IBM Security Forum

Soluções para um ambiente seguro

Conformidade com PCI & Segurança em Aplicações Web

Felipe Freire
IT Specialist
pfreire@br.ibm.com

Agenda

- Introdução ao PCI
- Prazo: 30 de Junho de 2008 – sessão 6, sub-sessão 6.6 se tornou obrigatória
- A falta de conformidade pode causar danos
- Visão geral da segurança de aplicações
- Foco na raiz do problema
- Soluções IBM
- Recursos para PCI

PCI

- **O que é PCI – Payment Card Industry?**
  - Um conjunto mínimo de padrões de segurança usado para proteger os donos de cartões. Criado pela Visa, Mastercard, American Express e Discover.
- **Quem deve estar conforme?**
  - Todas empresas que aceitam pagamento com cartão de crédito e débito ou coletam, processam ou armazenam informações sobre transações.
- **O que precisa ser feito para estar em conformidade?**
  - Requer que todos os endereços de IP para interface com a internet sejam varridos ("*scaneados*") buscando vulnerabilidades.
- **Quais são as penalidades para falta de conformidade?**
  - As companias de cartões de crédito podem estabelecer multas de milhões de dólares
  - A capacidade de processar cartões de crédito pode ser revogada
  - Despesas associadas com roubo de informações; notificação dos possuidores de cartões

The 12 Requirements for PCI DSS Compliance

- **Build and Maintain a Secure Network**
  1. Install and maintain a firewall configuration to protect data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
  3. Protect stored cardholder data
  4. Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**
  5. Use and regularly update anti-virus software
  6. Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  7. Restrict access to cardholder data by business need-to-know
  8. Assign a unique ID to each person with computer access
  9. Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks**
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes

- **Maintain an Information Security Policy**
  12. Maintain a policy that addresses information security

Includes Web Application Security Guidelines

Section 6 Requirements

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.

6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:

6.5 Develop all web applications based on secure coding guidelines such as the Open Web application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security

Installing an application layer firewall in front of web-facing applications.

Section 6.6 Requirement Confusion

6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

1. Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security

2. Installing an application layer firewall in front of web-facing applications.

Clarification of Section 6.6 Requirements

Clarification on – "Code reviewed for vulnerabilities":

1. Manual review of application source code
2. Proper use of automated application source code analyzer (scanning) tools
3. Manual web application security vulnerability assessment
4. Proper use of automated web application security vulnerability assessment (scanning) tools

Clarification on – "By an organization that specializes in application security":

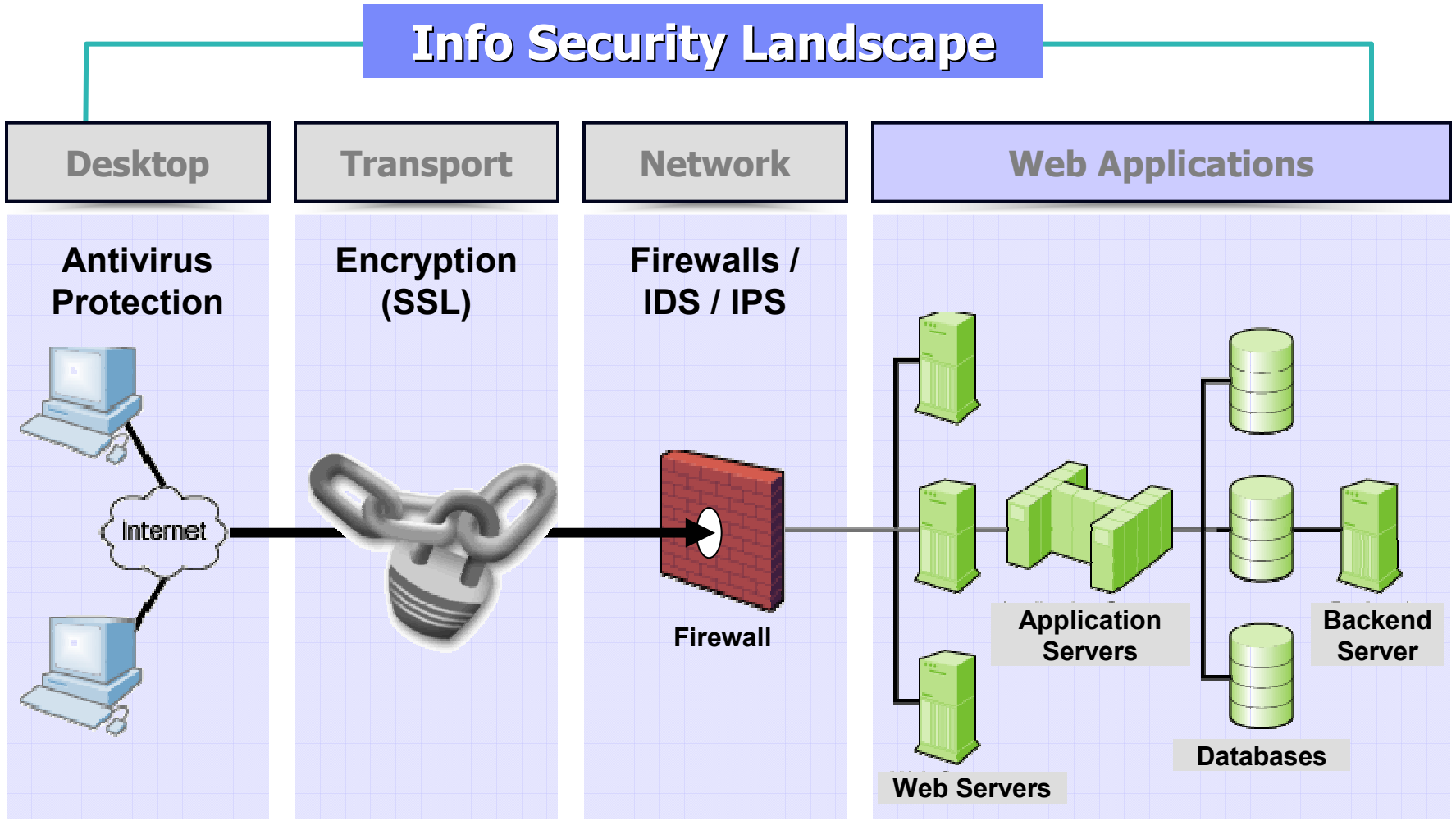
- Manual reviews/assessments may be performed by a qualified internal resource or a qualified third party.

https://www.pcisecuritystandards.org/pdfs/04-22-08.pdf

What Does This Mean?

- Merchants must employ specialized solutions – like IBM Rational® AppScan® -to perform thorough vulnerability analysis of applications
- The company performing the analysis must also have the internal expertise to understand the findings and make appropriate changes
- Alternative: outsource the application assessments to specialized vendors such as IBM ISS

Application Security - Understanding the Problem



State of the Application Security Threat

Growing Threat

- Past customer spending focused on Network security – yet 75% of attacks come through web applications – market is now focusing on spending on web application security
- Mitre group indicates that application issues (XSS and SQL Injection) are the top 2 hacks
- Most websites are vulnerable (Watchfire/Gartner)

Analyst Views

*"*Gartner estimates that **90 percent of externally-accessible applications today are web-enabled, and that two-thirds of them have exploitable vulnerabilities.**

"64% of developers are not confident in their ability to write secure applications"

Microsoft Developer Research

- **Security Breach** **Cost of Application Security Breach**
  - Every lost record costs $138 to the organization who lost it
  - Media Attention > Brand Damage > Sharp Decline in Stock Prices

Where Do These Problems Exist?

Type:

- Customer facing services
- Partner portals
- Employee intranets

Source:

1. Applications you buy – e.g. COTS
2. Applications you build internally
3. Applications you outsource

Non-Compliance Can Hurt!

Stiff Penalties for Failure to Compliance

1. Loss of charge card privileges
   - This would be a death sentence for many businesses!
2. Fines levied by the credit card companies
   - Can be millions of dollars
3. Expenses associated with disclosing data loss
   - Notification of affected cardholders, credit checking services
   - Note: there is no evidence that a security breach adversely impacts customer loyalty
4. Civil action
   - TJX is being sued all over (banks, class action)

What's the Root Cause of this Problem?

1. Software developers were never trained (or mandated) on security

2. Existing defenses do not address application level threats

3. Security teams are focused on other issues (network, desktops, etc) and overwhelmed

4. No defined policy, accountability or process to deal with this issue

Focus on the Root of the Problem

- Compliance doesn't automatically mean security
  - Security isn't static
    - New vulnerabilities are frequently announced
    - Enhancing and maintaining applications
  - How frequently do code changes occur? Code changes = new policies or additional fine tuning of your application firewalls = administrative costs
- Your code is the last and best defense
  - Unique and custom web applications need unique and custom security measures
  - "Hard and crunchy on the outside, soft and gooey on the inside"

How much do security defects cost?

	Found in Design	Found in Coding	Found in Integration	Found in Beta	Found in GA
Design Errors	1x	5x	10x	15x	30x
Coding Errors		1x	10x	20x	30x
Integration Errors			1x	10x	20x

PCI: "…the team writing the software should not perform the final review or assessment and verify the code is secure."

Short Term Objectives:

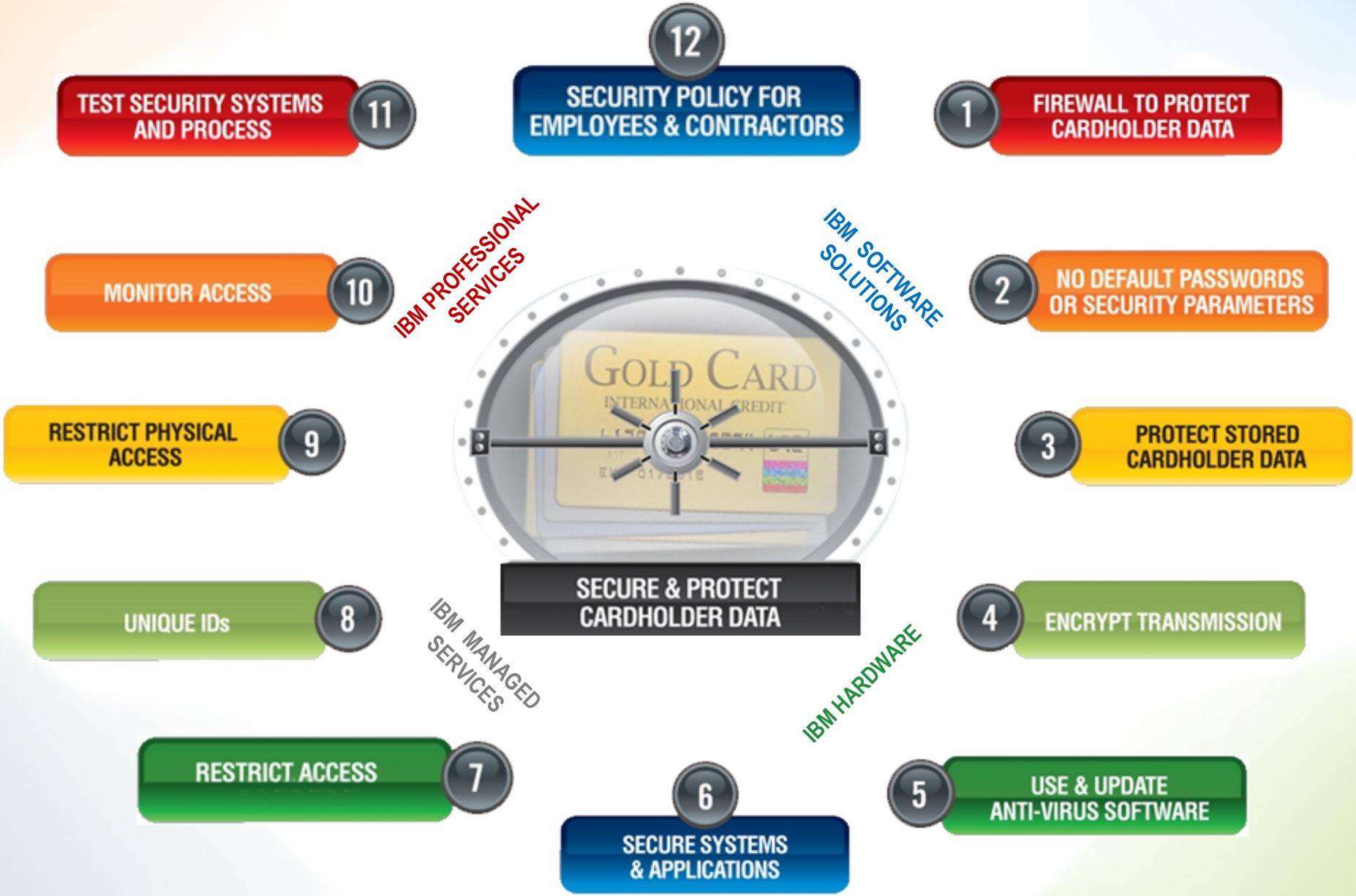
- Code Review and Assessments **(independent of development team)**
- Comply with new PCI Requirement 6.6 Clarification **(June 30 deadline)**

Long Term Objectives:

- Implement a secure software development process
- Tools should be made available to software developers and integrated into their development suite

IBM Solutions for Application Security and PCI

IBM Services, Software and Hardware:
IBM has solutions to address all 12 PCI requirements



IBM Solutions for PCI 6.6

- Application Code Review
  - Manual review of application source code
  - Proper use of automated source code analyzer (scanning) tools
  - Manual web application security vulnerability assessments
  - Proper use of automated web application security vulnerability assessment (scanning) tools.

Options:

In house: Rational AppScan

Outsource: IBM Services

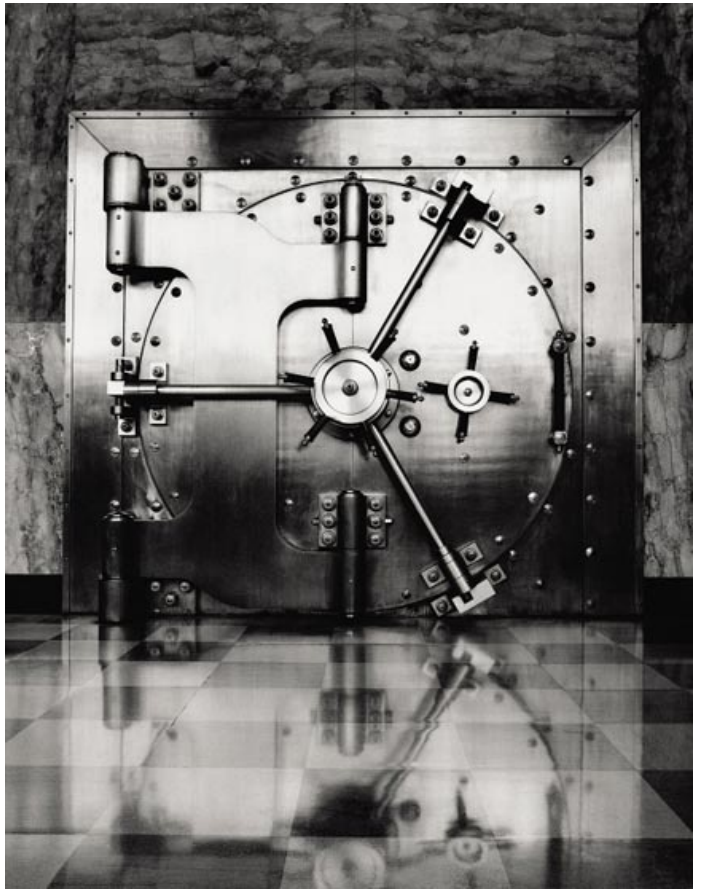
IBM ISS Professional Services offerings

- **PCI Assessments**
  - Assessment of companies that accept, store, or process credit card information for compliance with the Payment Card Industry (PCI) Data Security Standard

- **Application Security Assessments**
  - Remote attack simulation in which security experts attempt to penetrate an application, using techniques similar to those used by malicious attackers
  - Identification and exploitation of application vulnerabilities to determine application security and accessibility of data

IBM Rational AppScan

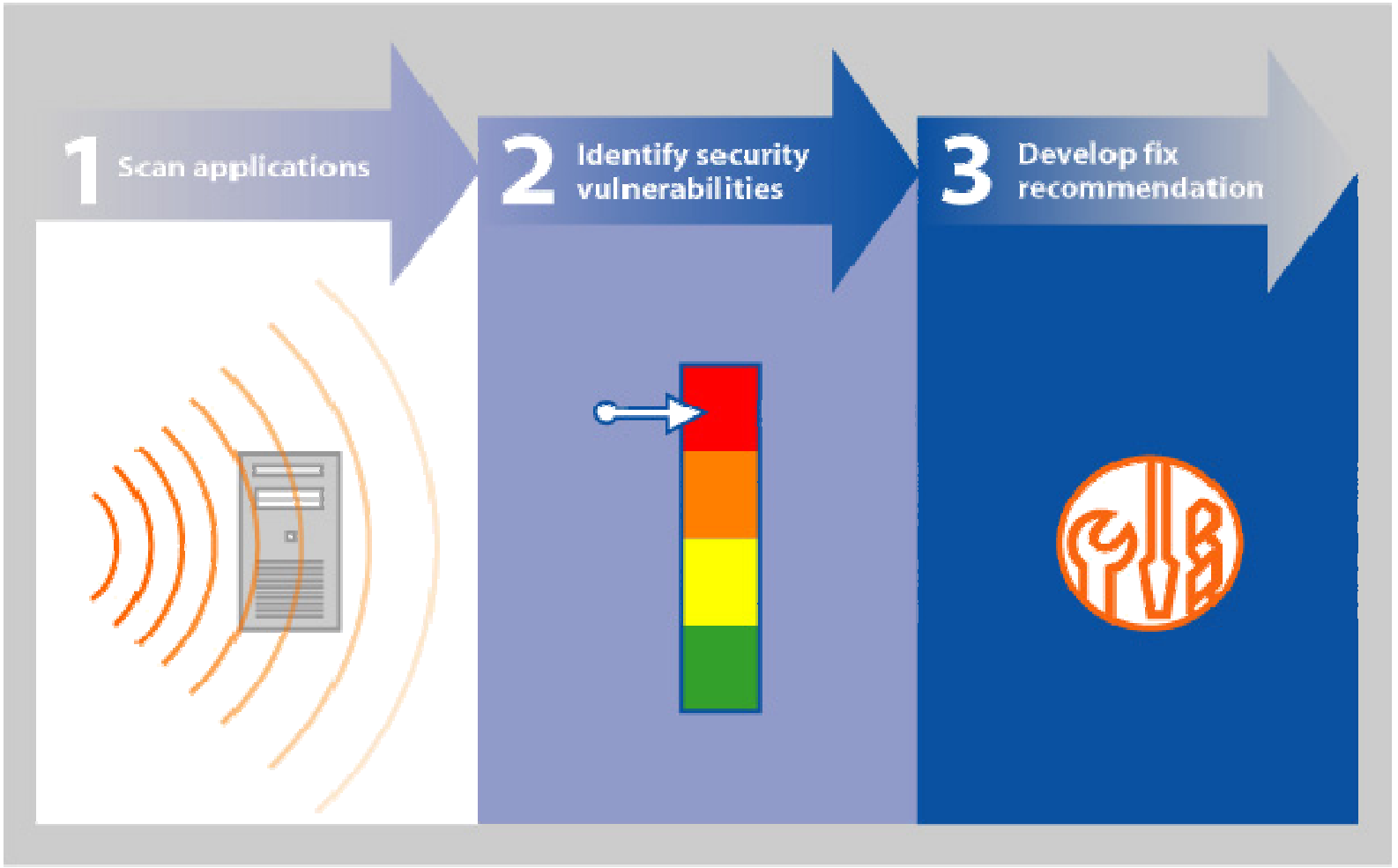
- The market leader
  - Rational acquired Watchfire in 2007
  - #1 in numerous industry “bake offs”
- Automatically scans web applications for vulnerabilities
  - SQL Injection
  - Cross-site Scripting
- Provides clear recommendations on how to fix them
  - i.e. Character sanitization



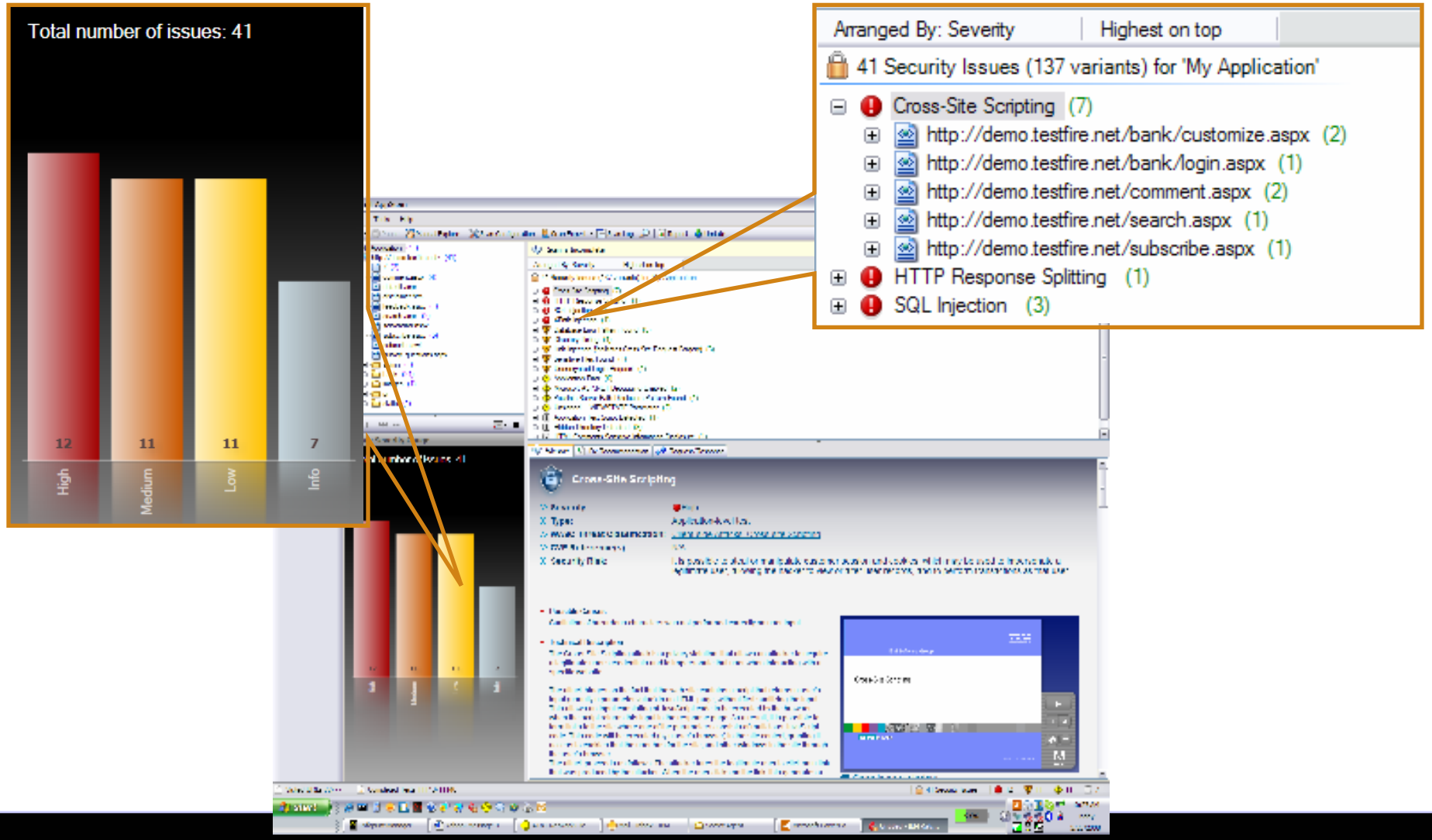
The Result?

Improved security, lower costs, and the ability to meet PCI standards for application security

How Does IBM Rational AppScan Work?



Easy to Understand Results – Issues and Priorities



Understanding the Problem

Advisory | Fix Recommendation | Request/Response

Cross-Site Scripting

Severity: High
Type: Application-level test
WASC Threat Classification: Client-side Attacks: Cross-site Scripting
CVE Reference(s): N/A
Security Risk: It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Possible Causes

Sanitation of hazardous characters was not performed correctly on user input

Technical Description

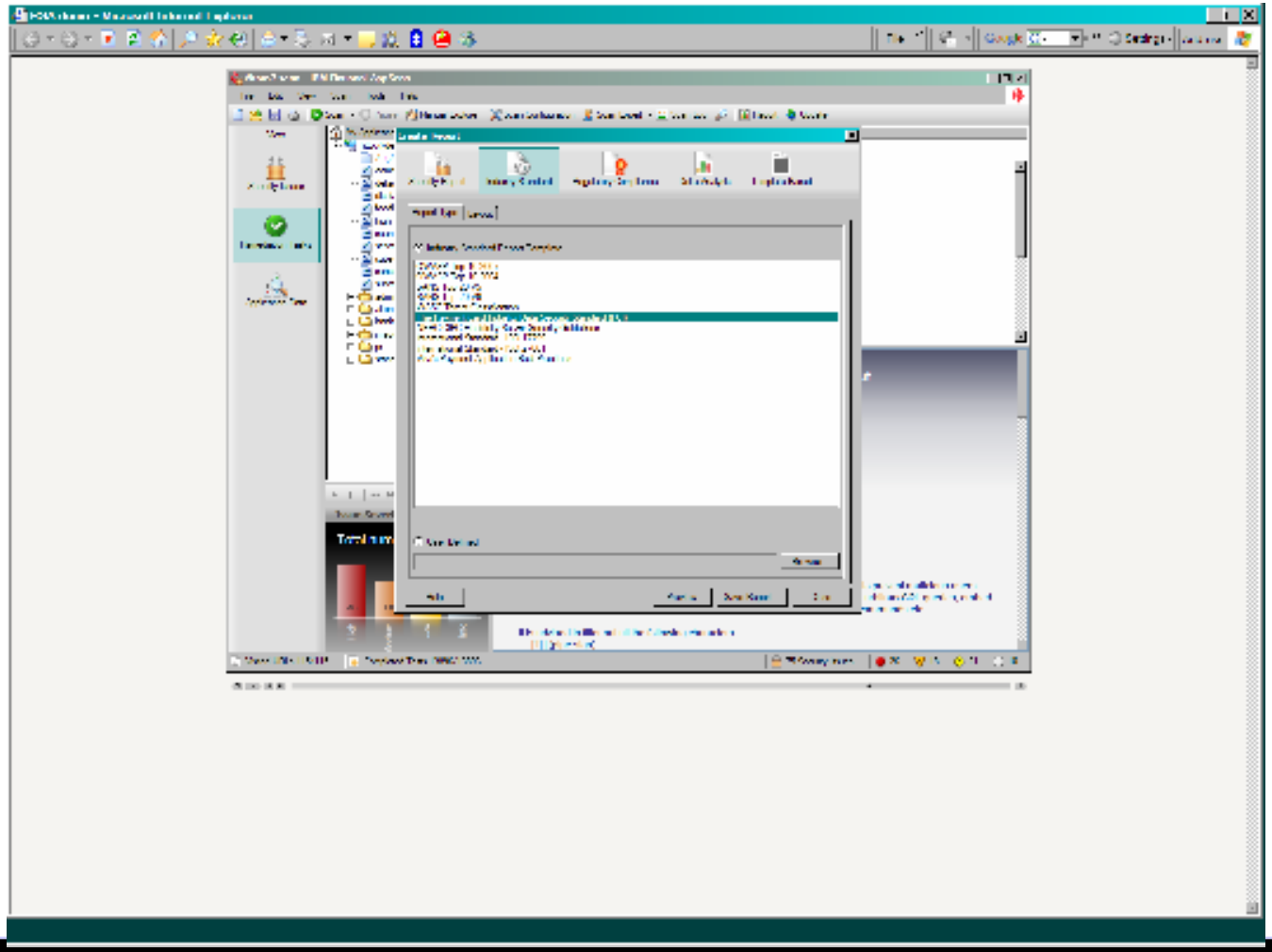
The Cross-Site Scripting attack is a privacy violation, that allows an attacker to acquire a legitimate user's credentials and to impersonate that user when interacting with a specific website.

The attack hinges on the fact that the web site contains a script that returns a user's input (usually a parameter value) in an HTML page, without first sanitizing the input. This allows an input consisting of JavaScript code to be executed by the browser when the script returns this input in the response page. As a result, it is possible to form links to the site where one of the parameters consists of malicious JavaScript code. This code will be executed (by a user's browser) in the site context, granting it access to cookies that the user has for the site, and other windows in the site through the user's browser.
The attack proceeds as follows: The attacker lures the legitimate user to click on a link that was produced by the attacker. When the user clicks on the link, this generates a request to the web-site containing a parameter value with malicious JavaScript code. If the web-site embeds this parameter value into the response HTML page (this is the essence of the site issue), the malicious code will run in the user's browser.

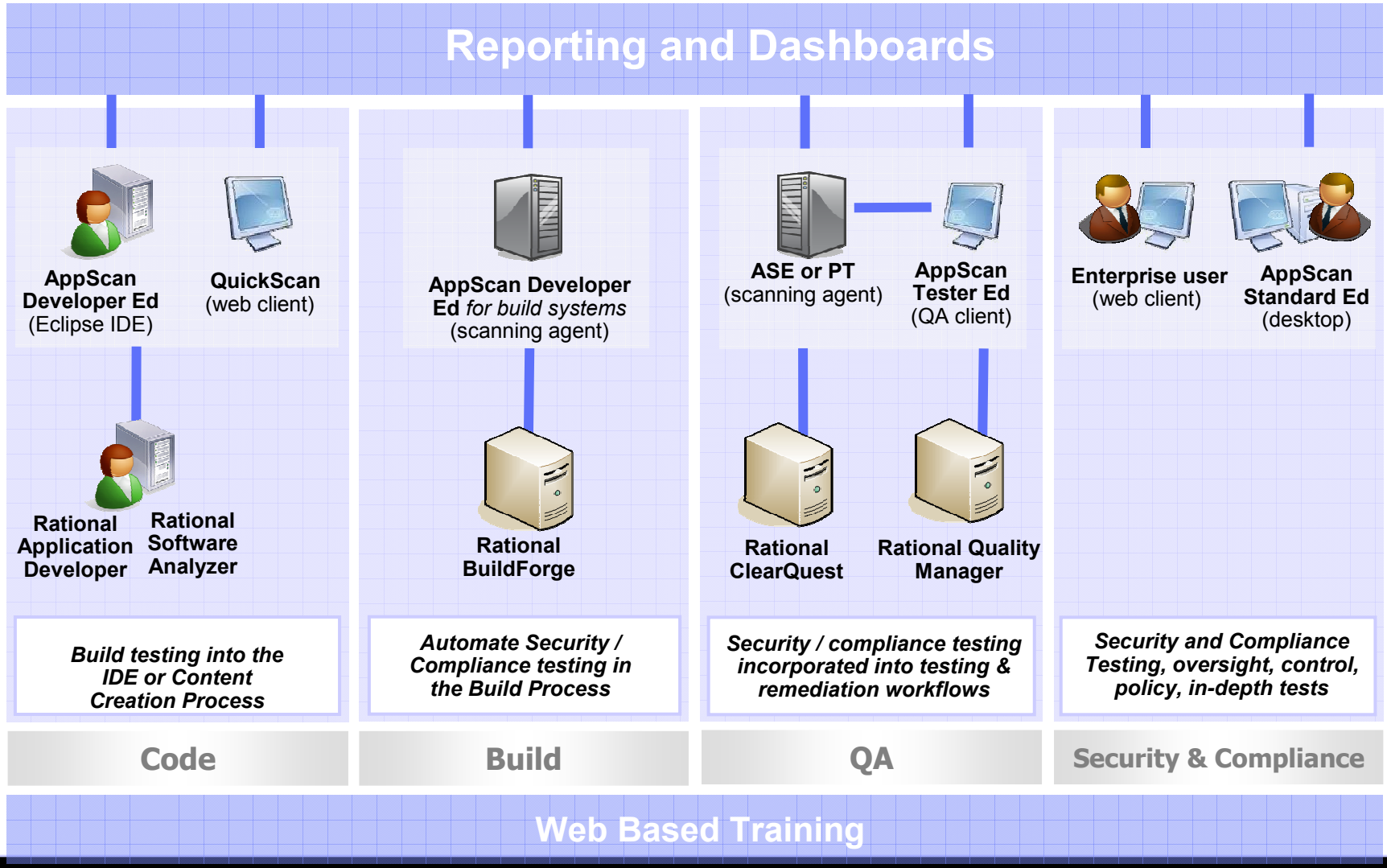
Open in new window

Integrated web-based training raises internal security expertise

PCI Compliance Reports



AppScan Solutions in the SDLC



PCI Compliance Resources

- **IBM PCI Resources**
  http://www-306.ibm.com/software/tivoli/governance/security/pci.html
- **IBM Rational AppScan**
  http://www-306.ibm.com/software/rational/offerings/testing/webapplicationsecurity/
- **IBM Tivoli Access Manager for e-business**
  http://www-306.ibm.com/software/tivoli/products/access-mgr-e-bus/
- **IBM Internet Security Solutions**
  http://www-935.ibm.com/services/us/index.wss/offerfamily/igs/a1025846
- **PCI Security Standards Council**
  http://www.pcicouncil.org