Training opportunity for graduates/young professionals from Switzerland

Reference	Title	Duty Station
CH-2020-HIF-IHS	**Cyber Security**	**ESTEC**

Overview of the unit's mission:

Within ESA's IT Department, the IT Security Section is responsible for Security related projects, services and operations. The team implements security projects delivering new cybersecurity capabilities, operates security systems and applications and offers security engineering and consultancy services to ESA. The Section also runs the IT Department's Information Systems Management System (ISMS) which is based on ISO27001. The Section hosts ESACERT, ESA's Computer Emergency Response Team which is responsible for security monitoring, incident handling and response. ESACERT also participates in security awareness campaigns and user communication through info-flashes, guidelines and articles.

Overview of the field of activity proposed:

Risk-based Vulnerability Management:

In order to cope with the ever-increasing Cyber Threats, the IT Department is looking to optimise, automate and speed-up its current vulnerability management processes and tools. The goal is to switch from ad-hoc and manual to frequent and automated vulnerability scanning and to combine discovered vulnerabilities with risk, in order to correctly prioritize corrective actions.

The activity encompasses assessing, testing and piloting a highly automated risk-based vulnerability management solution for systems connected to ESA's corporate networks across all of ESA's sites and establishments.

As trainee, you will be tasked to implement an initial proof of concept, validate it and enhance it together with other members of the team, before gradually adding new features and capabilities.

Some intended capabilities of the solution are:

- automated discovery of systems and services connected to ESA networks
- automated and regular vulnerability scanning
- automated and continuous collection of configuration, information of systems and networks
- real-time visibility on ESA's attack surface wrt. its infrastructure assets, their configuration and vulnerabilities
- context-aware vulnerability assessments based on multiple sources (scanners, asset configuration, …) and proposed actions to improve
- optimised and prioritised patch management and mitigation actions based on risk-level and exposure
- generation of objective risk scores that can be used for risk prioritization, risk trending, Cyber Security strategy amendments, audits etc.
- cyber-attack simulations in order to understand the impact and derive improvements to be made
- security policy compliance and recommendations based on configuration changes, exposure and related risks
- use of multiple global Threat Intelligence sources to support all of the above

You will have the opportunity and need to work in close collaboration with ESACERT, other members of the IT Security Section and the Security and Shared Infrastructure Services Division, and ESA-wide Service and System managers. you will therefore have the opportunity to validate your work in a very challenging and interesting operational environment.

You are encouraged to visit the ESA website: www.esa.int/esa

Required education:

- Master-level degree in a technical or scientific discipline;
- Passion for IT/Cyber Security;
- Good interpersonal and communication skills;
- Ability to work in a multicultural environment, autonomously and as part of a team;
- Fluency in English and/or French, the working languages of the agency.