SECURITY ARCHITECT

Location	Amsterdam or Cambridge
Reports to	Senior Manager: Security Products and Services
Hours	Full time
Contract	This is a permanent role. If the role is offered in our Netherlands (Amsterdam) or our UK office (Cambridge), it will be offered as a 1-year definite contract with the possibility of an indefinite contract thereafter

Purpose and Context

Reporting to the Manager of the Security Products and Services portfolio , this role is a member of the CITO team.

GEANT delivers products and services to the European National Research and Education Networks (NRENs). Amongst these services are a growing number of security services such as DDOS protection, threat analysis, training and awareness and cryptographic services. Apart from delivering security products and services, the Security Products and Services team also assists the GÉANT CISO, GÉANT internal IT and the GÉANT SOC with security expert advice.

This role requires the design, development and implementation of technical infrastructure and security systems/tools for GÉANT and partner NRENs. Responsibilities include technical design and implementation of tools, processes and systems used to provide security services, as well as providing information security advisory and consulting services. Currently the portfolio focuses on network based protection services like DDoS, Cyber Threat Intelligence and DNS based protection services.

Role Accountabilities

- Design, develop, engineer, implement and/or manage cybersecurity tools and systems/infrastructure;

- Direct the information security knowledge base for maintaining a current knowledge of the security technologies, threats, vulnerabilities concepts and controls, including appropriate countermeasures, and advising on security best practices and recommendations;

- Produce security architecture, design documentation, best practice recommendations, secure system configurations and other documents for GÉANT and NRENs;

- Perform threat intelligence and technology watch activities; Participate in security experts groups within the R&E community and the wider security arena;

- Develop and maintain the GÉANT security roadmap which guides security developments for GÉANT and the NRENs for the next 5 years;

- Contribute and provide expert input towards the development of security processes/workflows; Contribute towards the development, adoption of, and ensure compliance with security policies and processes;

- Build and work in international teams in EU-funded projects;

- Develop, procure and/or customise required security tools and technologies;

- Present the development of new security systems, tools and/or processes at appropriate forums (e.g. committees, working groups, external stakeholders); Network with key stakeholders and partners.

- Other duties as may reasonably be required

Working Arrangements

We are adopting a flexible-hybrid model which means that employees will work flexibly between a remote and office environment. Weekly visits to the office are required for most employees to support our values and collaborative culture and enable our teams to deliver great work. These arrangements will be role dependent and must be agreed with your line manager. For this role we anticipate that you will be required in the office at least 2 days per week. This requirement may change, and you may be required to attend the office on more days per week from time to time or on an on-going basis if the needs of the business change.

Business Travel

Regular business travel will be required in this role (5 to 8 trips per year). Travel will mainly be within Europe, but some worldwide travel may be required, typically each travel will be 2 to 5 days.

Experience, Knowledge and Skills

Essential

- Extensive ICT experience (networks, architecture and/or development) including experience within information security (preferably security management and security architecture)

- Extensive experience devising Security Roadmaps and underlying security architecture for products and services

- Expert knowledge of security concepts and technologies for networking, high performance computing and collaboration with a broad basis of ICT knowledge

- Expert knowledge of (security) architecture principles

- Deep understanding of the principles around product and service lifecycles.

- Knowledge of open-source tools and of operating systems

- Skills in at least two of the following areas:

  o (network) Security threat detection and analysis technologies

  o Cyber threat intelligence, threat analysis

  o Detection sensors and analysis of sensor data (e.g. honeypots, intrusion detection / prevention systems, netflow, traffic/protocol analysis);

  o Security architecture principles

  o Securing High Speed networks

- Degree, or a comparable level of experience, in IT, information systems, computer science, cyber security, security architecture, engineering or related field

"Nice to Have" Skills and Experience

- Previous general ICT experience in a service delivery environment
- Experience with DDOS detection and mitigation
- Experience with relevant standards (e.g. ISO 27001) and frameworks (e.g. NIST)
- Experience in Research and Education environment