IAEA
International Atomic Energy Agency

Job Description for Professional Posts

Reference: MT2025/16

Position and Grade:	Associate IT Security Engineer, P2
Organizational Unit:	Security Systems Unit Infrastructure Services Section Division of Information Technology
Duty Station:	Vienna, Austria
Type/Duration of Appointment:	FT – JPO, 1 year

Organizational Setting

The Division of Information Technology provides support to the IAEA in the field of information and communication technology (ICT), including information systems for technical programmes and management. It is responsible for planning, developing and implementing an ICT strategy, for setting and enforcing common ICT standards throughout the Secretariat and for managing central ICT services. The IAEA's ICT infrastructure comprises hardware and software platforms, and cloud and externally hosted services. The Division has implemented an IT service management model based on ITIL (IT Infrastructure Library) and Prince2 (Projects in a Controlled Environment) best practices.

The Infrastructure Services Section (ISS) is responsible for implementing, maintaining, and administering the ICT systems and services for high availability; designing, implementing, and operating IT security services; and managing the data centre. The platforms include Microsoft Windows servers, Linux servers, Oracle EBS infrastructure, data storage, and transmission networks, serving more than 2500 staff, as well as over 10000 external users around the world. The Section includes three Units: Network and Telecommunications, Enterprise Systems, and Security Systems.

Main Purpose

The purpose of the post is to help the IAEA information and communication technology services define and create repeatable and consistent processes to strengthen IAEA information security posture. Under the supervision of the Security Systems Unit (SSU) Head, the Associate IT Security Engineer acts as the primary IT security events handler and reporter of cyber threats. He/she operates processes related to security operations, such as incident monitoring & response, threats & vulnerabilities management, security research, as well as threat prevention/detection tools administration. He/she will collect and interpret information and events generated by internal security monitoring tools, and external threat intelligence providers. Furthermore he/she will be working with peers and senior security engineers to address information security research, and development and delivery of a comprehensive cyber security program for the IAEA.

Role

The Associate IT Security Engineer is (i) a technical analyst supporting the design and formulation of security measures, procedures and standards on all aspects of cyber threats detection, prevention, and response; (ii) a solution provider, coordinating service delivery; (iii) a team member actively involved in planning, implementing, testing and administration of IT security systems; and (iv) a security incident handler.

Partnerships

Under the supervision of the Security Systems Unit (SSU) Head the Associate IT Security Engineer actively participates in the development and delivery of a comprehensive IT security program. The IT Security Operations Engineer works closely with other members of the Security Systems Unit and resolve problems related to cyber security threats detection, response, and mitigation. The incumbent also interacts with other staff in the division, technical staff from other organisational units, and security vendors for the purpose of continuous improvements and evolution of cyber security operations and organisational security posture.

Functions / Key Results Expected

- Assists in operating several security operations processes and activities related to IT security events; IT security vulnerabilities; threat intelligence; risk assessment; incident management; and the configuration and management of security controls and countermeasures.
- Monitors, recommends and, in consultation with management, implements process improvements for security operations. Provides reports regarding related aspects of IT security operations. Assists in refining alerting and improving threat information escalates the most critical events and impact anomalies Operates and improves all aspects of security event management, threat management, including automation.
- Operates Installation, configuration, and management of security operations tools and systems; the expansion and refinement of collection sources and by creating security operations reports automatically and distributing them to the appropriate audience.
- Performs initial assessment and review of security events and vulnerabilities and generates detailed reports; escalates issues as appropriate.
- Interfaces with security and IT professionals throughout the Department and the Agency to assist on the resolution of complex security issues and incidents and collaborates on the documentation results and lessons learned.
- Coordinate and deliver training and instruction to junior level IT and IT security staff regarding security operations processes and participates in security awareness programs, testing, and training.
- Operates security assessment procedures for systems, system configurations, information assets, and changes related to authentication, authorisation, security baselines, confidentiality, and auditing, analyse the results, and provide reports and guidance to the relevant stakeholders and system owners. Communicate vulnerability and security relevant information to stakeholders and assist with remediation planning.
- Performs other various security operations tasks as assigned.

Competencies and Expertise (do not revise or edit)

Core Competencies		
Competence	**Occupational Role**	**Behavioural Indicator**
Communication	Individual Contributor	Communicates orally and in writing in a clear, concise and impartial manner. Takes time to listen and understand the perspective of others and proposes solutions.
Achieving Results	Individual Contributor	Takes initiative in defining realistic outputs and clarifying roles, responsibilities and expected results in the context of the Department/Division's programme. Evaluates his/her results realistically, drawing conclusions from lessons learned.
Teamwork	Individual Contributor	Actively contributes to achieving team results. Supports team decisions.
Planning and Organizing	Individual Contributor	Plans and organizes his/her own work in support of achieving the team or Section's priorities. Takes into account potential changes and proposes contingency plans.

Functional Competencies		
Competence	**Occupational Role**	**Behavioural Indicator**
Client orientation	Associate	Establishes effective relationships with clients to understand and meet or exceed their needs. Finds ways to ensure client satisfaction.
Commitment to continuous process improvement	Associate	Identifies opportunities for process, system and structural improvement as well as improving current practices, increasing effectiveness and achieving efficiency gains. Actively supports the application of sound quality management standards and process improvement.
Technical/scientific credibility	Associate	Acquires and applies new skills to remain up to date in his/her area of expertise. Reliably applies knowledge of basic technical/scientific methods and concepts.

Expertise	
Expertise	**Description**
Information Technology| IT Security	Expertise in SIEM administration, utilisation of technical of threat intelligence, and collection and analysis of logs to conduct analysis for evidence of malicious activities.
Information Technology| Information Security and Risk Management	Expertise in information security with experience in various aspects of information security and security operations processes, including incident and event management; vulnerability management; and threat intelligence.
Information Technology| Technical Writing	Experience in writing technical investigations reports, creating and delivering threat intelligence briefings, and formulating mid-term threat remediation plans and strategies.

Education, Experience and Language Skills

- University Degree in Computer Science, IT Security or Information Security.
- Minimum of two years of relevant work experience in one of the following areas: operational security monitoring, security incident response, technical threat intelligence, or security research experience.
- Demonstrated experience using Firewalls, Intrusion Detection/Prevention Systems, Proxy Servers, and Log Aggregation Technology to conduct analysis for evidence of network penetrations and data theft.
- Demonstrated experience using intrusion detection, security event management systems, and other applicable security tools.
- Demonstrated ability to drive changes and provide tangible results.
- Excellent oral and written command of English. Knowledge of other official IAEA languages (Arabic, Chinese, French, Russian and Spanish) is an asset.