Job Title: IT Security Engineer IO1053

Requisition ID **5762** - Posted - (France, 13067 St Paul Lez Durance Cedex) - **Business Operations** - **New Posting**

The ITER Organization brings together people from all over the world to be part of a thrilling human adventure in southern France—building the ITER Tokamak. We require the best people in every domain.

We offer challenging full-time assignments in a wide range of areas and encourage applications from candidates with all levels of experience, from recent graduates to experienced professionals. Applications from under-represented ITER Members and from female candidates are strongly encouraged as the ITER Organization supports diversity and gender equality in the workplace.

Our working environment is truly multi-cultural, with 29 different nationalities represented among staff. The ITER Organization Code of Conduct gives guidance in matters of professional ethics to all staff and serves as a reference for the public with regards to the standards of conduct that third parties are entitled to expect when dealing with the ITER Organization.

The south of France is blessed with a very privileged living environment and a mild and sunny climate. The ITER Project is based in Saint Paul-lez-Durance, located between the southern Alps and the Mediterranean Sea—an area offering every conceivable sporting, leisure, and cultural opportunity.

To see why ITER is a great place to work, please look at this video

Application deadline: 03/04/2022
Domain: Corporate
Division: Information Technology
Job Family: Project Support
Job Role: Project Officer
Job Grade: P3
Language requirements: Fluent in English (written & spoken)
Contract duration: Up to 5 years

Purpose

As IT Security Engineer, you will lead security improvement projects that would reinforce four security functions; Predict, Prevent, Detect and Respond to cyber security incidents. Also, you will take an active role in supporting the security operations by investigating and responding to security incidents. Providing the right level of IT security is essential for all the processes & components of the ITER Project. Finally, you will also take part in ensuring the cybersecurity needed by the Project across all its components.

Background:

Attached to the IT Division, the IT security activities aim at protecting the ITER information against cyber threat and offering adequate security controls to enable the ITER Project. By providing always the right level of security, it ensures that information systems remain efficient while providing the security needed for the ITER Project execution. A constant collaboration with the other IT activities, sections and teams allows to design, implement and maintain secure IT systems and business minded policies and procedures.

IT Security is involved in all part of the complex IT ecosystem of the ITER Organization, securing access from thousands of users to hundreds of services running on hundreds of servers and VMs, including a Scientific Data & Computing Center hosting leading edge storage and high performance computing cluster of thousands of cores. IT Security is also ensuring cybersecurity and compliance of I&C systems composing the ITER Machine.

Key Duties, Scope, and Level of Accountability

- Coordinates, initiates and manages IT Security projects to execute the IT Security Roadmap;
- Ensures that the Organization's data and infrastructure are protected by developing and enabling the appropriate security controls;
- Plans, implements, manages, maintains, monitors and proposes upgrades as necessary to IT security measures for the protection of the IO data, systems and networks;
- Participates in the change management process;
- Interacts, reports and communicates with the relevant ITER Organization units to support them, guide them and acts as a troubleshooter to analyze and solve cyber security incidents;
- May be requested to be part of any of the project/construction teams and to perform other duties in support of the project;
- May be required to work outside ITER Organization reference working hours, including nights, week-ends and public holidays.

Measure of Effectiveness

- Implements protective measures to prevent any major cyber security incident;
- Provides IT Security services within the defined timeline and expected quality;
- Manages IT Security projects successfully within the defined cost, schedule and quality;
- Handles cybersecurity incidents to completion;
- Drafts and/or reviews IT Security documentation within expected quality (procedures updates, security assessments, etc.).

Experience & Profile

- ***Professional Experience:***
  - At least 5 years of experience in managing IT Security primarily with a defensive objective.
- ***Education:***
  - Master degree in Computer Science, IT, Systems Engineering or relevant discipline;
  - Relevant cyber security certification is considered as an advantage (CISSP, CISM, CEH…);
  - Ability to obtain and maintain French Security clearance;
  - The required education degree may be substituted by extensive professional experience involving similar work responsibilities and/or additional training certificates in relevant domains.
- ***Language requirements:***
  - Fluent in English (written and spoken).
- ***Technical competencies and demonstrated experience in:***
  - Managing IT security by planning assessments, performance reporting, updating policies and security measures, performing business impact analysis, risk

assessment and an overall business continuity strategy ensuring recovery capabilities;
    - Project Management: Planning, measuring progress of project work, managing risks/costs and reporting on progress;
    - Writing Skills: Ability to write structured documents in a clear, concise and accurate manner;
    - Cybersecurity awareness, trends and hacking techniques. Regulations for critical infrastructures;
    - Working with a variety of technologies; capability to address and troubleshoot security problems.
    - Using Windows security solutions, Firewalls (functionality and maintenance), endpoint security;
    - Managing a SIEM solution (preferably ELK) and security tools (Sysmon, TheHive, MISP,…);
    - AD Security, PIM, PAW and other security mechanisms of Microsoft/Azure environment;
    - IT security specifics for I&C/SCADA environment would be preferable.
- ***Behavioral competencies:***
    - Ability to work in a team, under pressure in a fast-paced environment.
    - Strong attention to detail with an analytical mind and excellent problem-solving skills.
    - Good understanding of the human factor of IT Security.
    - Collaborate: Ability to facilitate dialogue with a wide variety of contributors and stakeholders;
    - Communicate Effectively: Ability to adjust communication content and style to deliver messages to work effectively in a multi-cultural environment; Ability to convince by building support for ideas and initiatives through the effective presentation of facts and evidence;
    - Drive results: Ability to persist in the face of challenges to meet deadlines with high standards;
    - Manage Complexity: Ability to analyze multiple and diverse sources of information to understand problems accurately before moving to proposals;
    - Instill trust: IT Security is a critical function that requires high standards of team mindset, trust, excellence, loyalty and integrity.

The following important information shall apply to all jobs at ITER Organization:

- Maintains a strong commitment to the implementation and perpetuation of the ITER Safety Program, ITER Values (Trust; Loyalty; Integrity; Excellence; Team mind set; Diversity and Inclusiveness) and Code of Conduct;
- ITER Core technical competencies of 1) Nuclear Safety, environment, radioprotection and pressured equipment 2) Occupational Health, safety & security 3) Quality assurance processes. Knowledge of these competencies may be acquired through on-board training at basic understanding level for all ITER staff members;
- Implements the technical control of the Protection Important Activities, as well as their propagation to the entire supply chain;

- May be requested to work on beryllium-containing components. In this case, you will be required to follow the established ITER Beryllium Management Program for working safely with beryllium. Training and support will be provided by the ITER Organization;
- May be requested to be part of any of the project/construction teams and to perform other duties in support of the project;
- Informs the IO Director-General, Domain Head, or Department/Office Head of any important and urgent issues that cannot be handled by line management and that may jeopardize the achievement of the Project’s objectives.