

Who's watching your back?

Foundstone[®]
Professional Services A DIVISION OF McAfee

Services Datasheet

Software Security Policies, Procedures and Standards

BENEFITS

Having appropriate policies, procedures and standards allows an organization to help define a security bar that all applications must achieve. This in turn allows business analysts to define security requirements based on these standards, designers and developers to adhere to these standards, testers to test for violation of these standards and deployment / maintenance engineers to ensure ongoing compliance with these.

DELIVERABLES

Our deliverables includes some or all of the following:

- Secure Application Development Policy
- Secure Coding Standards
- Secure Application Deployment Standards
- Application Threat Modeling Methodology
- Application Security Code Review Methodology
- Application Security Quality Assurance Methodology
- Application Portfolio Risk Assessment Methodology
- Security Requirements Engineering Methodology
- Security Knowledge Management Process Development
- Tool Integration Process Development

In Foundstone's experience most security defects are caused due to the fact that developers and other stakeholders in the software development lifecycle have not been told what they must do and what they must not. This is best done through the use of policies and procedures. However, simply having one and not the other makes achieving the end goal of more secure applications harder to achieve. It is therefore vital that as organizations set out on their quest to integrate security into their software development lifecycle that they provide their development staff with the right knowledge to do their job.

Methodology

Foundstone approaches the delivery of these standards by first determining which of them are relevant to your organization. This can be based on language or technology in use as well as specifics such as versions and underlying servers. Foundstone can then work with your team to provide a draft for review of content. Following this, Foundstone can customize content and layout to adhere to your corporate standards. Finally, Foundstone will deliver the finished product as a document or set of documents as appropriate.

Scope

The scope of this engagement is determined by the number of documents to be developed, the degree of customization and the types of technologies involved.

Deliverables

Foundstone can provide some or all of the following types of deliverables as part of this engagement:

Secure Application Development Policy

Foundstone will develop a Secure Application Development Policy that is applicable to common development platforms (e.g. Java, C++, .NET, etc.). The policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (SDLC) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects. This document does not describe specific implementation steps required in software to follow the policy but is instead focused on the architecture at large. The audience for this policy is application architects, designers, developers, and those deploying and managing software developed within your organization. Foundstone recommends that the policy be used in conjunction with the standards described below.

The policy is based upon the eight-axis Foundstone Software Security Frame:

- Configuration Management
- Data Protection in Storage & Transit
- Authentication
- Authorization
- User & Session Management
- Data Validation
- Error Handling & Exception Management
- Logging & Auditing

Secure Coding Standards

Foundstone will develop a set of secure coding standards that are specific to the platform(s) outlined below:

- .NET / C#
- C++
- C
- ColdFusion
- PHP
- Perl
- Java (Java SE/Java EE)

These coding standards are also based upon the eight-axis Foundstone Software Security Frame. The standard provides platform-specific guidance for implementing the Secure Application Development Policy, described above. While these standards can stand on their own, Foundstone strongly recommends that these be deployed in conjunction with the Secure Application Development Policy described above.

Secure Application Deployment Standards

Foundstone will develop a set of secure application deployment standards that are specific to the platform(s) outlined below:

- .NET/C#
- ColdFusion
- PHP
- Perl
- Java (Java SE/Java EE)

These deployment standards are also based upon the eight-axis Foundstone Software Security Frame. The standard provides platform-specific guidance for deploying applications in accordance with the Secure Application Development Policy, described above. While these standards can stand on their own, Foundstone strongly recommends that these be deployed in conjunction with the Secure Application Development Policy described above.

Application Threat Modeling Methodology

Foundstone will develop a Threat Modeling Methodology for your organization based on the threat modeling techniques used by our consultants. The methodology will be flexible for use in a number of development environments and throughout the development lifecycle by individu-

als that are not security subject matter experts. Classification of threats will be based upon the eight-axis Foundstone Software Security Frame described above.

The methodology will additionally provide advice on documenting the threat model, however, the specific mechanisms used by your organization to document threat models are beyond the scope of the methodology.

Application Security Code Review

Methodology

Foundstone will develop an Application Security Code Review Methodology for your organization based on the code review techniques used by our consultants. The methodology will provide specific steps to review application source code, configuration and databases for commonly identified vulnerabilities using a variety of open source and commercial tools but mostly focused on manual reviews that augment your existing code review processes. The methodology is designed to be used with web-based, thick-client and thin-client applications.

Application Security Quality Assurance

Methodology

Foundstone will develop an Application Security Quality Assurance Methodology for your organization based on the penetration testing techniques used by our consultants. The methodology will provide specific steps to test software for commonly identified vulnerabilities using a variety of open source and commercial tools along with the manual methods required to validate findings. The methodology is designed to be used with web-based, thick-client and thin-client applications.

Application Portfolio Risk Assessment

Methodology:

Foundstone will develop a process and framework for prioritizing applications for security assessments and activities during a security enhanced software development lifecycle. This could include a self audit questionnaire that will allow stakeholders to determine the key activities that they must engage in at a very minimum to provide the business with the security assurance levels needed. It is important to note that

these activities will be highly dependent on their responses to the questionnaire and factors that influence risk for the organization such as compliance goals, company policies and specific security features.

Security Requirements Engineering Methodology

One of the most ignored parts of a security enhanced software development life cycle is the security requirements engineering process. One of the prime reasons for this oversight is that security is assumed to be a technical issue and therefore best handled during architecture and design or better still during implementation. Since software requirements are often written by business analysts who are non-technical, this is a common conclusion. Foundstone will work with your organization to develop a process that is light-weight and allows non-subject matter experts to effectively document and detail security requirements for application development projects.

Security Knowledge Management Process Development

Often at Foundstone we see organizations fall victim to issues that were fixed in other parts of the organization - sometimes even within the same team! While this is embarrassing, it is often a symptom of the lack of effective knowledge management. Valuable lessons can be learned from the experiences and mistakes of others both within the same organization and externally. While training is certainly an important aspect in improving overall security consciousness among developers, it is also important that developers have access to a central repository and portal for providing them with guidance on a day to day basis. This is especially important in large development organizations.

Foundstone can therefore help your organization develop an effective process for security knowledge management. This will account for both designing a channel that is effective in disseminating such information and also in maintaining confidentiality when needed.

Tool Integration Process Development

Foundstone will work with your organization to build a process around integrating technology investments such as web application scanning tools, web application firewalls and static source code analysis tools into the existing development processes. The process developed by Foundstone in conjunction with key stakeholders at your organization will focus on both the assessment perspective for software developers, testers and security analysts as well as the audit and oversight perspective for management. Foundstone can also help during the product evaluation process by aiding your organization in designing bake-offs and developing an assessment criteria as you compare the various vendor tool offerings.

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.