



The recruitment policy of the WTO is to seek to attract and retain staff members offering the highest standards of competence, efficiency and integrity. As an Equal Opportunities Employer, the WTO gives full regard to merit and diversity.

---

**Vacancy Notice No.:** EXT/F/16-88

**Issued on:** 20 December 2016

**Title:** IT Security Analyst

**Application Deadline (CET):** 31 January 2017

**Grade:** 8

**Division:** Information Technology Solutions (446)

**Contract Type:** Fixed-term

**Starting Salary:** CHF 112,441 net per annum (approximate)

**Duration:** Two years with the possibility of extension

**Other Conditions:** In accordance with WTO Staff Regulations and Staff Rules and WTO Pension Plan Regulations.

The World Trade Organization offers an attractive compensation package including an annual net salary (subject to mandatory deductions for pension contributions and health insurance), dependency benefits, pension plan, health insurance scheme, separation grant, and 30 days annual leave. Benefits for internationally recruited staff may include travel and removal expenses on appointment and separation, installation grant, education grant, rental subsidy, and home leave.

Additional information on the compensation package is provided on the WTO website:

[https://www.wto.org/english/thewto\\_e/vacane\\_e/comp\\_package\\_e.pdf](https://www.wto.org/english/thewto_e/vacane_e/comp_package_e.pdf).

**The Secretariat of the WTO is seeking to fill a position of IT Security Analyst in the Information Technology Solutions Division.**

#### **General Functions**

Reporting to the IT Security Officer, the IT Security Analyst will undertake the following responsibilities:

1. Perform information security risk assessments and assist in internal audit for security issues.
2. Define procedures for the security management, the security requirements of operating systems, network components and applications, the access control principles.
3. Coordinate and perform the technical implementation of the policies as well as installation and maintenance of the necessary security controls.
4. Participate in planning for, detection of, and response to information security-related events or incidents.
5. Identify security alerts, analyse their relevancy to the Organization's infrastructure, inform and co-ordinate timely mitigation measures. Advise the Organization with current information about information security technologies.
6. Fully participate in the new developments and evolution of the ICT systems to ensure that the security components are adequately tested and implemented.
7. Monitor compliance with information security policies and procedures.

8. Participate in planning, implementation and testing of appropriate disaster recovery and business continuity measures and procedures.

## **REQUIRED QUALIFICATIONS**

### **Education:**

An advanced university degree with specialization in Security or Networking, or basic university degree in Computer Science, Mathematics, Physics, Engineering or related field combined with work experience equivalent to an advanced university degree.

### **Knowledge and Skills:**

Excellent knowledge of enterprise LAN / WAN technologies, TCP/IP protocol stack, including routing, firewalling, and VPN concepts.

Close familiarity with common infrastructure services and applications protocols (DNS, DHCP, HTTP, SMTP, FTP, etc.).

In-depth knowledge of Windows and Linux operating systems -- management, architecture, networking environments, security models and controls.

Thorough knowledge of common authentication and authorisation mechanisms, encryption, digital certificates.

Thorough understanding of modern Web technologies, security challenges of Web applications.

Understanding of database design and programming concepts, ability to write and understand SQL.

Familiarity with information security audit, penetration test, forensics, and monitoring toolset (e.g. nmap, Nessus, Metasploit, Pangolin, Nikto, Snort, pentest web proxies, etc.).

Fluent system programming skills; excellent command of at least one general-purpose or shell scripting language (e.g. Perl, bash, posh, Python, etc.)

Basic reverse engineering skills.

Knowledge of information security standards, best practices and governance is desirable.

Experience of integration of heterogeneous systems following common protocols (e.g. SNMP, SMTP, LDAP, Syslog, etc.) is desirable.

Ability to approach problems in an analytical and systematic way.

Fast learner.

Ability to work under stress.

Ability to work autonomously.

The following interpersonal capabilities are required: present technical facts to knowledgeable specialised audiences; persuade others to a point of view using facts; face and cope with conflict situations with colleagues; work as a member of a team, relating to others, while working independently to achieve his/her objectives; relate to and build relationships with colleagues; and communicate information in a clear way and understand information.

### **Work Experience:**

At least 5 years of relevant professional experience.

### **Languages:**

A very good command of English is required. Knowledge of French or Spanish would be an asset.

**Additional Information:**

IN ORDER TO BE CONSIDERED, APPLICANT MUST PASS A PRELIMINARY TECHNICAL TEST. PLEASE FIND BELOW INSTRUCTIONS ON THE TEST:

Input data for the technical test is available at <https://www.wto.org/library/icons/vn-infosec-pre.zip>

The archive contains two files:

1. crypt.bin -- encrypted data
2. o-hsucrpt-e -- executable used for encryption (Linux x86-64 architecture)

The task is to decrypt the data by reverse-engineering the executable. Clear-text data must be submitted when submitting the application through the E-Recruitment website [Applicants will be asked to provide the answer as part of the on-line application process].

ANY APPLICATION WHICH DOES NOT CONTAIN THE DECRYPTED DATA WILL NOT BE CONSIDERED.

The position may be offered at a lower grade if the selected candidate does not fully meet all the required qualifications.

Only applications from nationals of WTO Members will be accepted.

The WTO may use various communication technologies such as video or teleconference for the assessment and evaluation of candidates. The recruitment process may also involve the use of various forms of testing, assessment centres, interviews and reference checks.

Candidates not selected whose performance in the selection process nevertheless shows them to be suitable for a similar position may be kept on a roster for up to 18 months, and may subsequently be called upon as and when the need arises for additional resources.

---

APPLICANTS MAY BE REQUIRED TO SIT A WRITTEN EXAMINATION

---

APPLICANTS WILL BE CONTACTED DIRECTLY IF SELECTED FOR AN INTERVIEW

---

Please note that all candidates must complete an online application form. To apply, please visit the WTO's E-Recruitment website at: <https://erecruitment.wto.org>. The system provides instructions for online application procedures.

All applicants are encouraged to apply online as soon as possible after the vacancy has been posted and well before the closing date – Central European Time (CET) – stated in the vacancy announcement.

PLEASE NOTE THAT APPLICATIONS RECEIVED AFTER THE CLOSING DATE WILL NOT BE ACCEPTED

**The WTO is a non-smoking environment.**