EUROPEAN SPACE AGENCY

SAGA Security Engineer

Job Req ID: 13941
Closing Date: 16 December 2021
Publication: Internal & External
Vacancy Type: Permanent
Date Posted: 17 November 2021
Vacancy in the Directorate of Telecommunications and Integrated Applications.

ESA is an equal opportunity employer, committed to achieving diversity within the workforce and creating an inclusive working environment. We therefore welcome applications from all qualified candidates irrespective of gender, sexual orientation, ethnicity, beliefs, age, disability or other characteristics. Applications from women are encouraged.

This is a non-renewable post for a limited duration of 4 years and is classified A2-A4 on the Coordinated Organisations' salary scale.

Location

ESTEC, Noordwijk, Netherlands

Description

SAGA Security Engineer reporting to the 4S Strategic Programme Line Manager in the Telecom Technologies, Products and Systems Department, Directorate of Telecommunications and Integrated Applications. You will report hierarchically to the 4S Strategic Programme Line Manager and functionally support the SAGA Implementation Manager.
You will be responsible for the end-to-end system security architecture-related activities to support the SAGA project, this being a component of the ESA ARTES Secure Satcom for Safety and Security (4S) programme, and to support the EC EuroQCI initiative. This is a dual-role position, combining Cyber Security Analyst and System Security Engineer.

Duties

You will be the technical authority to enable the team(s) to deliver a system that is resilient to growing cyber equipment threats, now and in the future, for this complex emerging technology area. The role covers all areas of information security, cyber, and information assurance, across land, sea, air, and space environments.

You will be responsible for integrating security in the development of SAGA and will work closely with the EuroQCI team. You will also help the software development teams to threat model, vulnerability scan and penetration test the early software, system and architecture, while identifying the required control points in the application stack.
You will work closely with developers to diagnose, document and remediate security vulnerabilities, in addition to being responsible for evaluating, recommending and implementing security-related software. Furthermore, you must be comfortable leading and training developers in secure best practices.
You will be managing the delivery of security requirements and associated tasks through all phases of the acquisition lifecycle. You will also be required to develop and manage the security case at project level, and to identify and manage the security risks, protecting assets through-life, ensuring that capability remains operational.
You will need to fulfil a number of roles:

- The Cyber Security Analyst role is to help protect our customer networks from cyber security threats such as hackers, cyber terrorists and malware that can steal or corrupt sensitive customer data.

- The System Security Engineer role is to design the capability for monitoring, maintaining and configuring SAGA networks and security devices, such as switches, routers, firewalls, virtual private networks (VPNs), and HSMs. Together with the Saga Systems Engineer, you will develop the system architectures, requirements and sub-system specifications, working primarily on delivering a cryptographic key distribution solution targeting user needs.

Duties Continued
Your main tasks and responsibilities will cover:

- Being responsible for security end-to-end system architecture, security operations, key management and cryptography;
- Being responsible for security engineering for hardware elements (TEMPEST, KMS hardware, KMFs, HSMs, RNGs, data processing) for space and ground segments;
- Being responsible for software engineering for software related to key generation and management and other security-critical elements;
- Being the Technical Interface for key / key-material exchange between SAGA and EuroQCI;
- Being the focal point for designing, supporting, and maintaining SAGA cyber-security processes and procedures;
- Providing the focus for building and maintaining asset maintenance cyber security policy, which includes support within SAGA remote systems, as well as customer systems and networks;
- Providing a technical interface with the client (Member States and EC) and industrial developers;
- Being responsible for design authority oversight of system upgrades, design changes and maintenance;
- Building and maintaining reference systems for the support system upgrades and patches;
- Collaborating with other teams to improve systems security and monitoring;
- Acting as the technical authority within the team on cyber and security, applying standard security techniques and architectures to mitigate security risks;
- Understanding the operational environment of the equipment and the cyber security risks that this presents, identifying threats, vulnerabilities and mitigations;
- Leading the development of security artefacts, including the security management plan, security cases and security case reports;
- Providing advice on the residual cyber security risk associated with user experimentation, entry into service, and through life, to customers and users, supporting the development of any resulting risk balance cases as a technical authority;
- Leading the development of new processes and strategies, where required, to enable TIA and the SAGA team to make the most of emerging technology, and understanding the changing threat environment;
- Assessing industry-delivered equipment and design artefacts, while continually exploring emerging technologies and innovation, in line with customer and capability requirements;
- Creating trial security instructions and coordinating project security working groups;
- Developing and providing assurance on security policy, contract requirements and other contract artefacts to ensure equipment is secure by design;
- Supervising and mentoring the more junior team members;
- Recommending security measures and software to protect systems and information infrastructure, including firewalls and data encryption programs to protect the SAGA system;
- Documenting and researching security breaches and assessing the damage they cause. Working with customer security teams to perform tests and uncover network and system vulnerabilities;
- Helping remediate detected vulnerabilities to maintain a high-security standard in line with organisation- wide best practices for IT security;

- Researching security enhancements and making recommendations to management;
- You will be working in a cross-functional team which spans the departments of the Directorate and is supported by technical experts from within the matrix structure. You will also be interfacing closely with the various project teams, as well as the related industrial teams.

Technical competencies
Multi-disciplinary knowledge of area of responsibility
Knowledge of industrial costs and schedule aspects, space system development and PA standards
Complex project risk management processes
Knowledge of ESA and industrial development, verification and procurement processes

Behavioural competencies
Result Orientation
Operational Efficiency
Fostering Cooperation
Relationship Management
Continuous Improvement
Forward Thinking

Education
A Master's degree in a scientific or engineering discipline is required.

Additional requirements
Your experience and qualifications should include:

- Development, systems engineering and integration of complex heterogenous systems and sub-systems, including software;
- System architecture and requirement decomposition;
- Requirement validation (SMART);
- Development of subsystem specifications to meet system requirements;
- Integration activities from component level up to systems level, including hardware and software elements;
- Competence in problem-solving and analytical techniques in a methodical and logical manner to solve integration challenges;
- Development of appropriate integration plans and procedures;
- Supporting Test Readiness Reviews / integration events;
- Integration and formal verification testing;
- Producing technical progress reports and test/trial reports;
- *SO Standards - ISO27001 (Implementer experience).

Engineering experience in complex space programmes (preferably in telecommunications) and up to launch and in-orbit testing is desirable.

Direct experience of working with the EC or a commercial telecommunications company and operator will be a distinct advantage.

Please be advised that due to the nature of security, these roles are reserved for ESA Member State nationals only.

You must be eligible to obtain security clearance from national authorities.

Other information
For behavioural competencies expected from ESA staff in general, please refer to the ESA Competency Framework.
The working languages of the Agency are English and French. A good knowledge of one of these is required. Knowledge of another Member State language would be an asset.
The Agency may require applicants to undergo selection tests.

At the Agency we value diversity and we welcome people with disabilities. Whenever possible, we seek to accommodate individuals with disabilities by providing the necessary support at the workplace. The Human Resources Department can also provide assistance during the recruitment process. If you would like to discuss this further please contact us at contact.human.resources@esa.int.

Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada, Latvia, Lithuania and Slovenia.

According to the ESA Convention, the recruitment of staff must take into account an adequate distribution of posts among nationals of the ESA Member States*. When short-listing for an interview, priority will first be given to internal candidates and secondly to external candidates from under-represented or balanced Member States*. (https://esamultimedia.esa.int/docs/careers/NationalityTargets.pdf)
In view of the limited duration of this post, internal candidates are strongly advised to contact their HR advisor before applying.

In accordance with the European Space Agency's security procedures and as part of the selection process, successful candidates will be required to undergo basic screening before appointment.

Recruitment will normally be at the first grade in the band (A2); however, if the candidate selected has little or no experience, the position may be filled at A1 level.
*Member States, Associate Members or Cooperating States.