



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

Category 'Best
Security Company'

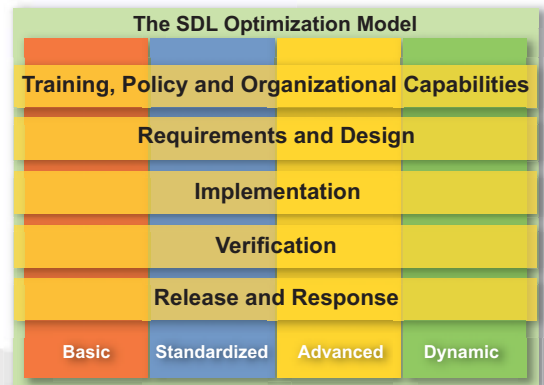
SDL:
Customization and
Optimization

SDL: Customization and Optimization

» Tailoring the Security Development Lifecycle for Your Organization

It is the goal of NGSSoftware to help organization's adopt as many of the principles of SDL as is possible, applicable and achievable for that organization's specific case. It is rare for any two companies to have the same needs, restrictions or overheads and as such the implementations of lifecycle goals must be optimized and customized to tailor a model that works for you. By using the SDL Optimization Model, NGSSoftware are able to:

- » Enable organizations outside of Microsoft to create more secure, and privacy enhanced software by successfully implementing SDL in a way that has no detrimental impact to operations.
- » Allow organizations to self-assess current software development security practices (after all, you know them better than anyone!) and create a strategy for gradual improvement.
- » Provide a consistent and effective framework for SDL consultancy services that in turn provides *effective SDL implementation* and a *mechanism for measuring progress*.



» Measuring SDL Maturity Levels

To understand where an organization is with current SDL activities and to gain a picture of where development and uptake can be achieved over time, the SDL Optimization Model sets maturity levels to be measured against when planning for progress:

- » **Basic** - Characterized by manual, voluntary or localized processes; minimal central control and nonexistent, undefined or unenforced policies and standards for secure architecture, design, development, testing, compliance and other common security practices. Overall security health of applications and services is often unknown due to a lack of security tools and resources and where security practices exist they are considered ad-hoc or are mainly reactive and driven by external pressures.
- » **Standardized** - This level of maturity is characterized by security practices and standards being introduced into the development lifecycle. Organizations at this level are able to assess the security and privacy risk of new projects and select the best candidates for implementing security and privacy practices into the development lifecycle. In general, the organization has realized the value of basic standards and policies, yet still has significant room to improve. Security and privacy practices are still only applied to pilot projects or suitable candidates, and executive support for effort is considered tacit. Where companies find themselves at this level, much of the SDL effort is still spent in the later phases of the lifecycle and in security response, where improvements come at a higher cost than more integrated and proactive practices can deliver at high optimized levels.
- » **Advanced** - Advanced level represents the minimum set of tasks necessary for a claim of adherence to the Microsoft SDL or the core principles behind it. At this level, executive support is explicit and all new and high risk projects fall under the mandate for SDL practices and quality gates. Security and privacy practices are integrated throughout the software development lifecycle and each feeds into the next, getting the most out of all efforts. Security testing guidelines are in place and tools are effectively used to reduce costs. Security response is rapid and controlled with the application of security and privacy efforts at earlier lifecycle phases, assisting in reducing the overall cost of producing secure software.
- » **Dynamic** - Companies with dynamic SDL processes are acutely aware of the strategic value that a fully-realized SDL provides in helping them protect customers, staff or business operations in general, innovate efficiently and stay ahead of competitors. Unlike at the Advanced level where SDL practices are still targeted only to certain products and projects, organizational training goals are in place and the mandate for secure software at this level covers all applicable projects across the entire organization. Increasing security assurance is attained with each release cycle and legacy systems have been brought into compliance. Teams have internalized, developing secure software and many practices proceed without assistance from security expertise external to that team. Security effort can be focused on proactive innovation and tool customizing in addition to reactive incident response.



» SERVICES



THE QUEEN'S AWARDS
FOR ENTERPRISE:
INTERNATIONAL TRADE
2007



AWARDS
2008
EUROPE
WINNER

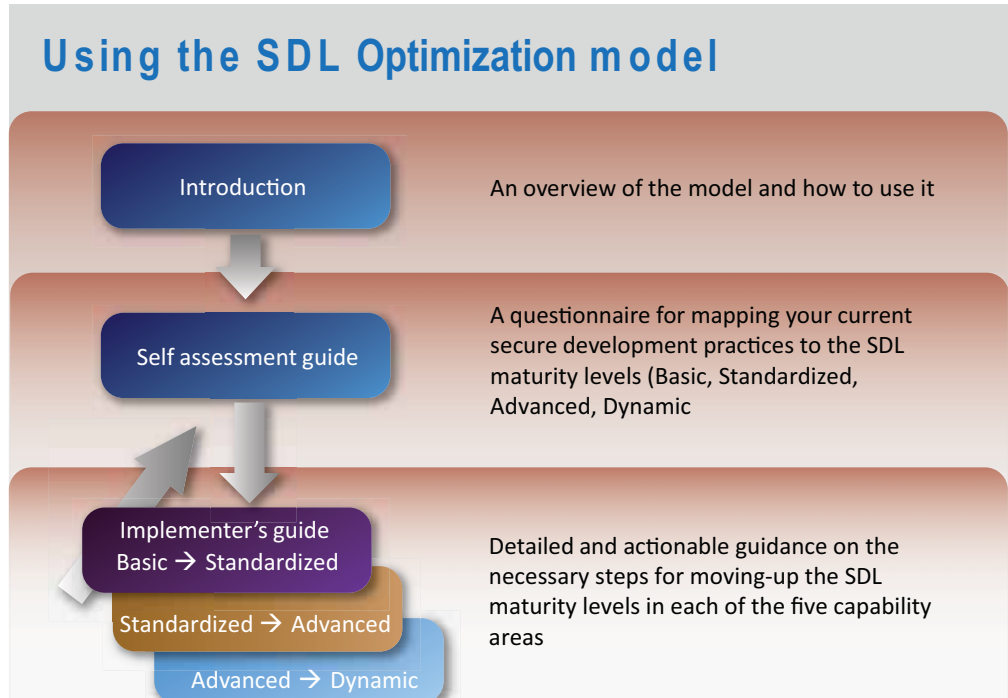
Category 'Best
Security Company'

SDL:
Customization and
Optimization

SDL: Customization and Optimization

» Using the SDL Optimization Model

NGSSoftware are able to assist and guide an organization through the adoption of SDL, using a format of the SDL Optimization model provided by Microsoft:



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