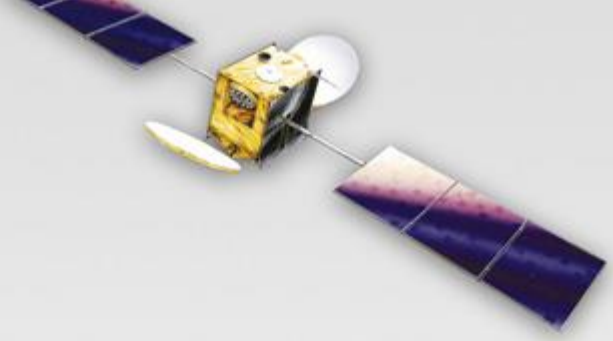


JOB OFFER

ESSP, a private company with 7 major European Air Navigation Service Providers as shareholders, manages the operation and supports the adoption of the European Satellite Based Augmentation System to GPS: EGNOS.

ESSP Corporate Video: https://www.youtube.com/watch?v=ojO8TAitQoc

The adoption of this service is rapidly growing given it allows correcting the GPS signal and offers enhanced features with accurate positioning and integrity within safety-of-life services context such as public transportation.

ESSP Website: https://www.essp-sas.eu/careers/

ESSP recruits a:

CYBERSECURITY ENGINEER - (F/M)

Being part of the Security Team and reporting directly to the Chief Security Officer, the Cybersecurity Engineer will be in charge of activities related to the Security Department missions, to the benefit of ESSP or its Customers.

Those activities range from the design, the qualification, the implementation and the operation of security solutions to security expertise provided to Projects, IT and Operational Teams or to our Customers.

The Cybersecurity Engineer will do security risk analyses and proposes security measures for mitigating risks; he/she will also able to deliver security studies requiring its unique technological or methodological expertise.

The Cybersecurity Engineer is responsible for:

Security solutions

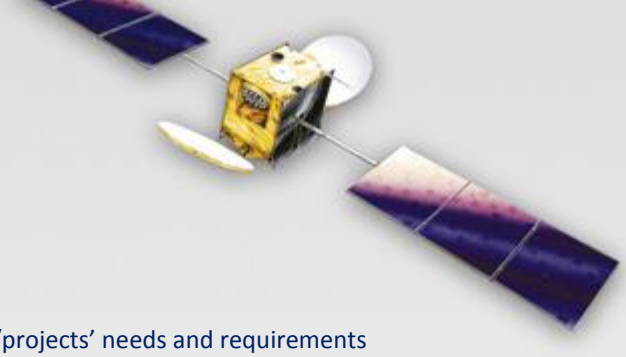
- Management of security projects
- Design of security architectures and solutions
- Security risk analyses
- Test and qualification of security solutions and systems
- Support to IT & Operations (incidents, evolutions, recommendations, …)

Cybersecurity expertise

- Security watch (technologies, threats, …)
- Security audits (scans, pentests, configurations, hardening, etc.)
- Security assessments (equipment, OS, application, source code, etc.)
- Promotion of best practises (operational security, system development, security monitoring, etc.)
- Security monitoring (SIEM, Event Correlation, Alerting, …)

Security governance and control

- Security requirements analysis
- Definition of security policies, processes and operational procedures (SecOPS)
- Security directives and guidance documentation



PROFILE

Generic Skills:

- Be able to :
  - Understand, analyse and reformulate users/customers/projects' needs and requirements
  - Define and write technical documentation; have editorial capabilities
  - Act as consultant and facilitate the decision making process
  - Evaluate the impacts of technologies and solutions on information systems and operations
- Have pedagogical capabilities
- Have good communication skills; able to lead technical meetings
- Rigorous, pragmatic and discrete
- Curiosity and ability to self-learning
- Autonomous with good capability for team work
- Good English Level (B1-B2) - CECRL
- Good knowledge of MS Office (Word, Excel, PowerPoint, Project and Visio)

Specific Skills:

- Good knowledge of information systems and IT technologies
- Good knowledge of:
  - System security (Linux, Windows, VM, system hardening, …)
  - Network security (firewalls, IPS/IDS, VPN, proxy/reverse proxy, WAF, antimalware, …)
  - Authentication (AD, LDAP, Kerberos, Radius, smartcards, PKI, ...)
  - Communication and data security (encryption, IPSEC, etc.)
- Knowledge of cybersecurity tools (SIEM, Nessus, Kali, …)

The knowledge of one or more of the following domains would be considered an advantage:

- Knowledge of security risk assessment methodologies (ISO 27005, EBIOS, …)
- Some experience of scripting (PowerShell, Shell, Python, VBS, …) or dev (VB.NET, C#, …)
- Knowledge of GNSS and CNS technologies
- Practical knowledge of ISO2700x series
- European regulation applicable to Information System Security and to GNSS in particular
- Communication technologies for radio and space segments

Job Requirements:

Available for travels in Europe

Access to this position may require a Personal Security Clearance (PSC) at "EU-Confidential" level

Engineer, Master or equivalent degree

A first professional experience (and/or traineeship in cybersecurity) is desirable.

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.