JOB OFFER

Created in 2009, **ESSP** is a young and dynamic company, a **pan European service provider**, certified by EASA (the European Union Aviation Safety Agency) to deliver safety-critical services. Our mission is to operate and provide **Communication, Navigation and Surveillance** (CNS) services, among which, the main one is, the **EGNOS service** (the European Geostationary Navigation Overlay Service), on behalf of the EUSPA (the European Agency for Space).

ESSP Corporate Video: *https://www.youtube.com/watch?v=ZkszX-ptzAY*
ESSP Website career: *https://www.essp-sas.eu/human-resources/careers/*

In ESSP we are looking for a:

SITE SECURITY EVOLUTION ENGINEER - (F/M)

We are looking for a Site Security Evolution Engineer who will be in charge of physical security for EGNOS sites located in Europe (and beyond) in order to ensure security maintenance as per regulatory and operationnal requirements. In complement, she/he contributes to the Security Evolution Team's activities on security impact analyses, the definition of security architecture or governance policy.

For these activities, we are looking for someone with at least **5 years' experience in** security ideally in sensitive sites security domain, with a **very good level of English** (minimum B2).

Your main responsibilities/activities will be:

The Site Security Evolution Engineer is responsible for:

- Ensure the implementation and adherence to the security policy of the installations of subsystems deployed on sites and to the requirements for operational sites related to standards (particularly ISO 27001) or changes in the legal or regulatory framework (Ministries, EASA, or other),
- Contribute to security monitoring of country/geopolitical risks and participate to the implementation of security measures adjusted according to evolving risks,
- Assess the specific constraints of the sites in collaboration with the Site Engineers,
- Lead the Site Engineers on all aspects related to security,
- Contribute to the validation of the level of site's compliance with security requirements,
- Monitor the implementation of security requirements on the sites carried out by Site Engineers,
- Provide support to Site Engineers in preparing or carrying out site controls, particularly those with high critical security conditions or requirements.
- In coordination with the Security Operations team, capitalize on site audit reports, anomalies, incidents, and quarterly site security management reports delivered by the Site Engineers,
- In coordination with the Security Operations team, contribute to root cause analysis of security anomalies/incidents, validation of action plans, and participation in the closure of anomalies/incidents.

As security specialist:

- Design and optimize security architectures with a focus on risk mitigation, ensuring alignment with business objectives and compliance requirements,
- Lead security risk analyses (e.g. qualitative/quantitative risk assessments, threat modeling) to identify, prioritize, and mitigate risks,
- Develop and maintain expertise in security governance, including the development of risk-informed policies, standards, and controls,

- Support compliance initiatives by conducting risk-based assessments and ensuring adherence to internal policies and external regulations (e.g., ISMS, ISO 27001, NIST, GDPR),
- Conduct security control assessments and gap analyses, incorporating risk findings into remediation plans,
- Support third-party risk assessments, including supplier risk assessments and contract reviews,
- Advise and train on risk treatment strategies (e.g., acceptance, mitigation, transfer) and communicate recommendations to stakeholders.

As a Security Team member:

- Actively contribute to the company risk management by identifying and escalating security risks in projects and operations,
- Proactively participate in change management by assessing the security risks associated with new technologies, systems, or processes,
- Effectively support incident response by providing risk context and architectural insights during investigations.

PROFILE:

Generic Skills:

- Autonomy, practicality, rigor, and precision
- Discretion
- Communication and negotiation skills
- Ability to take responsibility and defend one's point of view
- Strong teamwork skills
- Very good level of English (B2-C1) – CEFR
- Proficiency in MS Office (Word, Excel, PowerPoint, Project, Visio)

Specific Skills:

- Ability to identify cybersecurity needs
- Good knowledge of physical security solutions
- Knowledge of French and European regulations relating to classified information (II901, IGI 1300, IGI 2102, etc.)
- Practical knowledge of the ISO 27000 series
- Basic understanding of audit practices
- Basic understanding of risk analysis

Knowledge of the following areas would be an asset:

- GNSS and associated security
- Common Criteria (ISO/IEC 15408)
- Knowledge of space-based communication technologies and LAN/WAN technologies
- Security frameworks and standards
- Risk management methodologies

JOB SPECIFICATIONS:

Available for punctual travels mainly in Europe and at international level
Experience in projects in an international context (European)
Subject occasionally to on-call duty 24 hours a day, in accordance with the ESSP system in place.

HUMAN RESOURCES

Recruitment process:

- **1st interview** is held by the direct manager of the position you applied for (technical interview)
- **2nd interview** is held by HR Unit

Remuneration package:

- **Variables**: bonuses based on objectives
- Profit-sharing
- **Teleworking**: up to 2 days/week
- **Tickets Restaurant (card)**
- **Family Health Insurance**
- **Sustainable Mobility Package**: Home/Office travels reimbursement if car shring or bicycling
- Reimbursement of **75% of public transport** subscription

Please send your application file only by e-mail to the following address: **recrut@essp-sas.eu**

Job Location: Toulouse (France)

Type of Contract: Full time / Permanent

ESSP is committed to cultural diversity, gender equality and the employment of disabled workers.