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=u_FKtcaN8YE*
ESSP Website career: *https://www.essp-sas.eu/human-resources/careers/*

In ESSP we are looking for an:

NETWORK SECURITY ENGINEER - (F/M)

We are looking for a **Network Security Engineer** who will be in charge of Network security related assets and functions, who will provide technical expertise to ESSP Teams.

For these activities, we are looking for someone with at least **3 years' experience in IT Security**, with a very **good level of English** (minimum B2).

Your main responsibilities/activities will be:

The technical expertise related to the security subsystems and function of the Network:

- Analysing events related to the Network security functions or subsystems. In case of suspicion of security event, the security team is alerted,
- Ensure the level 2 of maintenance, raise and analyse the "Observations Reports" for the security subsystems,
- Support the production of operational procedures to maintain and operate the security subsystems,
- Ensure the deployment of the new version of the security subsystems,

Interfacing with the Security team for all topics related to Network security:

- Analyse/Manage vulnerabilities detected by the Security team. Interact with Security team and the network service provider to define and implement a remediation plan to tackle critical vulnerabilities,
- Ensure the security requirements deployment for the internal activities of the Network team as well as in the operational and maintenance baselines,
- Analyse and deploy the Product Security Requirements for the applicable tools,
- Analyse and provide the data that will feed the SIEM and the asset management tool (tools managed by Security team). The data provisioning can be done through a dedicated tool. You will be in charge of the maintenance and the evolutions of the data provisioning tool in line with Security and Network requirements,
- Support Security for the audit (internal and external), the penetration test (prepare the test platform) and the risk analysis.

The maintenance of the tools used by the network team (as back-up):

- Ensure the administration tasks of the Network monitoring processing chain: configuration updates, configuration management, user management, incidents investigation…,
- Ensure the administration tasks of the remote sites monitoring processing chain: configuration updates, configuration management, user management, incidents investigation…,
- Inventory and document the tools used by the Network team for technical investigation and monitoring,
- Ensure the interface with ESSP team in order to maintain the test platform network and to manage hardware and software configurations,
- Execute some of the functional tests on the test platform (ex: reproduction of network problems…).

The evolution of the existing tools and the development of new ones (as backup):

- Ensure the evolutions of existing tools, such as the real-time data processing, the integration of new releases,
- In coordination with Product Assurance requirements, ensure the qualification of those evolutions and new tools: design document updates, production of test procedures and test reports, scheduling and animation of key-points,
- Update the test environment network for different needs: evolutions of the ground segment, specific technical investigation, requests coming from the Security team,

PROFILE:

- Good knowledge of cyphering and authentication methods
- Good knowledge of security equipment/methods: IDS, IPS, Firewall, SIEM, IPSec, PKI
- Good knowledge of ELK (Elastic Logstach, Kibana)
- Software development: Python 3, shell script
- Time Series Database: InfluxDB
- Data visualisation: Grafana
- Configuration management tool: GitLab
- General knowledge of each layer of the OSI model (Open Systems Interconnection)
- General knowledge in network security (IP/port filtering, firewall ASA, Diode, IDS, IPS, SIEM)
- Good knowledge of the following protocols: Ethernet, IP, TCP, UDP, SNMP, FTP SFTP, SSH
- Knowledge of Switch/Routers/Firewalls Cisco CLI environment (Command Line Interface)
- Network tools: Wireshark, TShark, HP OpenView
- Rigour
- Strong autonomy
- Initiative and synthesis spirit
- Capability to assume responsibilities
- Team player spirit
- Skills in Microsoft software suites (MSOffice, MSProject, etc.)

JOB REQUIREMENTS:

Engineering degree in Telecom Engineering, Cybersecurity or equivalent
Available for punctual travels mainly in Europe
Subject to constraints of minimum presence during normal vacation periods (July/August, Christmas, February, Easter).
Subject to on-call duty

Human Resources information:

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

Element of package of remuneration:

- **Variable**: 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 sharing or bicycling
- **Reimbursement of 75% of public transport**

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.