



Securitybyte

Securing the information DNA

OWASP

AppSec Asia



Microsoft® Security Development Lifecycle (SDL) Threat Modeling

Varun Sharma
Security Engineer, ACE Team,
Microsoft IT Information Security Group
Microsoft India
varun.sharma@microsoft.com

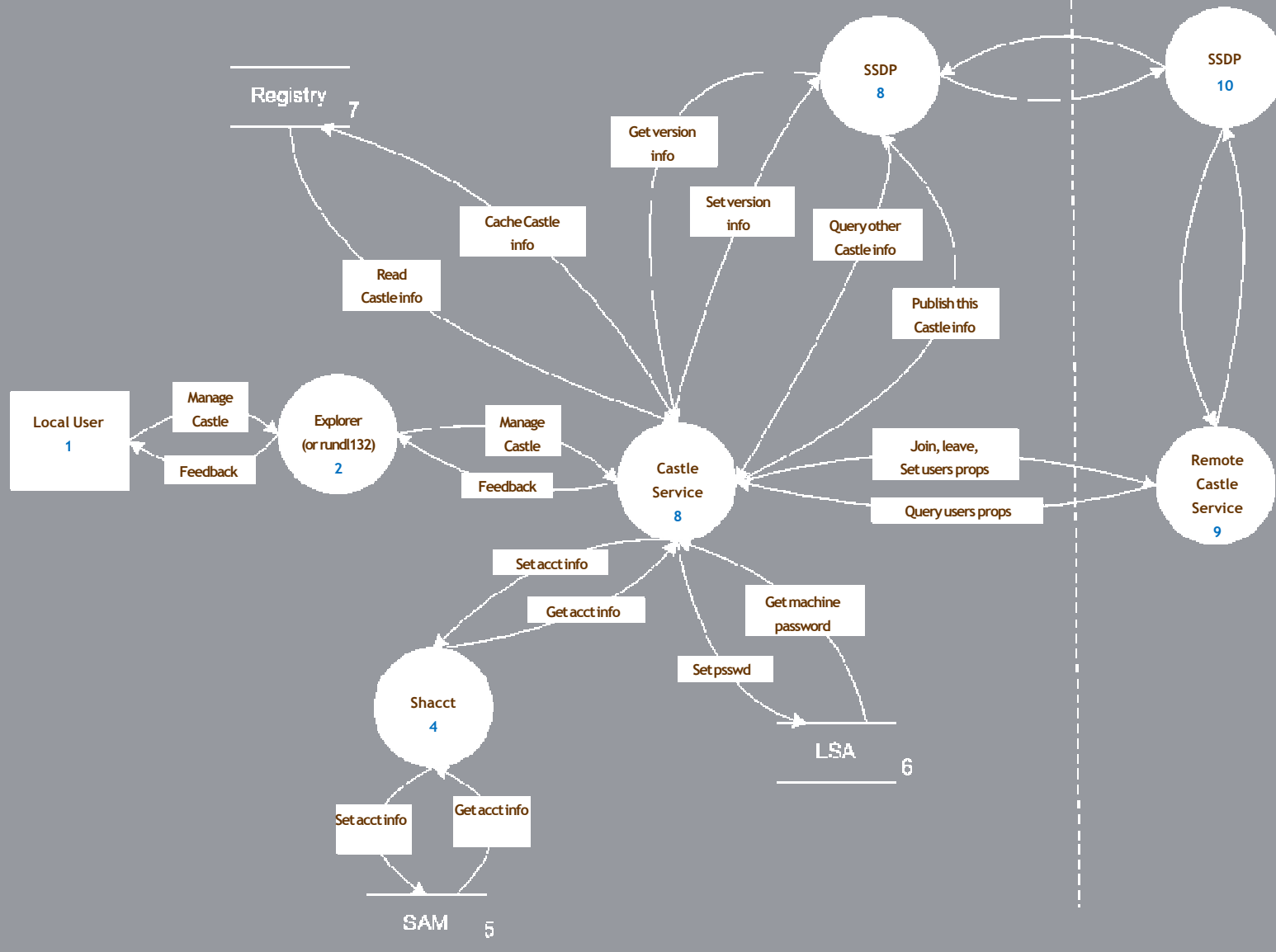
Agenda

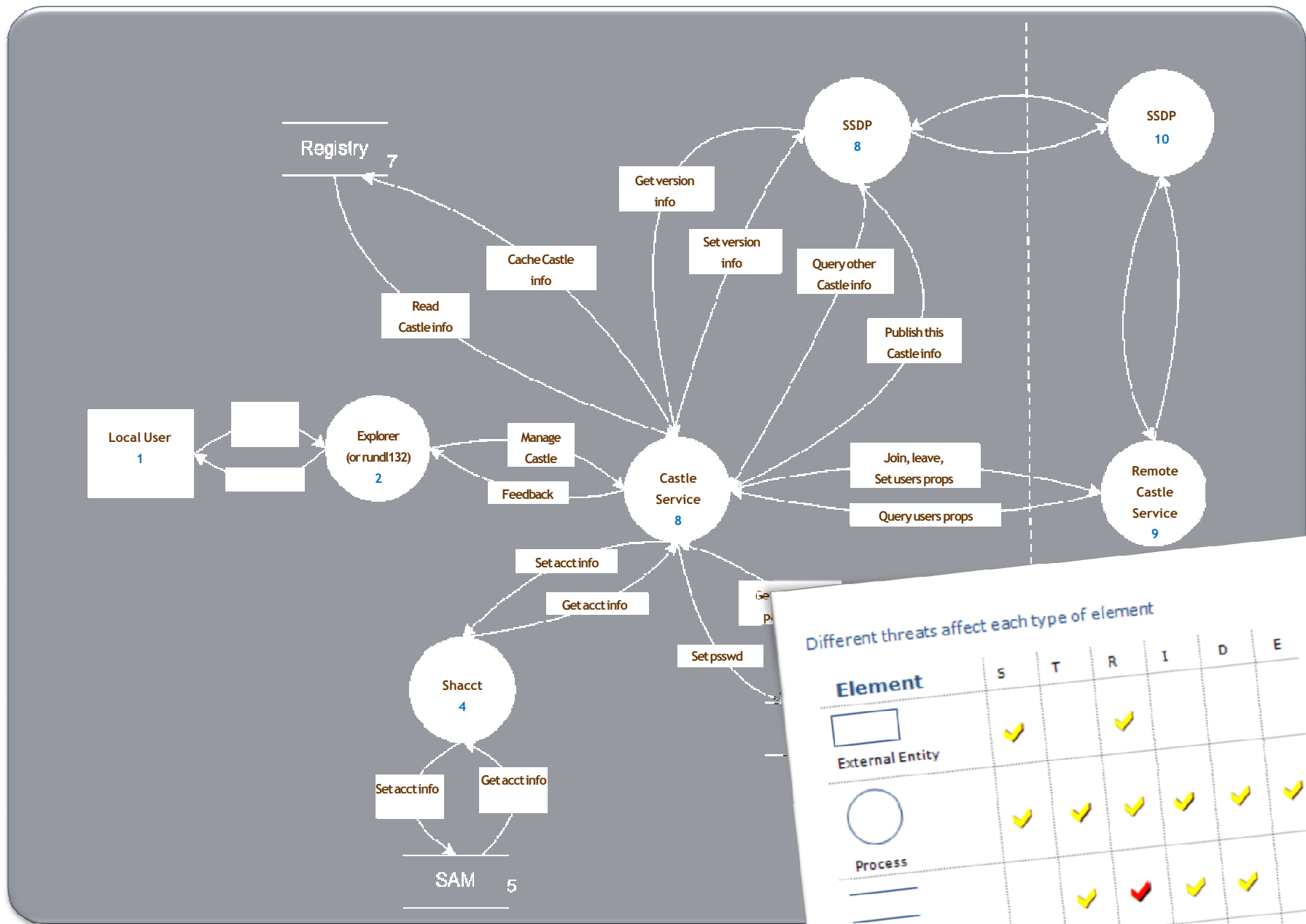
- Threat Modeling Basics
- The SDL Approach to Threat Modeling
- Demo

Threat Modeling Basics




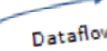
- **Who?**
 - The bad guys will do a good job of it
 - Maybe you will...your choice
- **What?**
 - A repeatable process to find and address all threats to your product
- **When?**
 - The earlier you start, the more time to plan and fix
- **Why?**
 - Find problems when there's time to fix them
- **How?**

How to Threat Model





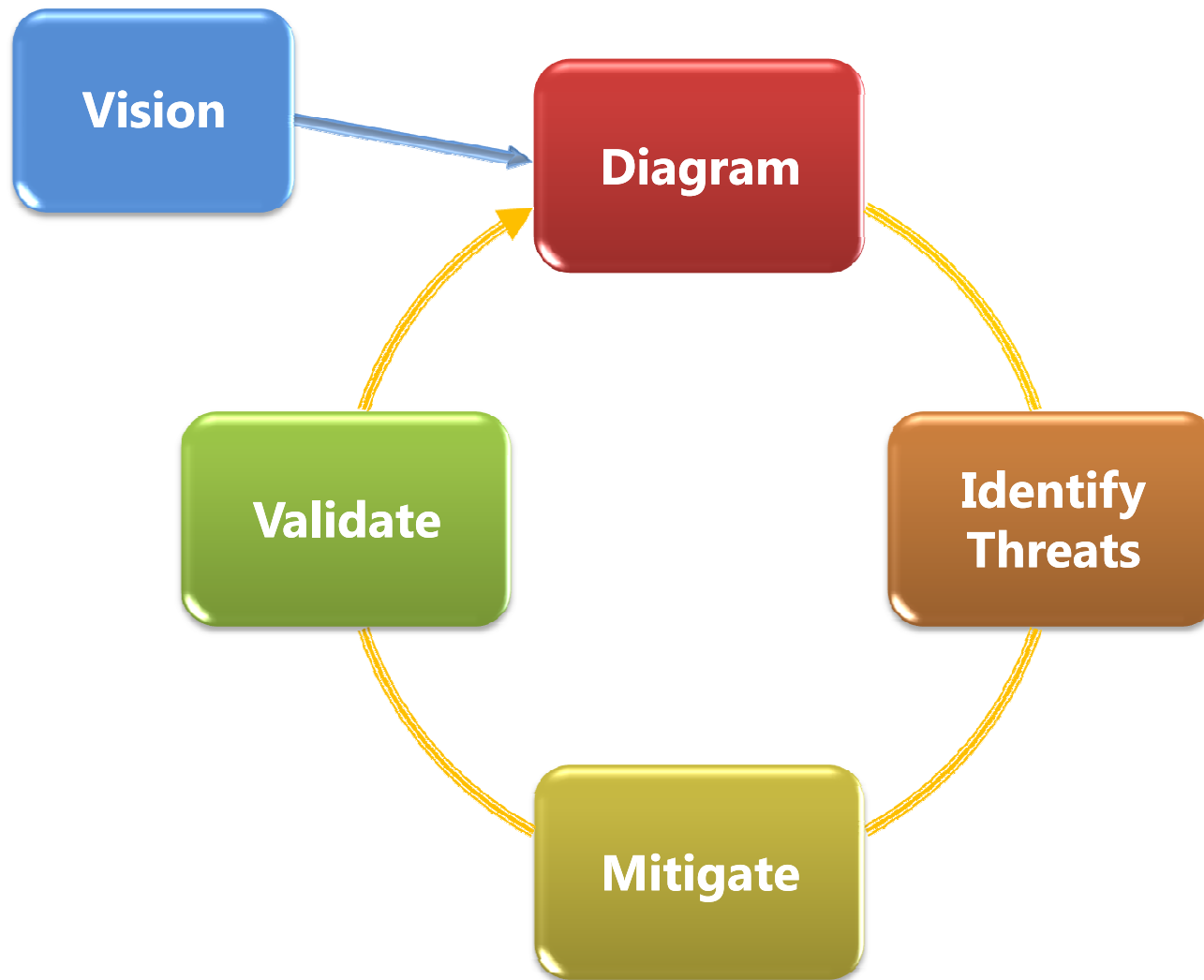
Different threats affect each type of element

Element	S	T	R	I	D	E
 External Entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	✓	✗	✓	✓
 Dataflow		✓			✓	✓

Any Questions?

- Everyone understands that?
- Spotted the several serious bugs?
- Let's step back and build up to that

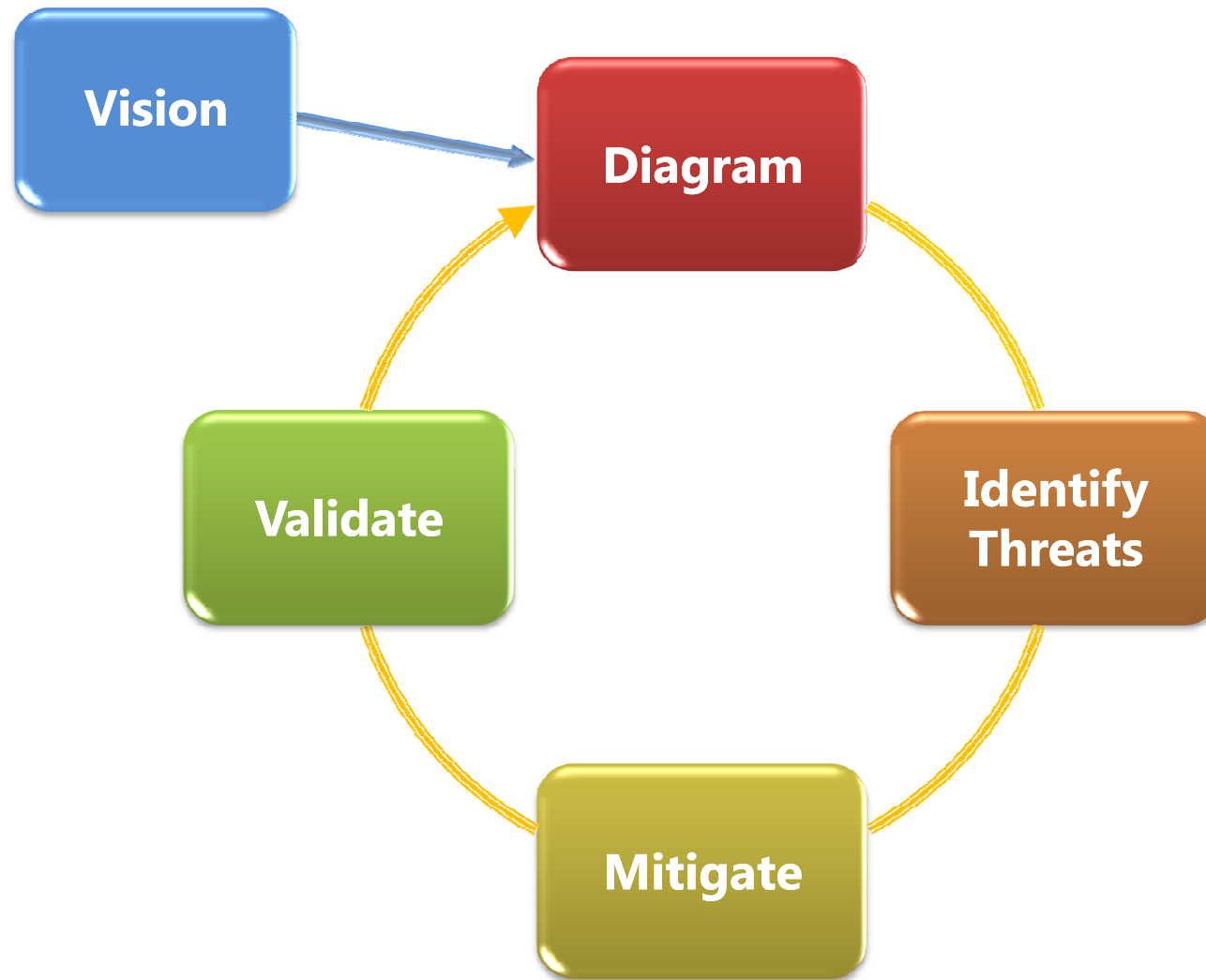
The Process in a Nutshell



Vision

- **Scenarios**
 - Where do you expect the product to be used?
 - Live.com is different from Windows Vista
- **Use cases / personas**
- **Add security to scenarios, use cases**
 - Think about what are you telling customers about the product's security...

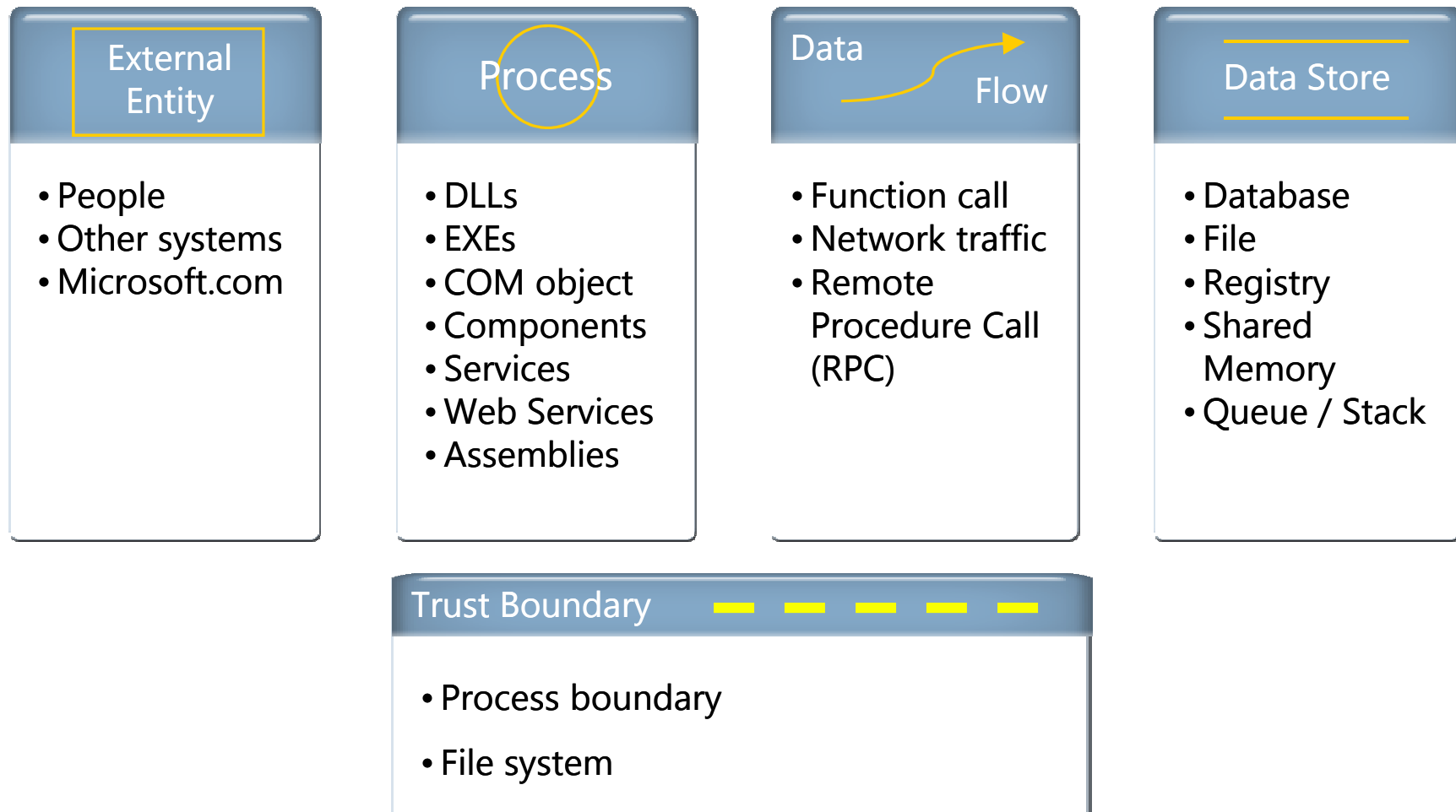
The Process: Diagramming



Diagramming Overview

- **Create diagrams**
 - Data Flow Diagrams (DFD) are one way to represent a system
 - Include processes, data stores, data flows
 - Include trust boundaries
 - Diagrams per scenario may be helpful
- **Update diagrams as product changes**
- **Enumerate assumptions, dependencies**

Diagram Elements: Examples



Creating Diagrams: Analysis or Synthesis?

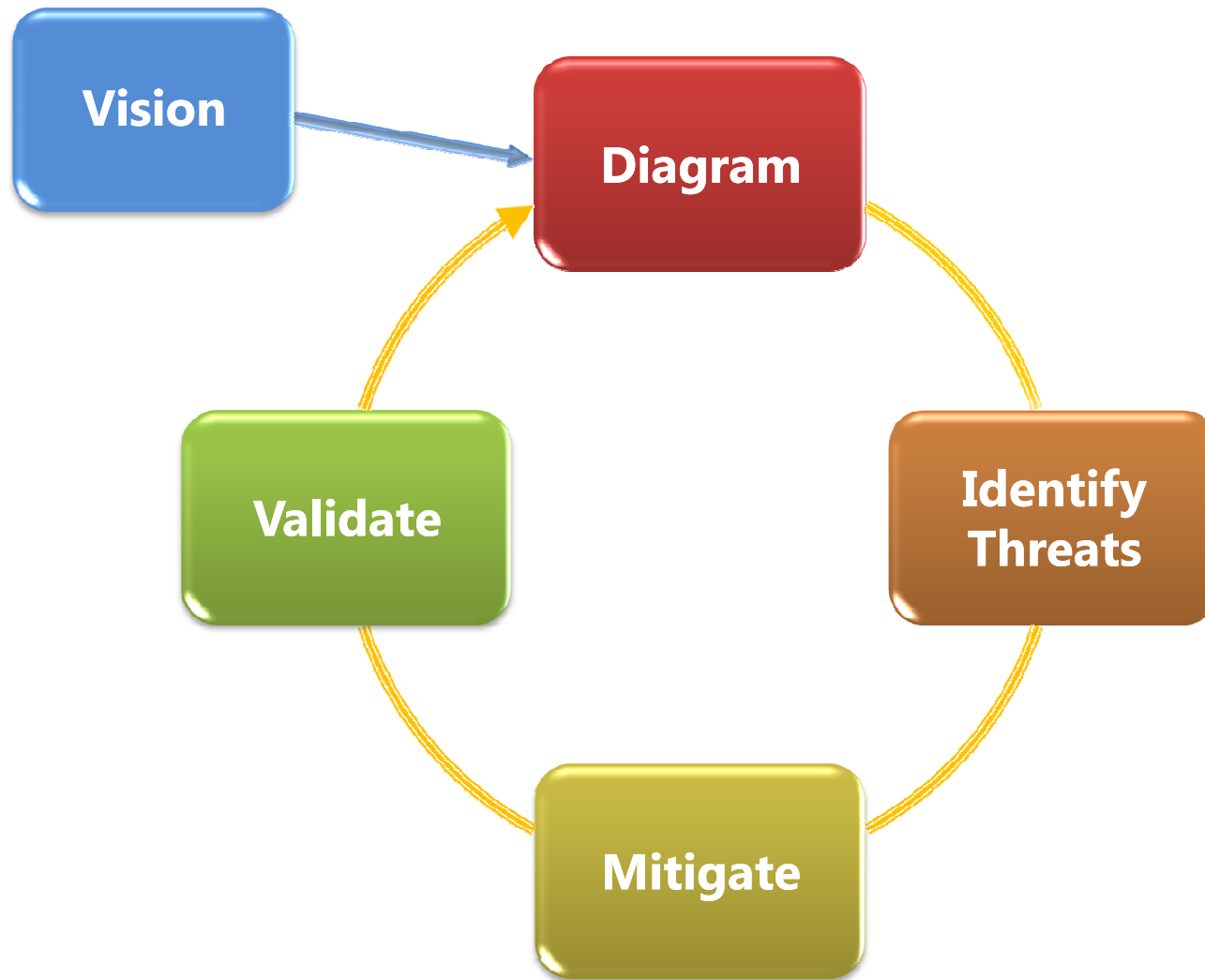
- **Top down**

- Gives you the “context” in context diagram
- Focuses on the system as a whole
- More work at the start

- **Bottom up**

- Feature crews know their features
- Process not designed for syntheses
- More work overall

The Process: Identifying Threats



Identify Threats

- Experts can brainstorm
- How to do this without being an expert?
 - Use STRIDE to step through the diagram elements
 - Get specific about threat manifestation

Threat

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Property we want

Authentication

Integrity

Nonrepudiation

Confidentiality

Availability

Authorization

Threat: Spoofing

Threat	Spoofing
Property	Authentication
Definition	Impersonating something or someone else
Example	Pretending to be any of billg, microsoft.com, or ntdll.dll

Threat: Tampering

Threat Tampering

Property Integrity

Definition Modifying data or code

Example Modifying a DLL on disk or DVD, or a
packet as it traverses the LAN

Threat: Repudiation

Threat	Repudiation
Property	Non-Repudiation
Definition	Claiming to have not performed an action
Example	“I didn’t send that email,” “I didn’t modify that file,” “I certainly didn’t visit that Web site, dear!”

Threat: Information Disclosure

Threat	Information Disclosure
Property	Confidentiality
Definition	Exposing information to someone not authorized to see it
Example	Allowing someone to read the Windows source code; publishing a list of customers to a Web site


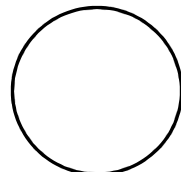


Threat: Denial of Service

Threat	Denial of Service
Property	Availability
Definition	Deny or degrade service to users
Example	Crashing Windows or a Web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole

Threat: Elevation of Privilege

Threat	Elevation of Privilege (EoP)
Property	Authorization
Definition	Gain capabilities without proper authorization
Example	Allowing a remote Internet user to run commands is the classic example, but going from a “Limited User” to “Admin” is also EoP

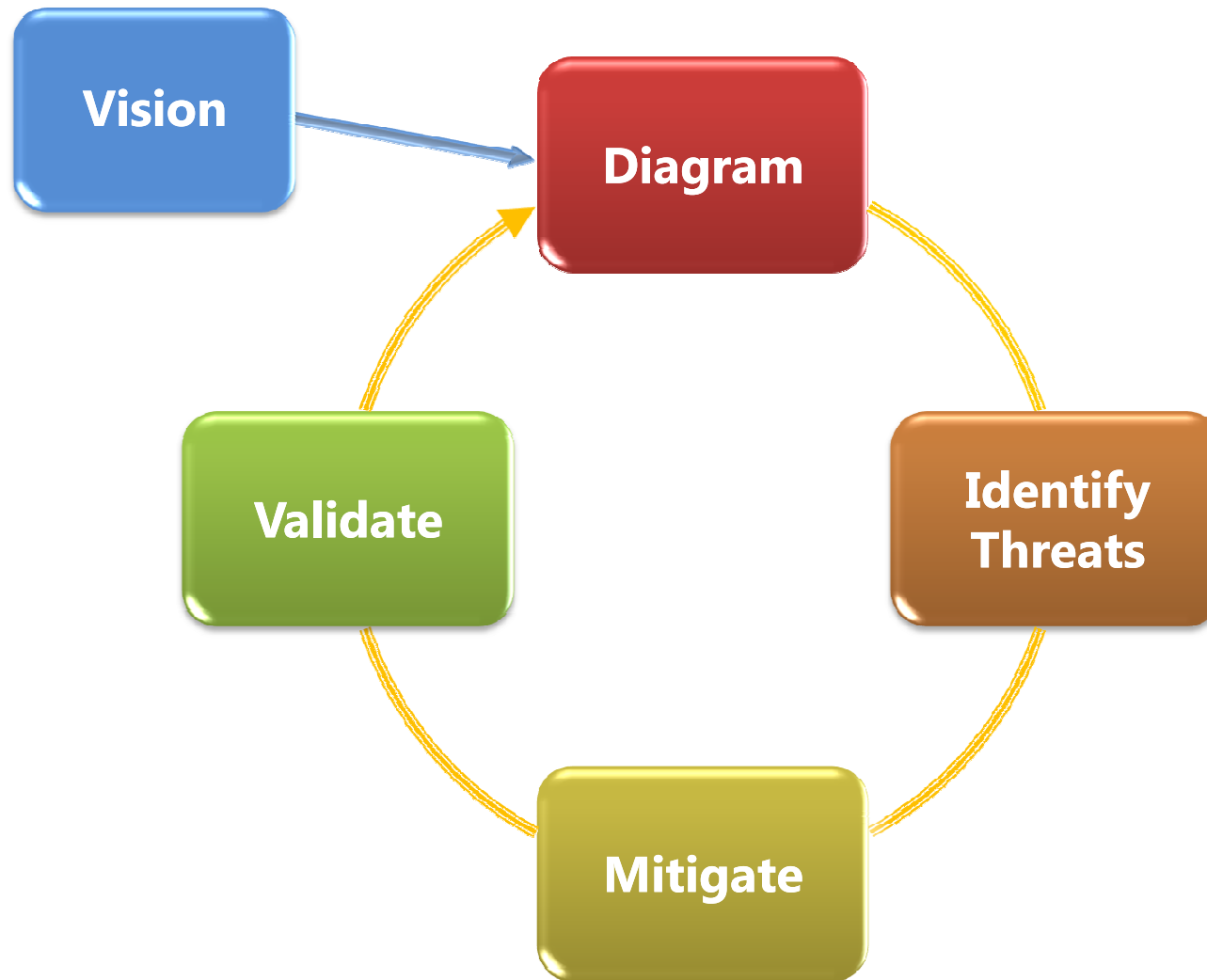
Different Threats Affect Each Element Type

ELEMENT	S	T	R	I	D	E
 External Entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	✓	✓	✓	
 Data Flow		✓		✓	✓	

Apply STRIDE Threats to Each Element

- For each item on the diagram:
 - Apply relevant parts of STRIDE
 - Process: STRIDE
 - Data store, data flow: TID
 - Data stores that are logs: TID+R
 - External entity: SR
 - Data flow inside a process:
 - Don't worry about T, I, or D
- This is why you number things

The Process: Mitigation



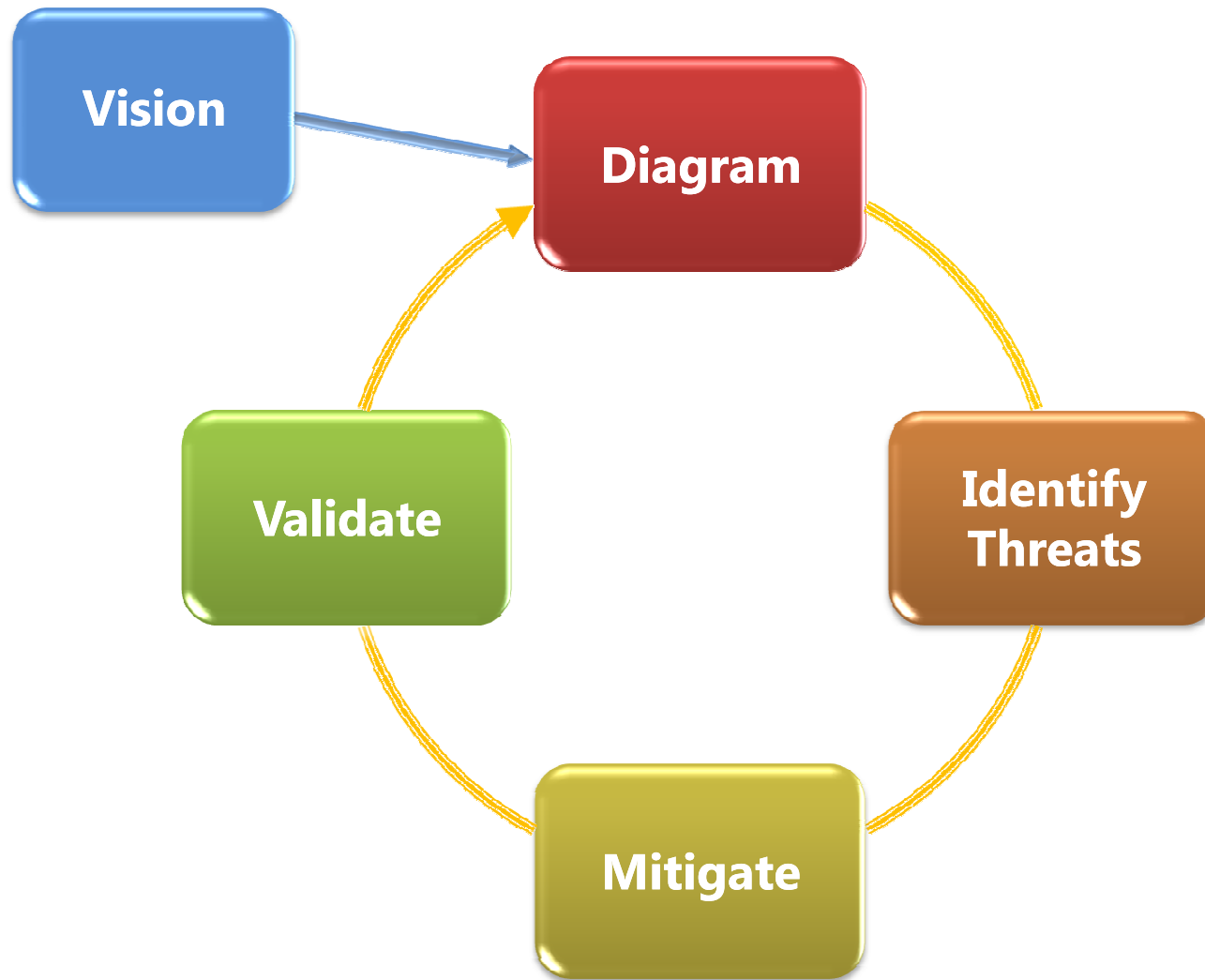
Mitigation Is the Point of Threat Modeling

- **Mitigation**
 - To address or alleviate a problem
- **Protect customers**
- **Design secure software**
- **Why bother if you:**
 - Create a great model
 - Identify lots of threats
 - Stop
- **So, find problems and fix them**

Inventing Mitigations Is Hard: Don't do it

- Mitigations are an area of expertise, such as networking, databases, or cryptography
- Amateurs make mistakes, but so do pros
- Mitigation failures will appear to work
 - Until an expert looks at them
 - We hope that expert will work for us
- When you need to invent mitigations, get expert help

The Process: Validation



Validating Threat Models

- **Validate the whole threat model**
 - Does diagram match final code?
 - Are threats enumerated?
 - Minimum: STRIDE per element that touches a trust boundary
 - Has Test / QA reviewed the model?
 - **Tester approach often finds issues with threat model or details**
 - Is each threat mitigated?
 - Are mitigations done right?

Demo

Call to Action

- Threat model your work!
 - Start early
 - Track changes
- Talk to your “dependencies” about security assumptions
- Learn more

Threat Modeling Learning Resources

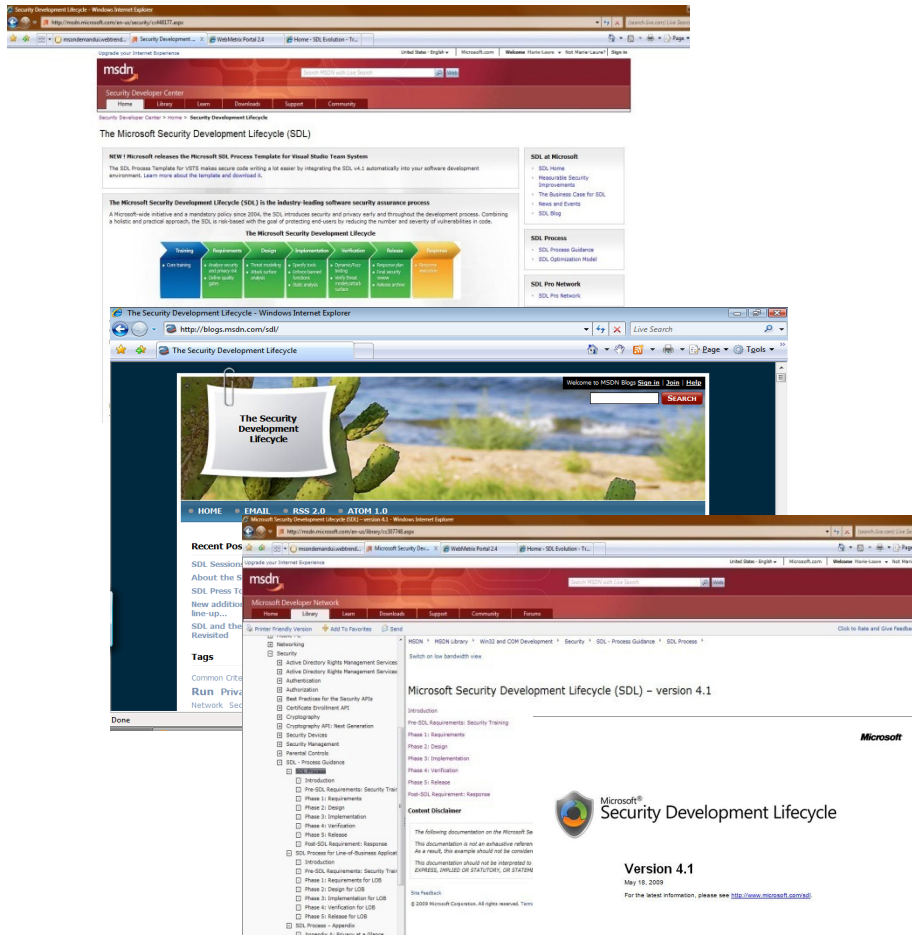
■ MSDN Magazine

- Reinvigorate your Threat Modeling Process
<http://msdn.microsoft.com/en-us/magazine/cc700352.aspx>
- Threat Modeling: Uncover Security Design Flaws Using The STRIDE Approach
<http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx>

■ Books

- The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software (Howard, Lipner, 2006) “Threat Modeling” chapter

Resources



SDL Portal:

<http://www.microsoft.com/sdl>

SDL Blog:

<http://blogs.msdn.com/sdl/>

SDL Process on MSDN

<http://msdn.microsoft.com/en-us/library/cc307748.aspx>

Microsoft IT Information Security

www.msinfosec.com

Microsoft ACE (Assessment, Consulting, and Engineering) team blog

http://blogs.msdn.com/ace_team/

Questions?

