Microsoft

Operational security for online services overview

Microsoft Trustworthy Computing
October 21, 2013

Legal disclaimer

Acknowledgments

Authors
Mike Reavey
Frank Simorjay
Steve Lipner

Contributors and Reviewers
Jamie Blair
Grant Bugher
Mark Estberg
Mark Cartwright
Cristin Goodwin
Chris Hale
Adrienne Hall
Carlene Heath
Marc Lauricella
Ken Malcolmson
Tim Rains
Matt Thomlinson
Stevan Vidich
Lori Woehler

Introduction

Microsoft is committed to delivering trustworthy cloud services, and is in a unique position to do so based on its experience, investments, and history of commitment over the past 10+ years toward the creation and delivery of secure, private, and reliable computing experiences. This white paper provides insight into how Microsoft applies its resources to online services in ways that extend beyond traditional standards and methodology to deliver industry-leading capabilities.

Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world that deliver more than 200 online services to more than 1 billion customers and 20 million businesses in 88 countries.

Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them.

OSA helps make Microsoft cloud-based services' infrastructure more resilient to attack by decreasing the amount of time needed to prevent, detect, contain, and respond to real and potential Internet-based security threats, thereby increasing the security of those services for customers.

The goals of OSA are straightforward:

- Establish a scalable process to improve operational security across all Microsoft cloud service offerings.
- Respond to security challenges as they emerge from the evolving threat landscape by providing simple, predictable updates to the framework that continuously improve operational processes and procedures used by Microsoft engineering teams.
- Reduce threat identification and response times by ensuring that online services have effective attack detection capabilities and are capable of fielding a unified response team that can resolve incidents rapidly and at scale.

- Complement recognized standards such as NIST Special Publication 800-53 (the standard that underlies Federal Information Security Management Act [FISMA] certifications – referred to later in this paper as NIST 800-53) and ISO 27001.
- Be flexible enough to work with a broad range of Microsoft cloud services, from those that make up small custom solutions to large services used by both consumer and enterprise customers.
- Maintain a high level of service availability and minimize the impact of both planned and unplanned incidents to customers.

Background

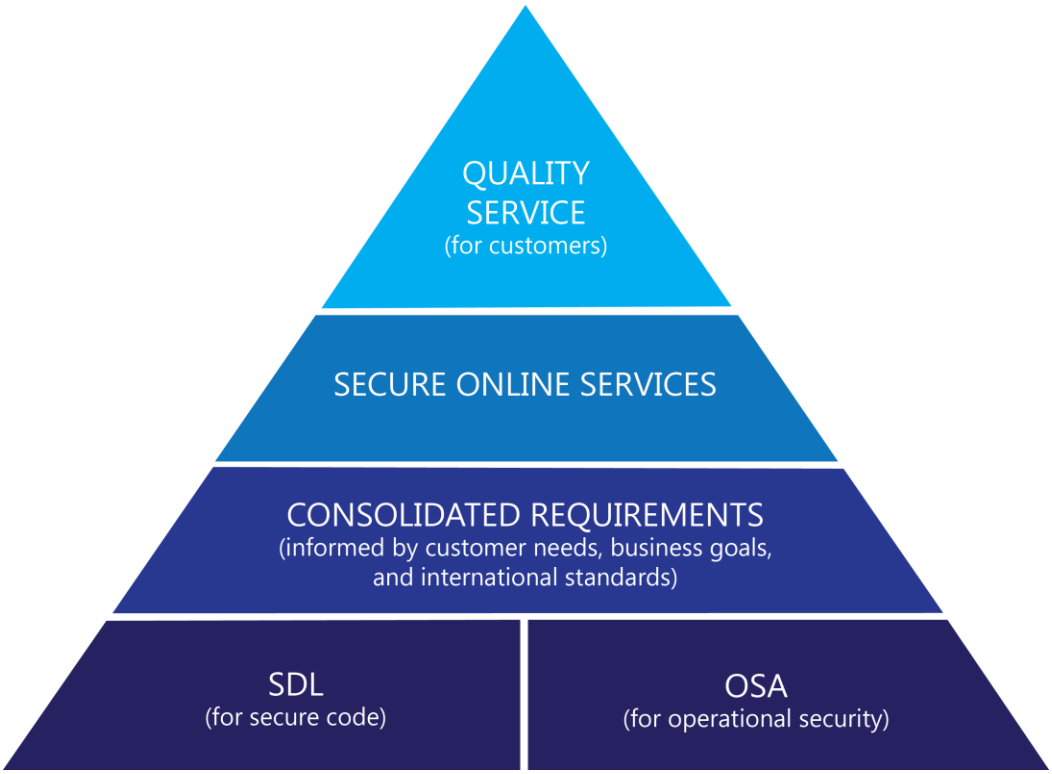
Since 2004, the SDL has helped developers build more secure software and address software security assurance requirements. However, building secure software is only one aspect of maintaining a system's security. Successful network attacks can take advantage of infrastructure-related security shortcomings such as system misconfiguration and abuse of privileges.

OSA addresses operational security needs in a way that takes advantage of SDL knowledge and processes. OSA is a framework that focuses on infrastructure issues to help ensure secure operations throughout the lifecycle of cloud-based services. The following list includes a number of ways that OSA adds considerable value to the focus on infrastructure issues and operational security:

- Use of a proven methodology for verification and continuous improvement that was first established with the SDL and is closely tied to Microsoft Security Response Center (MSRC) incident response processes.
- Support of Microsoft internal security policies that align with standards such as NIST 800-53, ISO 27001, and other related industry guidance that applies to a broad range of cloud services. It also reflects Microsoft experience in the secure operation of online services.
- Protection against Internet-based external threats.
    - OSA is designed to better discover attacks as a way to inform future security improvements.
    - OSA prescribes key security controls that Microsoft has seen to be effective in mitigating known attacks and previously unknown vulnerabilities.
- Decades of Microsoft experience operating cloud services at scale.
- Integration with the SDL, so that changes in operations can result in changes to the development of software used in operations and vice-versa. More importantly, OSA creates a feedback cycle that Microsoft can use to update its operational processes more rapidly than a typical policy cadence can support.

- Repeatable practices and methodology that are used to actively and continuously update services to improve security and resolve incidents as quickly as possible.

The following figure illustrates the complementary nature of SDL and OSA in supporting secure online operations and providing optimal quality for Microsoft customers. Consolidated requirements are based on customer needs, business goals, and international standards; SDL and OSA help mitigate risk and protect Microsoft and its customers from security threats.



The foundation of secure online services consists of the following elements:

- SDL, to ensure the software that underlies the service is designed and developed with security in mind throughout its entire lifecycle.
- OSA, to ensure the deployment and operation of the service includes effective security practices throughout its lifecycle.

OSA is built on the fundamental principles of threat modeling, designing secure configurations, testing operational effectiveness, and promptly responding to and remediating security concerns. It includes a high degree of automation and telemetry to ensure the effectiveness of operational procedures.

OSA supports external compliance requirements; that is, it doesn't obviate the need for them. Microsoft cloud services employ a comprehensive compliance framework that is designed to

help customers comply with their own specific regulatory requirements. However, given that the scope of OSA focuses on a broad range of cloud services, OSA doesn't require all controls from all compliance regimes; to do so would be untenable and inefficient for many markets. Instead, OSA focuses on those controls that are proven to be most effective against Internet-based threats across the operations of all services, including controls not described by any compliance regime.

Elements of OSA

This section describes OSA elements, including key roles that are involved in its implementation as well as the development and updating of the OSA process.

Scope of OSA

The scope of OSA is limited to a set of control objectives or domains most likely to be affected by external Internet-based attack. This set of domains closely aligns with and maps to the control areas that are used by NIST 800-53 and ISO 27001. OSA defines the aspects of these domains by first establishing baseline requirements that each service should meet or exceed. These baseline requirements are then used to establish a test plan that can be used to validate a service's security during an assessment.

Creating these baseline requirements allows OSA to effectively test services before *and* during operation. OSA requirements for some domains involve collecting documentation or training staff to ensure that they have skills that ensure work of appropriate quality; requirements for other domains can take advantage of automated solutions that are able to demonstrate that operational baseline requirements are being addressed. OSA also ensures that information about the effectiveness and security of operational processes is considered confidential, and that this information is appropriately protected and secured.

Key personnel roles in OSA

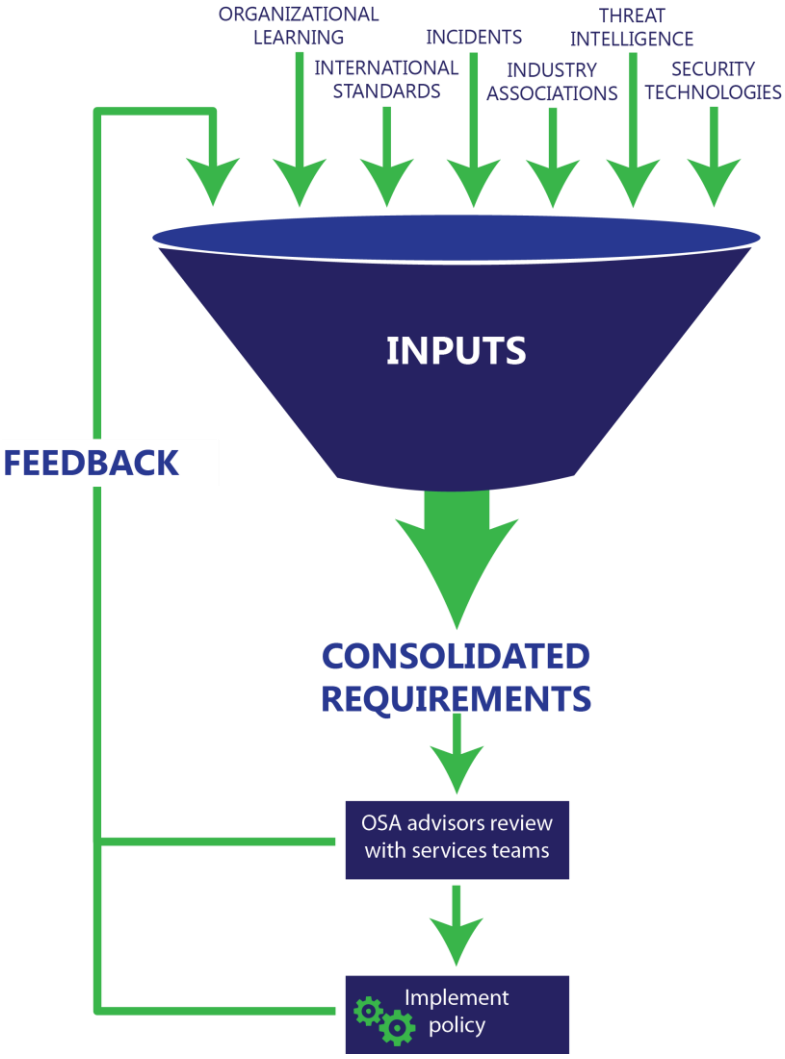
Key roles for OSA implementation include the following:

- **OSA advisor**, who partners with appropriate cloud service owners to drive threat models and to ensure that OSA baseline requirements are addressed and issues are resolved in a timely manner.
- **OSA policy creator**, who aggregates all input to create new security baselines on a regular rhythm across Microsoft.
- **Operations security leads**, who are knowledgeable about the implementation of Microsoft security policy, standards, and procedures.
- **SDL security champs**, who maintain an understanding of the natural alignment between operational and application security in online services.
- **Subject matter experts**, who can help solve complex security problems or design technical solutions in response to specific security challenges.

OSA methodology

The three key processes of OSA are as follows:

- Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant.
- Developing and applying centralized review processes to consolidate all requirements to establish the OSA baseline requirements.
- Engaging and implementing the new requirements and baselines.



These processes are designed to ensure that systemic issues are identified across the operations of all services, and the identification of these issues informs the evolution of OSA itself. Therefore, it is important that process activities are performed by those who serve in the key OSA roles described earlier.

The preceding diagram provides a high-level view of how the OSA process works. Inputs consist of many different types of information, including:

- **Organizational learning** and improvements are collected and can be used to improve Microsoft services. These improvements and learnings are then absorbed into the OSA process.
- **International standards** and mature external security practices, such as updates to NIST SP 800-53, ISO 27001, and other relevant practices. These standards and practices are integrated to reflect community best practices and avoid duplication of effort on the part of services teams.
- **Security incidents** and threats from attackers who seek to take advantage of publicly acknowledged security vulnerabilities and configuration shortcomings that create vulnerabilities. Microsoft employs a Security Information Management process that aligns with ISO/IEC 18044 and NIST SP 800-61.
    - Through incident responses, effective mitigations against new attack trends and behaviors as well as new security technologies and security solutions are often implemented quickly, and later become part of a domain baseline.
- **Industry associations** and experts that provide Microsoft with insight into organizational needs, which influence organizational learning as well as industry standards.
- **Threat intelligence** programs such as the Microsoft Security Intelligence Report (SIR), which analyzes the threat landscape using data from Internet services and more than 600 million computers worldwide.
- **Security technologies** and security solutions that are developed both inside and outside of Microsoft to protect against security threats.

The OSA process also uses feedback from online service teams within Microsoft to continuously evaluate and improve the OSA process. This feedback is also considered confidential, and it is protected in accordance with Microsoft internal policies.

The OSA process helps ensure that Microsoft cloud operational services are sufficiently nimble and agile to accomplish their operational goals. The consolidated requirements are designed to achieve the following outcomes:

- Facilitated compliance, because systemic issues are identified across all online services operations.
- Continuously updated controls and mitigations, which lead to enhanced security programs.
- A continuously updated OSA process that improves operational cadence and optimizes operations.

- World-class cloud services that deliver on the promise of cloud computing for individual customers as well as organizations of all sizes.

Wherever possible, implementation efforts include tools to facilitate OSA compliance and automate measurement against the OSA baselines. Such automated measurements may include aggregating data from existing tooling (such as vulnerability scanners) that can be mapped against OSA baselines on a continuous basis.

Conclusion

The rapid increase in the popularity and scale of cloud services has necessitated the formal integration of security practices into online service operations and development over the past several years. Just as the SDL was developed to address the need for more secure code, OSA was developed to address the need for more secure operations. And just as SDL has continued evolving, OSA will continue to evolve over time as requirements change, new threats develop, and tools mature.

OSA is an important process that Microsoft uses to make its networks more resilient to attack and increase the security of its cloud-based services. OSA helps Microsoft achieve this increased resilience and security by extending the foundation of Microsoft cloud-based services to protect against Internet-based security threats and by incorporating best practices and methodology to continuously update services to improve security and resolve incidents as quickly as possible.

For additional information, see

Microsoft Security Development Lifecycle (SDL)

Trusted Cloud site on Microsoft TechNet

Global Foundation Services