Cyber Security and Threat Engineer

We are a leading worldwide provider of navigation devices and wearable technology, with a focus on developing, designing and supporting superior products. As an engineering and technology company, we have a keen focus on recruiting talent in the fields that support Garmin business and products.

Our benefits are designed to lead an evolving marketplace, support innovation and encourage a healthy balance between work and life. They allow our associates to make their own decisions about their wellbeing and future and consistently rank Garmin as a top tier benefits provider when compared to other high-tech employers.

Your role would be to contribute collaboratively and professionally in a team environment to secure the local IT network.

In this role, you will be responsible of:

- Performing penetration and security assessment testing
- Conducting advanced security audits
- Using IT security, networking and web technologies to circumvent security controls
- Making use of methods of threat modeling and vulnerability assessment including vulnerability scanners, password crackers, network protocol attacks etc.
- Ensuring that all security requirements are met or exceeded
- Designing and developing solutions to enhance performance of security systems
- Researching and measuring feasibility of new offensive security technologies or various approaches in order to make recommendations and suggest solutions
- Communicate with business stake holders to align on risk assessment and/or vulnerability remediation plan

We are looking for a new colleague with the following skills and knowledge:

- Experience in the usage of Metasploit or similar penetration tools
- Proficient with Nmap, Linux, Web Vulnerabilities identification and exploitation, OWASP methodology;
- Familiar with Burp suite/ZAP, Kali, Nexpose, Nessus, ASM, OSSTMM, NIST 800-115;
- Willing to learn or experience with device hacking / reverse engineering of products and devices
- Driven problem solver with proven success in solving difficult problems
- Excellent time management and follow-up skills
- Quality and effectiveness in work documentation and organization
- Business English proficiency

Desirable qualifications and background include:

- BS in Computer Science, Information Technology or Management Information Systems
- 5-7 years of experience in IT Security in a corporate environment

Would be a plus:

- Found and reported vulnerabilities in CVE databases;
- Active in local IT Security groups;
- Mobile Pentesting

If you are considering to apply for one of our open positions, please go through our Candidate Privacy Policy and then, send your resume to careers.cluj@garmin.com. We will consider your application as a consent to Garmin's candidate policy. If you do not agree with those terms, please mention it in your application e-mail.

- Certifications/Courses: CEH; OSCP; OSCE; CISSP