SDL Training

Daniel M Beck

UMGC – SDEV-360

June 30, 2020

SDL Training

In the software development industry, it has become imperative that all members of the project be trained to the most recent concepts that the companies use to develop their software. As seen in figure 1, core trainings are the basis for all the processes of the Security Development Lifecycle (SDL). "A number of key knowledge concepts are important to successful software security" and such "each technical member of a project team (Developer, Tester, Program Manager) should be exposed to the knowledge concept:" (MICROSOFT SECURITY DEVELOPMENT LIFECYCLE (SDL), 2008).

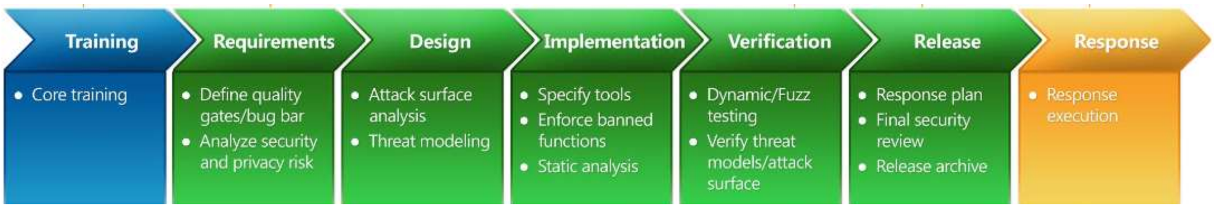

Figure 1, Introduction to the Microsoft®Security Development Lifecycle (SDL)

1. Secure Design

Implementing secure design can have a major impact on the entire project. If the design is flawed, then the project will generate a multitude of problems down the road. Part of a secure design can involve attack surface reduction which can be described as "the total number of places where an attacker could compromise your organization's devices or networks" (Dhiman, 2020). Knowing how to limit these surfaces leaves less opportunities for attackers to infiltrate the software.

2. Threat Modeling

Threat models have been implemented to create:

1. "An abstraction of the system"
2. "Profiles of potential attackers, including their goals and methods"

3. “A catalog of potential threats that may arise (Shevchenko, 2018).”

Using threat models has allowed developers to have a better view of potential threats so that they can be preemptively blocked.

3. Secure Coding

Proper security training develops secure coding principles which help developers gain knowledge of techniques to prevent attack such as a SQL injection. A “SQL Injection is a code injection technique that hackers can use to insert malicious SQL statements into input fields for execution by the underlying SQL database” (How to Protect Against SQL Injection Attacks). A successful attack can erase or expose an entire database making the software useless while exposing all the data of the software users.

4. Security Testing

Security testing helps developers uncover vulnerabilities, threats, and risks in a software application. Security testing such as risk assessment, “which involves analysis of security risks observed in the organization” (What is Security Testing?), allows developers to learn how to test their code against known security risks. This can help prevent future attacks by exposing weaknesses in the software.

5. Privacy

Security training creates an effective defense of users and business’ private information. A topic of privacy is privacy testing which refers to tests that are performed on the software to test that privacy requirements and guidelines are implemented correctly.

Conclusion

These training concepts will help lay the groundwork for a successful software development. Training in these areas will also help to fill in any gaps in education between the developers involved in the project. Along with keeping teams informed within the organization, about new findings in security, companies should have individuals from teams attend training sessions periodically to learn of any new risks that their company would benefit from implementing.

References

Dhiman, M. (2020, June 24). Use attack surface reduction rules to prevent malware infection - Windows security. Retrieved June 30, 2020, from https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

Essential Software Security Training for the Microsoft SDL [PDF]. (2010, June 02). Microsoft Corporation.

How to Protect Against SQL Injection Attacks. (n.d.). Retrieved June 30, 2020, from https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/how-protect-against-sql

Introduction to the Microsoft®Security Development Lifecycle (SDL) [PDF]. (2008). Microsoft Corporation.

MICROSOFT SECURITY DEVELOPMENT LIFECYCLE (SDL). (2008). Retrieved June 30, 2020, from http://www.cs.fsu.edu/~jowett/MS_SDL_Version_3.2.pdf

Shevchenko, N. (2018, December 03). Threat Modeling: 12 Available Methods. Retrieved June 30, 2020, from https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

What is Security Testing? (n.d.). Retrieved June 30, 2020, from https://www.guru99.com/what-is-security-testing.html