

Building a Secure Application Development Process with the Rational AppScan Family

John Smith

Senior Security Architect, IBM Rational

johnsmith@uk.ibm.com



IBM Rational Software Development Conference 2008

WHERE TEAMS ARE **R-HEROES**



Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
 - People
 - Tools
 - Process/Governance
- Rational solutions
 - Education
 - Software
 - Services

Avoiding the Headlines...



Jan 18, 2007

Massive Security Breach Reveals Credit Card Data

The TJX Companies, a large retailer that operates more than 2,000 retail stores under brands such as Bob's Stores, HomeGoods, Marshalls, T.J. Maxx and A.J. Wright, said on Wednesday that it suffered a massive computer breach on a portion of its network that handles credit card, debit card, check and merchandise transactions in the United States and abroad.



CNBC's Easy Money

BusinessWeek uncovers that the cable channel's own design flaw may be behind the investigation into its million-dollar stock-picking co...



USDA admits data breach, thousands of social security numbers revealed

Thursday, 17 April 2007

(Axcress News) Washington - The US Department of Agriculture (USDA) admitted that a security breach allowed social security and other personal information of over 63,000 recipients of federal farm loans be made available on a public website in violation of Federal privacy laws.



Visa, Amex Cut Ties with CardSystems

July 19, 2005 -- Visa USA Inc. and American Express Co. are cutting ties with the payment-processing company that left 40 million credit and debit card accounts vulnerable to hackers in one of the biggest breaches of consumer data



BJ's Settles Case with FTC over Customer Data

FTC alleges weak security at wholesale club led to fraudulent sales valued in the millions

JUNE 17, 2005 -- After credit card data for thousands of customers was used to make fraudulent purchases in other stores, BJ's Wholesale Club Inc. has agreed

Motivations for Secure Applications

Web applications are the #1 focus of hackers:

XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)

Most sites are vulnerable:

90% of sites have security issues (IBM)

78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)

Web applications are high value targets for hackers:

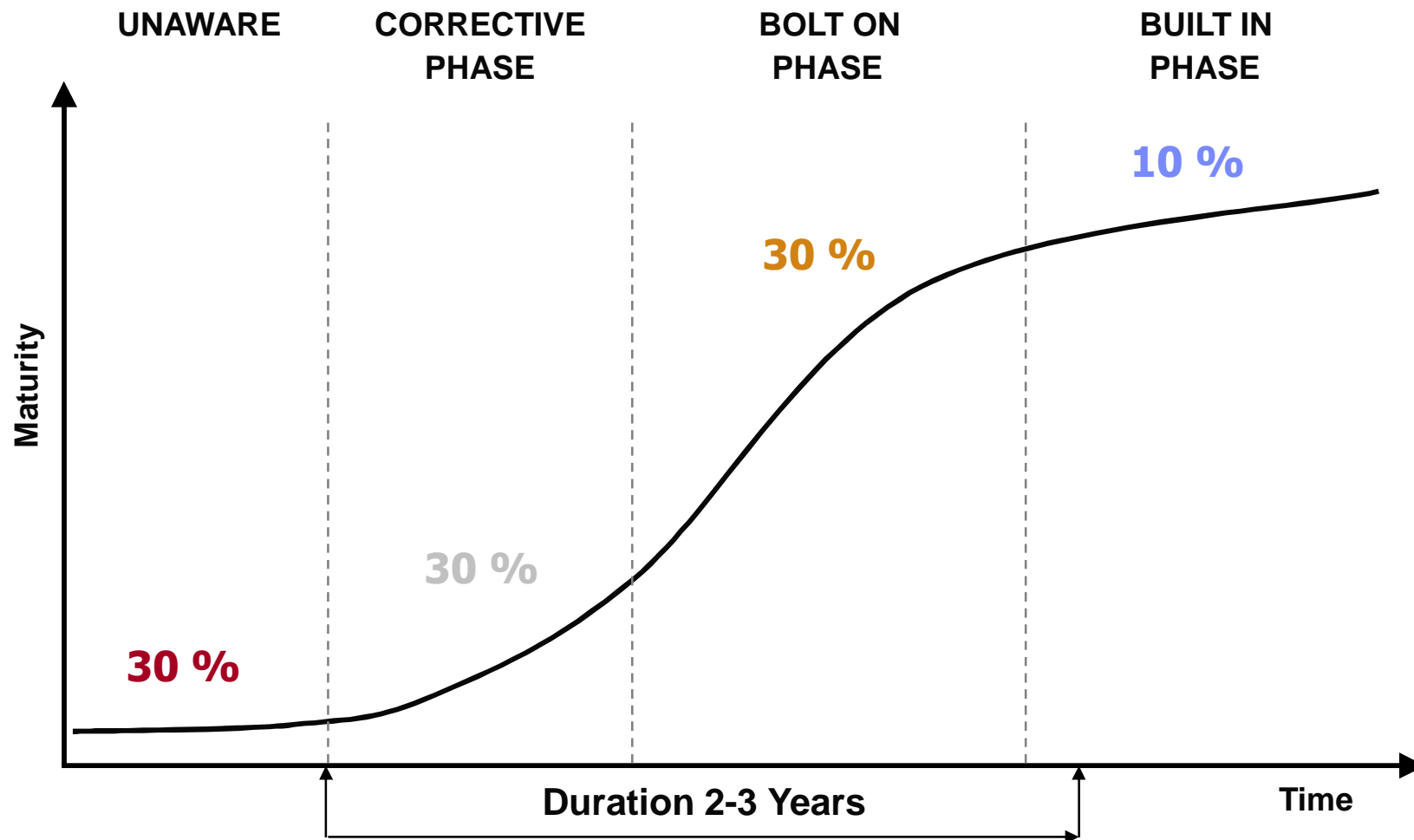
Customer data, credit cards, ID theft, fraud, site defacement, etc

Compliance requirements:

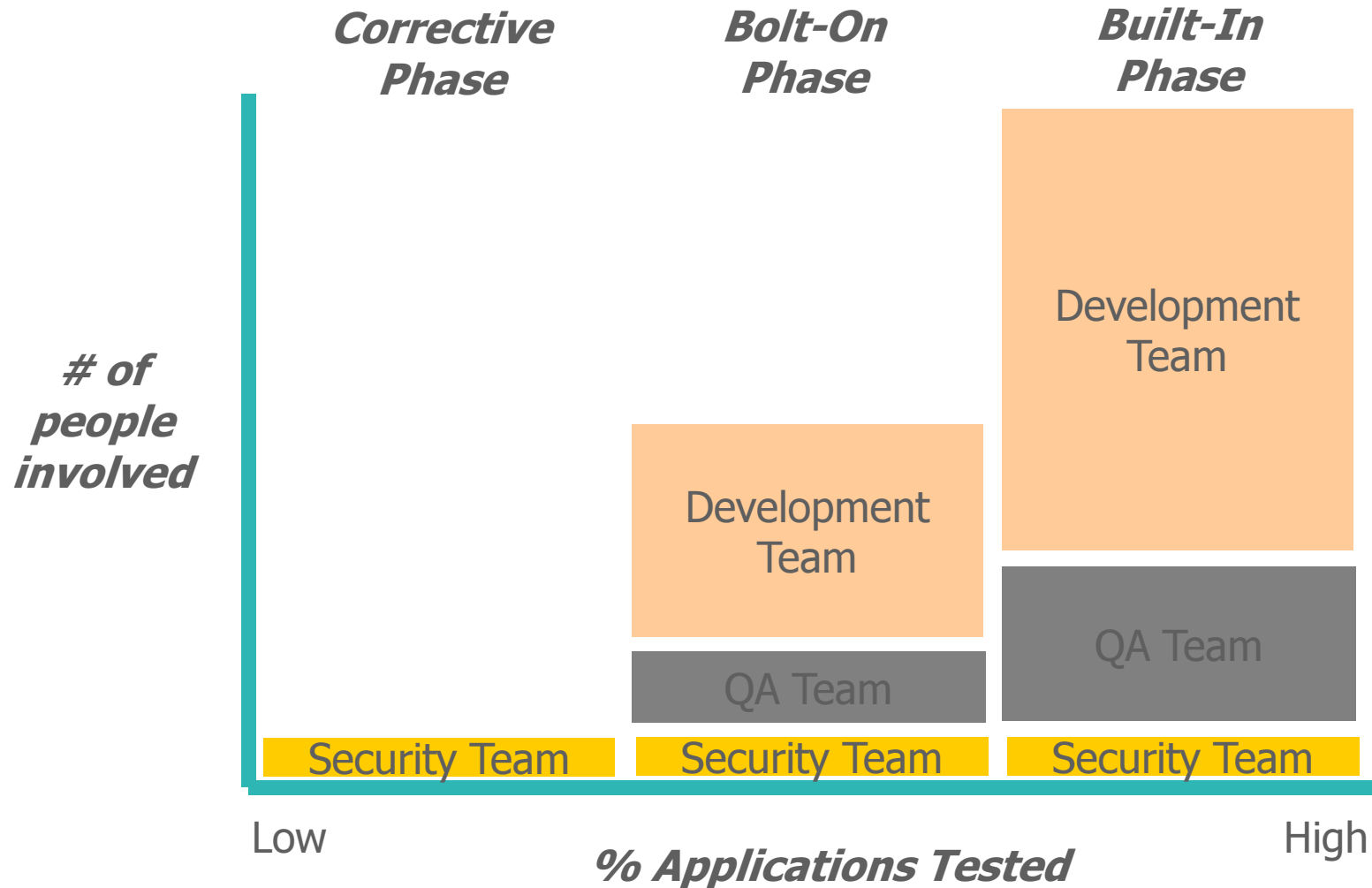
Payment Card Industry (PCI) Standards, Sox/EuroSox, Basel II etc.



Phases of Application Security Maturity



The need to scale



Cost Benefits of Early Detection



Source: IBM Systems Sciences Institute

Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
 - People
 - Tools
 - Process/Governance
- Rational solutions
 - Education
 - Software
 - Services

Ingredients

- People
- Tools
- Process/Governance

People

- Many different stakeholders in Application Lifecycle
 - Business Owners
 - Architects
 - Developers
 - Testers
 - ...
- Education is the Key
 - Understanding the Vulnerabilities
 - Secure Coding Principles
 - Corporate Security Policy
 - ...

Tools

- Security is a Quality problem
 - Defect Management
 - Test Management
 - Test Automation
- Security Testing Tools based on 2 complimentary approaches:
 - Black-Box Testing
 - White-Box Testing
- Lets look at an example...

SQL Injection

User input is embedded as-is in predefined SQL statements:

```
query = "SELECT * from tUsers where
userid='" + iUserID + "' AND
password='" + iPassword + "'";
```

hackbook

Username:

Password:

Remember me

Login

[Forgot Password?](#)



UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

Hacker supplies input that modifies the original SQL statement, for example:

```
iUserID = ' or 1=1 --
```



UserID	Username	Password	Name
1	admin	\$#koeFor56	Administrator

How Black-Box Scanners Work

The image shows a browser window with the URL `https://login.hackbook.com/login.php`. The page displays a login form with fields for Username and Password, a 'Remember me' checkbox, and a 'Login' button. An error message is shown on the page:

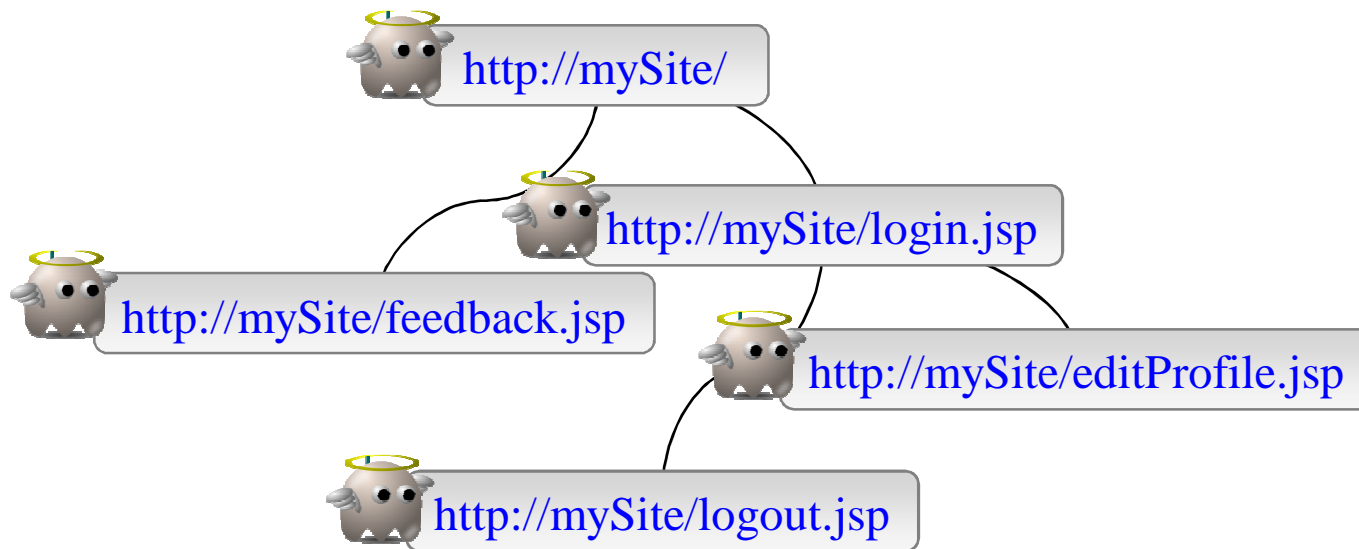
An Error Has Occurred
 Summary: Syntax error (missing operator) in query expression 'username = '' AND password = 'foobar'.
 Error Message Details:
 System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'psaok'. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at Altoro.Authentication.ValidateUser(String userName, String password).in

A blue arrow points from the 'Forgot Password?' link on the login form to a callout box containing the following SQL injection payload:

```
SELECT * from tUsers where
userid="" AND password='foobar'
```

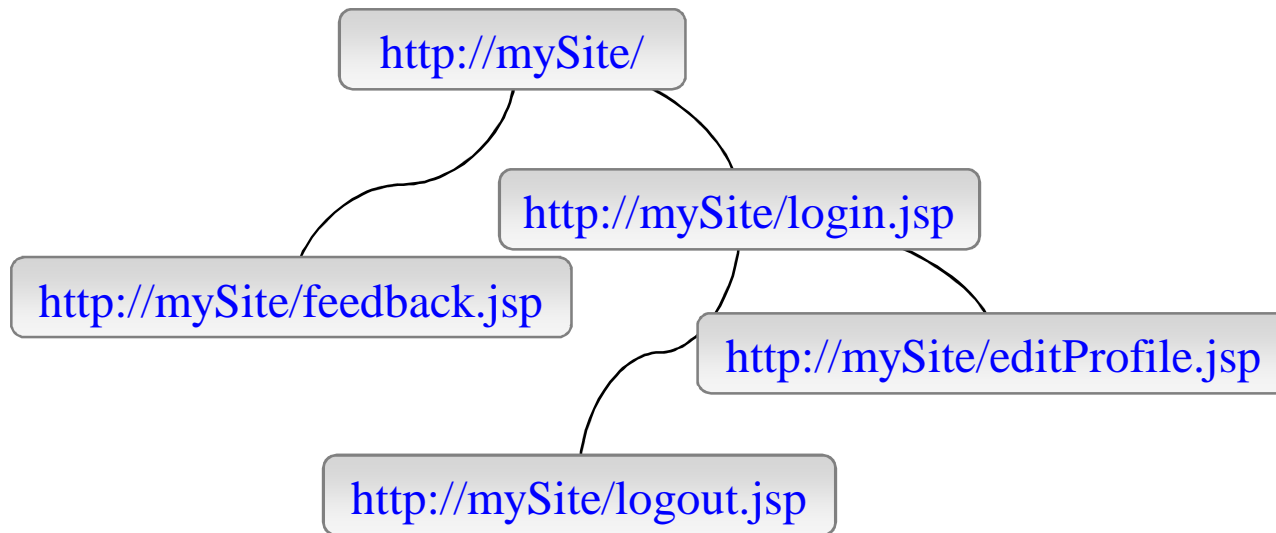
How Black-Box Scanners Work

Stage 1: Crawling as an honest user



How Black-Box Scanners Work

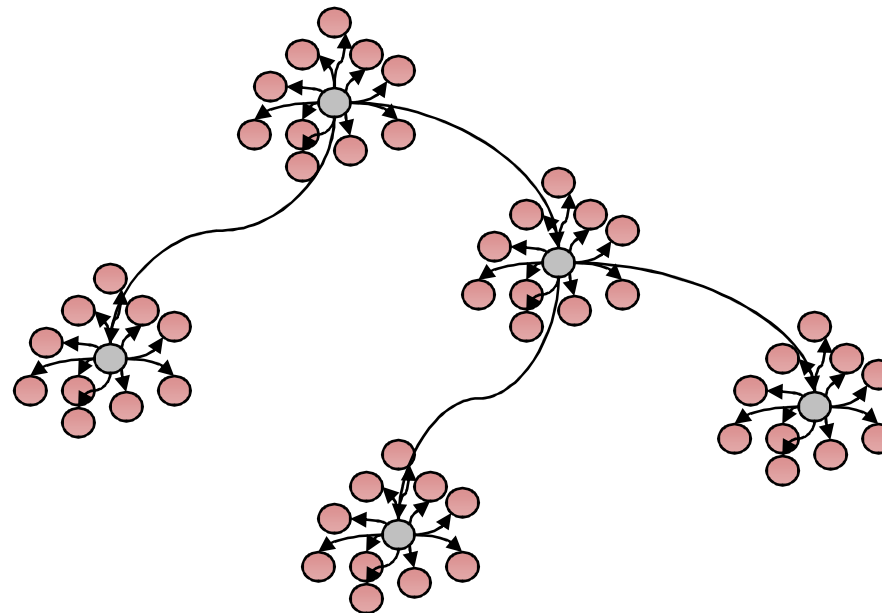
Stage 1: Crawling as an honest user



How Black-Box Scanners Work

Stage 1: Crawling as an honest user

Stage 2: Testing by tampering requests



How White-Box Scanners Work

```
// ...  
String username = request.getParameter("username");  
String password = request.getParameter("password");  
  
// ...  
String query = "SELECT * from tUsers where " +  
    "userid='" + username + "' +  
    "AND password='" + password + "'";  
  
// ...  
ResultSet rs = stmt.executeQuery(query);
```

Source – a method returning tainted string

User can change executed SQL commands

Sink - a potentially dangerous method

How White-Box Scanners Work



```
String username = request.getParameter("username");
```

```
// ...  
String username = request.getParameter("username");  
String password = request.getParameter("password");
```

```
// ...  
String query = "SELECT * from tUsers where " +  
    "userid='" + username + "'";
```

```
String query = "SELECT ..." + username
```

```
// ...  
ResultSet rs = stmt.executeQuery(query);
```

```
ResultSet rs = stmt.executeQuery(query);
```

A Common Fix (not the best one...)

```
// ...
String username = request.getParameter("username");
String password = request.getParameter("password");

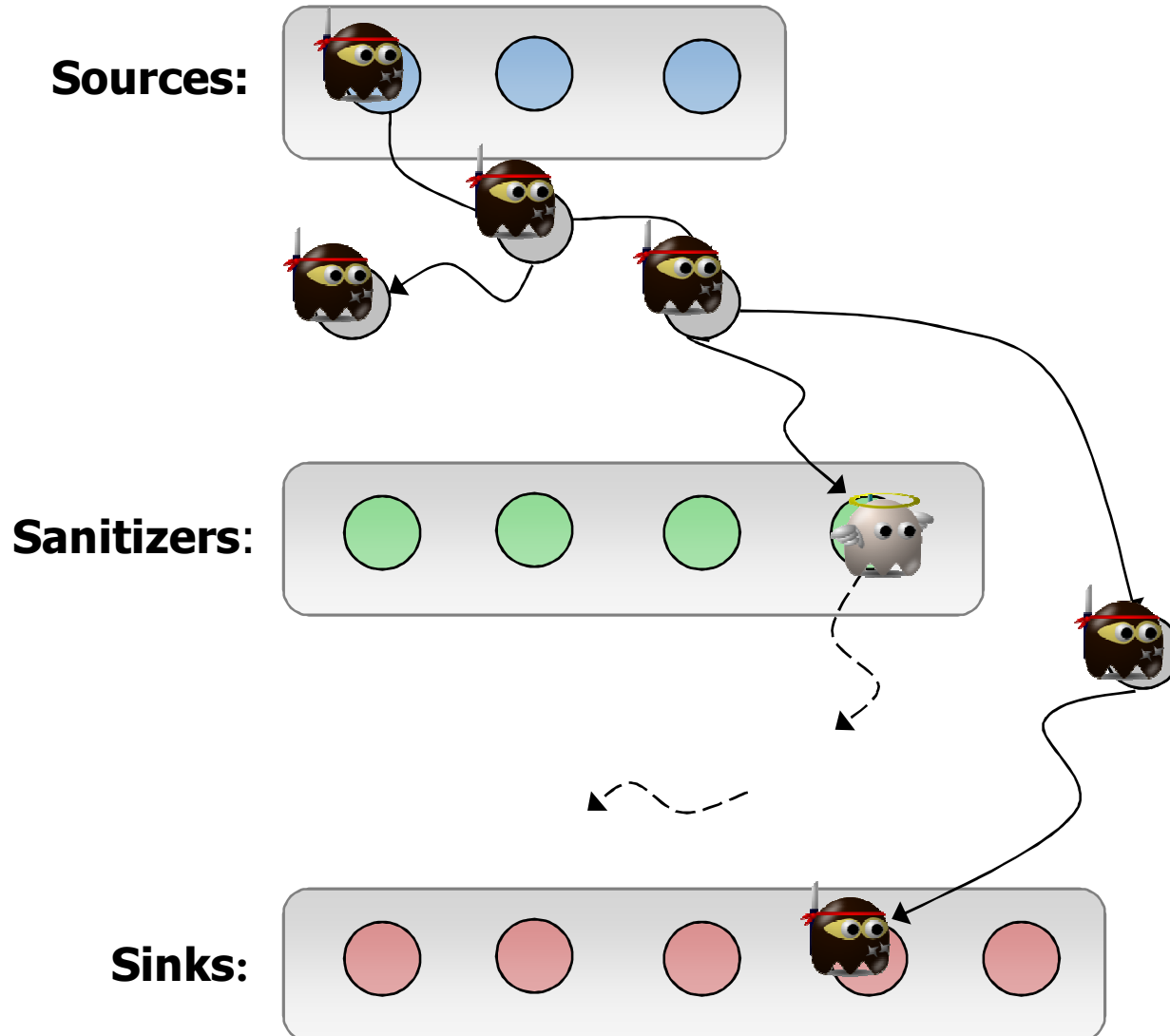
// ...
String query = "SELECT * from tUsers where " +
    "userid='" + Encode(username) + "' " +
    "AND password='" + Encode(password) + "'";

// ...
ResultSet rs = s.executeUpdate(query);
```



Sanitizer:
a method returning
a non-tainted string

How WB Scanners Work



Processes/Governance

*“We are what we repeatedly do.
Excellence, then, is not an act but a habit”*

Ralph Waldo Emerson

- Well defined and understood processes allow Habits of Excellence to be formed
- Strong governance ensures that Habits of Excellence are formed consistently throughout the organisation

Agenda

- Motivations for Secure Application Development
- Ingredients for Secure Application Development
 - People
 - Tools
 - Process/Governance
- Rational solutions
 - Education
 - Software
 - Services

Rational Education

- Web Based Training
 - Comprehensive Curricula
 - Product Training
 - Security Training
 - Secure Coding Principles
 - Customisable
- Immersion Training
 - Onsite, working within your infrastructure
 - Tailored to your needs

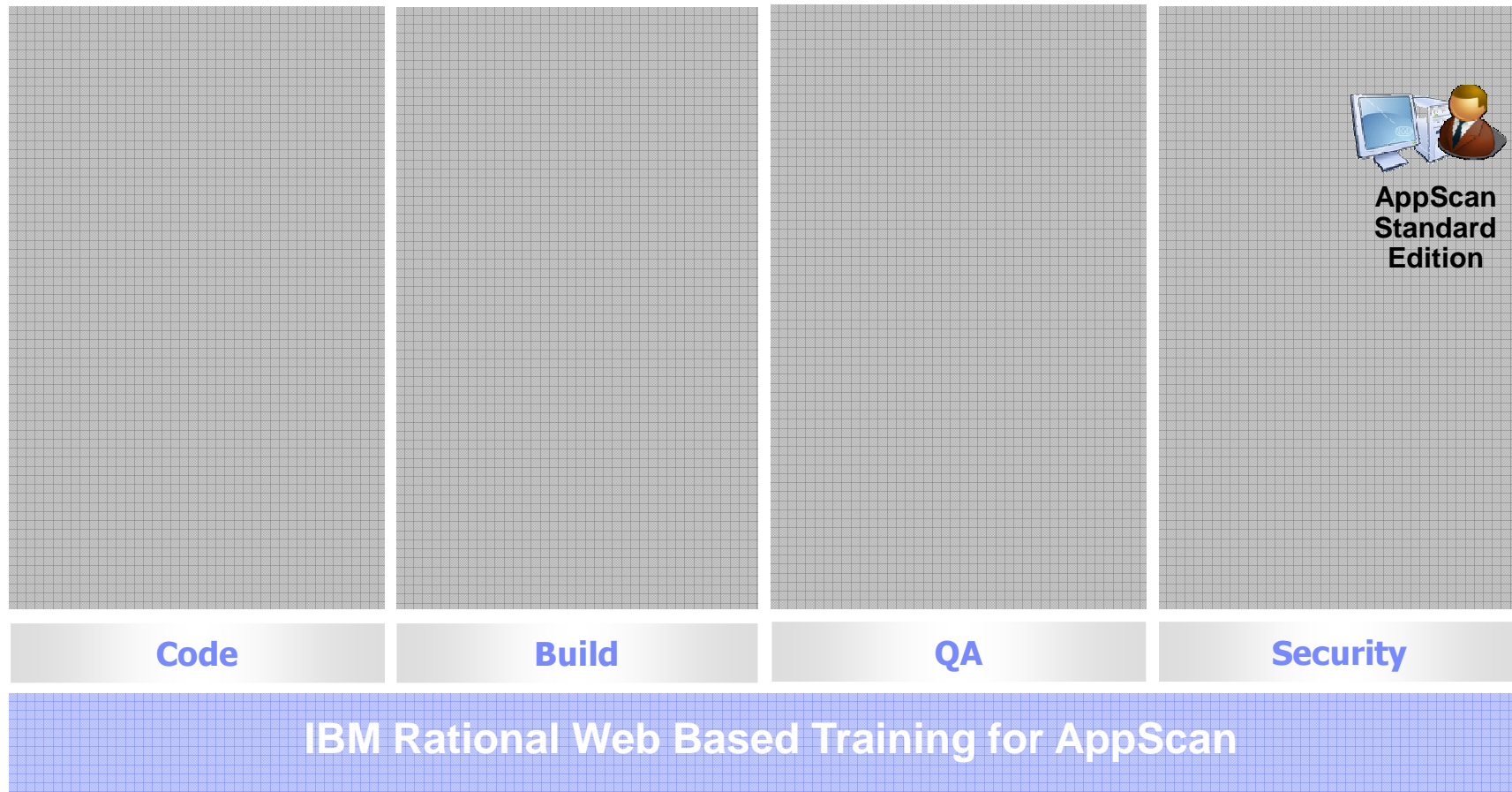
Rational Services

- Software as a Service
 - AppScan On Demand
 - Managed Services
- Deployment Services
 - Ease the deployment path
 - Integration with your infrastructure
- Consultancy
 - Help you find a path to security

Rational Software

- Complete Quality Management Solution
 - Rational Quality Manager
 - Rational Clearquest
 - Rational Functional Tester
 - Rational Performance Tester
 - ...
- Specific Toolset for Application Security
 - AppScan Product Family

IBM Rational AppScan SDLC Ecosystem



AppScan Standard Edition

- Best in class Black-Box Testing
 - AJAX Support
 - Multi-Step Process Support
 - Advanced Login Management
- Extensible Plug-in Architecture
 - Integrate with systems and processes
- Easy to use, drives Education process
 - Scan Expert for configuration assistance
 - Integrated WBT Modules

AppScan Standard Edition

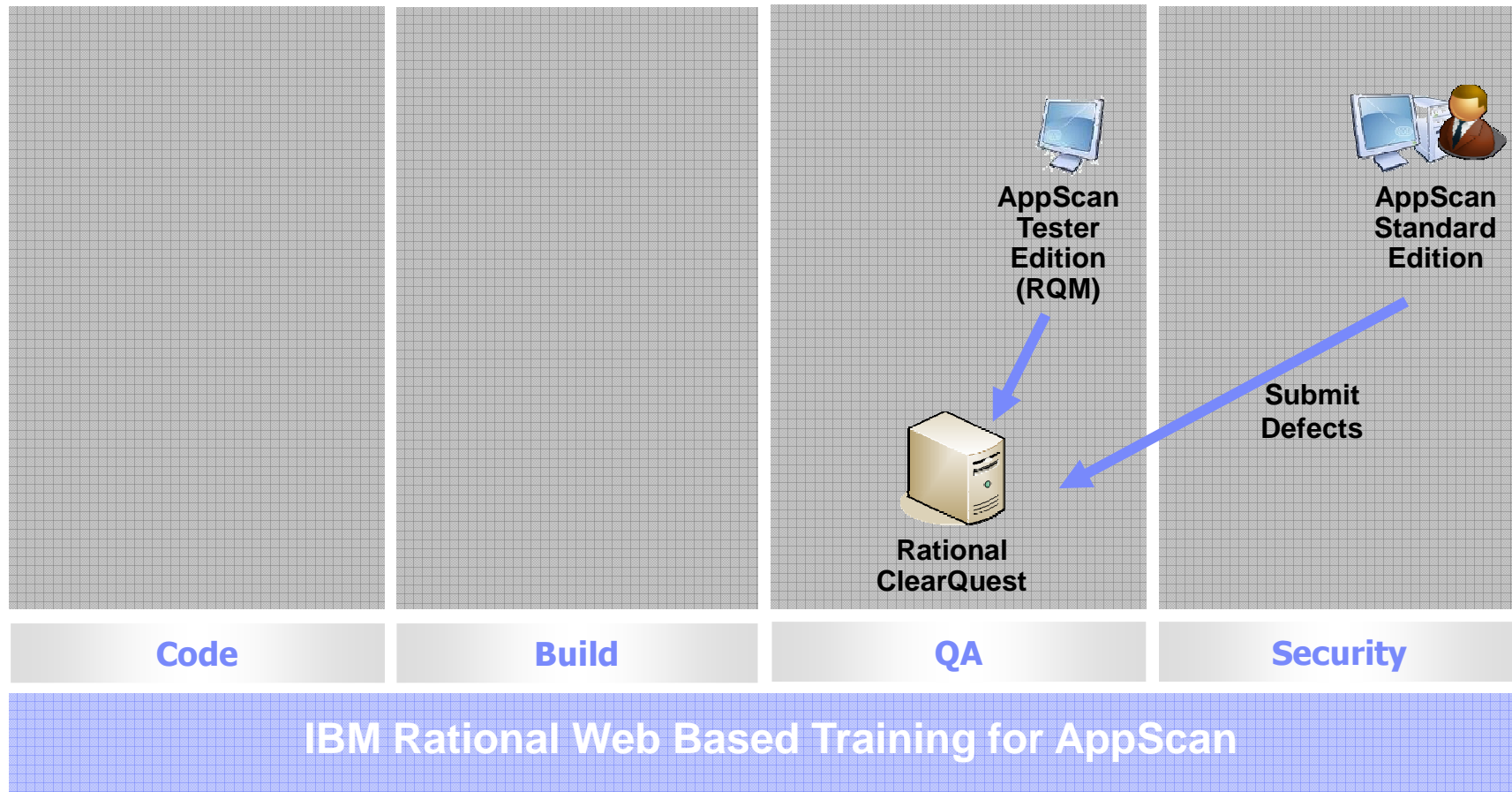
Find the Security Issues

Detailed Advisories and Fix Recommendations

Scan the entire App or just a portion

The screenshot displays the IBM Rational AppScan interface. On the left, a tree view shows the application structure for 'demo.testfire.net', including files like 'cgi.exe', 'comment.aspx', and folders like 'admin', 'altoro', 'bank', 'images', and 'static'. The main pane shows a list of 63 security issues, with 'ASP.NET Forms Authentication Bypass' and 'Blind SQL Injection' at the top. A detailed advisory for 'HTTP Response Splitting' is expanded, showing a severity of 'High' and a WASC classification of 'Client-side Attacks: Content Spoofing'. The technical description explains how an attacker can deface the site or steal session data by injecting malicious characters. An example shows a crafted request to '/redir_lang.jsp?lang=English' and the resulting split HTTP response. At the bottom, an 'Issue Severity Gauge' shows 25 High, 4 Medium, 23 Low, and 11 Info issues.

IBM Rational AppScan SDLC Ecosystem



Security Auditors and Quality Assurance Specialists have complimentary skills and responsibilities



- Knows security in-depth
- Knows corporate and industry standards
- Can exploit security defects to prove impact
- Is responsible for the security of application

- Makes testing repeatable
- Reports on test coverage, release readiness
- Triages and manages defects
- Scales testing effort across a large team
- Already part of the development process



Phased adoption of security testing in QA

Engaging your QA team in security testing, one step at a time



Tracking security defects like other defects is the first building block



- Benefit to have the bugs tracked properly
- Begins to bring security into the normal dev process
- QA Team gains awareness/begins to learn about security
- Security Auditors benefit from having the issue they find tracked properly
- Can prioritize security work against other work, triage



Manage your security testing like other types of testing

- QA teams know how to manage testing
 - What are we going to test?
 - How are we going to test it?
 - Who is going to do the work?
 - How frequently are we going to retest?
 - What hardware and software are required for the test?
 - How much of the application has been tested?

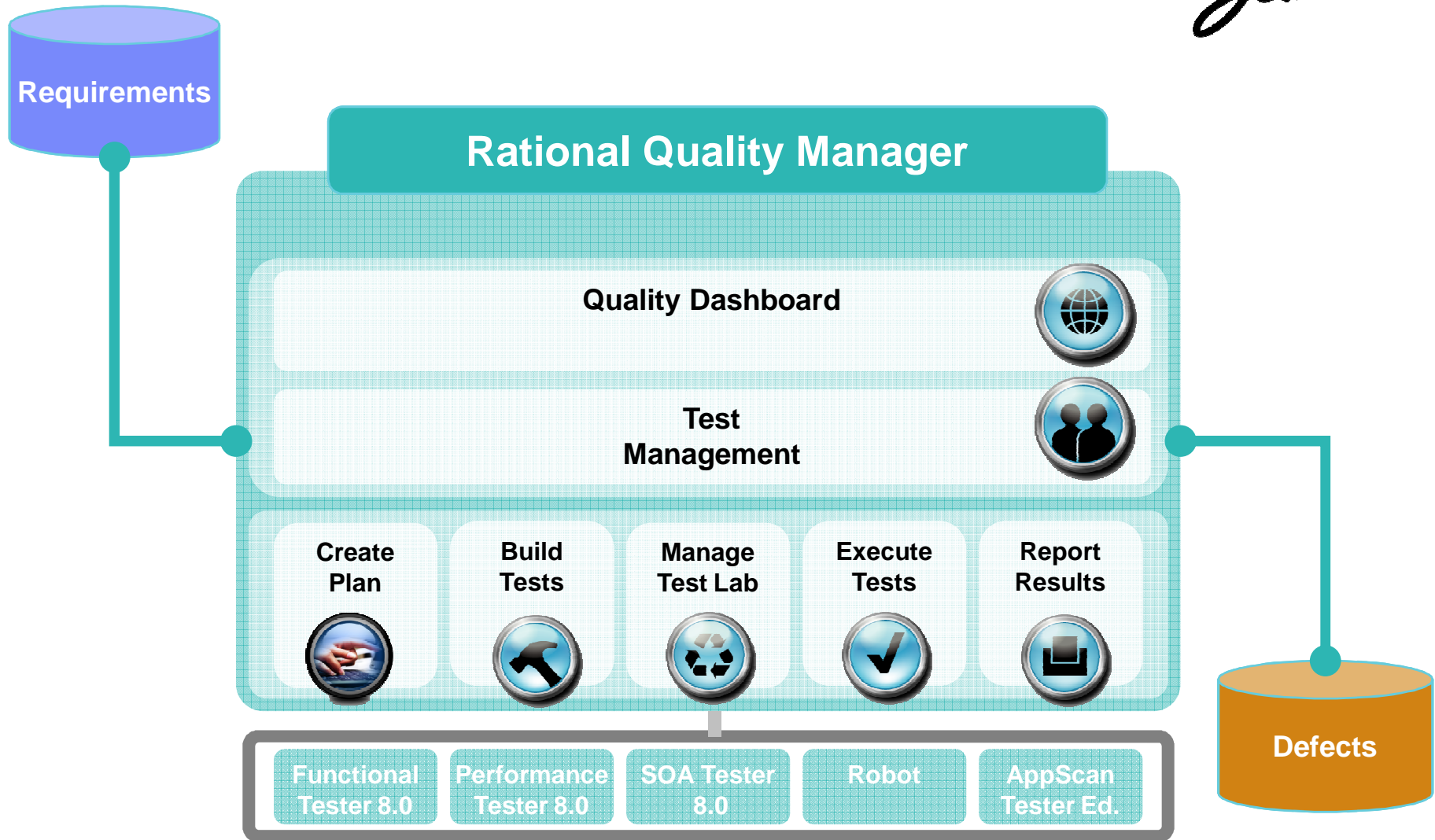
- Test Plan, Test Cases, Test Scripts
 - Include security tests
 - Monitor and report on test coverage

Enable your testers to create security tests



- QA begins writing their own security tests
- By now have acquired some security knowledge in the team
- Leverage skills of experts to scale out testing to more junior testers
 - Templates to capture expert knowledge, making it easy for more junior testers
- Authoring a simple Security Test can be as easy as making a recording
 - Familiar if they are using Rational Functional Tester or Rational Performance Tester

Jazz

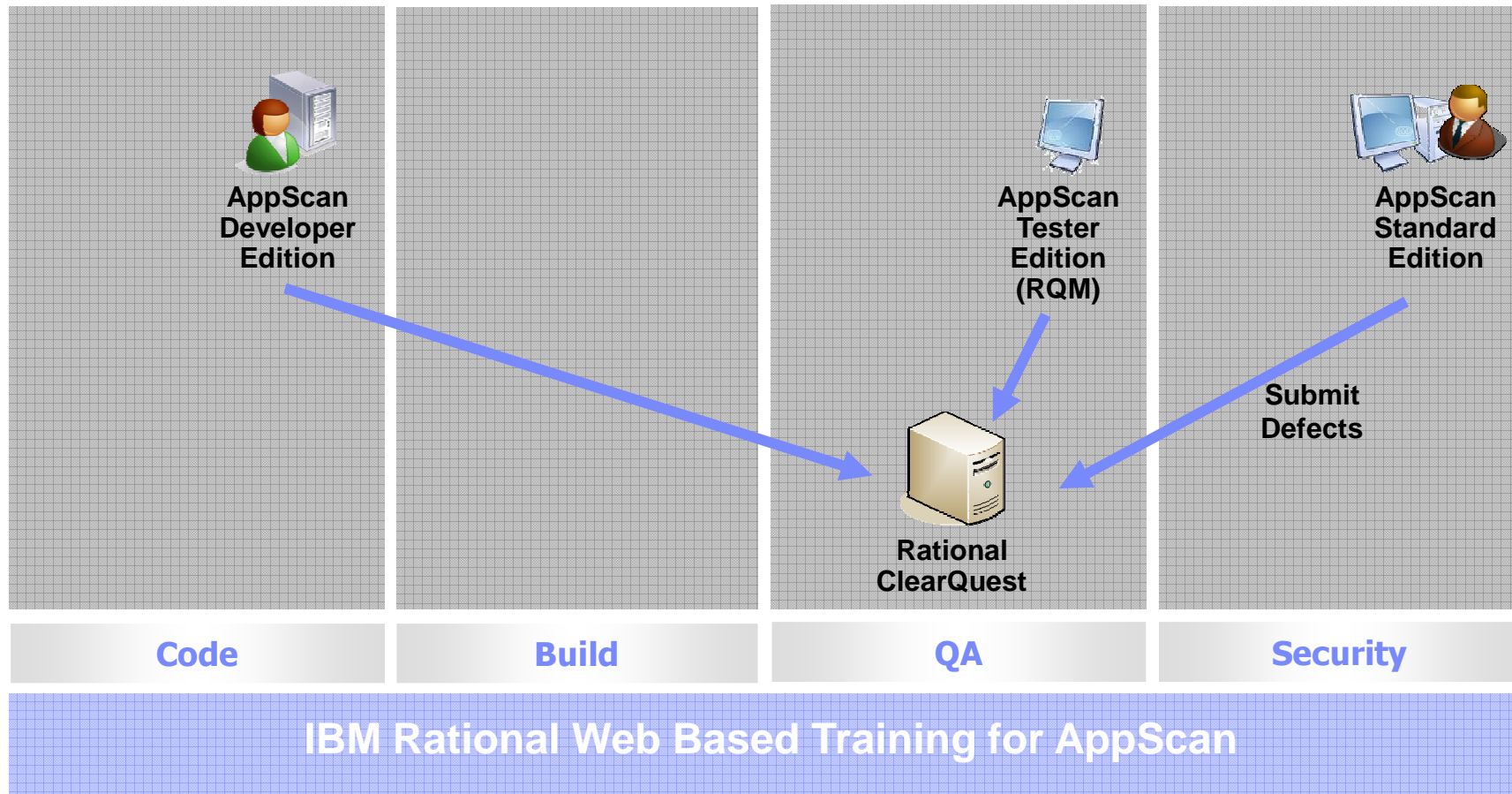


AppScan Tester Edition

- Black-Box Testing Technology

- Integrate Security Testing into well governed QA Process
 - Leverage RQM Test Management Platform
 - Delegate security testing

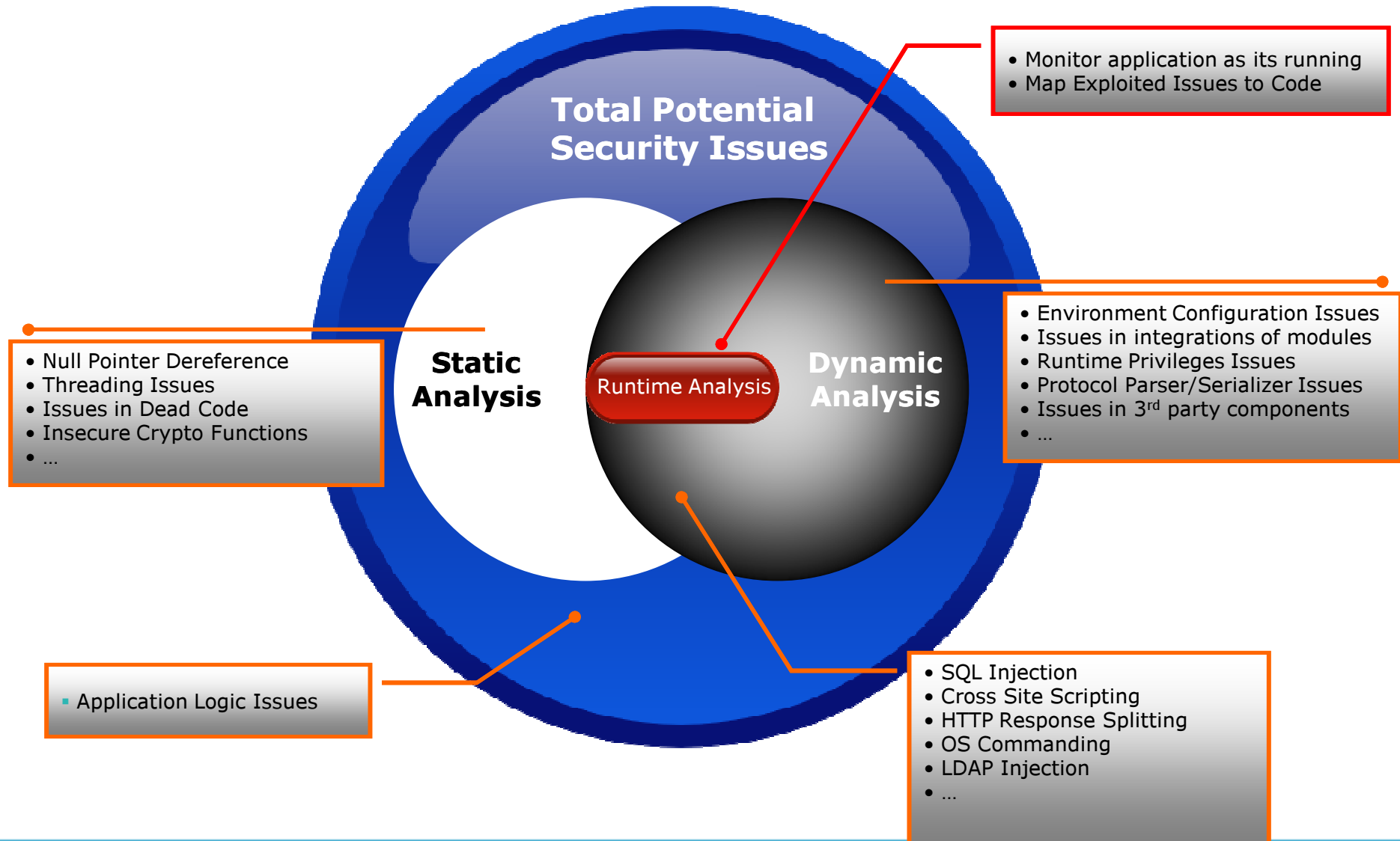
IBM Rational AppScan SDLC Ecosystem



AppScan Developer Edition

- Includes White-Box, Black-Box & Runtime Analysis
 - Side-by-side, gain the strengths of all techniques
- Uses Composite Analysis , merging the different ways
 - CA overcomes the weaknesses of each technique, such as:
 - Theoretical White-Box issues confirmed by Black-Box
 - Black-Box Coverage measured with Runtime Analysis
- Extreme Emphasis on Accuracy & Actionable Results
 - Innovative Static String Analysis dramatically improves accuracy
 - Runtime Analysis maps Black-Box issues to code
 - Correlated Black-Box & White-Box results practically guaranteed

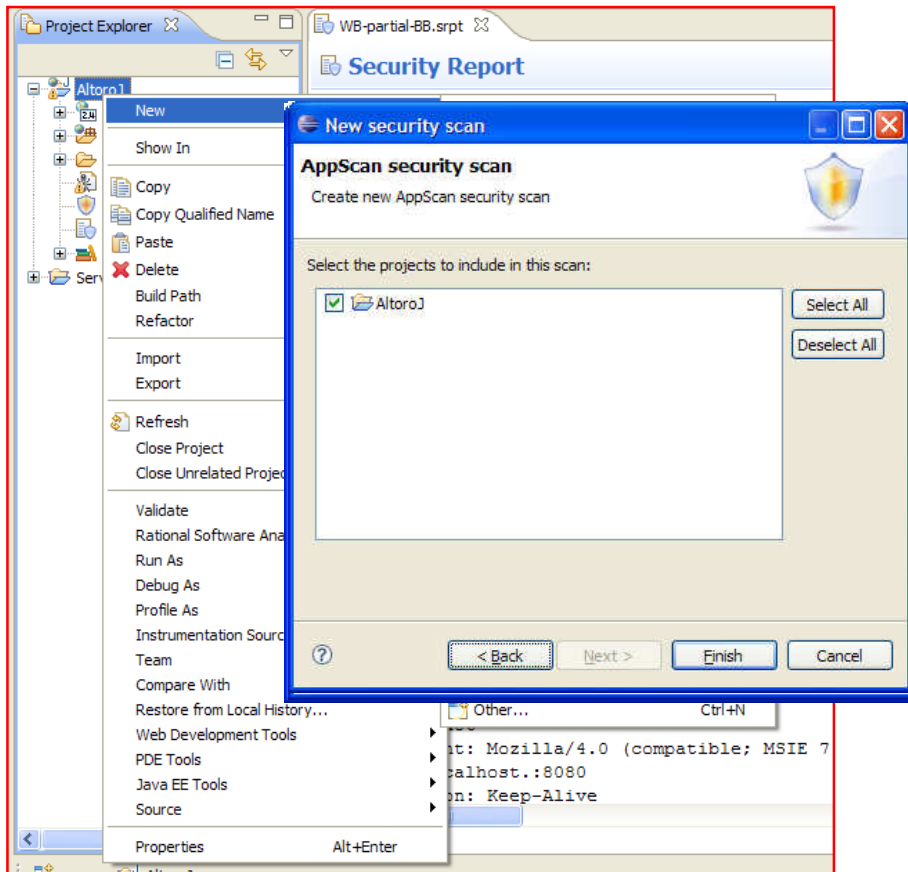
Security Issues Coverage

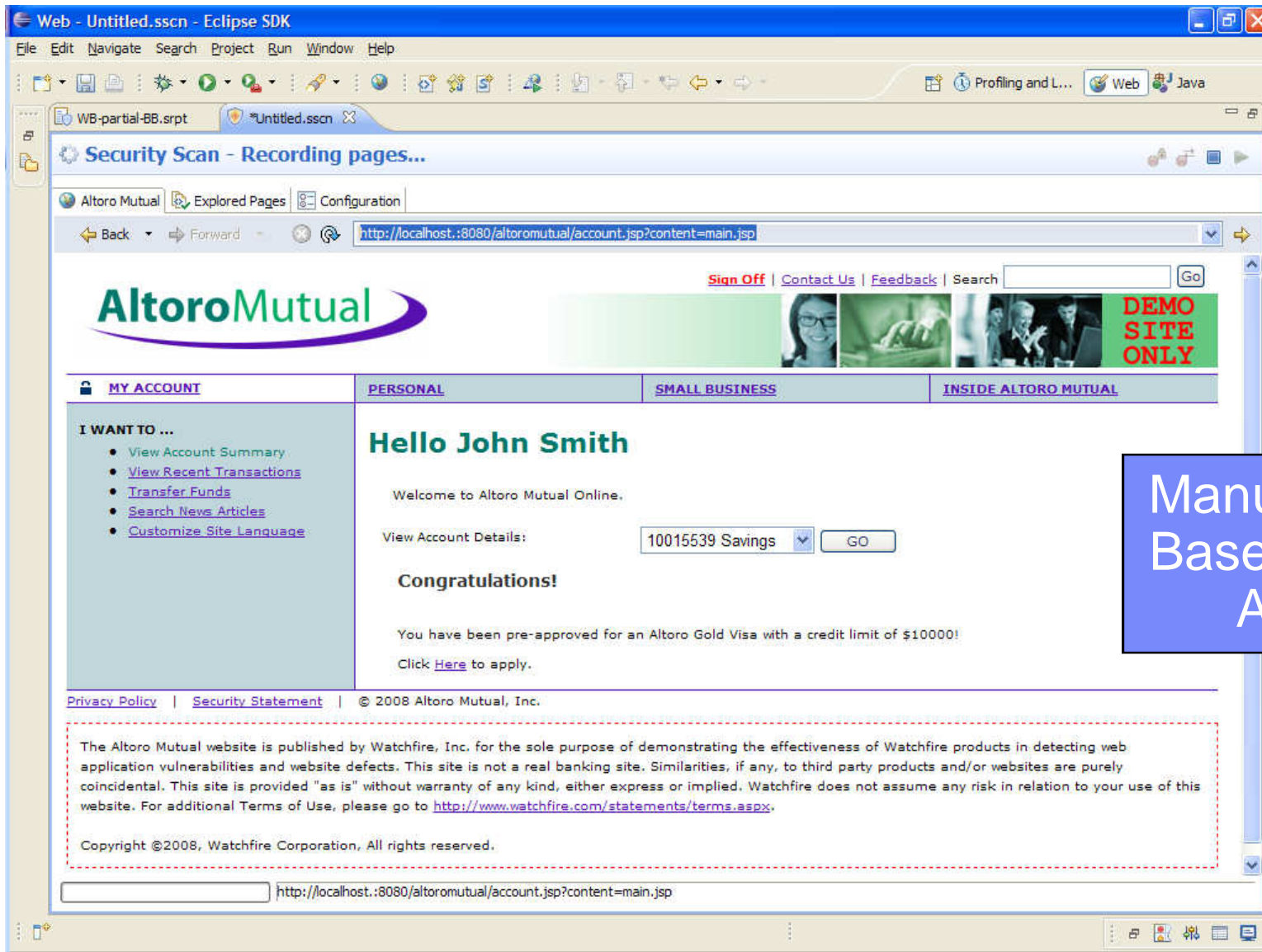


Self-Serve Security Testing for Developers

- Detailed results include all you need to know
 - Comprehensive information about each security issue and its impact
 - Clear prioritization account for security risk and exploitability
- Remediation view turns risk into tasks
 - Look at the problems from a development tasks perspective
 - Risk manifested in task priority
- Detailed Fix Recommendations clarify needed action
 - Complete with platform-specific code examples
 - Retest capabilities enable verifying the fix works
- Built in and accompanying training supports self-serve
 - Issue-specific flash-based training built into product
 - Product & Security Web-Based Training will be available at GA

Wizard-based Scan Creation



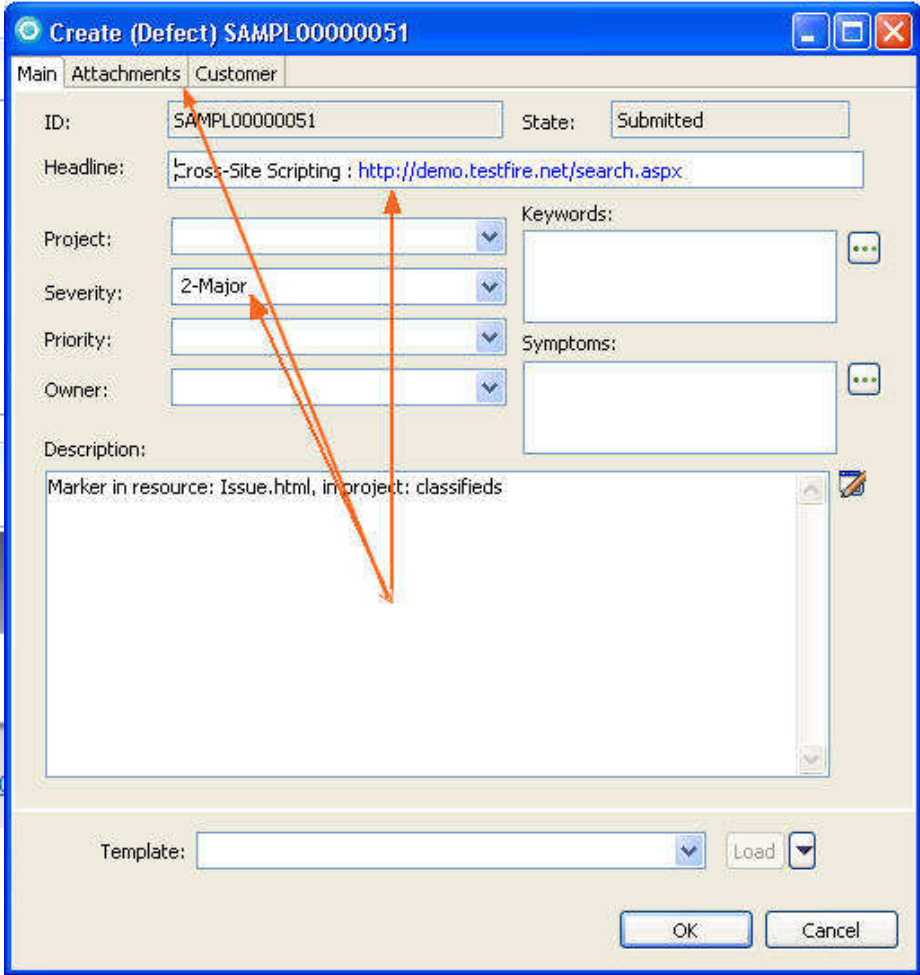
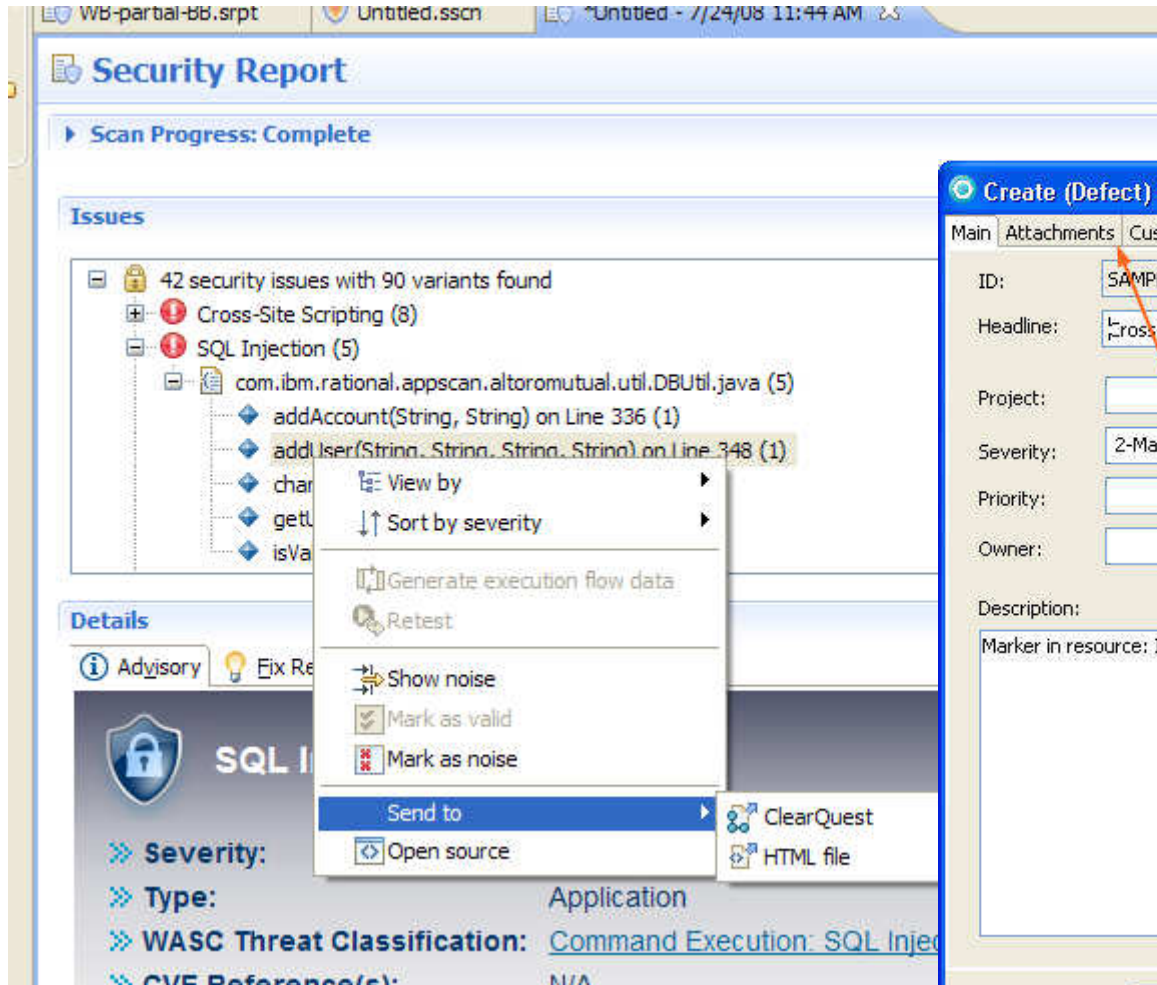


Manual-Explore
Based Dynamic
Analysis

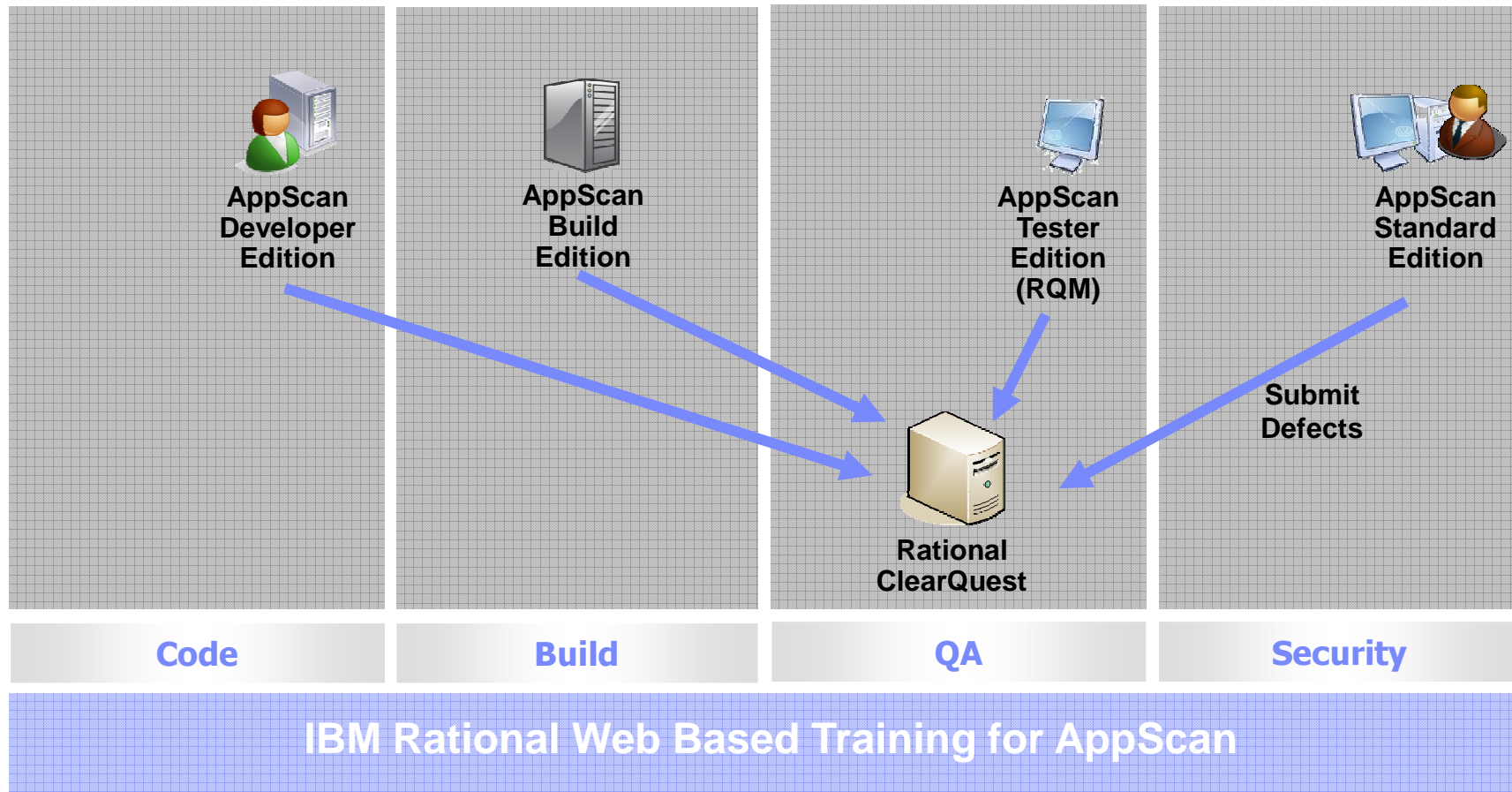
The screenshot shows the Eclipse SDK Security Report interface. The top toolbar includes File, Edit, Navigate, Search, Project, Run, Window, and Help. The main window displays a 'Security Report' for a scan that is complete. Under the 'Issues' section, there are four categories of vulnerabilities: Cross-Site Scripting (11), SQL Injection (5), SSI Injection (4), and Link Injection (facilitates Cross-Site Request Forgery) (8). The 'Details' section for the selected issue is expanded, showing 'Possible Causes' (Sanitization of hazardous characters was not performed correctly on user input) and a 'Technical Description' of a Cross-Site Scripting attack. A 'Demonstration' video player is embedded in the details view, showing a browser window with a security warning and a 'Security' dialog box. A link 'Open in new window' is visible below the video player.

Actionable Results
 Prioritized, include all the info to understand and remediate issues

Built-in Export
to ClearQuest



IBM Rational AppScan SDLC Ecosystem

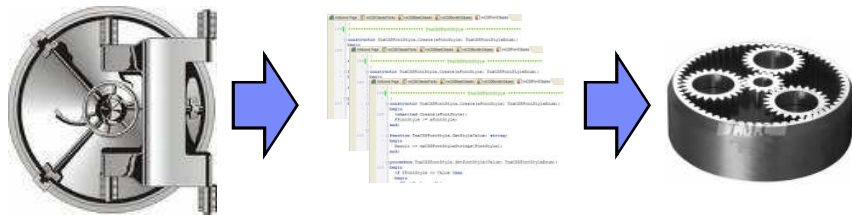


AppScan Build Edition

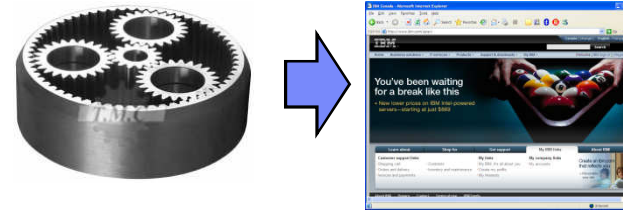
- Allows scans created by either AppScan Standard or Developer Edition to be processed in a non-UI / scriptable mode
- Provides generic command line support for integration into any build environment
- Provides a BuildForge Adaptor so that integrating AppScan testing is an experience that should be familiar/expected for a BuildForge practitioner

AppScan Build Edition Use-Case

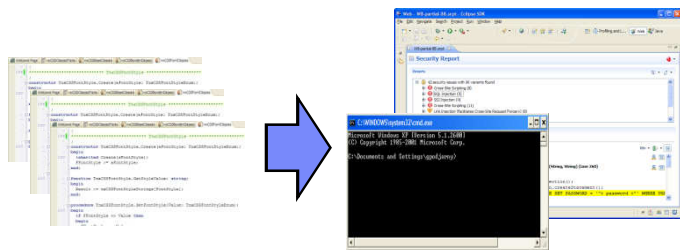
1. Build System compiles code



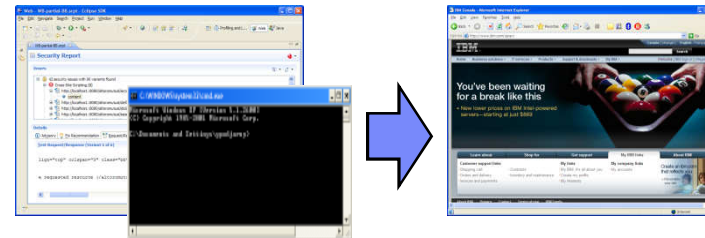
3. Application auto-deployed



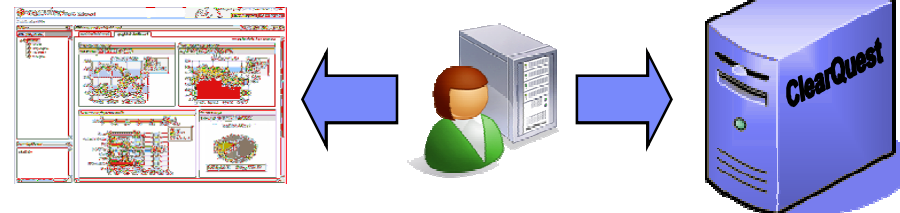
2. RASBE Static Analysis Invoked



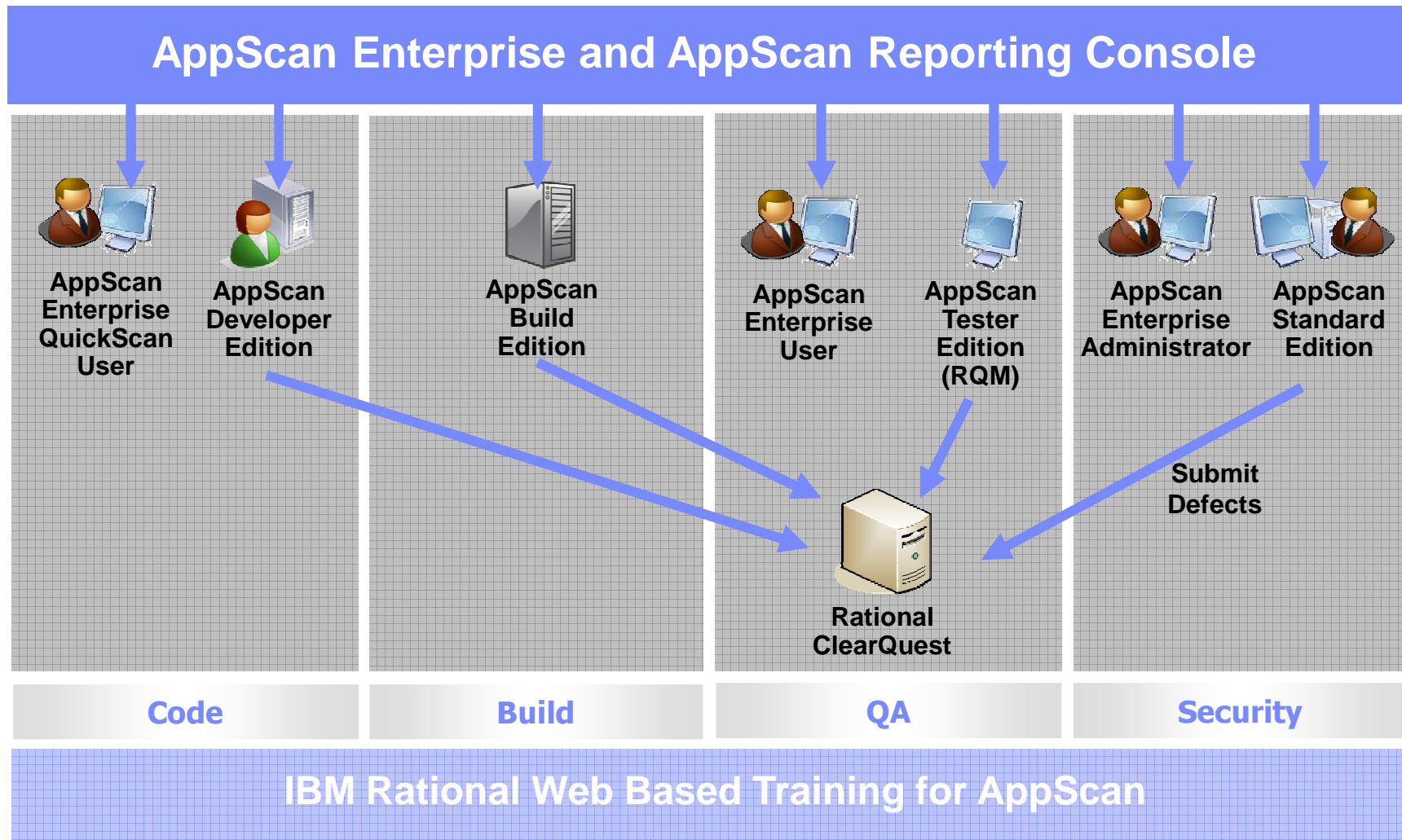
4. RASBE Dynamic Analysis Invoked



5. Found issues logged



IBM Rational AppScan SDLC Ecosystem



AppScan Enterprise Edition

scalable, web-based, multi-user solution to manage web application security

IBM Rational AppScan Enterprise Edition Jim (Analyst) | Help | Support | About | Log Out

Navigation Tree:

- Frank
- Jim
- Developers
 - Admin
 - Andrew
 - Chris
 - Jennifer
- Templates

Issue Severity History

All Report Packs

Issue Management History

All Report Packs

Issue Severity by Report Pack

WASC Threat Classification

All Report Packs

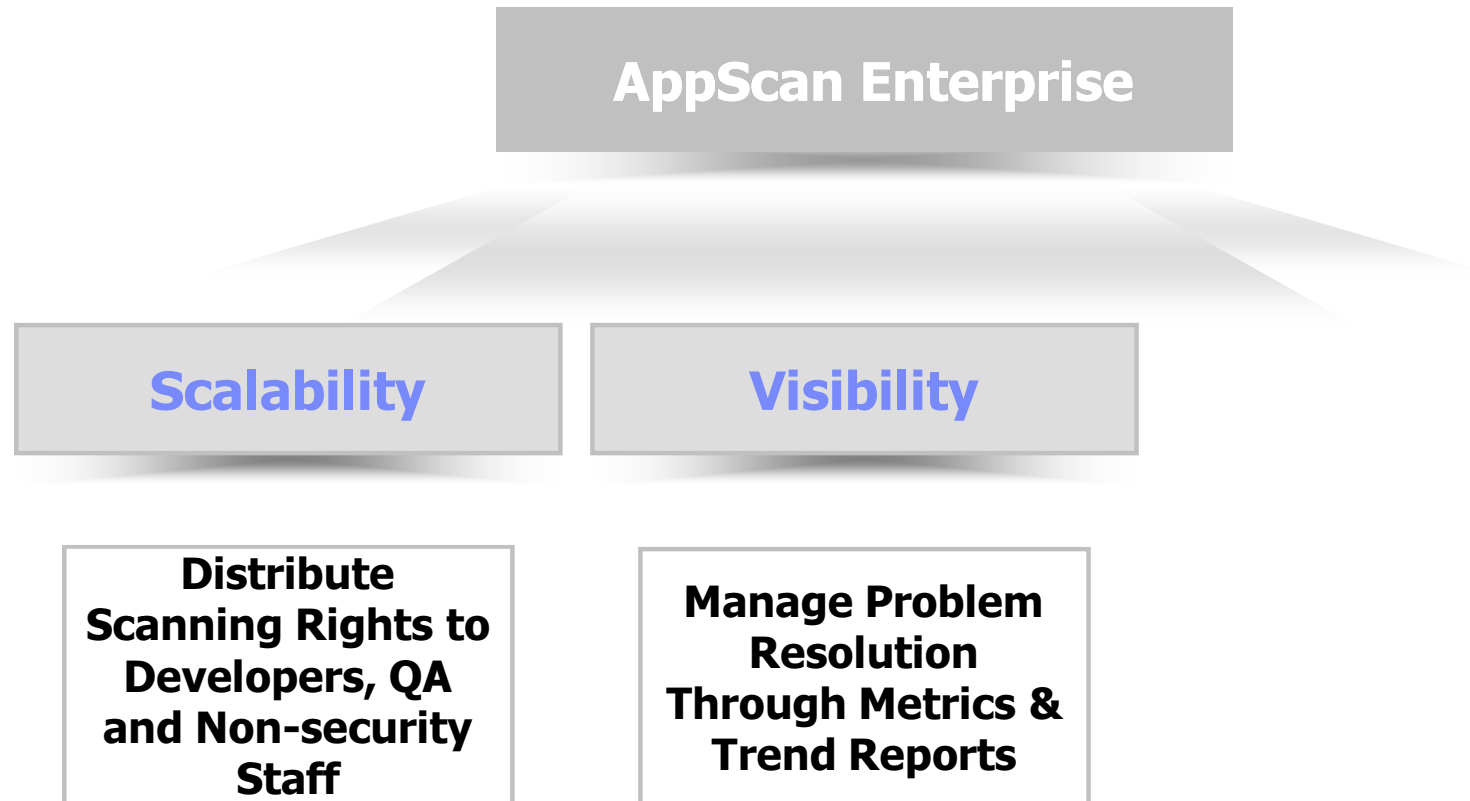
Recently Viewed

- Analysts
- Applications
- Security Issues (Investment Banking)
- Report Pack Summary (Investment Bank)
- Sarbanes-Oxley Act (SOX) (Investment)
- Activity Log (Test Admin)
- Report Pack Summary (Test Admin)
- Personal Banking

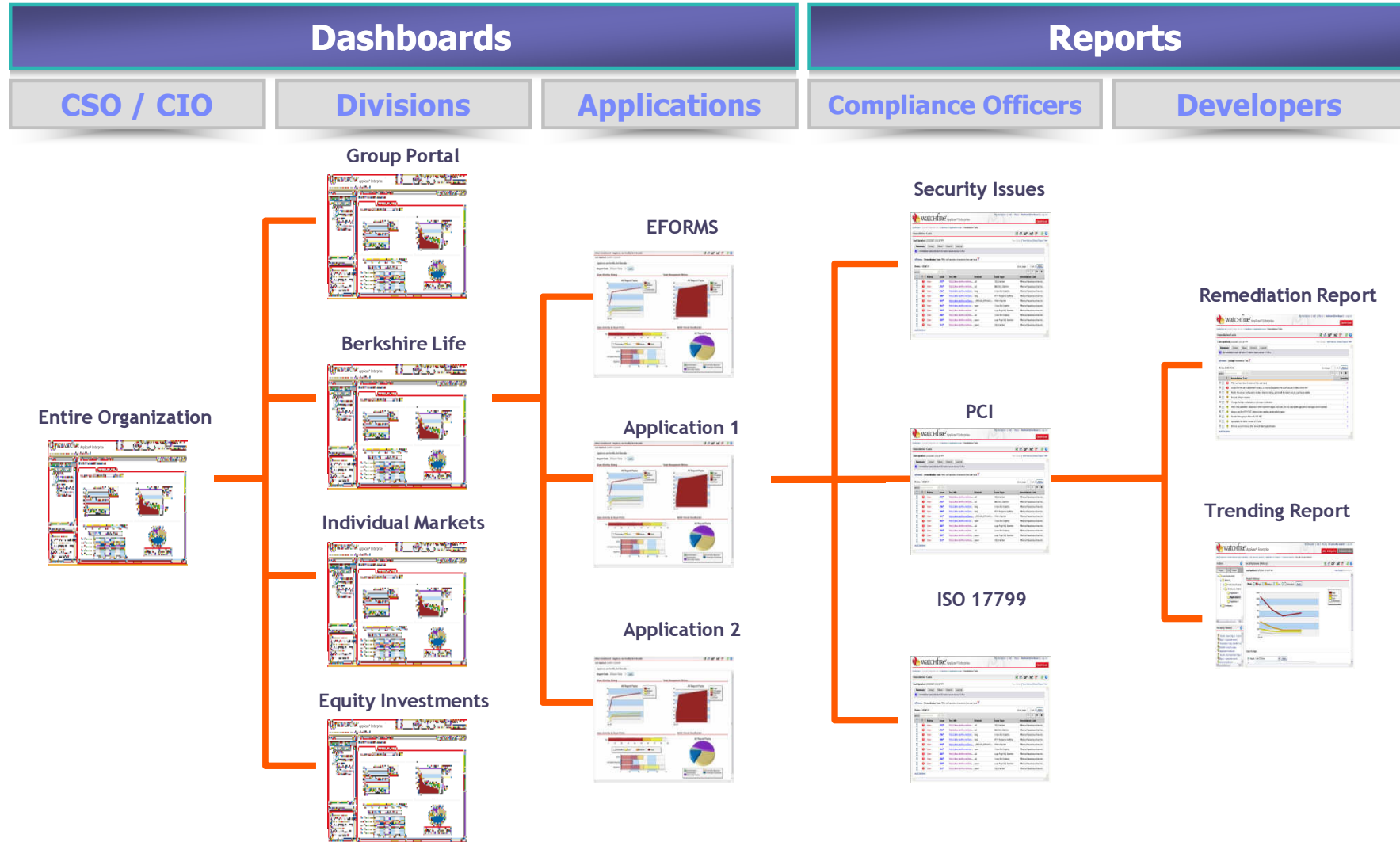
QM05

49

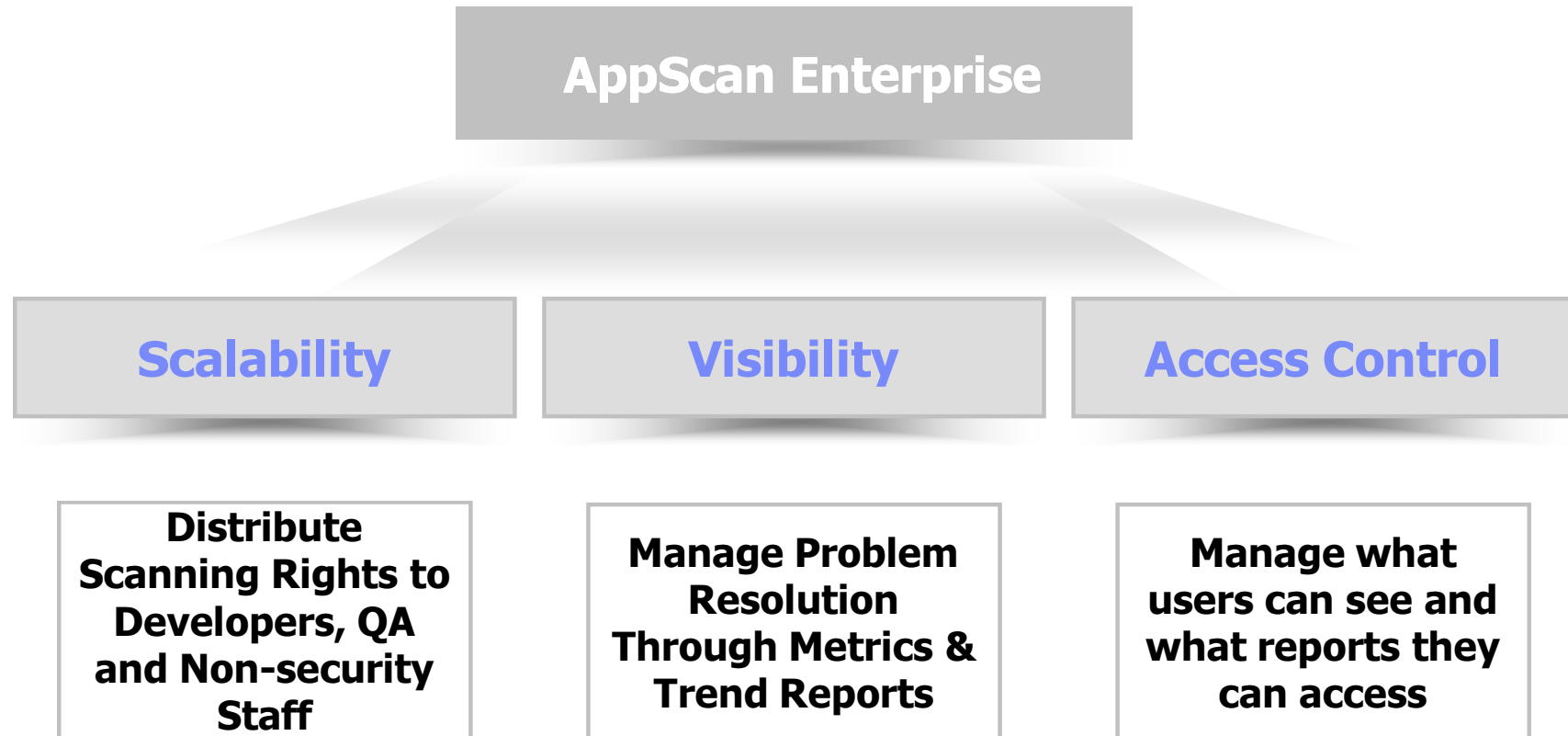
The Power of AppScan Enterprise



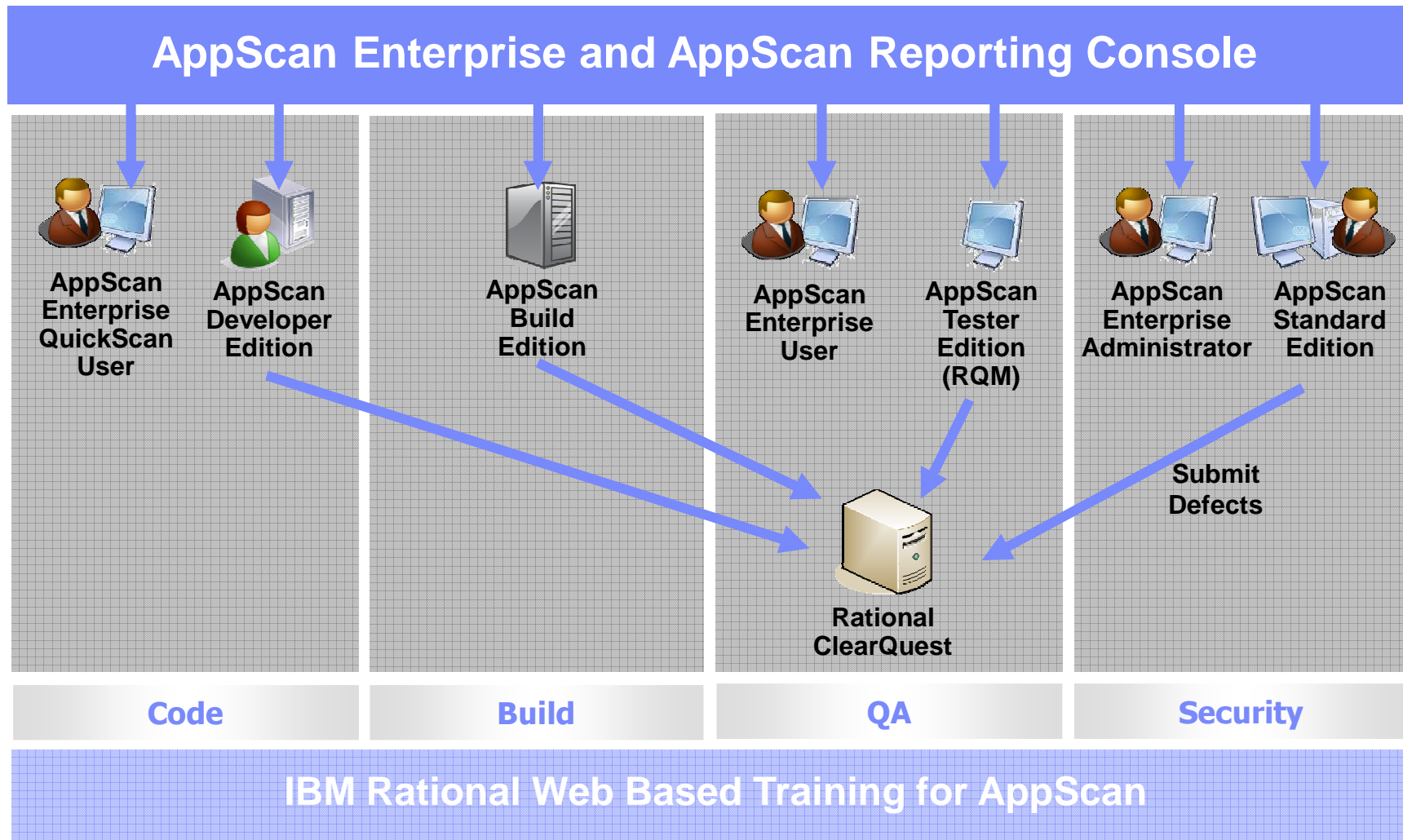
Visibility throughout the Enterprise



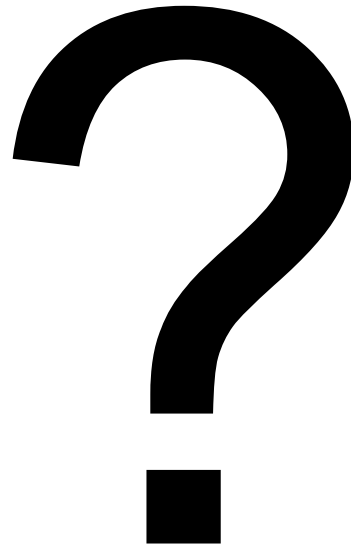
The Power of AppScan Enterprise



IBM Rational AppScan SDLC Ecosystem



Questions



QuickScan – What Is It?

- QuickScan gives developers black box scanning capability from a simple, self-service web portal

- QuickScan leverages administrator-defined Scan Templates, so running a scan is as simple as clicking a button
 - Shields developers from the complexity of configuring a scan
 - Keeps control in the hands of the security team