CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

How to Develop More Secure Software: Practices from Thirty Organizations

Key Message: Organizations can benchmark their software security practices against 109 observed activities from 30 organizations.

Executive Summary

For the past several years, Cigital has been working with organizations that have robust software security initiatives – to identify and characterize the activities they perform throughout the software development life cycle. This work is reflected in the Building Security In Maturity Model (BSIMM). BSIMM version 2 is an observation-based scientific model that describes the collective software security activities in 30 organizations across 7 market sectors. BSIMM can be used as a measuring stick or benchmark to compare an organization's software security practices with others.

In this podcast, Gary McGraw, Chief Technology Officer for Cigital and Sammy Migues, Principal Consultant and Director of Knowledge Management for Cigital, discuss the growing number of software security efforts and identify some of the most important and most commonly occurring practices for developing more secure software. Gary, Sammy, and Brian Chess discussed the first version of BSIMM in a previous CERT podcast.

PART 1: BUILDING SECURITY IN MATURITY MODEL (BSIMM): AN UPDATE

Background

The BSIMM project came about as a study of real-world software security initiatives, most of which have been in progress over the last 5 years or so. BSIMM describes what the project team observed in practice. BSIMM is a descriptive (not a prescriptive) model. It describes observed practice but does not recommend what organizations should do.

BSIMM is available for anyone to use under the Creative Commons license and is available for download from the BSIMM web site. BSIMM is primarily intended for people who are leading a software security group or initiative within an organization.

The BSIMM Software Security Framework (SSF) comprises 12 practices that represent aggregations of 109 observed activities from 30 organizations.

Organizations Participating in BSIMM

The first version of BSIMM reflected software security activities from 9 organizations in 3 market sectors. Version 2 reflects the experiences of 30 organizations in 7 market sectors. Those who are willing to be identified include Adobe, Aon, Bank of America, Capital One, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Intel, Intuit, Microsoft, Nokia, QUALCOMM, Sallie Mae, Standard Life, SWIFT, Symantec, Telecom Italia, Thomson Reuters, VMware, and Wells Fargo.

The market sectors represented by these firms include financial services, software vendors, technology firms, healthcare, insurance, energy, and media.

Having data from 30 organizations allows the BSIMM team to perform statistical analysis to validate the model at the activity level, to better determine what activities correlate with one another, and to compare/contrast high maturity organizations.

PART 2: KEY ACTIVITIES; MOST COMMONLY OBSERVED ACTIVITIES

Terminology

BSIMM organizes 109 software security *activities* into 12 *practices*.

A second key aspect is to make sure that there is sufficient staff in the SSG to help development projects. The average size of an SSG is one percent of the total number of developers. For example, if an organization has 100 developers, there should be at least one full time SSG member. This SSG size ratio has consistently held for BSIMM version 1 (9 organizations) and version 2 (30 organizations). The BSIMM project team has observed SSGs from 1-2 people up to 100 people.

Those leading SSGs are typically no more than 3 or 4 levels removed from the CEO so they operate at a fairly high level of authority and responsibility in their organizations. This provides them with ready access to required resources.

SSGs are able to quickly allocate their resources to address specific problems and activities on specific development projects. Examples include making code review happen, making sure all compliance requirements are addressed, and ensuring that bugs are removed from code before it goes into production.

Augment an SSG with a Software Security Satellite

Often, SSG members cannot cover all of the bases. People who don't report directly to the SSG but are interested in improving software security are referred to as the "satellite" in BSIMM.

Satellite members may include business analysts, product managers, testers, operations staff, and other developers.

Most Common Activities

In their article "What Works in Software Security," BSIMM authors describe 15 of the most common activities that they observed across at least 20 of the 30 organizations. A few of these are as follows:

- Identify gate locations and gather artifacts on how these gates work. Security gates are documented as part of an existing software development lifecycle (SDLC) process (SM 1.4 in BSIMM).
- Know all of your regulatory pressures and have a unifying approach (CP 1.1 in BSIMM).
- Provide awareness training for everyone (T 1.1 in BSIMM).
- Build and publish security features (AA 1.1 in BSIMM).
- Identify software defects found in operational monitoring and feed them back into development (CMVM 1.2 in BSIMM).

PART 3: MAKING THE BUSINESS CASE; GETTING STARTED

Business-based Arguments for Software Security

One justification for software security is understanding the cost of a correcting a defect found in operations vs. a defect identified during development (typically requiring significantly less cost and resources).

All organizations that have a software security initiative under way are convinced of its business value. Several firms are using BSIMM results to justify their continued investments up to the board level. They are also able to demonstrate that investments are impacting software security in the right direction.

Organizations are moving from selling based on fear and uncertainty (the early days), to selling to meet compliance requirements (the middling days), to selling software security because customers implicitly expect it and are increasingly demanding it.

Having the observation-based data in BSIMM is also a compelling argument, for comparison and benchmarking.

Getting Started

The first key step is to put somebody in charge who can actually get things done. This is most likely someone in the executive ranks, not necessarily a lead software developer.

Next, identify existing pockets of expertise and solid practice and build on these.

Figure out what is most important with respect to software security such as privacy, compliance, or addressing top attacks and vulnerabilities.

Use BSIMM to help select a starter set of common activities.

What's Next for BSIMM

The BSIMM project team has identified 70 organizations that have software security initiatives under way and plan to interview many of those that have yet to participate.

There is a community developing around BSIMM that plans to address cost and effectiveness issues.

The BSIMM project team is in the process of re-measuring firms that were in the original set of 9 organizations, to be able to describe how people are improving their software security initiatives over time.

The BSIMM Advisory Board includes Steve Lipner, Microsoft; Eric Baize, EMC; Jeff Cohen, Intel; Yana Uselito, Nokia; and Brad Arkin, Adobe.

There is a conference planned for fall 2010 and a moderating mailing list. The project team is hoping to double the size of the BSIMM2 study for BSIMM3, expected in early 2011.

Resources

BSIMM version 2: http://www.bsimm2.com.

McGraw, Gary; Chess, Brian; Migues, Sammy; Nichols, Elizabeth. "Software [In]Security: BSIMM2." May 12, 2010.

McGraw, Gary; Chess, Brian; Migues, Sammy. "Software [In]security: What Works in Software Security; Fifteen Common Activities from BSIMM2." February 26, 2010.