Innovate2011

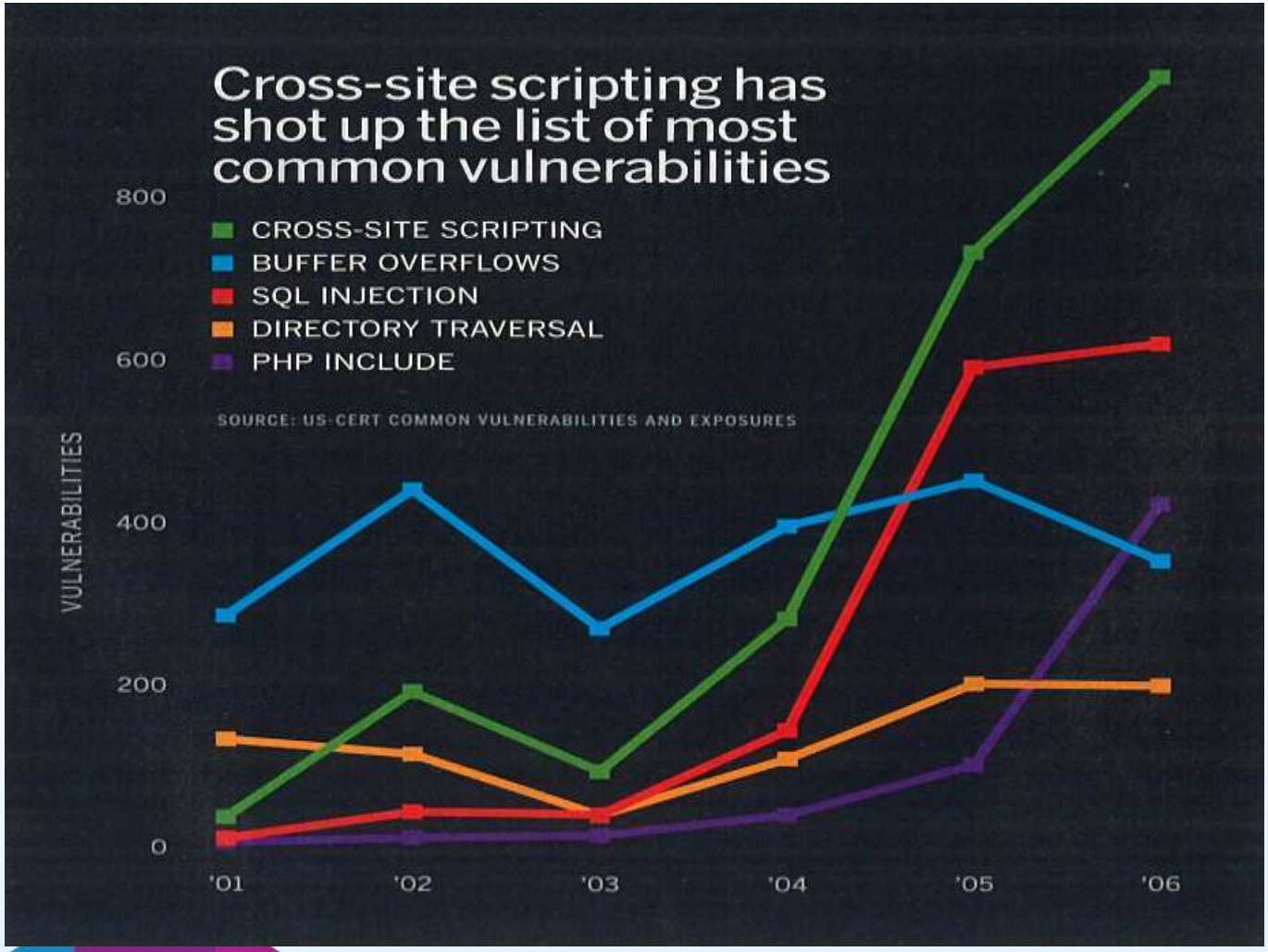
The Premier Software and Product Delivery Event

Software. Everyware.

Asegurando sus Aplicaciones: Hackeo Ético

Miguel A. Dzay Lemus
Rational IT Specialist
IBM Software México, Rational

Los Hackers se están Enfocando en las Aplicaciones Web

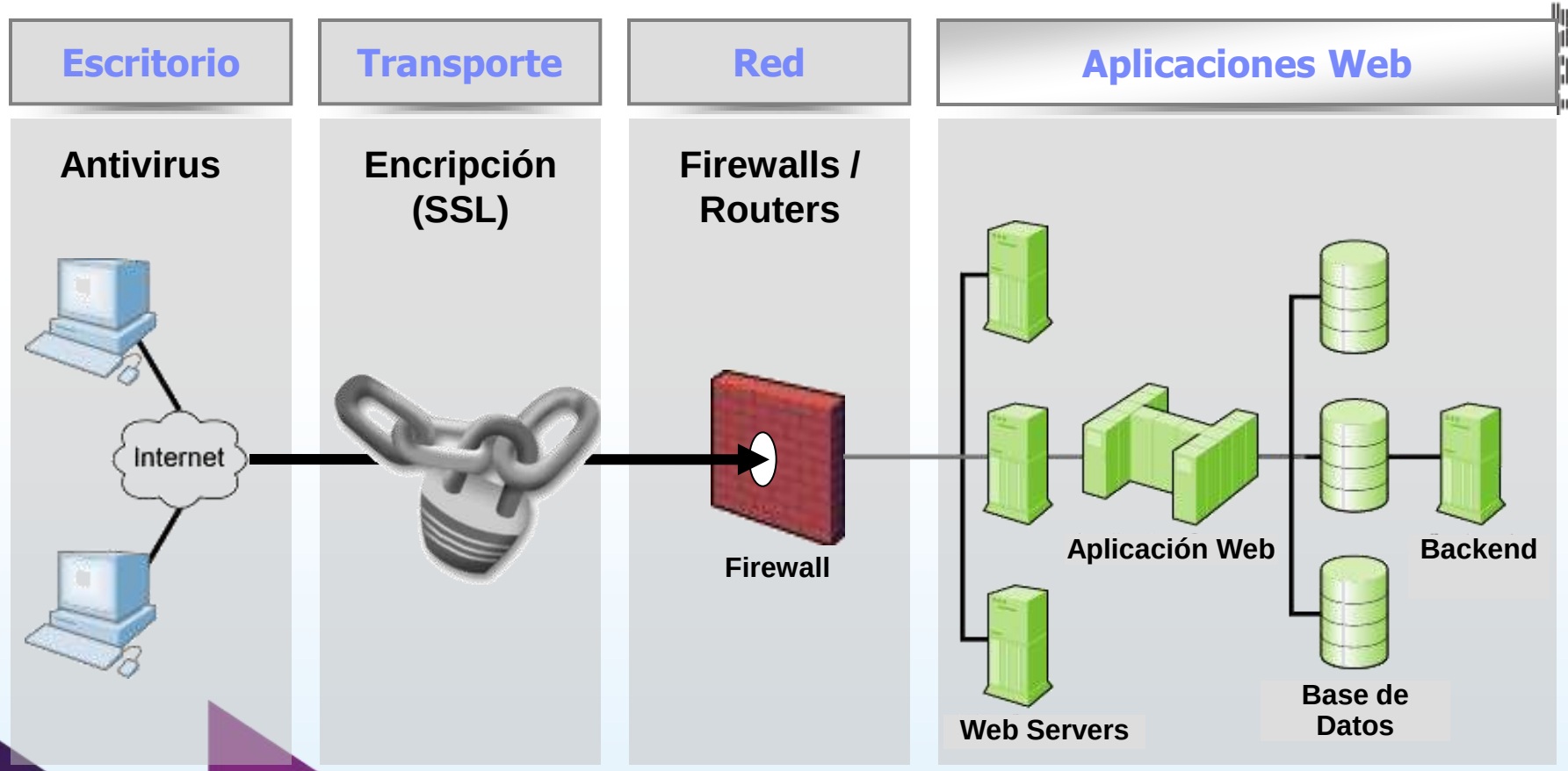


Motivadores del Mercado

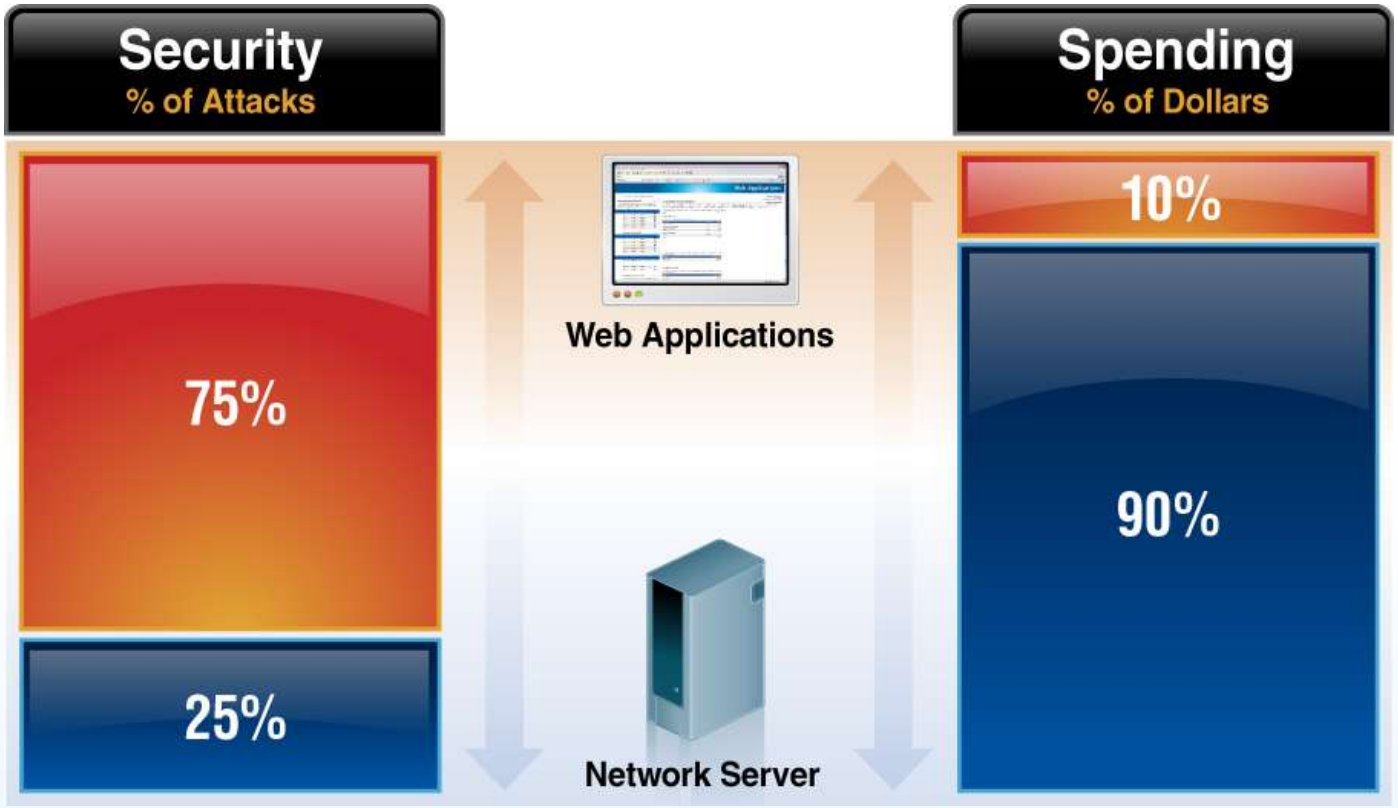
- **Cumplimiento de Regulaciones**
  - eCommerce: PCI-DSS, PA-DSS
  - Sarbanes Oxley
  - ISO 27001
  - ISO 27002
  - y más....

Hackers Break Into Playstation Network 2011

La Seguridad de Aplicaciones Requiere de un Acercamiento Diferente



La Realidad



75% De todos los ataques están dirigidos al Web

2/3 De todas las aplicaciones son vulnerables

**Gartner

Costos de las diferentes fuentes de defectos

Costos no tomados en cuenta:

- Notificar al cliente
- Multas
- Demandas
- Daño en la reputación
- Erosión de la Brand
- Costo de Reparación

¿Por que son las aplicaciones tan vulnerables?

- A los desarrolladores se les exige que entreguen funcionalidad en tiempos y costos pero no se les pide que desarrollen aplicaciones segura
- Los desarrolladores no tienen practicas de desarrollo seguro
- Las aplicaciones son cada ves mas complicadas y con mas interconexiones

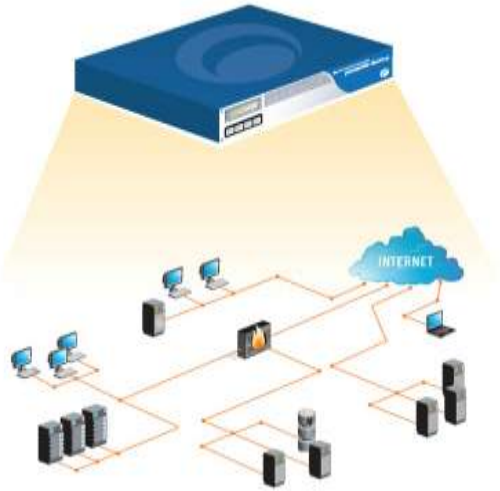
Volúmenes grandes de aplicaciones continúan siendo liberadas llenas de defectos de seguridad...

¿Como funciona Rational AppScan?

Automatiza la detección y Análisis de Vulnerabilidades en Aplicaciones Web

1 → 2 → 3

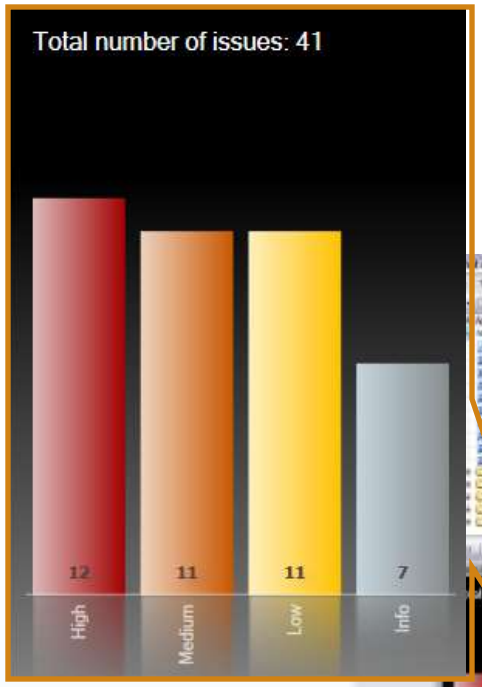
Revisa las Aplicaciones

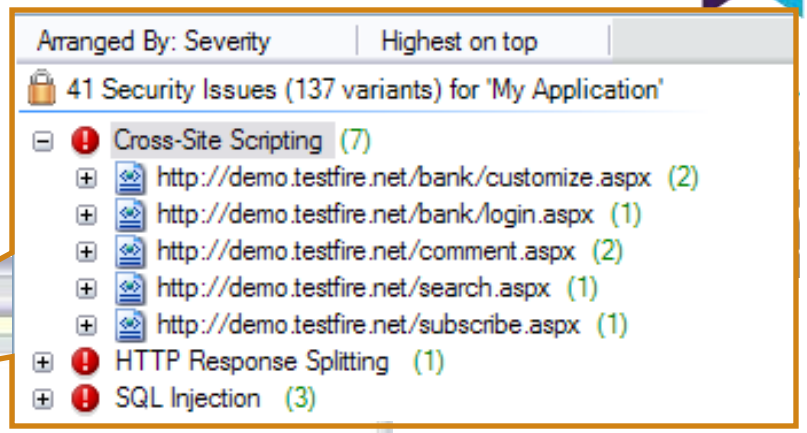


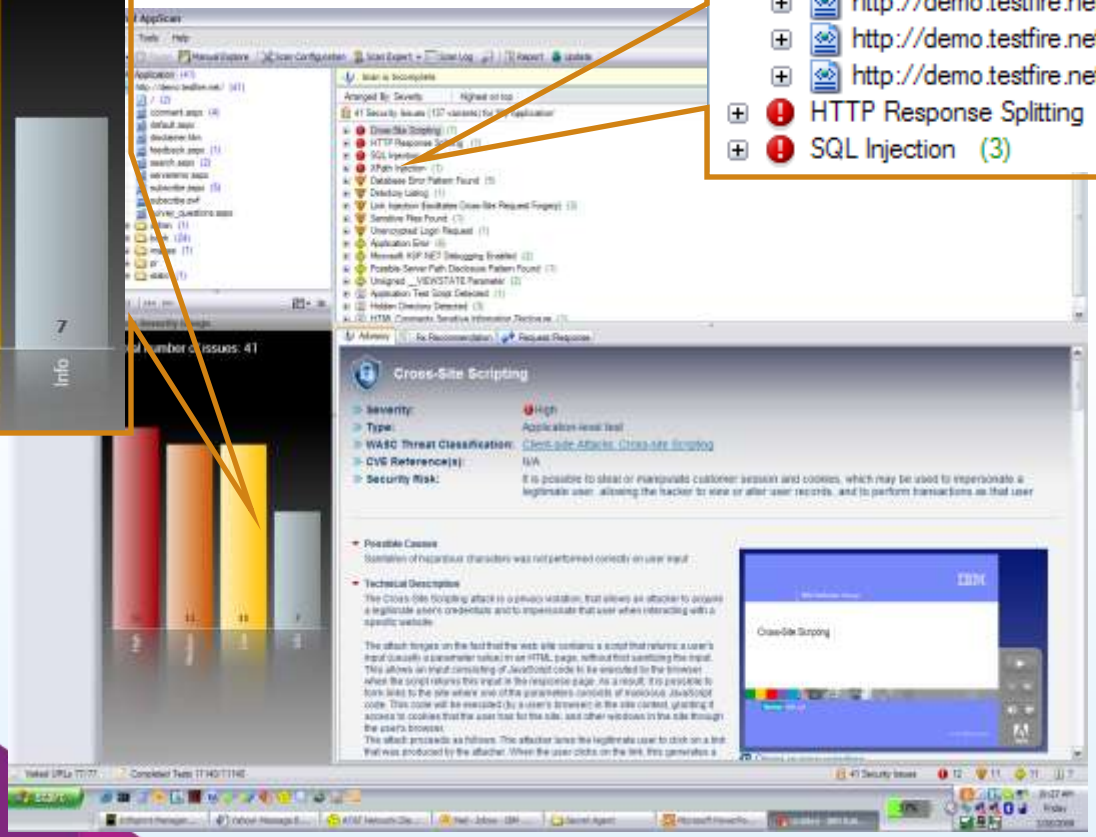
Analiza
(identifica problemas)

Reporta
(detalles & acciones a tomar)

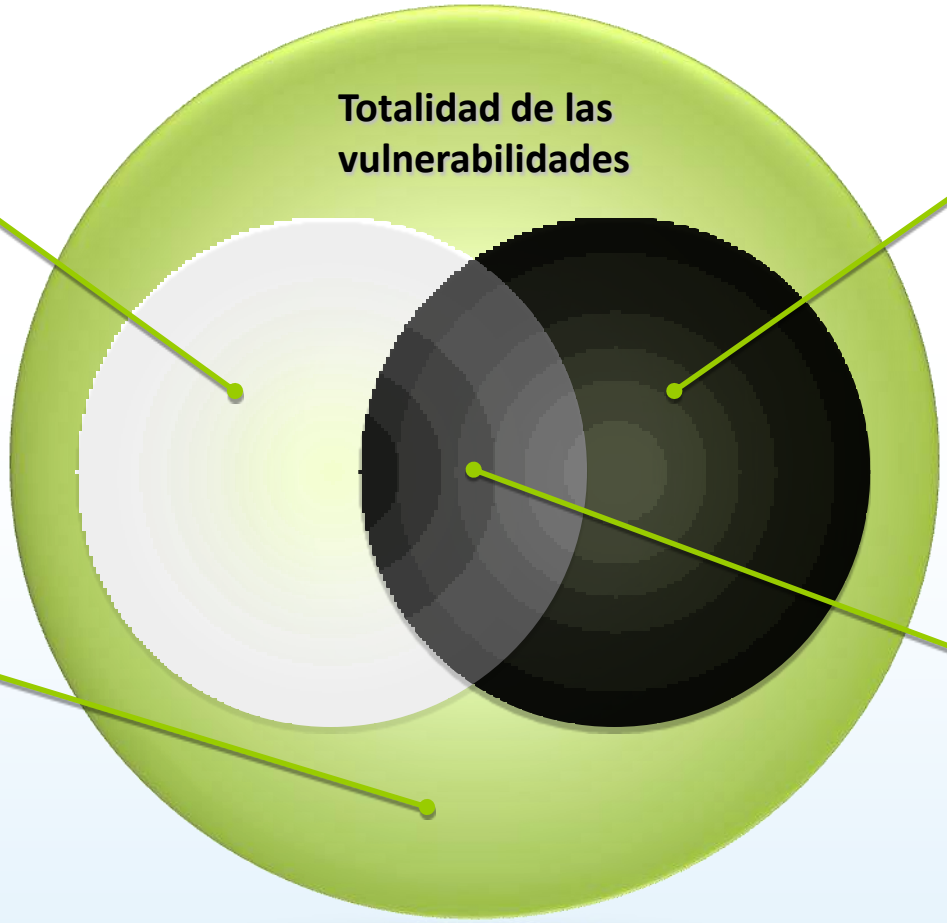
Resultados Fácil de Entender – Problemas y Prioridades







DAST y SAST – Cobertura de issues



Análisis Estático

- Null pointer dereference
- Threading issues
- Code quality issues
- Issues in dead code
- Insecure crypto functions
- Issues in back-end application code
- Stored vulneabilities
- Complex SQL injection

Análisis Dinámico

- Environment configuration issues
- Patch level issues
- Runtime privileges issues
- Authentication issues
- Protocol parser/serializer issues
- Session management issues
- Issues in external 3rd party web components
- Cross-site request forgery
- Malware analysis

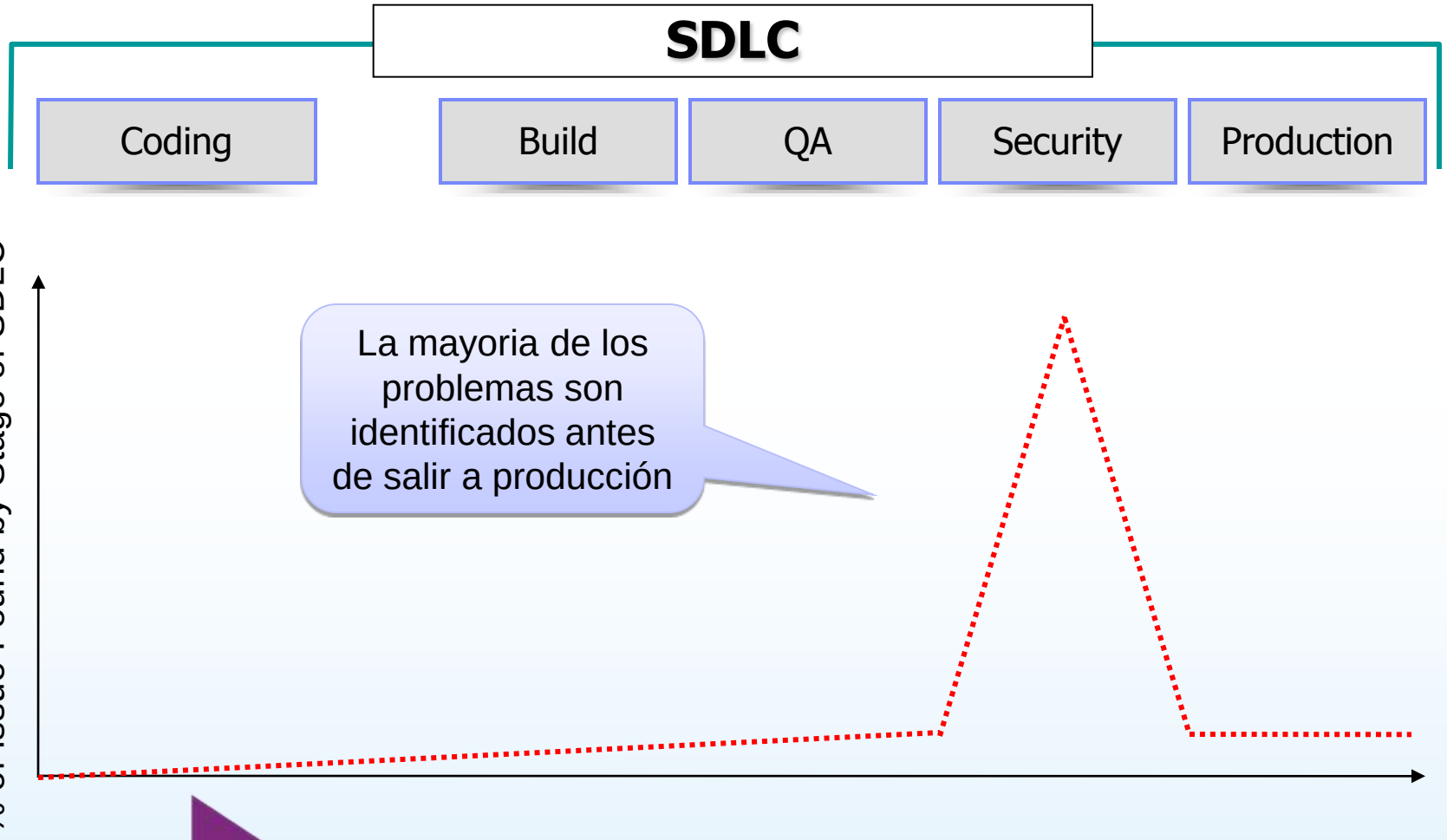
Assesment Manual

- Business logic issues

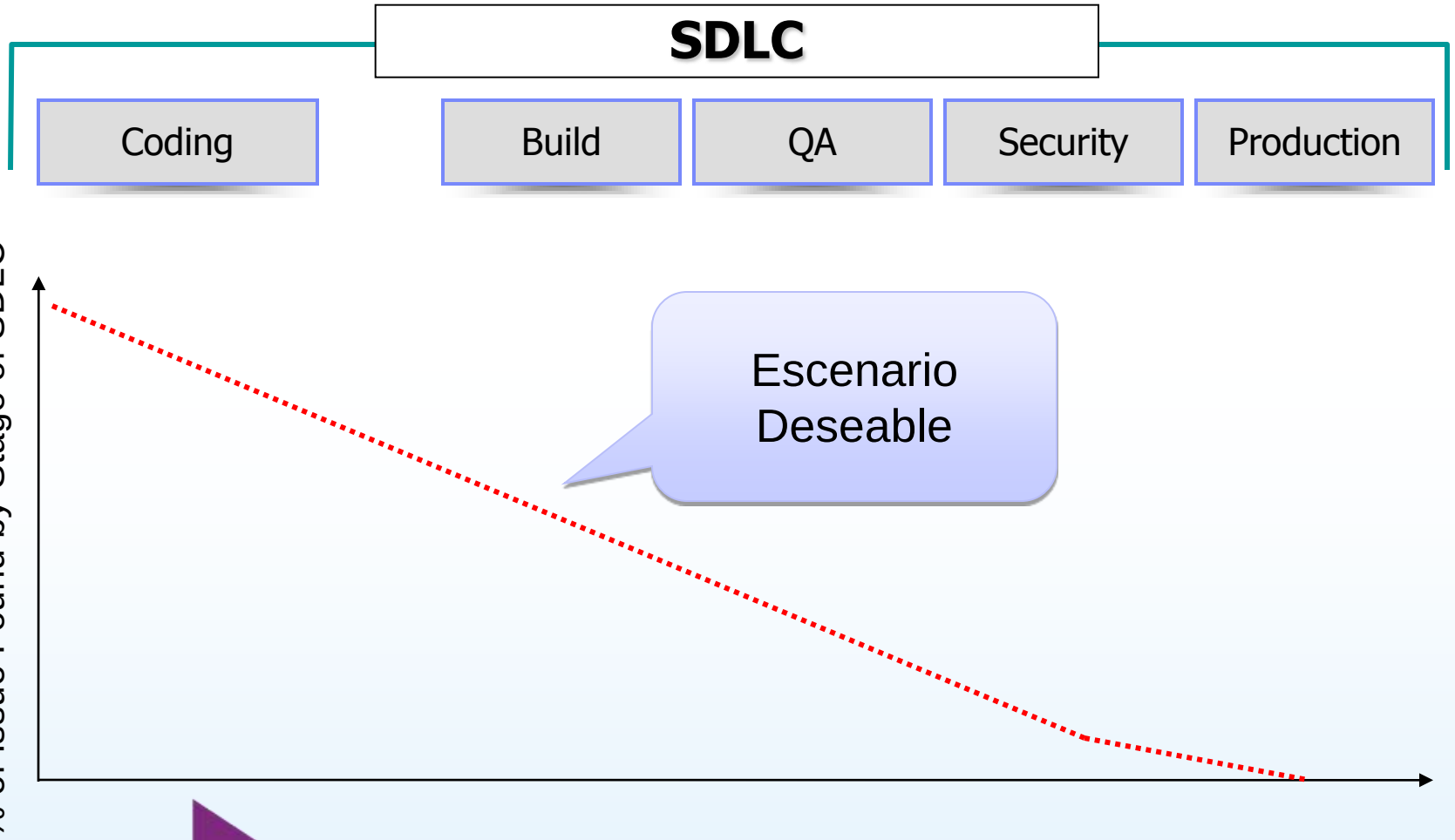
Dinámico y Estático

- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- XPath Injection
- Path Traversal
- Buffer Overflows
- Format String Issues

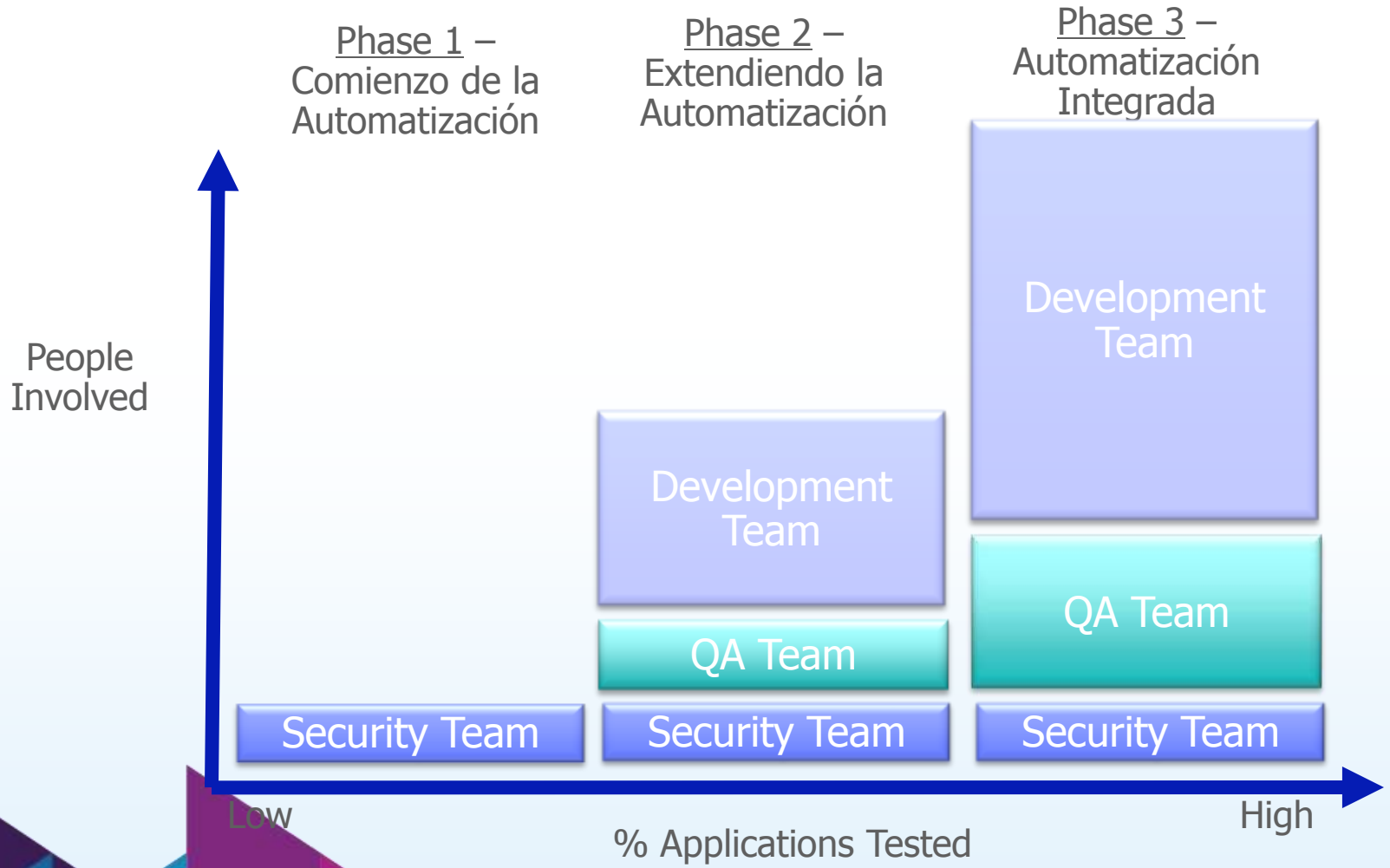
Pruebas de Seguridad en el Ciclo de Pruebas



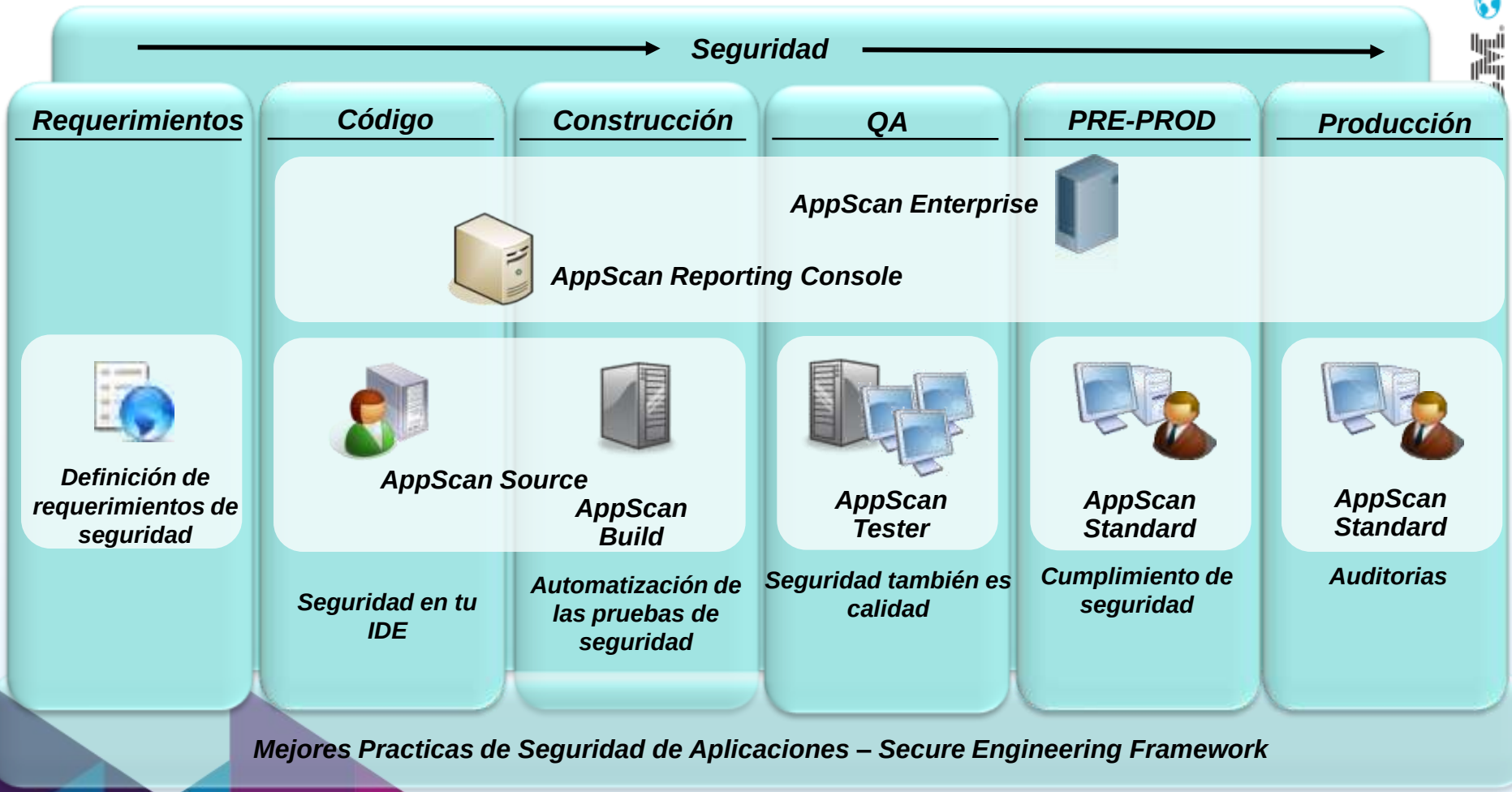
Pruebas de Seguridad como parte del Ciclo de Desarrollo



La Necesidad de Escalar las Pruebas de Seguridad

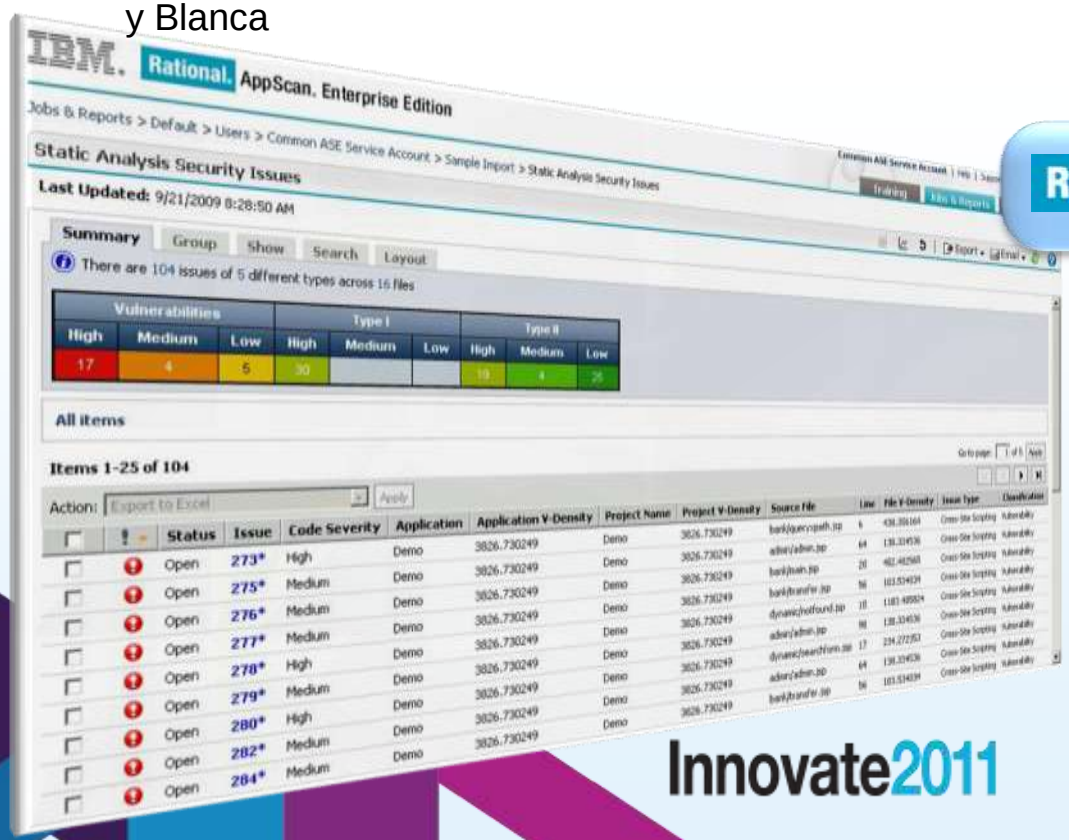


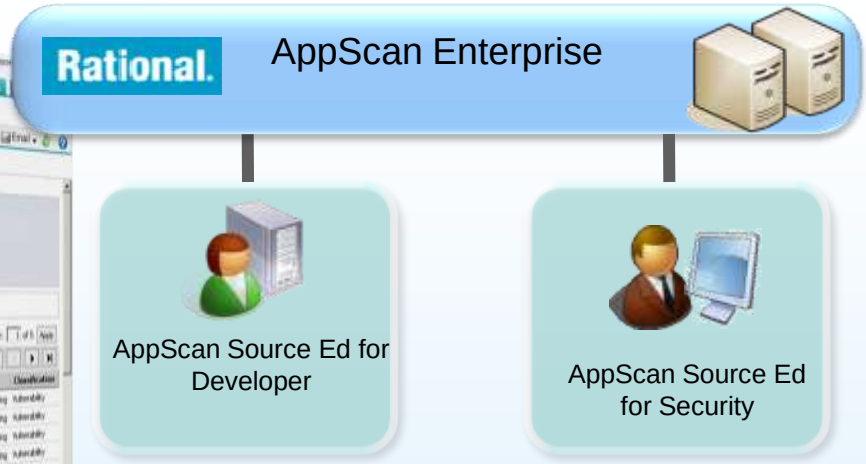
Ecosistema IBM Rational AppScan



Issue Correlation

- **Integración con AppScan Enterprise**
  - AppScan Source es capaz de exportar directamente hacia la consola de AppScan Enterprise para la correlacion de resultados de Caja Negra y Caja Blanca
  - Provee un dashboard centralizado de seguridad y un motor de reporteo de tendencia para Caja Negra y Blanca

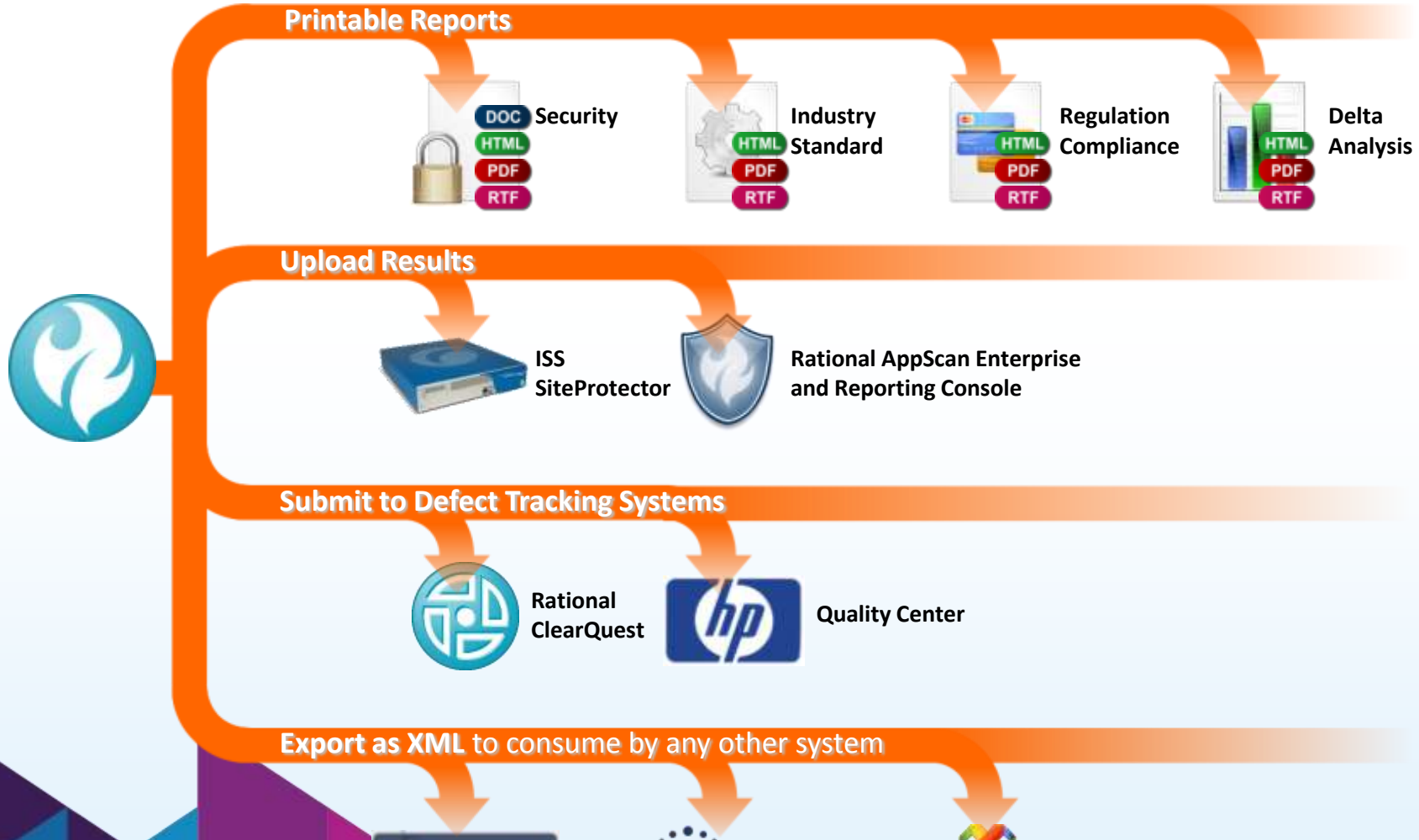




Software. Everyware.

www.ibm.com/software/mx/rational

Capacidades de Reporteo e integracion con DAST



Cross-Site Scripting

URL: http://local/altoro/comment.aspx

Entity: comment.aspx

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

High

CVSS Metrics Scoring (8)

Base

Temporal

Environmental

The script AppScan injected seems to be included in the response. If the screen shot below shows a simulation of the pop-up that the injected script produced, this is proof that the application is vulnerable to Cross-Site Scripting. If not, to verify this vulnerability: 1) Open the Request/Response tab and click Show in Browser, and see if a pop-up appears. (Note that some script syntaxes are browser specific, so if the injected alert doesn't pop up, try a different browser (View Source > Save As...). 2) Check the validity of the alert script(s) in the raw test response.

Rendered Test Response

Click to View Full Size