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 :

SECURITY EVOLUTIONS TEAM MANAGER - (F/M)

As part of the creation of a new position, we are looking for a **Security Evolution Team Manager** who will be in charge of **security evolutions activities in support of ESSP activities and services provided to ESSP clients.** For these activities, we are looking for someone with at least **5 years' experience in** operational IT security or SOC operation or Cyber Crisis operations and critical and/or complex technical systems in the space, aviation or industry sectors. A team management experience and a **very good level of English** (minimum B2) are also needed.

Your main responsibilities/activities will be:

As a Team Manager:

- Lead and organize the Security Evolutions Team, ensuring the delivery of high-quality security architecture, governance, compliance, and risk analysis solutions.
- Oversee the development and implementation of security architectures and frameworks, integrating risk analysis as a core component of decision-making.
- Identify and planify training needs to maintain the team's expertise in security risk assessment methodologies, governance, and compliance.
- Ensure team deliverables quality (e.g., risk assessments, architectures, compliance reports) align with regulatory requirements and organizational objectives.
- Collaborate closely with SOC, IT, operational and business units to embed risk-aware security practices into projects and operations.

As a Security Specialist:

- Design and optimize security architectures with a focus on risk mitigation, ensuring alignment with business goals and compliance requirements.
- Lead security risk analysis (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 adherence to internal policies and external regulations (for instance : PSSI, ISO 27001, NIST, GDPR)
- Perform security control assessments and gap analyses, integrating risk findings into remediation plans.
- Support third-party risk evaluations, including vendor risk assessments and contract reviews.
- Advise and train on risk treatment strategies (e.g., acceptance, mitigation, transfer) and communicate recommendations to stakeholders.

As a Member of the Security Team:

- Actively contribute to enterprise risk management by identifying and escalating security risks in projects and operations.
- Proactively participate in change management, assessing 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:

- Team management ability and ability to effectively organize transversal activities
- Initiative capabilities and proactivity
- Leadership and influence in change management
- Strong analytical and problem-solving abilities
- Excellent communication abilities (written and verbal)
- Stakeholder management and collaboration
- Project and time management
- Critical thinking and decision-making
- Adaptability in evolving security landscapes

Specific Skills:

- Security Risk Analysis: Expertise in qualitative/quantitative risk assessments, threat modeling, and risk treatment strategies
- Security Architecture: Design and review of secure architectures for systems, networks, and applications
- Security Governance: Development and enforcement of security policies, standards, and frameworks
- Compliance Management: Ensuring adherence to regulatory requirements (e.g., ISO 27001, NIST, GDPR)
- Third-Party Risk Management: Vendor risk assessments and contract reviews
- Threat Modeling: Identifying and mitigating potential threats in systems and processes
- Security Controls: Designing and implementing technical and organizational controls
- Incident Response Support: Providing risk context and architectural insights during incidents

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

- Cloud security architectures (AWS, Azure, GCP)
- Zero Trust and least-privilege principles
- Security frameworks and standards
- Risk management methodologies
- Secure software development lifecycle (SDLC) and DevSecOps
- Identity and Access Management (IAM) and Privileged Access Management (PAM)
- Data protection and privacy regulations
- Industry-specific compliance requirements
- Scripting and automation for security assessments
- Relevant certifications (e.g., CISSP, CISM, CRISC, CISA)

JOB SPECIFICATIONS:

Available for punctual travels mainly in Europe

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.