

Case study/page 1

End-to-End Application Security Work for a Major European Client

Luxoft's Application Security Team integrates into the Secure Development Lifecycle operated by the client to ensure compliance to a range of security requirements, including in-house policies, PCI DSS and data protection legislation

Protecting the sensitive data collected, transmitted, stored and processed within IT systems requires utmost attention to application security throughout the development lifecycle. While the ways of doing this in various settings are well understood by now, actually operating a full end-to-end application security process is often prohibitively expensive. The high cost of application security is explained by the nature of the technical skills required for this work and by the scarcity of specialists with the security-oriented mindset and relevant experience. Most companies facing this problem settle for a compromise and operate a reduced set of application security activities, hoping that the savings achieved this way can justify the risks involved. A major European company decided to take a different approach: it operates a fully-fledged application security process at an acceptable cost by doing most of its application security work from a nearshore facility operated by its partner Luxoft.

The engagement model in this case is nearshoring rather than outsourcing: the client owns all the processes involved and directly manages the personnel supplied by Luxoft, who effectively form part of the in-house Application Security Team. Only a few members of the overall team are based in Western Europe, which is what makes the overall cost of the team acceptable to the client. Luxoft plays a major role in hiring and training application security specialists and in maintaining a secure environment in which their highly sensitive work can be done safely.

Client:

A major European company with some 30 million customers

Summary:

The client needs to operate a full end-to-end Application Security process for its in-house IT systems at an acceptable cost.

Challenge:

Find the perfect IT partner capable of performing the full cycle of Application Security activities required by an industrial-strength Secure Development Lifecycle.

Tools:

- ◆ HP Fortify
- ◆ HP WebInspect
- ◆ HP QualityCenter
- ◆ WebScarab
- ◆ Wireshark
- ◆ Burp Suite
- ◆ Security browser plugins

Platforms:

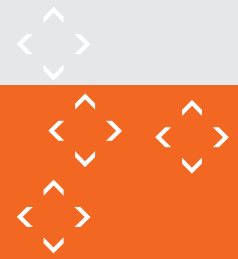
- ◆ RedHat & CentOS Linux
- ◆ MS Windows
- ◆ iOS
- ◆ Android
- ◆ Symbian

Applications in scope:

- ◆ WEB-based
- ◆ SOA-based
- ◆ Mobile clients
- ◆ Desktop

Programming languages:

- ◆ Java
- ◆ .NET
- ◆ C/C++
- ◆ Objective C
- ◆ PHP
- ◆ SQL & PL/SQL



Case study/page 2

The Application Security team operates a robust end-to-end process integrated into the client's Secure Development Lifecycle. The key activities performed by the nearshore members of the team are as follows:

- ◆ Providing advice and guidance to development teams in performing Application Security analysis and Threat Modelling for business requirements and technical designs. Reviewing the reports resulting from this analysis.
- ◆ Reviewing business requirements and technical designs for compliance to the relevant Application Security standards. Providing detailed written feedback on the shortcomings and recommendations for rectifying them.
- ◆ Consultancy services to business owners of in-house systems and to development teams in finding compromise solutions that meet the needs of the business without creating unacceptable security risks. This consultancy work is performed at all levels: business requirements, technical feasibility, conceptual solution, technical architecture, system design, implementation decisions, coding and testing.
- ◆ Weekly code scanning for every development project (with a specialist proprietary tool maintained and configured for the up-to-date client specific security requirements by a trained expert within the nearshore team). Providing detailed feedback, with references to the respective standards, and recommendations for rectifying the issues discovered.
- ◆ White-box security assessment of every development project at the Solution Integration Testing stage. This involves manual security audit (against the client's Security Requirements to development and Application Security best practices) and automated scanning with specialist tools followed by the manual analysis of potential vulnerabilities discovered by the tools.
- ◆ The Luxoft team also provides expert input into the client's security policies, standards and best practices.



About LUXOFT:

- ◆ Luxoft is an emerging global leader in application and product-engineering outsourcing services for enterprise IT organizations and software vendors.
- ◆ Luxoft builds lasting partnerships with its clients, such as Boeing, Deutsche Bank, UBS, Dell, IBM, and other global leaders, based on the culture of engineering excellence, innovation, and deep domain expertise.
- ◆ Luxoft offers global delivery capability through its network of state-of-the-art delivery centers in North America, Central & Eastern Europe, and Asia.

www.luxoft.com

For more information, please contact:

Alexander Pinaev
Managing Director,
Technology Services
E-mail: APinaev@luxoft.com
Tel: +7 (812) 333-15-44
x (85) 4602
Mobile: +7 (921) 421-6430

Luxoft HQ
10-3, 1-Volokolamsky proezd
123060 Moscow, Russia
Tel: +7(495) 967-8030

Luxoft USA
225 West 34th Street, Ste. 1707
New York, NY 10122
Tel: + 1 (212) 964-9900