Security: When and what?

- Design
- Development
- Testing
- Secure by design
- Secure by default
MSF Agile + SDL 5.0 in Team Foundation Server

+ SDL Threat Modeling Tool
WPL

- Web Protection Library

- AntiXSS
  - White Lists
  - Secure Globalization

- Security Runtime Engine
  - Cross Site Scripting
  - SQL Injections
Static Code Analysis

■ FxCop
  ▸ Analysis of performance, design and security issues
  ▸ Primarily focused on Code Access Security

  "Have you used security features the right way?"

■ CAT.NET - Code Analysis Tool
  ▸ Previously only an internal tool

  "Have you written your other features securely?"
Pex and Moles

- Pex automatically generates test suites
  - High code coverage
  - Interesting input/output values

- Moles allows to replace .NET methods with delegates
WACA

- Web Application Configuration Analyzer
  - CAT.NET 2.0
  - IIS and .NET Framework
  - SQL Server
  - Windows Permissions

- Export report
  - Excel, HTML, TFS

- Remote scans
CodeContracts

- Express coding assumptions
  - Pre-conditions
  - Post-conditions
  - Object invariants

- Static and runtime checking

- Documentation Generation
How to keep updated!

blogs.msdn.com/securitytools

msdn.microsoft.com/security

msdn.microsoft.com/practices

www.codeplex.com

msdn.se