Application Security –
Security through the complete SDLC process

Keith Pope, North East IOT, IBM (AppScan)

IBM Software

PCTY2010

Pulse Comes to You

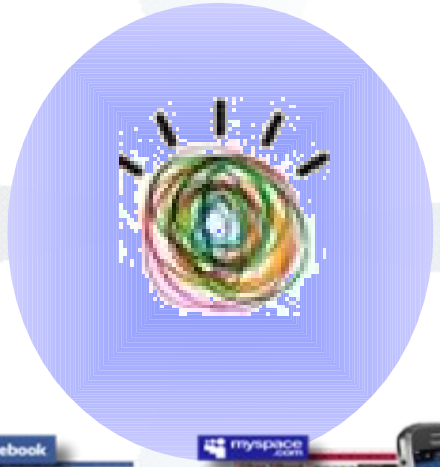
Optimising the World's Infrastructure

[27 May, London]

The Smarter Planet

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



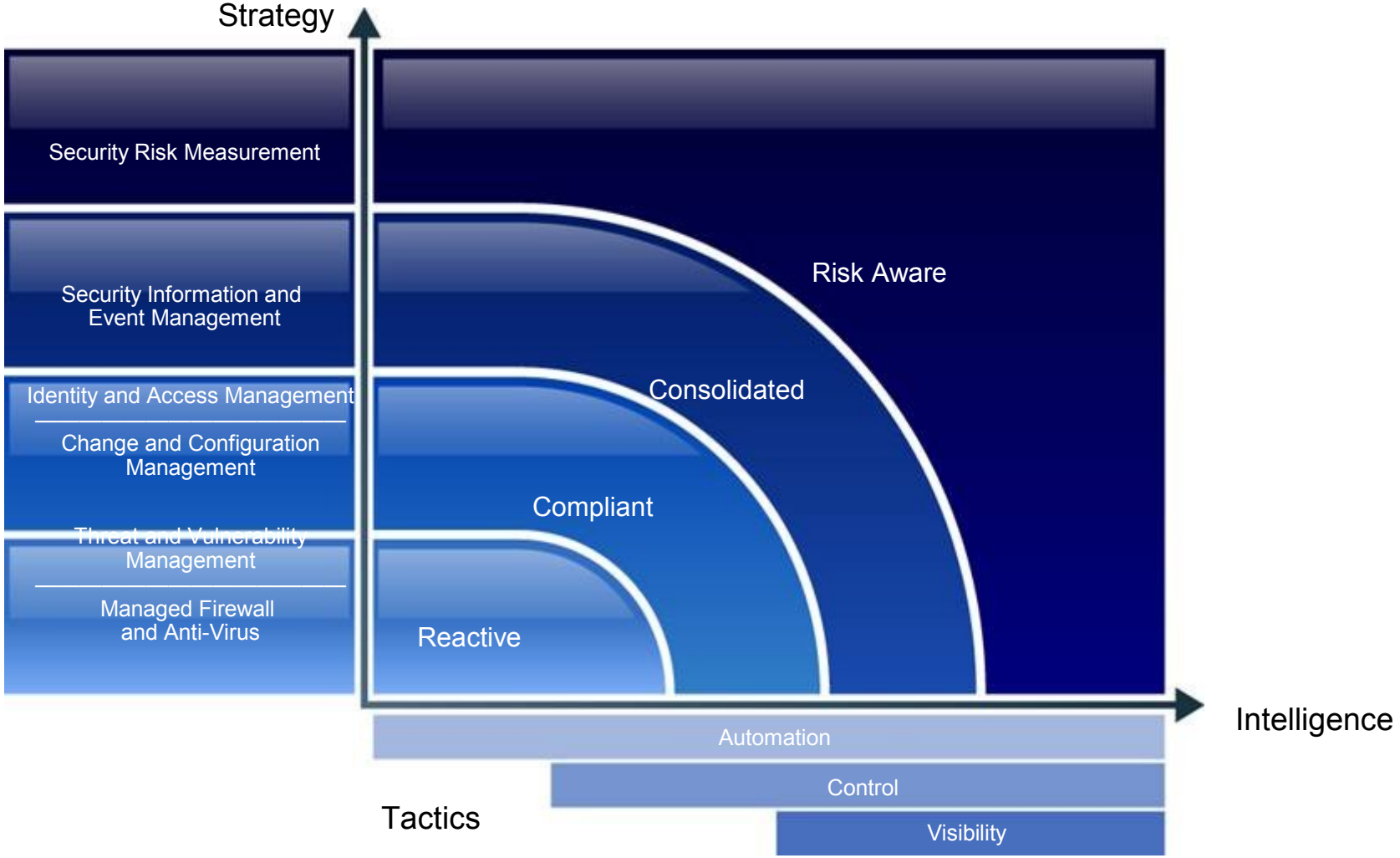
Access to streams of information in the Real Time

New Forms of Collaboration

New possibilities.
New complexities.
New risks.

Building Effective Risk Management Capability

Enabling Greater Maturity in Information Security Practices

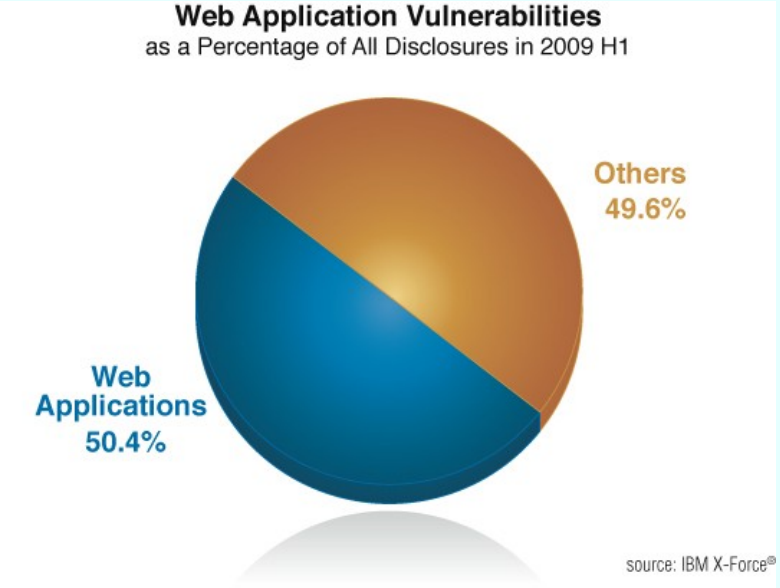


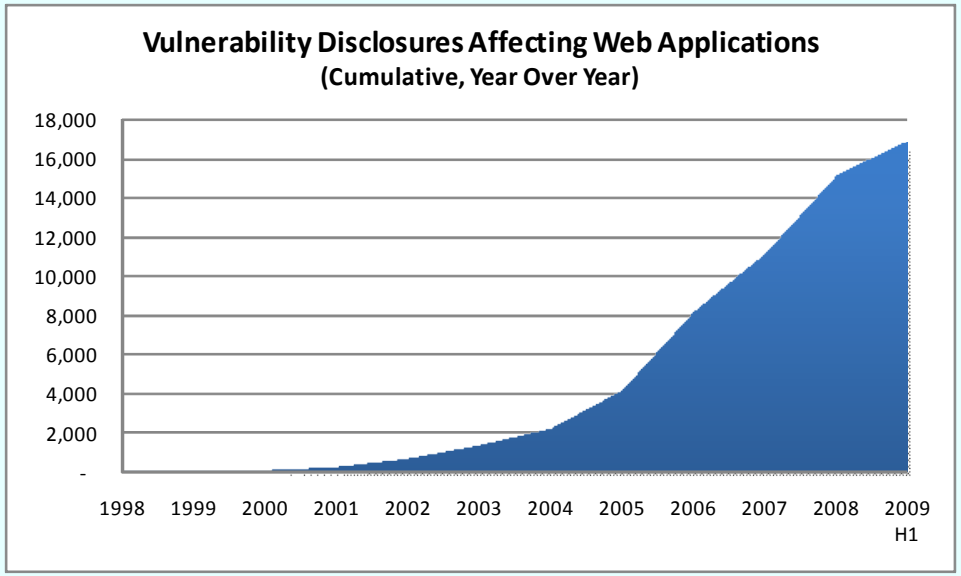
Application Vulnerabilities Continue to Dominate

Web application vulnerabilities represented the largest category in vulnerability disclosures (55% in 2008)

In 1H09, 50.4% of all vulnerabilities are Web application vulnerabilities

SQL injection and Cross-Site Scripting are neck and neck in a race for the top spot



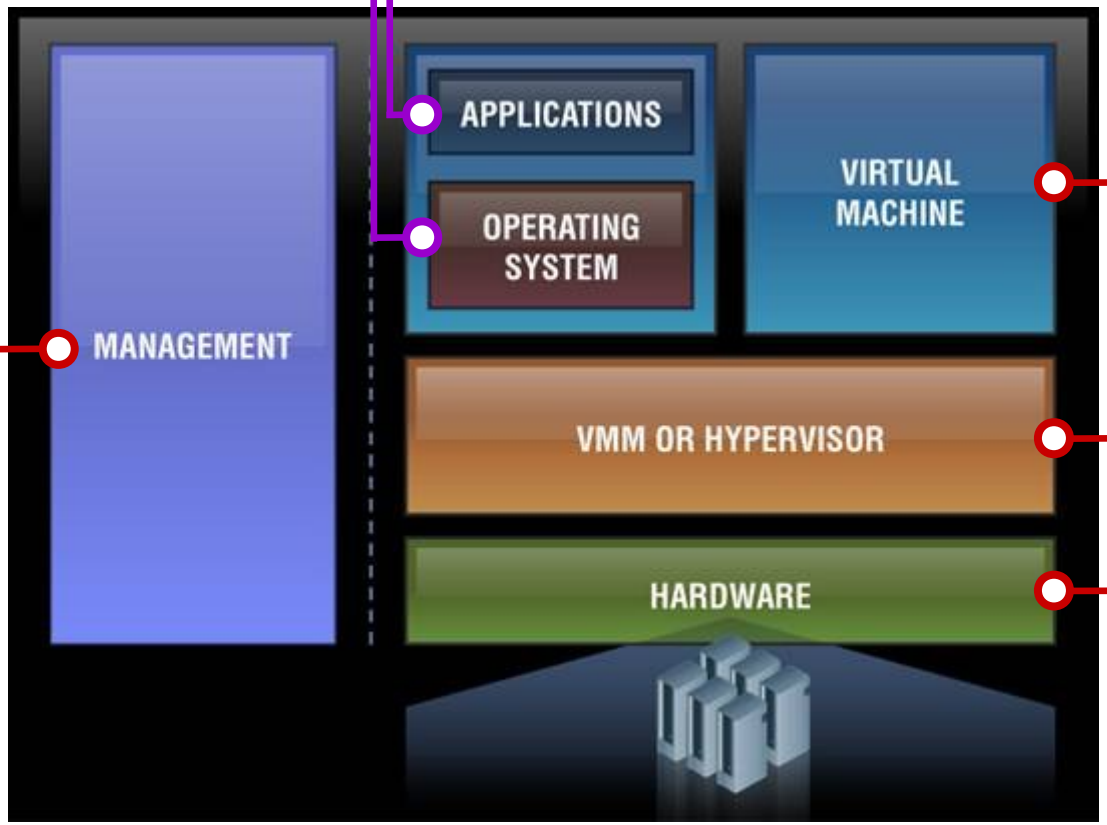


IBM Internet Security Systems 2009 X-Force® Mid-Year Trend & Risk Report

More Components = More Exposures and More Difficulty in Integrating Risk Management with Virtualized Environments

- Traditional Threats
- New threats to vm environments

Traditional threats can attack VMs just like real systems



Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

Security Solutions Must Address Key *Business* Challenges

REDUCE COSTS

MITIGATE RISKS

INCREASE PRODUCTIVITY

- Provide immediate savings and lower total cost of ownership
- Ensure business continuity
- Enable innovation

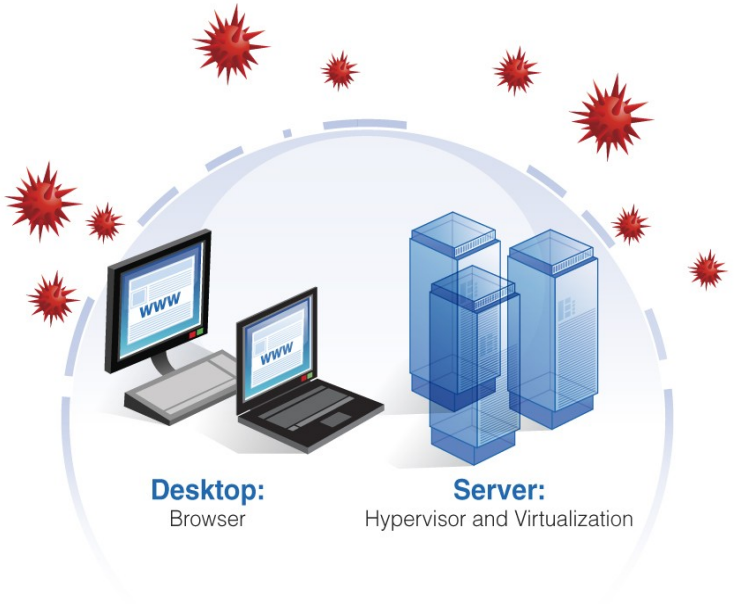
Complexity remains the biggest security challenge!*

Integration is key to managing the cost and complexity of the evolving landscape

*InformationWeek 2008 Security Survey

Market Drivers

- **Increase in vulnerabilities / disclosures**
  - *Application security has become the top threat*
- **Regulatory Compliance**
  - Requirements such as PCI, HIPAA, GLBA, etc
- **User demand**
  - For rich applications is pushing development to advanced code techniques – *Web 2.0* introducing more risks to threats
- **Enterprise Modernization**
  - Driving traditional applications to online world (SOA), increasing corporate risk
- **Cost cutting in current economic climate**
  - Demands increased efficiencies

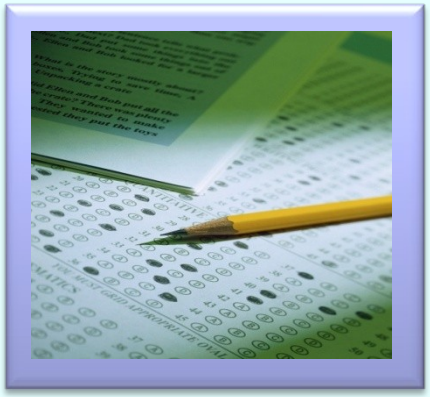


Cost to fix a defect

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

During the **coding** phase
$25/defect

During the **build** phase
$100/defect



During the **QA/Testing** phase
$450/defect

Once **released** as a product
$16,000/defect

Law suits, loss of customer trust, damage to brand

The increasing costs of fixing a defect….

Capers Jones, Applied Software Measurement, 1996
* Source: NIST, 'Assesses Technical Needs of Industry to Improve Software Testing', June 28, 2002

Application and Process

Keep applications services secure, protected from malicious or fraudulent use, and hardened against failure and catastrophe.

Assess and Implement Secure Development Processes	Static Source Code Vulnerability Analysis **(IBM acquisition of Ounce Labs)** Dynamic Application Vulnerability Analysis **(IBM AppScan)**
Mitigate Application Vulnerabilities	Real-Time Detection and Blocking of Application Vulnerabilities **(IBM Proventia Gx)** Real-Time Message Security (SOAP etc.) **(IBM DataPower)**
Manage Application Access Controls	Single Sign-On and Self-Service Password Management **(IBM Tivoli Access Manager family)** Fine-grained Entitlements **(IBM Security Policy Manager)** Enforce Trust Across Boundaries **(IBM Federated Identity Manager)**

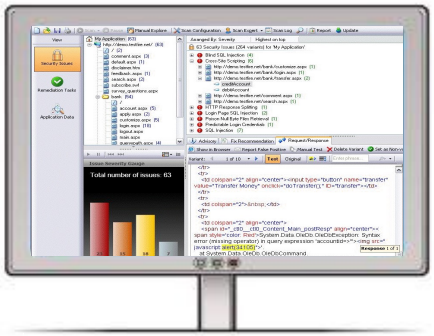
How does Application Security Testing work?

1

Explore source code and/or web site to detect structure

2

Identify Vulnerabilities ranked after severity and show how it was identified

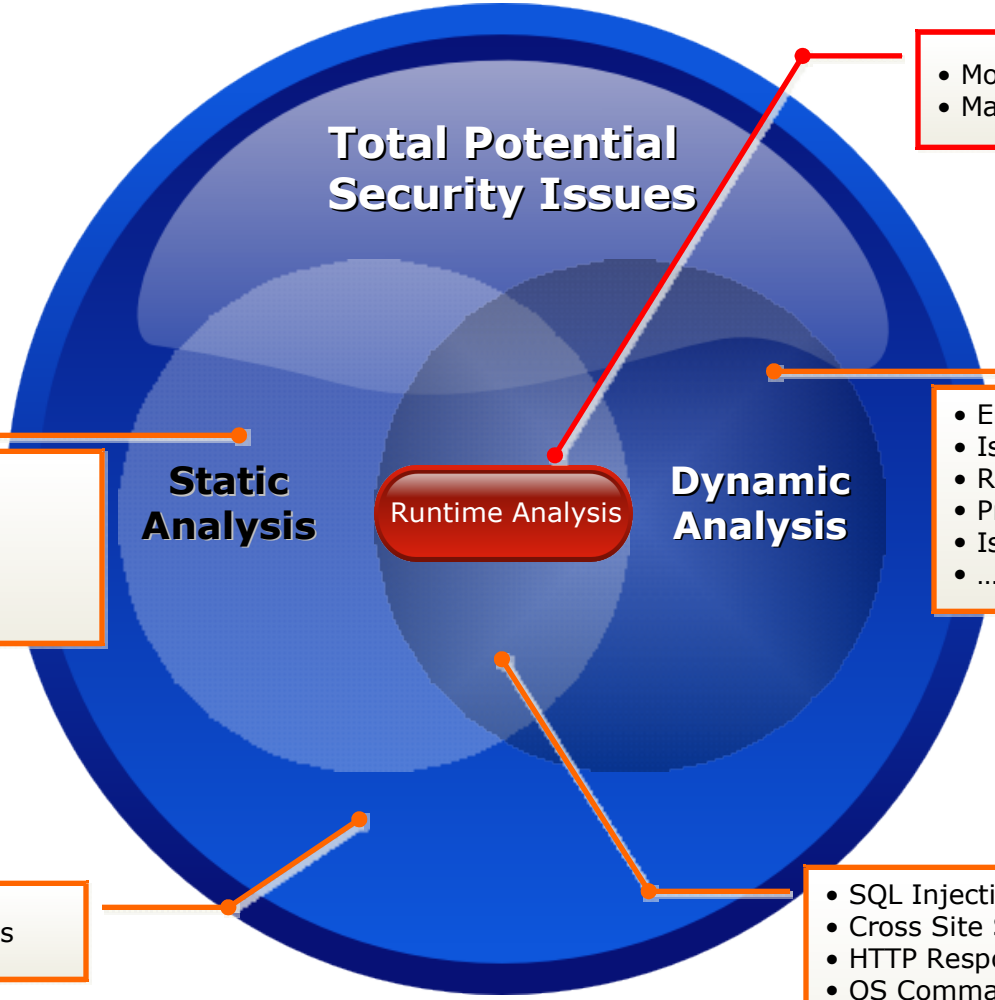


Virtual-SOC Portal

3

Advanced remediation, fix recommendations and security enablement

Security Issues Coverage



- Monitor application as its running
- Map Exploited Issues to Code

- Null Pointer Dereference
- Threading Issues
- Issues in Dead Code
- Insecure Crypto Functions
- …

- Environment Configuration Issues
- Issues in integrations of modules
- Runtime Privileges Issues
- Protocol Parser/Serializer Issues
- Issues in 3rd party components
- …

- Application Logic Issues

- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- …

Flexible Deployment Options

Source for Automation

-Standard Ed

Build

Configure
Scan
Triage

Development

- Source Ed Developer
- Source Ed Remediation
- Enterprise QuickScan

Configure
Scan

QA

Tester Ed for RQM

Source Ed Core

Enterprise portal & Report Console

Configure
Scan
Triage
Remediate
Verify

Functions:

Security Requirements
Configure
Scan
Triage
Remediate
Verify

Security Requirements
Configure
Scan
Triage

-Standard Ed

-Source Ed for Security

Security

Compliance

IBM Software

PCTY2010

Pulse Comes to You