Microsoft Seguridad TI al descubierto

Simon Roses Femerling
ACE Services
Microsoft Corporation

Microsoft | Information Security

¿Quién soy?

- ACE Services en Microsoft
- Ex : PwC, @Stake entre otras…
- Ingeniero Informático, postgrado en Tecnología por Harvard University
- Autor OWASP Pantera
- Ponente: RSA, DeepSec, OWASP y eventos Microsoft
- CISSP, CEH

¡Quién lo iba a decir!

Agenda

- Seguridad Software: Por fin!!
- Security Development Lifecycle (SDL) en TI
- Herramientas Seguridad por la cara!
- Q&A

Seguridad Software: Por fin!!

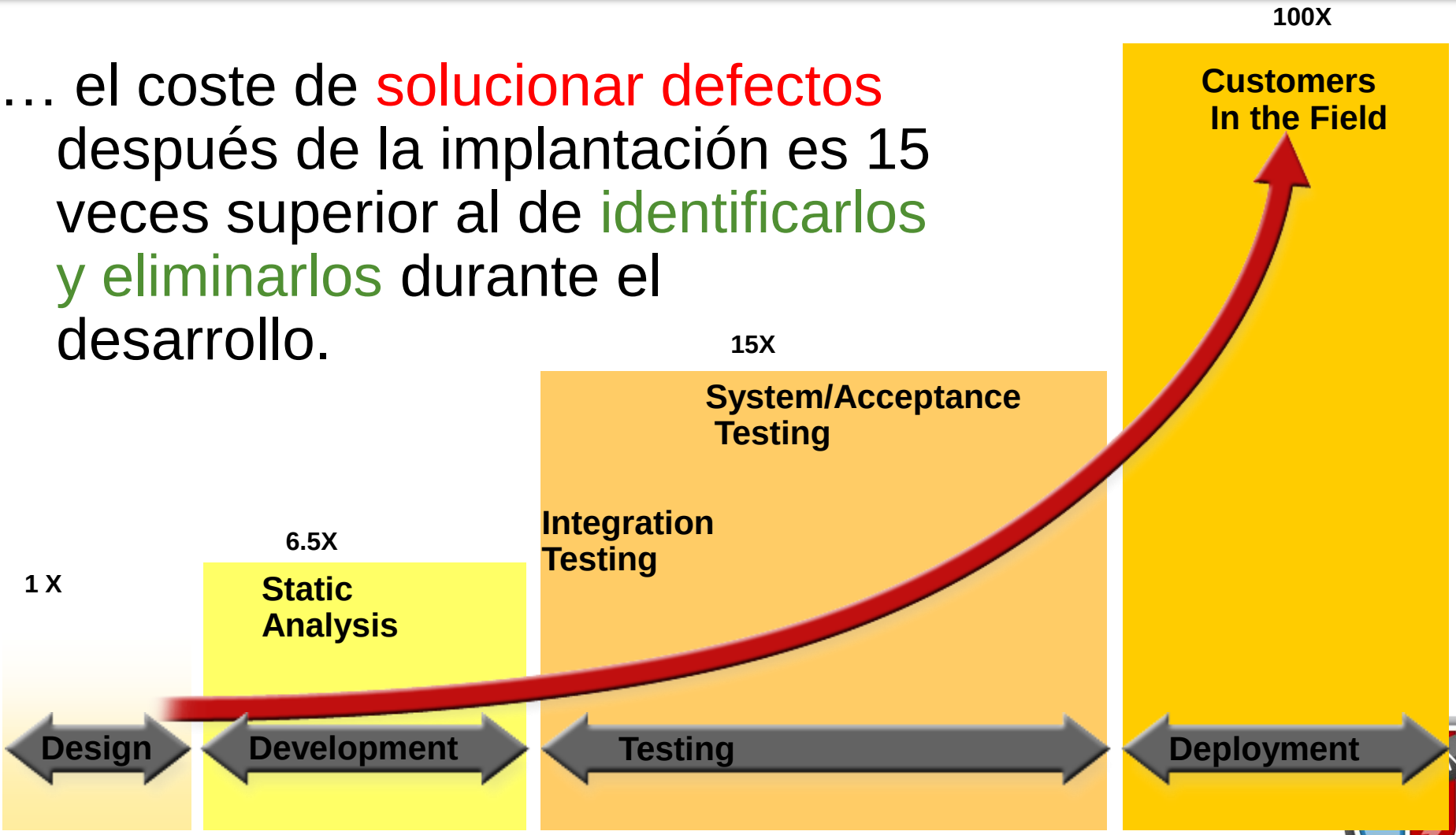
Microsoft | Information Security

Desarrollo de Software

- Arquitectura: Completado
- Diseño: Completado
- Desarrollo: Completado
- Pruebas: Completado
- Revisión Seguridad: ?????

Trauma #1 Seguridad Reactiva

… el coste de solucionar defectos después de la implantación es 15 veces superior al de identificarlos y eliminarlos durante el desarrollo.



Source IDC and IBM Systems Sciences Institute

Trauma #2 Seguridad Reactiva

CNNMoney

40M credit cards hacked

Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards.

June 20, 2005: 3:18 PM EDT
By Jeanne Sahadi, CNN/Money senior writer

MSNBC HOME

Britain warns of major e-mail attack

Hackers seen aiming at government, corporate networks

The Associated Press
Updated: 1:42 p.m. ET June 16, 2005

In 2004, 78% of enterprises hit by viruses, 49% had laptops stolen, 37% reported unauthorized access to information

--2004 CSI and FBI Computer Crime and Security Survey

ACE TEAM

Trauma #3 Seguridad Reactiva

Personas

Frustración, moral baja, conflictos

Efecto colateral

Red corporativa en riesgo

Aprende de lo que Microsoft aprendió

From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

Today, in the developed world, we do not worry about electricity and water services being available. Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

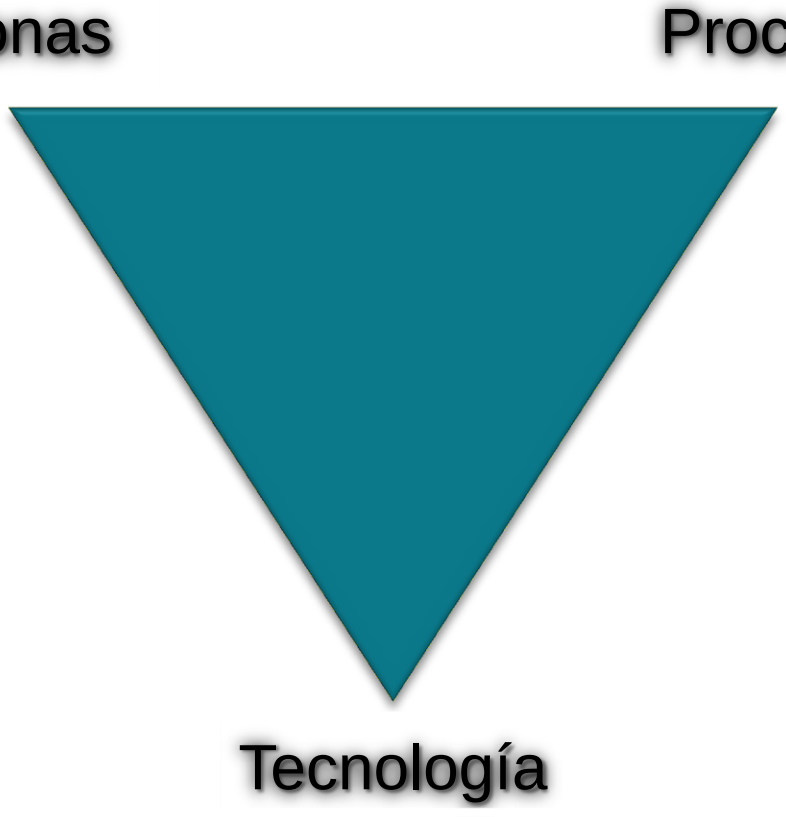
Great features won't matter unless customers trust our software.

So now, when we face a choice between adding features and resolving security issues, we need to choose security.
This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

Security Development Lifecycle (SDL) en TI

Microsoft | Information Security

Seguridad: Tecnología, Procesos y Personas



Framework Seguridad: SD3 + C

Secure by Design

- Modelo de Amenazas
- Revisión Código
- Mejoras de los Procesos

Secure by Default

- Funciones sin uso no predeterminadas
- Reducción de la superficie de ataque
- Privilegios Mínimos

Secure by Deployment

- Mejores Prácticas
- Herramientas Seguridad
- Formación y Concienciación

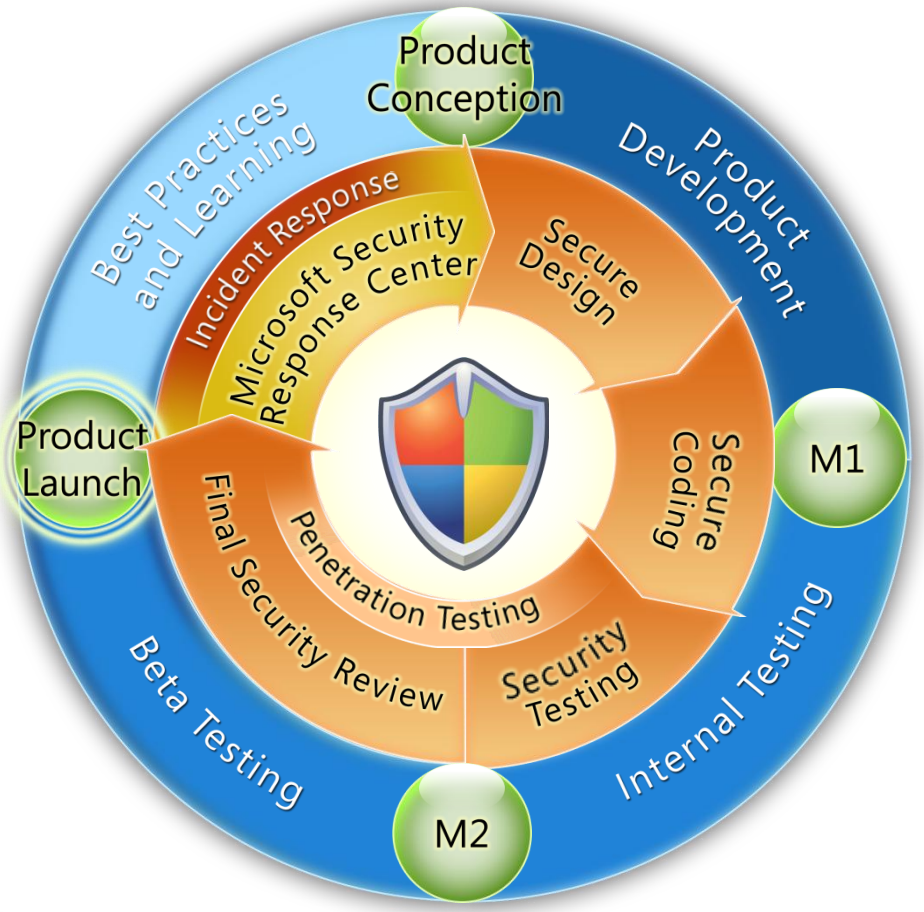
Communications

- Comunidades
- Transparencia
- Política publica

Security Development Lifecycle (SDL)

- Proceso para integrar tareas de seguridad en todo el SDLC
- Variantes SDL
  - SDL = Productos
  - SDL-TI / SDL-LOB = Aplicaciones Negocio
  - SDL/Agile

Security Development Lifecycle (SDL) II



Process

- Defines security requirements and milestones
- MANDATORY if exposed to meaningful security risks
- Requires response and service planning
- Includes Final Security Review (FSR) and Sign-off

Education

- Mandatory annual training – internal trainers
- BlueHat – external speakers on current trends
- Publish guidance on writing secure code, threat modeling and SDL; as well as courses

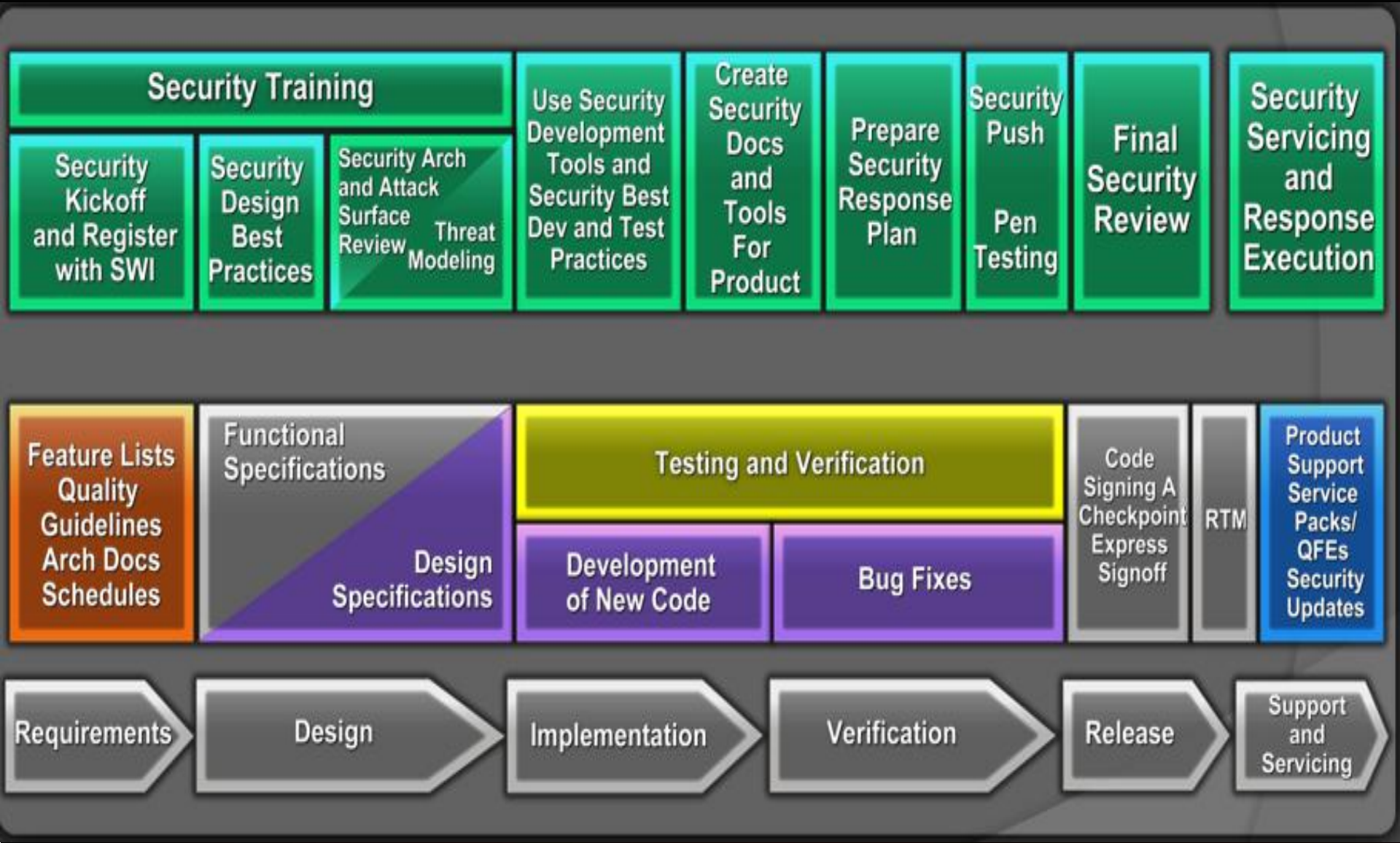
Accountability

- In-process metrics to provide early warning
- Post-release metrics assess final payoff (# of vulns)
- Training compliance for team and individuals

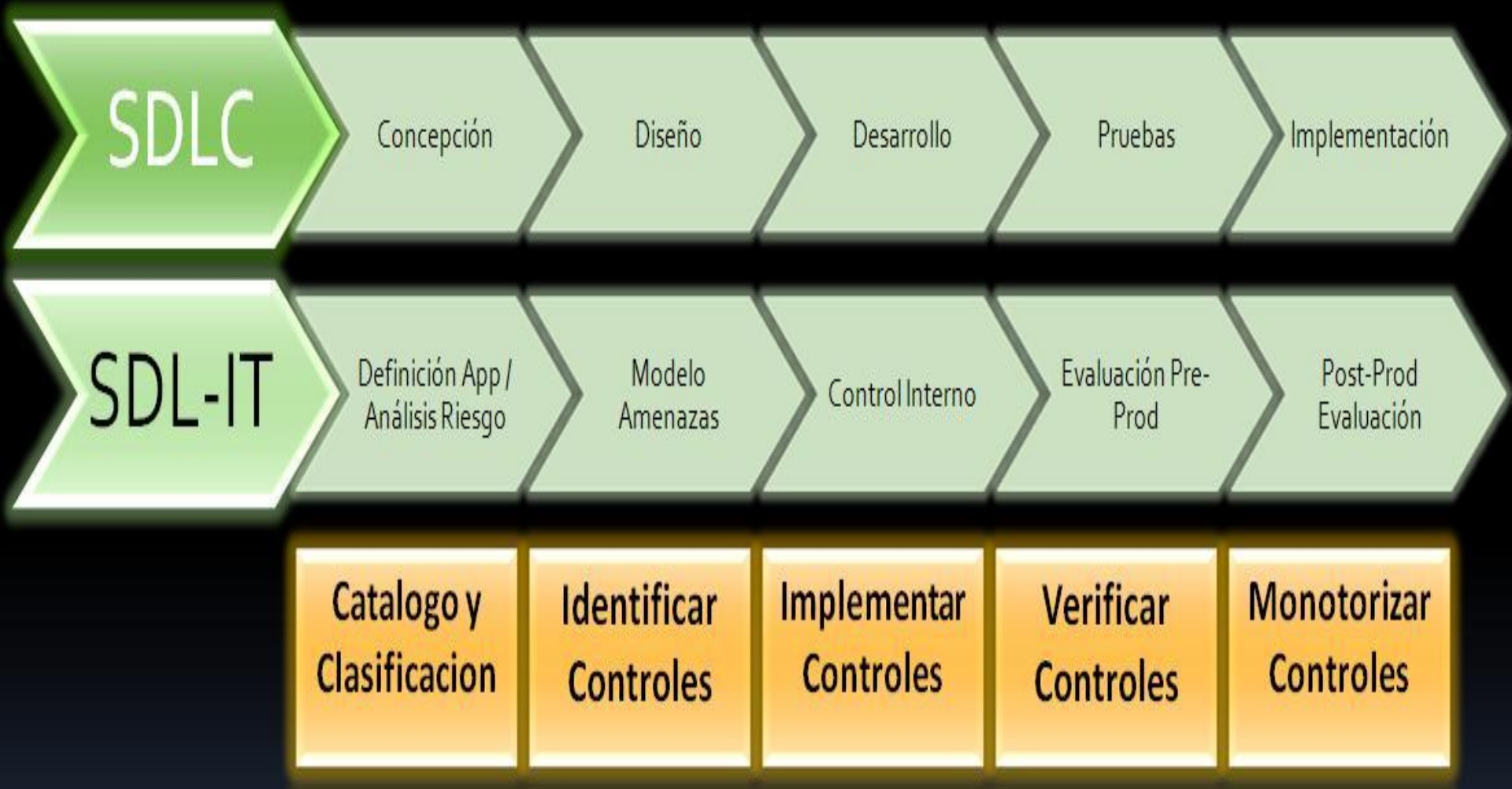
Microsoft Product Development Lifecycle

Microsoft Security Development Lifecycle

SDL


Security Training
Security Kickoff and Register with SWI
Security Design Best Practices
Security Arch and Attack Surface Review
Threat Modeling
Use Security Development Tools and Security Best Dev and Test Practices
Create Security Docs and Tools For Product
Prepare Security Response Plan
Security Push
Pen Testing
Final Security Review
Security Servicing and Response Execution
Feature Lists
Quality Guidelines
Arch Docs
Schedules
Functional Specifications
Design Specifications
Testing and Verification
Development of New Code
Bug Fixes
Code Signing A Checkpoint Express Signoff
RTM
Product Support Service Packs/ QFEs Security Updates
Requirements
Design
Implementation
Verification
Release
Support and Servicing

SDL-TI / SDL-LOB



SDL no es opcional!

- Respaldo de Alta Dirección
- Los grupos de desarrollo trabajan con seguridad
- Proceso formal y documentado
- Formación / herramientas

Arsenal

- Modelo de Amenazas
- Revisiones Diseño
- Revisiones Código
- Implantaciones Seguras
- Análisis estático
- Análisis Dinámico
- Fuzzers
- Pentest
- …

Y esto funciona??

- **SÍ**, aunque no es perfecto está claro que es un proceso continuo y en constante evolución

- Jeff Jones http://blogs.technet.com/security/

Objetivo?

Mejores productos!!!!!!

Herramientas Seguridad por la cara!

Microsoft | Information Security

Ha llegado la Navidad ☺

- Modelo de Amenazas: Threat & Modeling Analysis (TAM)
- Desarrollo Seguro: AntiXSS
- Análisis estático: CAT.NET

Modelo de Amenazas (TM)

Proceso para analizar un sistema y determinar los riesgos potenciales que existen en sus componentes y datos

Beneficios TM

- Seguridad desde el principio, en fase diseño
- Los riesgos son mitigados antes de escribir código
- Reducir el coste de solucionar fallos antes que más tarde

TM pasos básicos

- **Quién?** Tu y tu equipo debéis crear el TM
- **Qué?** Proceso para identificar y mitigar riesgos en tu producto
- **Cuándo?** En la fase de diseño antes de desarrollo (básicamente antes de escribir código!!)
- **Por qué?** Para desarrollar productos seguros desde el principio
- **Cómo????** TAM es tu amigo ☺

TM Proceso

Identificar Activos

Definición Arquitectura

Descomposición Aplicación

Identificar Riesgos

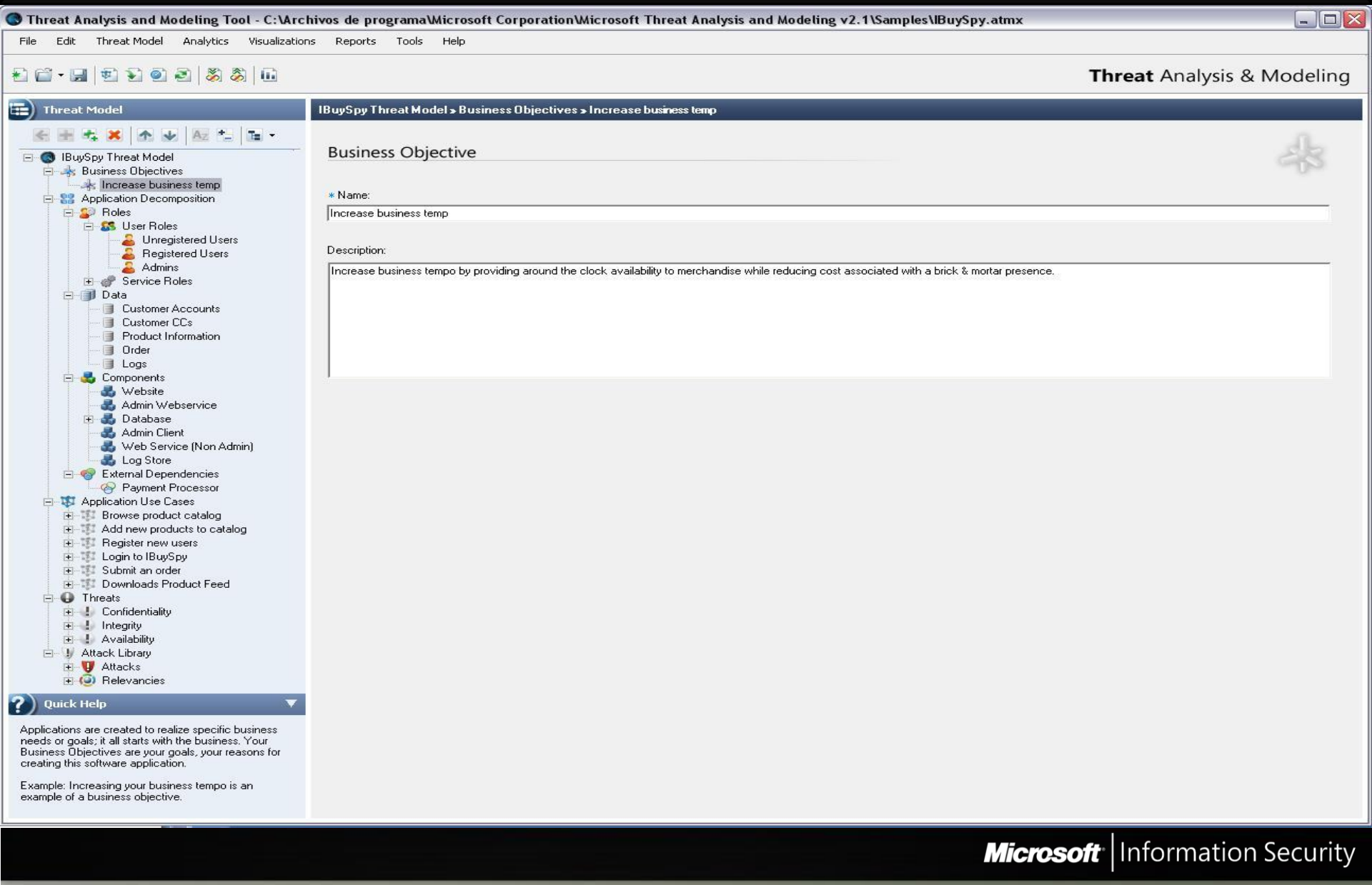
Clasificar Riesgos

Documentar Riesgos

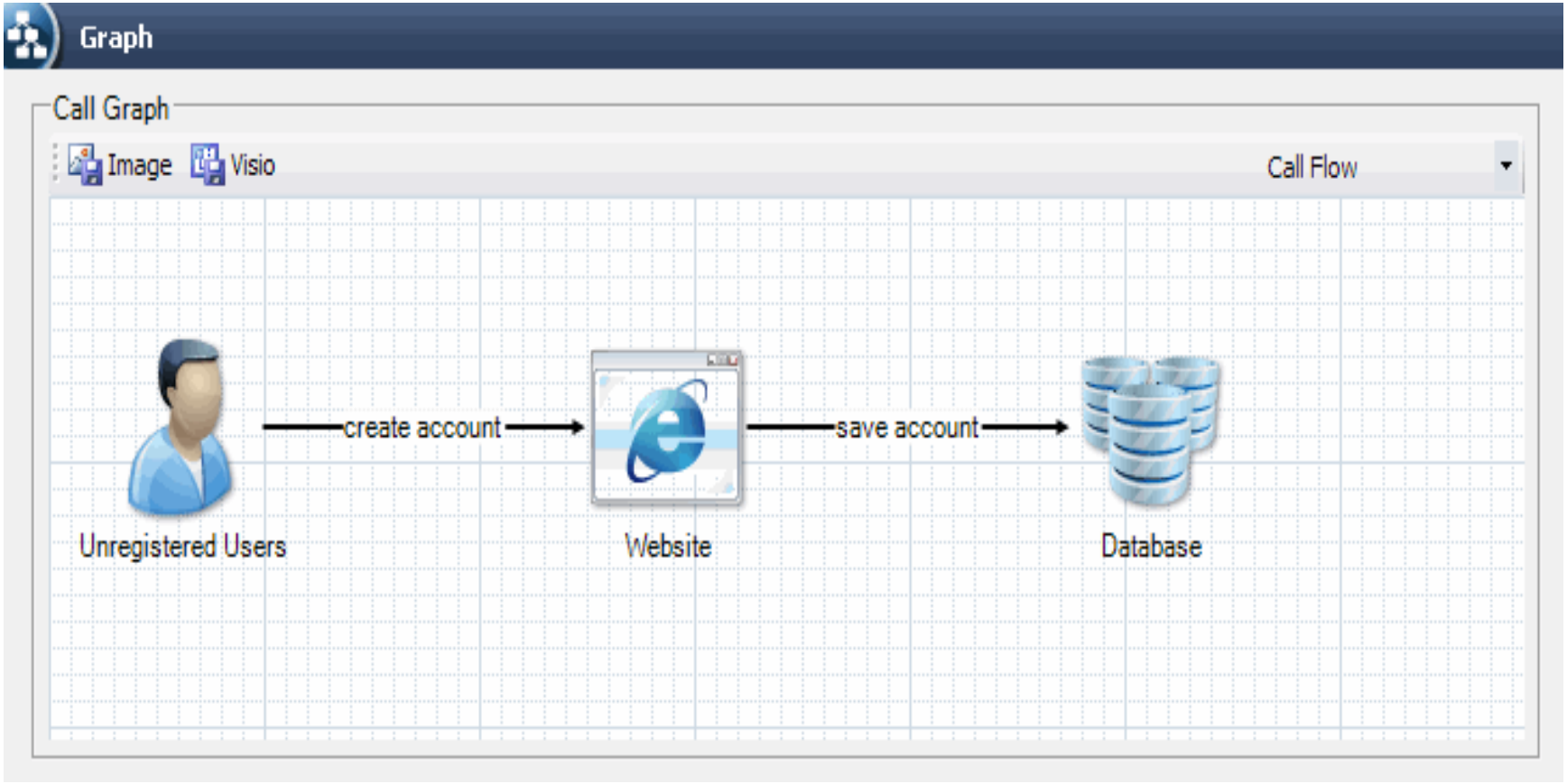
Threat & Modeling Analysis (TAM)

- TAM es una potente herramienta que facilita la creación de TM-LOB
- Utiliza CIA
- Perspectiva desde el desarrollador
- Librería de Ataques
- Análisis y Visualización

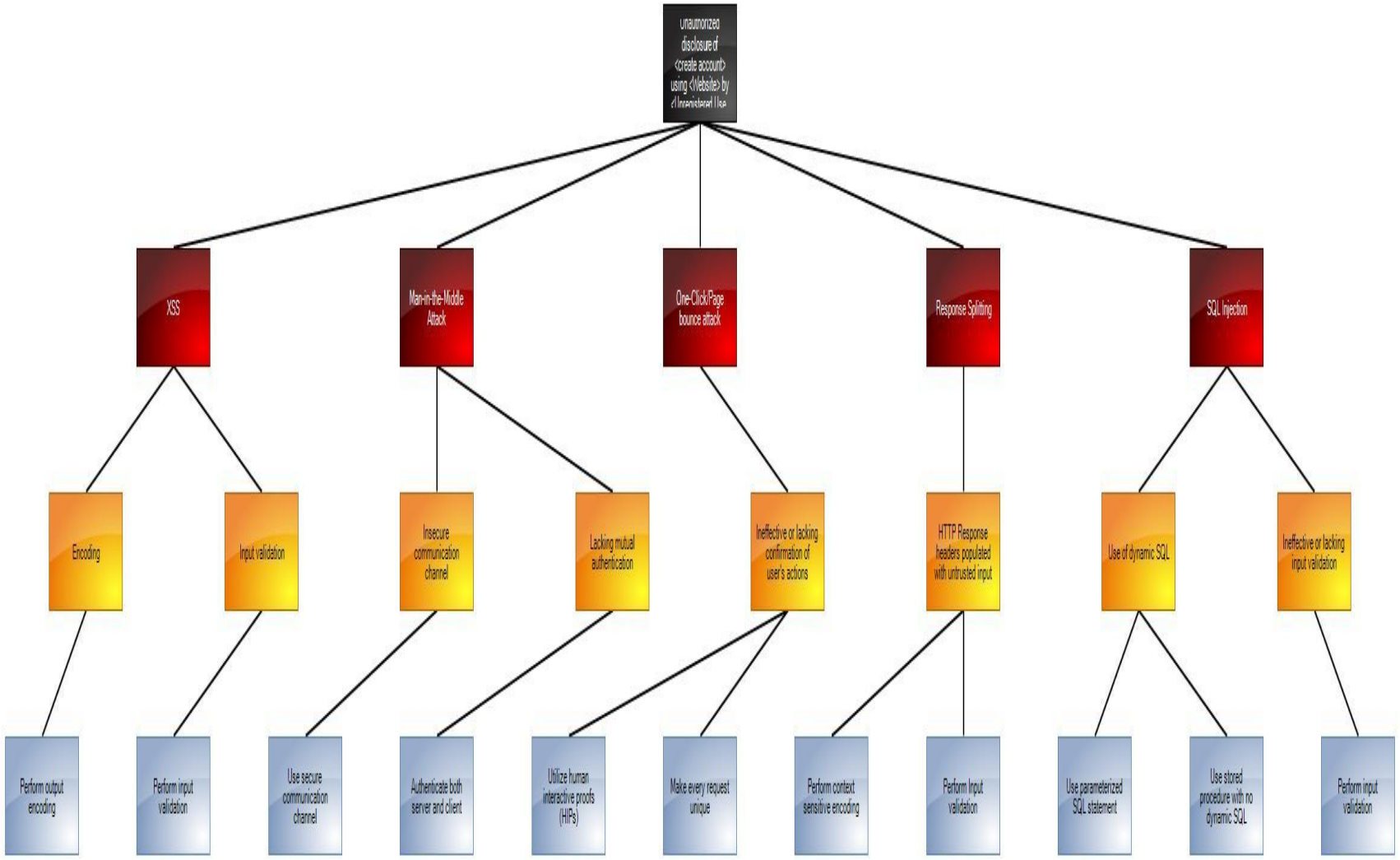
TAM GUI


Threat Analysis and Modeling Tool - C:\Archivos de programa\Microsoft Corporation\Microsoft Threat Analysis and Modeling v2.1\Samples\IBuySpy.atmx
File
Edit
Threat Model
Analytics
Visualizations
Reports
Tools
Help
Threat Analysis & Modeling
Threat Model
IBuySpy Threat Model
Business Objectives
Increase business temp
Application Decomposition
Roles
User Roles
Unregistered Users
Registered Users
Admins
Service Roles
Data
Customer Accounts
Customer CCs
Product Information
Order
Logs
Components
Website
Admin Webservice
Database
Admin Client
Web Service (Non Admin)
Log Store
External Dependencies
Payment Processor
Application Use Cases
Browse product catalog
Add new products to catalog
Register new users
Login to IBuySpy
Submit an order
Downloads Product Feed
Threats
Confidentiality
Integrity
Availability
Attack Library
Attacks
Relevancies
Quick Help
Applications are created to realize specific business needs or goals; it all starts with the business. Your Business Objectives are your goals, your reasons for creating this software application.
Example: Increasing your business tempo is an example of a business objective.
IBuySpy Threat Model > Business Objectives > Increase business temp
Business Objective
* Name:
Increase business temp
Description:
Increase business tempo by providing around the clock availability to merchandise while reducing cost associated with a brick & mortar presence.

Casos de Uso TAM



TAM SecGraph



AntiXSS

- Validación de datos .NET
- Lista Blanca
- URL, JS, XML, etc…
- Disponible 1.5 pero 3.0 en las próximas semanas!!!!

Metodología AntiXSS

- **1 Paso**: Revisar el código ASP.NET con información de entrada y salida
- **2 Paso**: Determinar si esta información es controlada por el usuario
- **3 Paso**: Determinar el contexto de la información
- **4 Paso**: Validar apropiadamente

Uso de AntiXSS 1.5

#1
// Vulnerable code
// Note that un-trusted input is being as an HTML attribute
Literal1.Text = “<hr noshade size=**[un-trusted input here]**>”;

// Modified code
Literal1.Text = “<hr noshadesize=”+Microsoft.Security.Application.AntiXss.HtmlAttributeEncode(**[un-trusted input here]**)+”>”;
#2

```
<html>
 <b>
  Hello, <%= AntiXss.HtmlEncode(Request.Form[“UserName”]) %>
 </b>
</html>
```

AntiXSS 3.0

- Validación XHTML
- Mejoras en rendimiento
- Security Runtime Engine (SRE)

Security Runtime Engine (SRE)

- Protege las aplicaciones web ASP.NET
- Se ejecuta como un modulo http_module en IIS 6.0 / 7.0
- Protección contra XSS
- Fácil de implantar / configurar

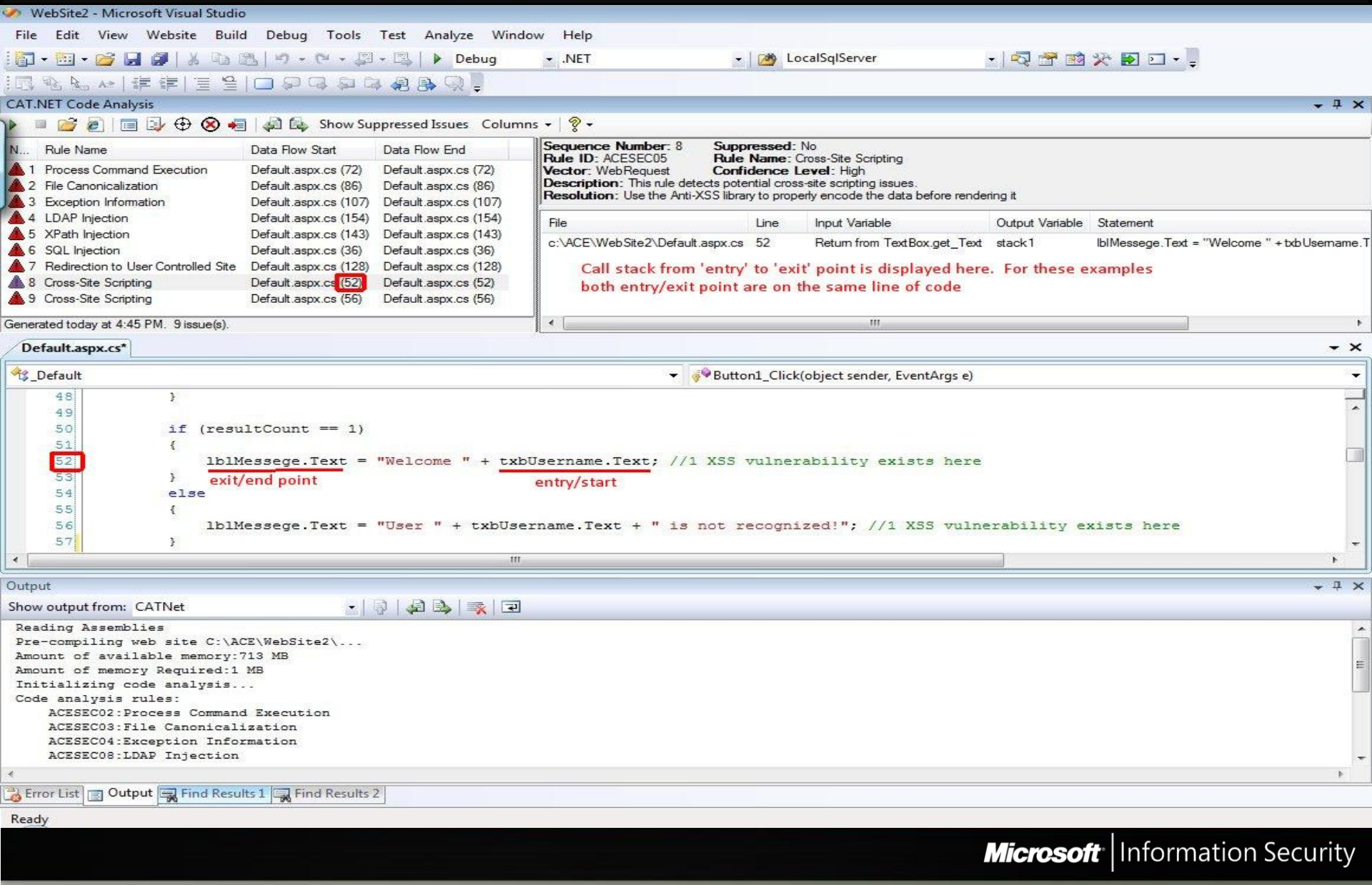
CAT.NET

- Análisis Estático en .NET
- Uso obligatorio en MS
- CAT.NET detecta *Exploitable Code Paths*
- Integración VS2005 / VS2008 o cliente independiente

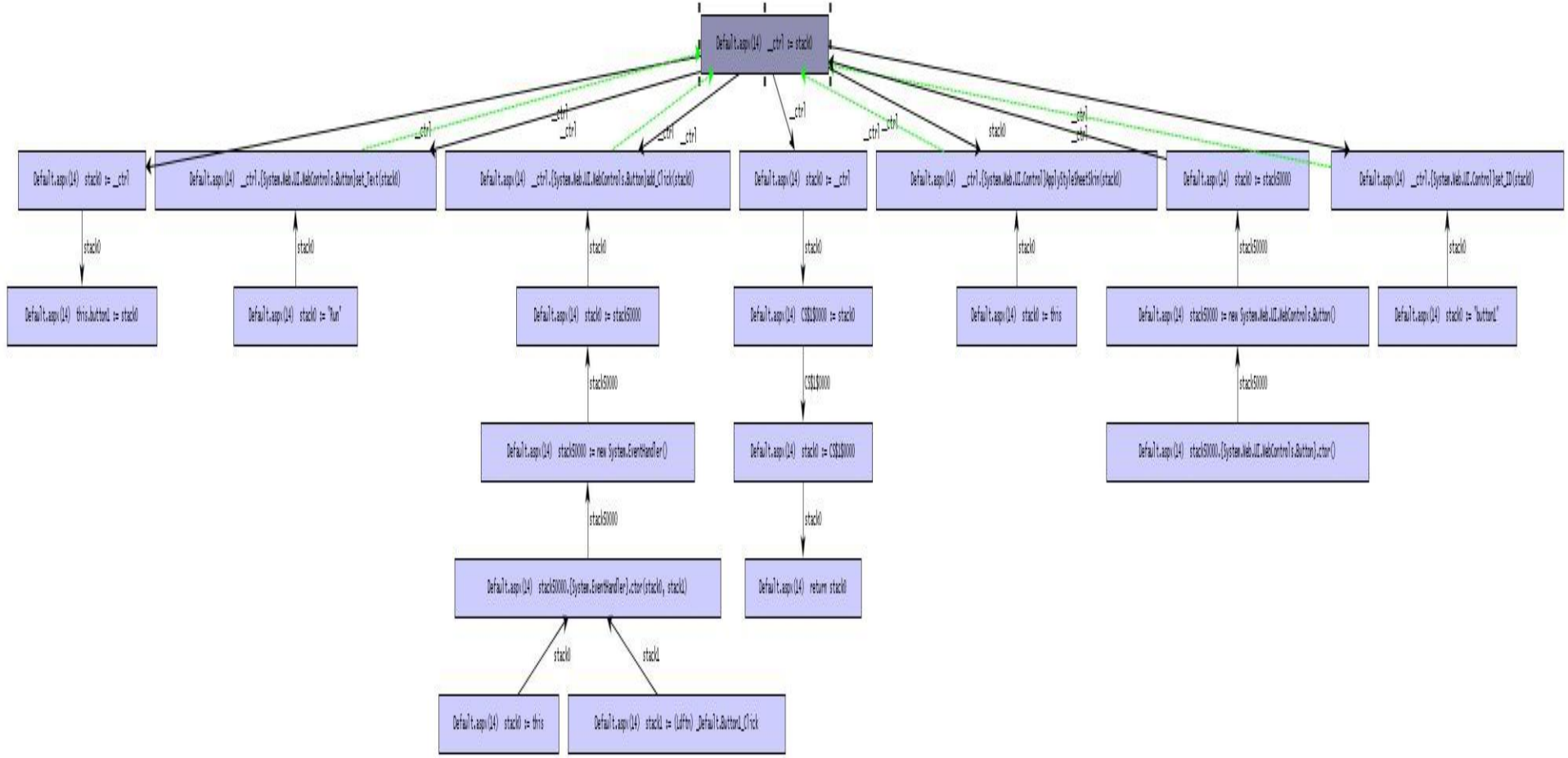
Vulnerabilidades en código

- CAT.NET actualmente identifica:
  - SQL Injection
  - LDAP injection
  - Xpath Injection
  - Cross-Site Scripting (XSS)
  - File Canonicalization
  - Exception Information
  - Process Command
  - Redirection

CAT.NET en acción!



Una imagen vale más que 1000 palabras…



Enlaces

- Threat Analisys & Modeling (TAM): http://www.microsoft.com/downloads/details.aspx?FamilyId=59888078-9DAF-4E96-B7D1-944703479451&displaylang=en
- Documento de cómo Ford Motors utiliza TAM para identificar y mitigar riesgos en sus proyectos. https://buildsecurityin.us-cert.gov/daisy/bsi/resources/published/articles/932-BSI.html
- Demo de nuestra herramienta de análisis de código fuente, detecta vulnerabilidades Cross Site Scripting (XSS) para .NET http://www.microsoft.com/Downloads/details.aspx?FamilyID=19a9e348-bdb9-45b3-a1b7-44ccdcb7cfbe&displaylang=en
- AntiXSS: librería para desarrollo seguro en .NET, validación de datos http://www.microsoft.com/downloads/details.aspx?FamilyId=EFB9C819-53FF-4F82-BFAF-E11625130C25&displaylang=en
- Security Development Lifecycle (SDL) http://www.microsoft.com/downloads/details.aspx?familyid=2412c443-27f6-4aac-9883-f55ba5b01814&displaylang=en
- SDL TM http://msdn.microsoft.com/en-us/security/dd206731.aspx

Blogs

- ACE Team
  http://blogs.msdn.com/ace_team/default.aspx
- Threat Modeling http://blogs.msdn.com/threatmodeling/
- SDL http://blogs.msdn.com/sdl/
- CISG http://blogs.msdn.com/cisg/

Fin

- Q&A

- Importante: Cerveza / cubatas (vodka limón, Margaritas, Mojitos, etc…) son siempre bienvenidos ☺

- Simon Roses Femerling
simonros@microsoft.com

Microsoft®

Your potential. Our passion.™