# Enterprise Application Security Program

## GE's approach to solving the root cause and establishing a Center of Excellence

**Darren Challey**
GE Application Security Leader

imagination at work

# Agenda

- ✓ Why is AppSec important?
- ✓ Why is it so hard?
- ✓ Changing the culture
- ✓ Critical success factors
- ✓ Structuring an enterprise program:
  - Guidance
  - Education
  - Tools
- ✓ Managing vendors
- ✓ Creating a center of excellence

imagination at work

# Why is Application security important?

imagination at work

# Press we like!

2005, 2006 Global Most Admired Companies (#1)
*Fortune*

FORTUNE
2005 WORLD'S MOST ADMIRED COMPANIES
Industry Champion – Ranked #1

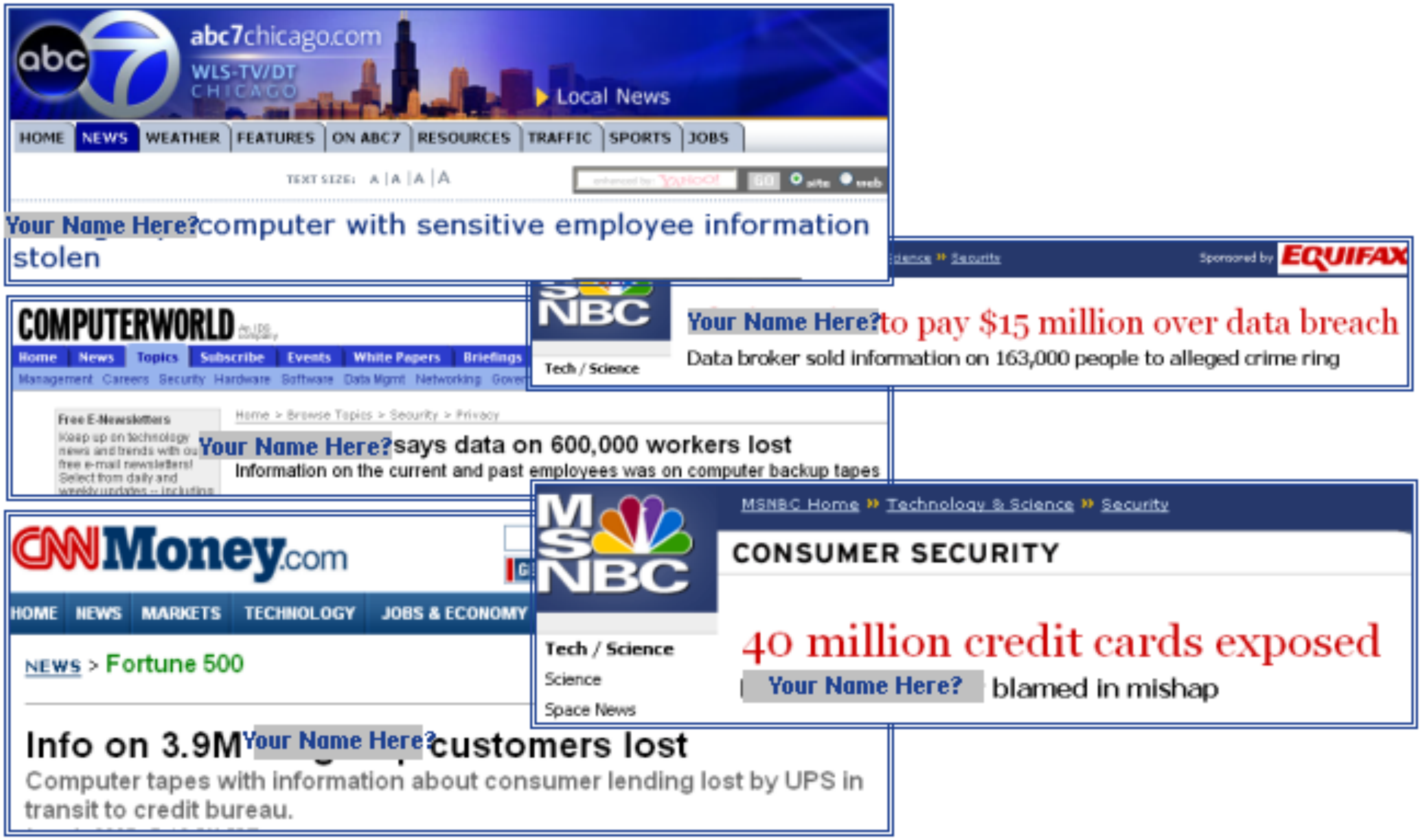
Seven consecutive years:
*World's Most Respected Company*
*Financial Times*

FINANCIAL TIMES

2004 – Named a member of the Dow Jones Sustainability Index

05
Member of Dow Jones Sustainability Indexes
DJSI

# Press we can't afford …


abc7chicago.com
WLS-TV/DT CHICAGO
Local News
HOME NEWS WEATHER FEATURES ON ABC7 RESOURCES TRAFFIC SPORTS JOBS
TEXT SIZE: A | A | A | A
COMPUTERWORLD
Home News Topics Subscribe Events White Papers Briefings
Management Careers Security Hardware Software Data Mgmt Networking
Home > Browse Topics > Security > Privacy
Free E-Newsletters
MSNBC
Tech / Science
Science
Space News
Sponsored by EQUIFAX
MSNBC Home » Technology & Science » Security
CONSUMER SECURITY
CNNMoney.com
HOME NEWS MARKETS TECHNOLOGY JOBS & ECONOMY
NEWS > Fortune 500

Your Name Here? computer with sensitive employee information stolen

Your Name Here? to pay $15 million over data breach

Data broker sold information on 163,000 people to alleged crime ring

Your Name Here? says data on 600,000 workers lost

Information on the current and past employees was on computer backup tapes

40 million credit cards exposed

Your Name Here? blamed in mishap

Info on 3.9M Your Name Here? customers lost

Computer tapes with information about consumer lending lost by UPS in transit to credit bureau.

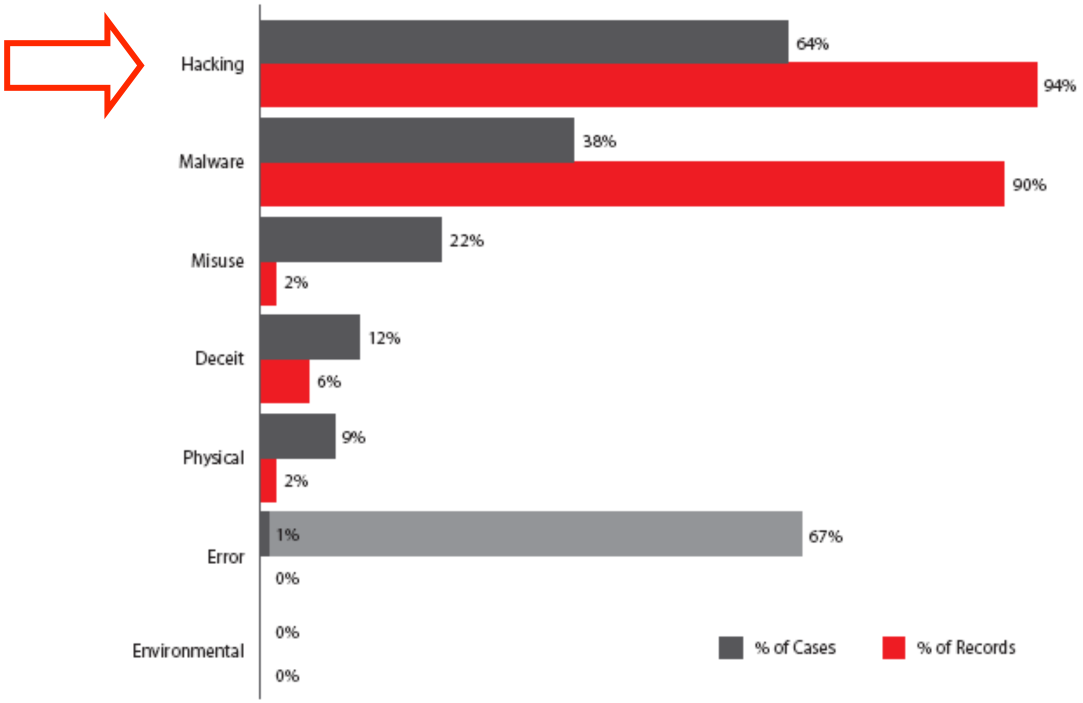
## Significant reputational, regulatory & financial harm

imagination at work

# AppSec is a large data loss source

Loss or disclosure of PII (Personally Identifiable Information) is required to be reported (thus good

Figure 13. Threat categories by percent of breaches (black) and records (red)



Source: Verizon's 2009 Data Breach Investigations Report – Figure 13

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

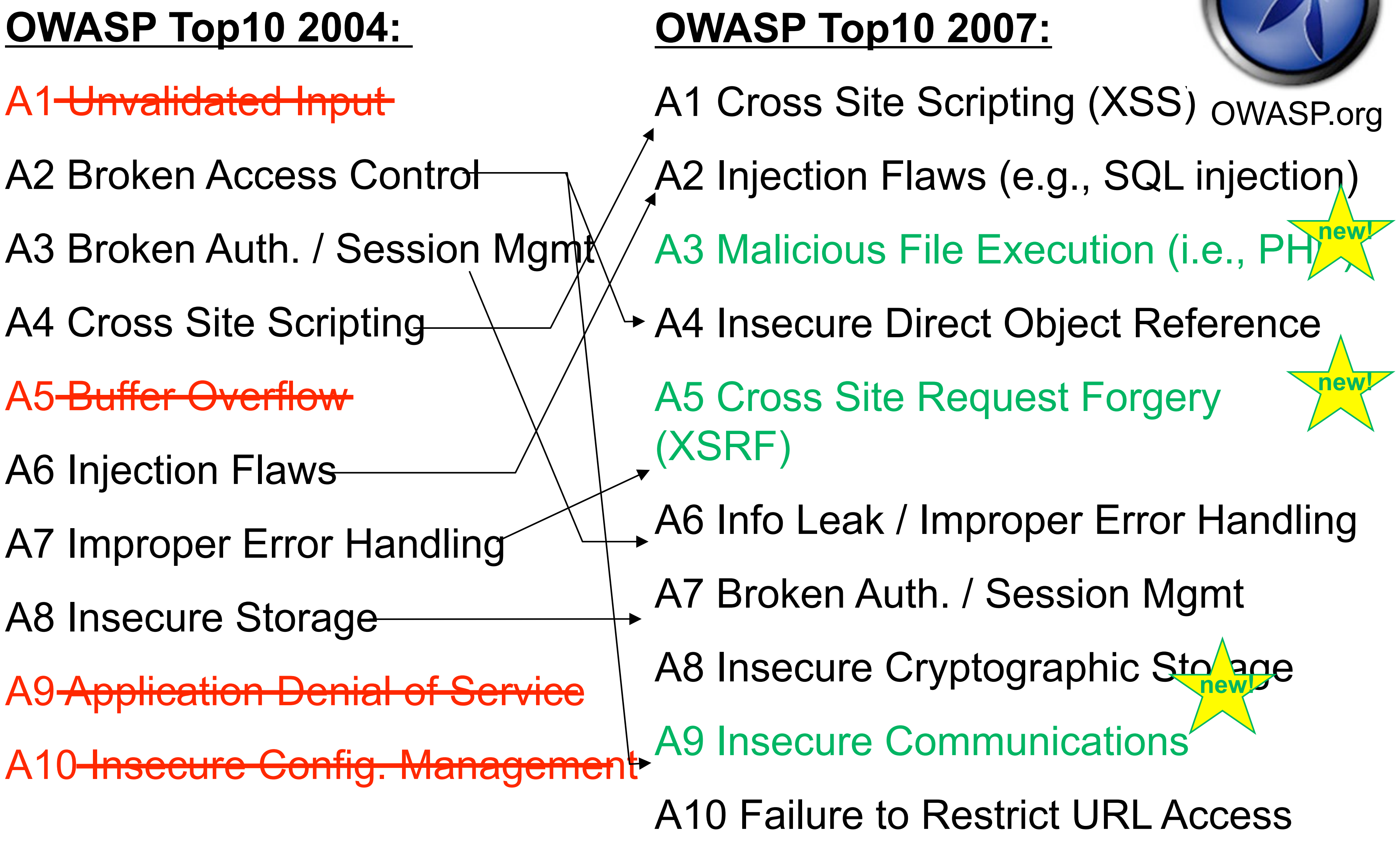
imagination at work

# Challenges, why is this so hard?

imagination at work

# AppSec changes rapidly

OWASP.org



**OWASP Top10 2004:**

A1 ~~Unvalidated Input~~

A2 Broken Access Control

A3 Broken Auth. / Session Mgmt

A4 Cross Site Scripting

A5 ~~Buffer Overflow~~

A6 Injection Flaws

A7 Improper Error Handling

A8 Insecure Storage

A9 ~~Application Denial of Service~~

A10 ~~Insecure Config. Management~~

**OWASP Top10 2007:**

A1 Cross Site Scripting (XSS)

A2 Injection Flaws (e.g., SQL injection)

A3 Malicious File Execution (i.e., PHP) new!

A4 Insecure Direct Object Reference

A5 Cross Site Request Forgery (XSRF) new!

A6 Info Leak / Improper Error Handling

A7 Broken Auth. / Session Mgmt

A8 Insecure Cryptographic Storage new!

A9 Insecure Communications

A10 Failure to Restrict URL Access

imagination at work

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

# Changing landscape

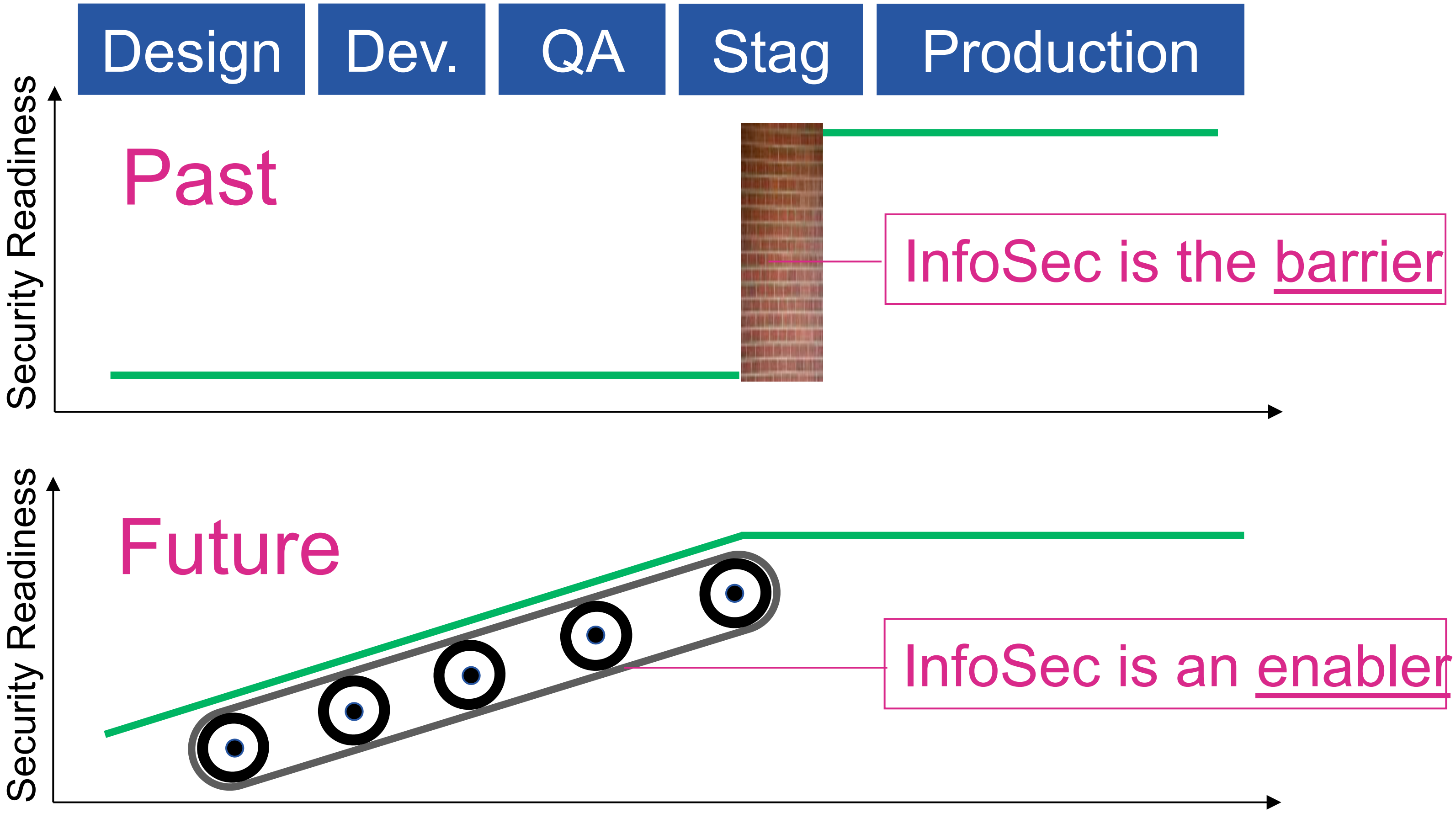
1. Increased skill and talent pool of technically proficient individuals willing to break the law
2. Growing volume of financially valuable data online (PII and corporate intellectual property
3. Development of criminal markets (black markets) to facilitate conversion to money

***attackers now have effective skills, something to steal, and a place to sell it***

**Completely one-sided: we must find <u>all</u> vulnerabilities while the bad guys only need to find <u>one</u>**

imagination at work

# Becoming an enabler (not a barrier)



Past

InfoSec is the barrier

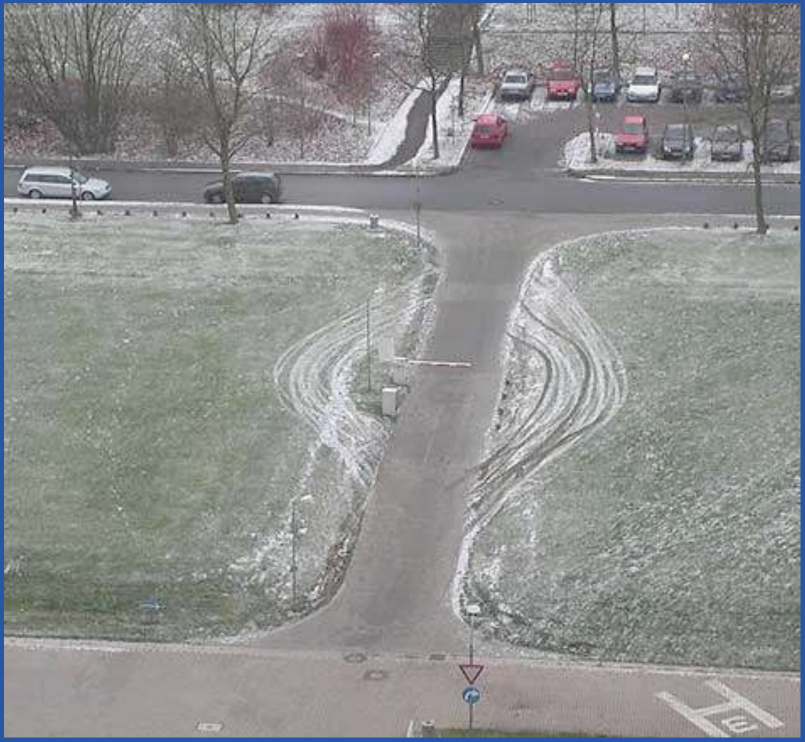
Future

InfoSec is an enabler

Must inject application security earlier through Guidance, Education and Tools

imagination at work

# Ineffective tollgates lead to …

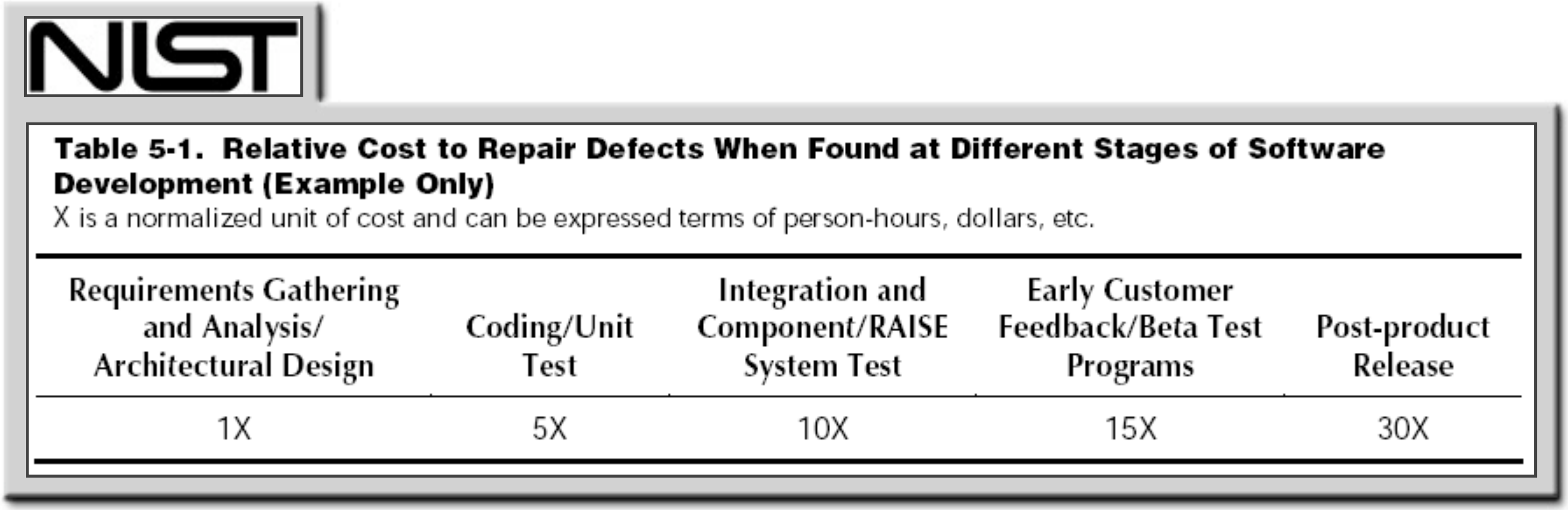


Must understand the development and deployment process and integrate rather than mandate

imagination at work

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

# Applying security at the right time



NIST

**Table 5-1. Relative Cost to Repair Defects When Found at Different Stages of Software Development (Example Only)**

X is a normalized unit of cost and can be expressed terms of person-hours, dollars, etc.

| Requirements Gathering and Analysis/ Architectural Design | Coding/Unit Test | Integration and Component/RAISE System Test | Early Customer Feedback/Beta Test Programs | Post-product Release |
|---|---|---|---|---|
| 1X | 5X | 10X | 15X | 30X |

$ $ $ $ $ $ $ $ $ $ $ $ $

$ http://www.nist.gov/director/prog-ofc/report02-3.pdf

# Solving the problem for the enterprise

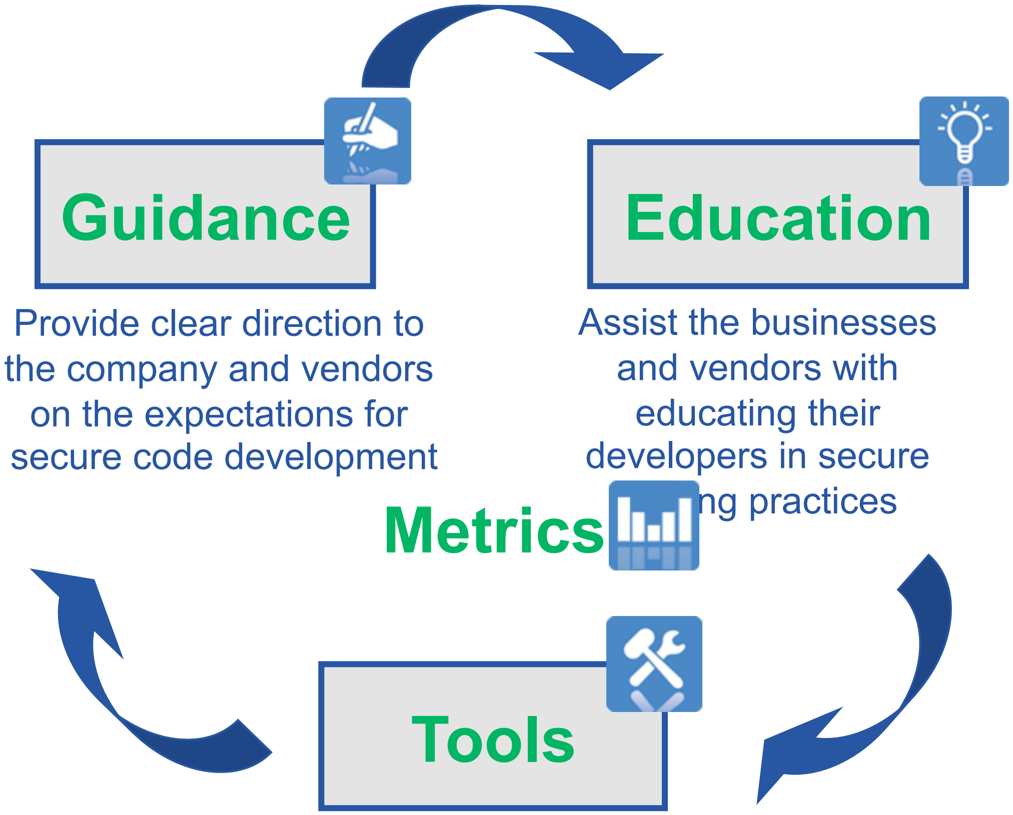
Culture
Change

# Some success factors

- ✓ Form a **mission** and **strategy**
- ✓ Develop **policy** (but not corporate "mandate")
- ✓ Gain **executive buy-in** (cost / benefit / risk)
- ✓ Understand the **magnitude** of problem (metrics)
- ✓ Asset **inventory** and **vulnerability management**
- ✓ Develop **standards** (what should I do and when?)
- ✓ Establish a formal **program** (strong **leadership**)
- ✓ Focus on **education** and training materials
- ✓ Develop **in-house** expertise, services and "COE"
- ✓ Continuous improvement, **measurement**, KPI
- ✓ **Communicate, communicate, communicate …**
- ✓ Drive a **culture change** (shared need, WIIFM)
- ✓ Communicate **expectations** with vendors
- ✓ Implement **incentives** (and penalties)
- ✓ **Digitize** after the process is solid (tools)

# AppSec program mission & structure

**The Application Security Program will achieve and maintain a strong application security posture across the company through the implementation of consistent and unified guidance, education and tools.**



Guidance

Provide clear direction to the company and vendors on the expectations for secure code development

Education

Assist the businesses and vendors with educating their developers in secure ng practices

Metrics

Tools

Identify tools to ensure secure code, assist in the deployment of those tools

Guidance

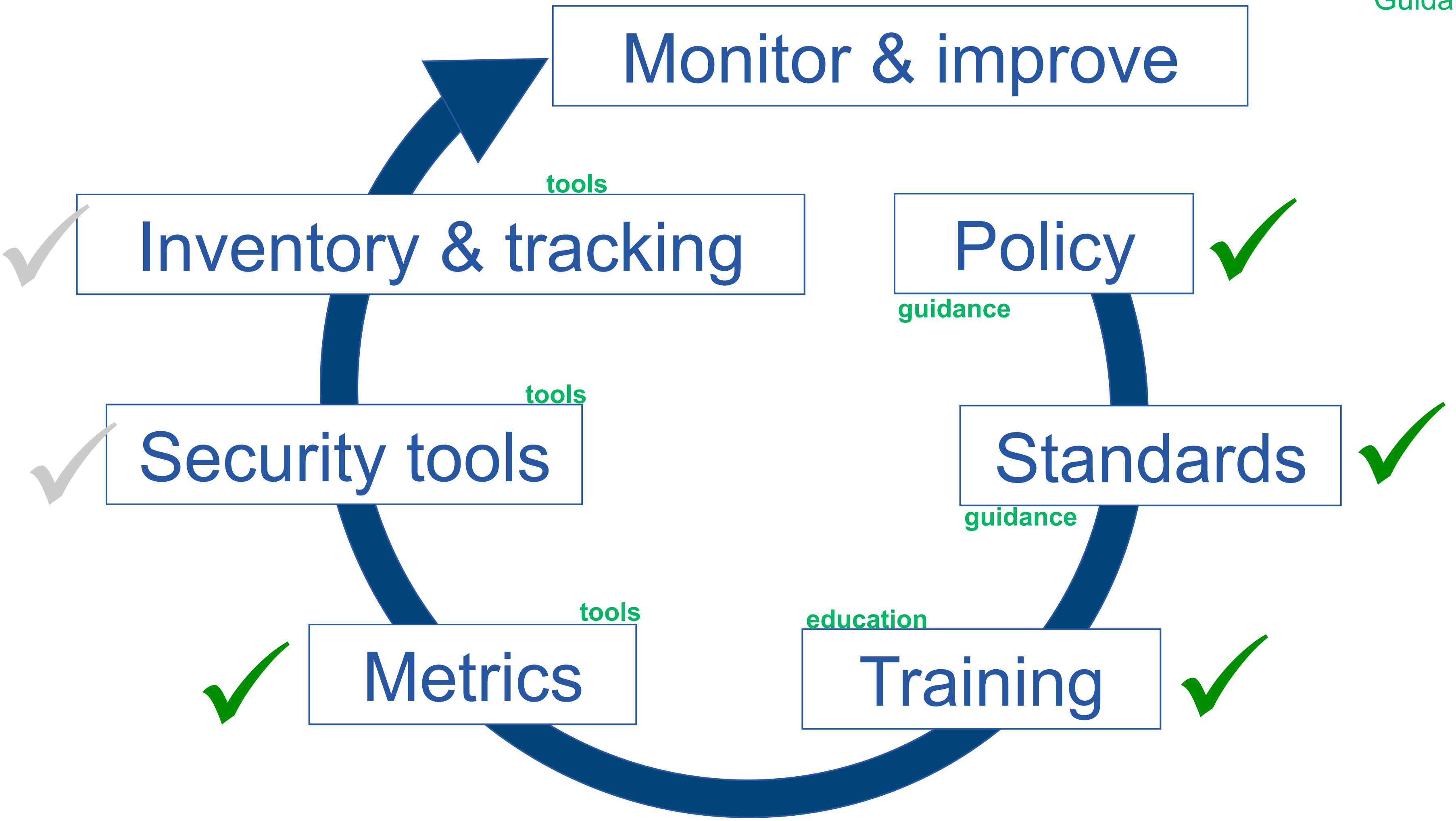
Education

Tools

imagination at work

# AppSec program strategy

Guidance



Monitor & improve

tools

✓ Inventory & tracking

Policy ✓

guidance

tools

✓ Security tools

Standards ✓

guidance

tools

✓ Metrics

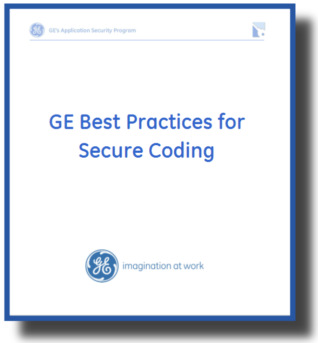
education

Training ✓

imagination at work

# Guidance

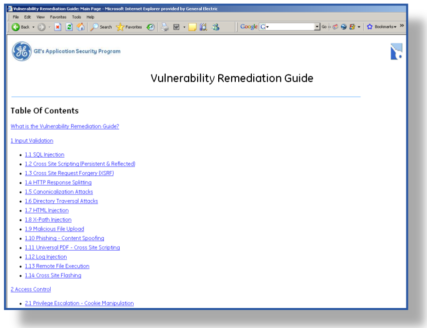
Guidance


GE's Application Security Program

GE Best Practices for Secure Coding

imagination at work

Secure Coding Guidelines


Vulnerability Remediation Guide: Main Page - Microsoft Internet Explorer provided by General Electric

GE's Application Security Program

Vulnerability Remediation Guide

Table Of Contents

What is the Vulnerability Remediation Guide?

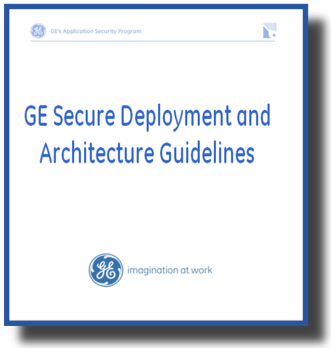
1 Input Validation

- 1.1 SQL Injection
- 1.2 Cross Site Scripting (Persistent & Reflected)
- 1.3 Cross Site Request Forgery (XSRF)
- 1.4 HTTP Response Splitting
- 1.5 Canonicalization Attacks
- 1.6 Directory Traversal Attacks
- 1.7 HTML Injection
- 1.8 X-Path Injection
- 1.9 Malicious File Upload
- 1.10 Phishing - Content Spoofing
- 1.11 Universal PDF - Cross Site Scripting
- 1.12 Log Injection
- 1.13 Remote File Execution
- 1.14 Cross Site Flashing

2 Access Control

- 2.1 Privilege Escalation - Cookie Manipulation

Vulnerability Remediation Guide

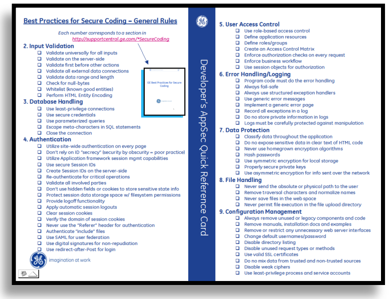

GE's Application Security Program

GE Secure Deployment and Architecture Guidelines

imagination at work

Secure Deployment

GE Application Security Working Group


Best Practices for Secure Coding – General Rules

*Each number corresponds to a section in* http://supportcentral.ge.com/*SecureCoding

GE Best Practices for Secure Coding

2. Input Validation

- ❑ Validate universally for all inputs
- ❑ Validate on the server-side
- ❑ Validate first before other actions
- ❑ Validate all external data connections
- ❑ Validate data range and length
- ❑ Check for null-bytes
- ❑ Whitelist (known good entities)
- ❑ Perform HTML Entity Encoding

3. Database Handling

- ❑ Use least-privilege connections
- ❑ Use secure credentials
- ❑ Use parameterized queries
- ❑ Escape meta-characters in SQL statements
- ❑ Close the connection

4. Authentication

- ❑ Utilize site-wide authentication on every page
- ❑ Don't rely on ID "secrecy" (security by obscurity = poor practice)
- ❑ Utilize Application framework session mgmt capabilities
- ❑ Use secure Session IDs
- ❑ Create Session IDs on the server-side
- ❑ Re-authenticate for critical operations
- ❑ Validate all involved parties
- ❑ Don't use hidden fields or cookies to store sensitive state info
- ❑ Protect session data storage space w/ filesystem permissions
- ❑ Provide logoff functionality
- ❑ Apply automatic session logouts
- ❑ Clear session cookies
- ❑ Verify the domain of session cookies
- ❑ Never use the "Referer" header for authentication
- ❑ Authenticate "include" files
- ❑ Use SAML for user federation
- ❑ Use digital signatures for non-repudiation
- ❑ Use redirect-after-Post for login

imagination at work

Developer's AppSec Quick Reference Card

5. User Access Control

- ❑ Use role-based access control
- ❑ Define application resources
- ❑ Define roles/groups
- ❑ Create an Access Control Matrix
- ❑ Enforce authorization checks on every request
- ❑ Enforce business workflow
- ❑ Use session objects for authorization

6. Error Handling/Logging

- ❑ Program code must do the error handling
- ❑ Always fail-safe
- ❑ Always use structured exception handlers
- ❑ Use generic error messages
- ❑ Implement a generic error page
- ❑ Record all exceptions in a log
- ❑ Do no store private information in logs
- ❑ Logs must be carefully protected against manipulation

7. Data Protection

- ❑ Classify data throughout the application
- ❑ Do no expose sensitive data in clear text of HTML code
- ❑ Never use homegrown encryption algorithms
- ❑ Hash passwords
- ❑ Use symmetric encryption for local storage
- ❑ Properly secure private keys
- ❑ Use asymmetric encryption for info sent over the network

8. File Handling

- ❑ Never send the absolute or physical path to the user
- ❑ Remove traversal characters and normalize names
- ❑ Never save files in the web space
- ❑ Never permit file execution in the file upload directory

9. Configuration Management

- ❑ Always remove unused or legacy components and code
- ❑ Remove manuals, installation docs and examples
- ❑ Remove or restrict any unnecessary web server interfaces
- ❑ Change default usernames/password
- ❑ Disable directory listing
- ❑ Disable unused request types or methods
- ❑ Use valid SSL certificates
- ❑ Do no mix data from trusted and non-trusted sources
- ❑ Disable weak ciphers
- ❑ Use least-privilege process and service accounts

Quick Reference Card

Contractual language

GE Application Security Program

Focused on elimination and early detection of application security defects.

imagination at work

2009 Calendar

Desk Calendars

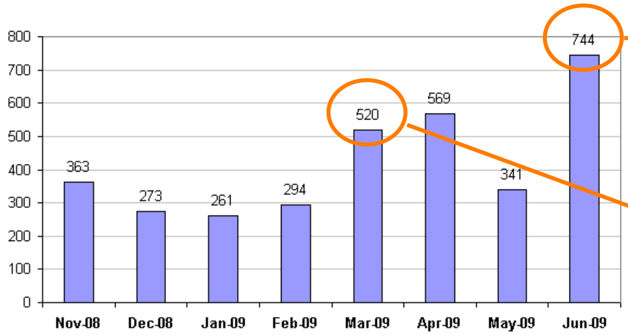
imagination at work

# Guidance

Guidance

## AppSec Calendars helped increase visitors to key Guidance materials

hits for “Best Practices for Secure Coding” spiked in March & June



June 2009

Guidance

SSDLC, BPSC, VRG, BPSDB, SDAG

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 |  |  |  |  |

Guidance

Available application security guidance:

SSDLC - Secure Software Development Life Cycle
BPSC - GE Best Practices for Secure Coding
VRG - Vulnerability Remediation Guide
BPSDB - GE Best Practices for Secure Databases
SDAG - Secure Deployment and Architecture Guide

GE Internal - Proprietary - All Rights Reserved

*More information on back*

imagination at work GE Application Security Program

March 2009

GE Best Practices for Secure Coding

http://sc.ge.com/*SecureCodin

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 |  |  |  |  |

Best Practices for Secure Coding

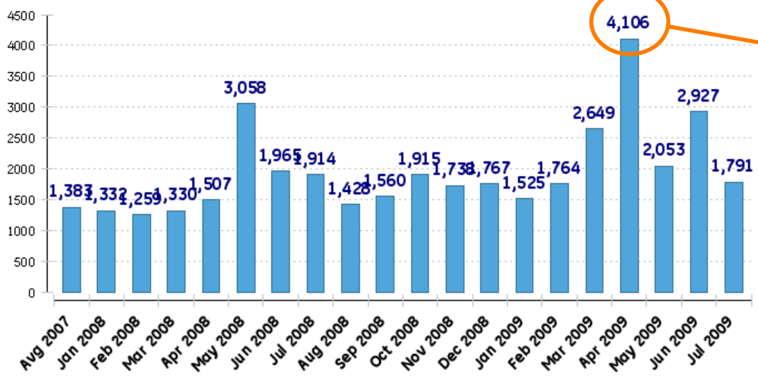
This GE Guide outlines how to develop secure code and is intended to be followed by developers as a "checklist" of important items needed to develop secure code and applications. A Quick Reference Card summarizes these activities in a convenient checklist (see April and the last page of this calendar).

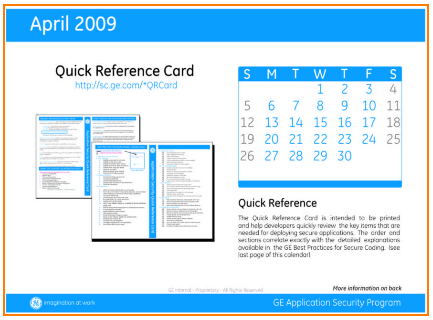
GE Internal - Proprietary - All Rights Reserved

*More information on back*

imagination at work GE Application Security Program

# Downloads Per Month On Support Central





April 2009

Quick Reference Card

http://sc.ge.com/*QRCard

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
|  |  |  | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 |  |  |

Quick Reference

The Quick Reference Card is intended to be printed and help developers quickly review the key items that are needed for deploying secure applications. The order and sections correlate exactly with the detailed explanations available in the GE Best Practices for Secure Coding. (see last page of this calendar)

GE Internal - Proprietary - All Rights Reserved

*More information on back*

imagination at work GE Application Security Program

downloads doubled in April when Quick Reference Card with “Quick links” appeared

# Education

Education

**CBT1:** Intro to AppSec at GE (60 min)

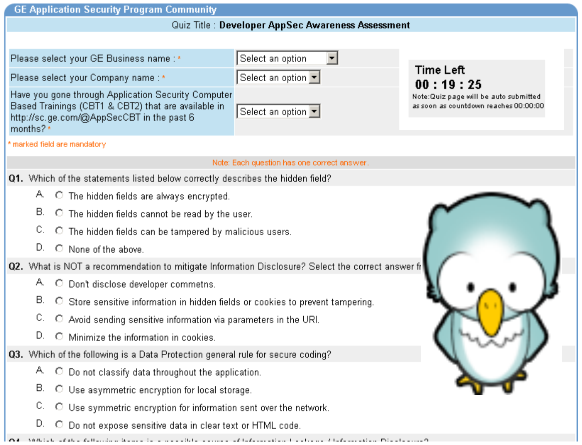
GE Best Practices for Secure Coding

**CBT2:** GE Best Practices for Secure Coding (90 min)

~~**CBT3:** Attack Profiles & Countermeasures (120~~ min)

## Developer Awareness Assessment:

- 100’s of internally-developed questions
- Randomized questions, timed completion
- Vendors track their own results
- Allows tailoring of training / awareness programs



GE Application Security Program Community

Quiz Title : **Developer AppSec Awareness Assessment**

| | | |
|---|---|---|
| Please select your GE Business name : * | Select an option | Time Left<br>**00 : 19 : 25**<br>Note:Quiz page will be auto submitted as soon as countdown reaches 00:00:00 |
| Please select your Company name : * | Select an option | |
| Have you gone through Application Security Computer Based Trainings (CBT1 & CBT2) that are available in http://sc.ge.com/@AppSecCBT in the past 6 months? * | Select an option | |

* marked field are mandatory

Note: Each question has one correct answer.

**Q1.** Which of the statements listed below correctly describes the hidden field?

A. ○ The hidden fields are always encrypted.

B. ○ The hidden fields cannot be read by the user.

C. ○ The hidden fields can be tampered by malicious users.

D. ○ None of the above.

**Q2.** What is NOT a recommendation to mitigate Information Disclosure? Select the correct answer fr

A. ○ Don't disclose developer commetns.

B. ○ Store sensitive information in hidden fields or cookies to prevent tampering.

C. ○ Avoid sending sensitive information via parameters in the URI.

D. ○ Minimize the information in cookies.

**Q3.** Which of the following is a Data Protection general rule for secure coding?

A. ○ Do not classify data throughout the application.

B. ○ Use asymmetric encryption for local storage.

C. ○ Use symmetric encryption for information sent over the network.

D. ○ Do not expose sensitive data in clear text or HTML code.

**Q4.** Which of the following items is a possible source of Information Leakage / Information Disclosure?

imagination at work

# Tools

Tools

- ✓ COE AppSec assessment services
- ✓ Vendor framework & Metrics
- ✓ Compliance Handbook
- ✓ Common objects repository
- ✓ GE Enterprise Application Security
- ✓ Scanning & Monitoring tools

```
codebase="http://download.ma
 WIDTH=400 HEIGHT=300>
 <PARAM NAME=movie VALUE="ki
NAME=play VALUE=true> <PARAM
VALUE=high> <PARAM NAME=bgco
<EMBED src="kikkomaso.swf" p
bgcolor=#000000  WIDTH=400 H
TYPE="application/x-shockwav
PLUGINSPAGE="http://www.macr
```

GE EAS

Enterprise Application Security

Automation is the way to go (but the tools are not quite there yet)

imagination at work

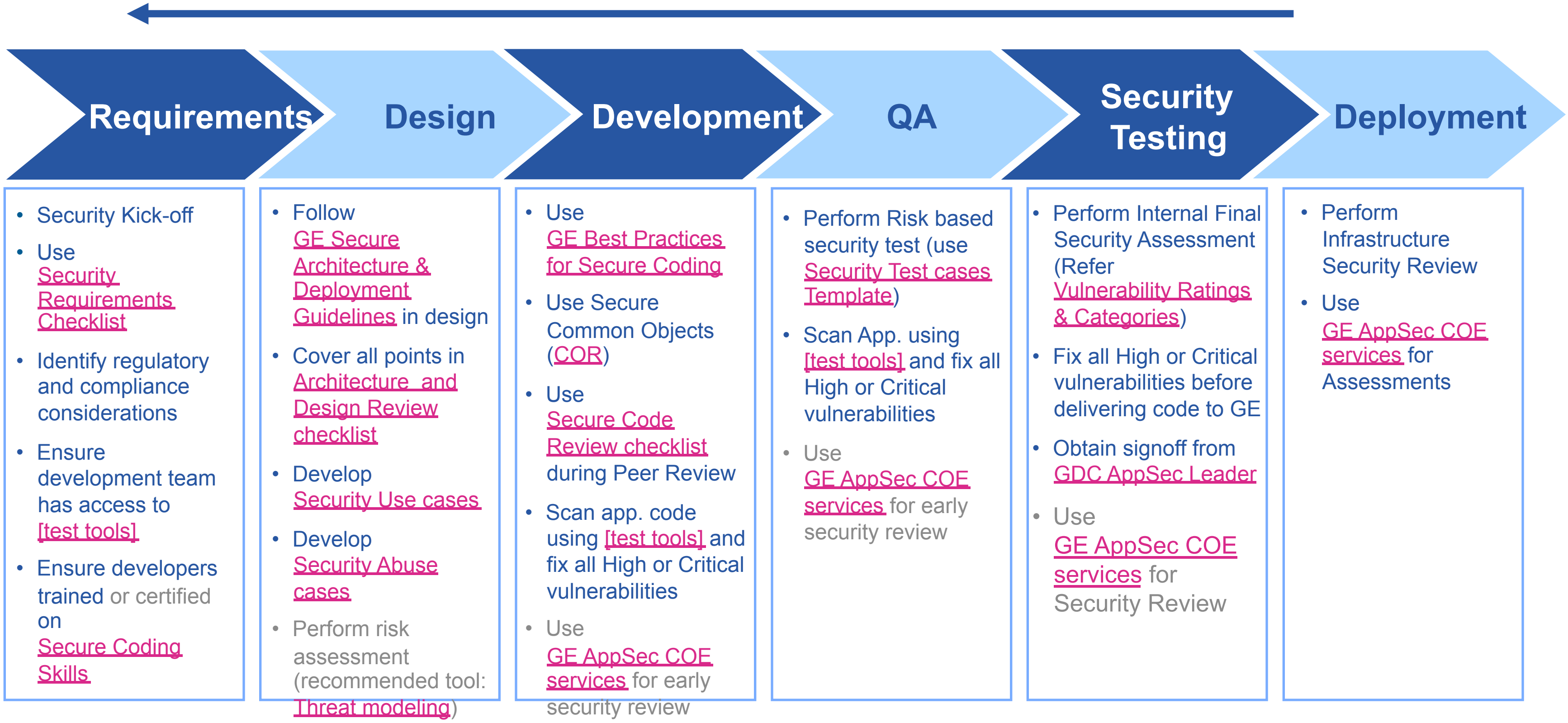
# Managing vendor performance

imagination at work

# GE secure SDL framework

Tools

Goal: prevent, detect or correct security defects earlier



**Requirements**

- Security Kick-off
- Use Security Requirements Checklist
- Identify regulatory and compliance considerations
- Ensure development team has access to [test tools]
- Ensure developers trained or certified on Secure Coding Skills

**Design**

- Follow GE Secure Architecture & Deployment Guidelines in design
- Cover all points in Architecture and Design Review checklist
- Develop Security Use cases
- Develop Security Abuse cases
- Perform risk assessment (recommended tool: Threat modeling)

**Development**

- Use GE Best Practices for Secure Coding
- Use Secure Common Objects (COR)
- Use Secure Code Review checklist during Peer Review
- Scan app. code using [test tools] and fix all High or Critical vulnerabilities
- Use GE AppSec COE services for early security review

**QA**

- Perform Risk based security test (use Security Test cases Template)
- Scan App. using [test tools] and fix all High or Critical vulnerabilities
- Use GE AppSec COE services for early security review

**Security Testing**

- Perform Internal Final Security Assessment (Refer Vulnerability Ratings & Categories)
- Fix all High or Critical vulnerabilities before delivering code to GE
- Obtain signoff from GDC AppSec Leader
- Use GE AppSec COE services for Security Review

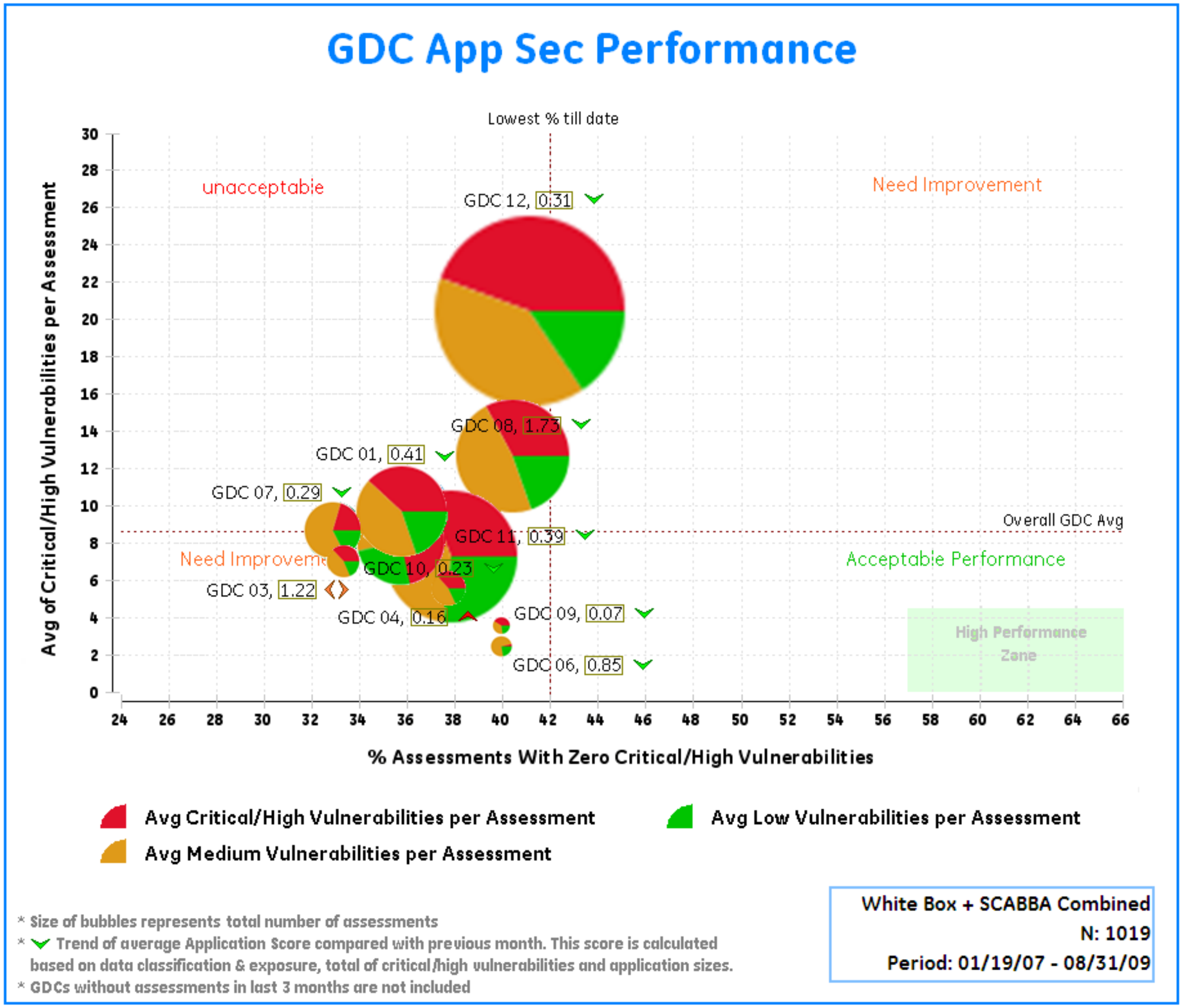
**Deployment**

- Perform Infrastructure Security Review
- Use GE AppSec COE services for Assessments

imagination at work

# Vendor AppSec Performance

Tools



GDC App Sec Performance

White Box + SCABBA Combined
N: 1019
Period: 01/19/07 - 08/31/09

* Size of bubbles represents total number of assessments

* ✓ Trend of average Application Score compared with previous month. This score is calculated based on data classification & exposure, total of critical/high vulnerabilities and application sizes.

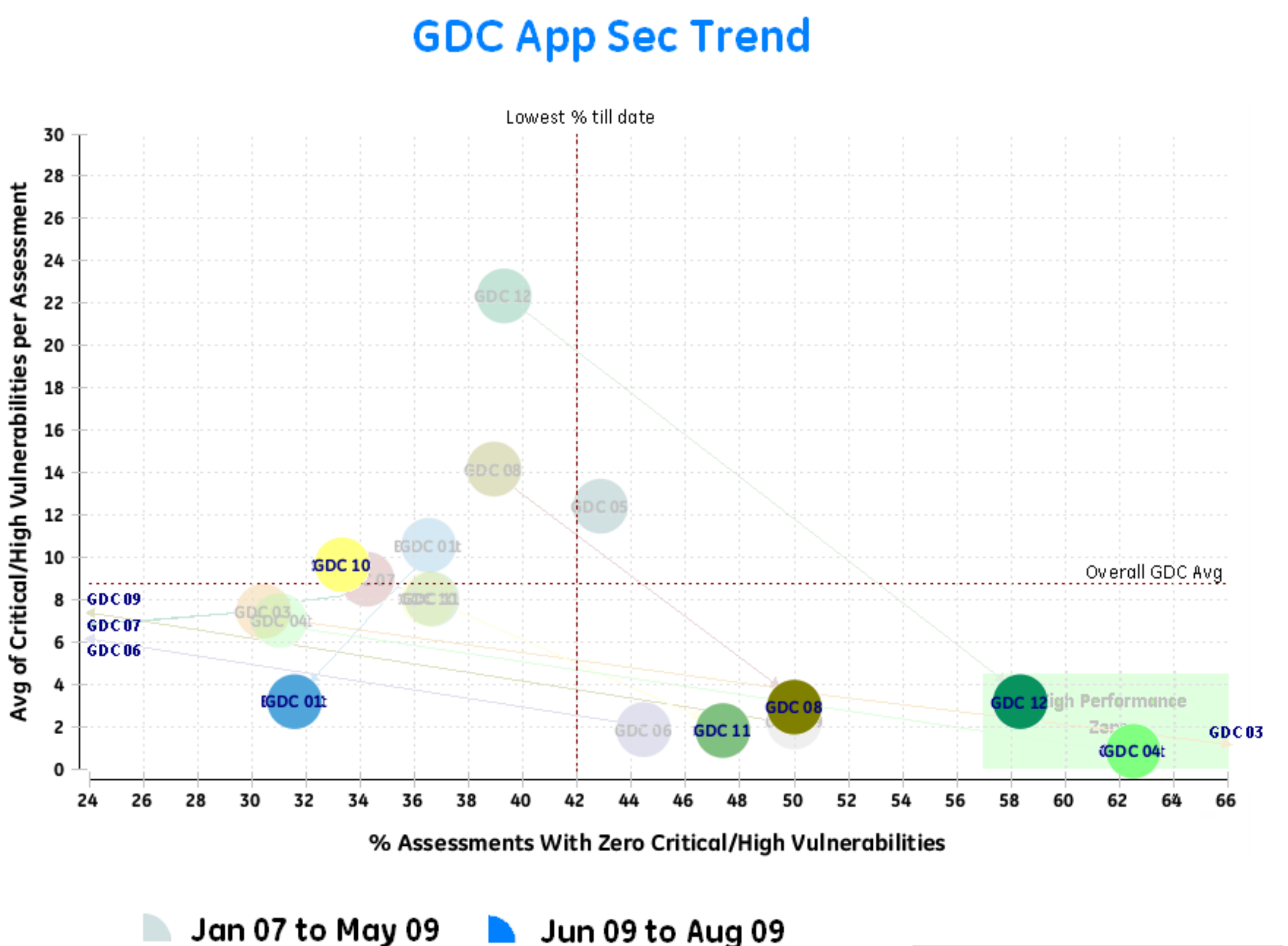
* GDCs without assessments in last 3 months are not included

imagination at work

# Vendor AppSec Performance

Tools

## GDC App Sec Trend



White Box + SCABBA Combined
N: 1019
Period: 01/19/07 - 08/31/09

* GDCs without assessments during showed periods are not included

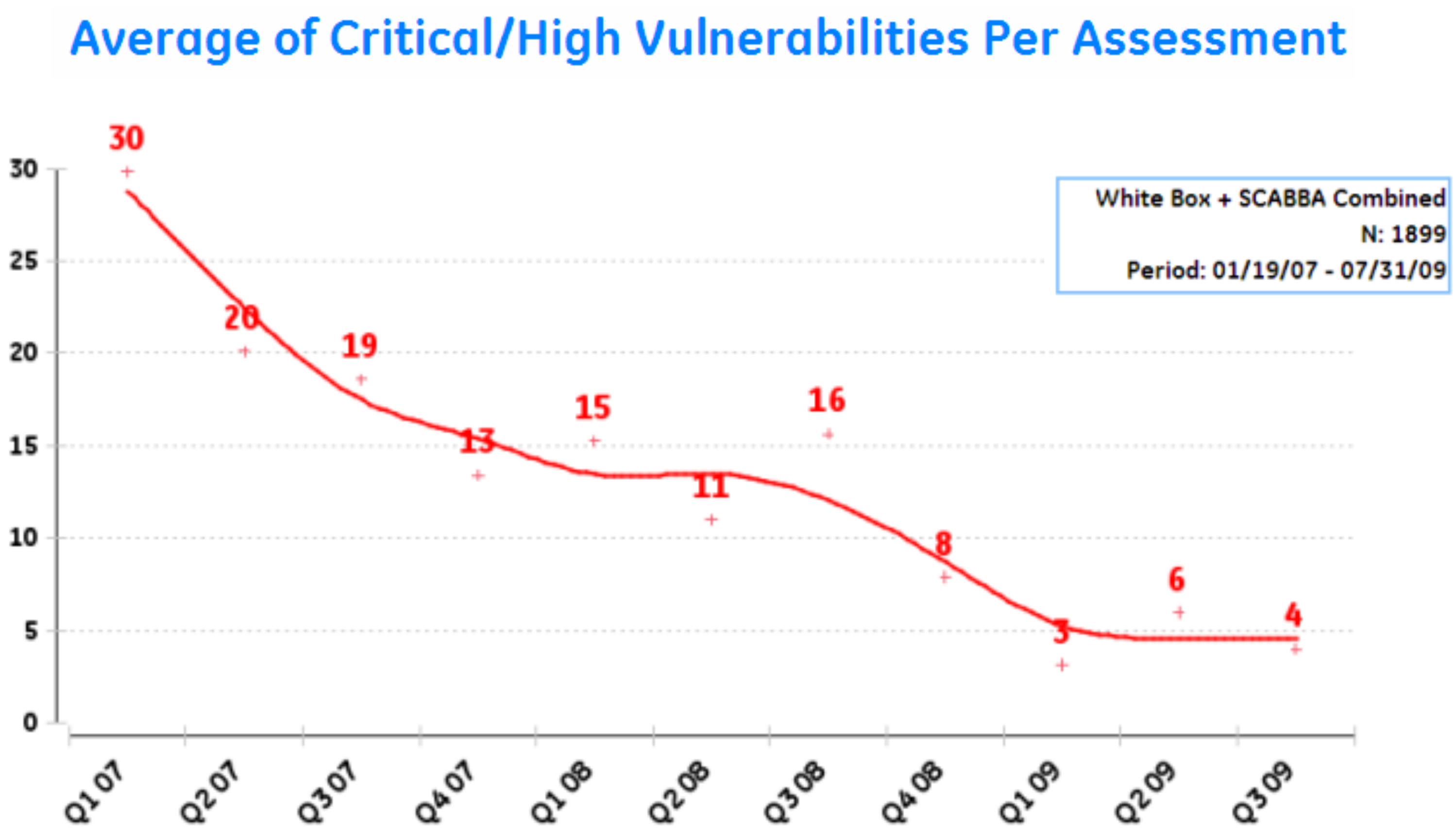
imagination at work

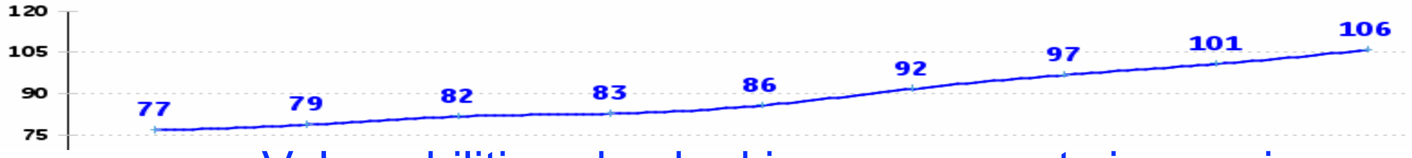
# So is any of this making a difference?

imagination at work

# Is it making a difference?

Tools





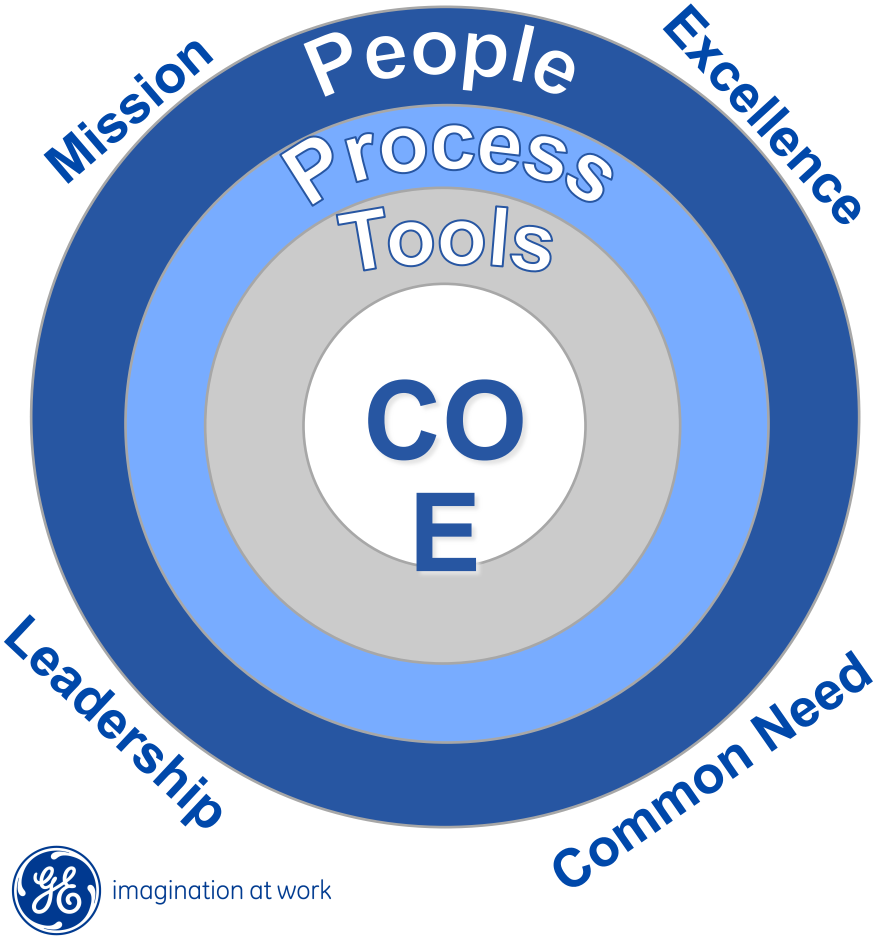
Vulnerabilities checked in assessments increasing

imagination at work

# Forming a “center of excellence”

# What is a COE?

A “Center of Excellence” combines the best available people, processes and tools to deliver low cost / high quality services and guidance under strong leadership with a clear mission.



## People

- Expertise (internal and external)
- Multi-disciplinary capability
- Cross-business steering committee

## Process Excellence

- Standard engagement model
- Cycle time reductions through Lean
- Managed w/ metrics to drive behavior
- Leverage Internal best practices
- External benchmarking

## Tools

- Central deployment / management
- Leverage enterprise agreements
- Start with process, follow with tools

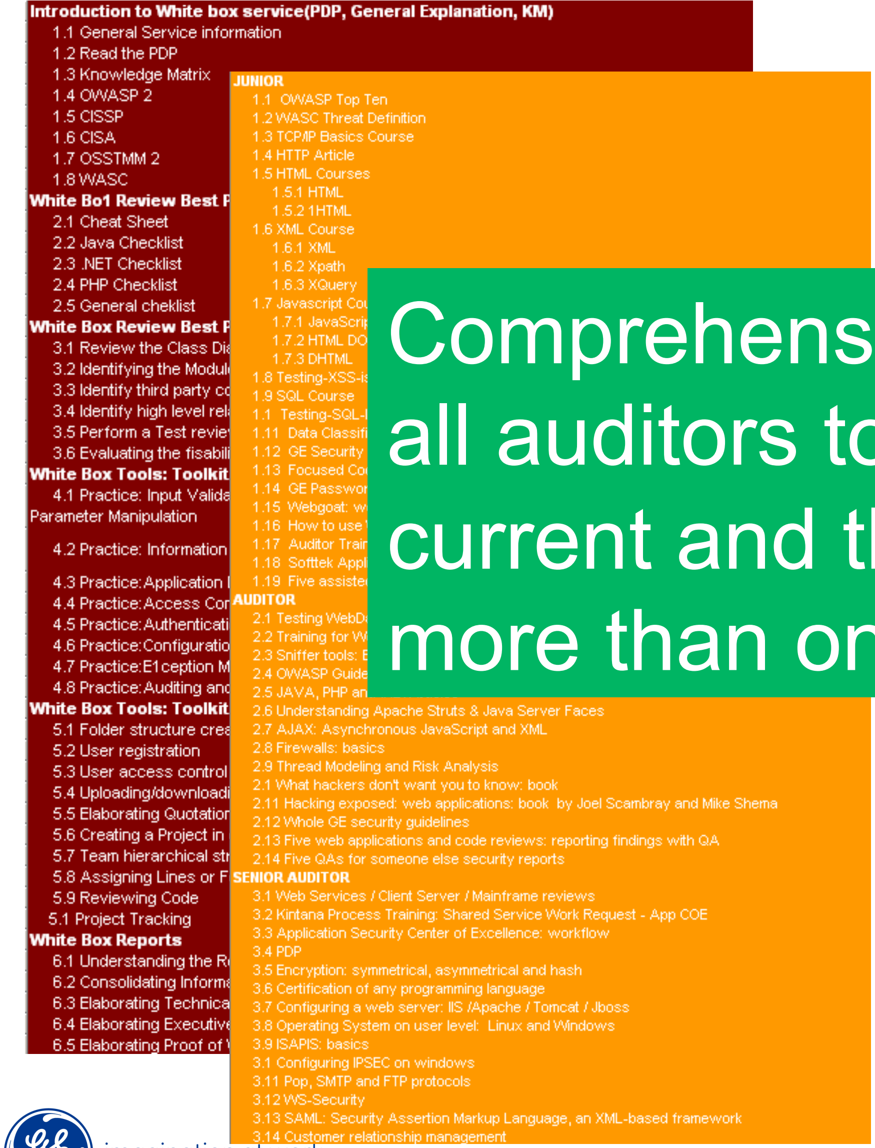
imagination at work

# Softtek Facilities

## Biometric Access:

## Privacy Glass:

# Formal training & defined roles



**Introduction to White box service(PDP, General Explanation, KM)**
- 1.1 General Service information
- 1.2 Read the PDP
- 1.3 Knowledge Matrix
- 1.4 OWASP 2
- 1.5 CISSP
- 1.6 CISA
- 1.7 OSSTMM 2
- 1.8 WASC

**White Bo1 Review Best P**
- 2.1 Cheat Sheet
- 2.2 Java Checklist
- 2.3 .NET Checklist
- 2.4 PHP Checklist
- 2.5 General cheklist

**White Box Review Best P**
- 3.1 Review the Class Dia
- 3.2 Identifying the Modul
- 3.3 Identify third party co
- 3.4 Identify high level rela
- 3.5 Perform a Test revie
- 3.6 Evaluating the fisabili

**White Box Tools: Toolkit**
- 4.1 Practice: Input Valida Parameter Manipulation
- 4.2 Practice: Information
- 4.3 Practice:Application I
- 4.4 Practice:Access Cor
- 4.5 Practice:Authenticati
- 4.6 Practice:Configuratio
- 4.7 Practice:E1ception M
- 4.8 Practice:Auditing anc

**White Box Tools: Toolkit**
- 5.1 Folder structure crea
- 5.2 User registration
- 5.3 User access control
- 5.4 Uploading/downloadi
- 5.5 Elaborating Quotation
- 5.6 Creating a Project in
- 5.7 Team hierarchical str
- 5.8 Assigning Lines or F
- 5.9 Reviewing Code
- 5.1 Project Tracking

**White Box Reports**
- 6.1 Understanding the R
- 6.2 Consolidating Informa
- 6.3 Elaborating Technica
- 6.4 Elaborating Executive
- 6.5 Elaborating Proof of V

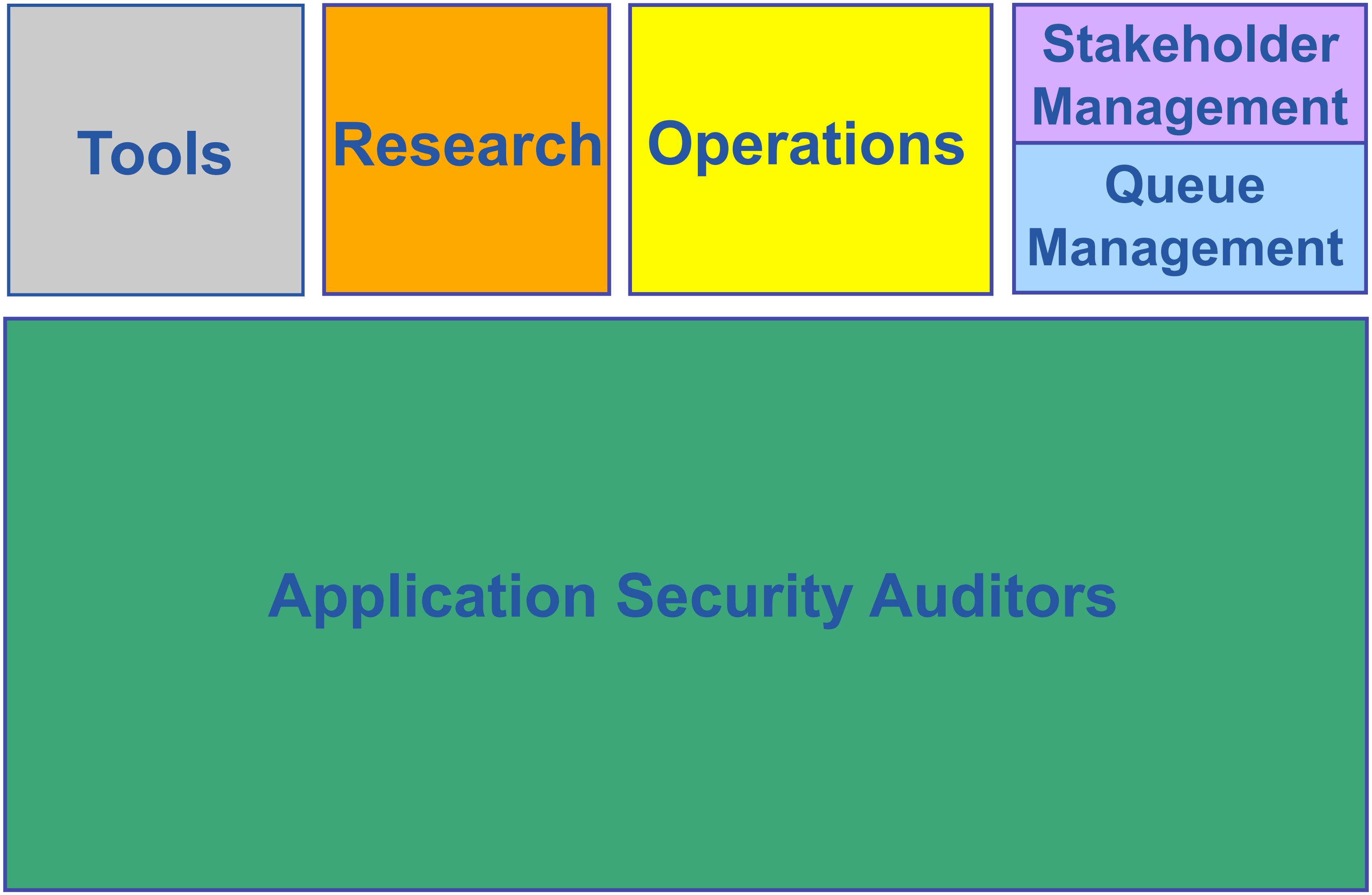
**JUNIOR**
- 1.1 OWASP Top Ten
- 1.2 WASC Threat Definition
- 1.3 TCP/IP Basics Course
- 1.4 HTTP Article
- 1.5 HTML Courses
  - 1.5.1 HTML
  - 1.5.2 1HTML
- 1.6 XML Course
  - 1.6.1 XML
  - 1.6.2 Xpath
  - 1.6.3 XQuery
- 1.7 Javascript Cou
  - 1.7.1 JavaScrip
  - 1.7.2 HTML DO
  - 1.7.3 DHTML
- 1.8 Testing-XSS-is
- 1.9 SQL Course
- 1.1 Testing-SQL-I
- 1.11 Data Classifi
- 1.12 GE Security
- 1.13 Focused Co
- 1.14 GE Passwor
- 1.15 Webgoat: w
- 1.16 How to use
- 1.17 Auditor Trai
- 1.18 Softtek Appl
- 1.19 Five assiste

**AUDITOR**
- 2.1 Testing WebD
- 2.2 Training for W
- 2.3 Sniffer tools: E
- 2.4 OWASP Guide
- 2.5 JAVA, PHP an
- 2.6 Understanding Apache Struts & Java Server Faces
- 2.7 AJAX: Asynchronous JavaScript and XML
- 2.8 Firewalls: basics
- 2.9 Thread Modeling and Risk Analysis
- 2.1 What hackers don't want you to know: book
- 2.11 Hacking exposed: web applications: book by Joel Scambray and Mike Shema
- 2.12 Whole GE security guidelines
- 2.13 Five web applications and code reviews: reporting findings with QA
- 2.14 Five QAs for someone else security reports

**SENIOR AUDITOR**
- 3.1 Web Services / Client Server / Mainframe reviews
- 3.2 Kintana Process Training: Shared Service Work Request - App COE
- 3.3 Application Security Center of Excellence: workflow
- 3.4 PDP
- 3.5 Encryption: symmetrical, asymmetrical and hash
- 3.6 Certification of any programming language
- 3.7 Configuring a web server: IIS /Apache / Tomcat / Jboss
- 3.8 Operating System on user level: Linux and Windows
- 3.9 ISAPIS: basics
- 3.1 Configuring IPSEC on windows
- 3.11 Pop, SMTP and FTP protocols
- 3.12 WS-Security
- 3.13 SAML: Security Assertion Markup Language, an XML-based framework
- 3.14 Customer relationship management

Comprehensive training program for all auditors to ensure skills are kept current and that auditors can provide more than one type of service.

# COE team structure



Tools

Research

Operations

Stakeholder Management

Queue Management

Application Security Auditors

# Application Assessment Types

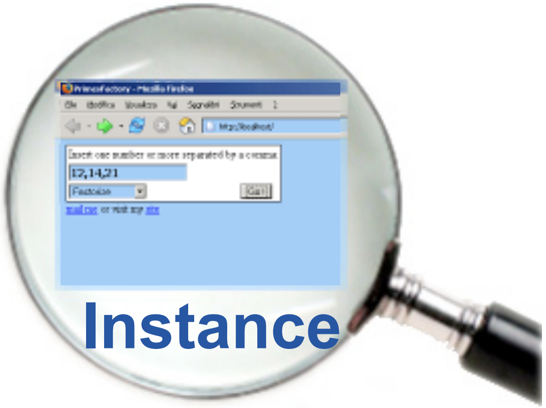
## Black / Gray Box

**Benefits:**

- Quick, cost-effective and targeted
- No source code needed
- Identify configuration issues
- Many more findings vs. scanner

**Better at finding:**

- Access Control / Auth. issues
- Configuration Mgt. Issues
- Input Validation (faster)



Insert one number or more separated by a comma.

12,14,21

mail me or visit my site

## White Box

**Benefits:**

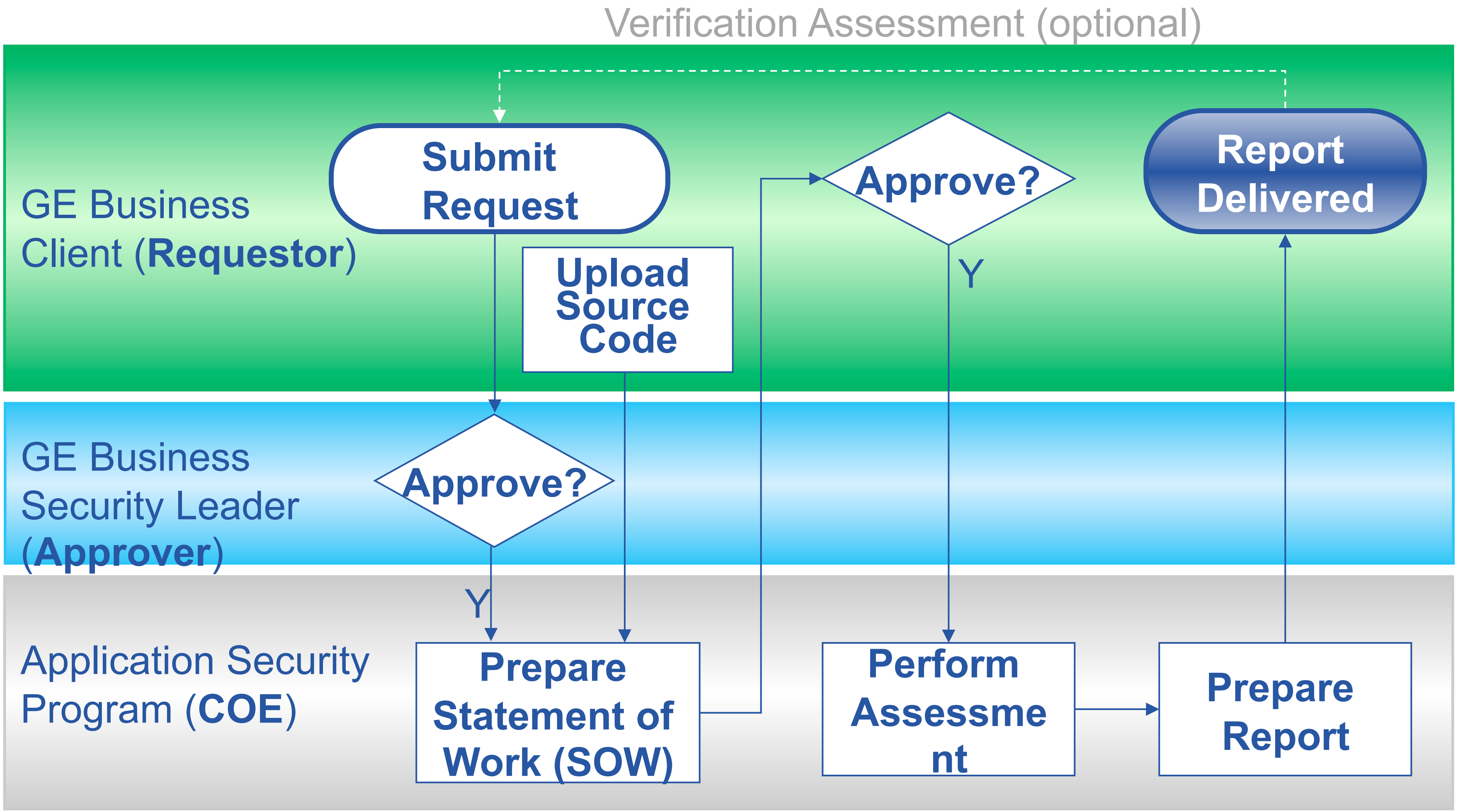
- Comprehensive, seeks all vulnerabilities
- Does not require a “live instance”
- Detailed developer remediation help

**Better at finding:**

- Sensitive information
- Input validation problems
- Exception management issues
- Back doors, logic bombs

```
codebase="http://download.mac
 WIDTH=400 HEIGHT=300>
 <PARAM NAME=movie VALUE="kil
NAME=play VALUE=true> <PARAM
VALUE=high> <PARAM NAME=bgcol
<EMBED src="kikkomaso.swf" pl
bgcolor=#000000  WIDTH=400 HE
TYPE="application/x-shockwave
PLUGINSPAGE="http://www.macro
```

# Application assessment process


Verification Assessment (optional)
GE Business Client (**Requestor**)
GE Business Security Leader (**Approver**)
Application Security Program (**COE**)
Submit Request
Upload Source Code
Approve?
Report Delivered
Approve?
Y
Y
Prepare Statement of Work (SOW)
Perform Assessme nt
Prepare Report

imagination at work

# Vulnerability criticality ratings

## 1 Impact

**High** - important assets or functions compromised, total data corruption or all services completely lost

**Medium** - data corruption possible or primary services interrupted

**Low** - non-critical assets or minimal secondary services affected, minor data corruption

## 2 Likelihood

**Low -** vulnerability is very difficult to discover, very difficult to exploit or not directly exposed and attacker would gain very limited application access

**Medium** - vulnerability is relatively difficult to discover, relatively difficult to exploit and attacker would gain limited application access

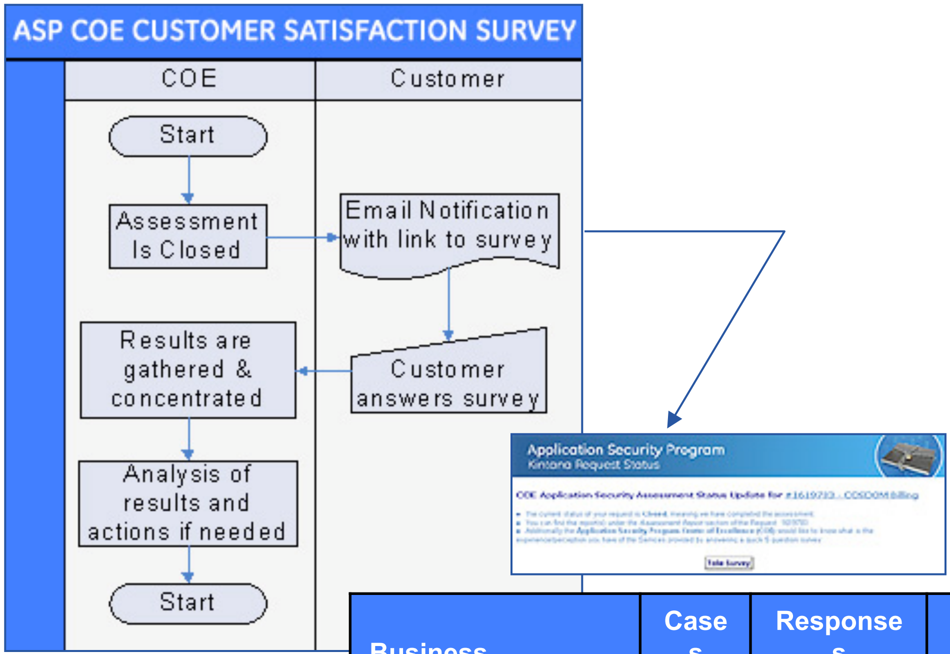
**High** - vulnerability is publicly known , easy to discover, easy to exploit, and attacker would gain full application access

## 3 Vulnerability Criticality Rating

| Impact | Likelihood: Low | Likelihood: Medium | Likelihood: High |
|---|---|---|---|
| High | Medium | High | Critical |
| Medium | Low | Medium | High |
| Low | Info. | Low | Medium |

imagination at work

# COE customer satisfaction survey


ASP COE CUSTOMER SATISFACTION SURVEY
COE
Customer
Start
Assessment Is Closed
Email Notification with link to survey
Customer answers survey
Results are gathered & concentrated
Analysis of results and actions if needed
Start

Application Security Program
Kintana Request Status

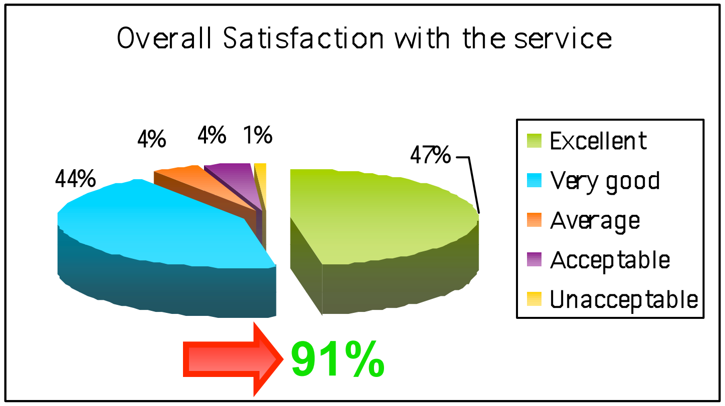
COE Application Security Assessment Status Update for #1619710 - [illegible]

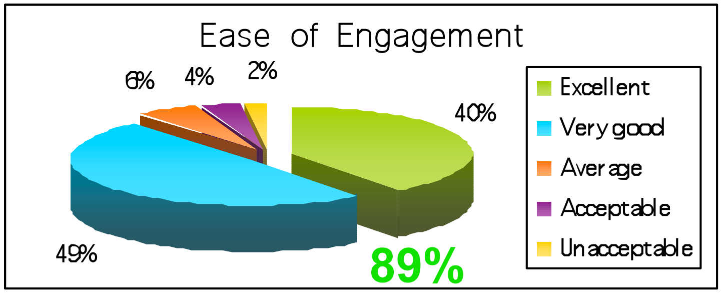
- The current status of your request is **Closed**, meaning we have completed the assessment.
- You can find the report(s) under the Assessment Report section of the Request. [illegible]
- Additionally the **Application Security Program Center of Excellence (COE)** would like to know what is the experience/perception you have of the Services provided by answering a quick 5 question survey.

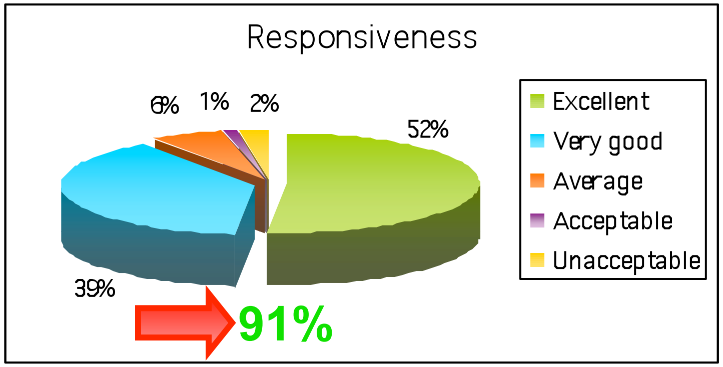
| Business | Cases | Responses | Resp. Rate |
|---|---|---|---|
| Enterprise Solutions | 11 | 1 | 9.1% |
| GE Commercial Finance | 149 | 20 | 13.4% |
| GE Corporate | 166 | 16 | 9.6% |
| GE Healthcare | 60 | 17 | 28.3% |
| GE Industrial | 59 | 21 | 35.6% |
| GE Infrastructure | 404 | 60 | 14.9% |
| GE Money | 110 | 19 | 17.3% |
| NBCU | 38 | 1 | 2.6% |
| SABIC-IP | 14 | 0 | 0.0% |
| Unknown | 0 | 8 | N/A |
| **Total** | **1011** | **163** | **16.1%** |

**05/19/2008 to 05/31/2009**

imagination at work







# Questions?

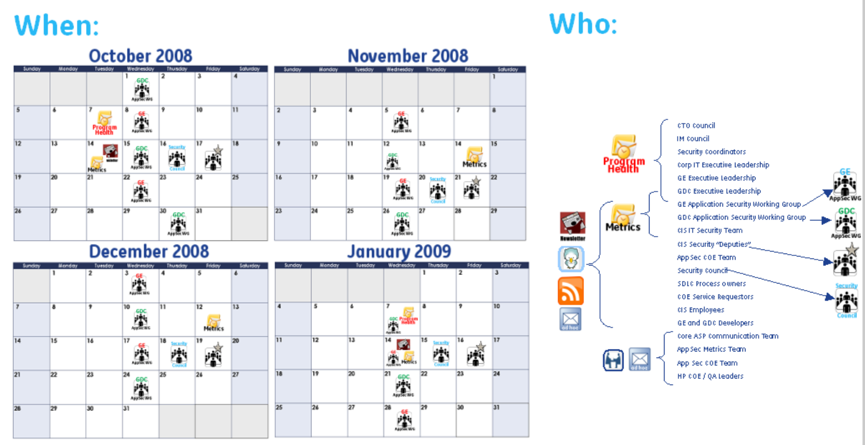
# Appendix

imagination at work

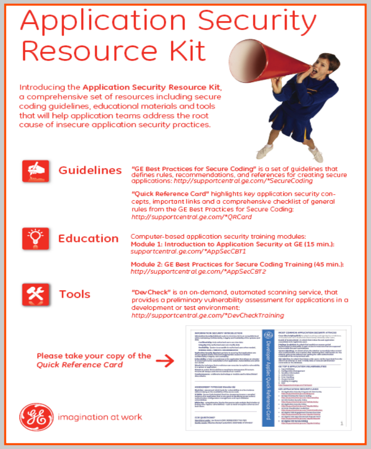
# Tools

## Communicate … Communicate … Communicate

Tools



Communication plan



Application Security Resource Kit

Introducing the **Application Security Resource Kit**, a comprehensive set of resources including secure coding guidelines, educational materials and tools that will help application teams address the root cause of insecure application security practices.

**Guidelines** "GE Best Practices for Secure Coding" is a set of guidelines that defines rules, recommendations, and references for creating secure applications: *http://supportcentral.ge.com/*SecureCoding*

"Quick Reference Card" highlights key application security concepts, important links and a comprehensive checklist of general rules from the GE Best Practices for Secure Coding: *http://supportcentral.ge.com/*QRCard*

**Education** Computer-based application security training modules:
**Module 1: Introduction to Application Security at GE (15 min.):** *supportcentral.ge.com/*AppSecCBT1*

**Module 2: GE Best Practices for Secure Coding Training (45 min.):** *http://supportcentral.ge.com/*AppSecCBT2*

**Tools** "DevCheck" is an on-demand, automated scanning service, that provides a preliminary vulnerability assessment for applications in a development or test environment: *http://supportcentral.ge.com/*DevCheckTraining*

**Please take your copy of the *Quick Reference Card*** →

Developer AppSec Quick Reference Card

imagination at work

Posters

GE Application Security Program

Focused on elimination and early detection of application security defects.

2009 Calendar

January 2009

GE Application Security Program Mission & Strategy
http://sc.ge.com/@AppCOE

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
|  |  |  |  | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

GE AppSec Program

Programs mission is to eliminate or reduce security defects from GE Applications through effective communication and consistent application of Guidance, Education and Tools.

More information on back

GE Application Security Program

January Additional Details

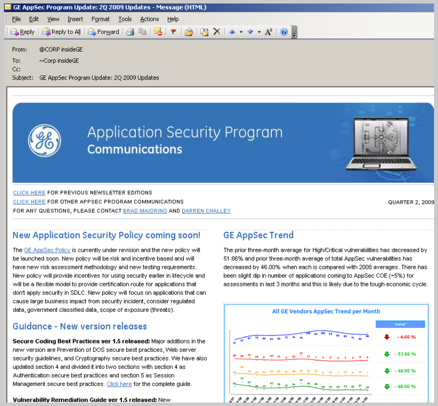
GE Application Security Program Mission & Strategy

The Application Security Program will achieve and maintain a strong application security posture across The Company through the implementation of consistent Guidance, Education, and Tools.

COE site - http://sc.ge.com/@AppCOE

GE Application Security Program

2009 Awareness calendar



From: @CORP insideGE
To: ~Corp insideGE
Cc:
Subject: GE AppSec Program Update: 2Q 2009 Updates

Application Security Program
**Communications**

CLICK HERE FOR PREVIOUS NEWSLETTER EDITIONS
CLICK HERE FOR OTHER APPSEC PROGRAM COMMUNICATIONS
FOR ANY QUESTIONS, PLEASE CONTACT BRAD MAIORINO AND DARREN CHALLEY

QUARTER 2, 2009

**New Application Security Policy coming soon!**

The GE AppSec Policy is currently under revision and the new policy will be launched soon. New policy will be risk and incentive based and will have new risk assessment methodology and new testing requirements. New policy will provide incentives for using security earlier in lifecycle and will be a flexible model to provide certification route for applications that don't apply security in SDLC. New policy will focus on applications that can cause large business impact from security incident, consider regulated data, government classified data, scope of exposure (threats).

**Guidance - New version releases**

**Secure Coding Best Practices ver 1.5 released:** Major additions in the new version are Prevention of DOS secure best practices, Web server security guidelines, and Cryptography secure best practices. We have also updated section 4 and divided it into two sections with section 4 as Authentication secure best practices and section 5 as Session Management secure best practices. Click here for the complete guide.

**Vulnerability Remediation Guide ver 1.5 released:** New

**GE AppSec Trend**

The prior three-month average for High/Critical vulnerabilities has decreased by 51.86% and prior three-month average of total AppSec vulnerabilities has decreased by 46.00% when each is compared with 2008 averages. There has been slight dip in number of applications coming to AppSec COE (~5%) for assessments in last 3 months and this is likely due to the tough economic cycle.

All GE Vendors AppSec Trend per Month

| Trend * |
|---|
| - 4.65 % |
| - 51.86 % |
| - 48.05 % |
| - 46.00 % |

Newsletters

imagination at work

# Darren Challey Biography

## Currently GE Application Security Leader:

- Lead a cross-business "AppSec Working Group"
- Establish policies, procedures and best practices
- Provide company-wide guidance, services and tools
- Maintain company-wide AppSec metrics program
- Partner with GE vendors to "fix root cause"

## Prior Roles and Businesses:

- IT Controller and IT SOx Leader (GE Corporate)
- Six Sigma Black Belt (GE Commercial Finance)
- Web Master & Program Manager (GE Commercial Finance)
- Electrical, Mechanical & Nuclear Engineer (GE Energy and GE KAPL)

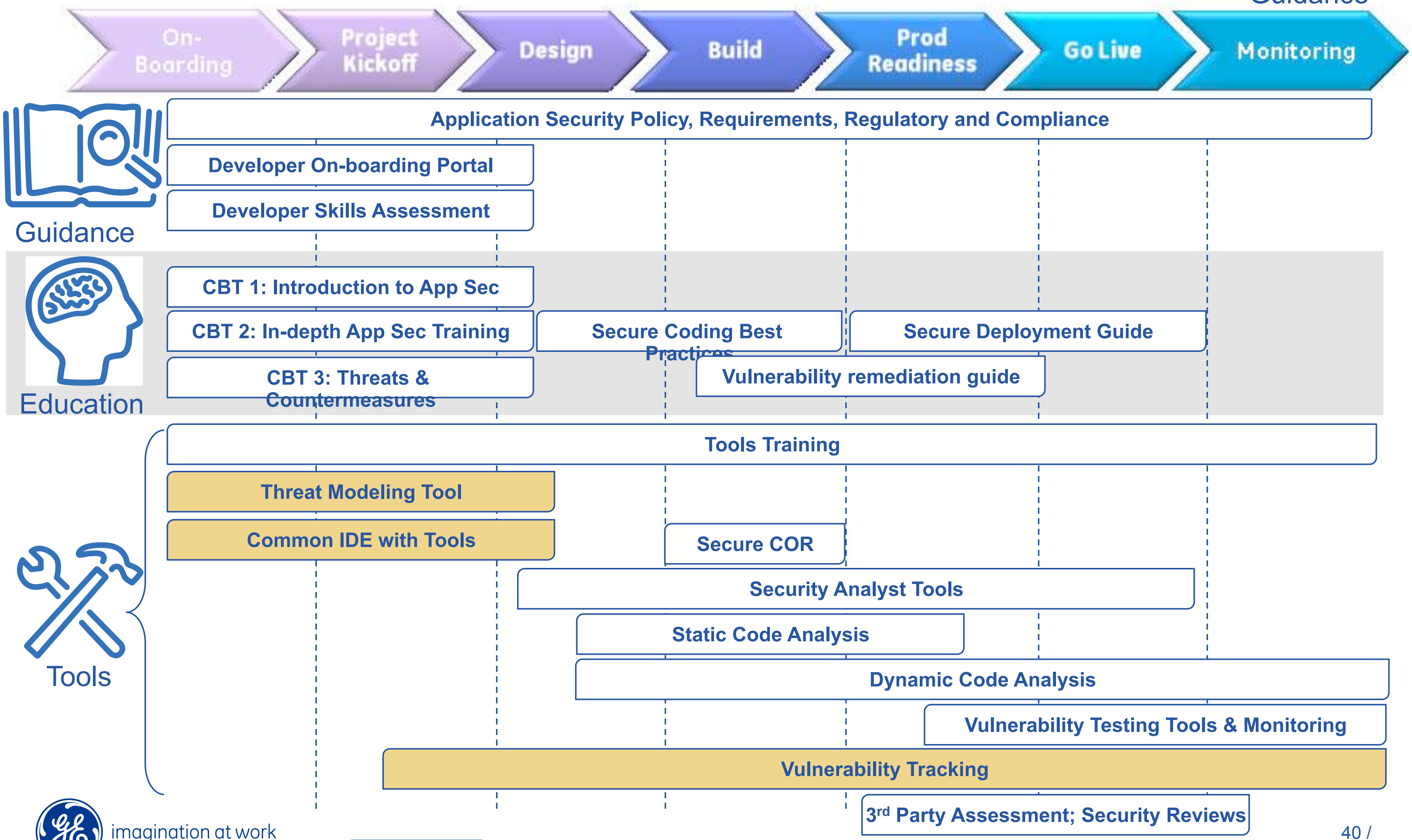
## Degrees and Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Edison Engineering Development Program Graduate
- Master of Engineering, Computer Systems - Rensselaer Polytechnic Inst.
- Bachelor of Science, Mechanical Engineering – Union College

imagination at work

# Secure SDLC and GE-EAS

Guidance



Application Security Policy, Requirements, Regulatory and Compliance

Developer On-boarding Portal

Developer Skills Assessment

CBT 1: Introduction to App Sec

CBT 2: In-depth App Sec Training

Secure Coding Best Practices

Secure Deployment Guide

CBT 3: Threats & Countermeasures

Vulnerability remediation guide

Tools Training

Threat Modeling Tool

Common IDE with Tools

Secure COR

Security Analyst Tools

Static Code Analysis

Dynamic Code Analysis

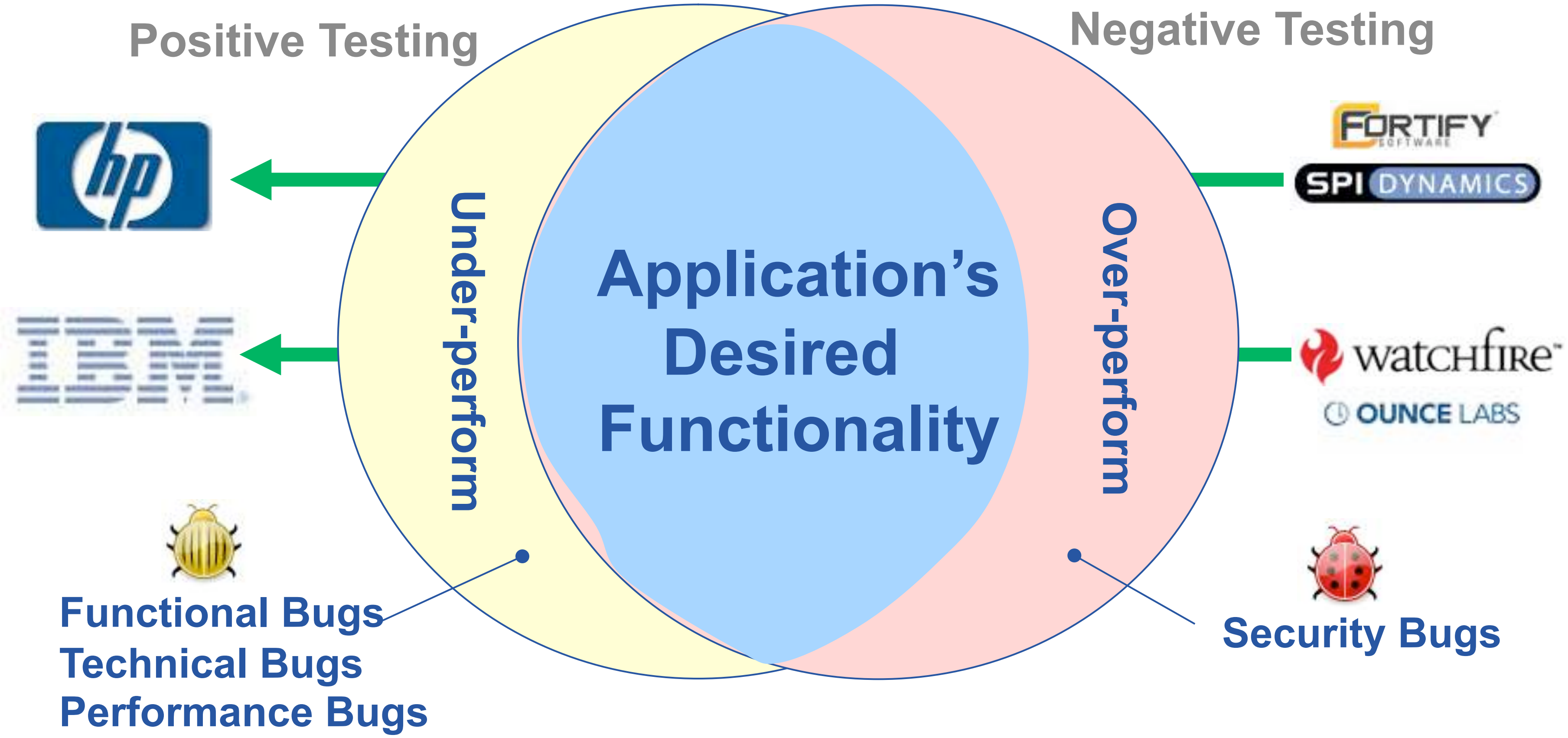
Vulnerability Testing Tools & Monitoring

Vulnerability Tracking

3rd Party Assessment; Security Reviews

In process

# SW Quality Assurance / Security Convergence



(Doesn't do what it should)

(Does more that it should)