IT Insights

A service of Microsoft IT Showcase

Microsoft IT security experts offer support for internal and external customers

May 2015

The Assessment, Consulting & Engineering (ACE) team within Microsoft IT helps hundreds of Microsoft teams and external Microsoft customers worldwide with customized implementation of the Security Development Lifecycle (SDL).

Executive Summary

The ACE team is a group of highly specialized experts in Microsoft IT who serve as security consultants on line of business (LOB) application development. ACE experts support all worldwide subsidiaries and business units within Microsoft and offer consulting services externally to Microsoft customers.

Security Development Lifecycle at Microsoft

The SDL is a security assurance process focused on software development that has been a mandatory Microsoft-wide policy since 2004. The broad goal of the Microsoft SDL is to reduce the number and severity of software vulnerabilities by implementing specific yet flexible and scalable security and privacy practices throughout all phases of development. This goal is achieved by observing three core concepts:

- **Education.** Ongoing training and knowledge sharing for all technical job roles is critical to an organization's ability to respond appropriately to changes in technology and the accompanying security threats.
- **Continuous process improvement.** Because security risk is not static, understanding the cause and effect of security vulnerabilities requires frequent evaluation of security processes and adaptive response to change. Regular data collection and use of metrics help guide process changes.
- **Accountability.** The SDL requires archiving of all data necessary to service an application in a crisis. When paired with detailed security response and communication plans, clear and concise guidance can be provided to all parties.

For detailed information about the Microsoft SDL, see the link in the Resources section.

Assessment, Consulting & Engineering team at Microsoft

The ACE team is a Microsoft IT group in the Information Security & Risk Management (ISRM) organization. ISRM promotes safe, secure, and available services through risk management; enables embedded business security practices; ensures integration of security with technology; and upholds service commitments to the business. Within ISRM, ACE is a group of highly specialized security experts whose mission is to drive application excellence into production by providing application engineering leadership through security and privacy analysis services. In addition to working very closely with internal Microsoft IT customers, ACE team members serve as global consultants on line of business security for subsidiaries and business units within Microsoft, as well as for external Microsoft customers.

Line of business focus

The ACE team at Microsoft is specifically focused on LOB applications—the set of internal-use applications most critical to running an enterprise, such as accounting, governance, human resources, and billing. Although the ACE team's SDL processes are broadly parallel to those used by teams developing external software products, their services are most relevant to the needs of other IT organizations that are working on their own LOB applications.

The SDL for LOB applications focuses on a subset of the overall SDL process, but it's no less critical. The belief that internal corporate applications, used by "trusted" authenticated users, carry a lower security risk than external applications is a common and dangerous misconception. Significant insider threats are easily overlooked because of this misconception, which can result in substantial security failures such as lost or leaked data.

For example, the line between internal and external applications can be blurred with applications that accommodate Internet access. This functionality could potentially expose an internal application to the same Internet threats that any ecommerce application might face, which could result in stolen commodities such as intellectual property or trade secrets. A fundamental goal of the ACE team is to highlight, help correct, and ultimately prevent such dangerous assumptions and insufficient security practices.

Evolution of SDL within ACE

Over the last several years, ACE made a gradual but deliberate move away from predominantly manual design and code reviews to a more proactive approach, which focused security processes on the design and development phases and virtually eliminated work during testing. Security efforts also began to extend beyond the application code and focus on vulnerabilities in overall strategy and infrastructure, to protect applications from being exploited through other channels.

As the number of Microsoft teams that relied on ACE security services continued to expand, ACE began a concerted effort toward a more organized approach to security, focusing on extensive role-specific training that allowed responsibility to shift to the development teams themselves. ACE established a risk-based classification model that empowered the application teams to adopt security planning and evaluation as an integrated part of the development process. Lower-risk applications were placed in a "self-service" model, in which trained developers, program managers, and architects on the application team acted as the security experts.

A pool of ISRM Information Security Managers continues to work closely with business process units in Microsoft IT, providing thought leadership, security strategy, and ongoing education for the application teams that are carrying out their own security efforts. This ACE-supported self-governance allows for proactive, efficient security processes, with quality ensured by a combination of sampling and checks and balances. The introduction of increasingly automated threat-modeling tools and integrated statistical analysis–based reporting for risk management has enabled application teams to be even more independent and proactive.

Results

This evolution in security best practices and processes has provided clear benefits. Microsoft IT has seen improved efficiency, noted fewer production delays, and enjoyed a positive shift in the dynamic between the security team and development teams.

Maximized efficiency

When assessing internal applications for compliance with security policy, the ACE team validates the correct implementation of more than 100 technical control procedures. These application reviews are focused on custom code and configuration at the application layer as well as infrastructure security. Additionally, the number of application reviews that are conducted by the ACE team has nearly doubled in the past couple of fiscal years. The team's reliance on finely tuned SDL procedures and tooling to support the security governance process allows them to keep up with the demand for these comprehensive reviews without significantly increasing resources.

Fewer production delays

The amount of effort required to fix a security deficiency is relative to the stage in the development cycle at which the deficiency is discovered. By implementing the ACE team's proactive approach to security processes, which focuses security efforts on the early phases of design and development, Microsoft IT can significantly reduce production delays. The following illustration, from the whitepaper *The Microsoft SDL: Return on Investment*, shows the chain of dependencies with the approximate proportion of required rework to fix a deficiency at each stage. A deficiency that is identified early in the process will have the smallest impact on the production schedule.

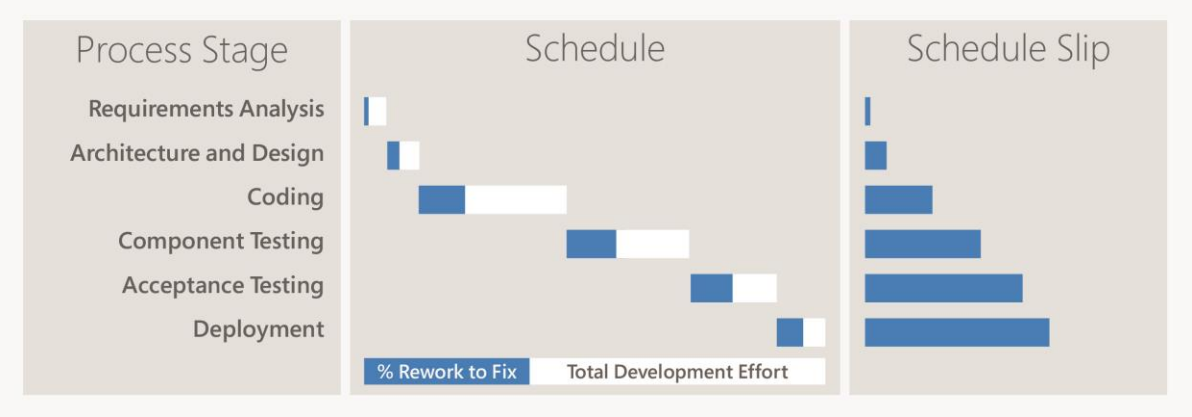

Figure 1. The relationship between the timing of security efforts and delays in the production schedule.

Better relationships

Collaborating on an established set of proactive security measures from the beginning of the development lifecycle created a true partnership between development teams and security teams in Microsoft IT. Shifting the role of a security team from regulation enforcer to partner can dramatically change the dynamic between security and development; success is defined as a joint effort to prevent security bugs, rather than a two-team process of finding and fixing them.

Implementing SDL today

Today the ACE team focuses primarily on four key phases of the SDL, which correspond with, and are implemented during, the key phases of the software development process.

1. **Training.** ACE provides role-specific training for all application team members responsible for security, including program managers, architects, developers, and testers.

2. **Requirements gathering.** It's critical that security requirements be established as early as possible because of the depth at which applications are integrated with core business functions. ACE recommends that security and privacy risk assessments be performed at the application portfolio level.

3. **Design.** Most security-related work occurs in the design phase. ACE provides support to help ensure that the design and architecture of the application are robust, incorporating threat modeling to prevent design-level issues.

4. **Implementation.** Much like product development teams, the ACE team strives to implement secure coding procedures—including use of approved tools, functions, and code review practices—as well as security of the infrastructure on which the applications are deployed.

ACE consulting

The ACE team continues to evolve and adapt, with the goal of providing a holistic risk management solution via a set of highly specialized services to internal and external clients. The Microsoft IT security experts who form ACE serve as consultants who can deliver a wide variety of security, privacy, and risk-assessment services, including support for traditional on-premises products and cloud-based services, such as Azure and mobile solutions.

As Microsoft IT, the primary customer of ACE, continues to transition its own LOB applications to the cloud, the ACE team will support all security-related efforts and challenges. ACE also offers its expertise to other groups within Microsoft as needed, with the flexibility to either augment a team's existing processes or provide a complete security service. This cross-group support commitment uniquely exposes ACE experts to security considerations that span a wide range of emerging products and technologies. Because Microsoft IT is a customer of other Microsoft product groups, the result is a continuous and synergistic feedback loop that benefits all parties.

The effects of this cooperative relationship also extend beyond Microsoft, directly benefiting the external Microsoft customers who want to take advantage of the ACE team's experience and expertise.

Services

The ACE team helps customers of any type (including both public sector and commercial), anywhere in world. ACE customizes its offerings to fit the security and privacy needs of each customer, from smaller businesses in need of a foundation of security essentials to large corporations with established security strategies interested in an independent analysis or recommendations for the latest security measures.

While ACE experts and other Microsoft IT subject matter experts regularly engage in complimentary consultation with Microsoft customers on a variety of IT topics via customer account managers, ACE also offers more extensive and individualized security services, including:

- **On-site analysis service.** SDL Maturity Assessments, including recommendations for an SDL program or program improvements.
- **Education.** Training and workshops covering secure application development and the entire SDL methodology, customizable to the size and needs of the company.
- **Design and code reviews.** In addition to support for traditional applications, also includes support for companies preparing to move applications to Azure, as well as support for mobile application development.
- **Infrastructure security consultation.** Proactive prevention of infrastructure exploitation.
- **Made-to-fit services.** Customized services based on specific security needs.

Learn more

Customers who are interested in having a discussion with a Microsoft IT subject matter expert, including a member of the ACE team, should ask their account manager to submit an IT Showcase request. Customers who are interested in any of the application security services mentioned in this article can contact their Microsoft services account executive to start an engagement with the ACE team at Microsoft IT.

Resources

Security Development Lifecycle at Microsoft:
http://microsoft.com/sdl

Security Development Lifecycle Publications Library:
https://www.microsoft.com/en-us/SDL/Resources/publications.aspx

The Microsoft SDL: Return on Investment
http://go.microsoft.com/?linkid=9696910

Microsoft Safety & Security Center:
http://microsoft.com/security

Enterprise Security & Privacy:
http://www.microsoft.com/enterprise/it-leaders/cybersecurity-privacy/default.aspx

Related content

Microsoft IT Executive Report: Reimagine Security
(Published January 2015)

For more information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Order Centre at (800) 933-4750. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

www.microsoft.com

www.microsoft.com/ITShowcase