|  |  |
| --- | --- |
| **Microsoft and the Adoption of the Security Development Lifecycle (SDL)** |  |

**Key Points:**

The Microsoft Security Development Lifecycle (SDL) is the software industry’s leading security assurance process:

* Building security and privacy into products from the ground up;
* Producing measurable reductions by reducing vulnerabilities;
* Helping to create a safer computing and Internet environment for everyone.

**Background: The Threat and the Response**

In the “old days,” many cyber-threats came from “hackers” looking to achieve little more than momentary notoriety. Today’s cyber-criminals, however, are increasingly sophisticated. The Microsoft Security Development Lifecycle is a full-system response to this growing threat. SDL builds privacy and security into every phase of software development, from the training of software engineers, to the design, implementation, testing and release of the product itself, to follow up education, tools and support for customers. The result of Microsoft’s company-wide adoption of SDL in 2004 has been a significantly reduced vulnerability count in flagship products such as Windows Vista, Microsoft Office and Microsoft SQL Server. With cyber attacks shifting to the application layer – software applications designed to work with a computer’s operating system -- Microsoft is making SDL resources, including tools, education, and processes available to other software developers, so that we can all work together to create a safer, more secure Internet/computing ecosystem.

**Building Security into Microsoft’s Culture**

The Microsoft SDL is a cultural as well as technological transformation that guides every part of our development cycle:

* All Microsoft developers go through SDL security training;
* Since 2004, no “enterprise class product” or product whose usage involves connection to the Internet can be released unless it meets SDL requirements;
* SDL is a “bottom up” as well as “top down” creative process, with product security teams in Office, Windows, SQL Server and other departments originating many of the security innovations that are then integrated into the company-wide SDL policy;
* SDL is not static, but a continuously improving system of requirements and technologies that is regularly updated in 6 month cycles in order to exploit newly developed techniques in “security science” and respond to and stay ahead of emerging threats;

**Dramatic Declines in Vulnerabilities**:

Since SDL was applied to the development of all relevant products in 2004, we have seen dramatic declines in vulnerabilities of Microsoft products to malicious attack:

* Vulnerabilities declined 45% in Windows Vista compared to the earlier Windows XP operating system;
* Vulnerabilities declined 35% in Internet Explorer 7 browser compared to Explorer 6, and high severity vulnerabilities declined 65%;
* SQL Server 2005 has had only 3 vulnerabilities compared to 34 for SQL Server 2003 in the first 36 months after release;
* Windows Vista, Internet Explorer 7 and SQL Server all beat the competition in terms of minimizing vulnerability counts.

**The Experts Agree: SDL is creating a more secure Internet:**

SDL is winning praise throughout the industry as having a marked effect in making software safer and more secure:

* “We actually consider Microsoft to be leading the software [industry] now in improvements in their security development life cycle [SDL]” – John Pescatore, VP of Gartner, February 2006, [www.crn.com](http://www.crn.com);
* “Microsoft’s Trustworthy Computing Initiative is perhaps the most advanced and comprehensive application security program in the industry” -- Chenxi Want, “Managing Application Security From Beginning to End,” Forrester Research, Inc, August 2007;
* “Why try to [hack] Vista when you have [easier, non-Microsoft targets like] Acrobat Reader installed, some antivirus software with shoddy file parsing, and the latest iTunes?” – Halvar Flake, Security Researcher, Microsoft BlueHat Conference, 9/07.[[1]](#footnote-2)

**SDL’s Success Means Cyber-Criminals Are Attacking New Targets**

In part because the SDL has been so successful in removing vulnerabilities, cyber-criminals are looking for easier targets of opportunity.

* Ninety percent of new vulnerabilities in 2007 were in applications, software that is layered above core operating systems, and only 10% in the operating systems themselves, according to Microsoft’s SIR Report;
* IBM’s x-force 2007 security report found that only 14% of vulnerabilities in 2007 were in software from the 5 largest software companies, i.e., Microsoft, Apple, Oracle, IBM, and Cisco.

*That is why Microsoft is actively working to share its SDL resources, including tools, education and processes with other developers so that together we can help make the entire computing ecosystem safer and more secure.*

1. Quotations from MS SDL Messaging Framework 042808. The Flake quote had been modified for a non-technical audience. The original quote reads; “Why try to chase a difficult overflow out of Vista when you have Acrobat Reader installed, some antivirus software with shoddy file parsing, and the latest iTunes?” [↑](#footnote-ref-2)