

HP Software EMEA Performance Tour 2013

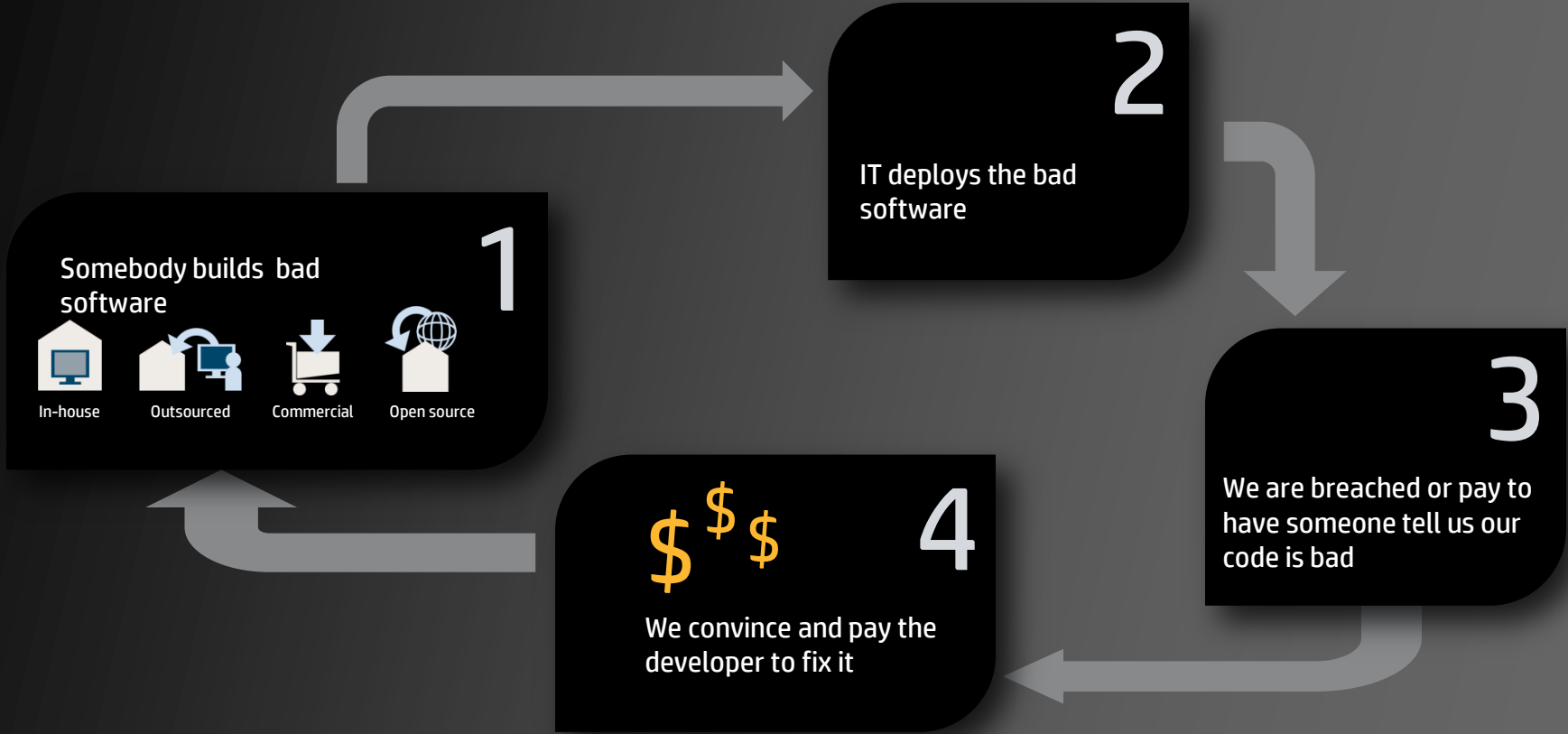
Zurich, Switzerland September 18





Integrating Application Security into Application Lifecycle Management

Migchiel de Jong / September 18, 2013



Agenda

- **Why be Concerned with Application Security?**
- **Most Common Application Security Program Approach Mistakes**
- **Characteristics of a Successful Application Security Program**
- **The technology perspective**



Why be concerned with Application Security ?



Building Effective Application Security Programs

Why be Concerned with Application Security?

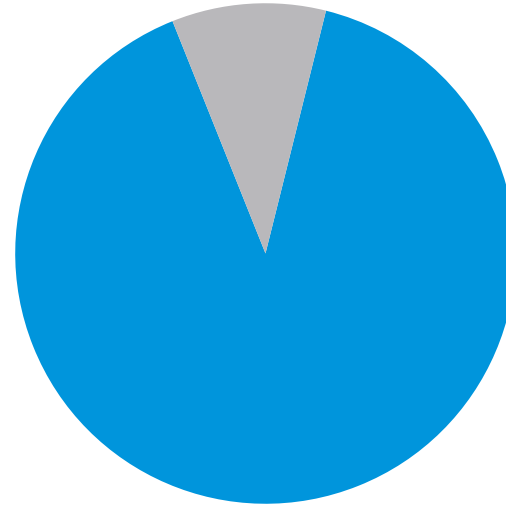
The End of the Corporate Network

- The Corporate Network as we know it will not exist in 10 years.
 - *Silicon Valley*
- The move to Cloud and Mobile Computing will greatly reduce the effectiveness of traditional perimeter security controls.
- But just how effective are these controls today?

The logo for Abiquo, featuring the word "abiquo" in a lowercase, sans-serif font with a stylized orange and blue graphic element.The logo for Accelops, featuring the word "accelops" in a lowercase, sans-serif font with a blue and orange graphic element.The logo for Akamai, featuring a stylized blue and orange graphic element above the word "Akamai" in a bold, sans-serif font.The logo for AppDynamics, featuring a stylized green and blue graphic element above the word "AppDynamics" in a sans-serif font.The logo for Apprenda, featuring a stylized blue and white graphic element above the word "apprenda" in a lowercase, sans-serif font.The logo for MegaWare, featuring the word "MegaWare" in a bold, sans-serif font with a stylized graphic element.The logo for Cloud9 analytics, featuring a stylized blue and white graphic element above the word "Cloud9" in a sans-serif font, with "analytics" in a smaller font below.The logo for CloudSwitch, featuring the word "CloudSwitch" in a bold, sans-serif font with a stylized graphic element.The logo for CloudTran, featuring the word "CloudTran" in a bold, sans-serif font with a stylized graphic element, and "The Cloud TP Company" in a smaller font below.The logo for Cumulux, featuring a stylized red and black graphic element above the word "CUMULUX" in a bold, sans-serif font.The logo for Eloqua, featuring the word "ELOQUA" in a bold, sans-serif font with a stylized graphic element.The logo for FinancialForce.com, featuring a stylized blue and white graphic element above the word "FINANCIAL" in a bold, sans-serif font, with "FORCE.COM" in a smaller font below.The logo for Oracle On Demand, featuring the word "ORACLE" in a bold, sans-serif font with a stylized graphic element, and "ON DEMAND" in a smaller font below.The logo for Salesforce.com, featuring the word "salesforce.com" in a lowercase, sans-serif font with a stylized graphic element.The logo for SAP Business ByDesign, featuring the word "SAP" in a bold, sans-serif font with a stylized graphic element, and "Business ByDesign" in a smaller font below.

Why be Concerned with Application Security?

- In a recent survey of 583 U.S companies conducted by Ponemon Research on behalf of Juniper Networks, 90% of the respondents said their organizations' computers had been breached at least once by hackers over the past 12 months.
- *[source: Computerworld, June 22, 2011]*

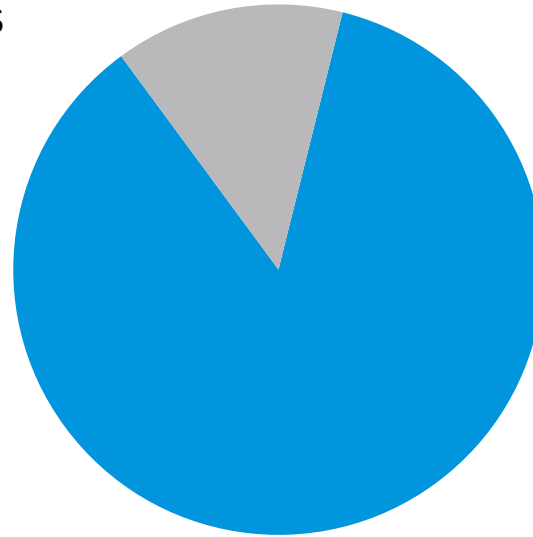


90%

■ Breached
■ Not Breached

Why be Concerned with Application Security?

- From scans of over 31,000 sites, over 85% showed a vulnerability that could give hackers the ability to read, modify and transmit sensitive data.
 - [Web Application Security Consortium].

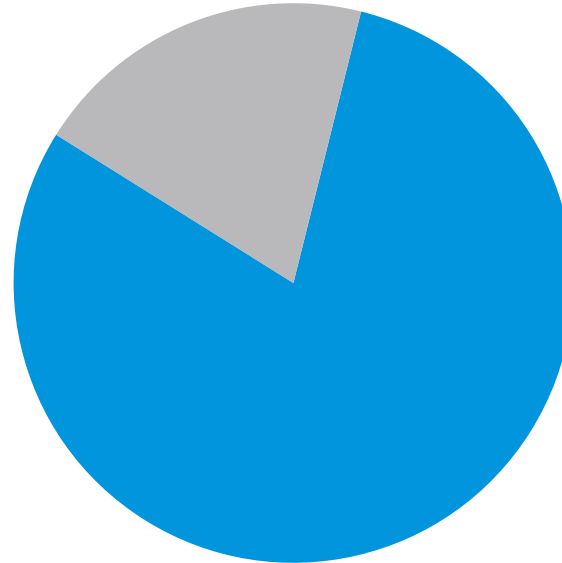


85%

■ Vulnerable
■ Secure

Why be Concerned with Application Security?

- “80% of Malicious Attacks happen at the application layer”.
 - [Gartner]



80%

■ Application Layer
■ Network / OS Layer

Most Common Application Security Program Approach Mistakes



Most Common Application Security Program Approach Mistakes

I have yet to see any problem,
however complicated, which,
when you look at it in the right way,
did not become still more complicated.

– Poul Anderson



Failed or ineffective application security programs almost always have one or more of the following characteristics:

- The view that application security is a “security” problem , and hence must be dealt with by the security team.
- The view that testing or “assessment” can and will resolve the problem.
- The view that “tools” and technology are the answer to solve the problem.
- The view that application security is an “all or nothing” endeavor.



Characteristics of a Successful Application Security Program



People seem to want to treat computer security like it's rocket science or black magic.

In fact, computer security is nothing but attention to detail and good design.

It's certainly possible to turn a computer security problem into a rocket-science or brain surgery class problem, but if you've done that it's almost a certain indication that you've already started down the wrong path.

[source: Marcus Ranum]

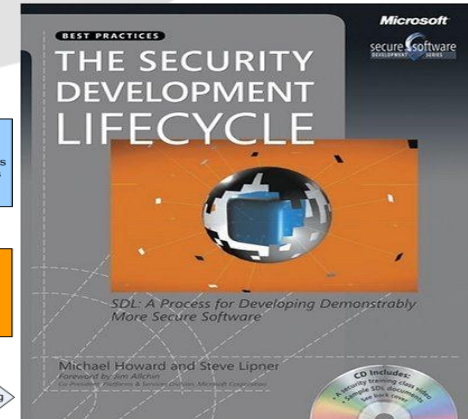
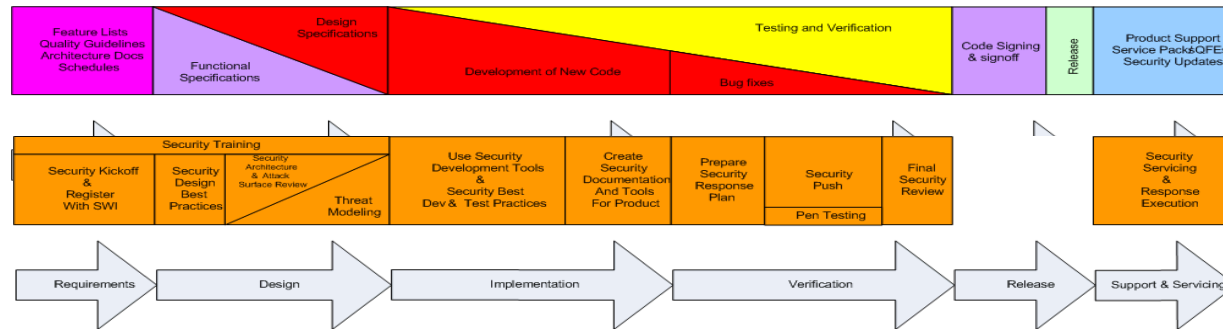
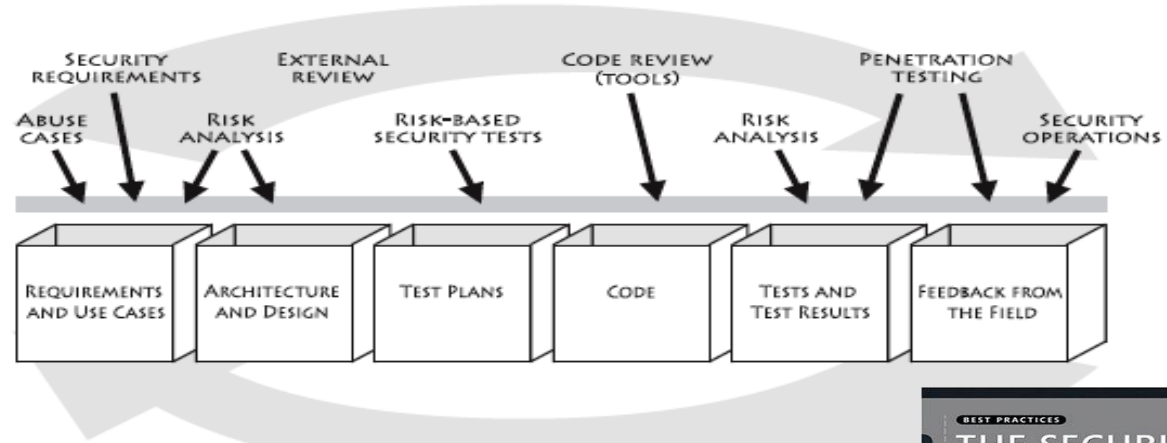
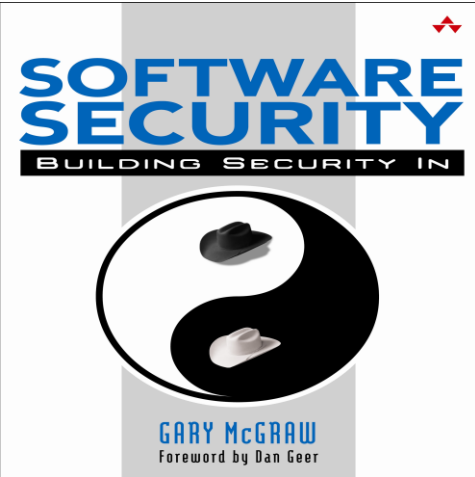


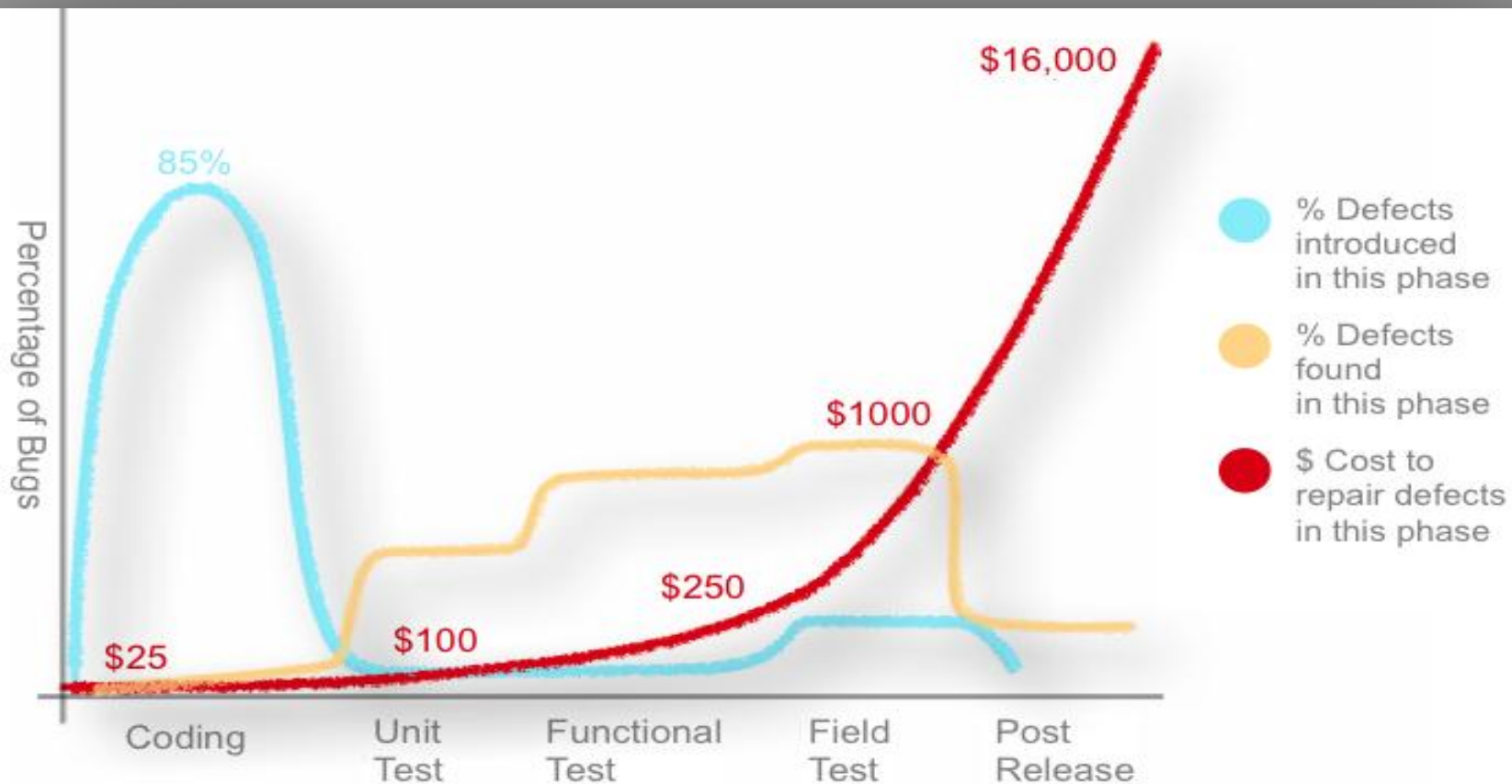
Successful application security programs:

- Recognize that application security, like all security, is a business problem.
- Have clearly defined Goals and Objectives that are understood and accepted throughout the organization
- Have a well defined Approach that includes:
 - The Capability to clearly define application security from a business risk perspective
 - The Capability to create secure code
 - The Capability to validate security requirements are being met
 - The Capability manage security defects in production

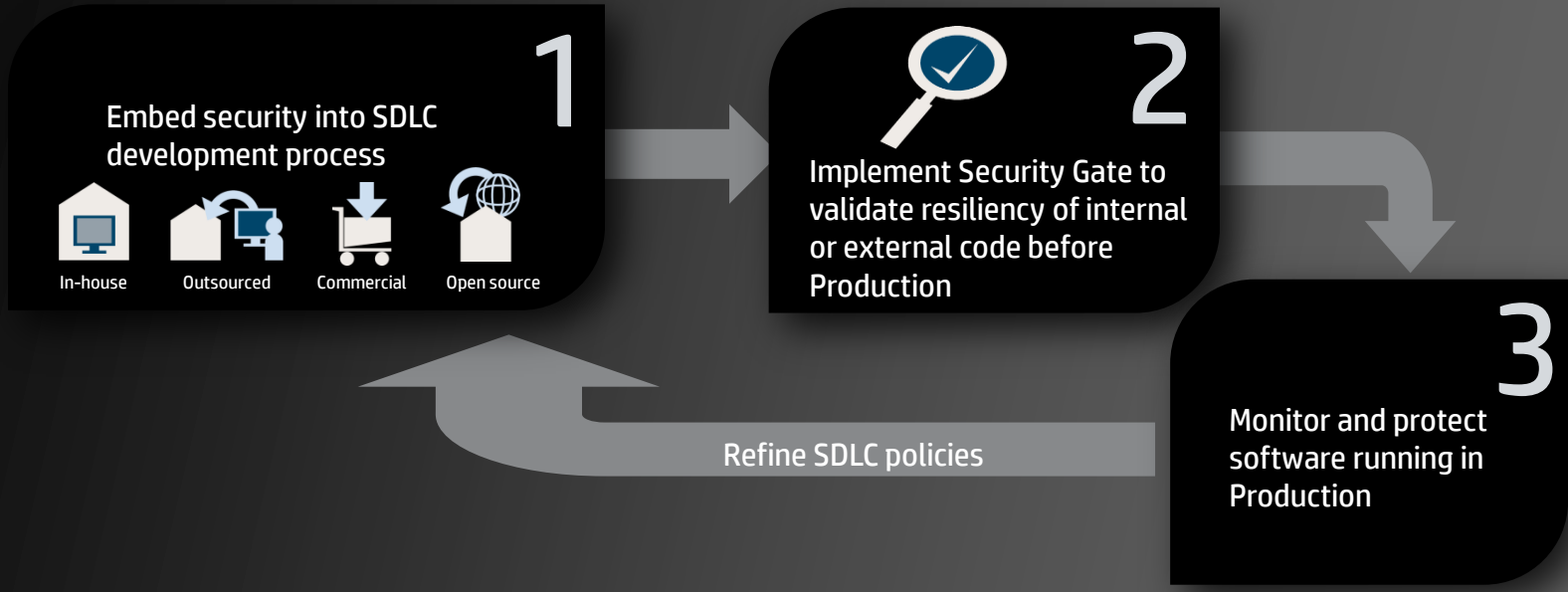


Security in the Development Lifecycle





Source: *Applied Software Measurement*, Capers Jones, 1996



This is Software Security Assurance





Alignment & Governance

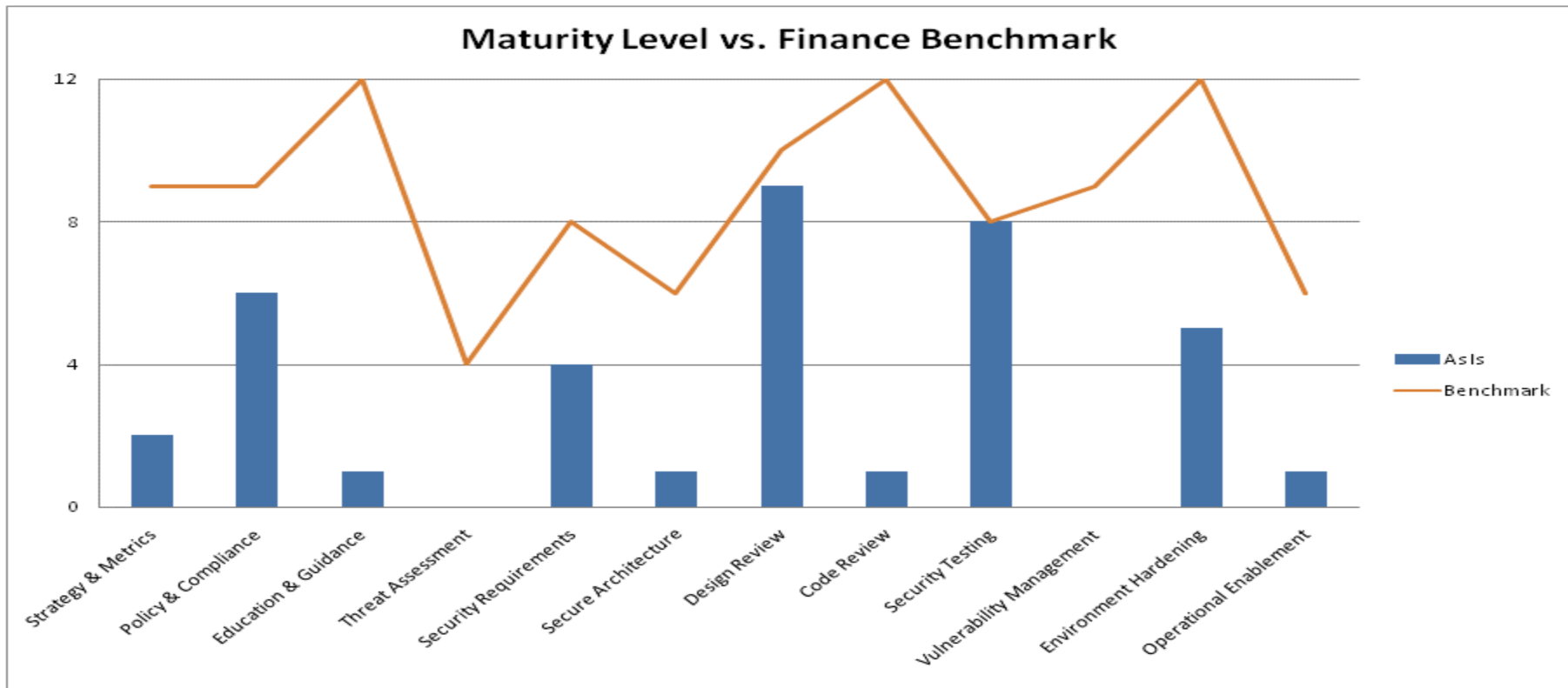
Requirements & Design

Verification & Assessment

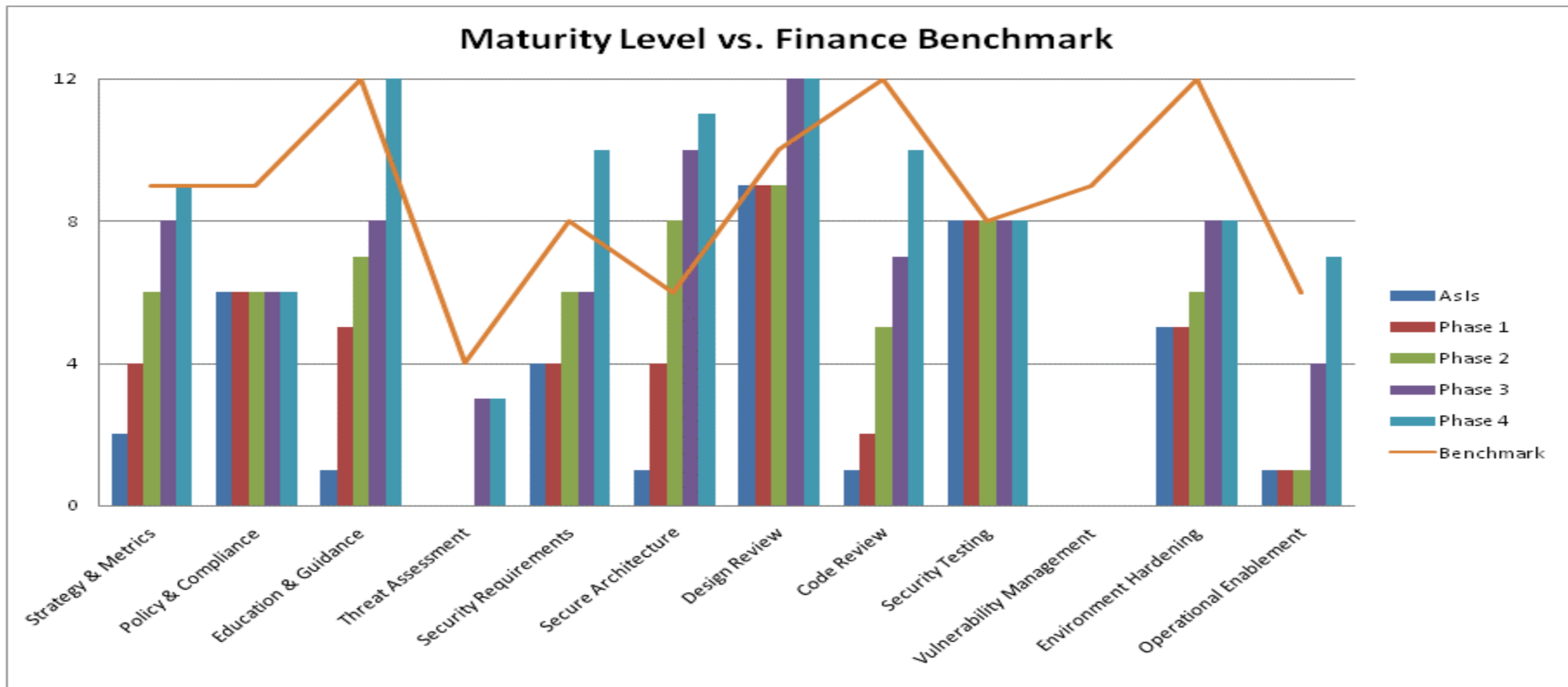
Deployment & Operations



SSA Benchmark



SSA Roadmap



SSA Best Practice Approach

- Quickly find and remediation of critical vulnerabilities
 - Don't “forget to fix” or “boil the ocean”
- Prevent introduction of new vulnerabilities
 - Integrate into existing SDLC with minimal process changes
 - Provide flexibility to integrate with new SDL as it rolls-out
- Provide support for the developers
 - Training in the context of their own code base
 - Mentoring as required
- Monitor and control
 - Automate gathering of vulnerability statistics and publish
 - Enforcement via security gate
- Continuous Improvement

The Technology Perspective



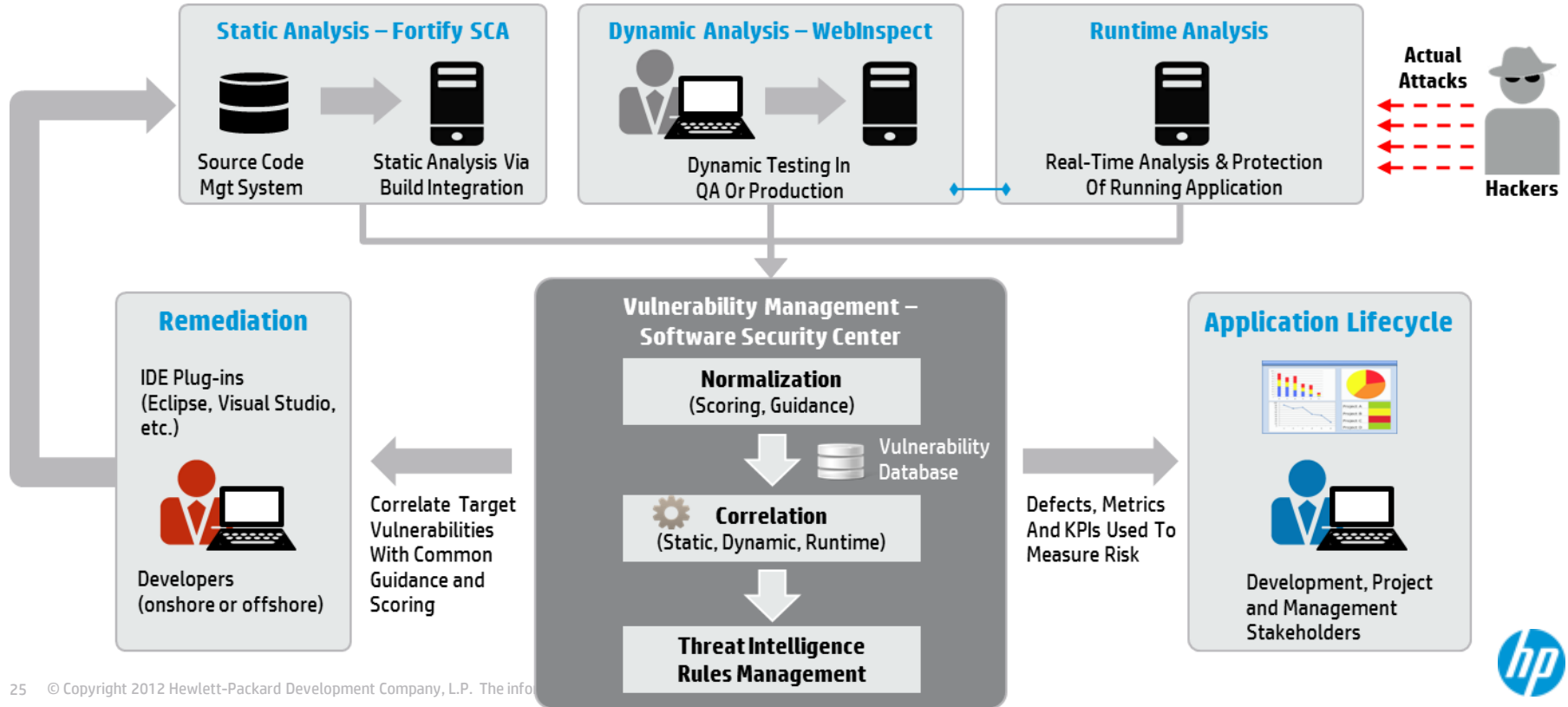
Solution Components

- **Static Application Security Testing (SAST)**
- **Dynamic Application Security Testing (DAST)**
- **Runtime Application Security Testing (RAST)**
- **Hybrid Analysis (combining SAST and DAST through RAST)**
- **FOD (SAST and DAST in the cloud)**



HP Fortify – Software Security Assurance

On-Premise and On-Demand



Fortify eLearning – Cloud Based Education

The screenshot shows the Fortify eLearning interface. At the top left is the Fortify logo. The main header reads 'Application Security Fundamentals' with navigation links for 'Help', 'Transcript', 'Notes', and 'Glossary'. Below the header, the breadcrumb trail indicates 'You are here: Handling Input and Output Security > Input Validation'. The main content area is titled 'Input Validation—Real-world Examples' and 'Challenge #1'. It features a 'Login' form with fields for 'User name' (containing 'John') and 'Password' (masked with asterisks), and a 'Submit' button. To the right of the form, text explains the focus on 'User Name' entry and why it's important for security. Below the form, 'Input Criteria: User ID' are listed: 'Length: Maximum 25 characters' and 'Data Type: Alphanumeric (A-Z, a-z, 0-9)'. A progress table shows two questions, both marked as 'Not Completed'. A blue instruction bar at the bottom says 'Click each Question button to open each issue and solve.' The footer displays 'Module - 5 Topic - 3/5' and a timer '01:50:36 / 02:16:09'.

Benefit –
Comprehensive,
scaleable, repeatable
and measureable



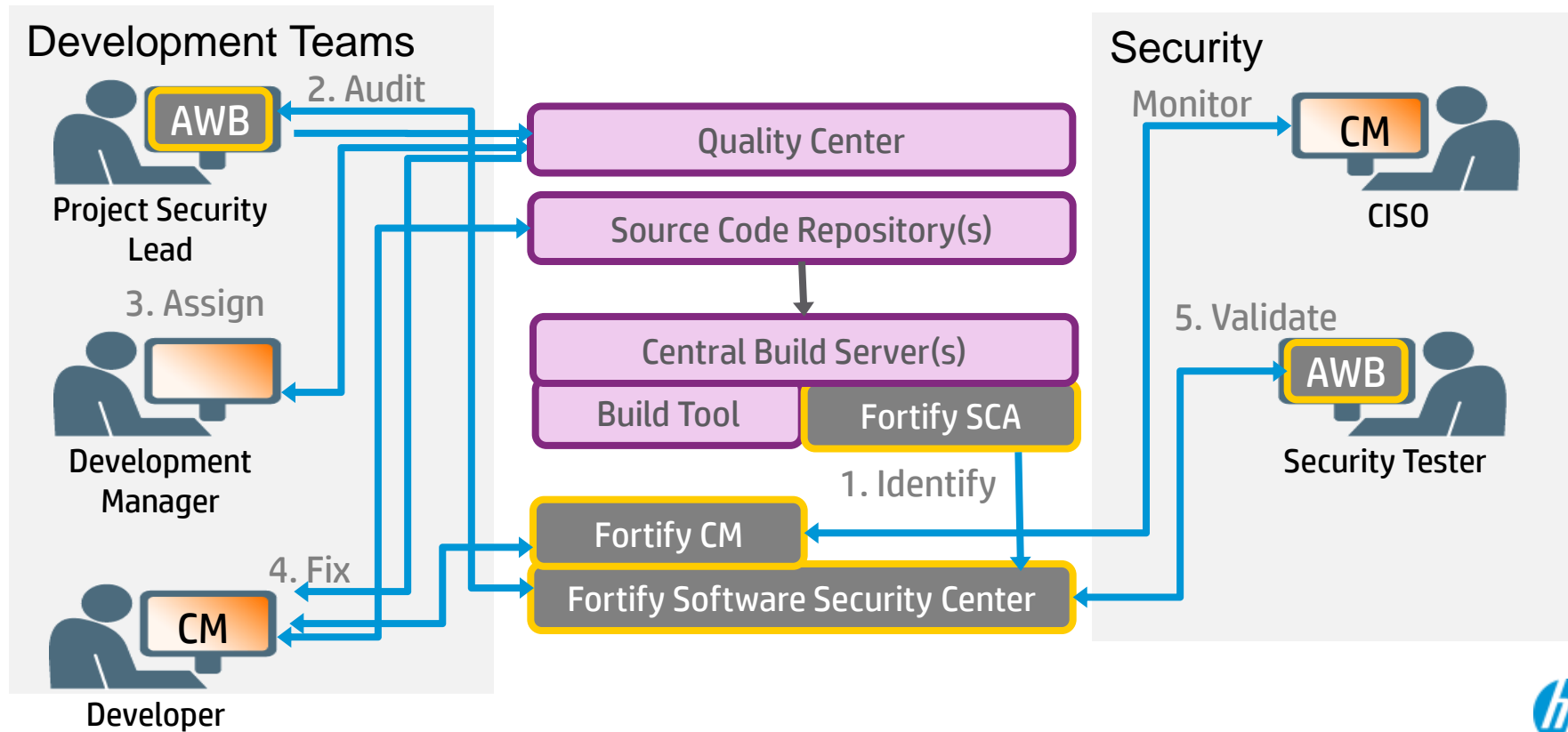
Fortify SCA – Early Lifecycle Security Testing

The screenshot displays the Fortify Audit Workbench interface. The top navigation bar includes 'Summary', 'Audit Guide', 'Scan', and 'Reports'. The main window is divided into several panes:

- Summary:** Shows a filter set of 'Medium' and a total of 1398 hot issues. A tree view on the left lists various categories, with 'SQL Injection - [27 / 783]' expanded to show multiple instances of 'admin_import_subscribers.asp:556 (SQL Injection)'. One instance is highlighted in red.
- Code Editor:** Displays the source code for 'admin_import_subscribers.asp'. Lines 552-556 show a SQL query construction: `strSQL = "SELECT * FROM " & strDatabaseTableName & ";"` and `rsImport.Open strSQL, adoImportCon`. Lines 560-561 show a loop: `Do While NOT rsImport.EOF`. Lines 562-566 show variable initialization: `blnEmailOK = True`, `blnEmailExists = false`, `strErrorFieldName = ""`, and `blnUserCodeOK = false`. Lines 569-570 show record counting: `lngTotalProcessed = lngTotalProcessed + 1`.
- Analysis Trace:** Shows a trace for 'Multiple Paths: 1 of 5'. The trace includes steps like 'management_centre_update.asp:77 - Read request.cookies()', 'management_centre_update.asp:77 - mid(0 : return)', 'management_centre_update.asp:77 - trim(0 : return)', 'management_centre_update.asp:77 - Assignment to struser', 'management_centre_update.asp:80 - idcharacterstrip(0 : ret', 'management_centre_update.asp:80 - Assignment to struser', 'delete_account.asp:76 - Read struserid', 'delete_account.asp:74 - Assignment to strsql', 'admin_import_subscribers.asp:556 - Read strsql', and 'admin_import_subscribers.asp:556 - open(0)'. The 'open(0)' step is highlighted.
- Issue Details:** Shows the issue 'admin_import_subscribers.asp:556 (SQL Injection) (multiple)'. The analysis is marked as 'Exploitable'. A note states: 'There are multiple issues selected. ... appended to each issue.' A warning icon and text indicate: 'this is a critical issue - must be corrected next release.'

Benefit – FINDS vulnerabilities in code and enables rapid FIXES

Example Implementation – Source Code Analysis



WebInspect – Late Lifecycle Security Testing

The screenshot displays the HP WebInspect interface. The main window shows a 'Scan Dashboard' for the target site 'http://zero.webappsecurity.com/'. The dashboard includes a 'Scan Info' section with 'Crawl 348 of 348' and 'Audit 854 of 854'. A 'Scan Status' section indicates 'Completed'. A 'Vulnerabilities' bar chart shows the following counts: Critical (106), High (92), Medium (8), Low (66), Info (22), and Best Practices (25). Below the chart is a table of 'Attack Type' with columns for 'Attacks', 'Critical', 'High', 'Medium', 'Low', 'Info', and 'Best Practices'. The table lists several attack types with their respective counts. A 'Risk' table at the bottom lists 10 vulnerabilities with their risk levels and counts.

Attack Type	Attacks	Critical	High	Medium	Low	Info	Best Practices
Manipulation	2,597	103	52	0	2	0	
Exploratory	10,111	1	26	4	37	8	
Other	6,216	2	14	4	27	14	

Risk	Count	Description
Critical	48	Cross-Site Scripting
High	6	Database Server Error Message
High	4	SQL Injection Confirmed (No Data Extraction)
High	1	IIS Global Server Variables Disclosure (global.asa.bak)
High	47	Microsoft ASP.NET or ASP Unicode Conversion Cross-Site Scripting
High	7	Unencrypted Login Form
High	6	Logins Sent Over Unencrypted Connection
High	3	Admin Section Must Require Authentication
High	1	WebApp Administrative Access Purposes

Benefit – FINDS vulnerabilities in QA and production environments – no code required.



Fortify OnDemand – Security Testing Service

The screenshot displays the Fortify OnDemand interface for a project named 'BigBankESMP'. The interface includes a navigation menu with 'Projects', 'Reports', and 'Administration'. The main content area is titled 'Fortify on Demand' and contains an 'Executive Summary' section. This section provides details about the company (BigBankESMP), project (SPLC), version (1.0), and analysis dates (Static: July 15, 2009; Dynamic: N/A). It also lists application type (E-Commerce), technology stack (Java/J2EE), and interfaces (Web Services (SOA), Web Access). A 'Fortify Security Rating' box shows a 4-star rating (★★★★) based on 64 issues, with a green checkmark for 'Static' analysis and a red X for 'Dynamic' analysis. Below this, there are two charts: 'Top 5 Prevalent Categories' (a pie chart) and 'Issues by Priority' (a 2x2 matrix). The 'Issues by Priority' matrix shows 44 High issues, 13 Low issues, and 7 Medium issues. At the bottom, there are two tables: 'Issues by Attack Vector' and 'Remediation Roadmap'.

Executive Summary

Company: **BigBankESMP**
 Project: **SPLC**
 Version: **1.0**
 Static Analysis Date: **July 15, 2009**
 Dynamic Analysis Date: **N/A**

Application Type: **E-Commerce**
 Technology Stack: **Java/J2EE**
 Interfaces: **Web Services (SOA), Web Access**

Project Type: **Application**
 Data Classification: **Customer personally identifiable**

Fortify Security Rating
 ★★★★★
 64 Issues
 Based on impact and likelihood of issues (see Appendix A).
 Static: **✓** Dynamic: **✗**

Top 5 Prevalent Categories

- Cross-Site Scripting: 35
- Cross-Site Request Forgery: 13
- SQL Injection: 5
- SQL Injection: Hibernate: 3
- Unreleased Resource: Streams: 3
- Other: 5

Issues by Priority

44 High	7 Critical
13 Low	7 Medium

Issues by Attack Vector

Attack Vector	Issues
Database	2
Network	0
Web	41
Web Service	0
Other	21
Total	64

Remediation Roadmap

To Achieve	Major Fixes	Minor Fixes
★★★★★	0	0
★★★★☆	0	0
★★★☆☆	0	44
★★☆☆☆	0	0
★☆☆☆☆	0	0
Total	0	44

Benefit – FINDS vulnerabilities in applications you don't develop



Fortify Governance – SDLC Process Control

FORTIFY 360 Server Welcome admin
Logout | Account | Preferences | About

Dashboard | **Projects** | Reports | Administration

Projects > Sample Training App - v. 1.1

Project: Sample Training App - v. 1.1
Issues | Requirements | Artifacts | General | Reports | Event Log | Access

Low Risk Active Development
Select item and...

Name	State
Low Risk Active Development	In Progress
Strategic Planning	In Progress
Allocate Time for Security Tasks	Awaiting Sign Off
Allocate Time for Security Bug Fixes during implementation phase	Signed Off
Allocate Budget for Security Bug Fixes during maintenance phase	In Progress
Architectural Review	In Progress
Build permission matrix for resource access	In Progress
Identify software attack surface	Document Rejected
Develop data-flow diagrams for sensitive resources	Not Started
Infrastructure Hardening	Not Started
Monitor baseline infrastructure configuration status	Not Started
Lockdown Environment	Not Started
Deployment Monitoring	Not Started
Verify Target URL	Not Started

Allocate Time for Security Tasks

State: **Awaiting Sign Off**
Satisfying Document: Document(s) Available
Document Type: Project Plan
Description: Time related to security tasks

Comments
admin 01-15-2009 2:18:31 PM
Document 'Project Plan' submitted for review by the team.

Benefit – FORTIFY's SDLC with consistent auditable approach



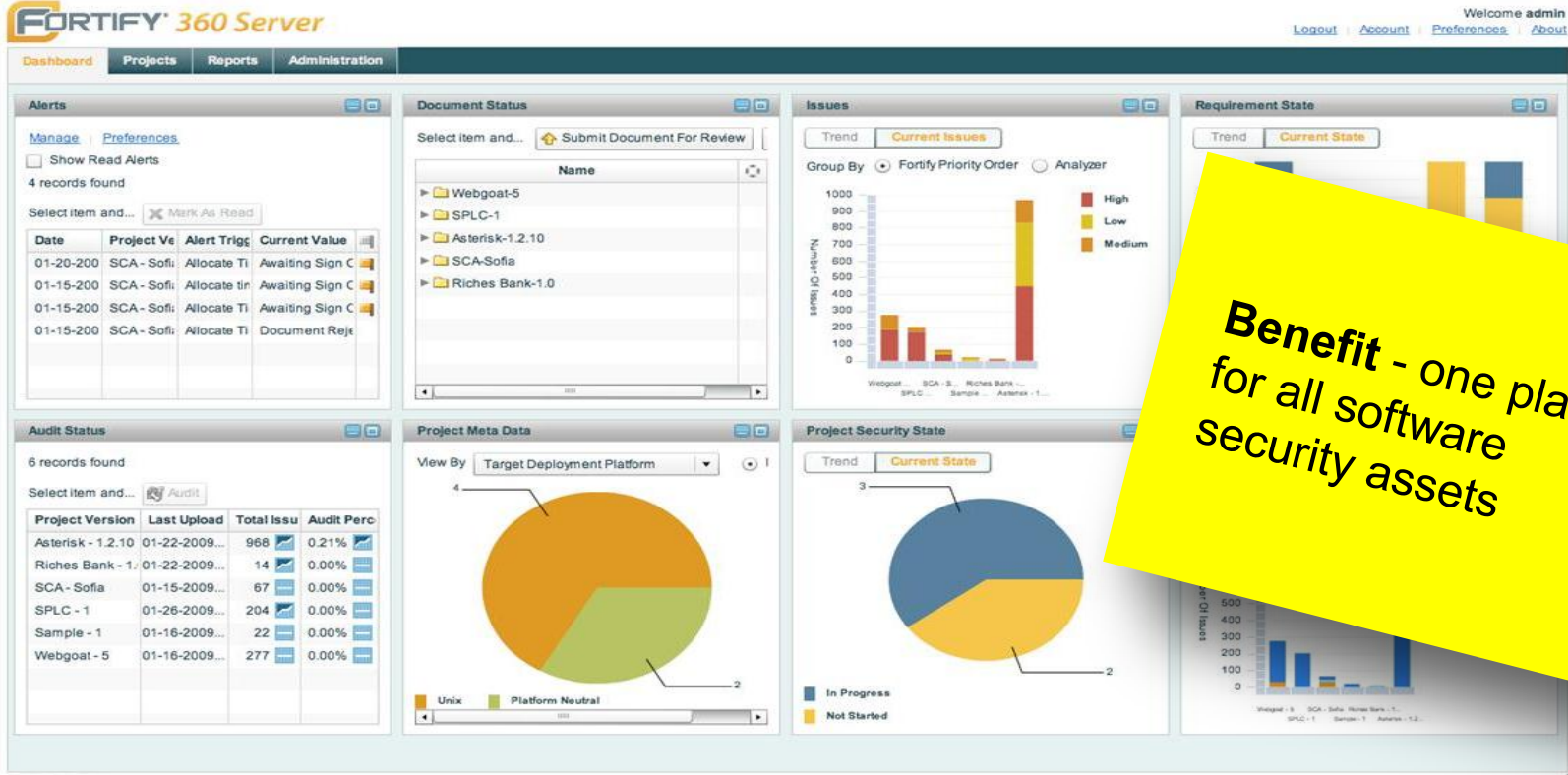
Fortify RTA – Application Deployment Protection

The screenshot displays the HP Fortify Software Security Center interface. At the top, the logo and navigation tabs (Dashboard, Projects, Runtime, Reports, Administration) are visible. The 'Security Events' section is active, showing a list of events with columns for Application, Host, Category, Action, Request IP Address, and Date. A detailed view of an 'SQL Injection' event is shown on the right, indicating a 'Critical' severity. A yellow callout box is overlaid on the right side of the screenshot.

Benefit – harden existing applications



Fortify SSC- Management Dashboard



Benefit - one place for all software security assets



Thank you

