



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



Category 'Best
Security Company'

SDL
Consultancy
Solutions

SDL Consultancy Solutions

NGSSoftware offers consultancy solutions in line with the key stages of the Security Development Lifecycle:

» Training

Training Needs Assessment:

- » Assessment of the basic security training needs for an organization in line with Microsoft Education & Awareness guidelines for Secure Design, Threat Modeling, Secure Coding, Security Testing and Privacy.
- » Recommendations for appropriate training at developer, tester, program / project manager and upper management levels.

Core Training:

- » Introduction to the Microsoft Security Development Lifecycle - A formal introduction to the concepts and practices of SDL, taking a novice to a practitioner in easy steps.
- » Introduction to Threat Modeling - Providing grounding in the important area of Threat Modeling, demonstrating how the process works, where benefit is gained and giving guidance for good threat models that meet the quality bar.
- » Basics of Secure Design, Development and Testing - The core concepts behind the SDL: goals and techniques for each area of practice, spliced with real world experience from technical instructors.
- » Privacy in Development - An introduction and grounding in the often overlooked area of Privacy as it relates to secure development. Never before have Privacy concerns been so topical; this training explains how to avoid the pit falls of securing private data.

» Requirements

- » Security Requirements - Identification and enumeration of appropriate security and privacy functionality for a given software project or sub-feature.
- » Design Requirements - Validation of technical design specifications to ensure appropriate considerations relative to the security requirements for a given software project or sub-feature.
- » Quality Gates - Creation and assessment of appropriate security and privacy quality measures such as "bug bars" and other quality metric.

» Design

- » Threat Modeling - The creation of Threat Models for security / privacy critical components using the STRIDE threat classification taxonomy.
- » Attack Surface Reduction - Identification and enumeration of the potential attack surface area for a given software project or component and make recommendations to reduce the attack surface.

» Implementation

Security Tools:

- » Identification and specification of the appropriate security tools based on the project type (e.g. managed vs. native code).
- » Guidance on the quality and applicability of available commercial and open source tools and make appropriate recommendations on adoption and use.

Banned Functions:

- » Clear explanation and rationale for deprecation of unsafe functions and guidelines for efficient ways to implement restrictions within the development environment. Recommendations for safe replacements, alternatives and complimentary development tools.

Static Analysis:

- » Identification and specification of appropriate static analysis tools to perform analysis of a given software project or sub-feature.
- » Triage and classification of static analysis tool output; identification of security vulnerabilities, code quality issues, false positives and false negatives as appropriate.
- » Clear explanation of results and contextual prioritization of problem resolution.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

**SDL
Consultancy
Solutions**

SDL Consultancy Solutions

» Verification

Dynamic Analysis:

- » Identification and specification of appropriate dynamic analysis test tools to perform analysis of a given software project or sub-feature.
- » Triage and classification of dynamic analysis tool output; identification of security vulnerabilities, false positives and false negatives as appropriate.
- » Clear explanation of results and contextual prioritization of problem resolution.

Fuzzing (Fuzz Testing):

- » Identification and specification of appropriate fuzz test tools to perform fuzz testing analysis of a given software project or sub-feature.
- » Triage and classification of fuzz testing results; identification of security vulnerabilities, false positives and false negatives as appropriate.
- » Clear explanations of results and contextual prioritization of problem resolution.

Threat Model Review:

- » Identification of points of divergence between original threat modeling and "code complete" projects - or the identification of threat modeling deficiencies as appropriate.
- » Concise and precise updates to threat model documents to reflect design / threat changes.
- » Identification of mitigations and/or recommended fixes for any vulnerabilities found.

Code Review:

- » Perform insightful review of source code to discover security vulnerabilities.

» Release

Incident Response Planning:

- » Creation of incident response planning that outline processes such as 24x7x365 contact information and incident escalation paths for engineering, marketing and management.
- » Provide plans and means to service all code including "out-of-band" releases and all licensed 3rd party code.

Final Security Review:

- » Create the plans for, or conduct a Final Security Review that includes the review of all threat models, validation of results from security tools, the review of all unfixed / declined security bugs and the review of exception requests.

Project Archiving:

- » Assist and advise on the archiving of security artifacts such as code symbols, threat models, Final Security Report, Final Project Sign-off Report, Incident Response Plans etc.

» Response & Operations

- » Assist in the provisioning of response solutions and the guidance for daily operation and administration tasks, where the software project is to be operated in-house, rather than an entity to be shipped.

To contact NGSSoftware to discuss the SDL Consultancy Practice in support of the Microsoft Security Development Lifecycle in your organization, or to engage NGSSoftware in SDL Consultancy under the Microsoft SDL Pro Network, please use the following details:

» Contact Details

Web: www.ngsssoftware.com/consulting/sdl/

Contact: sdl@ngsssoftware.com

NGSSoftware SDL Practice Manager: Kev Dunn
UK Head Office (London)
Next Generation Security Software Ltd
52 Throwley Way
Sutton
Surrey, SM1 4BF
United Kingdom

Tel: +44 (0)208 401 0070
Fax: +44 (0)208 401 0076

Copyright 2008, Next Generation Security Software Ltd. All rights reserved. Other marks and trade names mentioned are the property of their respective owners, as indicated. All marks are used in an editorial context without intent of infringement.