MS_logo_KMICROSOFT SDL - DEVELOPER STARTER KIT:

THREAT MODELING TOOL PRINCIPLES (LEVEL 100)

Version 1.0

The following questions accompany the materials for the Microsoft SDL - Developer Starter Kit Threat Modeling Tool 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](#_Toc233640752)

[1.1 Introduction 2](#_Toc233640753)

[2.0 Threat Modeling Tool Principles (Level 100) Questions 2](#_Toc233640754)

# 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 Tool 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 Tool 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 Tool Principles (Level 100) Questions

**Question #1:** Which of the following steps is not a step within the Microsoft SDL Threat Modeling Tool?

1. Draw Diagrams.
2. Analyze Model.
3. Describe Environment.
4. Launch Fuzz Tests.
5. Generate Reports.

**Answer:** The correct answer is “**D**”. The Microsoft SDL Threat Modeling Tool helps to automate the Microsoft SDL Threat Modeling process, which is a design-time assessment activity. Fuzz testing is performed against an operational application well after the design phase in the verification phase. The actual steps of the Microsoft SDL Threat Modeling Tool are the Draw Diagram, Analyze Model, Describe Environment and Generate Reports steps. These steps will help identify threats to an application design, whereas fuzz testing will help identify vulnerabilities in implemented code based on application designs.

**Question #2:** What is the goal of the Draw Diagram step when using the Microsoft SDL Threat Modeling Tool?

1. To model an application design as a data flow diagram to drive threat analysis.
2. To model an application design as a UML diagram to drive threat analysis.
3. To model an application design as a flow chart to drive threat analysis.
4. To model an application as a Specification and Description Language (SDL) diagram to drive threat analysis.

**Answer:** The correct answer is “**A**”. The Microsoft SDL Threat Modeling Tool uses data flow diagrams as the application modeling representation to drive threat analysis.

**Question #3:** The Microsoft SDL Threat Modeling Tool can be used to:

1. Create a baseline set of potential threats and mitigations for each data flow diagram element.
2. Create a comprehensive set of potential threats and mitigations for each data flow diagram element.
3. Identify all potential application vulnerabilities.

**Answer:** The correct answer is “**A**”. The Microsoft SDL Threat Modeling Tool can be used to create a baseline set of potential threats and mitigations for a modeled application design. Recall that no one assessment technique or tool can identify all possible threats and vulnerabilities, and therefore answers “B” and “C” are incorrect.

**Question #4:** In which Microsoft SDL Threat Modeling Tool step are security dependencies and assumptions documented?

1. Draw Diagram step.
2. Analyze Model step.
3. Describe Environment step.
4. Generate Reports.

**Answer:** The correct answer is “**C**”. Security assumptions and dependencies are documented in the Describe Environment step.

**Question #5:** The Microsoft SDL Threat Modeling Tool can be used by:

1. Security experts only.
2. Non-security experts only.
3. Both security experts and non-security experts.

**Answer:** The correct answer is “**C**”. The Microsoft SDL Threat Modeling Tool can be used by both security experts and non-security experts to arrive at a baseline set of threats facing application designs. The ability for non-security experts to use this tool is possible because the Microsoft SDL Threat Modeling Tool uses the STRIDE-per-element, which provides a mapping of known threats against DFD elements.