MS_logo_KMICROSOFT SDL - DEVELOPER STARTER KIT:

THREAT MODELING PRINCIPLES (LEVEL 100)

Version 1.0

The following questions accompany the materials for the Microsoft SDL - Developer Starter Kit Threat Modeling Principles (Level 100) presentation.

For the latest information, please see [http://www.microsoft.com/sdl](http://go.microsoft.com/?linkid=9672761).

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, SQL Server, Visio, Visual Basic, Visual C#, Visual C++, Visual Studio, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[1.0 Microsoft SDL - Developer Starter Kit Content Comprehension Questions 2](#_Toc233634391)

[1.1 Introduction 2](#_Toc233634392)

[2.0 Threat Modeling Principles (Level 100) Questions 2](#_Toc233634393)

# 1.0 Microsoft SDL - Developer Starter Kit Content Comprehension Questions

## 1.1 Introduction

“The Microsoft Security Development Lifecycle (SDL) is an industry-leading software security assurance process. A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture. Combining a holistic and practical approach, the SDL introduces security and privacy early and throughout all phases of the development process. It has led Microsoft to measurable and widely-recognized security improvements in flagship products, such as Windows Vista, Windows Server (2003 and 2008) and SQL Server. Microsoft is publishing the detailed SDL process guidance as part of its commitment to enable a more secure and trustworthy computing ecosystem.” -- [The Microsoft SDL 3.2 Whitepaper](http://go.microsoft.com/?linkid=9672762)

To help promote the adoption and awareness of the Microsoft SDL, Microsoft has developed content and demonstrations specifically for external developer audiences. The remainder of this document provides individuals who will present this content internally within their respective organizations with questions that may be used to ascertain comprehension of the subject matter addressed within the Microsoft SDL Training Module: Threat Modeling Principles (Level 100) presentation. These questions have been designed to enable the presenter to ascertain the extent at which the participating personnel with application development responsibilities have comprehended the subject matter addressed in the Threat Modeling Principles (Level 100) training module, as well as enabling the presenter to assess participants’ ability to apply the subject matter addressed to practical secure and trustworthy application development scenarios.

# 2.0 Threat Modeling Principles (Level 100) Questions

**Question #1:** Which of the following are steps in the Microsoft SDL Threat Modeling process?

1. Diagramming, Threat Enumeration, Mitigation and Validation.
2. Diagramming, Vulnerability Discovery.
3. Diagramming, Vulnerability Discovery, Fuzz Testing.
4. Vulnerability Discovery, Attack Path Identification.

**Answer:** The correct answer is “**A**”. The steps of the Microsoft SDL Threat Modeling process are Diagramming, Threat Enumeration, Mitigation and Validation.

**Question #2:** True or false: The Microsoft SDL Threat Modeling process can be used to replace the need for security expertise

1. True.
2. False.

**Answer:** The answer is “**B**” (false). The Microsoft SDL Threat Modeling process can be used in the absence of security-expertise to arrive at a baseline set of threats against an application design. However, it cannot and should not be used as a replacement for other sound security assessment activities, such as security code review and fuzz testing, which should be performed by security experts.

**Question #3:** A malicious user who may be able to impersonate the identity of a valid user for an application is an example of which STRIDE threat?

1. Spoofing.
2. Tampering.
3. Repudiation.
4. Information Disclosure.
5. Denial of Service.
6. Elevation of Privilege.

**Answer:** The correct answer is “**A**”. Spoofing is the threat of a malicious user being able to impersonate something or someone else.

**Question #4:** With respect to mitigating threats, what design mitigation approaches are recommended, in order of preference (most preferred to least preferred), according to the Microsoft SDL Threat Modeling process?

1. Use unique mitigations, accept risks in accordance with policies, use standard mitigations and redesign.
2. Use standard mitigations, redesign, use unique mitigations and accept risk in accordance with policies.
3. Redesign, use standard mitigations, use unique mitigations, and accept risk in accordance to policies.
4. Accept risk in accordance with policies, use unique mitigations, redesign and use standard mitigations.

**Answer:** The correct answer is “**C**”. Redesigning applications to eliminate identified threats is the preferred mitigation approach. Next is to use standard mitigations, such as IPsec to mitigate spoofing threats. After the use of standard mitigations, using unique mitigations where custom mitigations are employed is preferable. The least preferred mitigation approach in the list above is to accept risk in accordance to policies, which means that nothing is done in response to an identified threat.

**Question #5:** An application was threat modeled and was found to be susceptible to several threats. One of the threats is a malicious user being able to view data sent to and from the application while the data is in transit over public networks. The application design team redesigns the application to use SSL to protect data in transit to and from an application. The mitigation approach that the application design team chose is an example of which SDL Threat Modeling process mitigation approach?

1. Redesign.
2. Use standard mitigations.
3. Use unique mitigations.
4. Accept risk in accordance with policies.

**Answer:** The correct answer is “**B**”. SSL is a standard data protection protocol and the use of this protocol aligns with the ‘Use standard mitigations’ mitigation approach.

**Question #6:** True or false: The ideal phase within the software development lifecycle (SDLC) which to perform threat modeling is the Design phase.

1. True.
2. False.

**Answer:** The correct answer is “**A**” (true). Threat modeling is a process to assist application designers in identifying threats in application designs and therefore it is most advantageous to perform threat modeling at the design phase of the software development lifecycle. The Microsoft SDL Threat Modeling process can still be used after the Design phase, such as during the implementation or verification phases; however, at these later stages the effectiveness of threat modeling is not as high as in the design phase.