# Senior/Lead Security Engineer

## Hungary

EPAM is a leading global provider of digital platform engineering and development services. We are committed to having a positive impact on our customers, our employees, and our communities. We embrace a dynamic and inclusive culture. Here you will collaborate with multi-national teams, contribute to a myriad of innovative projects that deliver the most creative and cutting-edge solutions, and have an opportunity to continuously learn and grow. No matter where you are located, you will join a dedicated, creative, and diverse community that will help you discover your fullest potential.

We are looking for **Senior/Lead Security Engineer** to join our Team in Hungary.

## Responsibilities

- Driving Security Architecture & Solutions in collaboration with the Security Architect for our core digital portfolio and future products
- Conduct extensive Threat Modeling and analyze weaknesses within the system
- Work hand-on-hands with Security Architecture embedded Security-by-Design and Threat Modeling practices into the product development cycle
- Implement secure coding practices and provide secure libraries, ensuring the software is safeguarded at a foundational level
- Provide guidance on secure coding practices and conduct thorough code reviews, guiding the development team in addressing potential security issues
- Define global security models across core business verticals, ensuring secure integration with backend systems
- Develop appropriate technical and organizational security controls to mitigate identified risks, including encryption, access controls, and authentication mechanisms
- Execute Security-By-Design principles and contribute to driving Product Security Excellence
- Conduct security awareness training for employees developing, deploying, and maintaining medical devices

## Requirements

- Bachelor's Degree in Computer Science, Cybersecurity OR equivalent experience
- 5+ years of experience in Application Security, preferably in the medical or healthcare sector
- Relevant certifications such as Certified Application Security Engineer (CASE) or similar would be highly advantageous
- Expertise in secure coding practices and in-depth knowledge of at least one programming languages, including but not limited to .NET, Python, and JavaScript
- Familiarity with threat modeling methodologies and tools such as STRIDE, DREAD, or Attack Trees
- Advanced interpersonal skills with the ability to articulate complex technical concepts to non-technical personnel and conduct effective security awareness training
- Expertise with common security libraries, security controls, and common security flaws

- Security Knowledge: Solid understanding of network access, identity, access management, applied cryptography, network security methodologies, and secure software development methodologies
- Knowledge and experience identifying and understanding the most common application security vulnerabilities (OWASP Top 10)
- Deep expertise with more than one of the following areas
- API security
- Cryptography
- Identity and Access Management
- Application Security practices

## We offer

- Dynamic, entrepreneurial corporate environment
- Diverse multicultural, multi-functional, and multilingual work environment
- Opportunities for personal and career growth in a progressive industry
- Global scope, international projects
- Widespread training and development opportunities
- Unlimited access to LinkedIn learning solutions
- Competitive salary and various benefits
- Advanced wellbeing and CSR programs, recreation area