cigital

Building Security In Maturity Model

Fifteen Things That Everybody Does

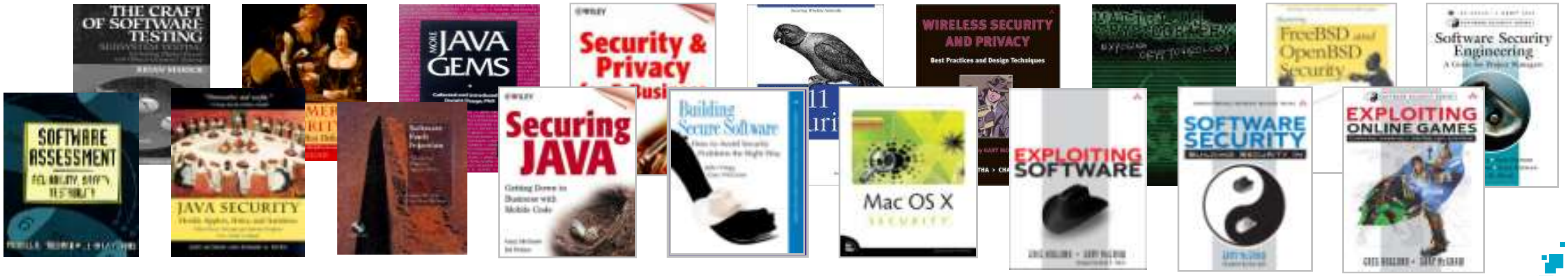
Gary McGraw, Ph.D.
Chief Technology Officer, Cigital

February 2010

Software Confidence. Achieved.

Cigital

- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security and software quality
  - Widely published in books, white papers, and articles
  - Industry thought leaders



© 2010 Cigital Inc.

Breaking new ground

- Building Security In Maturity Model
- Real data from (30) real initiatives
- McGraw, Chess, & Migues

cigital

FORTIFY

© 2010 Cigital Inc.

58 software security initiatives

- 31 Financial
- 9 ISV
- 9 Tech
- 2 Defense
- 5 Retail
- 1 Oil
- 1 Behemoth

- visa europe
- thomson/reuters
- BP
- SAP
- nokia
- ebay
- mckesson

- ABN/amro
- ING
- telecom italia
- swift
- standard life
- cigna
- AON

- microsoft
- dtcc
- emc
- fidelity
- adobe
- wells fargo
- goldman sachs
- google
- qualcomm
- morgan stanley
- usaf
- dell
- pershing
- the hartford
- barclays capital
- bank of tokyo
- ups
- bank of montreal
- sterling commerce
- coke
- mastercard
- apple

- cisco
- bank of america
- walmart
- finra
- vanguard
- college board
- oracle
- state street
- omgeo
- motorola
- general electric
- lockheed martin
- intuit
- vmware
- amex
- bank of ny mellon
- harris bank
- paypal
- symantec
- AOL
- CA
- time warner

cigital

© 2010 Cigital Inc.

BSIMM original nine

EMC^2
where information lives®

Microsoft®

Adobe®

Google™

DTCC®
The Depository Trust & Clearing Corporation

WELLS FARGO

QUALCOMM®

And two unnamed financial services firms

© 2010 Cigital Inc.

BSIMM Europe (nine EU firms)

NOKIA
Connecting People

STANDARD LIFE®

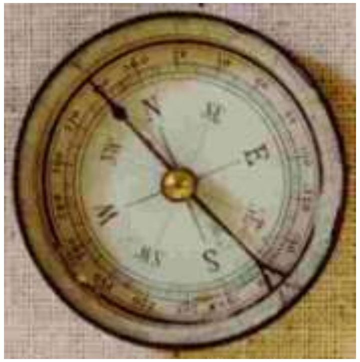
THOMSON REUTERS

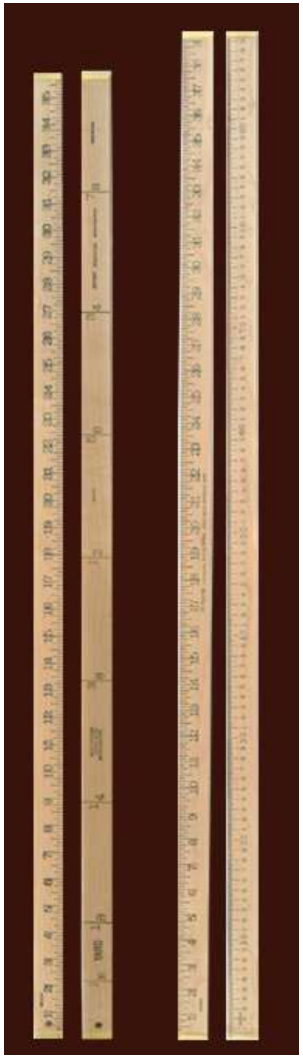
SWIFT

TELECOM
ITALIA

And four unnamed firms

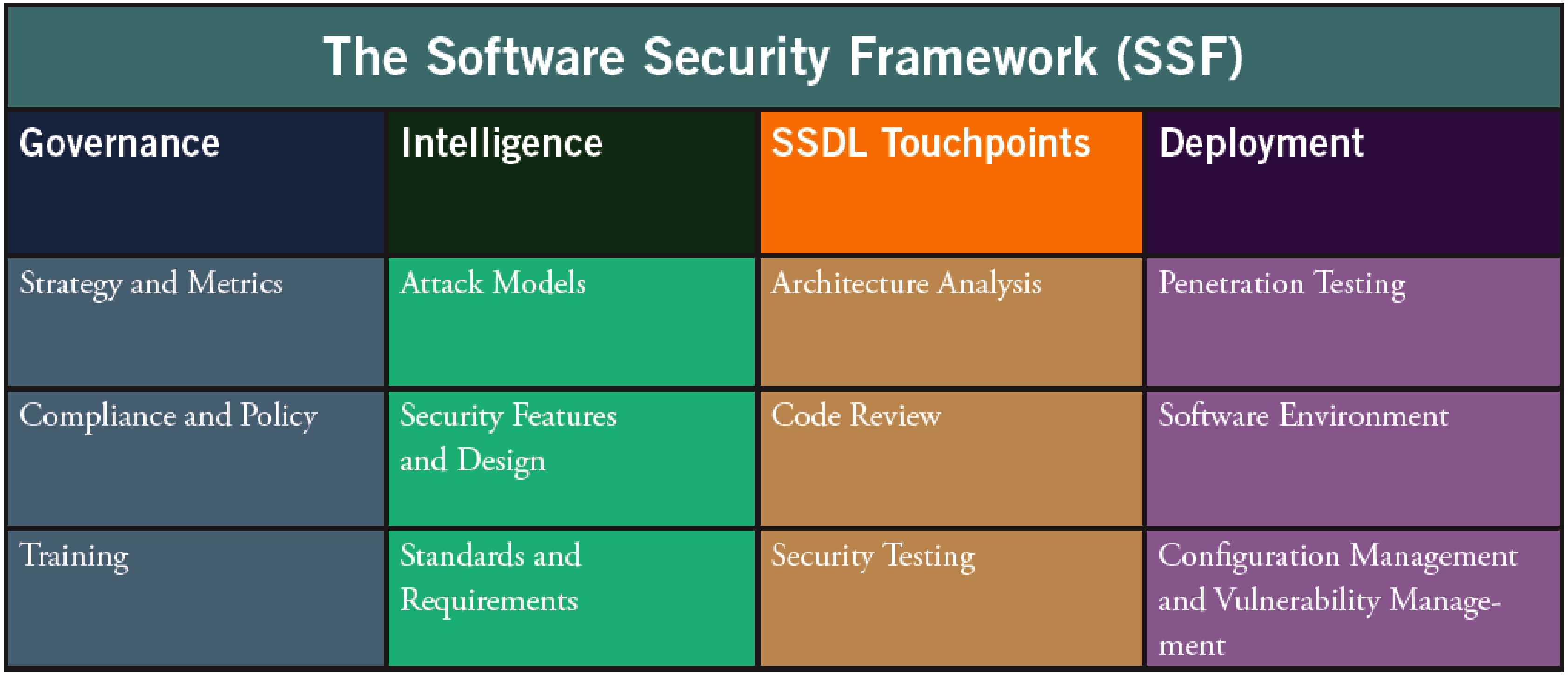
On cargo cults and divining rods





- InformIT article on BSIMM website http://bsi-mm.com

A Software Security Framework



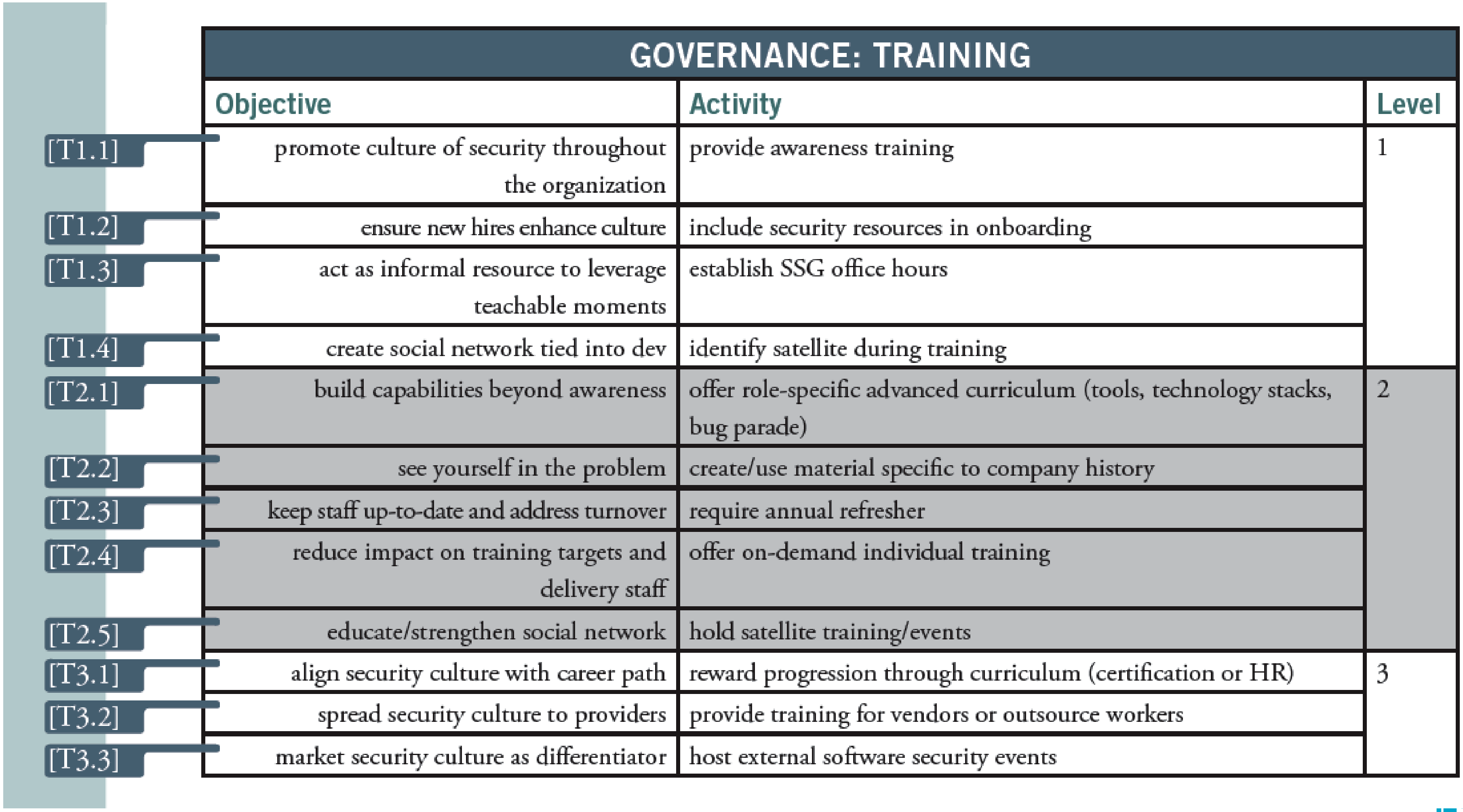
The Software Security Framework (SSF)

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

- Four domains
- Twelve practices
- See informIT article on BSIMM website http://bsi-mm.com

© 2010 Cigital Inc.

Training practice skeleton



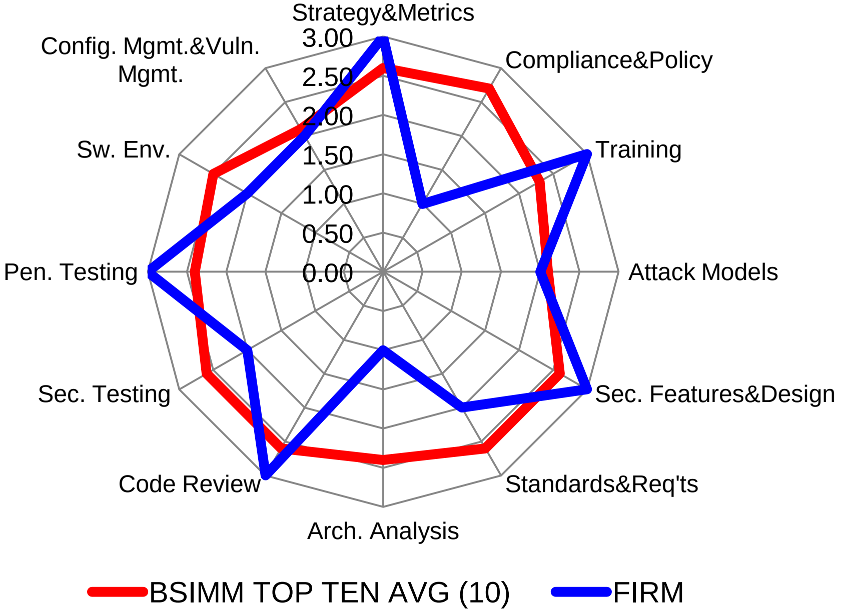
GOVERNANCE: TRAINING

	Objective	Activity	Level
[T1.1]	promote culture of security throughout the organization	provide awareness training	1
[T1.2]	ensure new hires enhance culture	include security resources in onboarding	
[T1.3]	act as informal resource to leverage teachable moments	establish SSG office hours	
[T1.4]	create social network tied into dev	identify satellite during training	
[T2.1]	build capabilities beyond awareness	offer role-specific advanced curriculum (tools, technology stacks, bug parade)	2
[T2.2]	see yourself in the problem	create/use material specific to company history	
[T2.3]	keep staff up-to-date and address turnover	require annual refresher	
[T2.4]	reduce impact on training targets and delivery staff	offer on-demand individual training	
[T2.5]	educate/strengthen social network	hold satellite training/events	
[T3.1]	align security culture with career path	reward progression through curriculum (certification or HR)	3
[T3.2]	spread security culture to providers	provide training for vendors or outsource workers	
[T3.3]	market security culture as differentiator	host external software security events	

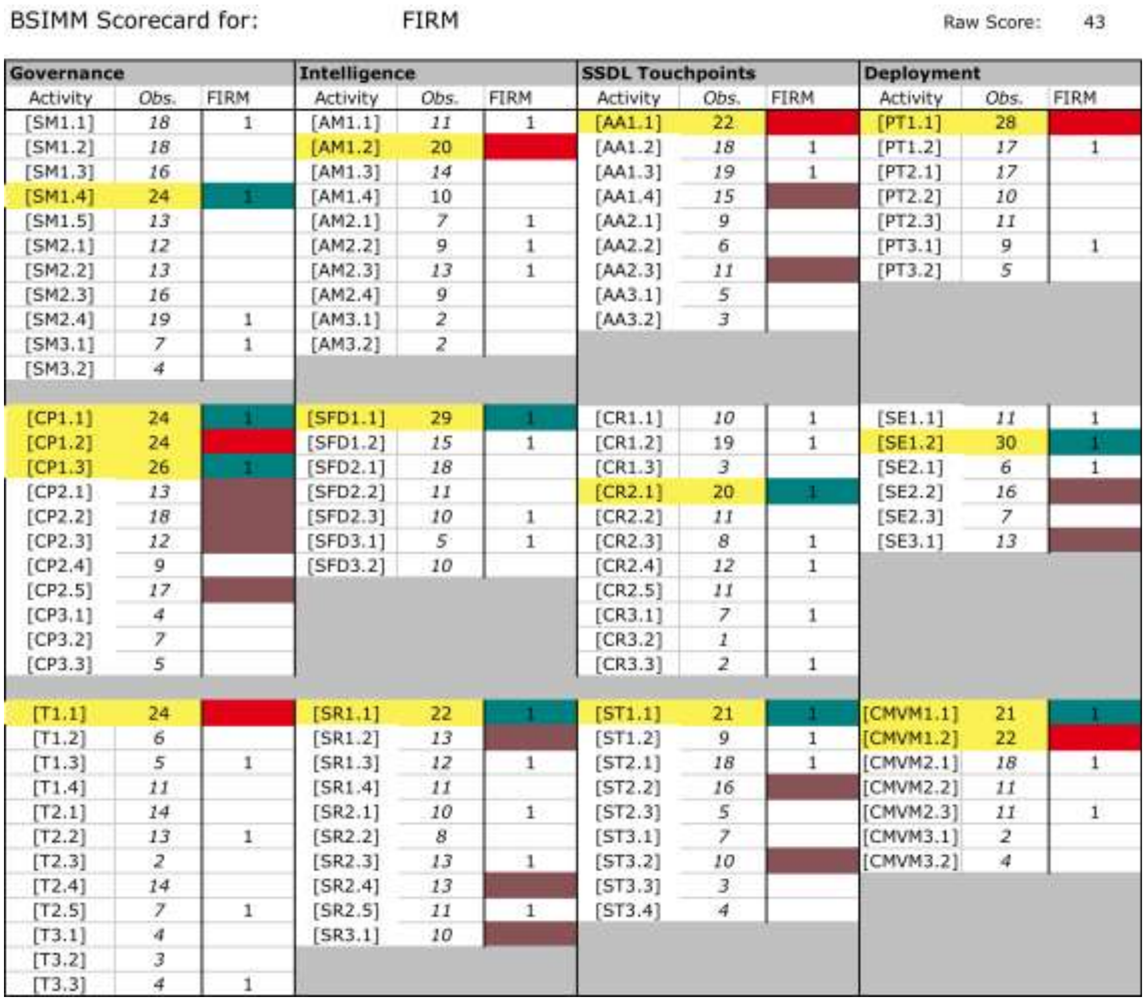
© 2010 Cigital Inc.

15 Things Everybody Does

- identify gates
- unify regulations
- know PII obligations
- publish policy
- awareness training
- data classification
- identify features
- security standards
- review security features
- static analysis tool
- QA boundary testing
- external pen testers
- good network security
- incident response
- close ops bugs loop



BSIMM Scorecard



BSIMM Scorecard for: FIRM

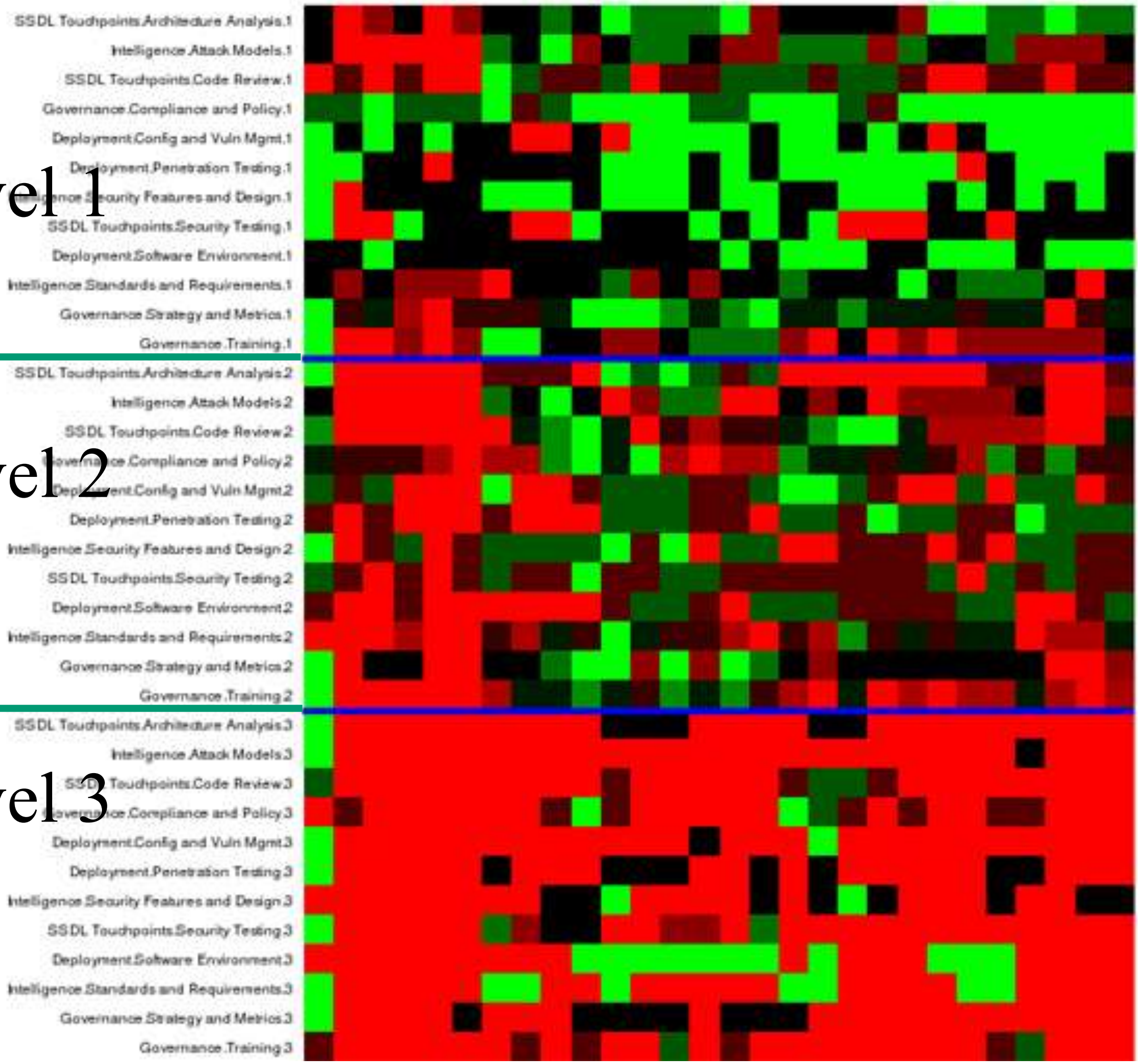
Raw Score: 43

Governance			Intelligence			SSDL Touchpoints			Deployment		
Activity	Obs.	FIRM	Activity	Obs.	FIRM	Activity	Obs.	FIRM	Activity	Obs.	FIRM
[SM1.1]	18	1	[AM1.1]	11	1	[AA1.1]	22	🟥	[PT1.1]	28	🟥
[SM1.2]	18		[AM1.2]	20	🟥	[AA1.2]	18	1	[PT1.2]	17	1
[SM1.3]	16		[AM1.3]	14		[AA1.3]	19	1	[PT2.1]	17	
[SM1.4]	24	🟩 1	[AM1.4]	10		[AA1.4]	15	🟫	[PT2.2]	10	
[SM1.5]	13		[AM2.1]	7	1	[AA2.1]	9		[PT2.3]	11	
[SM2.1]	12		[AM2.2]	9	1	[AA2.2]	6		[PT3.1]	9	1
[SM2.2]	13		[AM2.3]	13	1	[AA2.3]	11	🟫	[PT3.2]	5	
[SM2.3]	16		[AM2.4]	9		[AA3.1]	5				
[SM2.4]	19	1	[AM3.1]	2		[AA3.2]	3				
[SM3.1]	7	1	[AM3.2]	2							
[SM3.2]	4										
[CP1.1]	24	🟩 1	[SFD1.1]	29	🟩 1	[CR1.1]	10	1	[SE1.1]	11	1
[CP1.2]	24	🟥	[SFD1.2]	15	1	[CR1.2]	19	1	[SE1.2]	30	🟩 1
[CP1.3]	26	🟩 1	[SFD2.1]	18		[CR1.3]	3		[SE2.1]	6	1
[CP2.1]	13	🟫	[SFD2.2]	11		[CR2.1]	20	🟩 1	[SE2.2]	16	🟫
[CP2.2]	18	🟫	[SFD2.3]	10	1	[CR2.2]	11		[SE2.3]	7	
[CP2.3]	12	🟫	[SFD3.1]	5	1	[CR2.3]	8	1	[SE3.1]	13	🟫
[CP2.4]	9		[SFD3.2]	10		[CR2.4]	12	1			
[CP2.5]	17	🟫				[CR2.5]	11				
[CP3.1]	4					[CR3.1]	7	1			
[CP3.2]	7					[CR3.2]	1				
[CP3.3]	5					[CR3.3]	2	1			
[T1.1]	24	🟥	[SR1.1]	22	🟩 1	[ST1.1]	21	🟩 1	[CMVM1.1]	21	🟩 1
[T1.2]	6		[SR1.2]	13	🟫	[ST1.2]	9	1	[CMVM1.2]	22	🟥
[T1.3]	5	1	[SR1.3]	12	1	[ST2.1]	18	1	[CMVM2.1]	18	1
[T1.4]	11		[SR1.4]	11		[ST2.2]	16	🟫	[CMVM2.2]	11	
[T2.1]	14		[SR2.1]	10	1	[ST2.3]	5		[CMVM2.3]	11	1
[T2.2]	13	1	[SR2.2]	8		[ST3.1]	7		[CMVM3.1]	2	
[T2.3]	2		[SR2.3]	13	1	[ST3.2]	10	🟫	[CMVM3.2]	4	
[T2.4]	14		[SR2.4]	13	🟫	[ST3.3]	3				
[T2.5]	7	1	[SR2.5]	11	1	[ST3.4]	4				
[T3.1]	4		[SR3.1]	10	🟫						
[T3.2]	3										
[T3.3]	4	1									

- Top 10 things
  - green = good?
  - red = bad?
- “Blue shift” practices to emphasize
  - activities you should maybe think about in brown

© 2010 Cigital Inc.

How good are the levels we chose?

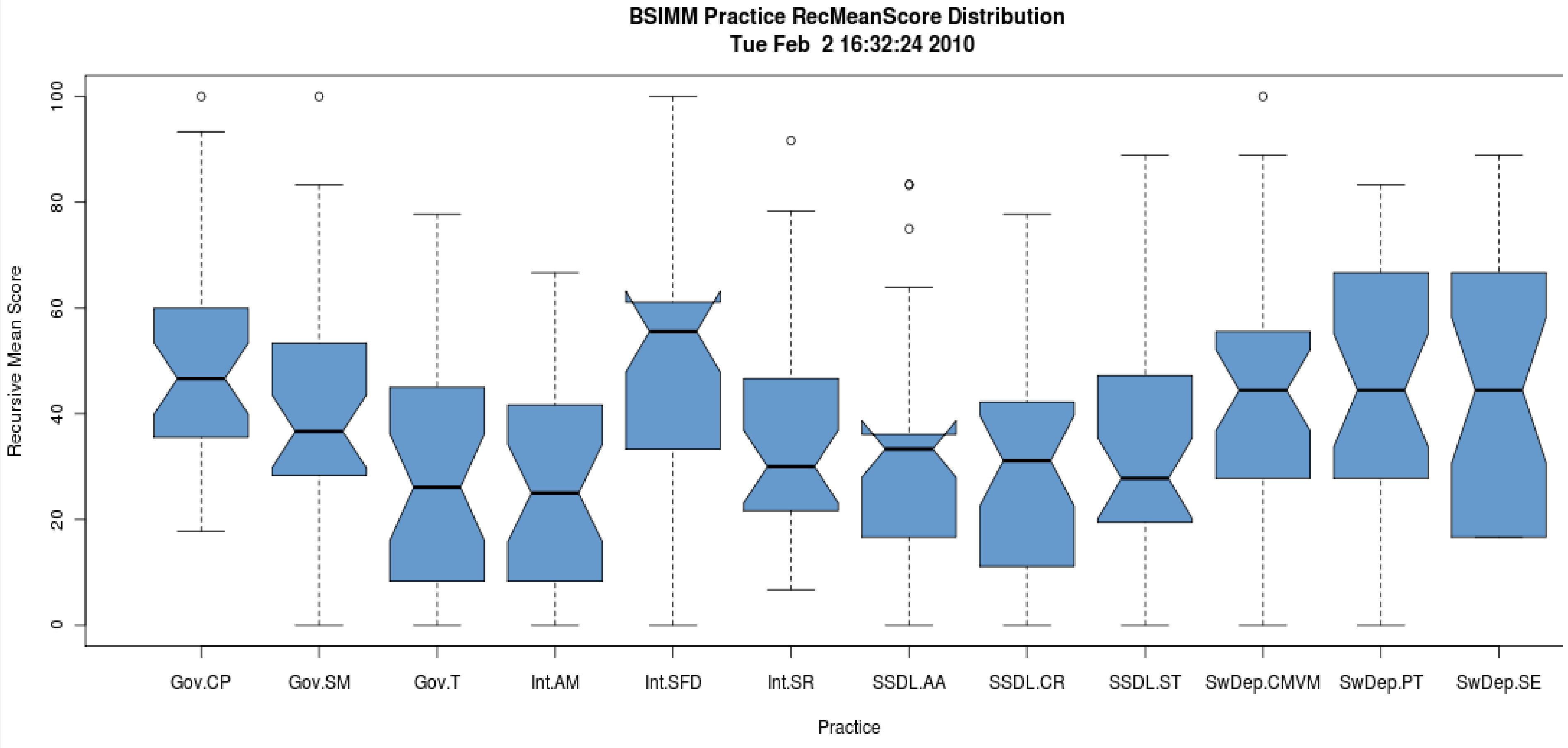


Maturity Level 1

Maturity Level 2

Maturity Level 3

Practices


BSIMM Practice RecMeanScore Distribution
Tue Feb 2 16:32:24 2010
Recursive Mean Score
0
20
40
60
80
100
Gov.CP
Gov.SM
Gov.T
Int.AM
Int.SFD
Int.SR
SSDL.AA
SSDL.CR
SSDL.ST
SwDep.CMVM
SwDep.PT
SwDep.SE
Practice

[SM1.4] 24/30 firms

Identify gate locations, gather necessary artifacts. The software security process will eventually involve release gates at one or more points in the software development lifecycle (SDLC) or SDLCs. The first two steps toward establishing these release gates is to identify gate locations that are compatible with existing development practices and to begin gathering the input necessary for making a go/no go decision. Importantly at this stage, the gates are not enforced. For example, the SSG can collect security testing results for each project prior to release, but stop short of passing judgment on what constitutes sufficient testing or acceptable test results.

© 2010 Cigital Inc.

[CP 1.1] 24/30 firms

Know all regulatory pressures and unify approach. If the business is subject to regulatory or compliance drivers such as FFIEC, GLBA, OCC, PCI DSS, SOX, SAS 70, HIPAA or others, the SSG acts as a focal point for understanding the constraints such drivers impose on software. The SSG creates a unified approach that removes redundancy from overlapping compliance requirements. A formal approach will map applicable portions of regulations to control statements explaining how the organization will comply.

MOTORCYCLE AND MOPED PARKING
UNR PARKING PERMIT REQUIRED
PARKING ONLY
MINIMUM $100.00 FINE TOWING ENFORCED
SERVICE VEHICLES ONLY PERMIT REQUIRED
SILVER 9 UNIVERSITY PERMIT REQUIRED
PATIENT PARKING PERMIT REQUIR
PLEASE OBTAI A PERMIT AT T CHECK-IN DES
15 MINUTE LOADING ZONE FLASHERS
RESERVED MINIMUM FINE OF $100 FOR VIOLATION
VAN
Access to Lower Campus

© 2010 Cigital Inc.

[CP 1.2] 24/30 firms

Identify PII obligations. The way software handles personally identifiable information (PII) could well be explicitly regulated, but even if it is not, privacy is a hot topic. The SSG takes a lead role in identifying PII obligations stemming from regulation, customer demand, and consumer expectations. It uses this information to promote best practices related to privacy. For example, if the organization processes credit card transactions, the SSG will identify the constraints that PCI DSS places on the handling of cardholder data.

© 2010 Cigital Inc.

[CP 1.3] 26/30 firms

Create policy. The SSG guides the rest of the organization by creating or contributing to policy that satisfies regulatory requirements and customer-driven security requirements. The policy provides a unified approach for satisfying the (potentially lengthy) list of external security drivers. As a result, project teams can avoid learning the details involved in complying with all applicable regulations. Likewise, project teams don’t need to re-learn customer security requirements on their own. The SSG policy documents are sometimes focused around major compliance topics such as the handling of personally identifiable information or the use of cryptography.

© 2010 Cigital Inc.

[T 1.1] 24/30 firms

Provide awareness training. The SSG provides awareness training in order to promote a culture of security throughout the organization. Training might be delivered by members of the SSG, by an outside firm, by the internal training organization, or through a computer-based training system. Course content is not necessarily tailored for a specific audience. For example, all programmers, quality assurance engineers, and project managers could attend the same Introduction to Software Security course.

© 2010 Cigital Inc.

[AM 1.2] 20/30 firms

Create data classification scheme and inventory. The organization agrees upon a data classification scheme and uses the scheme to inventory its software according to the kinds of data the software handles. This allows applications to be prioritized by their data classification. Many classification schemes are possible—one approach is to focus on PII. Depending upon the scheme and the software involved, it could be easiest to first classify data repositories, then derive classifications for applications according to the repositories they use.

RESTRICTED SOM1-01

TO 12D1—3—11—1

MAJESTIC—12 GROUP SPECIAL OPERATIONS MANUAL

EXTRATERRESTRIAL
ENTITIES AND TECHNOLOGY,
RECOVERY AND DISPOSAL

TOP SECRET/MAJIC
EYES ONLY

WARNING! This is a TOP SECRET—MAJIC EYES ONLY document containing compartmentalized information essential to the national security of the United States. EYES ONLY ACCESS to the material herein is strictly limited to personnel possessing MAJIC—12 CLEARANCE LEVEL. Examination or use by unauthorized personnel is strictly forbidden and is punishable by federal law.

MAJESTIC—12 GROUP • APRIL 1954

© 2010 Cigital Inc.

[SFD 1.1] 29/30 firms

Build/publish security features (authentication, role management, key management, audit/log, crypto, protocols). Some problems are best solved only once. Rather than have each project team implement all of their own security features, the SSG provides proactive guidance by building and publishing security features for other groups to use. Project teams benefit from implementations that come pre-approved by the SSG, and the SSG benefits by not having to repeatedly track down the kinds of subtle errors that creep into features such as authentication, role management, audit/logging, key management, and cryptography.

© 2010 Cigital Inc.

[SR 1.1] 22/30 firms

Create security standards. Software security requires much more than security features, but security features are part of the job as well. The SSG meets the organization’s demand for security features by creating standards that explain the accepted way to adhere to policy and carry out specific security-centric operations. A standard might describe how to perform authentication using J2EE or how to determine the authenticity of a software update. (See [SFD1.1] Build and publish security features for one case where the SSG provides a reference implementation of a security standard.

cigital

© 2010 Cigital Inc.

[AA 1.1] 22/30 firms

Perform security feature review. To get started with architecture analysis, center the analysis process on a review of security features. Reviewers first identify the security features in an application (authentication, access control, use of cryptography, etc.) then study the design looking for problems that would cause these features to fail at their purpose or otherwise prove insufficient. At higher levels of maturity this activity is eclipsed by a more thorough approach to architecture analysis not centered on features.

cigital

© 2010 Cigital Inc.

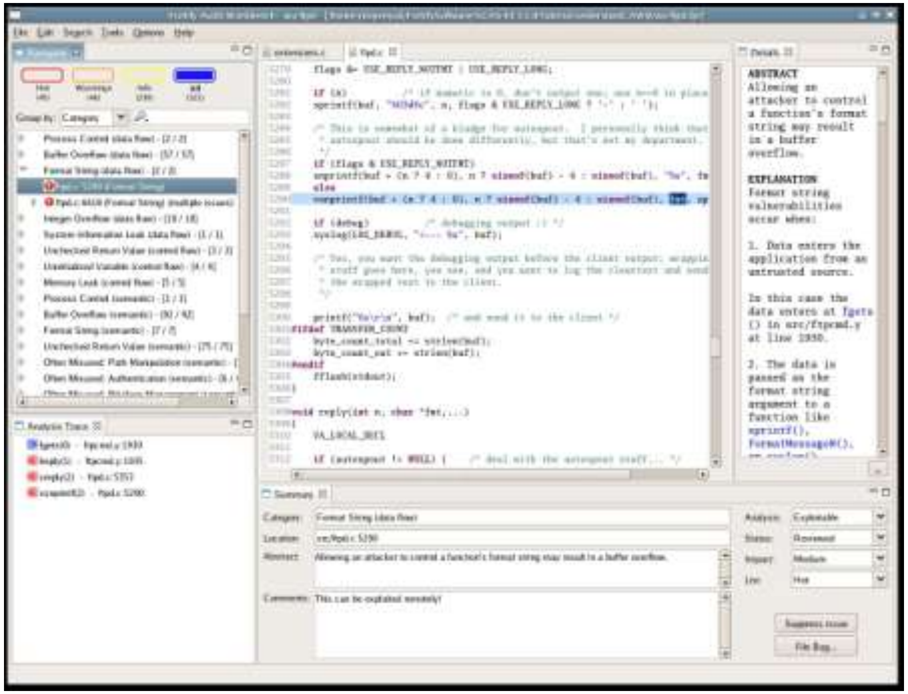
[CR 2.1] 20/30 firms

Use automated tools along with manual review. Incorporate static analysis into the code review process in order to make code review more efficient and more consistent. The automation does not replace human judgment, but it does bring definition to the review process and security expertise to reviewers who are not security experts.

FORTIFY

coverity

OUNCE LABS



- Process Control (data flow) - [2 / 2]
- Buffer Overflow (data flow) - [57 / 57]
- Format String (data flow) - [2 / 2]
- Integer Overflow (data flow) - [18 / 18]
- System Information Leak (data flow) - [1 / 1]
- Unchecked Return Value (control flow) - [3 / 3]
- Uninitialized Variable (control flow) - [4 / 4]
- Memory Leak (control flow) - [5 / 5]
- Process Control (semantic) - [1 / 1]
- Buffer Overflow (semantic) - [92 / 92]
- Format String (semantic) - [7 / 7]
- Unchecked Return Value (semantic) - [75 / 75]
- Often Misused: Path Manipulation (semantic)
- Often Misused: Authentication (semantic)

```
    printf("%s\r\n", buf);  /* and send it to the client */
#ifdef TRANSFER_COUNT
    byte_count_total += strlen(buf);
    byte_count_out += strlen(buf);
#endif
    fflush(stdout);
}

void reply(int n, char *fmt,...)
{
    VA_LOCAL_DECL

    if (autospout != NULL) {    /* deal with the autospout stuff... */
```

ABSTRACT
Allowing an attacker to control a function's format string may result in a buffer overflow.

EXPLANATION
Format string vulnerabilities occur when:

1. Data enters the application from an untrusted source.

In this case the data enters at fgets() in src/ftpcmd.y at line 1930.

2. The data is passed as the format string argument to a function like sprintf(), FormatMessageW(),

Category: Format String (data flow)
Location: src/ftpd.c:5290
Abstract: Allowing an attacker to control a function's format string may result in a buffer overflow.
Comments: This can be exploited remotely!
Analysis: Exploitable
Status: Reviewed
Impact: Medium
List: Hot

cigital

© 2010 Cigital Inc.

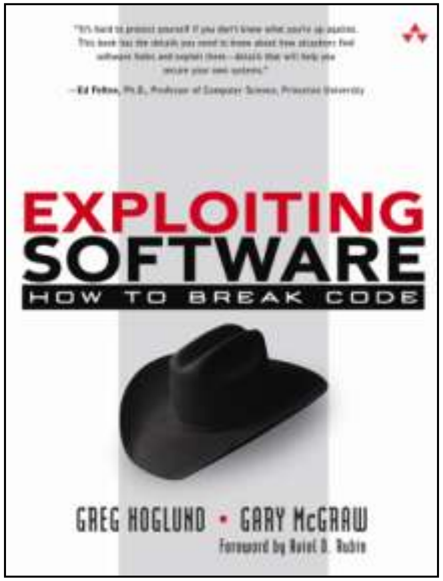
[ST 1.1] 21/30 firms

Ensure QA supports edge/boundary value condition testing. The QA team goes beyond functional testing to perform basic adversarial tests. They probe simple edge cases and boundary conditions. No attacker skills required.

© 2010 Cigital Inc.

[PT 1.1] 28/30 firms

Use external penetration testers to find problems. Many organizations are not willing to address software security until there is unmistakable evidence that the organization is not somehow magically immune to the problem. If security has not been a priority, external penetration testers demonstrate that the organization’s code needs help. Penetration testers could be brought in to break a high-profile application in order to make the point.



“It’s hard to protect yourself if you don’t know what you’re up against. This book has the details you need to know about how attackers find software holes and exploit them—details that will help you secure your own systems.”

—**Ed Felten**, Ph.D., Professor of Computer Science, Princeton University

EXPLOITING SOFTWARE

HOW TO BREAK CODE

GREG HOGLUND • GARY McGRAW

Foreword by Aviel D. Rubin

© 2010 Cigital Inc.

[SE 1.2] 30/30 firms

Ensure host and network security basics are in place. The organization provides a solid foundation for software by ensuring that host and network security basics are in place. It is common for operations security teams to be responsible for duties such as patching operating systems and maintaining firewalls.

cigital

© 2010 Cigital Inc.

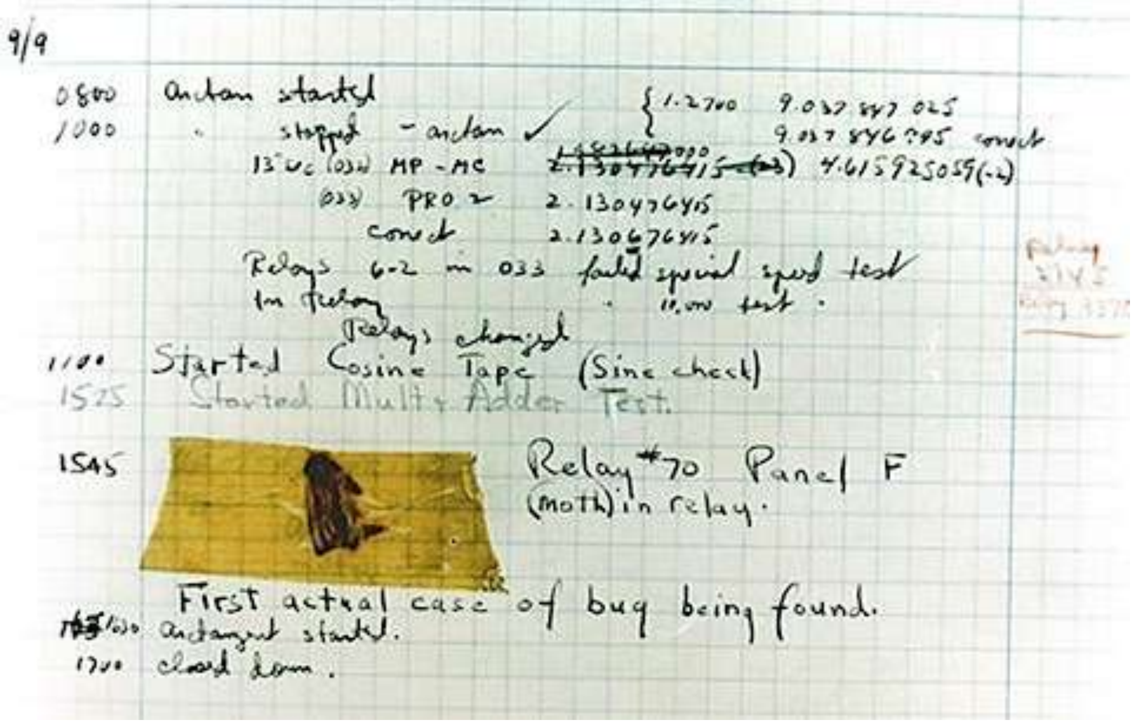
[CMVM 1.1] 21/30 firms

Create or interface with incident response. The SSG is prepared to respond to an incident. The group either creates its own incident response capability or interfaces with the organization’s existing incident response team. A regular meeting between the SSG and the incident response team can keep information flowing in both directions.

© 2010 Cigital Inc.

[CMVM 1.2] 22/30 firms

Identify software defects found in operations monitoring and feed them back to development. Defects identified through operations monitoring are fed back to development and used to change developer behavior. The contents of production logs can be revealing (or can reveal the need for improved logging).



9/9

0800 Arctan started
1000 " stopped - arctan ✓ {1.2700 9.037 847 025
9.037 846 995 correct
13" UC (032) MP - MC ~~1.982147000~~ ~~2.130476415~~ (-3)) 4.615925059(-2)
(033) PRO 2 2.130476415
correct 2.130676415
Relays 6-2 in 033 failed special speed test
In relay " 10,000 test.
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.
1545 Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
~~1600~~ 1630 Arctangent started.
1700 closed down.

Relay 2145
Relay 3370

© 2010 Cigital Inc.

Using BSIMM

- BSIMM released March 2009 under creative commons
  - http://bsi-mm.com
  - v1.5 includes Europe (November 2009)
  - Italian and German translations
  - steal the data if you want
- BSIMM is a yardstick
  - Use it to see where you stand
  - Use it to figure out what your peers do
- BSIMM is growing (30+)
  - BSIMM Europe
  - BSIMM Begin

cigital

© 2010 Cigital Inc.

Where to Learn More

informIT & Justice League

- www.informIT.com
- No-nonsense monthly security column by Gary McGraw

- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
  - Scott Matsumoto
  - Gary McGraw
  - Sammy Migues
  - Craig Miller
  - John Steven

cigital

© 2010 Cigital Inc.

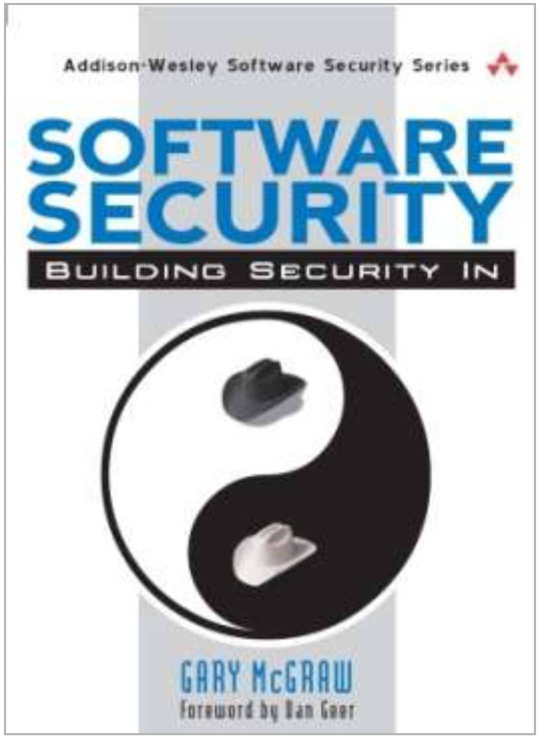
IEEE Security & Privacy Magazine + 2 Podcasts

- Building Security In
- Software Security Best Practices column edited by John Steven
- www.computer.org/security/bsisub/

- www.cigital.com/silverbullet
- www.cigital.com/realitycheck

© 2010 Cigital Inc.

Software Security: the book



- How to DO software security
  - Best practices
  - Tools
  - Knowledge
- Cornerstone of the Addison-Wesley Software Security Series
- www.swsec.com

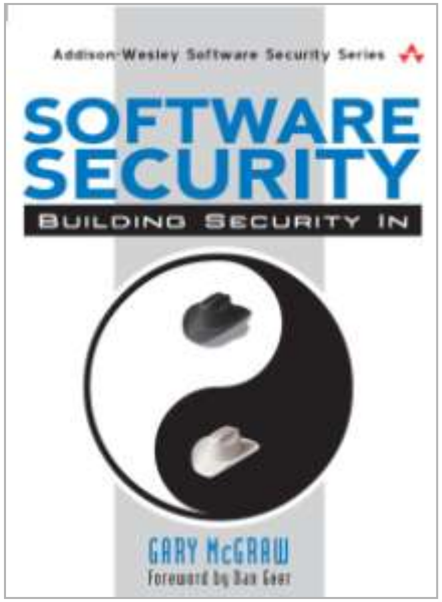
Addison Wesley

cigital

© 2010 Cigital Inc.

For more on BSIMM

- http://bsi-mm.com
- See the Addison-Wesley Software Security series
- Send e-mail: gem@cigital.com



cigital

Addison Wesley

"So now, when we face a choice between adding features and resolving security issues, we need to choose security."

-Bill Gates

© 2010 Cigital Inc.