Secure Software Development Life Cycle (SSDLC)

A common misconception is that applications should be secured after they are developed but before deployment to the production environment. Performing a security audit after they are completed typically results in a significant amount of security flaws. Some of these flaws can involve serious architectural issues. In a best case scenario, developers can expect to invest an immense amount of time and effort to fix these flaws. Worst case, the application may require recoding and an overhaul of its architecture. Performing application security in this manner is incredibly expensive and time consuming. Integrating security into the early phases of the software development life cycle neutralizes this cost and produces more secure applications in far less time.

However, in Foundstone’s experience many organizations have not yet formalized their secure software development program and consequently they spend more time reacting to security issues in completed applications rather than proactively eliminating issues before the applications are completed. Further, they see the same problems manifest themselves time and again in the same applications or in other applications in the organization’s portfolio. This is a clear sign that a strategic approach must be employed to avoid the endless bug-fix cycle.

Benefits
Using the results from the interviews and document analysis, Foundstone will develop a secure SDLC integration program including recommended policies, guidelines, and knowledge transfer to address the three fundamental areas of people, process, and technology that are critical to a successful development process.

The secure software development gap analysis process can significantly benefit from thorough security reviews of multiple of your applications to create a baseline. This testing could include threat modeling, code reviews and/or penetration testing. Creation of this baseline will allow Foundstone consultants to accurately determine the state of software security within your environment. This in turn helps during the gap analysis and in making recommendations that can truly help your organization improve its software security while still delivering IT projects on time and within budget.

Methodology
Foundstone will gain a comprehensive understanding and analysis of how your development teams work. Through interviews, analysis of documented SDLC procedures, and review of any known issues with existing applications, Foundstone will understand existing practices and be able to identify areas for improvement from a security perspective. A key part of this analysis will include examining existing and proposed touch points and artifacts to identify critical areas for improvement. Foundstone measures the maturity of your application security efforts and helps you determine next steps by evaluating your SSDLC against a baseline of our seven best practice areas:

1. Awareness and training
2. Assessment and audit
3. Development and quality assurance
4. Compliance
5. Vulnerability response
6. Metrics and accountability
7. Operational security
Integrating security early into the application development lifecycle produces more secure, robust applications at a lower cost.

Foundstone will further make recommendations of critical security activities that augment those that are already being performed in your existing SDLC. These activities will be those that offer high return-on-investment while adding minimal overhead to the software development process. Foundstone views this entire effort as a continuous improvement process that must be approached in a step-by-step manner, which can also provide significant efficiencies in the long term. For instance, companies find shorter QA cycles due to much higher code quality as one tangible benefit. As part of this approach, Foundstone considers the following key activities and makes recommendations on which will provide the most benefit to your organization.

**Results**

Foundstone will provide a detailed report describing the most efficient and effective manner to integrate security into the existing software development lifecycle. The report will document both existing practices and how those can be augmented across the three critical areas of people, process and technology. The recommendations could include the need to develop policies and guidelines such as coding standards or rolling out training to the key stakeholders for instance. The deliverable will look to leverage existing investments such as security tools effectively.

**The Foundstone Difference**

All Foundstone projects are managed using Foundstone’s proven Security Engagement Process (SEP) for project management. This process ensures continual communication with your organization to ensure the success of all Foundstone consulting engagements.