, Large Language Models (LLMs), and agentic AI systems—and ensures alignment of security operations with ITU's digital transformation strategy and applicable international cybersecurity frameworks.

DUTIES AND RESPONSIBILITIES

1. Manage the full lifecycle of complex cybersecurity projects and security infrastructure, from feasibility studies and architecture design to procurement, implementation, testing and commissioning of security technologies, including Security Information and Event Management (SIEM) platforms, Intrusion Prevention Systems/Intrusion Detection Systems (IPS/IDS), Next Generation Firewalls (NGFW), Secure Web Gateways and Endpoint Protection/EDR platforms. Oversee network security solutions across LAN/WAN, physical, virtual, on-premises, hybrid and multi-cloud environments, ensuring integration across Unix, Windows and Linux operating environments at ITU Headquarters, Field Offices, events and conferences. Prepare technical documentation, security assessments and bid evaluations, and support the Head of ICT Security with contract administration, including calls for bids, Service Level Agreement (SLA) definition, vendor performance monitoring and cost-effectiveness reporting.
2. Serve as ITU's primary technical interface with the external Managed Security Service Provider (MSSP) operating the 24/7 SOC and threat detection. Lead SLA validation and manage detection gap resolution. Direct SIEM use-case development and tuning, ensuring context-aware correlation rules for mission-critical servers, applications and users. Drive SOC modernization with automation pipelines and extended detection coverage, AI/ML-based threat detection, behavioral analytics, next-generation endpoint and identity protection. Manage ITU's internal incident response workflow (impact assessment, escalation, containment, eradication, post-incident review) in close coordination with the MSSP. Develop and stress-test incident response playbooks, disaster recovery procedures, and cyber-drill scenarios to ensure organizational resilience.
3. Operate and maintain security infrastructure and cloud security while driving cost-effective improvements. Deliver hands-on oversight of security stack: NGFW, IPS/IDS, Endpoint Protection Platform/Endpoint Detection and Response (EPP/EDR), Identity and Access Management (IAM), email security, storage, and information management systems. Continuously monitor events and directly troubleshoot complex incidents across network, systems, and applications. Manage multi-cloud security across Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) by enforcing security architecture, governance, and provider-specific controls. Oversee the identity lifecycle including passwordless authentication, Multi-Factor Authentication (MFA), biometrics, and Privileged Access Management (PAM).
4. Lead organization-wide cybersecurity awareness and training at Headquarters and in Field Offices. Update content for evolving threats, including social engineering, phishing, ransomware, and Artificial Intelligence (AI)-enabled attacks. Design and execute phishing simulations, then analyse results to target remediation efforts. Coordinate tabletops and cyber drills. Track effectiveness via metrics and feedback and report outcomes to senior management.
5. Assess security risks of disruptive technologies. This includes Artificial Intelligence and Machine Learning (AI/ML) systems, covering security evaluation of AI systems, protection of training data, model inference security, and defense against adversarial attacks. This also covers Large Language Model

(LLM) security, including prompt injection prevention, data leakage protection, access controls, and secure LLM deployment architecture. In addition, address agentic AI security through behaviour monitoring and containment strategies for autonomous AI agents. Secure ITU Job Description Form (September 2019) – page 3 of 5 collaboration tools, advanced encryption, and secure mobility solutions. Implement technical security controls for AI and LLM, advise business units on secure integration, and oversee responsible AI governance frameworks.

6. Direct vulnerability identification, security alert triage, and threat analysis programs, ensuring timely remediation across enterprise environments. Operationalize threat intelligence by translating threat feeds and intelligence reports into detection rules, remediation priorities, and stakeholder briefings. Deploy AI/ML-powered threat detection and automated response capabilities to reduce detection and response times. Lead threat intelligence sharing initiatives with UN system partners and relevant national Computer Emergency Response Teams (CERTs). Report threat impacts to the General Secretariat, Bureaux, and Field Offices in a timely and actionable manner.

7. Support the Head of ICT Security in managing the enterprise cybersecurity risk management program. This includes risk identification, assessment, and mitigation planning for Headquarters, Field Offices, Events, and Conferences. Integrate AI, LLM, and agentic AI risks into the organization-wide risk register. Track risk treatment plans and escalate emerging risks to senior management.

8. Manage the technical implementation of cybersecurity policies, standards, and regulatory requirements. Implement recommendations from the Internal Management Advisory Committee (IMAC), the Joint Inspection Unit (JIU), and external/internal auditors, and track remediation progress. Prepare Key Performance Indicators (KPIs), compliance dashboards, and reports for the ITU Council and Council Working Groups. Manage data protection technical controls, including encryption (at rest and in transit), data classification, Data Loss Prevention (DLP), and AI/LLM specific data handling policies. Enforce security baselines under the Data Governance and Data Classification frameworks and support the Cybersecurity Governance Committee.

CORE COMPETENCIES

Applying Expertise; Effective Communication; Learning and Knowledge Sharing; Organizational Commitment; Results-Focused, and; Teamwork and Collaboration.

FUNCTIONAL COMPETENCIES

Analysis, Judgement and Decision Making
Client and Service Orientation
Innovation and Facilitating Change
Leadership
Networking and Building Partnerships
Planning and Organising
Successful Management

TECHNICAL COMPETENCIES

- Strong knowledge of NGFW, IPS/IDS, segmentation, zero-trust, and SIEM correlation rules (Splunk/Sentinel/QRadar). Familiarity with EDR across endpoints, IAM, MFA, PAM, Zero Trust, and email security (DMARC/DKIM/SPF).
- Capacity to lead incident response, forensics, and vulnerability management. Familiarity with threat intelligence operationalization, SOC/MSSP SLAs, NIST CSF, and ISO 27001.
- Strong knowledge of multi-cloud security (AWS/Azure/GCP), AI/ML security (training data, model inference, adversarial defense), and LLM risks (prompt injection, data leakage). Familiarity with agentic AI security, encryption, and DLP.
- Ability to deliver cybersecurity projects (procurement, bids). Strong knowledge of vendor/SLA/contract performance management.

QUALIFICATIONS REQUIRED

Education:

Advanced university degree in Computer Science, Information Security, Cybersecurity, Information Systems or a related field OR education from a reputed college of advanced education with a diploma of equivalent standard to that of an advanced university degree in one of the fields above. For internal candidates, a first university degree in one of the fields above in combination with ten years of qualifying experience may be accepted in lieu of an advanced university degree for promotion or rotation purposes.

Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) are strongly preferred. GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), Certified Ethical Hacker (CEH), GIAC Security Essentials (GSEC), and Certified Information Systems Auditor (CISA), are desired.

Certified Cloud Security Professional (CCSP), Amazon Web Services (AWS) Certified Security – Specialty, Microsoft

Certified: Azure Security Engineer Associate, and Google Professional Cloud Security Engineer, are desired.

Experience:

At least seven years of progressively responsible experience in cybersecurity operations and security management, including at least three at the international level. A Doctorate in a related field can be considered as a substitute for three years of working experience.

Experience in SIEM, IPS/IDS, NGFW, EPP/EDR, network security; SOC/MSSP oversight with SLA management.

Experience in incident response, digital forensics, large-scale ICT security (DR, business continuity).

Experience with multi-cloud security (SaaS/IaaS/PaaS) and security assessments of AI/ML and LLM systems.

Experience in vulnerability management, threat intelligence, and cybersecurity project delivery (procurement, implementation, vendor management).

Languages:

Knowledge of one of the six official languages of the Union (Arabic, Chinese, English, French, Russian, Spanish) at advanced level and knowledge of a second official language at intermediate level. Knowledge of a third official language would be an advantage. (Under the provisions of Resolution No. 626 of the Council, a relaxation of the language requirements may be authorized in the case of candidates from developing countries: when candidates from such countries possess a thorough knowledge of one of the official languages of the Union, their applications may be taken into consideration.)

BENEFITS AND ENTITLEMENTS

Salary:

Total annual salary consists of a net annual salary (net of taxes and before medical insurance and pension fund deductions) in US dollars and a post adjustment (PA) (cost of living allowance). The PA is variable and subject to change without notice in accordance with the rates set within the UN Common System for salaries and allowances.

Annual salary from **\$ 86,027** + post adjustment **\$ 72,004**

Other allowances and benefits subject to specific terms of appointment, please refer to: [What We Offer](#)

INFORMATION ON RECRUITMENT PROCESS

Please note that all candidates must complete an on-line application and provide complete and accurate information. To apply, please visit the ITU [Careers](#) website. The evaluation of candidates is based on the criteria in the vacancy notice, and may include tests and/or assessments, as well as a competency-based interview. ITU uses communication technologies such as video or teleconference, e-mail correspondence, etc. for the assessment and evaluation of candidates. Please note that only selected candidates will be further contacted and candidates in the final selection step will be subject to reference checks based on the information provided. Messages originating from a non ITU e-mail account - @itu.int - should be disregarded. ITU does not charge a fee at any stage of the recruitment process.