SDLC SECURITY

TECHICON
GREATNESS THROUGH EXCELLENCE

SECURING THE SDLC

We understand that an issue found in the wild is exponentially more expensive to fix than found in-house. A security vulnerability can lead to financial losses and impact the company reputation and customer trust, leading to lost revenue.

TechIcon, Inc. is built by security and software developers, which is why we focus on software development with a cybersecurity perspective. We believe that a security feature is not the same as feature security; hence it is essential to left shift cybersecurity in SDLC.

A software engineer focuses on development issues, whereas a network administrator deals with them after the release. Therefore, modern software needs both expertise to be robust, resilient, and secure. TechIcon, Inc. provides three types of services that range from training your team to build secure products to owning your products' security.

CONSULTANCY

We develop the SDL process for you that meets your company's needs. We understand that each team and organization is unique and follows a unique SDLC. We also understand that changing development processes means an evolution of the methods and, more importantly, the people.

We identify the steps in your development processes that will improve your products' security posture and help you modify them smoothly and iteratively. A proper development process guarantees high quality and secure products.

WHY US?

At TechIcon, we have been testing software and improving the security posture of our clients for over three decades. With this extensive experience, we not only help your company build better products but also train your teams so that you can work efficiently towards your business goals.

8200 Greensboro Dr., Suite 900,
McLean, VA 22102, U.S.A

We believe that a security feature does not necessarily provide feature security, hence it is essential to identify and fix any compromised features.

SDLC SECURITY

TRAINING

Well-educated engineers build industry-leading products. SDL is not new; however, it is not a part of most academic curriculums. We have developed a training program for teaching SDL, its importance, and its implementation to engineers with varied software development and security experience levels.

We customize the training to meet your organization's needs and provide real-world examples that will enable your engineers to become up to speed with SDL in a short period.

TECHICON
GREATNESS THROUGH EXCELLENCE

IMPLEMENTING THE SDL IN SDLC

Software (or feature) security is the goal of SDL, and it aligns well with SDLC. We do this by adding and merging our Security Development Life Cycle - in part or full - with our clients' SDLC processes.

1

Securing Requirements
We create adversarial use cases - also known as the abuse cases - for your software. Our use cases help your team understand security attacks as they start thinking about the software.

2

Design
We Threat Model your system using successful techniques, e.g., STRIDE, P.A.S.T.A, and Trike, which results in robust and secure software.

3

Development
Our cybersecurity experts focus on finding the code issues during software development and testing using the following techniques:

1. Static Analysis
2. Dynamic Analysis
3. Peer Review

4

Testing
Our testing experts provide a range of software testing services that focus on finding security-specific issues including:

1. Penetration Testing
2. Software Testing