



Gradiant

#JOBS

rrhh@gradiant.org

In Gradiant we have a great work environment. We highly motivated in each of the projects that we develop. Gradiant is young, as the people who work with us. We face every day as a new challenge, with freshness, friendship and humor, enjoying a flexible schedule, adapted to the needs and motivations of each person. We are an essential tool for companies to generate profits through innovation, research and products designed “*a la carte*” for each customer or partner. In Gradiant we help companies to gain momentum by making them more competitive and profitable in the markets.

SECURITY TECHNICAL LEAD (STL) (OF0115)

The Security Technical Lead (STL) is a strategic position within Gradiant. The STL is expected to be experienced in security applications and tools (both from the industry and academic state of the art) and must be able to articulately consult with clients on these matters. The STL will be working with a project team on client facing engagements, as well as helping decide on Gradiant’s strategy with respect to security technologies (what projects to undertake, what technologies to develop,...). Typically on the larger projects the STL will work alongside a Project Manager that leads the engineering team implementing the projects, and that assists the STL in defining and validating the developed solution. On smaller engagements, it is possible that the STL takes on a hybrid role and directly leads the engineers besides designing the project. The STL must therefore be comfortable in taking on a technical lead role, as well as having management and strategic skills (or aspire to this) to steer the security-related activities at Gradiant

TECHNICAL LEAD KEY DIFFERENTIATORS:

- Technical skillset: Understanding of security and privacy properties, cryptographic algorithms (properties and uses), security protocols and implementations
- Project Management: Requirements, Planning, coordination and customer communication.
- Research & Innovation: Ability to integrate state of the art technologies into practical industrial developments. Ability to discern when the academic state of the art in security is ready to be transferred to industry, and ability to evaluate the effort needed for this task.
- Ability to absorb complex technical concepts and communicate them to a non-technical audience.

MINIMUM QUALIFICATIONS:

- Bachelor’s Degree in Computer Science or a relevant degree
- Knowledge of cryptography and cryptographic protocols
- Understanding across security domains, understanding the inter-relationships between major components.

PREFERRED QUALIFICATIONS:

- Experience with one or more standard security libraries.
- Experience in designing end-to-end secure solutions.
- Specialized education on security and privacy, or experience working in a security-related domain
- Strong connections to university groups, research centers and/or companies working on security and privacy
- Experience in privacy technologies, cloud security, mobile security, or embedded security.
- Experience working with non-technical clients.

RESPONSIBILITIES:

- Act as a technical point of contact for the customer and partner groups.
- Define Gradiant strategy in Security and Privacy (research lines, technology development, partnership strategy, etc.).
- Define Gradiant best practices in terms of Security and privacy
- Gather and document technical requirements and propose solutions based on client’s architectural needs (define architecture and high-level solution design).
- Develop and lead a small team of security-oriented engineers
- Work with Gradiant’s engineering areas and business development team to include security & privacy in project/business proposals.
- Own security&privacy aspects of project planning and execution.
- Interact with prospective customers during product demos/evaluations.
- Follow both the industrial and academic state of the art in security and privacy technologies

SEND YOUR CV (stating “OF0115” on the “object” field) TO RRHH@GRADIANT.ORG