EUROPEAN DEFENCE AGENCY
(E D A)

Vacancy notice EDA/2018/C028b
(Agency's Contractual Staff)

Post:	IT Security Administrator
Type of post :	Contractual Agent
Function group :	IV
Management of staff:	N.A.
Location:	Brussels
Indicative starting date:	
Level of Security Clearance:	SECRET UE/EU SECRET

Closing date for applications	14 March 2018

The selection of candidates will follow the EDA Staff Recruitment Procedure. Candidates must apply for this post via the EDA website http://www.eda.europa.eu - vacancies. Please note that to make an EDA on-line application you will need to create your EDA profile using a valid e-mail address and a password.

1. BACKGROUND

The European Defence Agency was established on 12 July 2004, and is governed by Council Decision (CFSP) 2015/1835 defining the statute, seat and operational rules of the European Defence Agency.

The Agency has its headquarters in Brussels.

The main task of the EDA is to support the Council and the Member States in their effort to improve the Union's defence capabilities in the field of crisis management and to sustain the Common Security and Defence Policy (CSDP) as it currently stands and as it develops in the future.

The Agency is structured into four directorates. Three operational directorates: Cooperation Planning & Support; Capability, Armaments & Technology; and European Synergies & Innovation and the Corporate Services Directorate.

2. THE AGENCY'S WAY OF WORKING

The Agency is an "outward-facing" organisation, constantly interacting with its shareholders, the participating Member States, as well as with a wide range of stakeholders. It works in an integrated way, with multi-disciplinary teams representing all the Agency's functional areas, to realise its objectives. Its business processes are flexible and oriented towards achieving results. Staff at all levels need to demonstrate the corresponding qualities of commitment, flexibility, innovation, and team-working; to work effectively with shareholders and stakeholder groups, formal and informal; and to operate without the need for detailed direction.

3. THE CORPORATE SERVICES DIRECTORATE

The Corporate Services Directorate manages the human resources, finance, legal, procurement and contract activities, as well as information technology, infrastructure and security, and corporate projects to ensure the smooth and efficient functioning of EDA.

4. DUTIES

Under the direction of the Head of the IT Unit, the IT Security Administrator will contribute to ensuring the necessary support of the Communications and Information Systems of the Agency.

In particular s/he will perform the following tasks within the IT Unit:

- provide and administer servers in a Microsoft Windows based environment (Active directory, Exchange, SharePoint, IIS, SQL) and cloud-based environment (Azure, AWS)
- administer network devices (switches, routers) and border protection devices (firewalls, intrusion prevention systems);
- administer Security Information and Event Management (SIEM) system;
- design and implement IT security and auditing policies;
- perform IT security monitoring and incident management;
- support of end-users in the use of the internal IT tools;

- design, manage and supervise networks and telecommunications;
- initiate, design, implement, monitor, audit and maintain IT security, risk and compliance technologies;
- document, evaluate existing solutions and propose risk mitigation solutions to enhance security and reduce risk exposure;
- execute security vulnerability testing;
- lead detailed technical evaluations of projects with respect to security;
- support and maintain EDA's Business Continuity & Disaster Recovery infrastructure;
- support and maintain EDA's systems for processing of EU classified information up to Secret EU;
- take on additional tasks as required in the interest of the service.

Duties may evolve according to development of the EDA's structure and activities, and the decisions of EDA management.

5. QUALIFICATIONS AND EXPERIENCE REQUIRED

a. Conditions for eligibility

- be a national of a Member State participating in the Agency;
- be entitled to his/her full rights as a citizen;
- have completed any obligations imposed on him/her by the laws concerning military service;
- produces the appropriate character references as to his/her suitability for the performance of his/her duties;
- be physically fit to perform his/her duties;
- have a thorough knowledge of one of the languages of the participating Member States and a satisfactory knowledge of another language of the participating Member States to the extent necessary for the performance of his/her duties;
- have no personal interest (financial, family relationship, or other) which could be in conflict with disinterested discharge of his/her duties within the Agency;
- hold, or be in a position to obtain, a valid Personnel Security Clearance Certificate (national or EU PSC at SECRET UE/EU SECRET level). Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSC, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself. Note that the necessary procedure for obtaining a PSCC can be initiated on request of the employer only, and not by the individual candidate;
- have a level of education which corresponds to completed university studies of at least three years attested by a diploma or be a graduate of a national or international Defence College.

b. Essential selection criteria

(1) Professional

The candidate will be required to demonstrate that he/she has:

- 5 years of professional experience acquired in positions related to the profile of the post;
- experience in administering servers primarily in a Microsoft Windows based environment;
- very strong network administration knowledge;
- excellent knowledge in implementing IT security and audits policies;
- experience in IT security monitoring and incident management;
- a very good knowledge of written and spoken English.

The candidate will preferably also have administration knowledge of the following:

- Microsoft Active Directory;
- Azure Active Directory;
- Microsoft Exchange 2010/2013;
- Office 365;
- Microsoft SharePoint 2010/2013
- Microsoft SQL 2005/2008/2008R2 server;
- Microsoft Hyper-V and Cluster environments;
- Microsoft IIS 7.5;
- in-depth knowledge and experience with firewalls and other border protection devices.

(2) Personal

All staff must be able to fit into the Agency's way of working (see para. 2). Other attributes important for this post include:

- the ability to work in a team and independently in his/her area of responsibility;
- a 'can-do' attitude;
- the ability to take decisions under pressure;
- the ability to focus on service and results, always with strong motivation;
- flexibility and innovation;
- genuine commitment to the Agency's objectives.

c. Desirable

- experience from cloud-based environments;
- knowledge of security policies and guides on handling EU classified information or equivalent high security environments;
- excellent skills in drafting IT documentation;
- experience in deploying and managing two-factor authentication systems;

- experience in administering Splunk for operational and security analysis of logs or other SIEM systems;
- experience in administering Microsoft Forefront Identity Manager or other Identity Management solutions;
- IT Security Certifications such as CISSP;
- already holding a valid security clearance certificate (minimum EU SECRET), from his/her national security authority.

6. INDEPENDENCE AND DECLARATION OF INTEREST

The IT Security Administrator will be required to make a declaration of commitment to act independently in the Agency's interest and to make a declaration in relation to interests that might be considered prejudicial to his/her independence.

7. APPOINTMENT AND CONDITIONS OF EMPLOYMENT

The IT Security Administrator will be appointed by the Chief Executive.

Recruitment will be as a member of the contractual staff of the Agency for a four-year period (unless a shorter period is mutually agreed between the parties). Renewal is possible within the limits set out in the EDA Staff Regulations. The successful candidate will be recruited as group IV .

The pay for this position consists of a basic salary of 3.404,15 € supplemented with various allowances, including as applicable expatriation or family allowances. The successful candidate will be graded on entry into service according to the length of his/her professional experience. Salaries are exempted from national tax, instead an Agency tax at source is paid. For further information on working conditions please refer to:
https://www.eda.europa.eu/jobs/WorkingatEDA

Failure to obtain the requisite security clearance certificate before the expiration of the probationary period may be cause for termination of the contract.

Candidates are advised that part of the recruitment process includes medical analyses and physical check-up with an Agency's Medical Adviser.

Applications are invited with a view to establishing a reserve list for the post of IT Security Administrator at the EDA. This list is valid until 31/12/2019, and may be extended by decision of the Chief Executive. During the validity of the reserve list, successful candidates may be offered a post in the EDA according to their competences in relation to the specific requirements of the vacant post.

Inclusion on the reserve list does not imply any entitlement of employment in the Agency.

8. EQUAL OPPORTUNITIES

The EDA is an equal opportunities employer and accepts applications without distinction on the grounds of age, race, political, philosophical or religious conviction, sex or sexual orientation and regardless of disabilities, marital status or family situation.

9. APPLICATION PROCEDURE

Candidates must submit their application electronically solely via the EDA website. Applications by any other means (hard copy or ordinary e-mail) will not be accepted. Applications must be submitted no later than midnight. Candidates are reminded that the on-line application system will not accept applications after midnight (Brussels time, GMT+1) on the date of the deadline.

When applying, candidates from Ministries of Defence or other governmental entities are encouraged to inform their national administration.

A selection committee will be appointed. Please note that the selection committee's internal proceedings are strictly confidential and that any contact with its members is forbidden.

If recruited, you will be requested to supply documentary evidence in support of the statements that you make for this application. Do not send any supporting or supplementary information until you have been asked to do so by the Agency.

Please note that once you have created your EDA profile, any correspondence regarding your application must be sent or received via your EDA profile.

For any prior enquiry, please refer to the FAQ (Frequently asked questions) section, or send an e-mail to recruitment@eda.europa.eu.

10. DATA PROTECTION

Please note that EDA will not return applications to candidates. The personal information EDA requests from candidates will be processed in line with Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The purpose of processing personal data which candidates submit is to manage applications in view of possible pre-selection and recruitment at EDA.
More information on personal data protection in relation to selection and recruitment can be found on the EDA website: http://www.eda.europa.eu/jobs/dataprotection