Pulse Comes to You 2012

Business without **LIMITS**

21 AUG 2012 | BANGKOK, THAILAND

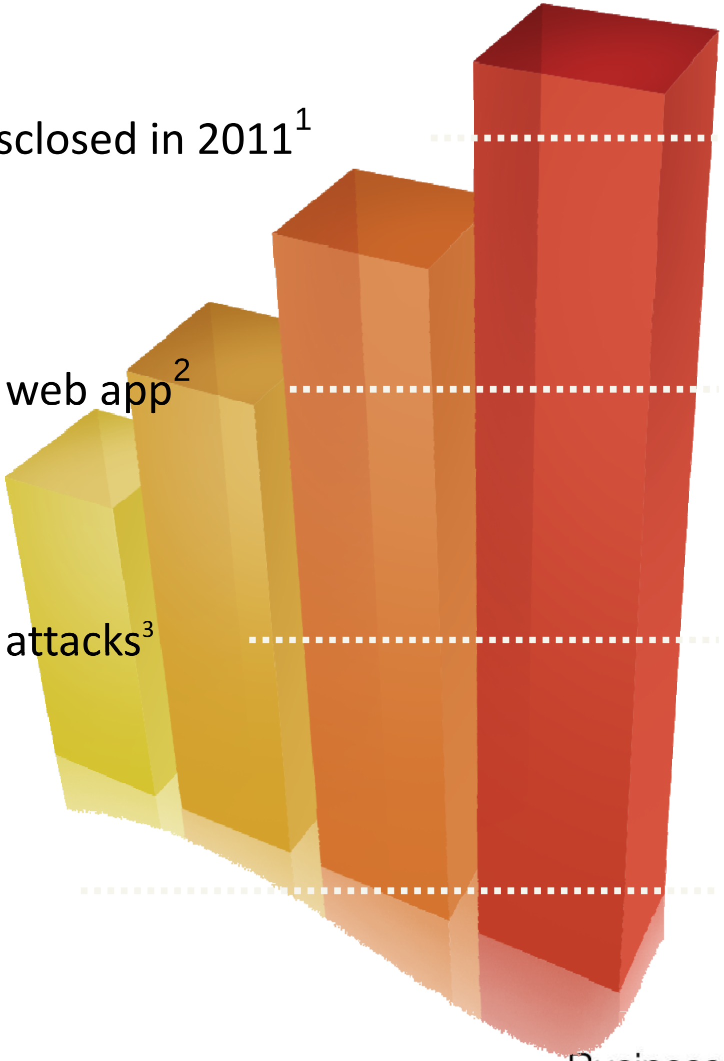
Driving Effective Application Security in the Enterprise

An End to End Approach to Addressing One of the Biggest Threats to a Business.

Sachin Raj

IBM Security, ASEAN

Application Security Statistics



Web application vulnerabilities / Total disclosed in 2011[1] 41%

Records compromised via attack against web app[2] 92%

Web Application attacks / All successful attacks[3] 54%

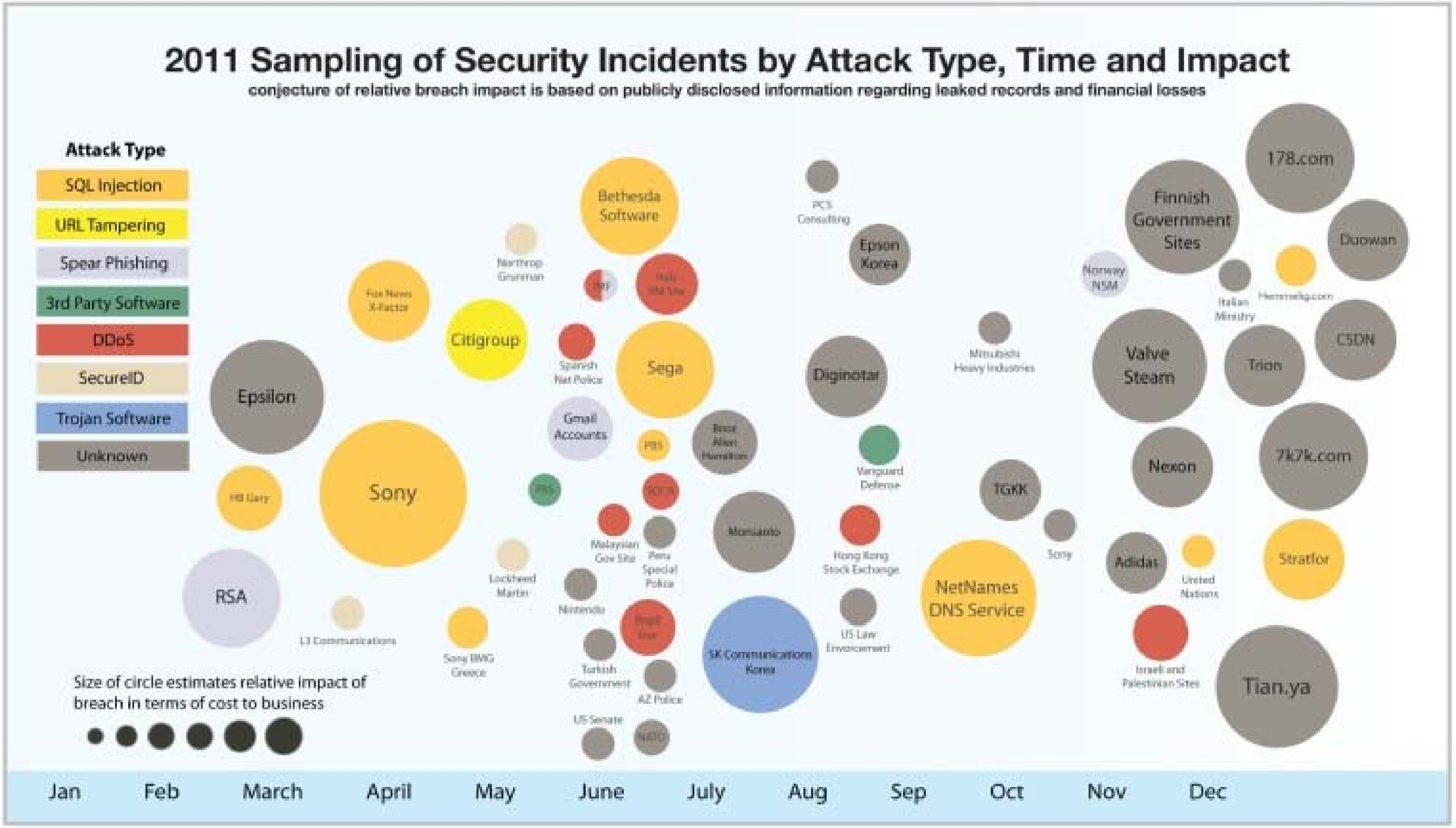
Tested sites do not comply with PCI DSS[4] 99%

[1] - IBM ISS X-Force Trend Report 2011

[2, 3] - Verizon 2010 Data Breach Investigations Report 2011

[4] - WASC Statistics Project - 2008

2011: Year of the security breach



2011 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Source: IBM X-Force® Research and Development

Application security challenges:

Security-development disconnect fails to prevent vulnerabilities in production applications

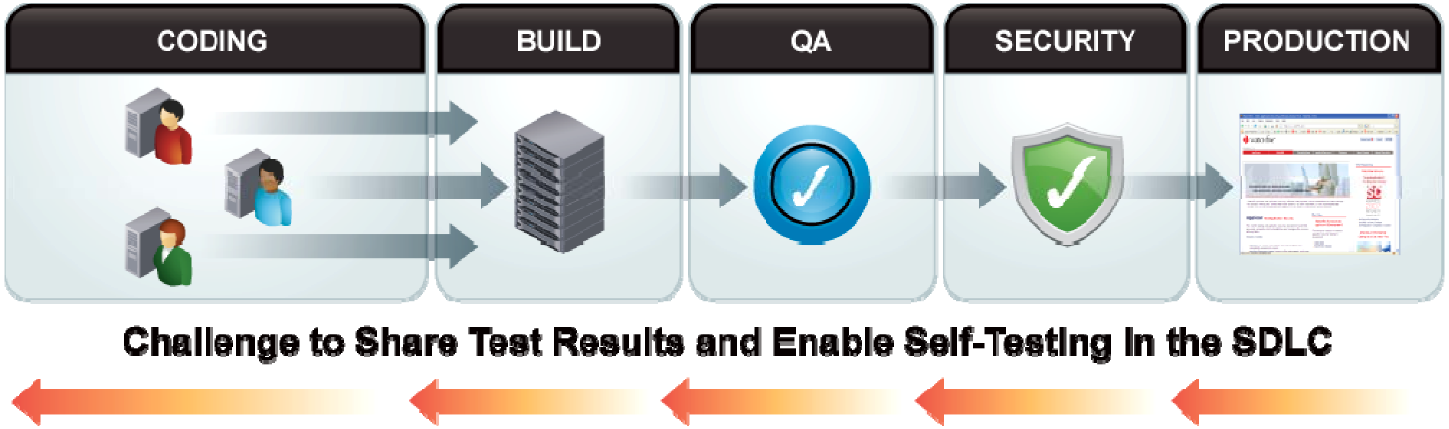
Developers Lack Security Insights

(or Incentives to Address Security)

- Mandate to deliver functionality on-time and on-budget – but not to develop secure applications
- Developers rarely educated in secure code practices
- Product innovation drives development of increasingly complicated applications

Security Team = SDLC Bottleneck

- Security tests executed just before launch
  - Adds time and cost to fix vulnerabilities late in the process
- Growing number of web applications but small security staff
  - Most enterprises scan ~10% of all applications
- Continuous monitoring of production apps limited or non-existent
  - Unidentified vulnerabilities & risk



Challenge to Share Test Results and Enable Self-Testing In the SDLC

Make applications secure, by design

Cycle of secure application development

Design

- Consider security requirements of the application & apply threat models
- Issues such as required controls and best practices are documented on par with functional requirements
- Secure code libraries maintained for reusable secure code

Development

- Create work items that map to security requirements
- Use secure code libraries
- Software is checked during coding for:
  - Implementation error vulnerabilities
  - Compliance with security requirements

Build & Test

- Map test plan to security requirements
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

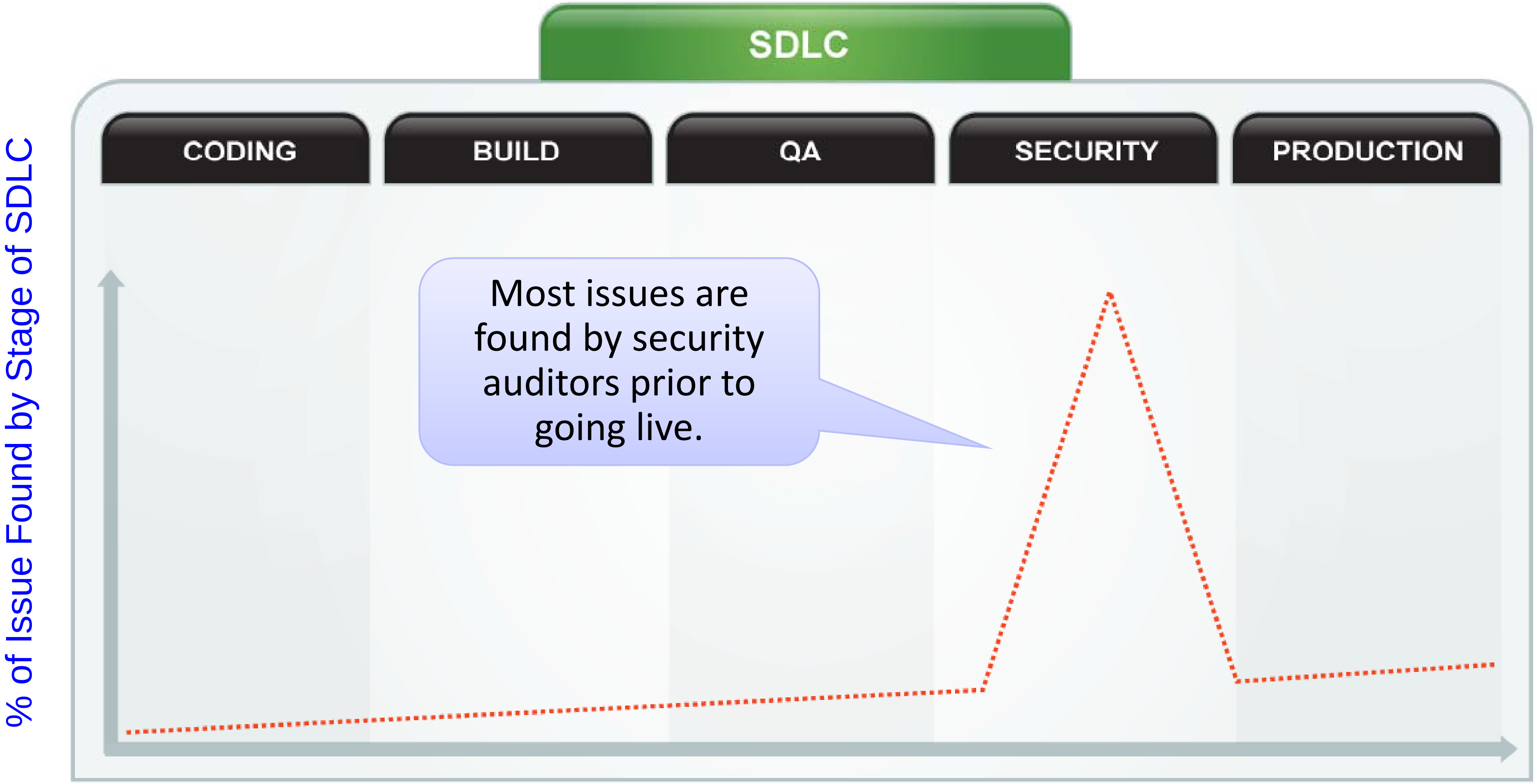
Deployment

- Configure infrastructure for application policies
- Deploy applications into production

Operational

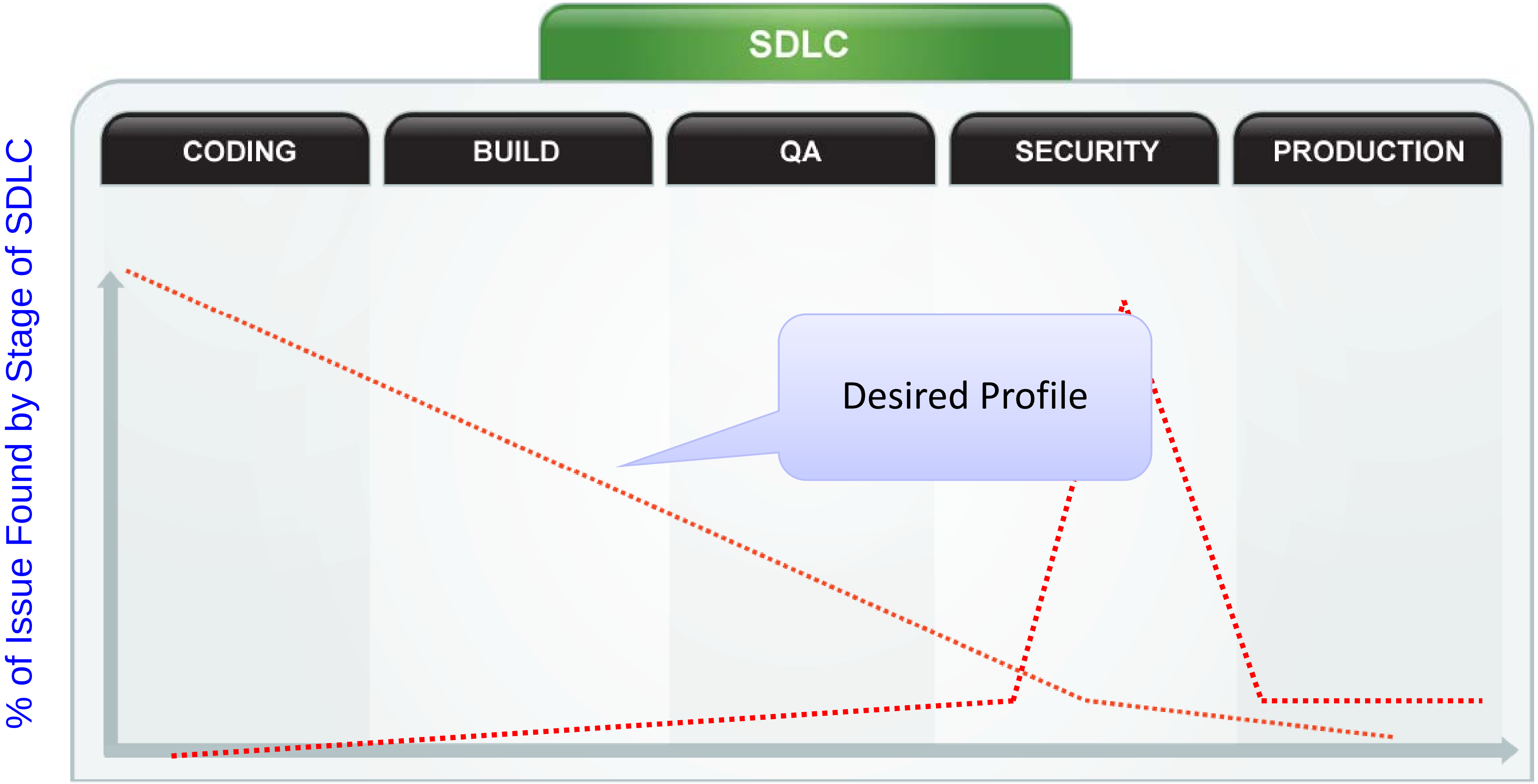
- Continuously monitor applications for appropriate application usage, vulnerabilities and defend against attacks

Security testing within the application life cycle



Most issues are found by security auditors prior to going live.

Security testing within the application life cycle



Pulse Comes to You 2012

Business without **LIMITS**

Cost is a significant driver

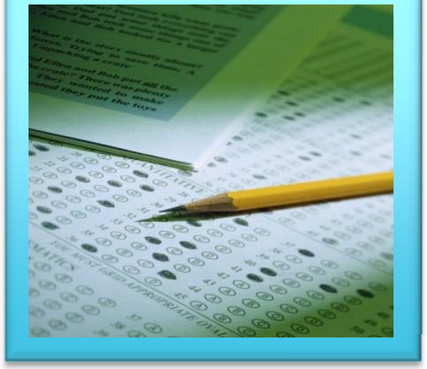
80% of development costs are spent identifying and correcting defects!*

During the CODING phase

$80/defect

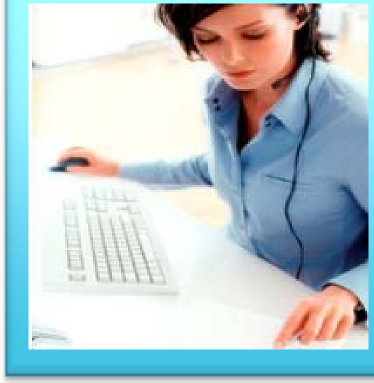
During the BUILD phase

$240/defect



During the QA/TESTING phase

$960/defect



Once released as a product

$7,600/defect

+

Law suits, loss of customer trust, damage to brand

*National Institute of Standards & Technology

Source: GBS Industry standard study

Defect cost derived in assuming it takes 8 hrs to find, fix and repair a defect when found in code and unit test. Defect FFR cost for other phases calculated by using the multiplier on a blended rate of $80/hr.

Solution requirements: advanced security testing + collaboration & governance through application lifecycle

Advanced Security Assessments

Dynamic Analysis

- Analysis of a running/ deployed application
- Key requirements
  - Threat coverage: WASC, OWASP Top 10, etc
  - Web Services/ SOA
  - Web 2.0 & Rich Internet Applications

Static Analysis

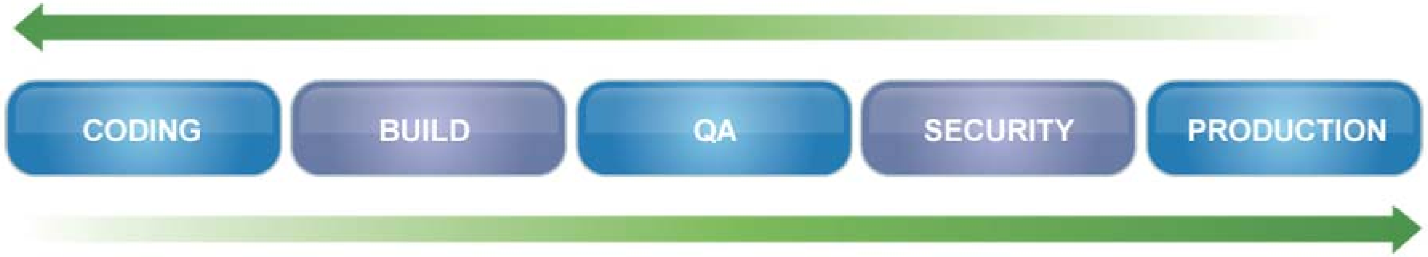
- Scanning source code for security issues
- Key requirements
  - Application/language support
  - Ease of use for non-security users (developers and build managers)

Runtime & Hybrid Analysis

- Glass box testing with runtime analysis
- Automated correlation of static & dynamic results
- Key requirements
  - Precise & Actionable results
  - Broad threat coverage

Collaboration & Governance in Application Lifecycle

Security testing, shared results, assign ownership



Track corrections and integrate with development systems

AppScan Standard

Web Application Assessments for Pen-Testers and Security Practitioners

Dynamic Analysis (black box)

- **Covers all relevant OWASP & WASC TCv2 threat classes**
  - SQL Injection
  - Cross-Site Scripting
  - HTTP Response Splitting
  - OS Commanding
  - LDAP Injection
  - XPath Injection
  - Buffer Overflows
  - ***1000s more***
- **Web 2.0 and Rich Internet Applications**
  - JavaScript & Ajax
  - Adobe Flash & Flex
- **Malware analysis**
  - Scan site with malware analysis from IBM X-Force Security Research
- **Web Services/ SOA**
  - SOAP/XML parser issues (External entities, XML blowup, etc.)
  - Application-layer issues
  - Infrastructure issues

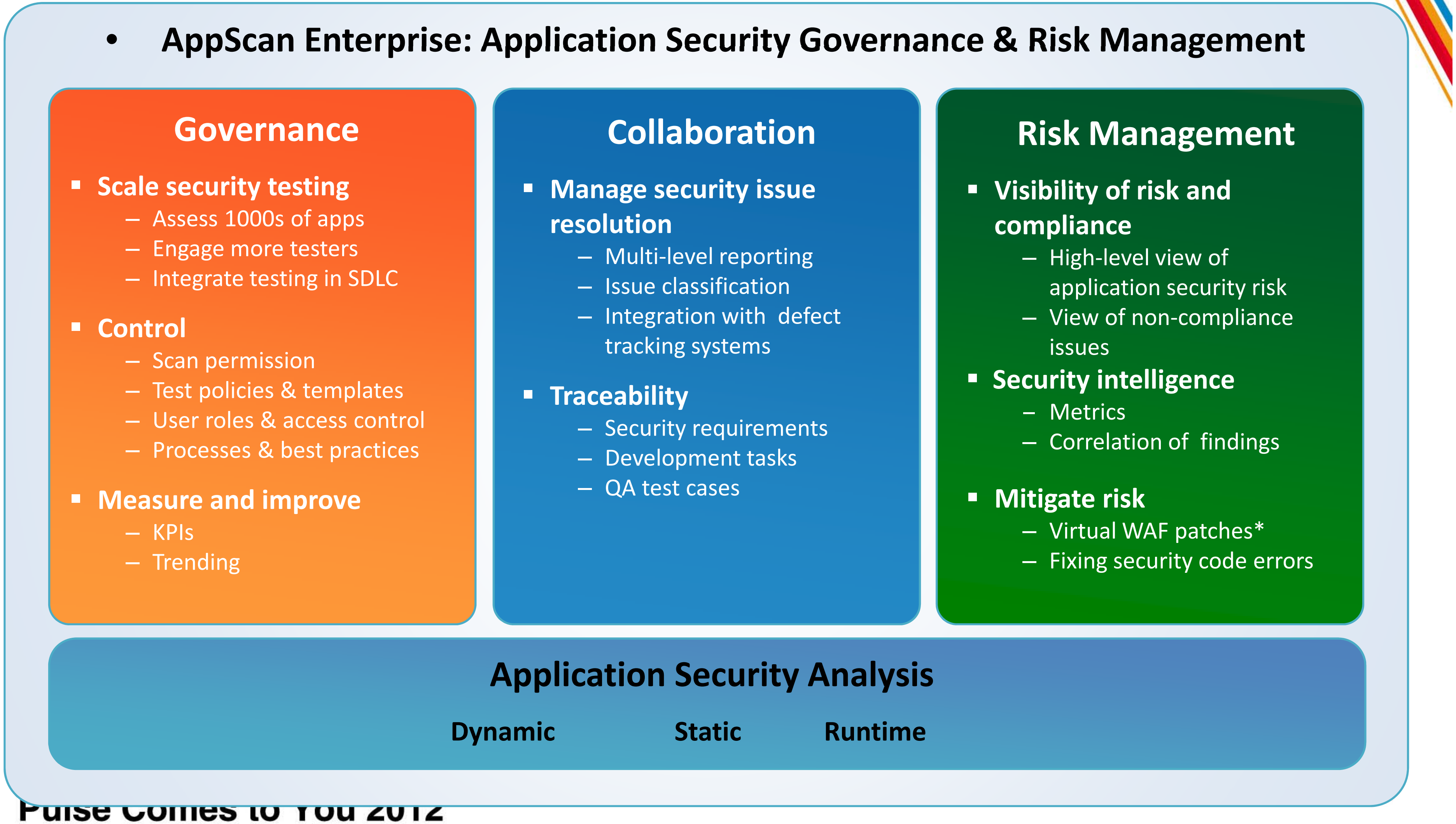
Hybrid Technology

- **Runtime Analysis (glass box testing)**
  - Expanded threat coverage with less configuration
  - Precise results (line of code) assist remediation
- **JavaScript Security Analyzer**
  - Static taint analysis of client-side JavaScript

Ease of Use

- **Configure & test**
  - Scan Expert provides recommended settings based on your apps
- **Details & guidance to correct the vulnerability**
  - Explanation of threat and recommended fix
- **Integrate with Defect Tracking Systems**
  - Rational® ClearQuest
  - HP Quality Center
- **Compliance & Reporting**
  - 40+ compliance reports
  - Executive-level summaries
  - Guidance for development

AppScan Enterprise



- AppScan Enterprise: Application Security Governance & Risk Management

Governance

- **Scale security testing**
  - Assess 1000s of apps
  - Engage more testers
  - Integrate testing in SDLC
- **Control**
  - Scan permission
  - Test policies & templates
  - User roles & access control
  - Processes & best practices
- **Measure and improve**
  - KPIs
  - Trending

Collaboration

- **Manage security issue resolution**
  - Multi-level reporting
  - Issue classification
  - Integration with defect tracking systems
- **Traceability**
  - Security requirements
  - Development tasks
  - QA test cases

Risk Management

- **Visibility of risk and compliance**
  - High-level view of application security risk
  - View of non-compliance issues
- **Security intelligence**
  - Metrics
  - Correlation of findings
- **Mitigate risk**
  - Virtual WAF patches*
  - Fixing security code errors

Application Security Analysis

Dynamic **Static** **Runtime**

AppScan Source

Source Code Analysis for Security Testing in Development & Build Automation

- ## Broad Application Support

Out of the Box for Security Testing

- Java
- JSP
- C
- C++
- Classic ASP (VB6)
- COBOL
- SAP ABAP*
- .NET
  - C#
  - VB.NET
  - ASP.NET
- PHP
- HTML
- Perl
- ColdFusion
- Client-Side JavaScript
- Server-Side JavaScript
- VBScript
- PL/SQL
- T-SQL

Code Quality Static Analysis

- Identify code-level quality defects within IDE
- Automate code quality analysis as part of the build process for centralized software code scanning
- Key Performance Indicators (KPIs) to help developers learn best practices
- Languages: Java, C, C++

Application Lifecycle Integrations

- **Develop**
  - IDE plug-ins to remediate identified issues (*Source for Remediation*)
  - Options to scan code locally from IDE (*Source for Developer*)
- **Build**
  - Automatically trigger security scans with each build (*Source for Automation*)
  - Review results from IDE or Security user & create work items for remediation
- **Security**
  - *Source for Security* power user creates SAST scans executed from IDE or in build automation
  - Executes advanced scans in pre-production security audits

* Requires Virtual Forge CodeProfiler for AppScan Source Edition

How does Rational AppScan work?

Automates Application Security Testing

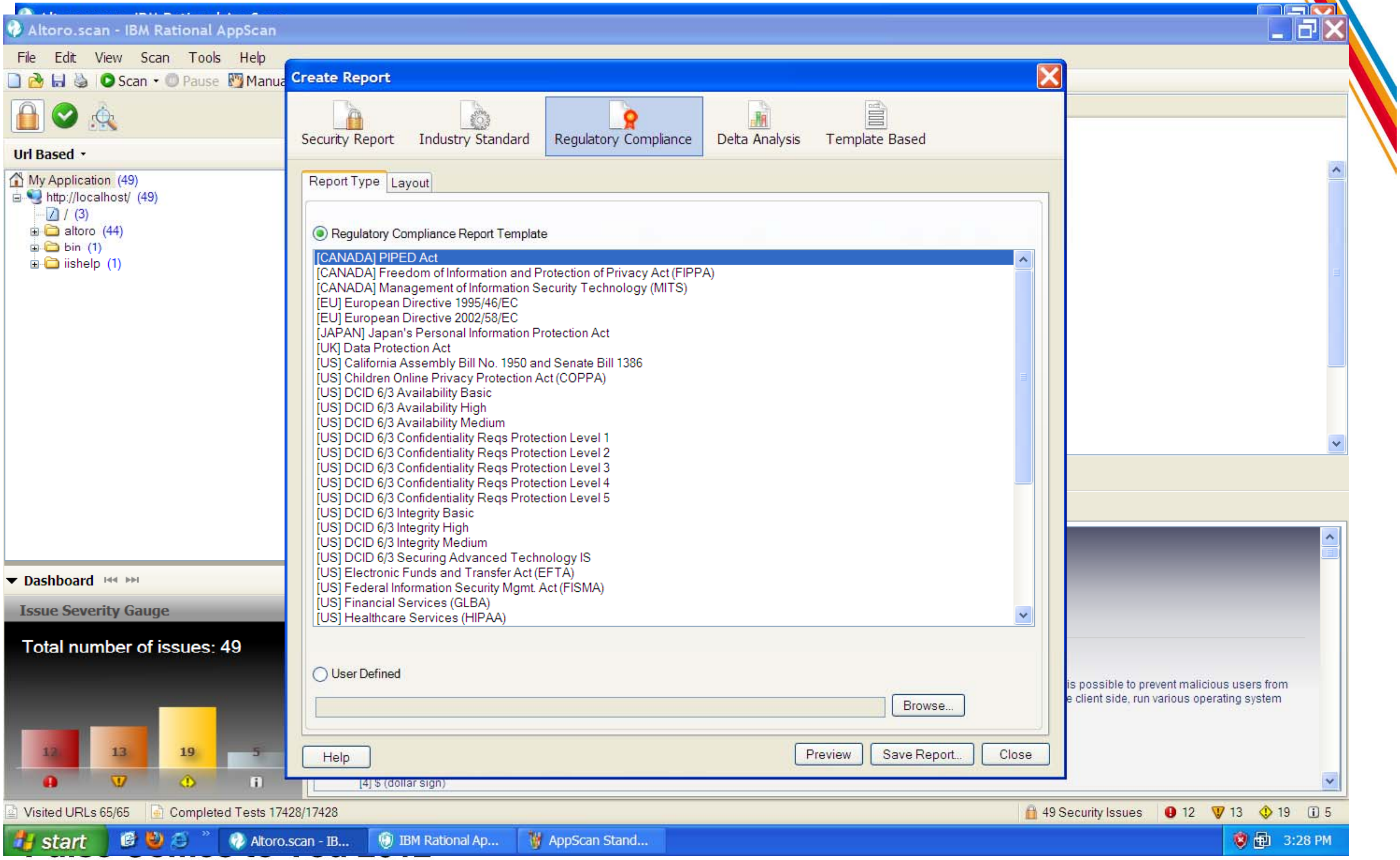
Same process for whitebox & blackbox

Scan applications

Analyze
(identify issues)

Report
(detailed & actionable)

AppScan - Dynamic Assessment



Total number of issues: 49

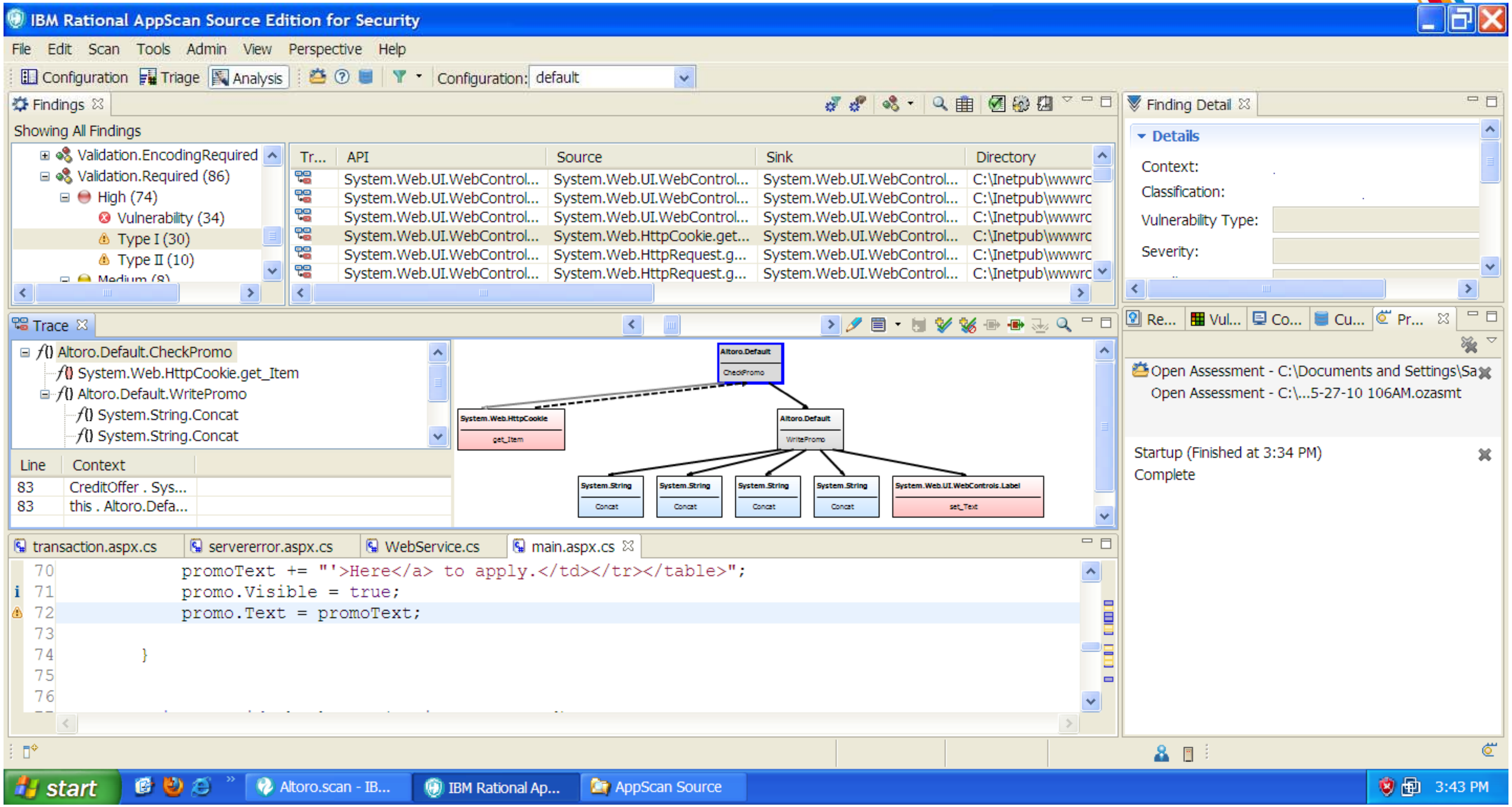
● Regulatory Compliance Report Template

[CANADA] PIPED Act
[CANADA] Freedom of Information and Protection of Privacy Act (FIPPA)
[CANADA] Management of Information Security Technology (MITS)
[EU] European Directive 1995/46/EC
[EU] European Directive 2002/58/EC
[JAPAN] Japan's Personal Information Protection Act
[UK] Data Protection Act
[US] California Assembly Bill No. 1950 and Senate Bill 1386
[US] Children Online Privacy Protection Act (COPPA)
[US] DCID 6/3 Availability Basic
[US] DCID 6/3 Availability High
[US] DCID 6/3 Availability Medium
[US] DCID 6/3 Confidentiality Reqs Protection Level 1
[US] DCID 6/3 Confidentiality Reqs Protection Level 2
[US] DCID 6/3 Confidentiality Reqs Protection Level 3
[US] DCID 6/3 Confidentiality Reqs Protection Level 4
[US] DCID 6/3 Confidentiality Reqs Protection Level 5
[US] DCID 6/3 Integrity Basic
[US] DCID 6/3 Integrity High
[US] DCID 6/3 Integrity Medium
[US] DCID 6/3 Securing Advanced Technology IS
[US] Electronic Funds and Transfer Act (EFTA)
[US] Federal Information Security Mgmt. Act (FISMA)
[US] Financial Services (GLBA)
[US] Healthcare Services (HIPAA)

○ User Defined

is possible to prevent malicious users from
e client side, run various operating system

AppScan - Static Assessment



Showing All Findings

- Validation.EncodingRequired
- Validation.Required (86)
  - High (74)
    - Vulnerability (34)
    - Type I (30)
    - Type II (10)
  - Medium (8)

Tr...	API	Source	Sink	Directory
	System.Web.UI.WebControl...	System.Web.UI.WebControl...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc
	System.Web.UI.WebControl...	System.Web.UI.WebControl...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc
	System.Web.UI.WebControl...	System.Web.UI.WebControl...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc
	System.Web.UI.WebControl...	System.Web.HttpCookie.get...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc
	System.Web.UI.WebControl...	System.Web.HttpRequest.g...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc
	System.Web.UI.WebControl...	System.Web.HttpRequest.g...	System.Web.UI.WebControl...	C:\Inetpub\wwwrc

Details

Context:

Classification:

Vulnerability Type:

Severity:

- f() Altoro.Default.CheckPromo
  - f() System.Web.HttpCookie.get_Item
  - f() Altoro.Default.WritePromo
    - f() System.String.Concat
    - f() System.String.Concat

Line	Context
83	CreditOffer . Sys...
83	this . Altoro.Defa...

```
            promoText += "'>Here</a> to apply.</td></tr></table>";
            promo.Visible = true;
            promo.Text = promoText;

        }
```

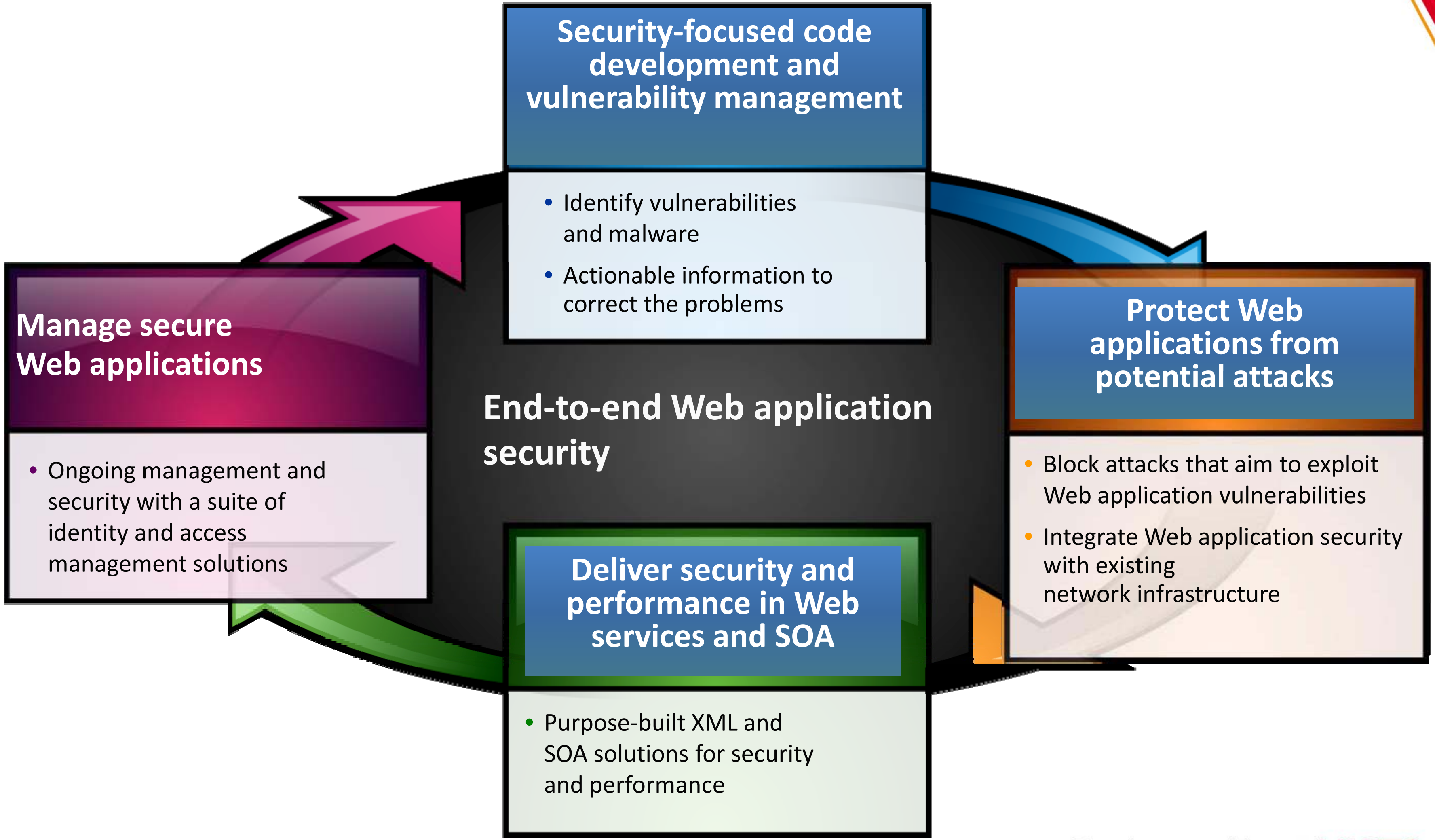
Open Assessment - C:\Documents and Settings\Sa
Open Assessment - C:\...5-27-10 106AM.ozasmt

Startup (Finished at 3:34 PM)
Complete

Business without **LIMITS**

Pulse Comes to You 2012

Protecting Deployed Applications in Real-time



Security-focused code development and vulnerability management

- Identify vulnerabilities and malware
- Actionable information to correct the problems

Protect Web applications from potential attacks

- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

Deliver security and performance in Web services and SOA

- Purpose-built XML and SOA solutions for security and performance

Manage secure Web applications

- Ongoing management and security with a suite of identity and access management solutions

End-to-end Web application security

Maintaining High Levels of Pre-emptive Protection

IBM X-Force®
Research and Development Team

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities/Exploits
- Malicious/Unwanted websites
- Spam and Phishing
- Malware
- Other emerging trends

IBM Security Network Intrusion Prevention System

Beyond traditional network IPS to deliver comprehensive security including:

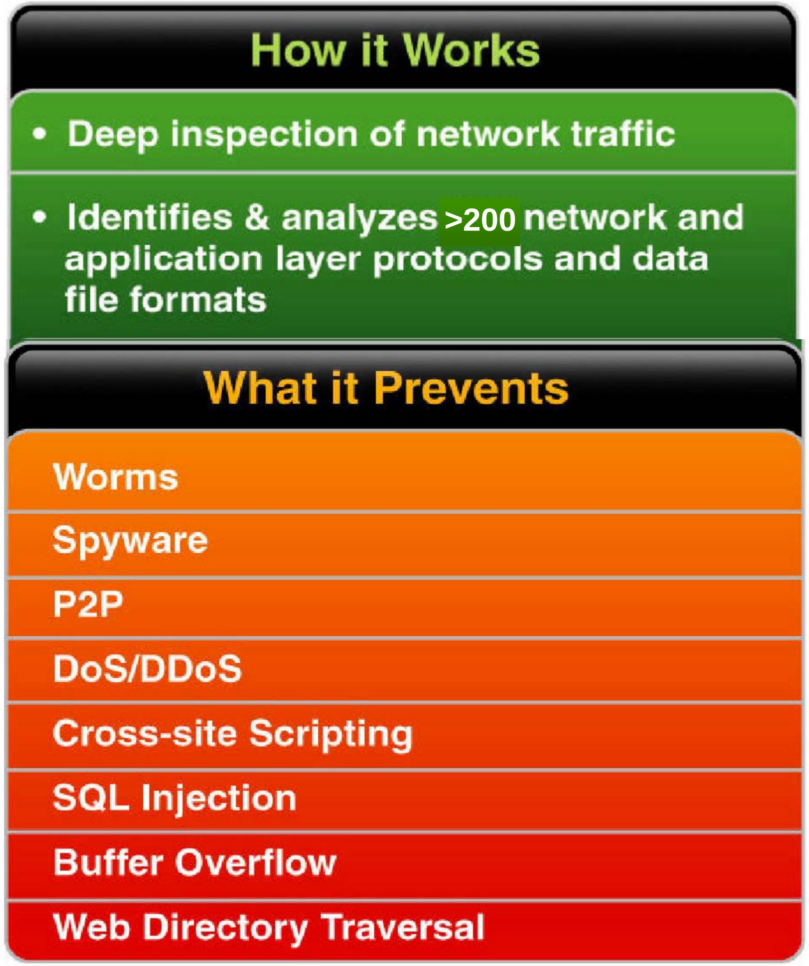
- Web application protection
- Protection from client-side attacks
- Data Loss Prevention (DLP)
- Granular policy control for virtual environments
- Application control
- Virtual Patch technology

Unmatched Performance through PAM 2.0 delivering 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

Evolving protection powered by world renowned X-Force research to stay “ahead of the threat”

Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

Evolving Security: The Protocol Analysis Module

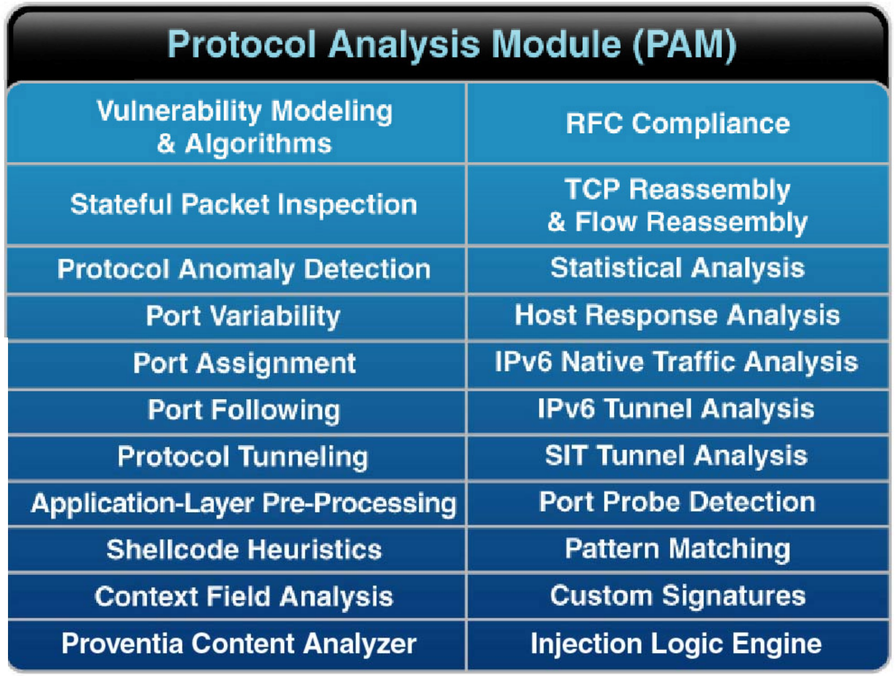


How it Works

- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal



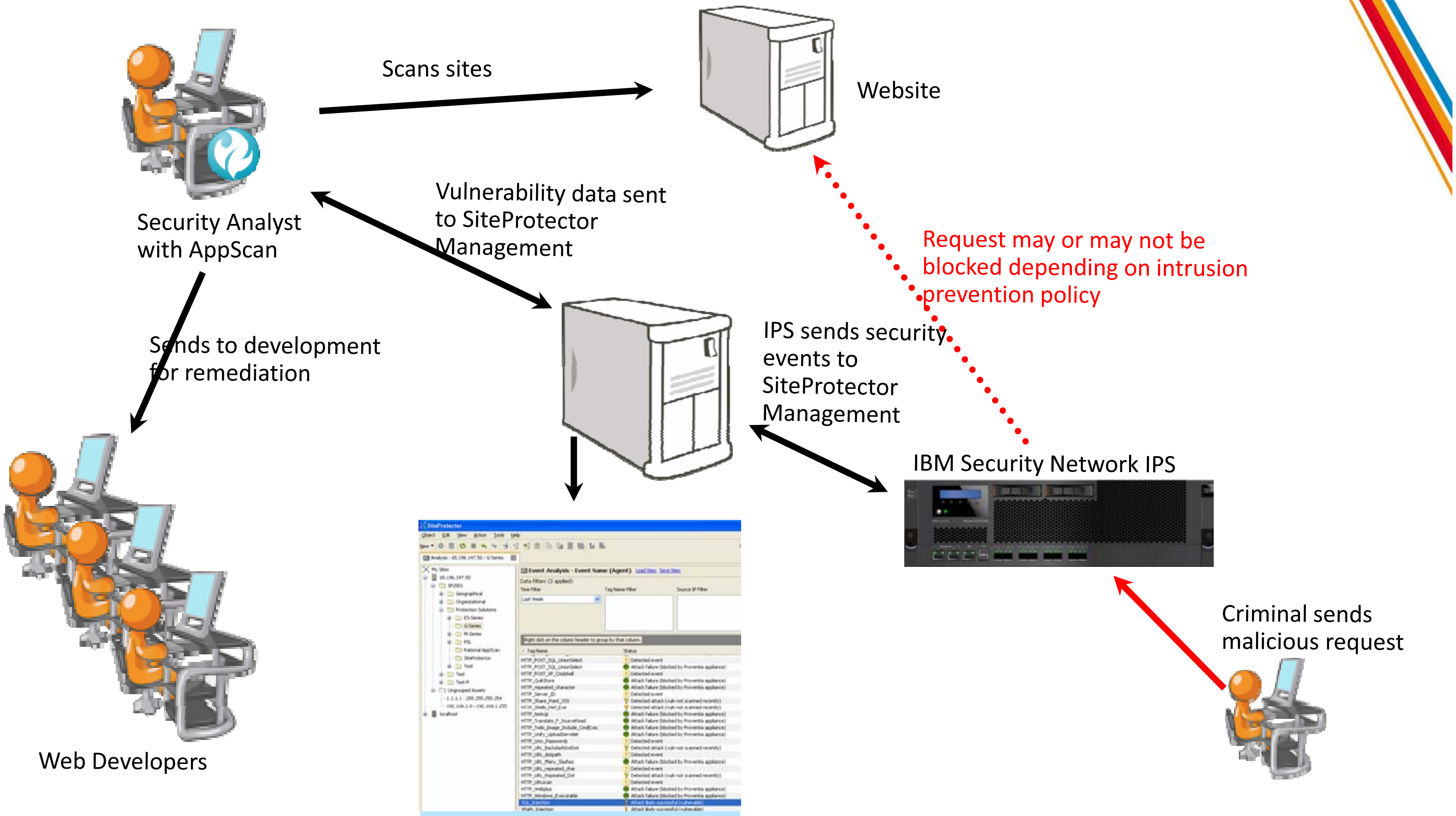
Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

NEW - Introducing PAM 2.0

- Takes advantage of next generation hardware
- Provides multi-threaded security inspection
- Delivers unprecedented levels of performance without compromising security

Integrating Application Vulnerability Scanning and IPS



Security Analyst with AppScan

Scans sites

Website

Vulnerability data sent to SiteProtector Management

Sends to development for remediation

Web Developers

IPS sends security events to SiteProtector Management

Request may or may not be blocked depending on intrusion prevention policy

IBM Security Network IPS

Criminal sends malicious request

SiteProtector

Object Edit View Action Tools Help

Analysis : 65.196.147.50 : G-Series

- My Sites
  - 65.196.147.50
    - SP2001
      - Geographical
      - Organizational
      - Protection Solutions
        - ES-Series
        - G-Series
        - M-Series
        - PSL
        - Rational AppScan
        - SiteProtector
        - Test
      - Test
      - Test-P
    - Ungrouped Assets
      - 1.1.1.1 - 255.255.255.254
      - 192.168.1.0 - 192.168.1.255
  - localhost

Event Analysis - Event Name (Agent) Load View Save View

Data Filters (3 applied)

Time Filter: Last Week

Tag Name Filter

Source IP Filter

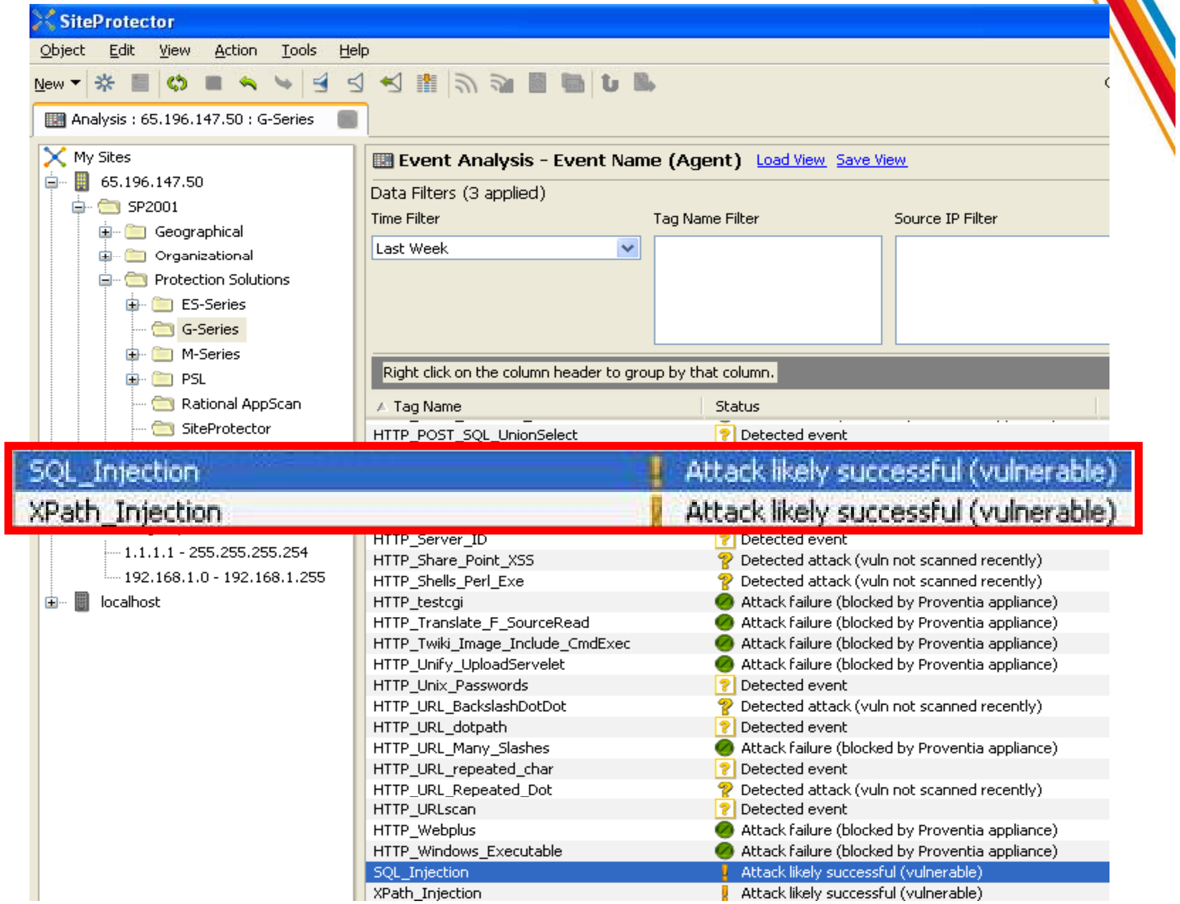
Right click on the column header to group by that column.

Tag Name	Status
HTTP_POST_SQL_UnionSelect	Detected event
HTTP_POST_SQL_UnionSelect	Attack Failure (blocked by Proventia appliance)
HTTP_POST_XP_Cmdshell	Detected event
HTTP_QuikStore	Attack Failure (blocked by Proventia appliance)
HTTP_repeated_character	Attack Failure (blocked by Proventia appliance)
HTTP_Server_ID	Detected event
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)
HTTP_testcgi	Attack Failure (blocked by Proventia appliance)
HTTP_Translate_F_SourceRead	Attack Failure (blocked by Proventia appliance)
HTTP_Twiki_Image_Include_CmdExec	Attack Failure (blocked by Proventia appliance)
HTTP_Unify_UploadServelet	Attack Failure (blocked by Proventia appliance)
HTTP_Unix_Passwords	Detected event
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)
HTTP_URL_dotpath	Detected event
HTTP_URL_Many_Slashes	Attack Failure (blocked by Proventia appliance)
HTTP_URL_repeated_char	Detected event
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)
HTTP_URLscan	Detected event
HTTP_Webplus	Attack Failure (blocked by Proventia appliance)
HTTP_Windows_Executable	Attack Failure (blocked by Proventia appliance)
SQL_Injection	Attack likely successful (vulnerable)
XPath_Injection	Attack likely successful (vulnerable)

AppScan vulnerability data is correlated with IPS attack data

A More Intelligent Approach to Web Application Security

- Correlates vulnerability data with actual attacks
- Understand which attacks have a high probability of success
- Increased insight helps in tuning IPS Web protection module
- Prioritize vulnerability remediation efforts based exposure



Data Filters (3 applied)

Time Filter

Last Week

Tag Name Filter

Source IP Filter

Right click on the column header to group by that column.

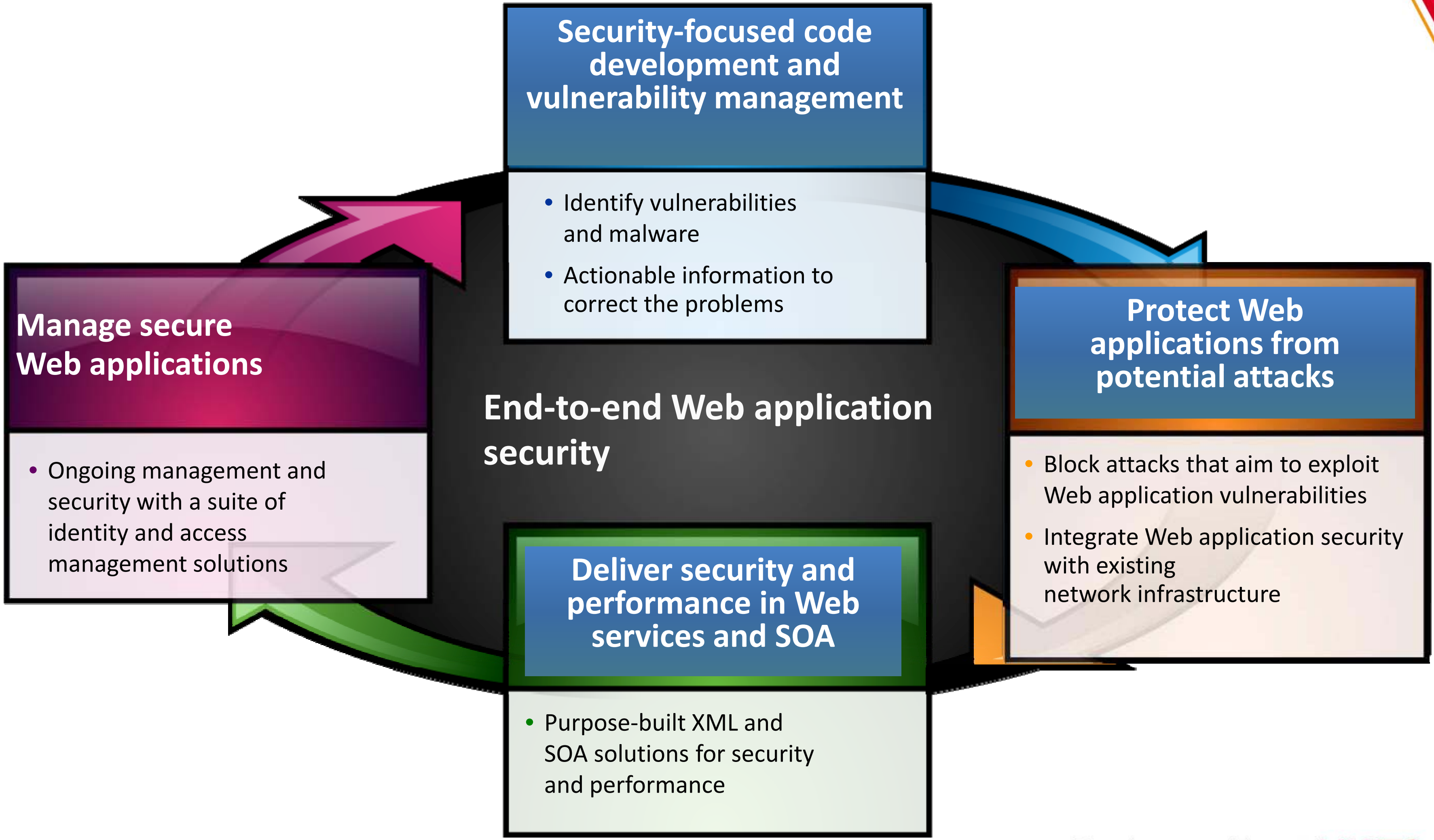
Tag Name	Status
HTTP_POST_SQL_UnionSelect	? Detected event
HTTP_Server_ID	? Detected event
HTTP_Share_Point_XSS	? Detected attack (vuln not scanned recently)
HTTP_Shells_Perl_Exe	? Detected attack (vuln not scanned recently)
HTTP_testcgi	● Attack failure (blocked by Proventia appliance)
HTTP_Translate_F_SourceRead	● Attack failure (blocked by Proventia appliance)
HTTP_Twiki_Image_Include_CmdExec	● Attack failure (blocked by Proventia appliance)
HTTP_Unify_UploadServelet	● Attack failure (blocked by Proventia appliance)
HTTP_Unix_Passwords	? Detected event
HTTP_URL_BackslashDotDot	? Detected attack (vuln not scanned recently)
HTTP_URL_dotpath	? Detected event
HTTP_URL_Many_Slashes	● Attack failure (blocked by Proventia appliance)
HTTP_URL_repeated_char	? Detected event
HTTP_URL_Repeated_Dot	? Detected attack (vuln not scanned recently)
HTTP_URLscan	? Detected event
HTTP_Webplus	● Attack failure (blocked by Proventia appliance)
HTTP_Windows_Executable	● Attack failure (blocked by Proventia appliance)
SQL_Injection	! Attack likely successful (vulnerable)
XPath_Injection	! Attack likely successful (vulnerable)

SQL_Injection ! Attack likely successful (vulnerable)
XPath_Injection ! Attack likely successful (vulnerable)

Pulse Comes to You 2012

Business without **LIMITS**

Putting the Pieces Together for End-to-End Application Security



Security-focused code development and vulnerability management

- Identify vulnerabilities and malware
- Actionable information to correct the problems

Protect Web applications from potential attacks

- Block attacks that aim to exploit Web application vulnerabilities
- Integrate Web application security with existing network infrastructure

Deliver security and performance in Web services and SOA

- Purpose-built XML and SOA solutions for security and performance

Manage secure Web applications

- Ongoing management and security with a suite of identity and access management solutions

End-to-end Web application security

Pulse Comes to You 2012

Business without **LIMITS**

Thank You