Driving Effective Application Security in the Enterprise: An End-to-End Approach to Addressing One of the Biggest Threats to a Business

Steven "Schmidtty" Schmidt
Application Security Technical Specialist
IBM Security Systems

Pulse2012

Meet the Experts. Optimise your infrastructure.

May 31 – June1

Sheraton on the Park Hotel, Sydney

The Smarter Planet

Challenges we face on a smarter planet

Key drivers for security projects

Increasing Complexity

Soon, there will be **1 trillion** connected devices in the world, constituting an "internet of things"

Rising Costs

Spending by U.S. companies on governance, risk and compliance will grow to **$29.8 billion** in 2010

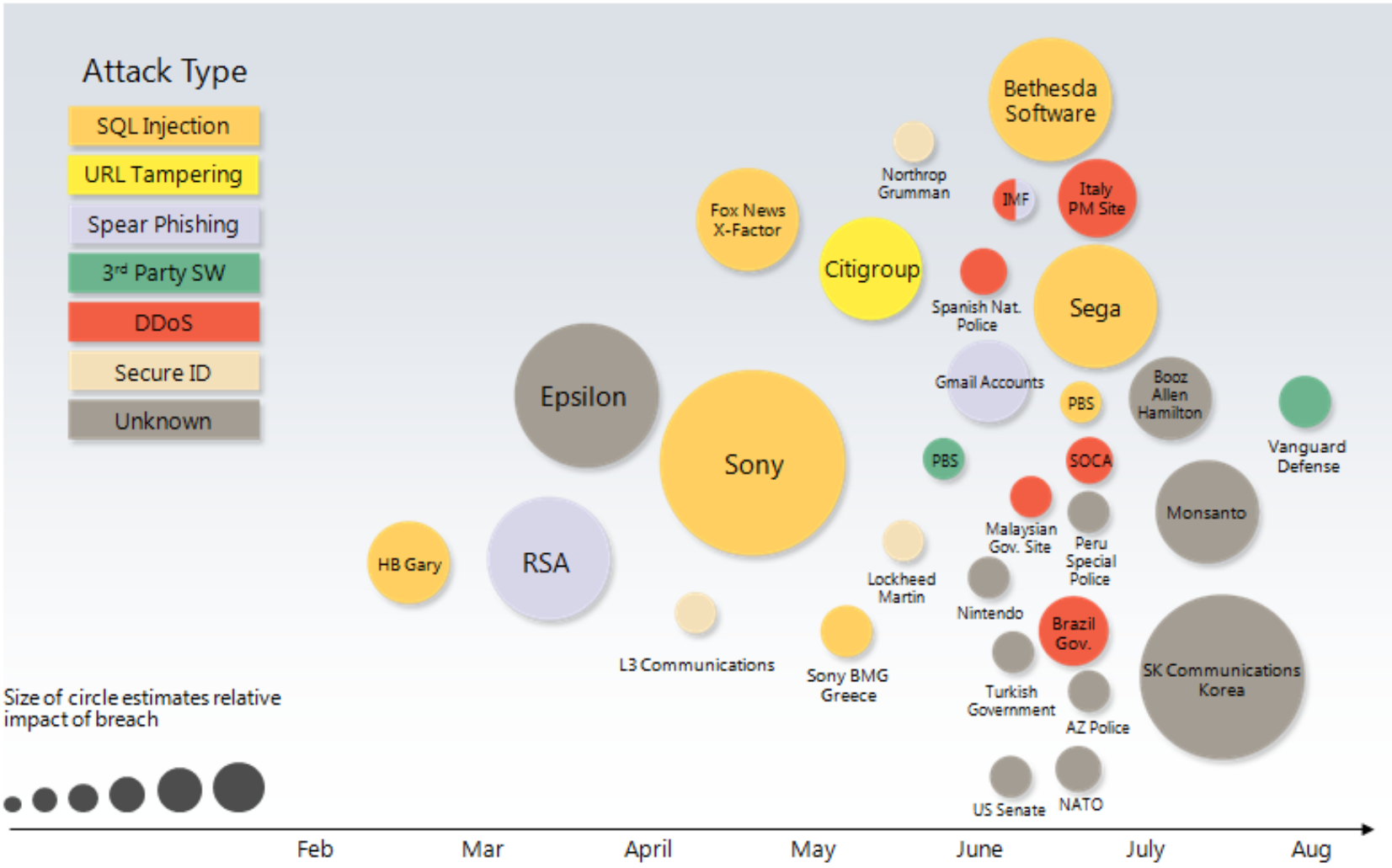
Ensuring Compliance

The cost of a data breach increased to **$214** per compromised customer record

Source ***http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html***

Story Time!

Targeted Attacks Shake Businesses and Governments

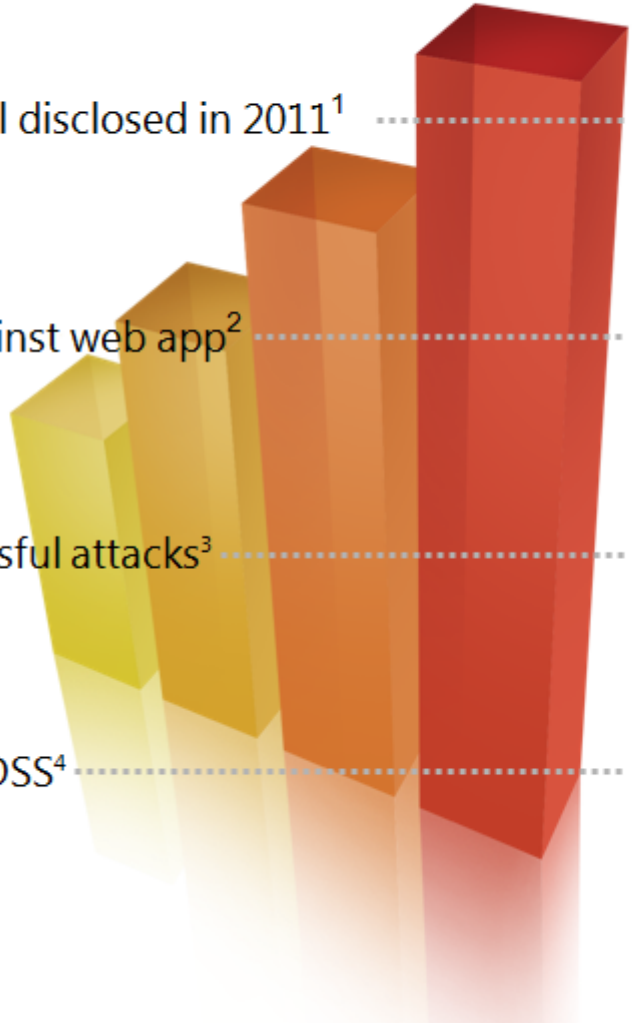


IBM Security X-Force® 2011 Midyear Trend and Risk Report September 2011

Web Application Vulnerabilities are still the greatest source of risk for organizations

IBM

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

Application Security Market Drivers

- **Regulatory & Standards Compliance**
  - eCommerce: PCI-DSS, PA-DSS
  - Financial Services: GLBA
  - Energy: NERC / FERC
  - Government: FISMA
- **User demand Increasing Risk**
  - Transformation of business processes to web applications & services
  - Rich application demand is pushing development to advanced code techniques – Web 2.0 introducing more exposures
- **Cost efficiencies**
  - Mitigate organizational risk with positive return on investment

"As attackers identify new ways to gain access to sensitive data, managing application security has become a big problem for our clients, and companies need solutions to proactively identify and fix vulnerabilities in their applications and comply with more and more regulations,"

Joey Peloquin, Director, Application Security, Fishnet Security.

Why Are Applications So Vulnerable?

Time to market, priorities

Lack of security education

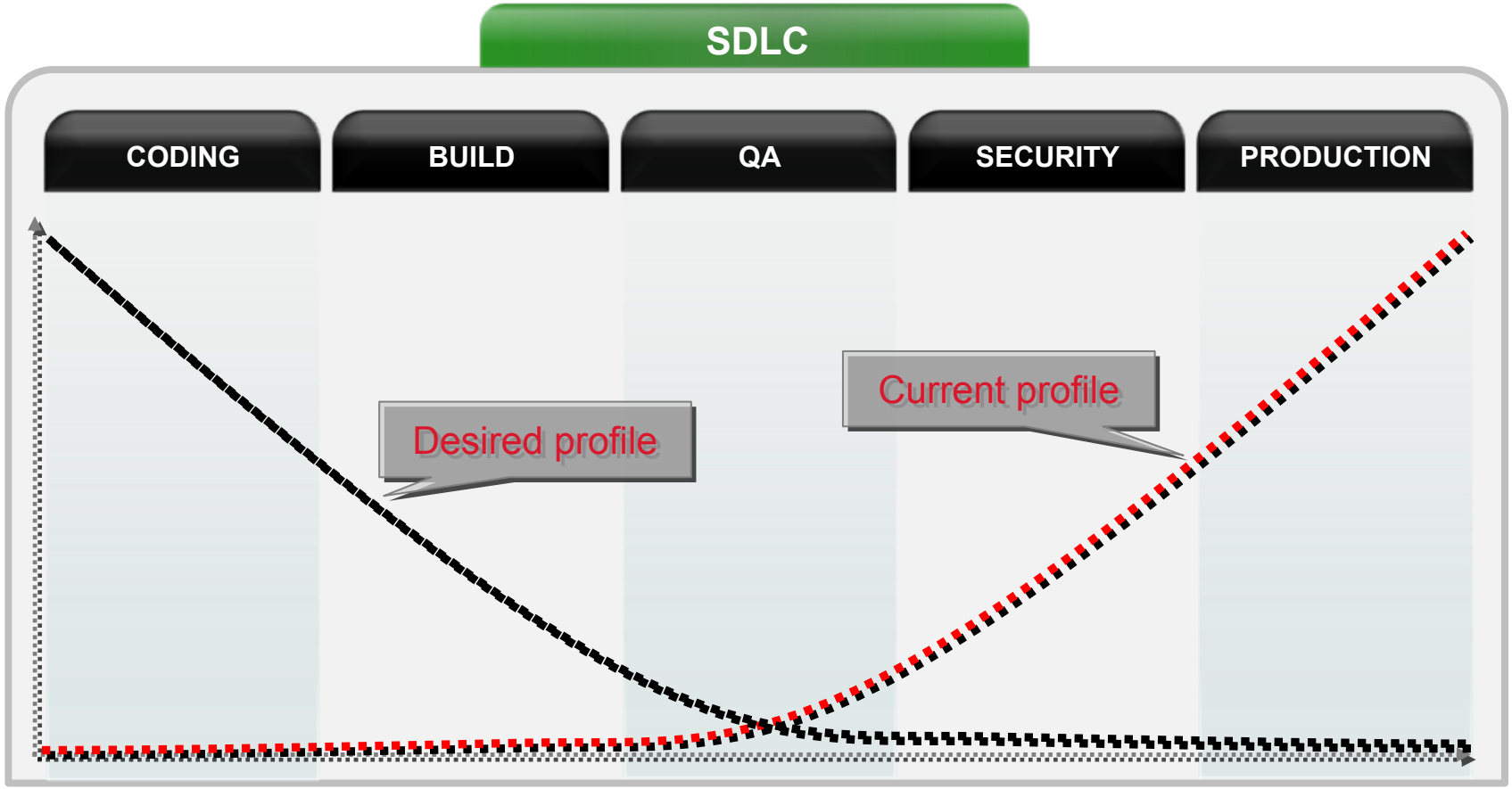
Complexity

Interconnectivity

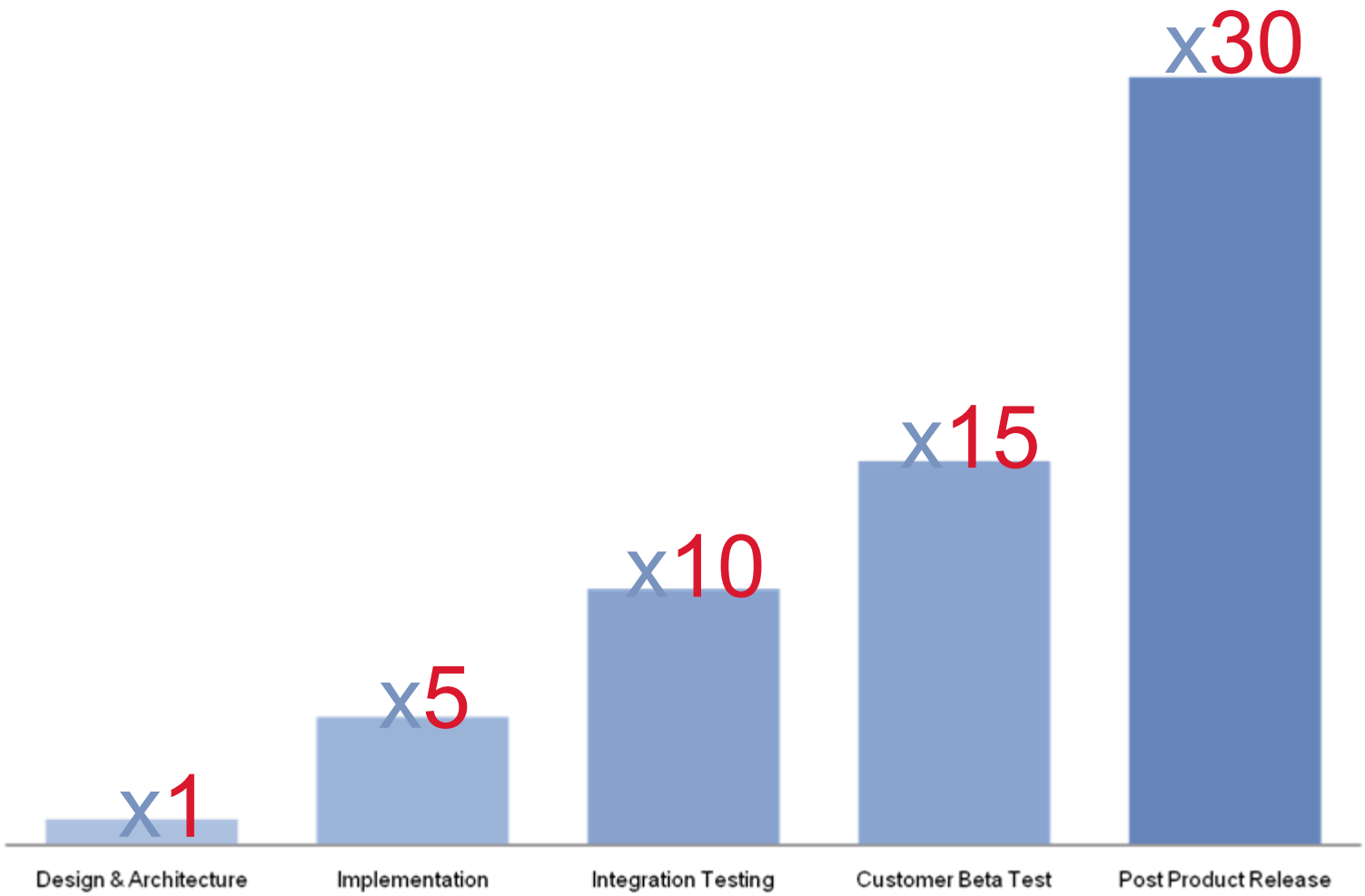
Network protections are not enough

More Story Time!

Security Testing Within the App Lifecycle

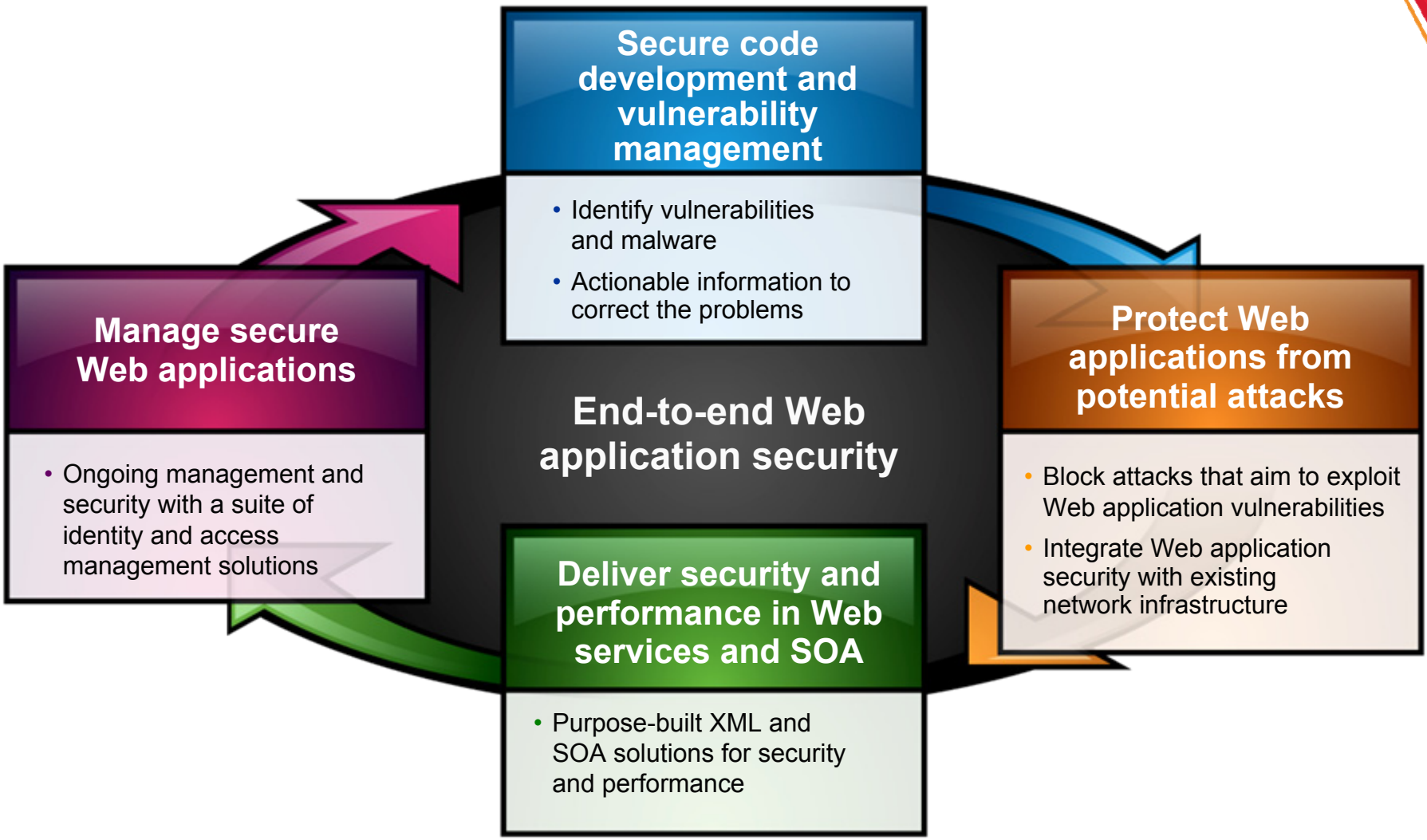


Cost of fixing software defects: The Artist formerly known as Security Issues



The Economic Impacts of Inadequate Infrastructure for Software Testing (NIST, 2002)

Application Safety – Protect Valuable Assets



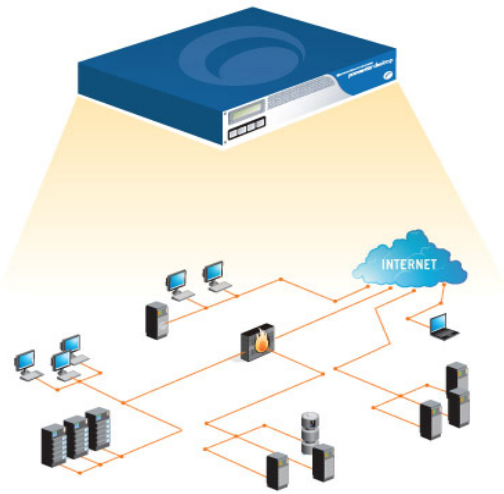
How does IBM Security AppScan work?

Automates Application Security Testing

Same process for whitebox & blackbox

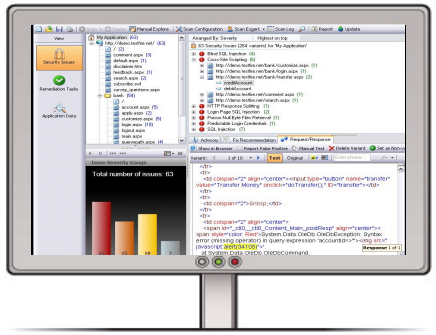
1 → 2 → 3

Scan applications



Analyze

(identify issues)



Virtual-SOC Portal

Report

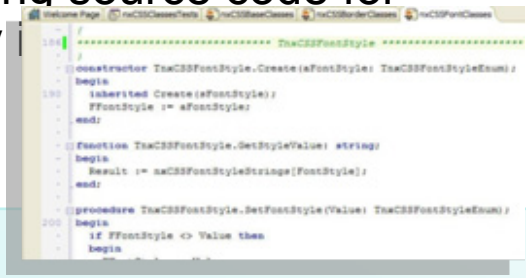
(detailed & actionable)

Security Testing Technologies...

Combination Drives Greater Solution Accuracy

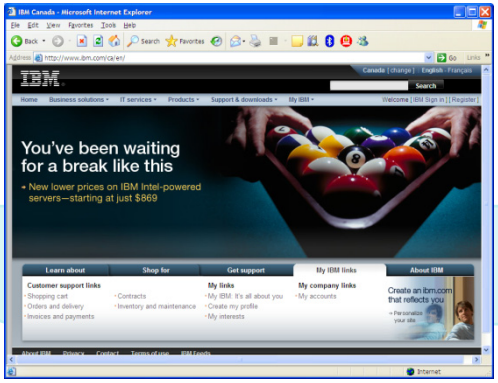
Static Code Analysis (Whitebox)

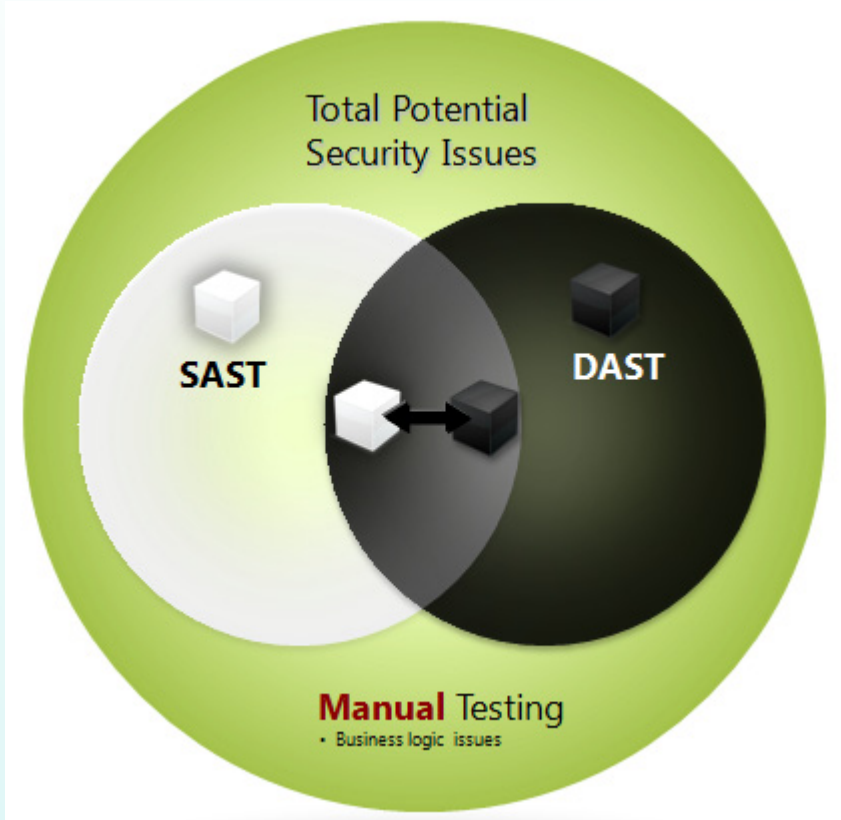
•Scanning source code for security i



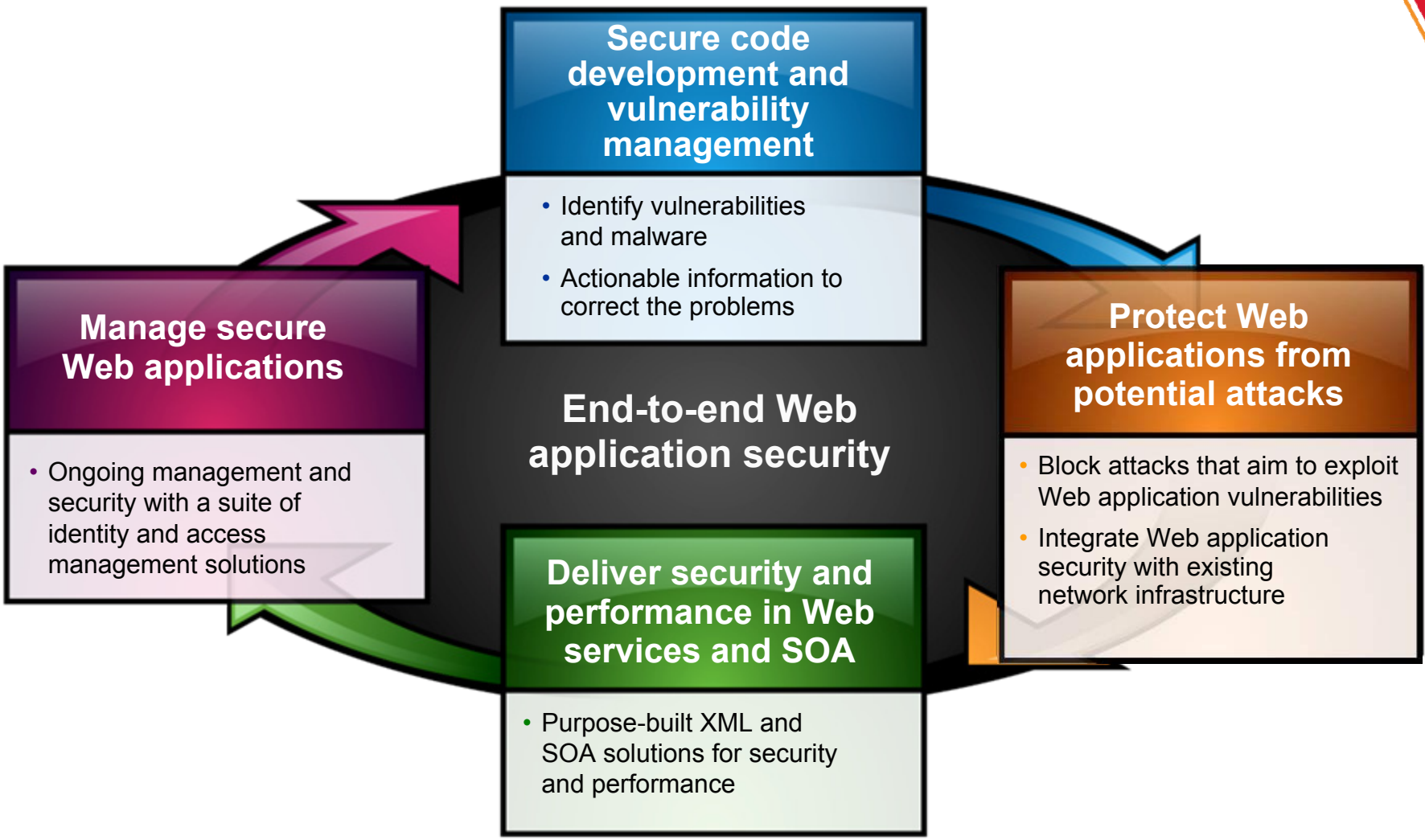
Dynamic Analysis (Blackbox)

▪Performing security analysis of a compiled application





Protecting Deployed Applications in Real-time



Yep, another story…

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

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

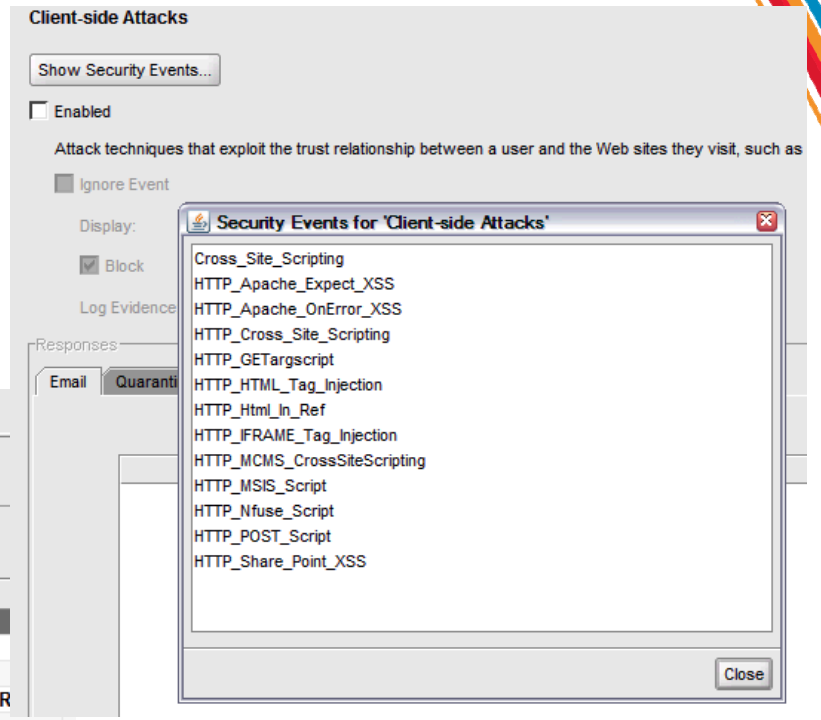
Millions of unique malware samples

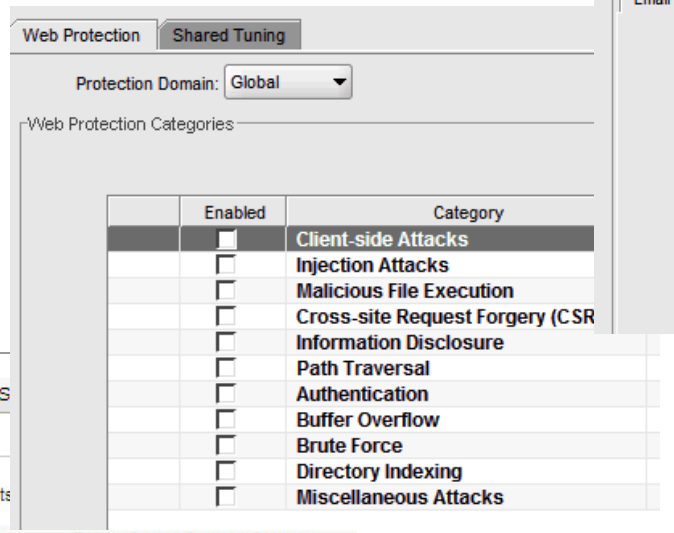
Provides Specific Analysis of:

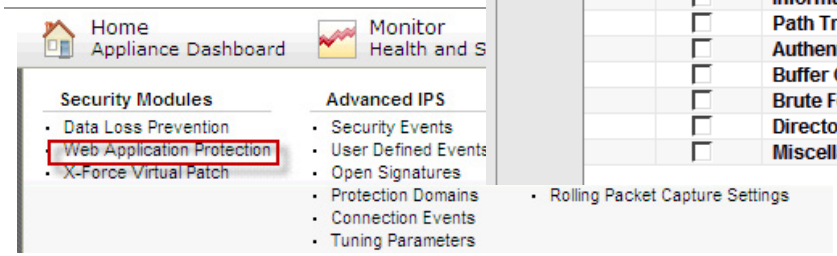
- Vulnerabilities/Exploits
- Malicious/Unwanted websites
- Spam and Phishing
- Malware
- Other emerging trends

A Look at IBM's Web Protection Module

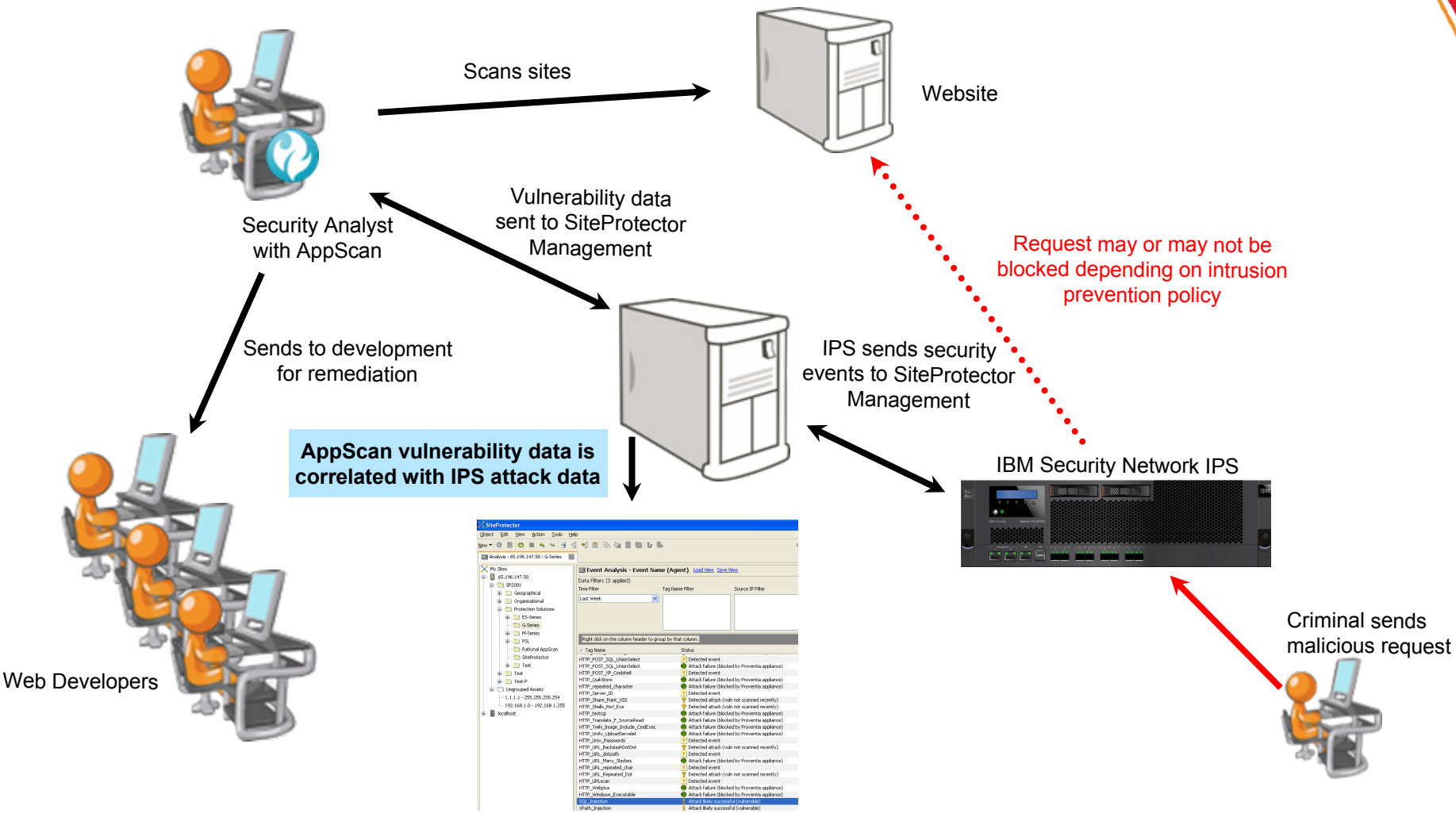
- Detects/blocks wide range of Web application attacks
- Critical such as SQL Injection and Cross-site Scripting/CSRF
- Path Traversal, Brute Force, and many more





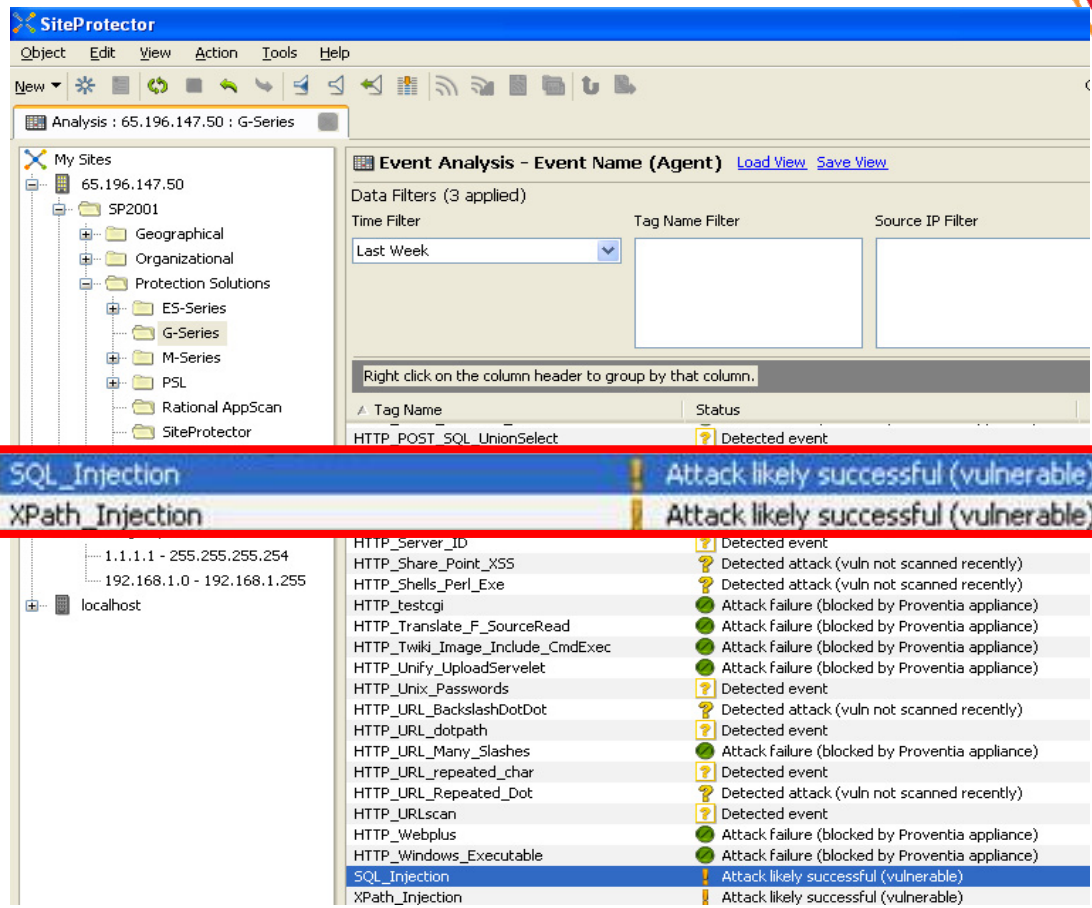


Integrating Vulnerability Scanning and IPS

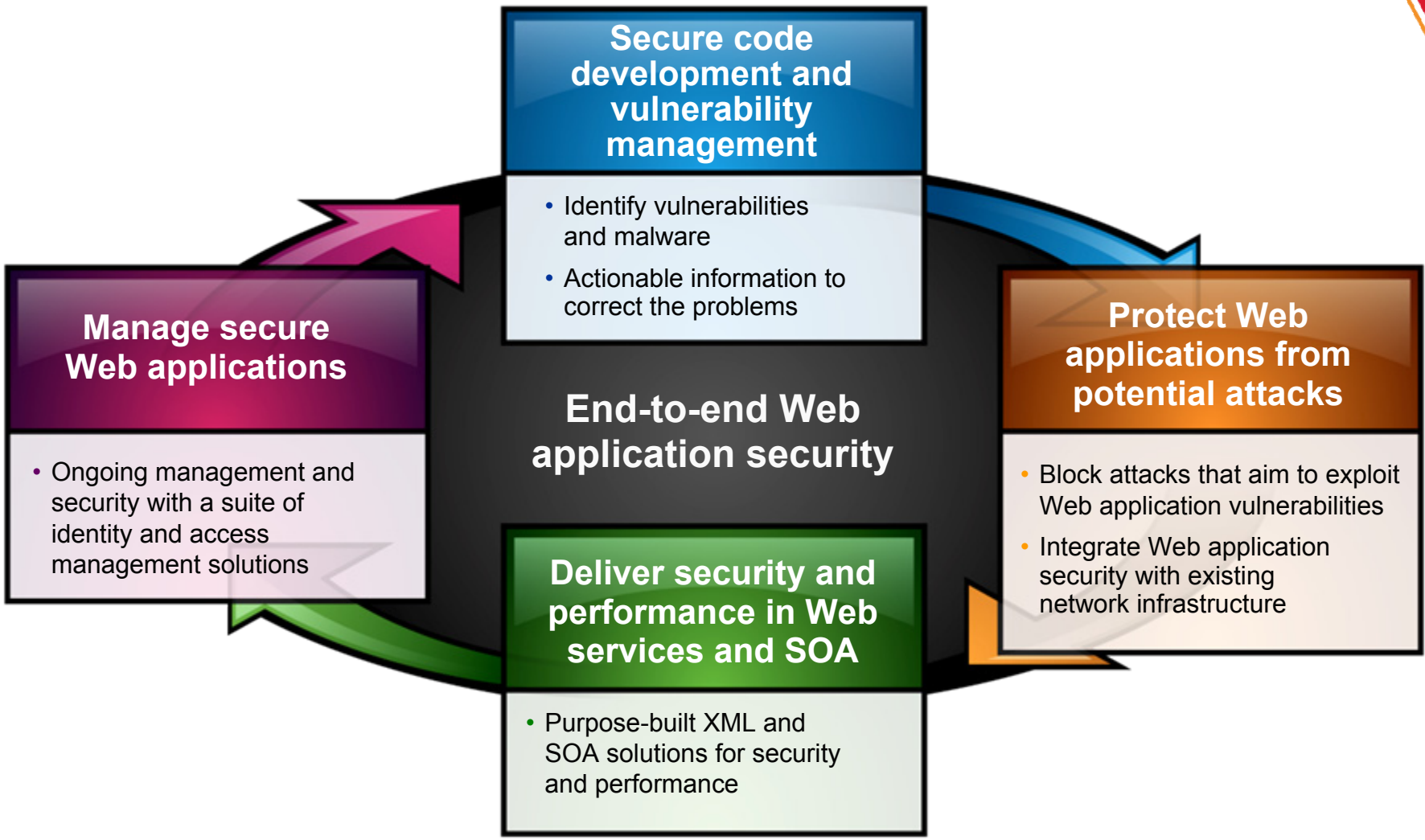


More Intelligent Insight into Web Application Threats

- 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



IBM can Help Protect your Valuable Assets



www.ibm.com/security

Acknowledgements, disclaimers and trademarks

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.