February 2013

Microsoft Security Development Lifecycle

Key Points

- The Microsoft Security Development Lifecycle (SDL) is Microsoft's security assurance process for software development that builds security into every phase of software development and provides defense-in-depth guidance and protection.
- The SDL is a hands-on set of procedures involving testers, developers, program managers, and architects working in concert with product security teams across the company. Its security innovations are integrated into Microsoft Office, the Windows operating system, Microsoft SQL Server, and many other Microsoft products and services.
- The SDL is continuously evolving and improving. It is updated to take advantage of newly developed defensive techniques in security science and in anticipation of emerging threats.
- Microsoft shares the SDL with the software industry. The SDL has been adopted (sometimes in a modified form) by a variety of software and hardware vendors, government agencies, and software development organizations.

BACKGROUND

Today's cyber security threats are complex, sophisticated, and ever-changing. They require an ongoing, multifaceted response from the information technology industry for development solutions that optimize software security and provide for safer computing experiences for people around the world.

The Microsoft Security Development Lifecycle (SDL) is Microsoft's security assurance process for software development that introduces security and privacy at every step of the way. It offers a holistic and practical approach to addressing evolving security threats and increasingly sophisticated cyber crime.

Microsoft developed the SDL process in 2004 as part of a defense-in-depth approach to security. It was created to reduce the number of vulnerabilities in Microsoft software and to give users high-quality, meticulously engineered, rigorously tested software that better defends against malicious attacks. Microsoft engineers and security experts realized that performing security activities as part of a repeatable process results in greater security gains and return on investment, and creates a more secure Internet environment. Using the SDL helps developers create software that has fewer, less severe vulnerabilities.

MICROSOFT APPROACH

- Using the SDL is a mandatory practice for product development at Microsoft. As shown below, it comprises a series of systematic security- and privacy-focused activities throughout the software development lifecycle— from technical training for engineers to processes for emergency responses after deployment.

- Software development is an evolving process and so is the SDL. While it's impossible to completely prevent all vulnerabilities during software development, when they do emerge, Microsoft engineers perform root-cause analysis to understand the problem. They then identify corrective actions and incorporate that knowledge into the next version of the SDL.

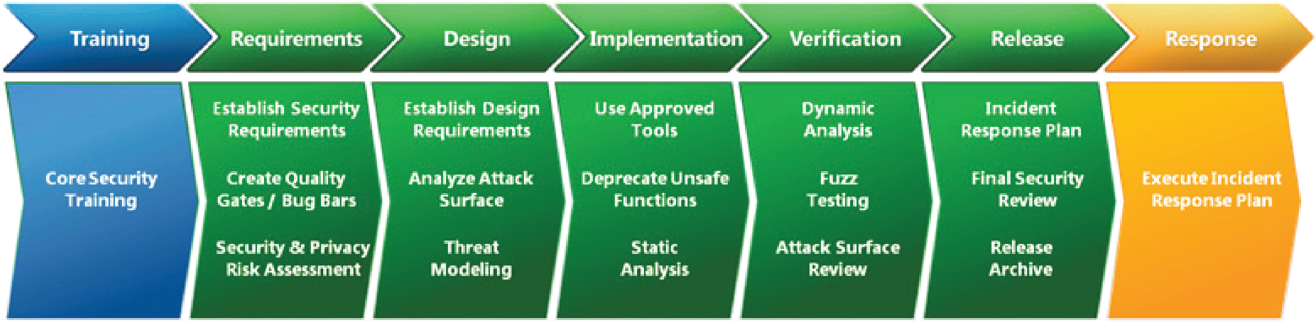
- Implementing the SDL has led to measurable improvements in the security and privacy of Microsoft's products.

POLICY CONSIDERATIONS

- Microsoft believes in a collective approach to security that involves the entire IT community, so the company shares security expertise, process guidance, and technology with developer and IT professional communities worldwide. As of 2012, IT professionals have downloaded Microsoft SDL guidance, white papers, and tools and resources more than a million times.

  The SDL Chronicles document how the Microsoft Security Development Lifecycle has helped public and private organizations change their engineering cultures and develop more secure software. Key industry leaders including Cisco and Adobe have based their security development methods on the Microsoft SDL.

- Any government approach to addressing the problems of information security should also protect innovation and ensure the continued adoption of new technologies. Government and industry can work together to establish appropriate principles that strike the right balance between regulation and innovation.



Helpful Resources

The Security Development Lifecycle
www.microsoft.com/sdl

The SDL Chronicles
aka.ms/SDL-Chronicles

Microsoft Trustworthy Computing
www.microsoft.com/twc/