Strategies to Ensure Applications are Secure by Design

Steve Hikida
Director, Security, Automation and Cloud Development – IBM Rational
hikida@ca.ibm.com

Innovate2011
The Rational Software Conference

Let's build a smarter planet.

The premiere software and product delivery event.
June 5–9, 2011 Orlando, Florida

Security is More than Operations

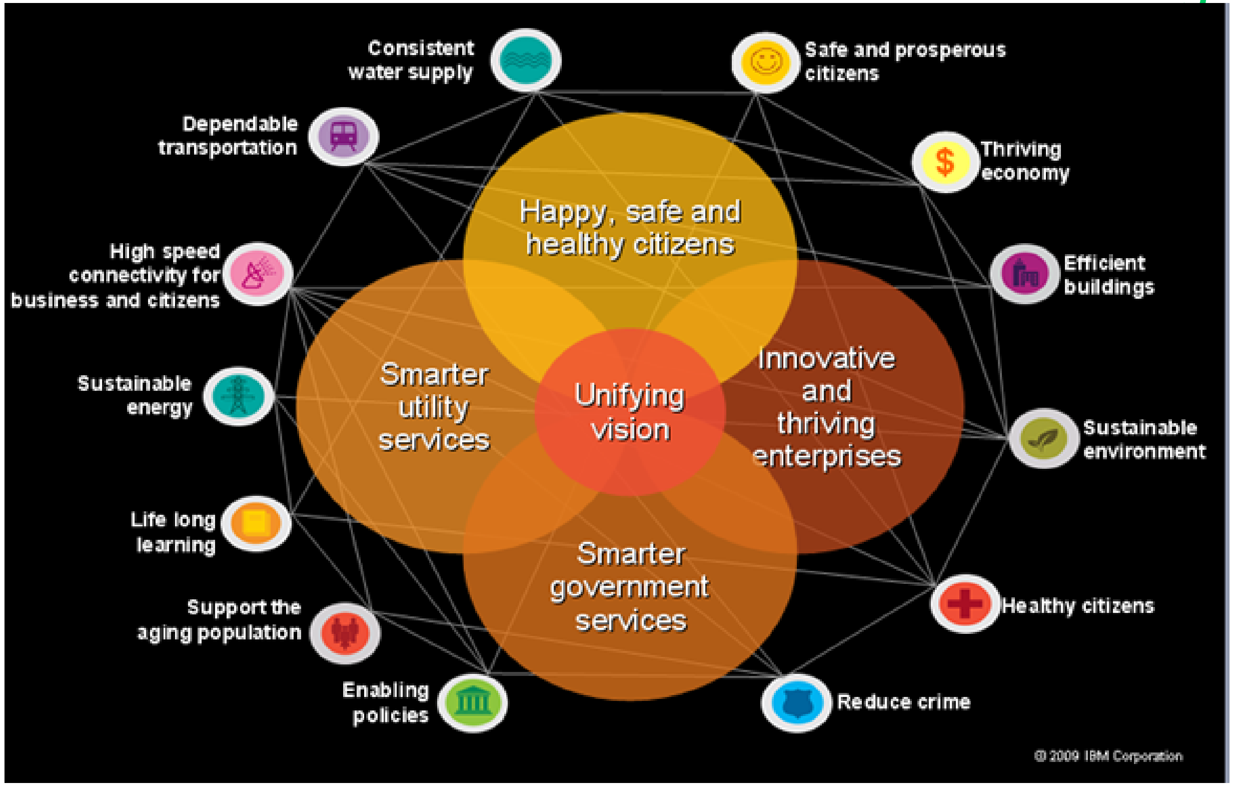
Why Development ***Needs*** *to Take Responsibility*

The Smarter Planet

Our world is getting **Instrumented**

Our world is getting **Interconnected**

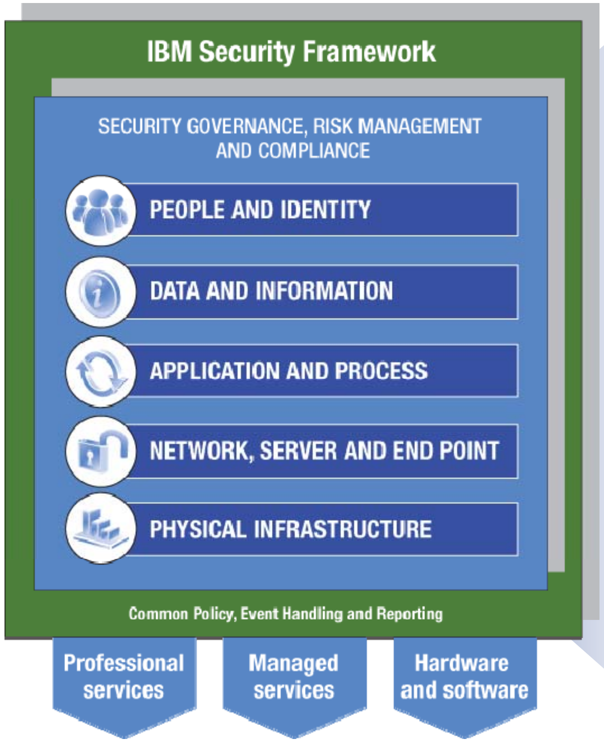
Our world is getting **Intelligent**


Consistent water supply
Safe and prosperous citizens
Dependable transportation
Thriving economy
High speed connectivity for business and citizens
Efficient buildings
Sustainable energy
Sustainable environment
Life long learning
Healthy citizens
Support the aging population
Enabling policies
Reduce crime
Happy, safe and healthy citizens
Smarter utility services
Unifying vision
Innovative and thriving enterprises
Smarter government services

© 2009 IBM Corporation

IBM Security Framework – Securing the Smarter Planet

SOFTWARE



PEOPLE AND IDENTITY
Mitigate the risks associated with user access to corporate resources

DATA AND INFORMATION
Understand, deploy, and properly test controls for access to and usage of sensitive data

APPLICATION AND PROCESS
Keep applications secure, protected from malicious or fraudulent use, and hardened against failure

NETWORK, SERVER AND END POINT
Optimize service availability by mitigating risks to network components

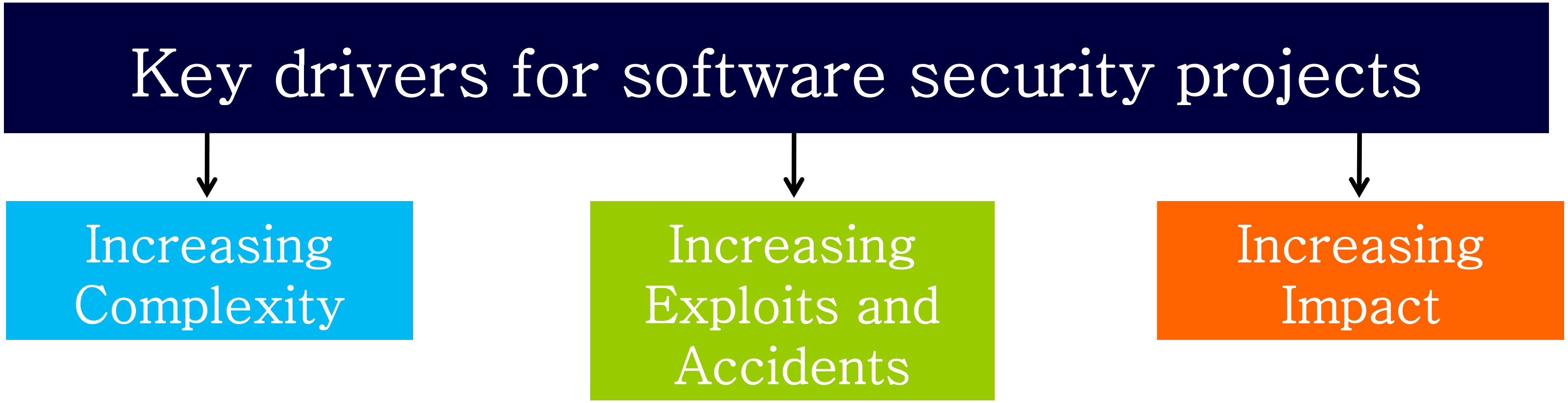
PHYSICAL INFRASTRUCTURE
Provide actionable intelligence on the desired state of physical infrastructure security and make improvements

Create & sustain security governance

Manage risk

Ensure compliance

Security Concerns Grow on the Smarter Planet



Key drivers for software security projects

Increasing Complexity

Increasing Exploits and Accidents

Increasing Impact

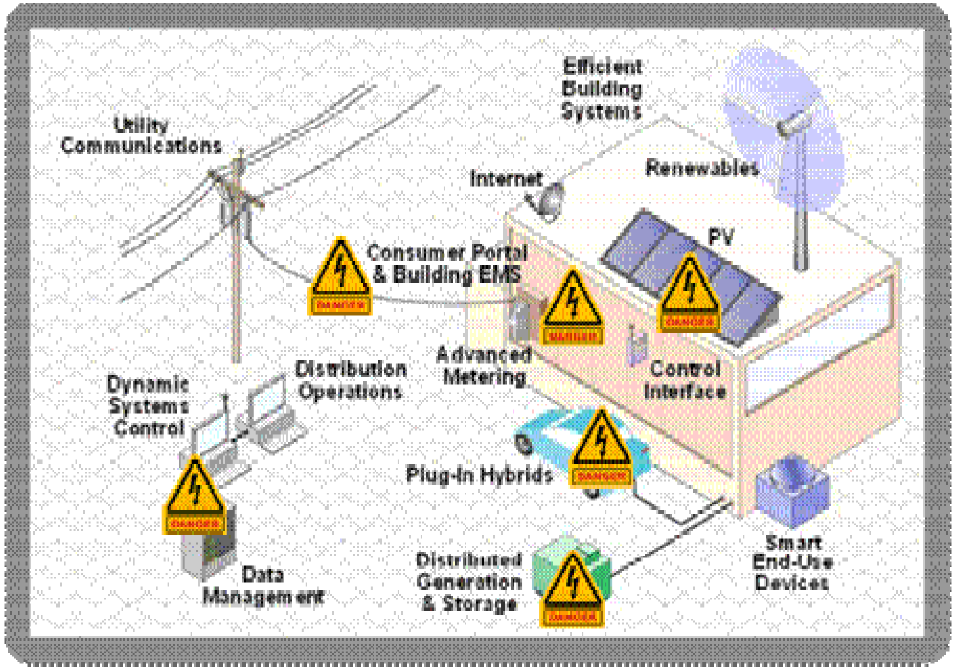
Soon, there will be **1 trillion** connected devices in the world, constituting an “*internet of things*”[†]

900+ Breaches reported
900+ M records exposed[‡]

The cost of a US data breach increased to $204 per compromised customer record and $6.8M Million per breach[Γ]

Sources [†] *http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html*
[‡] *2010 Verizon Business / US Secret Service Data Breach Investigations Report*
[Γ] *2010 Ponemon Institute Data*

Increased Connections Expose Outdated Software and Attitudes



"Electricity Grid in U.S. Penetrated by Spies"
WSJ/Siobhan Gorham – 04/08/2009

"Report highlights Smart Grid security vulnerabilities"
Jaikumar Vijayan – 09/29/2009

"Power Grid is Found Susceptible to Cyberattack"
Robert McMillan – 03/21/2009

"Researchers at the Idaho National Engineering Laboratory have shown that it's possible to remotely hack into a control system for an electrical generator and cause it to fail–not just stop, but actually fly apart."
Phil Windley | September 28, 2007 (ZDNet)

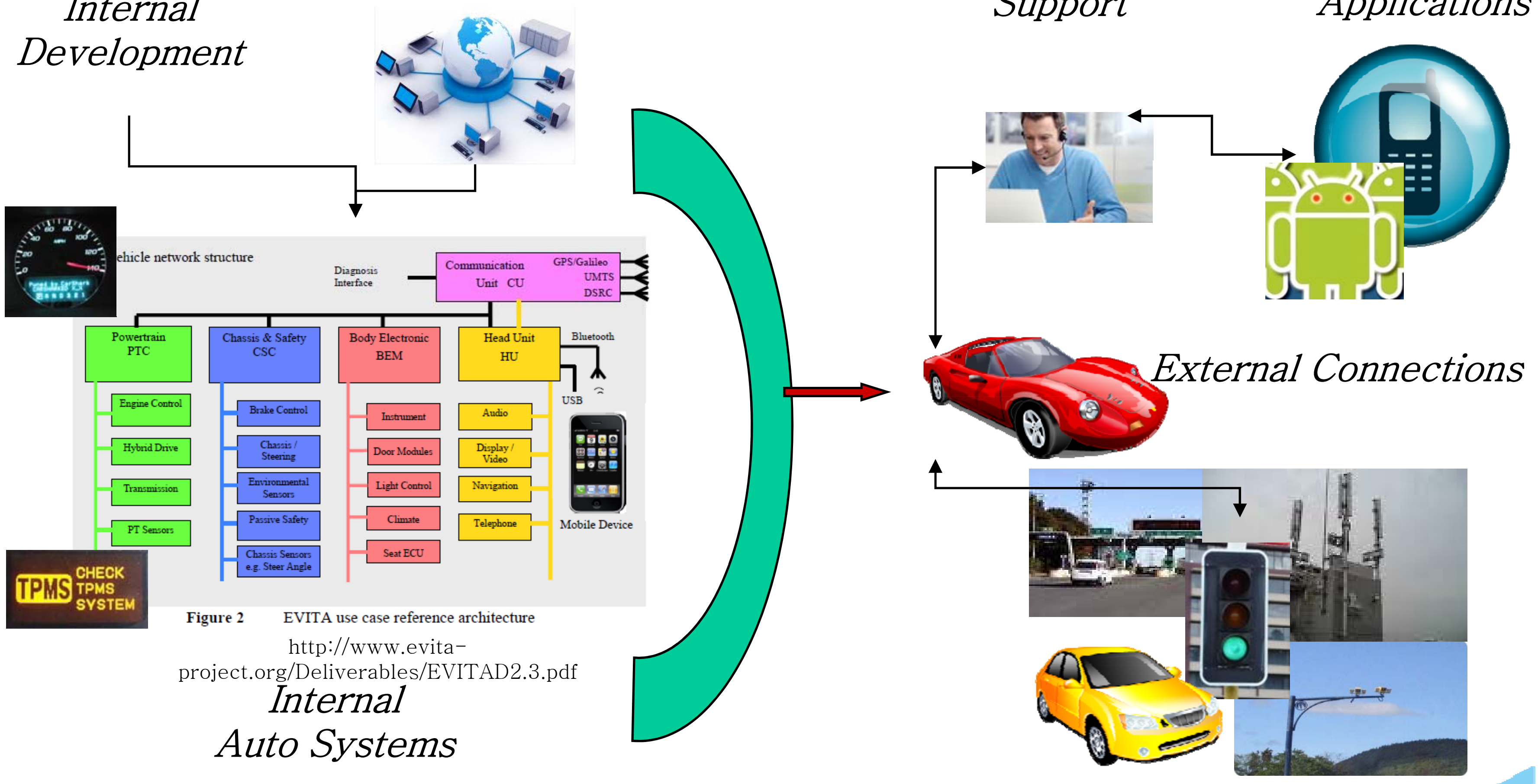
Complex Picture of Auto / IT System Interconnect

Outsourced / OEM Providers

Internal Development

Remote Support

Mobile Applications



External Connections

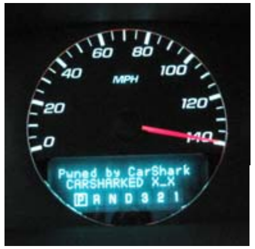
Figure 2 EVITA use case reference architecture

http://www.evita-project.org/Deliverables/EVITAD2.3.pdf

Internal Auto Systems

Research illuminating internal weaknesses

"Experimental Security Analysis of a Modern Automobile"
http://www.autosec.org/pubs/cars-oakland2010.pdf



"Surprisingly, also without needing to unlock the EBCM, we were also able to ***release the brakes*** *and* ***prevent them from being enabled****, even with car's wheels spinning at 40 MPH while on jack stands."*

*"****Self-Destruct.*** *Combining our control over various BCM components, we created a "Self-Destruct" demo in which* ***a 60-second count-down*** *is displayed on the Driver Information Center (the dash), accompanied by clicks at an increasing rate and horn honks in the last few seconds. In our demo,* ***this sequence culminated with killing the engine and activating the door lock relay*** *(preventing the occupant from using the electronic door unlock button)."*

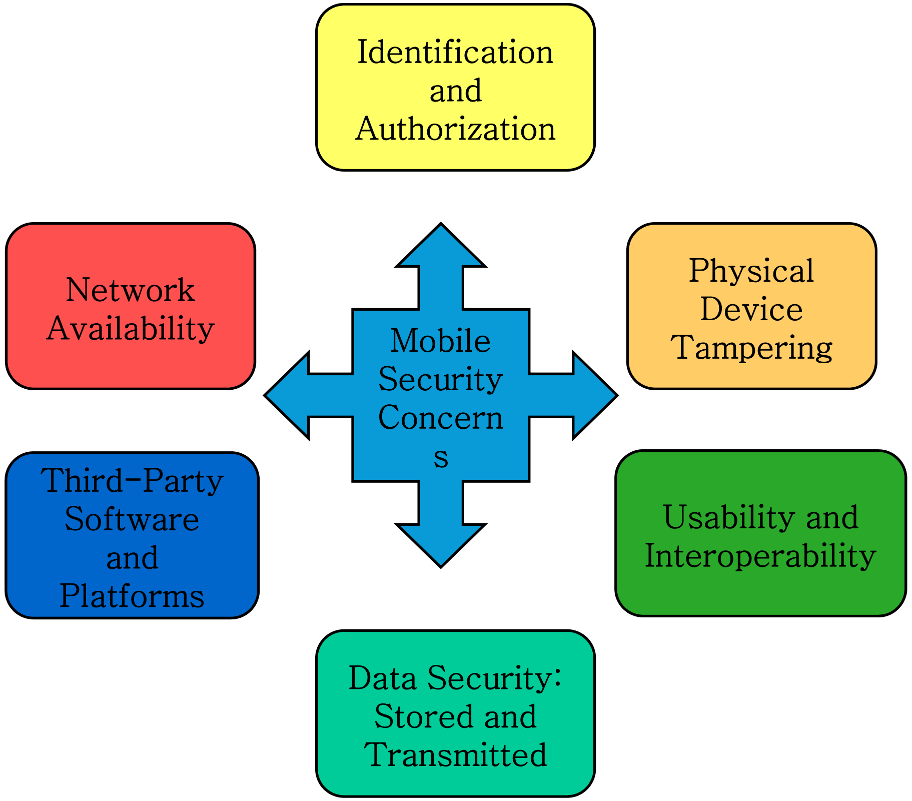
"Security and Privacy Vulnerabilities of In-Car Wireless Networks"
http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf

"…current protocols ***do not employ authentication*** *and vehicle implementations* ***do not perform basic input validation****, thereby allowing for remote spoofing of sensor messages."*

"The implementation of the in-car system appears to fully trust all received messages. We found ***no evidence of basic security practices****, such as input validation, being followed."*

"To our surprise, at the end of only two days of sporadic experiments involving triggering the TPMS warning on and off, we managed to crash the TPMS ECU and ***completely disabled the service****… Eventually, a visit to a dealership recovered the system at the cost of replacing the TPMS ECU."*

Mobile Platform Popularity Creating New Threat Vectors


Identification and Authorization
Network Availability
Mobile Security Concern s
Physical Device Tampering
Third-Party Software and Platforms
Usability and Interoperability
Data Security: Stored and Transmitted

"Fake Mobile Banking App Discovered in Android Marketplace"

Humberto Saabedra – 01/10/2010

"iPhone worm hijacks ING customers"

John Leyden – 11/23/2009

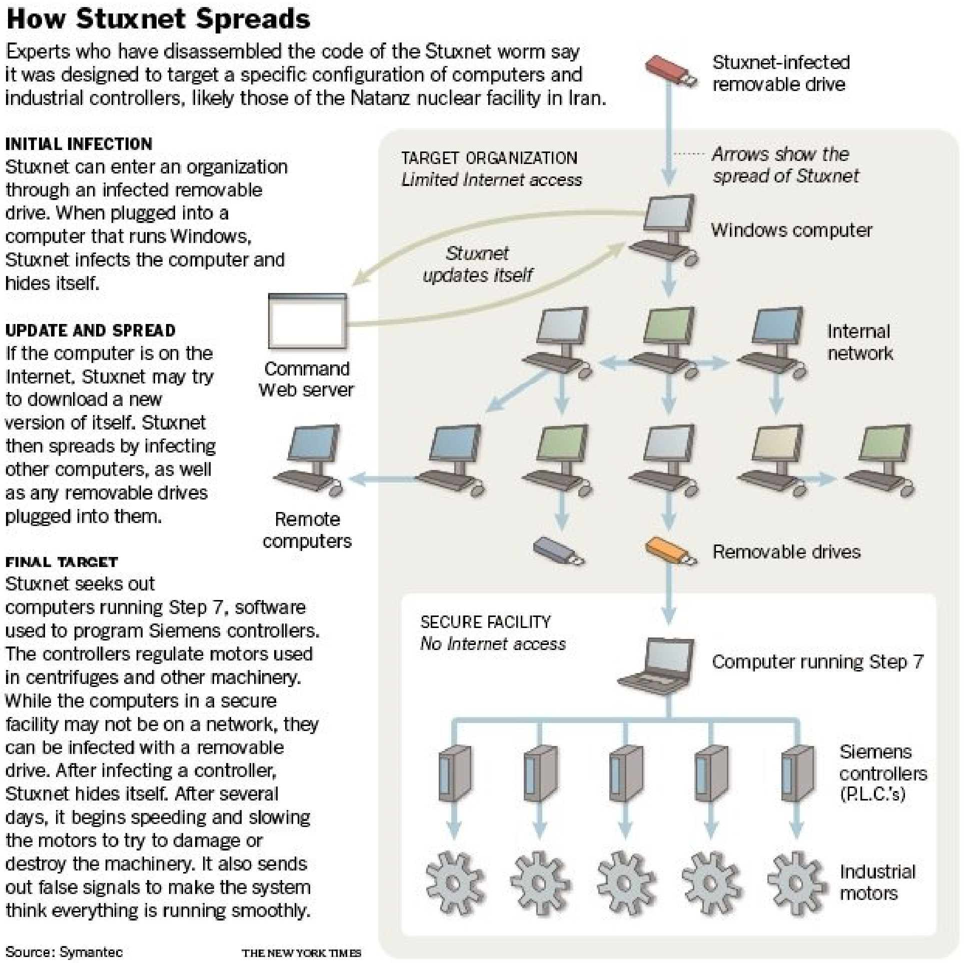
"Rootkit-based Exploits Could Eavesdrop Smartphones" – 01/25/2010

> *The researchers, who are presenting their findings at a mobile computing workshop in Maryland, are showing how a rootkit could cause a smartphone to eavesdrop on a meeting, track its owner's travels, or rapidly drain its battery to render the phone useless — all without the user's knowledge.*

"Pay-Per-Text Malware Hits Android Phones"

Andy Greenberg : Aug. 11 2010

Attacks are becoming more Sophisticated : Stuxnet



How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

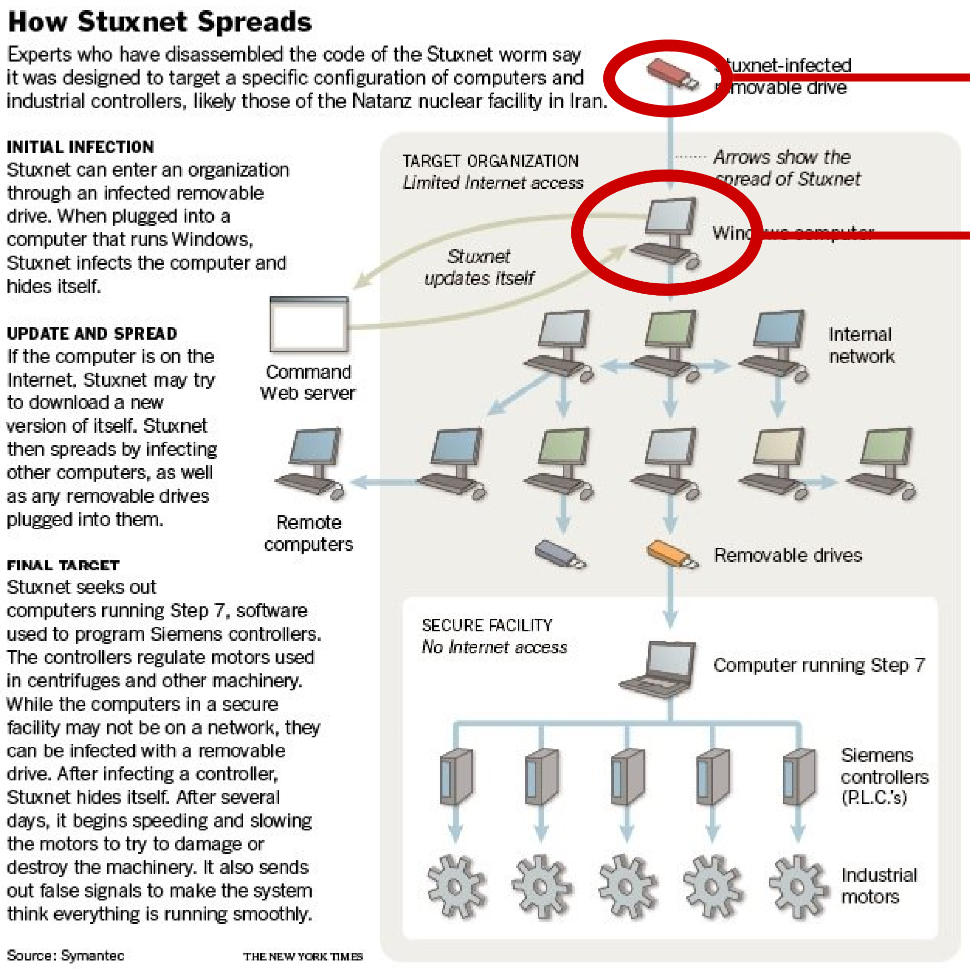
FINAL TARGET
Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

Source: Symantec THE NEW YORK TIMES

Stuxnet

- Targets specific controllers
- Is introduced via removable drives or network shares
- Updates itself via the Internet, and infects other computers and removable drives through a variety of attacks
- Always seeking target controllers
- Once on a controller, it hides itself and begins to cause physical damage

Unconventional paths to “Isolated” Systems



How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

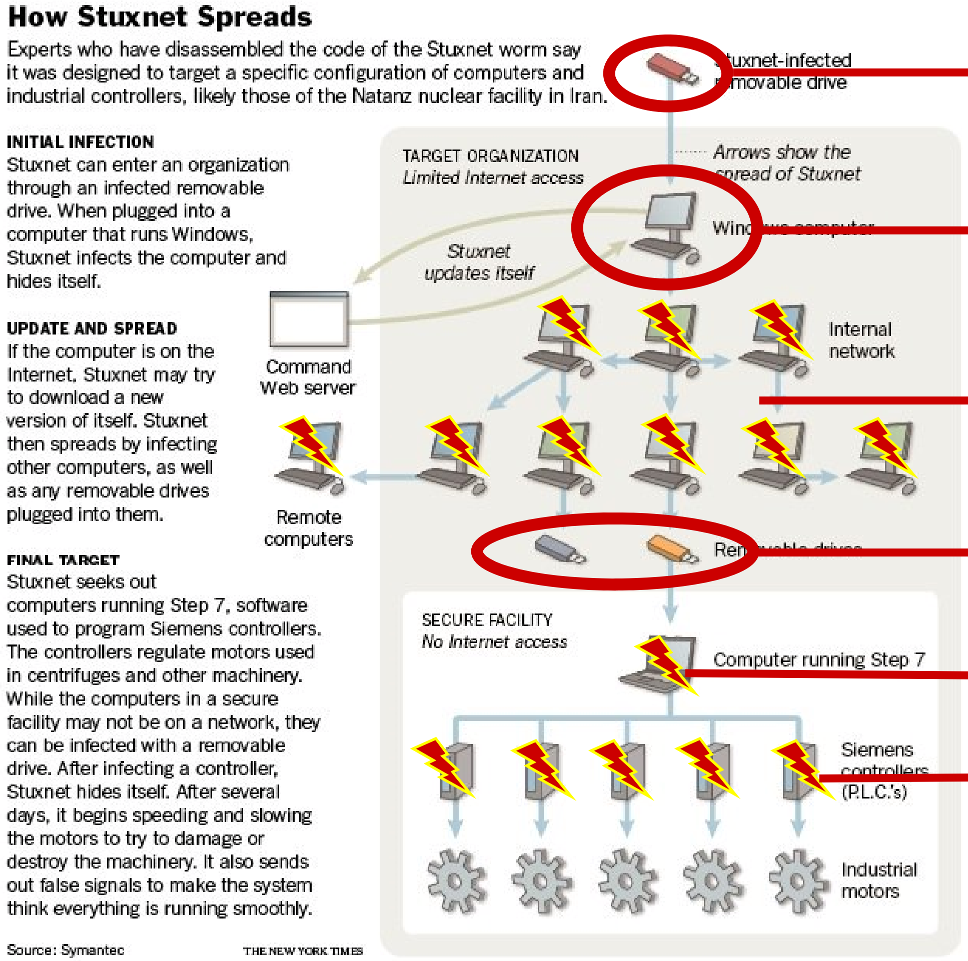
FINAL TARGET
Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

Source: Symantec THE NEW YORK TIMES

Infected USB Sticks are picked up by employees or contractors

Infection is passed to network connected computer

Targets now include lower level systems



How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

INITIAL INFECTION
Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

UPDATE AND SPREAD
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

FINAL TARGET
Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

Source: Symantec

THE NEW YORK TIMES

Infected USB Sticks are picked up by employees or contractors

Infection is passed to network connected computer

Automated attacks are executed against network accessible computers, passing the infection

Infection is passed to any USB stick that is inserted

Attack identifies target computer destination

Infected controlling computer corrupts controllers on “disconnected network”

Software Development Shares Responsibility

Theft

- Unauthorized access to customer private data
- Breach of physical security controls
- Leakage of financial / credit card data from infrastructures

Decreased User Satisfaction

- Inconsistent experience
- Frequent requirements for software updates
- Unexpected behaviors

Physical Danger

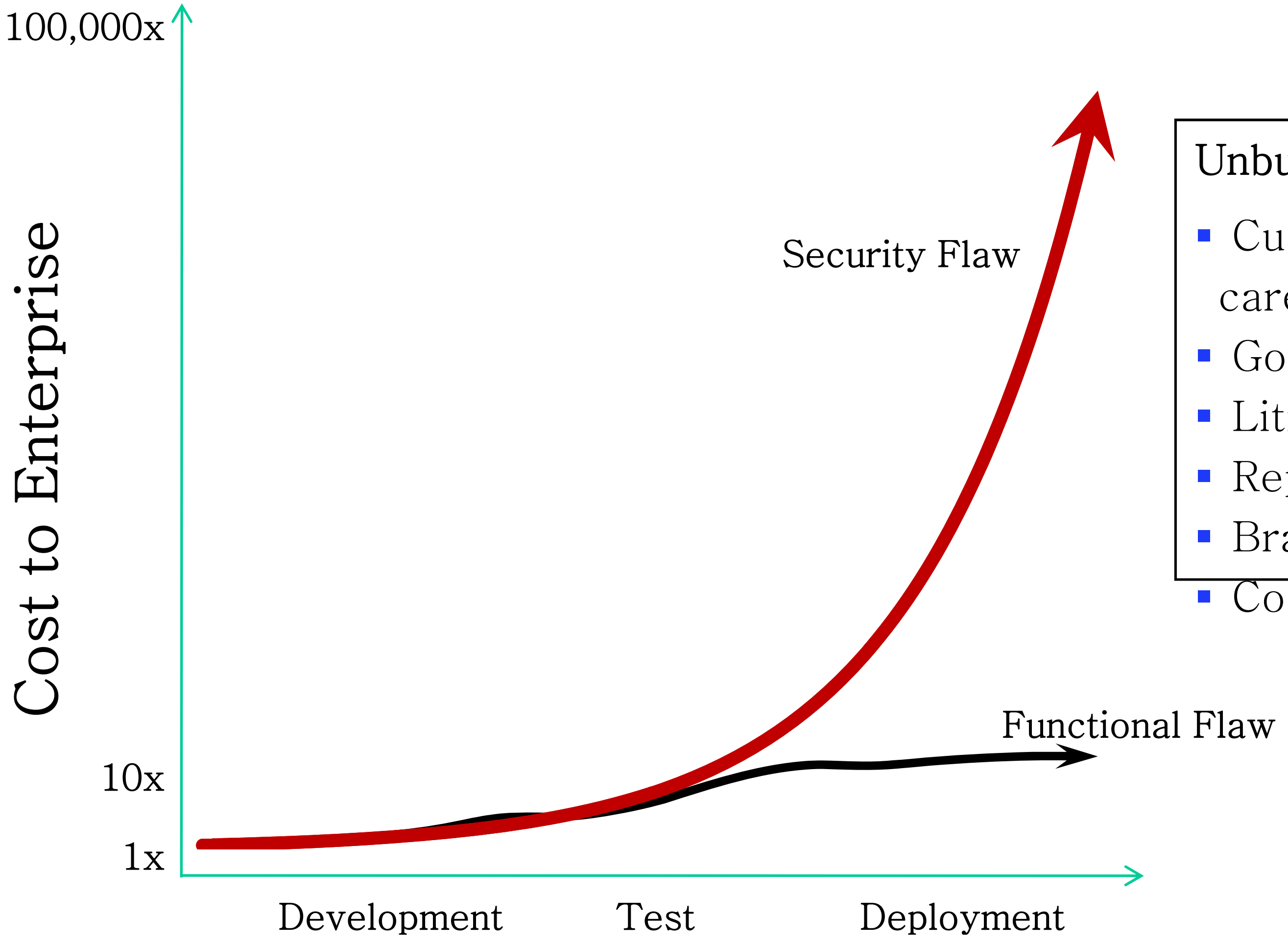
- Unauthorized control of functions
- Corrupted / modified data
- Denial of service against critical systems

MacPherson v. Buick Motor Company

The plaintiff, Donald C. MacPherson, a stonecutter, was injured when one of the wooden wheels of his 1910 Buick Runabout collapsed.

"…the manufacturer of this thing of danger is under a duty to make it carefully…"
--Judge Benjamin N. Cardozo 1916

Incremental and Unbudgeted Costs of Critical Breaches



Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

Accelerating Awareness and Progress: Secure by Design

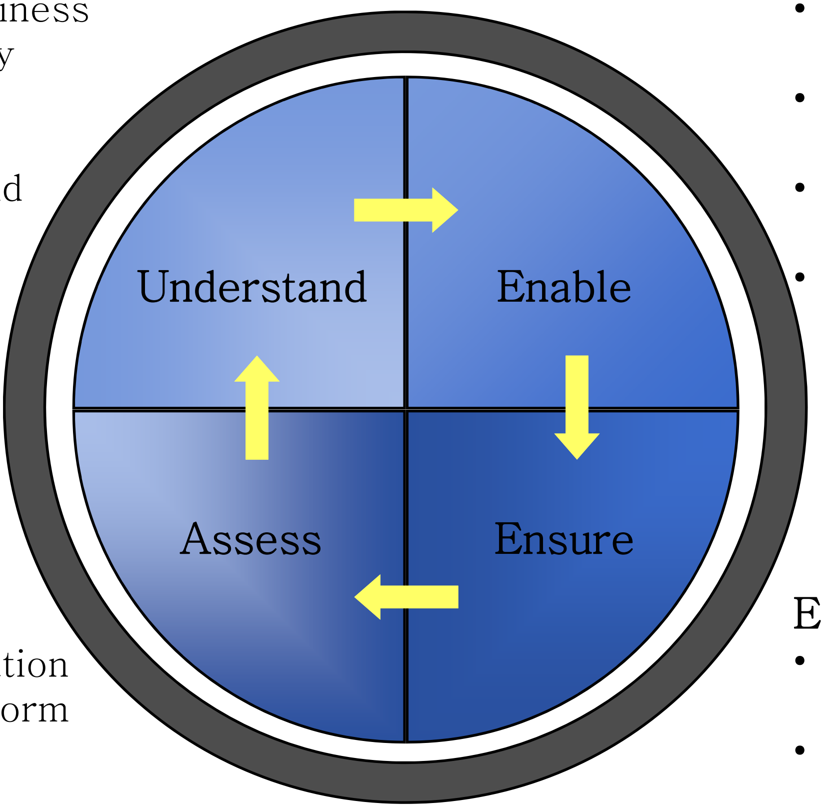
Secure by Design is a **cost-effective** approach to constructing **safe and reliable systems** by applying IBM's experience with security technologies and best practices in all phases of system creation, from conception through system design, construction and deployment.

Being **Secure by Design** reduces the **cost**, **risk**, and **unpredictability** of integrating new technologies.

Components of a Strategy to be Secure by Design

Understand Security Drivers

- Recognize specific business opportunity and priority
- Assess system risk to business
- Model likely threats and impacts



Enable System Security

- Mandate appropriate security controls within applications
- Implement system monitoring/logging
- Specify secure platform & configuration
- Document update management plan

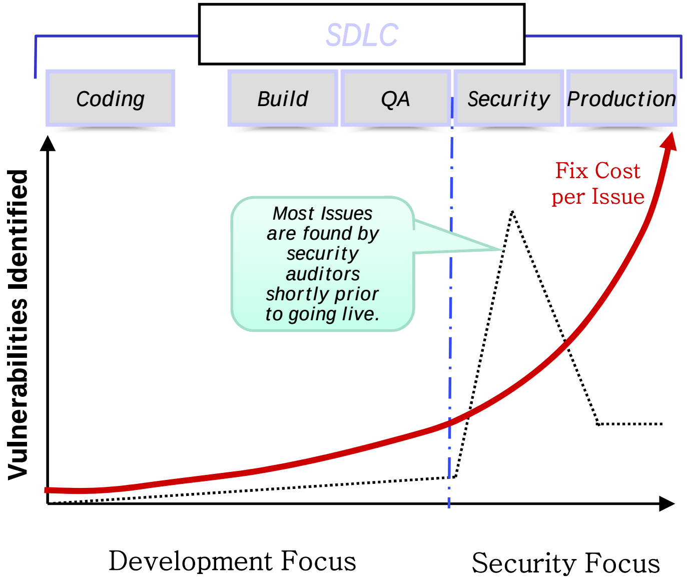
Assess Deployments

- Test composed application
- Verify security of platform configuration
- Establish process and schedule for regular checking

Ensure secure development

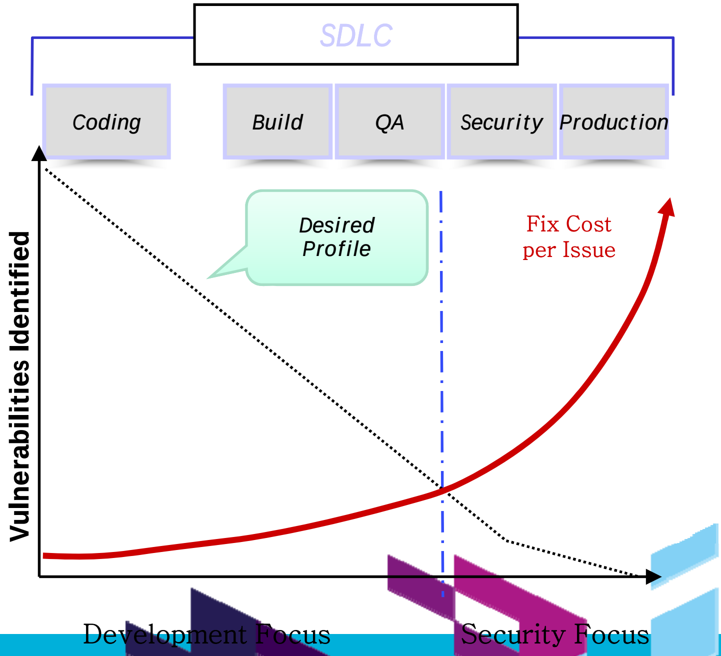
- Protect development infrastructure
- Verify safety of third-party software
- Check system for security during coding/build/integration stages

Moving to a Desirable End State



In early stages of adoption, security practitioners will assess applications during pre-deployment testing. **Costs are higher and window is shorter** to mitigate any issues found.

By integrating security into requirements, development and build/test/integration cycles, **identification occurs much earlier**, increasing find rate at a time when **fix costs are lowest.**



Additional Rationale for Going Through all of This

Cost-savings

Early introduction of security considerations is shown to save substantial costs in development, rework, breach mitigation and clean-up

Time to Market

Late stage identification of security issues is a common cause of deadline slips and unplanned tasking and rework

Protection of Reputation

Unaddressed vulnerabilities within deployed applications are a major risk to organizational reputation and customer confidence when breached

Regulatory Compliance

Requirements including PCI-DSS, HIPAA, and NERC CIP all mandate the security of IT infrastructures and include penalties for non-compliance

Competitive Differentiation

Increasingly, RFP and RFI content includes requests for vendor practices used to ensure the security of delivered systems and products

Institutionalizing Secure by Design

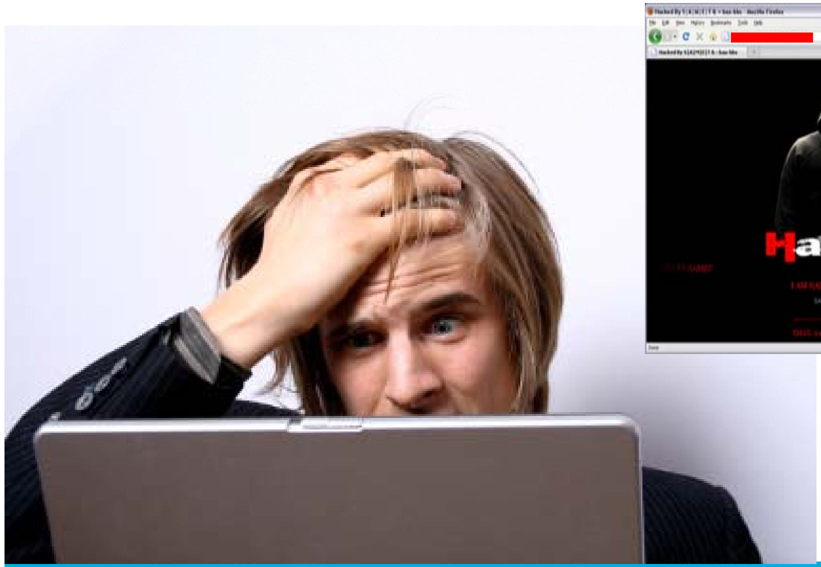
A Secure by Design Universe

Hacked: *When Things are Not Secure by Design*

The Reliable Times Daily

Popular Gaming Console Company Sued by Customer for $8.1 M Over Security Breach and Data Theft

Fun Games Corp. network entertainment unit was sued by a customer claiming it failed to protect users' personal information and credit card data that the company says may have been stolen by a hacker.



The Post

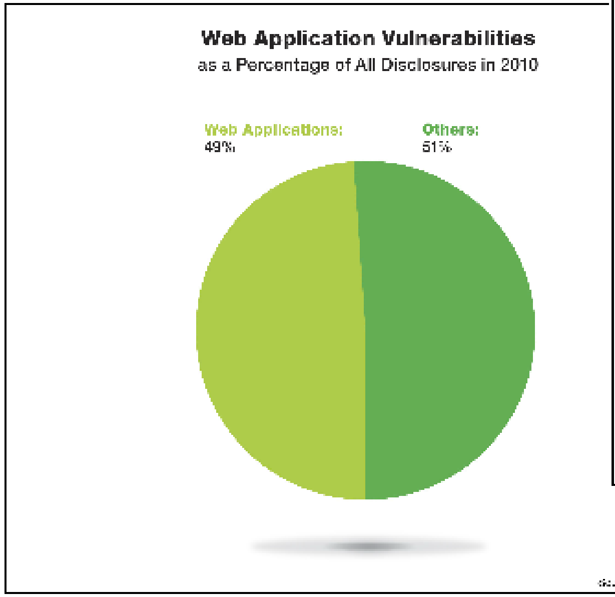
Company Found Negligent Over Security Breach

State Appeal Court issued ruling which found ABC Motors Corp. was negligent over a security breach…

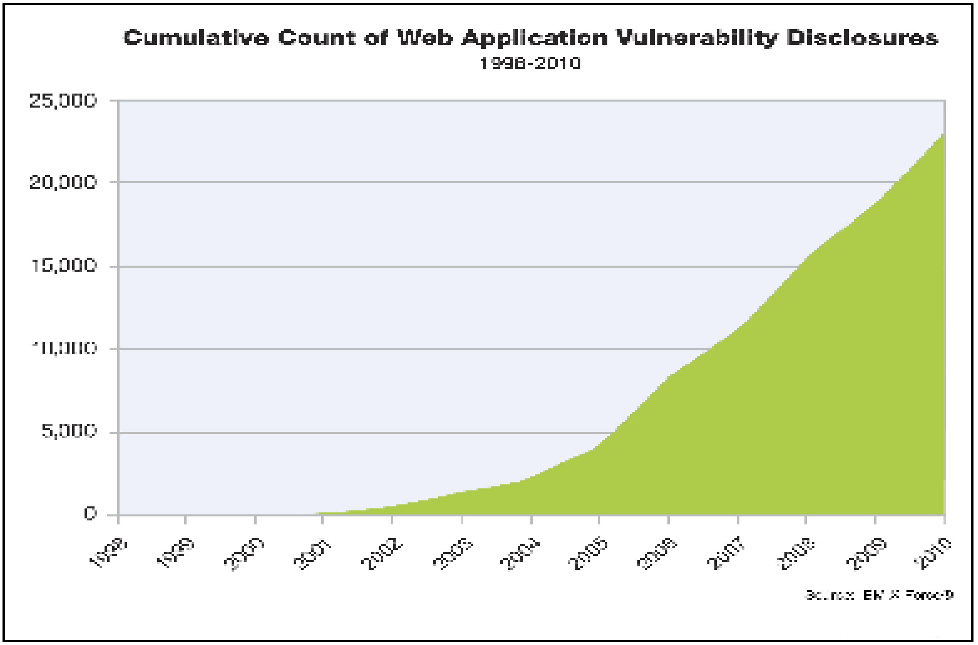
How could this have been prevented?

Application Vulnerabilities Continue to Grow

- **Web application vulnerabilities represent the largest category in vulnerability disclosures**
- **49% of all vulnerabilities were Web application vulnerabilities**
- **SQL injection and Cross-Site Scripting are neck and neck in a race for top spot**



Source: IBM X-Force®



Source: IBM X-Force®

IBM Internet Security Systems
2010 X-Force® Trend & Risk Report

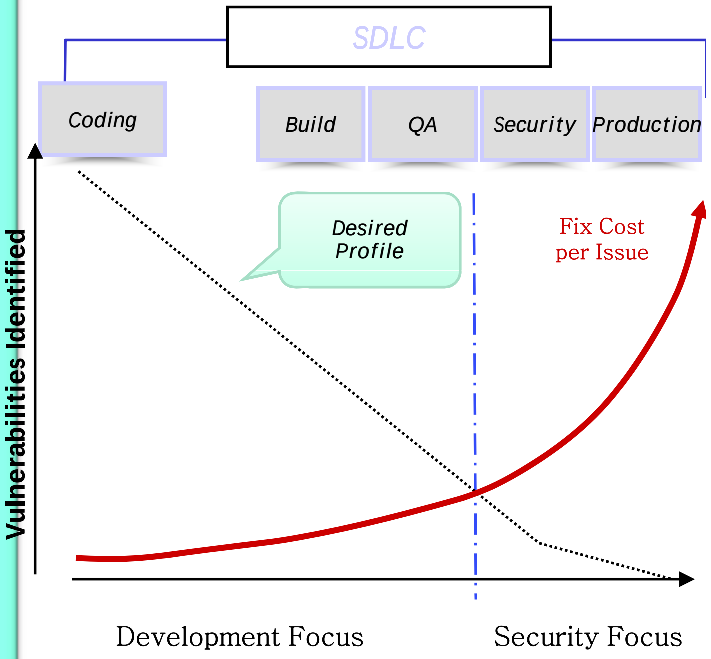
The Application Security Challenge

What?

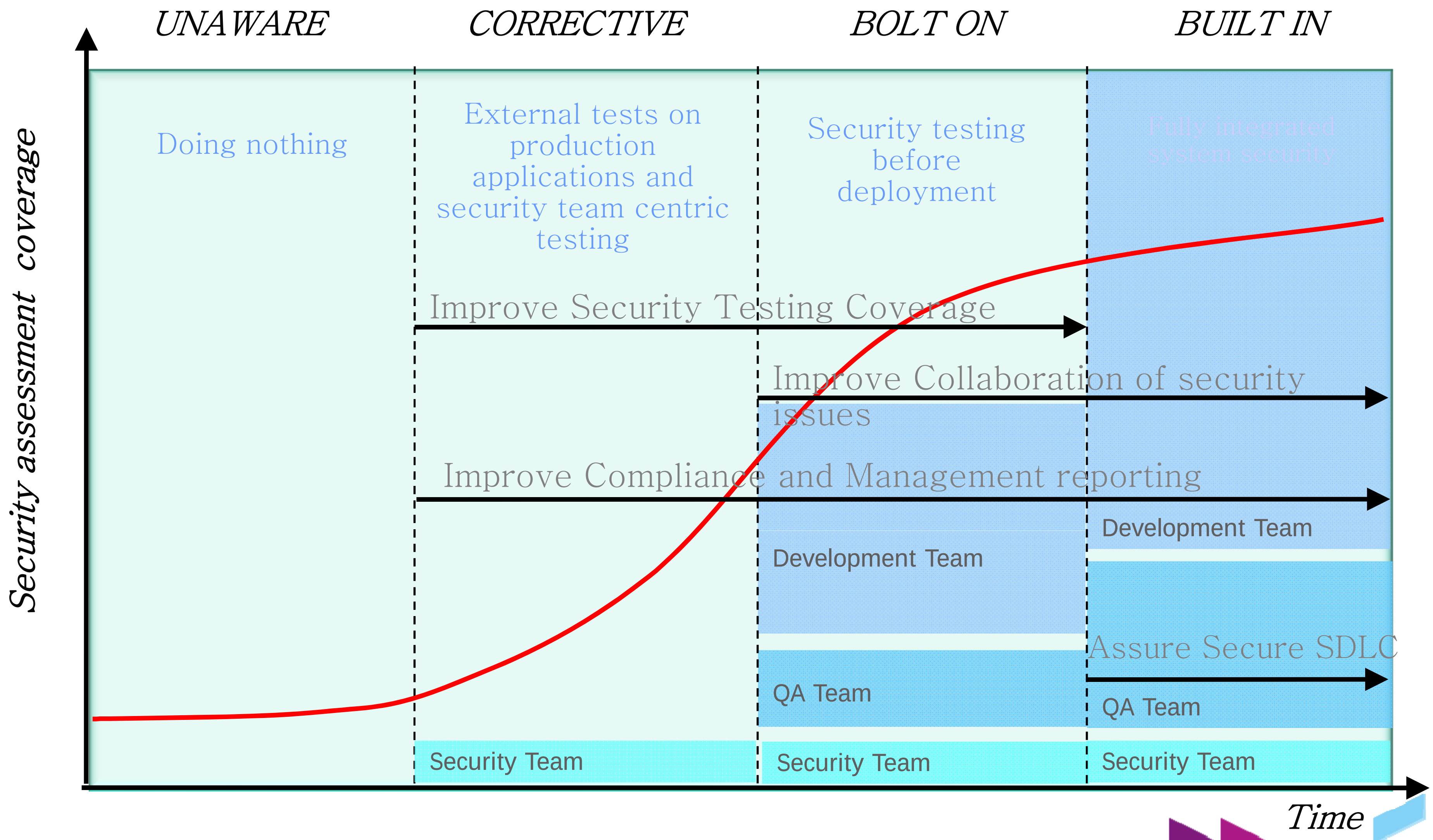
1. Need to **mitigate the risk** of a Security breach
2. Need to **find** and **remediate** these vulnerabilities
3. Must utilize a **cost effective** way of doing this that makes sense

Who?

- Software security represents the **intersection between security & development** – solution needs to be a joint collaboration
- Starts with Security Auditor (can also be outsourced)
- Larger organizations require the scaling of security testing into the development organization



Application Security Maturity Model



UNAWARE

CORRECTIVE

BOLT ON

BUILT IN

Security assessment coverage

Doing nothing

External tests on production applications and security team centric testing

Security testing before deployment

Fully integrated system security

Improve Security Testing Coverage

Improve Collaboration of security issues

Improve Compliance and Management reporting

Assure Secure SDLC

Development Team

Development Team

QA Team

QA Team

Security Team

Security Team

Security Team

Time

Make Applications Secure, by Design

Security as an Intrinsic Property of the Development Process

Design Phase

- Consideration is given to security requirements of the application
- Issues such as required controls and best practices are documented on par with functional requirements

Development Phase

- Software is checked during coding for:
  - ➢ Implementation error vulnerabilities
  - ➢ Compliance with security requirements

Build & Test Phase

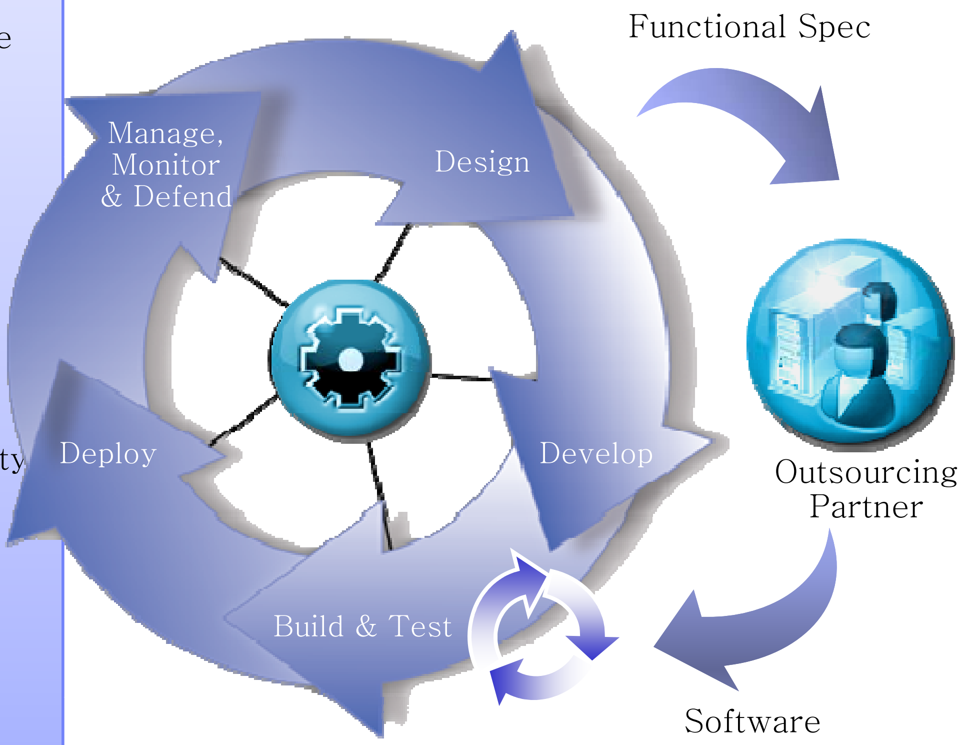
- Testing begins for errors and compliance with security requirements across the entire application
- Applications are also tested for exploitability in deployment scenario

Deployment Phase

- Configure infrastructure for application policies
- Deploy applications into production

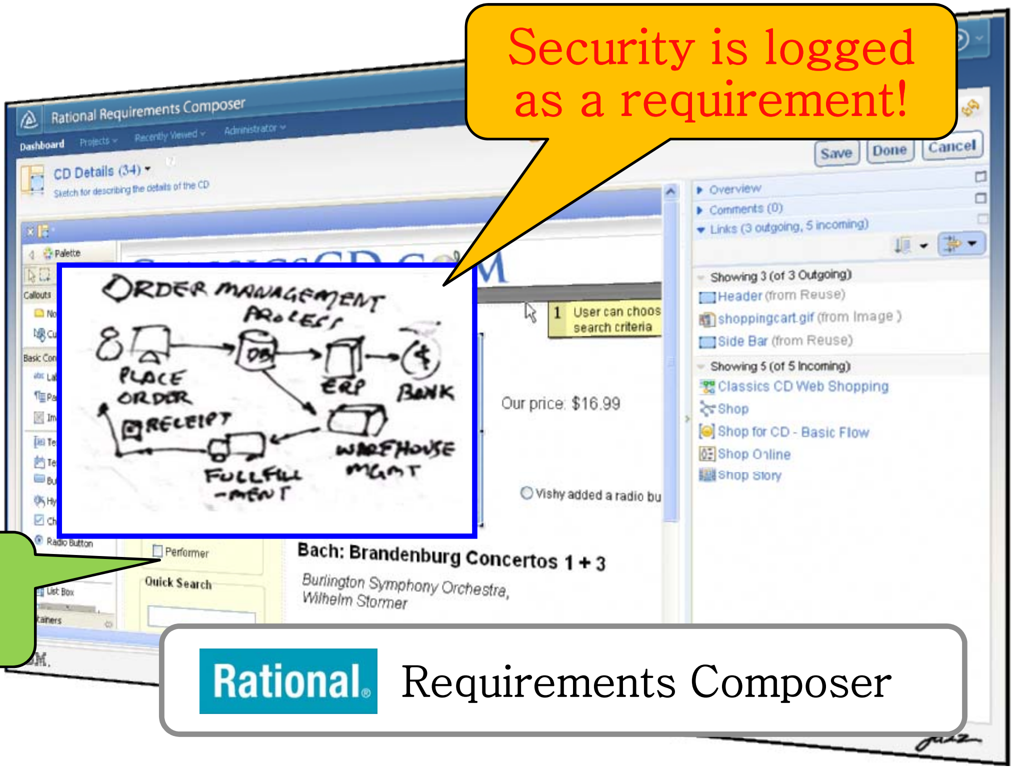
Operational Phase

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



A Secure by Design Universe: *Secure Requirements*

Project stakeholders gather information



Security is logged as a requirement!

Requirements logged into Rational Requirements Composer

Rational. Requirements Composer

IBM. Redbooks.

IBM's Secure Engineering Framework Redbook is used as a security guide

- Threat models are built and security requirements are added
- A security "champion" is appointed for the project

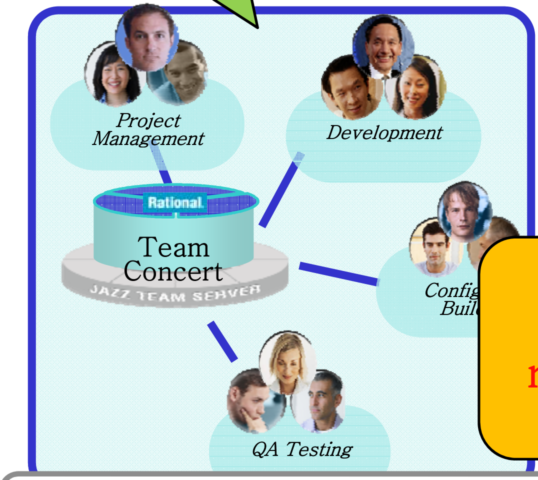
Security is core part of design!

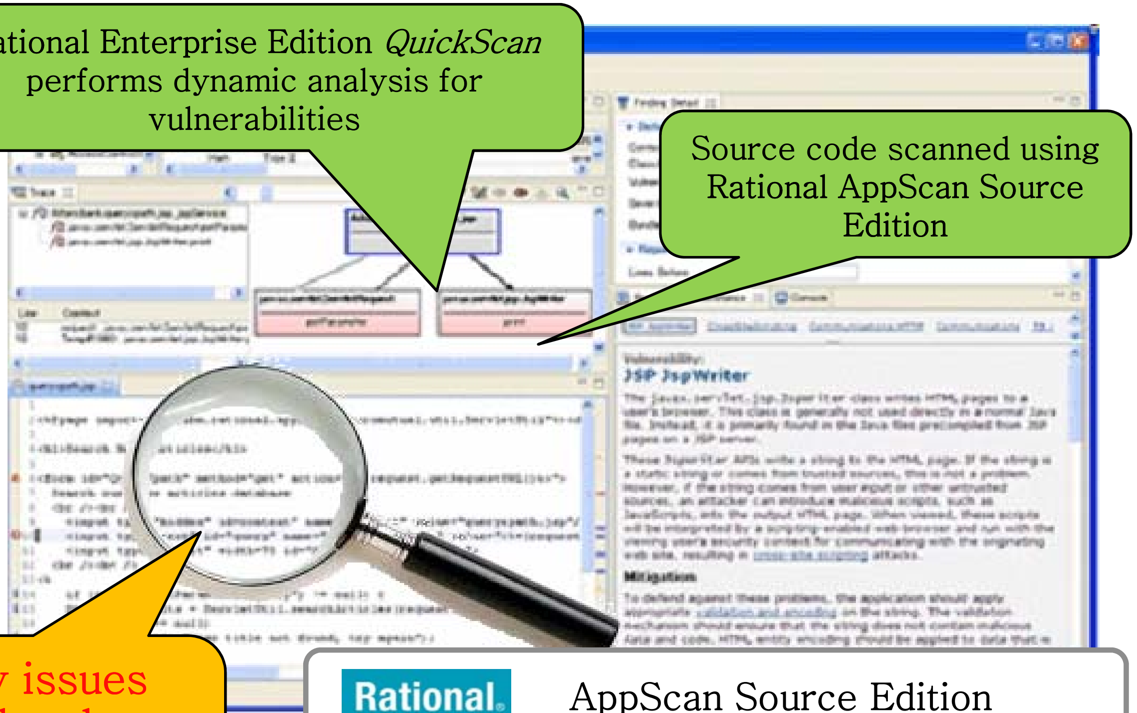
A Secure by Design Universe: *Secure Development*

Stories, tasks and defects logged in Rational Team Concert
• Security controls are added as stories / tasks

Rational Enterprise Edition *QuickScan* performs dynamic analysis for vulnerabilities

Source code scanned using Rational AppScan Source Edition

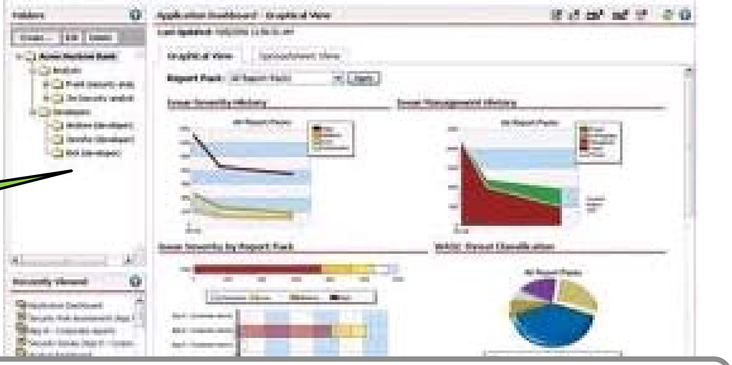




Security issues found and remediated during development!!

Rational AppScan Source Edition

Rational Team Concert



Rational AppScan Enterprise Edition's dashboarding capabilities gives deep insight to prevalence of risks, trends and analysis of types and source of security defects

Rational AppScan Enterprise Edition

A Secure by Design Universe: *Secure QA Testing*

QA team educated on application security and tools

QA teams build test plans for functional, UI and security controls. Rational AppScan Tester Edition used to detect vulnerabilities.

Security educated QA team looks for and detects security issues!!

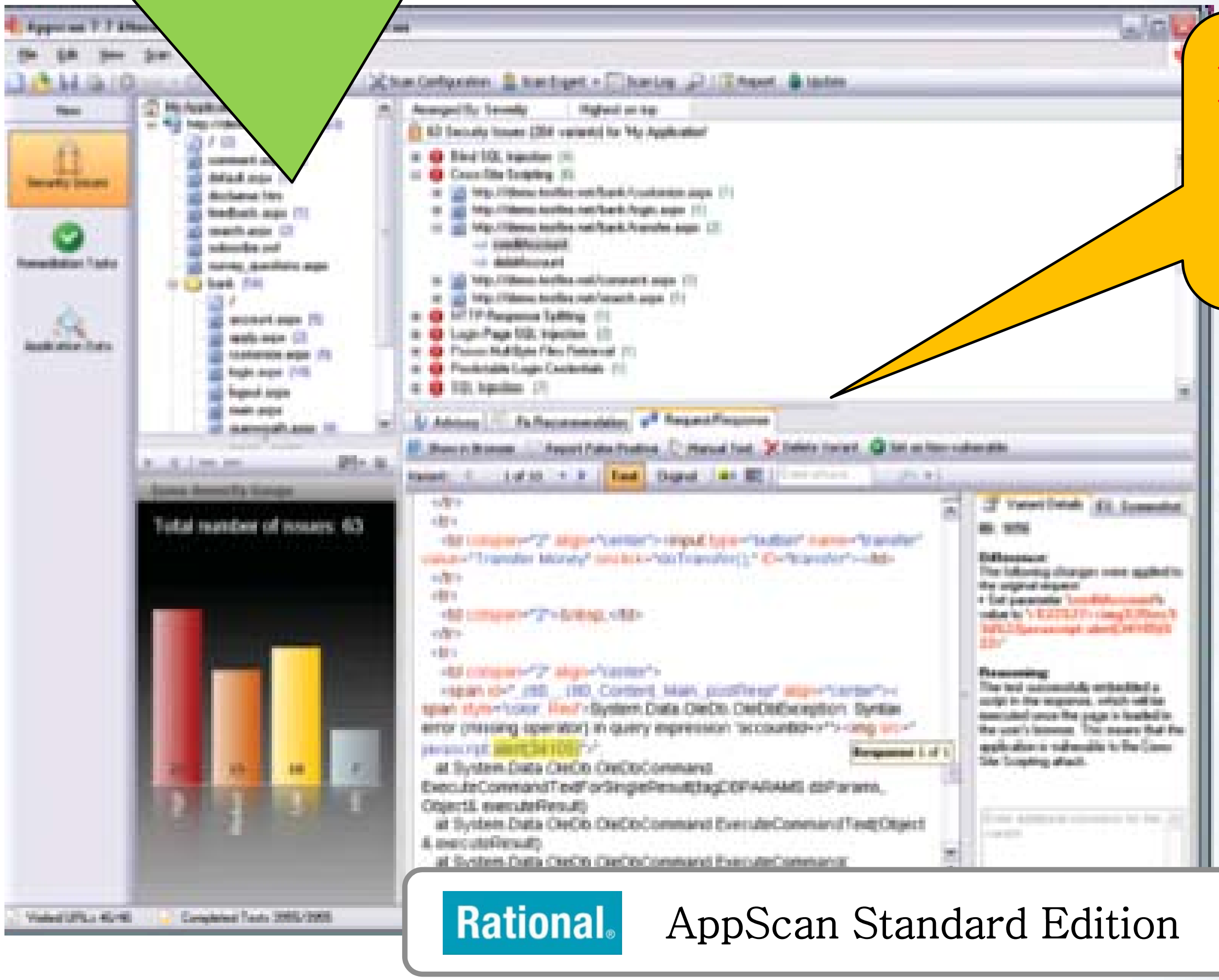
Rational. AppScan Tester Edition

Rational. Quality Manager

QA team locates functional, UI and security defects and logs them into Rational Quality Manager

A Secure by Design Universe: *Secure Deployment*

Rational AppScan Standard Edition is used to verify application prior to deployment



Infrastructure issues in underlying platforms are found and patched!!

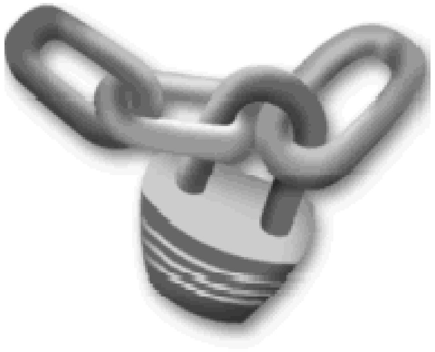
Rational. AppScan Standard Edition

A Secure by Design Universe: *The Success Story*

The Reliable Times Daily

Hackers Foiled! Popular Gaming Console Company Reputation Soars

Earlier this week, hackers attempted to locate security issues in Fun Games Corp. network entertainment unit online gaming application, but failed due to security controls in place. Consumer confidence and profits soar…



The Post

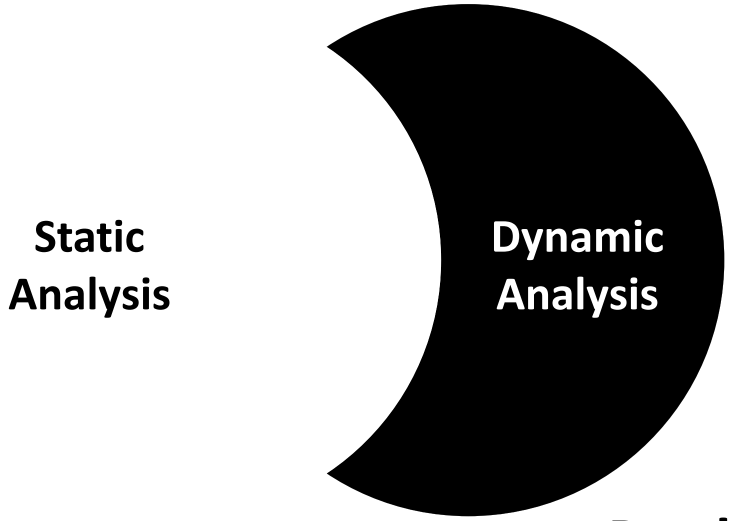
No News is Good News

Another boring news week with no security breaches to report for ABC Motors Corp.

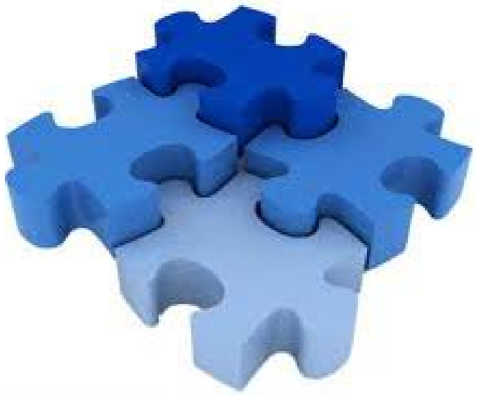
IBM Rational Solutions Institutionalize Secure by Design!

IBM Rational AppScan Imperatives

Maintain Security Leadership

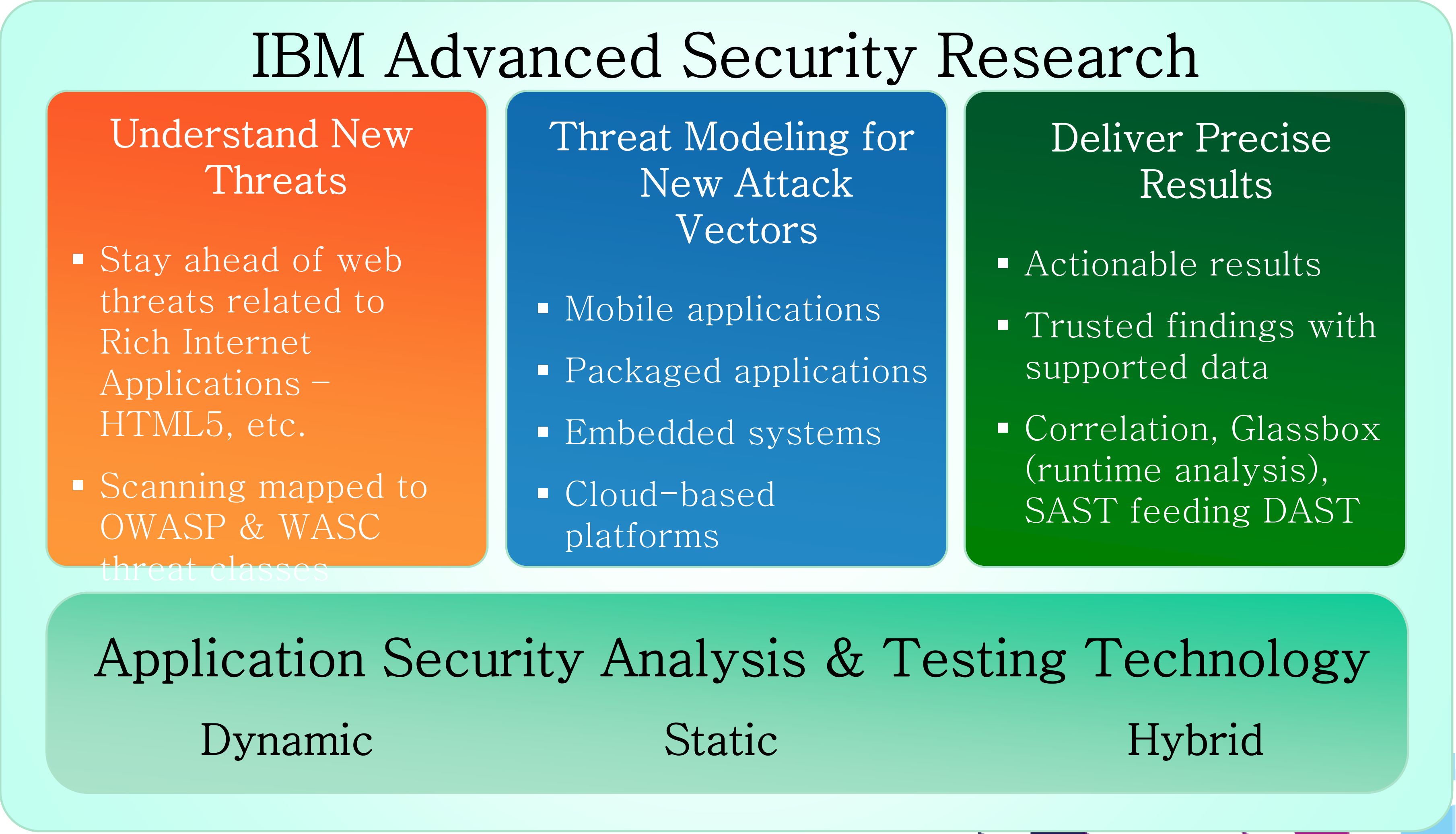


ALM Integrations



Productivity

Maintaining Application Security Leadership



IBM Advanced Security Research

Understand New Threats

- Stay ahead of web threats related to Rich Internet Applications – HTML5, etc.
- Scanning mapped to OWASP & WASC threat classes

Threat Modeling for New Attack Vectors

- Mobile applications
- Packaged applications
- Embedded systems
- Cloud-based platforms

Deliver Precise Results

- Actionable results
- Trusted findings with supported data
- Correlation, Glassbox (runtime analysis), SAST feeding DAST

Application Security Analysis & Testing Technology

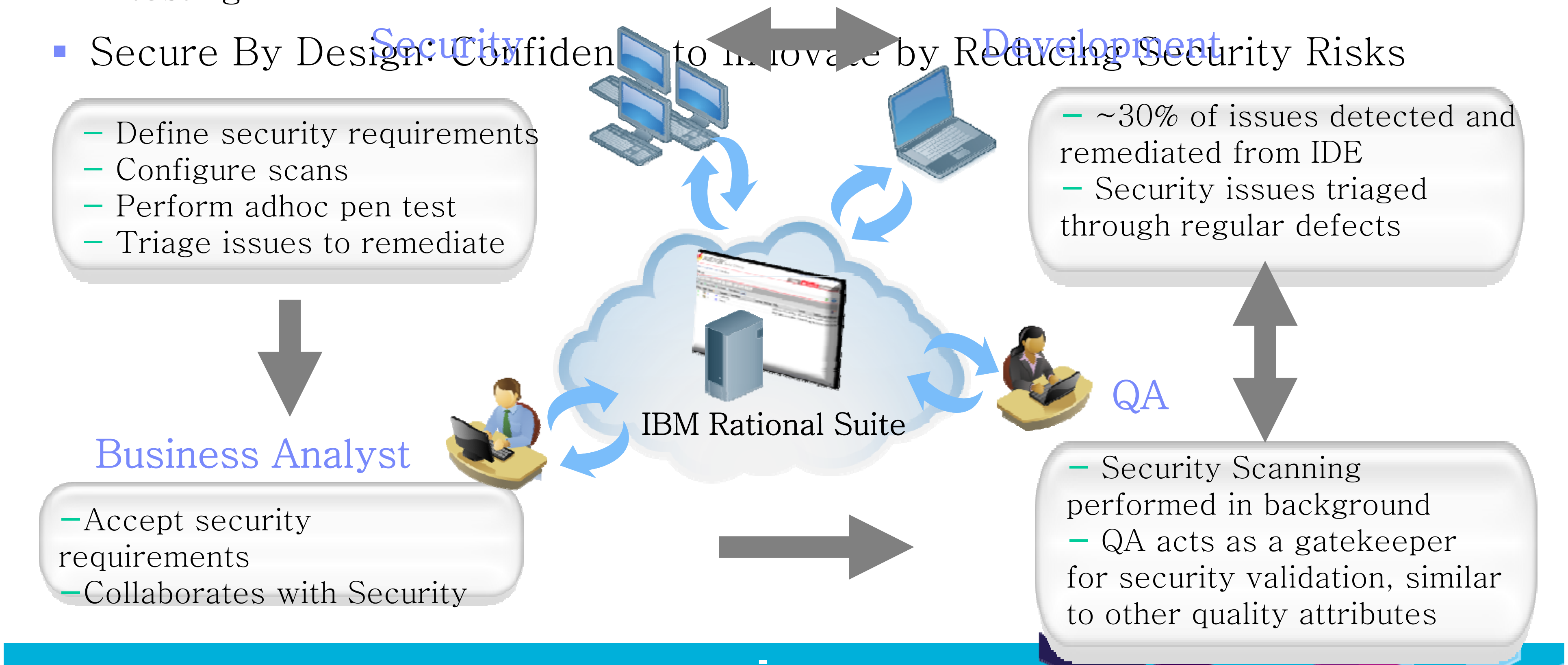
Dynamic

Static

Hybrid

Productivity: Enabling a Quantum Leap

- Security testing and collaborative workflows reduce risk BUT do not create value
  - Application security must evolve to go beyond testing and mitigation
  - Ex: Quality Management does not begin and end with functional or performance testing
- Secure By Design: Confidence to Innovate by Reducing Security Risks



Security:
- Define security requirements
- Configure scans
- Perform adhoc pen test
- Triage issues to remediate

Development:
- ~30% of issues detected and remediated from IDE
- Security issues triaged through regular defects

QA:
- Security Scanning performed in background
- QA acts as a gatekeeper for security validation, similar to other quality attributes

Business Analyst:
- Accept security requirements
- Collaborates with Security

Integration Across the Development Lifecycle

Institutionalize Secure by Design with IBM Rational

Rational

Rational ClearQuest	AppScan Enterprise, Source, Standard Push security defects
Rational Application Developer	**AppScan Source** Run scans and view results in RAD (for developers)
Rational Build Forge	**AppScan Build, Source** Run static & dynamic scans during build time
Rational Team Concert	**AppScan Enterprise, Source** Push security defects
Rational Quality Manager	**AppScan Enterprise, Source** Push security defects

WebSphere

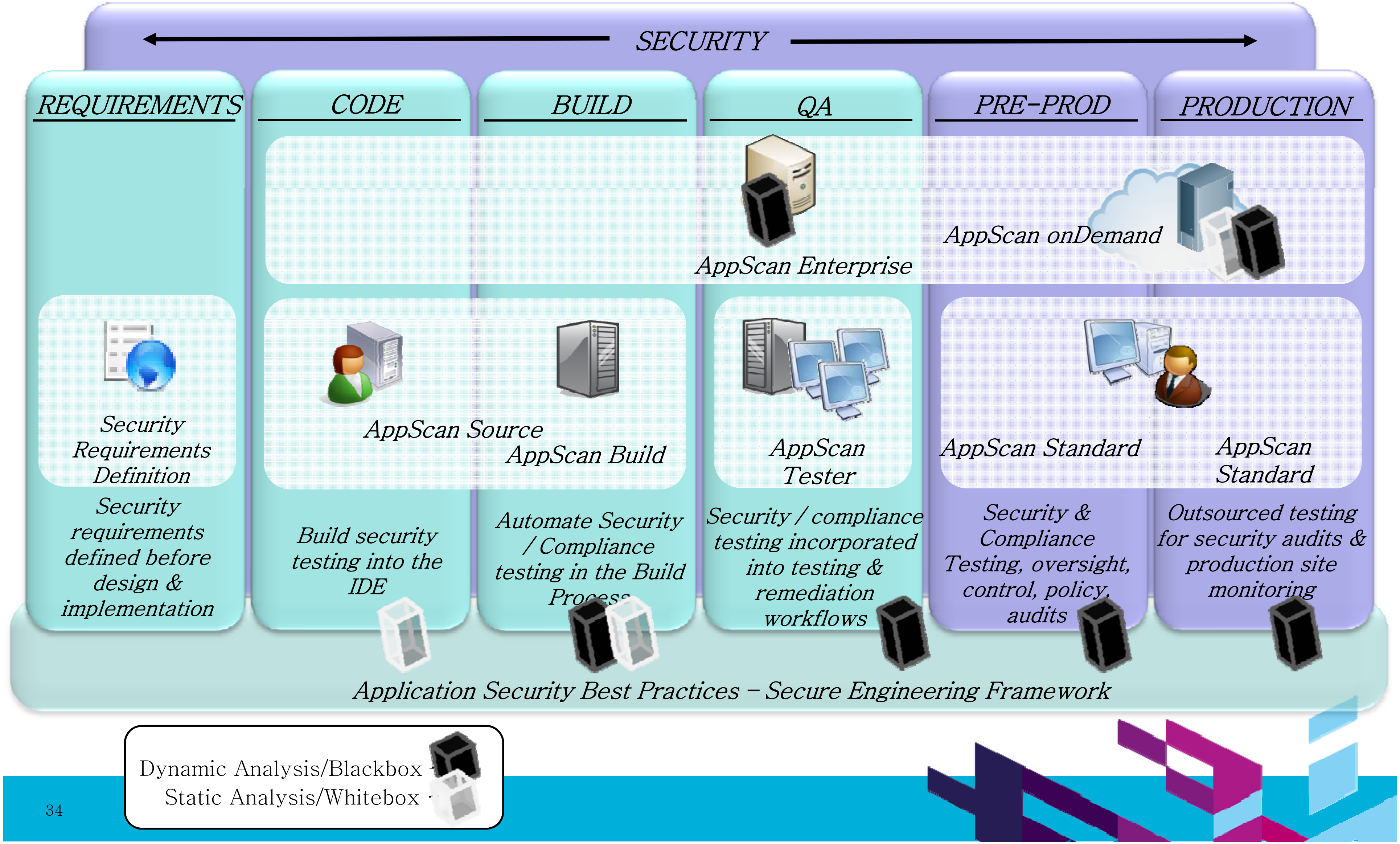
WebSphere Portal	**AppScan Enterprise** Automatic scan of portal-based applications (through remote REST APIs for URL decoding)
WebSphere Commerce	**AppScan Enterprise, Standard** pre-defined scan templates tailored for WSC applications

Tivoli

ISS VPS	**AppScan Standard** Malware scanning for web applications provided by ISS VPS & OrangeFilter API

IBM Rational AppScan Suite

Comprehensive Application Vulnerability Management across SDLC



SECURITY

REQUIREMENTS | CODE | BUILD | QA | PRE-PROD | PRODUCTION

AppScan Enterprise

AppScan onDemand

Security Requirements Definition

AppScan Source

AppScan Build

AppScan Tester

AppScan Standard

AppScan Standard

Security requirements defined before design & implementation

Build security testing into the IDE

Automate Security / Compliance testing in the Build Process

Security / compliance testing incorporated into testing & remediation workflows

Security & Compliance Testing, oversight, control, policy, audits

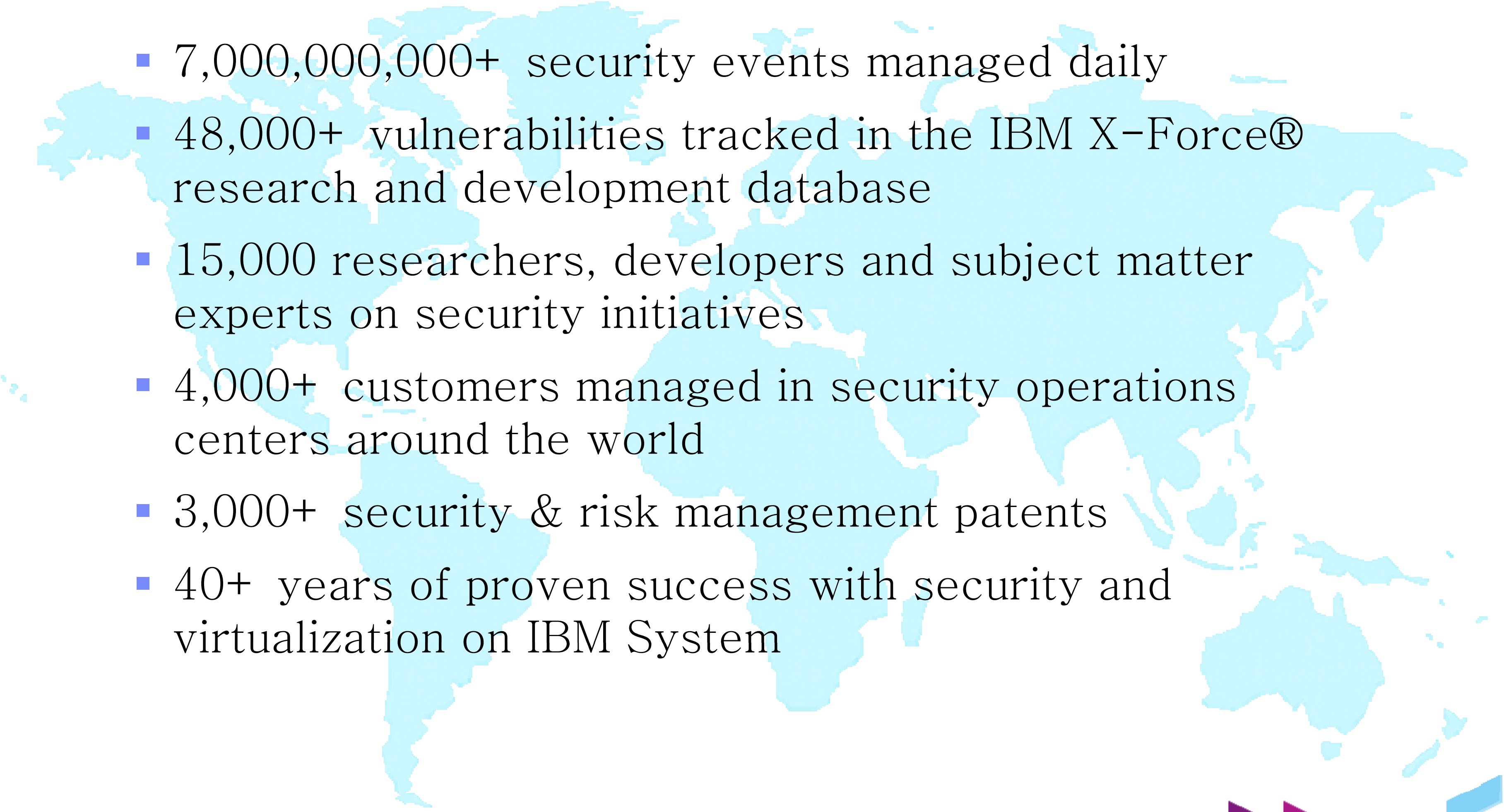
Outsourced testing for security audits & production site monitoring

Application Security Best Practices – Secure Engineering Framework

Dynamic Analysis/Blackbox

Static Analysis/Whitebox

IBM's Commitment and Investment in Security



- 7,000,000,000+ security events managed daily
- 48,000+ vulnerabilities tracked in the IBM X-Force® research and development database
- 15,000 researchers, developers and subject matter experts on security initiatives
- 4,000+ customers managed in security operations centers around the world
- 3,000+ security & risk management patents
- 40+ years of proven success with security and virtualization on IBM System

Questions

www.ibm.com/software/rational

Trademarks and Notes

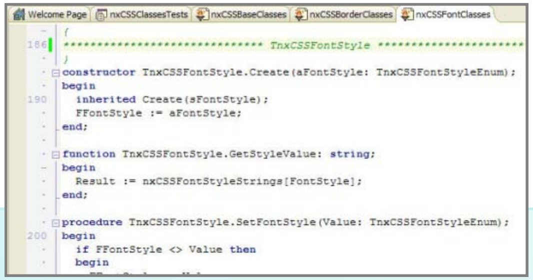
Backup

Security Testing Technologies...

Combination Drives Greater Solution Accuracy

Static Code Analysis (Whitebox)

- Scanning source code for security issues



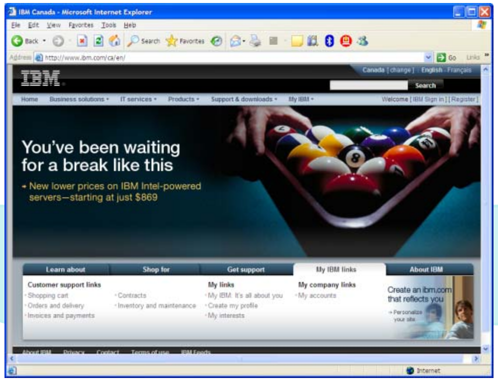
```
{
****************************** TnxCSSFontStyle ******************************
}
constructor TnxCSSFontStyle.Create(aFontStyle: TnxCSSFontStyleEnum);
begin
  inherited Create(sFontStyle);
  FFontStyle := aFontStyle;
end;

function TnxCSSFontStyle.GetStyleValue: string;
begin
  Result := nxCSSFontStyleStrings[FontStyle];
end;

procedure TnxCSSFontStyle.SetFontStyle(Value: TnxCSSFontStyleEnum);
begin
  if FFontStyle <> Value then
  begin
```

Dynamic Analysis (Blackbox)

- Performing security analysis of a compiled application


IBM Canada - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.ibm.com/ca/en/
Go Links
IBM
Canada [change] English Français
Search
Home Business solutions IT services Products Support & downloads My IBM
Welcome [IBM Sign in] [Register]
Learn about
Shop for
Get support
My IBM links
About IBM
About IBM Privacy Contact Terms of use IBM Feeds
Internet

You've been waiting for a break like this

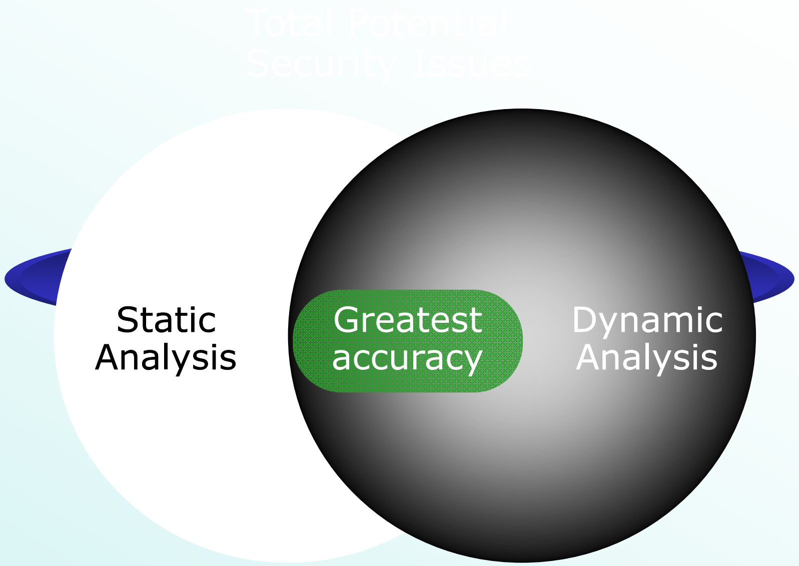
New lower prices on IBM Intel-powered servers—starting at just $869

Customer support links
- Shopping cart
- Orders and delivery
- Invoices and payments
- Contracts
- Inventory and maintenance

My links
- My IBM: It's all about you
- Create my profile
- My interests

My company links
- My accounts

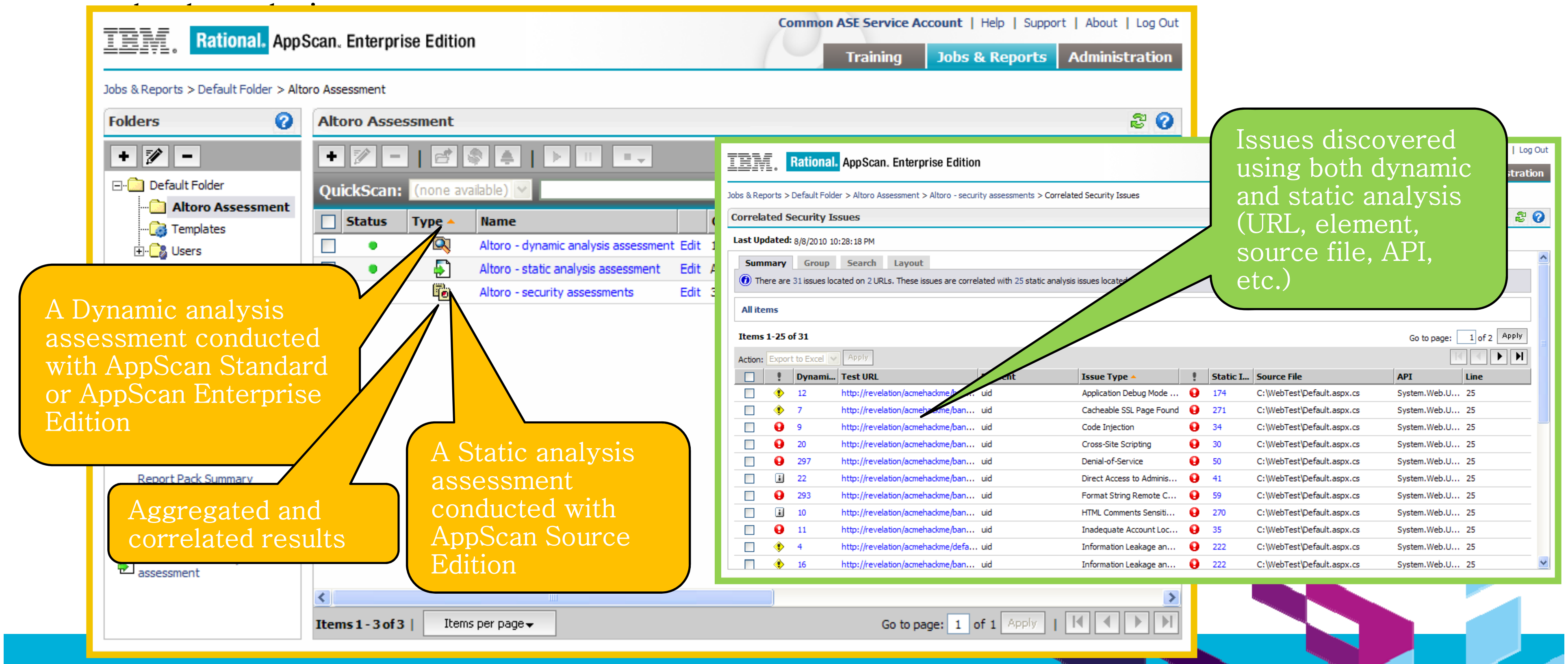
Create an ibm.com that reflects you
- Personalize your site



Hybrid Analysis

Automated Correlation of Static and Dynamic analysis results

- Why Correlate?
  - Validate results, e.g. validate an issue discovered using static analysis with dynamic analysis
  - Help triage and prioritize issues for remediation, e.g. there is much higher confidence that an issue is real and can be exploited if it was discovered using



IBM. Rational. AppScan. Enterprise Edition

Common ASE Service Account | Help | Support | About | Log Out
Training
Jobs & Reports
Administration

Jobs & Reports > Default Folder > Altoro Assessment

Altoro Assessment

QuickScan: (none available)

Status	Type	Name
●		Altoro - dynamic analysis assessment Edit
●		Altoro - static analysis assessment Edit
		Altoro - security assessments Edit

Items 1 - 3 of 3 | Items per page ▾ Go to page: 1 of 1 Apply

IBM. Rational. AppScan. Enterprise Edition

Jobs & Reports > Default Folder > Altoro Assessment > Altoro - security assessments > Correlated Security Issues

Correlated Security Issues

Last Updated: 8/8/2010 10:28:18 PM

There are 31 issues located on 2 URLs. These issues are correlated with 25 static analysis issues located

All items

Items 1-25 of 31

Go to page: 1 of 2 Apply

Action: Export to Excel Apply

□	!	Dynami...	Test URL	...ent	Issue Type	!	Static I...	Source File	API	Line
□	!	12	http://revelation/acmehackme/	uid	Application Debug Mode ...	!	174	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	7	http://revelation/acmeh...me/ban...	uid	Cacheable SSL Page Found	!	271	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	9	http://revelation/acmehackme/ban...	uid	Code Injection	!	34	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	20	http://revelation/acmehackme/ban...	uid	Cross-Site Scripting	!	30	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	297	http://revelation/acmehackme/ban...	uid	Denial-of-Service	!	50	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	i	22	http://revelation/acmehackme/ban...	uid	Direct Access to Adminis...	!	41	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	293	http://revelation/acmehackme/ban...	uid	Format String Remote C...	!	59	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	i	10	http://revelation/acmehackme/ban...	uid	HTML Comments Sensiti...	!	270	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	11	http://revelation/acmehackme/ban...	uid	Inadequate Account Loc...	!	35	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	4	http://revelation/acmehackme/defa...	uid	Information Leakage an...	!	222	C:\WebTest\Default.aspx.cs	System.Web.U...	25
□	!	16	http://revelation/acmehackme/ban...	uid	Information Leakage an...	!	222	C:\WebTest\Default.aspx.cs	System.Web.U...	25

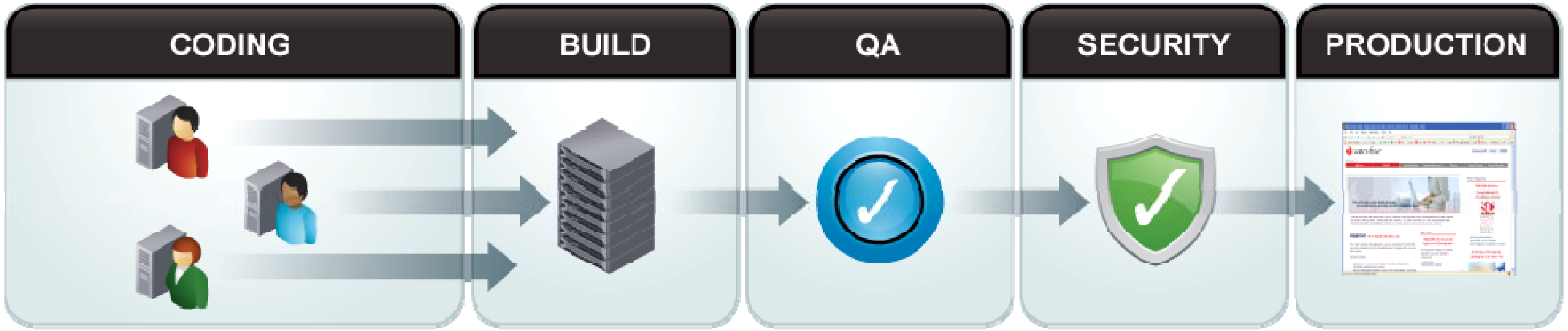
A Dynamic analysis assessment conducted with AppScan Standard or AppScan Enterprise Edition

A Static analysis assessment conducted with AppScan Source Edition

Aggregated and correlated results

Issues discovered using both dynamic and static analysis (URL, element, source file, API, etc.)

Integrating the Silos – Development, QA & Operations



Actionability

- Make scan information consumable by stakeholders and tools

Workflow

- Prioritization of security defects
- Remediation within standard development process

Enterprise Security Intelligence

- Application risk provides context to enterprise risk
- Application vulnerabilities enable custom protection

Application Security Analysis & Testing Technology

Correlation Glassbox

A Path to Secure Applications

Application & resource protection in operation

Secure application development across design, code, build, test phases

Web Application Protection
IBM Security

Identity & Access Management
IBM Security

Secure Web Services
WebSphere. software

Production-Site Monitoring
Rational. software

Deploy Application

Final Security Audit
Rational. software

Vulnerability Assessment Functioning Application
Rational. software

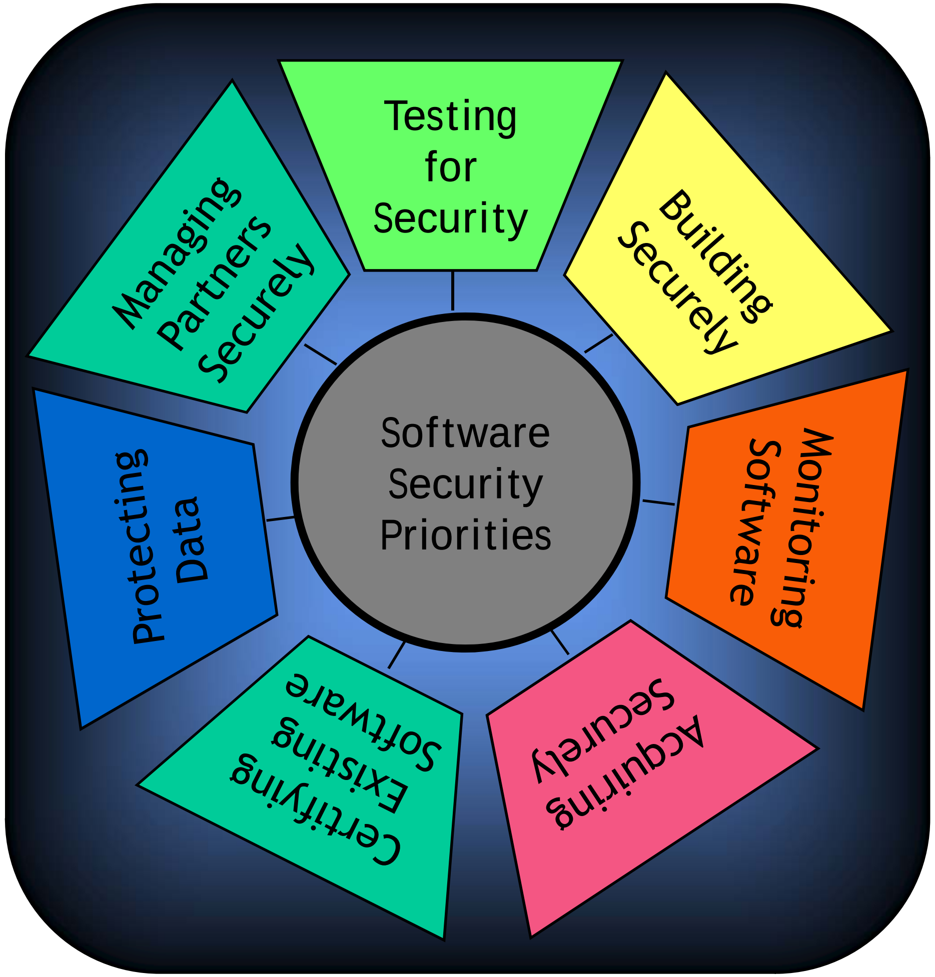
Vulnerability Assessment of Source Code
Rational. software

Policy & Requirements Definition
Rational. software

Risk Assessment
IBM Security Services

Operational Risk Mgmt
Proactive Risk Mitigation

The Risks of Indecision or Unbalanced Decisions



> *"It happens, indeed, to be the case that a thing to which movement this way and that is equally inappropriate is obliged to remain at the center."*
>
> \- **Aristotle**
> *De Caelo*, Book II