



¿Cómo mejorar la seguridad de las aplicaciones?

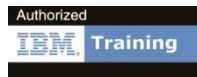
Alberto Escribano García- Jefe De División De Protección Informática
Canal de Isabel II
aescribano@gestioncanal.es

Ariel Súcari – Country Manager
Itera
ariel.sucari@iteraprocess.com

itera
it & business process

Canal
de Isabel II *gestión*

Factores para elevar la calidad



Todos reconocemos la importancia de tener un equipo de trabajo de calidad, motivado pero

Personas



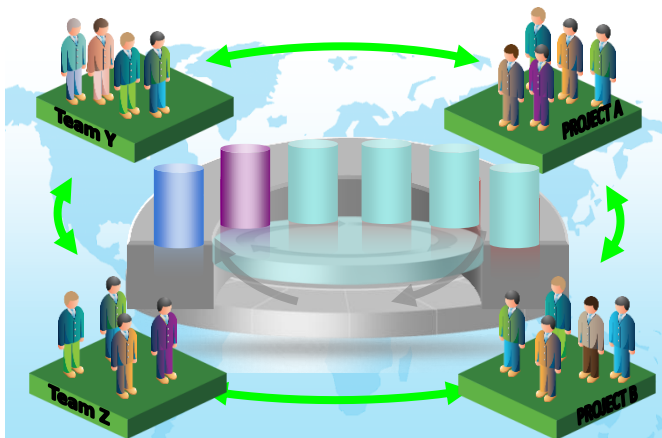
Tecnología

Procesos

Mejora Iterativa de Procesos



Soluciones

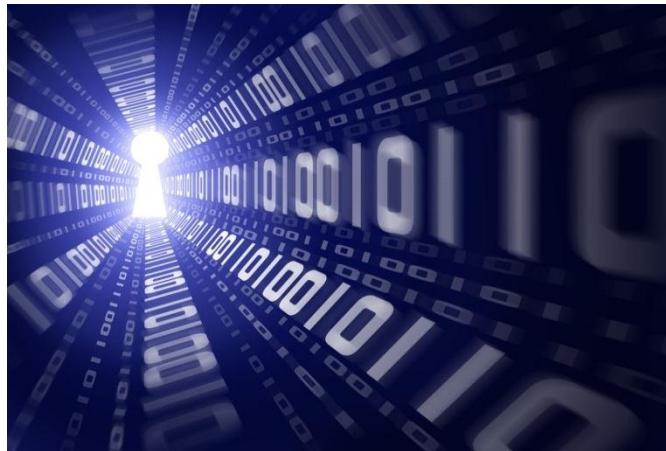


Ciclos de vida de desarrollo:

- Definición de procesos ágiles
- Automatización de procesos con Rational Team Concert
- Formación en procesos y herramientas
- Especialistas en: Rational ClearCase, ClearQuest, Doors, Quality Manager, Software Architect, RAD i y z Series.
- Websphere Portal y HATS

Desarrollo seguro de aplicaciones:

- Análisis de riesgos y vulnerabilidades
- Auditorías de código seguro
- Adaptación de procesos
- Tablero de control de vulnerabilidades
- Implantación de Rational Appscan

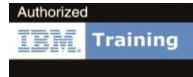


Soluciones de formación



Cursos Presenciales:

- PMP, RMP, ACP
- CMMI V1.3
- CEH V7, CHFI, ECSP, ECSA
- Lead Auditor ISO 27001, 20000
- ITIL & ITIL Expert
- Cobit
- TOGAF
- Rational
- BPM
- Cloud Computing



Cursos LIVE ONLINE:

- ITIL Foundation, Expert



Algunos clientes



Instituto Nacional
de Tecnologías
de la Comunicación

TELVENT



indra



Las 20 marcas mas valiosas del mercado



<http://www.brandfinance.com>

Las 20 marcas mas valiosas del mundo

Rank 2012	Rank 2011	Brand	Industry	Domicile	Brand Value 2012	Brand Rating 2012	Enterprise Value 2012	Brand Value / Enterprise Value 2012 (%)	Brand Value 2011	Enterprise Value 2011	Brand Value / Enterprise Value 2011 (%)	Brand Rating 2011
1	8	Apple	Technology	United States	70,605	AAA+	350,257	20%	29,543	244,382	12%	AAA
2	1	Google	Technology	United States	47,463	AAA+	155,895	30%	44,294	143,016	31%	AAA+
3	2	Microsoft	Technology	United States	45,812	AAA+	165,151	28%	42,805	165,725	26%	AAA+
4	4	IBM	Technology	United States	39,135	AA+	241,208	16%	36,157	189,718	19%	AA+
5	3	Walmart	Retail	United States	38,319	AA	155,189	25%	36,220	154,325	23%	AA
6	18	Samsung	Miscellaneous Manufacture	South Korea	38,197	AAA-	199,331	19%	21,511	113,327	19%	AA+
7	7	General Electric	Miscellaneous Manufacture	United States	33,214	AA+	468,287	7%	30,504	475,066	6%	AA+
8	16	Coca Cola	Beverages	United States	31,082	AAA+	83,696	37%	25,807	69,508	37%	AAA+
9	5	Vodafone	Telecommunications	United Kingdom	30,044	AAA+	189,232	16%	30,674	192,456	16%	AAA+
10	32	Amazon	Technology	United States	28,665	AA+	94,398	30%	17,780	64,132	28%	AA
11	10	AT&T	Telecommunications	United States	28,379	AA+	235,495	12%	28,884	235,987	12%	AA+
12	12	Verizon	Telecommunications	United States	27,616	AA	203,306	14%	27,293	381,093	7%	AA
13	11	HSBC	Banks	United Kingdom	27,597	AAA	122,741	22%	27,632	171,163	16%	AAA
14	n/a	NTT	Miscellaneous Manufacture	Japan	26,324	AAA-	359,332	7%	26,927	275,617	10%	AA+
15	14	Toyota	Automobiles	Japan	24,461	AA	209,855	12%	26,152	204,864	13%	AA+
16	9	Wells Fargo	Banks	United States	23,229	AA+	133,473	17%	28,944	136,069	21%	AA+
17	6	Bank of America	Banks	United States	22,910	AA+	50,527	45%	34,076	133,551	26%	AAA-
18	17	McDonald's	Restaurants	United States	22,230	AAA	102,389	22%	21,842	89,595	24%	AAA
19	30	Shell	Oil&Gas	Netherlands	22,021	AAA-	238,670	9%	18,605	222,664	8%	AAA-
20	27	Intel	Technology	United States	21,908	AA+	113,435	19%	19,078	92,546	21%	AA+

El oráculo de Omaha

Warren Buffett buys \$10bn IBM stake

Low-tech stock guru Warren Buffett drops long-standing antipathy to IT sector by buying **5% of IBM**, saying he had been 'hit between the eyes' by its competitive advantages



theguardian

INFORMÁTICA | Los expertos recomiendan usar otros navegadores

Microsoft advierte de un fallo de seguridad en Internet Explorer

- El fallo de seguridad afecta a cientos de millones de usuarios
- Los expertos recomiendan utilizar navegadores alternativos

El cibercrimen cuesta 482 millones de euros anuales en España

- Casi 22.000 personas fueron víctimas del cibercrimen en España en 2010
- Supuso alrededor de 388.000 millones de dólares en todo el mundo
- El tipo más común son los virus y el 'malware' contra ordenadores

INTERNACIONAL

Una madre que «hackeó» las notas de sus hijos podría ir a la cárcel

▶ Ahora se enfrenta a 42 años de cárcel o una multa de 90.000 dólares

▶ [COMENTARIOS](#)

▶ [IMPRIMIR](#)

[Sigue ABC.es](#)

[Facebook](#)

ORDENADORES | Antes incluso de su comercialización

Microsoft encuentra virus preinstalados en sus ordenadores en China

[Inicio](#) » [Actualidad](#) » [MuyTV](#) » [Noticias](#) » [Seguridad](#) » [Telefonía móvil](#)

Hackeo sencillo del sistema de desbloqueo facial de Android Jelly Bean

5/08/2012 | [Jesús Maturana](#) | [1 comentario](#)

 Me gusta

 [Twitter](#) 50

 +1 8

Android 4.1 Jelly Bean llega con un sistema de desbloqueo se muestra más seguro que los tradicionales desbloques de reconocimiento facial, fácilmente hackeables incluso con fotografías. En esta ocasión hacen uso de un "*detector de vida*" te pide que parpadees. Pero no es algo que no se pueda realizar de manera artificial en menos de un minuto.

Tanto es así que con 1 minuto de edición de **una fotografía cualquiera** -incluso buscada en Internet- del dueño, se **puede desbloquear un smartphone que esté bloqueado mediante este sistema** de seguridad.

Descifrar WPA2 es posible en menos de un día

30/07/2012 | Jesús Maturana | 0 comentarios

Me gusta

Twitter

45

+1

8



Mac App Store hackeado, aplicaciones gratis para todos

22/07/2012 | Jesús Maturana | 0 comentarios

Me gusta

Twitter 63

+1 4





El cirbercrimen cuesta cada año 114.000 millones de dólares en el mundo y 482 millones de euros en España, según Norton

Gobierno creará dos grupos contra ataques cibernéticos

22 de agosto de 2011 • 09:34 • actualizado a las 09:42

Pentagono admite “importante ataque cibernético” en el que 24 000 documentos fueron “hackeados”

El Pentágono de Estados Unidos (EE.UU.) anunció que el pasado mes de marzo sufrió un “importante ataque cibernético” en el que al menos 24 mil de sus documentos confidenciales fueron descalificados por hackers que presuntamente provenían de un contratista extranjero del Ejército.



Aumentan los ataques cibernéticos en móviles y redes sociales

En un año ha habido 286 millones de nuevas amenazas contra equipos conectados a internet

« Microsoft modifica el logotipo de Windows Phone

La división de televisores de Sony, en la cuerda floja »

McAfee denuncia uno de los mayores ataques cibernéticos conocido hasta la fecha

Elisabeth Rojas | 3/08/2011 | 7 comentarios

Me gusta

Tweet

8

+1

1



La compañía ha revelado en su blog la existencia de uno de los mayores ataques *on-line* conocidos, **cuyos objetivos habrían sido hasta 72 organismos públicos**, entre los que se encuentran gobiernos nacionales y Naciones Unidas. Aunque la lista de víctimas es larga: el Gobierno de Estados Unidos, Taiwán, India, Corea del Sur, Vietnam, Canadá, el Comité Olímpico Internacional, etc.



Centenares de hackers norcoreanos preparados para lanzar ataques cibernéticos



TECNOLOGÍA /

Sony ha contratado a detectives expertos en ataques cibernéticos para localizar a los piratas informáticos

Piratean el principal buscador chino

- ▶ El principal buscador chino por Internet, Baidu, ha sido pirateado este martes por internautas que se identificaron en un mensaje como del "ejército cibernético iraní", informó hoy el "Diario del

 Me gusta

 Tweet


0

 Compartir

Compartir  

Lulzsec y Anonymous se juntan para atacar cibernéticamente

Detenidos cinco activistas por ataques cibernéticos en Reino Unido



Ataque masivo a 75.000 ordenadores

Una empresa descubre uno de los mayores ciberataques, que ha afectado a 2.500 empresas en casi 200 países



Un hacker convierte en profesor universitario de literatura a Conan el Bárbaro



Asalto 'hacker' a Apple

Publican las contraseñas de 26 usuarios de un servidor

GENTE

Scarlett Johansson y el FBI buscan al hacker que robó sus fotos desnuda

Desde el miércoles, circulan en la red fotos de la actriz desnuda hechas con su teléfono móvil



Hackers amenazan con más ataques a Sony

La OTAN tampoco se libra de los ataques de `hackers`

SE DESCONOCE AUTORÍA

El Senado sufre otro ataque 'hacker' en menos de una semana

LA PÁGINA, DE 12 MILLONES DE EUROS, INOPERATIVA TODO EL DÍA

Sabotean la web de la Presidencia española y colocan una foto de Mr.Bean

La [web de la presidencia española de la UE](#) ha sufrido dos ataques hacker durante este lunes, primer día laborable de funcionamiento. En uno de ellos han colocado la foto de Mr Bean. La página, que ha costado 12 millones de euros, ha permanecido caída cerca de 10 horas. [El Gobierno niega el ataque.](#)

esRadio Emisión

PUBLICIDAD



Detenidos tres 'hackers' por
atacar las webs del PSM, el PP y
el programa 'Sálvame'



1.- 15 minutos sin Yahoo

El ataque duró sólo 15 minutos, pero ha pasado a la historia como uno de los más graves llevados a cabo contra webs importantes. El 9 de diciembre de 1997, unos hackers sustituyeron la página principal por otra que decía que todos los visitantes habían sido infectados con un peligroso virus. La solución, según los hackers, era sacar de inmediato al famoso hacker Kevin Mitnick de prisión.

2.- Asalto a La Moncloa

El 11 de agosto de 1999 la web oficial de La Moncloa se vio obligada a cerrar durante aproximadamente una hora, tras el ataque de un grupo de hackers, autodenominado "Alianze". Los hackers bloquearon sus contenidos y sustituyeron los textos por un escrito crítico, y convirtieron al presidente del Gobierno en un demonio.



3.- Espectacular ataque al New York Times

Otro de los ataques hacker más espectaculares de la historia fue el que sufrió el 13 de septiembre del 98 el New York Times. Durante nueve horas estuvo inundado de pornografía y acabó con varios archivos importantes destruidos. El ataque fue la repuesta de los hackers a John Markoff, periodista del prestigioso diario que había publicado un libro contando la vida de Kevin Mitnick.

4.- El CSIC dice no a la guerra

Un ataque muy reciente a un sitio español que causó gran revuelo fue el llevado a cabo contra el Consejo Superior de Investigaciones Científicas (CSIC). El 20 de marzo de este año un grupo de piratas informáticos modificó la portada de la web del CSIC con una imagen de "No a la guerra", y una foto composición que igualaba a Blair y Aznar con Hitler y Franco.



5.- El Columbia en llamas por un día

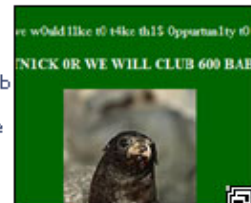
La página web de la NASA recibió uno de sus múltiples ataques hacker el 5 de marzo de 1997. Durante todo un día los usuarios que accedían a la web se encontraban una foto del trasbordador Columbia en llamas. Lo que fue considerado en forma unánime, además de un hackeo, sin duda, un chiste de mal gusto.

la web de Greenpeace

Otro ataque bastante sonado fue el que recibió la web de Greenpeace el 27 de enero de 1999. Aparentemente se trataba sólo de una broma, no fue un ataque ni contra las políticas ni contra la ideología que representa y suscribe la organización ecologista. Los "bromistas" colocaron en lugar de la portada del sitio una foto un tanto obscena. En fin, lo que se dice un hackeo de mal gusto.



6.- Un auténtico "animal" en



7.- Agencia Central de Estupidez o CIA

El 19 de septiembre del 96 la página principal de la CIA fue atacada y sus contenidos cambiados. Los hackers cambiaron inteligencia por estupidez en las siglas de la Agencia. Además, una vez dentro de la página, la intentar volver a tras pulsando el botón del navegador, el usuario acababa en otros sitios hackeados.

de tontas

Las cinco integrantes del famoso grupo calvas. Así es como se atacó a la web oficial del grupo durante todo un fin de semana, del 14 al 16 de noviembre de 1997. El ataque era una protesta contra la "cultura pop", en general y en particular a las Spice Girls. Todo un mal trago para un grupo cuya imagen es tanto o más importante que su música. Además, los hackers se quejaban del "uso que la masa hacía de Internet".



8.-Las Spice Girls, sin un pelo



9.- Apple e Intel se fusionan, según Macworld

La prestigiosa revista Macworld "aseguraba" el 4 de enero de 1999 en su página web que Apple e Intel, dos de las empresas más importantes de la industria informática se iban a fusionar. La sorprendente noticia fue inventada supuestamente por unos hackers suizos que quisieron jugarle una mala pasada al sitio y a sus lectores.

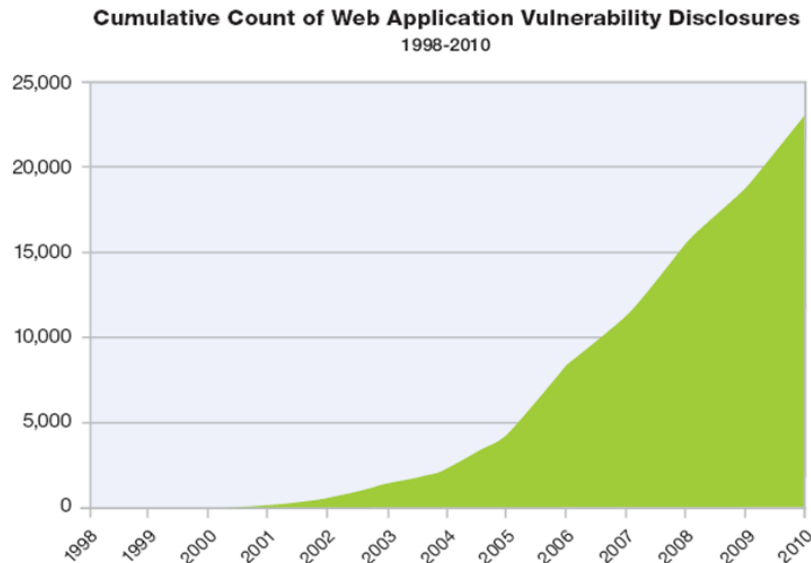
10.- Chicas en bikini y Unicef

Un grupo de hackers llamado "DAMM" penetró el 7 de enero del 98 de forma ilegal en la web de UNICEF. Este ataque se sumó a los muchos realizados por hackers pidiendo la liberación de Mitnick. La página hackeada mostraba a dos chicas en bikini y armadas, que aseguraban estar pasando hambre.



El problema

- **Las vulnerabilidades de las aplicaciones WEB dominan el panorama.**
 - 37% de las vulnerabilidades provienen de aplicaciones WEB (2011 1H)*
 - ~4K nuevas vulnerabilidades son reportadas cada año 2006-2010**



*IBM X-Force 2011 1H Trend & Risk Report

**IBM X-Force 2010 Trend & Risk Report

- Las vulnerabilidades se encuentran en una gran variedad de aplicaciones.

Aplicaciones en desarrollo

- Desarrollo interno
- Desarrollo tercerizado

Aplicaciones en producción

- Desarrolladas internamente
- Adquiridas
- Comerciales

¿Por qué deben ser seguras las aplicaciones?

- Es la cara de la organización
- El lugar donde se hace negocio
- La puerta de entrada de los datos



¿Qué puede ocurrir?

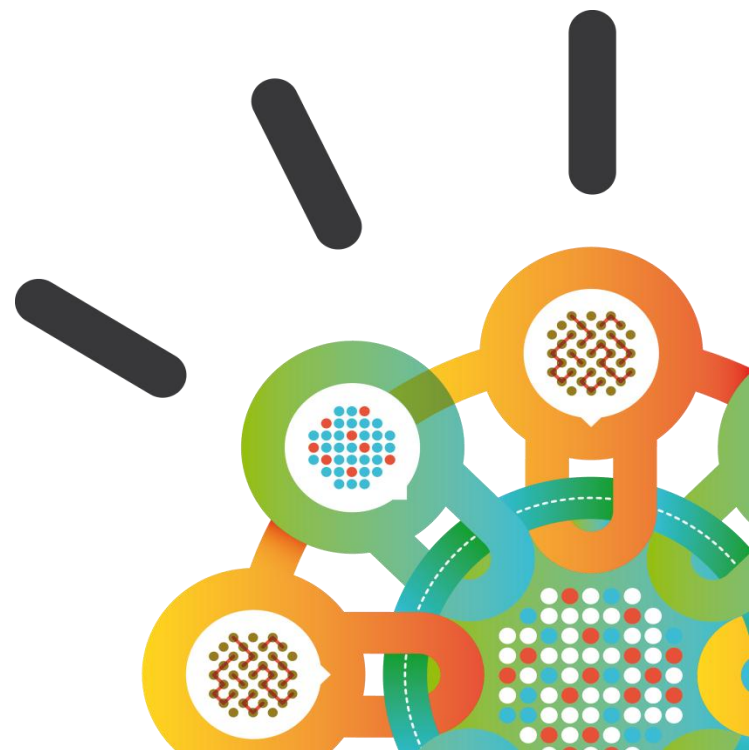
- Acceso no autorizado a datos sensibles
- Cambios inesperados en el sitio (Web site defacement)
- Indisponibilidad del servicio



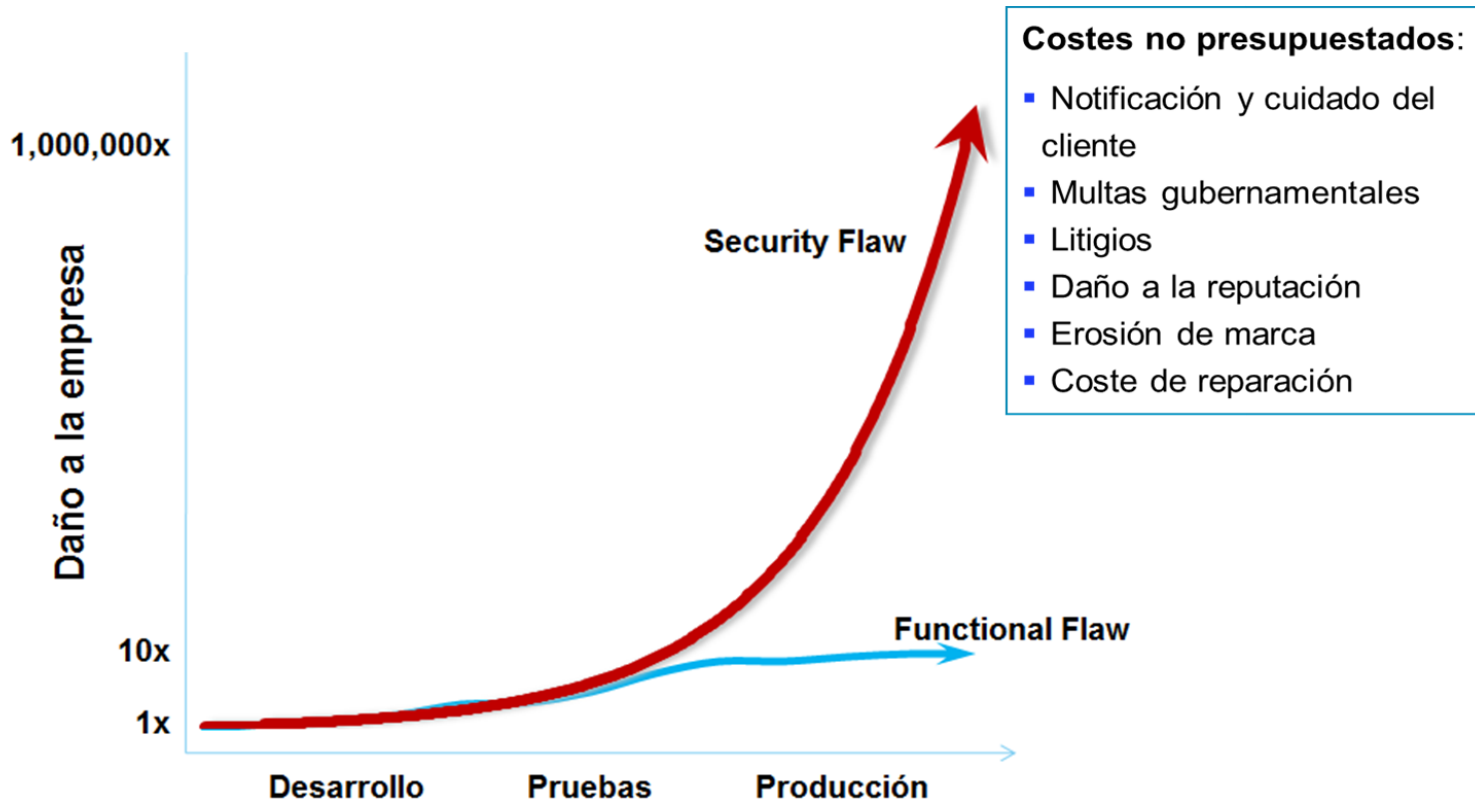
Security Intelligence.
Think Integrated.

IBM Security Appscan

Noviembre 2012



Los costes de los problemas de seguridad son asombrosos

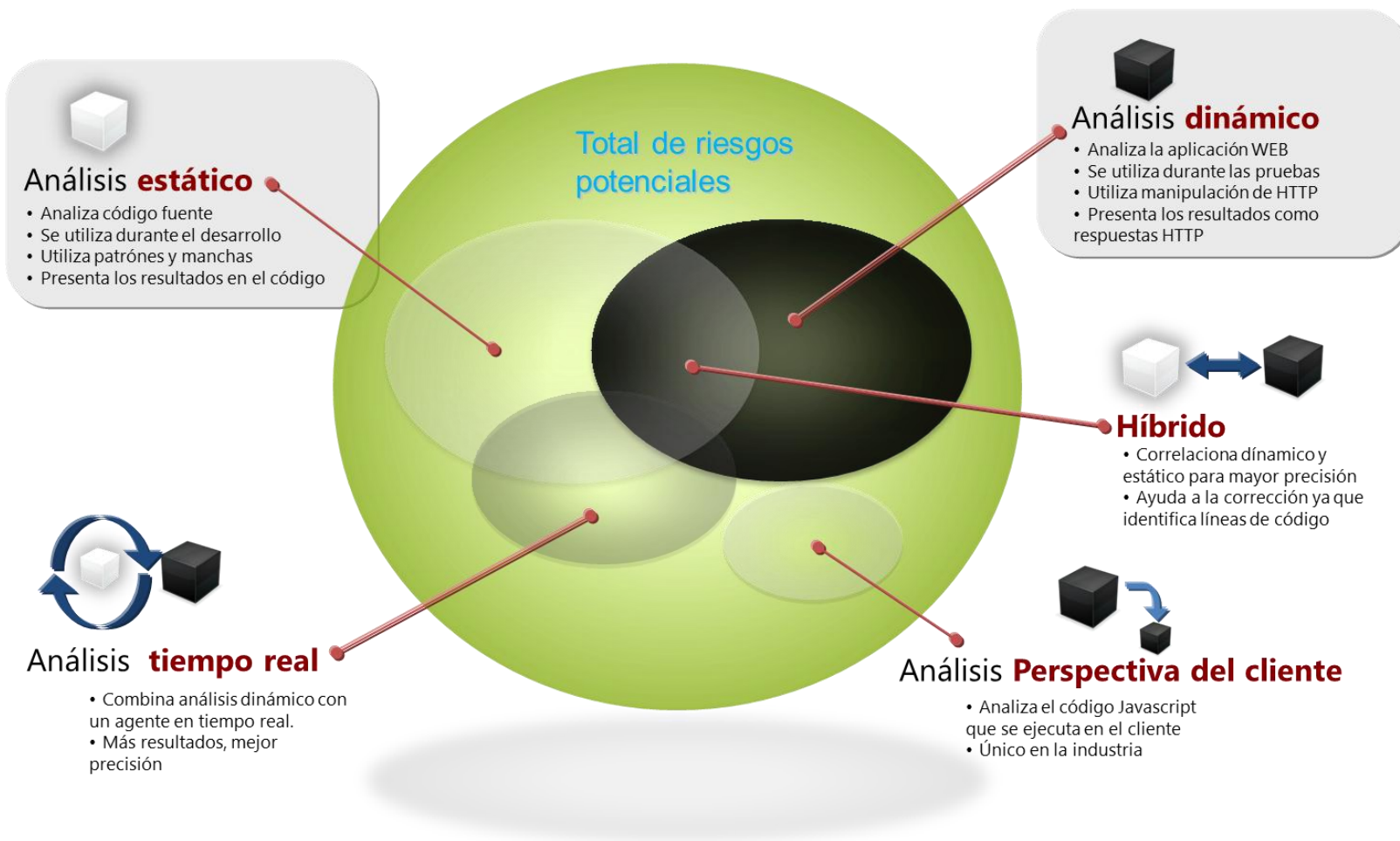


¿Para qué sirve Appscan?

- Encontrar las vulnerabilidades
- Administrar el riesgo
- Construir aplicaciones seguras



Pruebas de seguridad de aplicaciones



Análisis **estático**

- Analiza código fuente
- Se utiliza durante el desarrollo
- Utiliza patrones y manchas
- Presenta los resultados en el código



Análisis **dinámico**

- Analiza la aplicación WEB
- Se utiliza durante las pruebas
- Utiliza manipulación de HTTP
- Presenta los resultados como respuestas HTTP



Híbrido

- Correlaciona dinámico y estático para mayor precisión
- Ayuda a la corrección ya que identifica líneas de código



Análisis **tiempo real**

- Combina análisis dinámico con un agente en tiempo real.
- Más resultados, mejor precisión



Análisis **Perspectiva del cliente**

- Analiza el código Javascript que se ejecuta en el cliente
- Único en la industria

AppScan portfolio

AppScan Standard

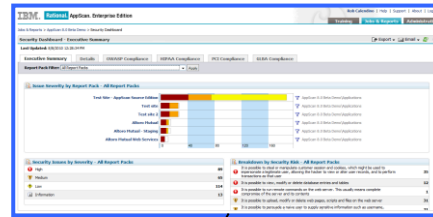
AppScan Source

AppScan Enterprise



Componentes de AppScan

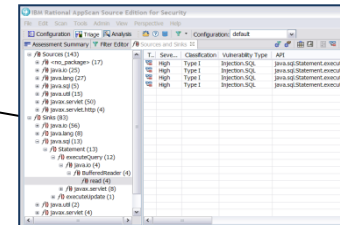
Cliente WEB
AppScan
Enterprise



AppScan
Enterprise
Server



AppScan Standard
(DAST desktop client)

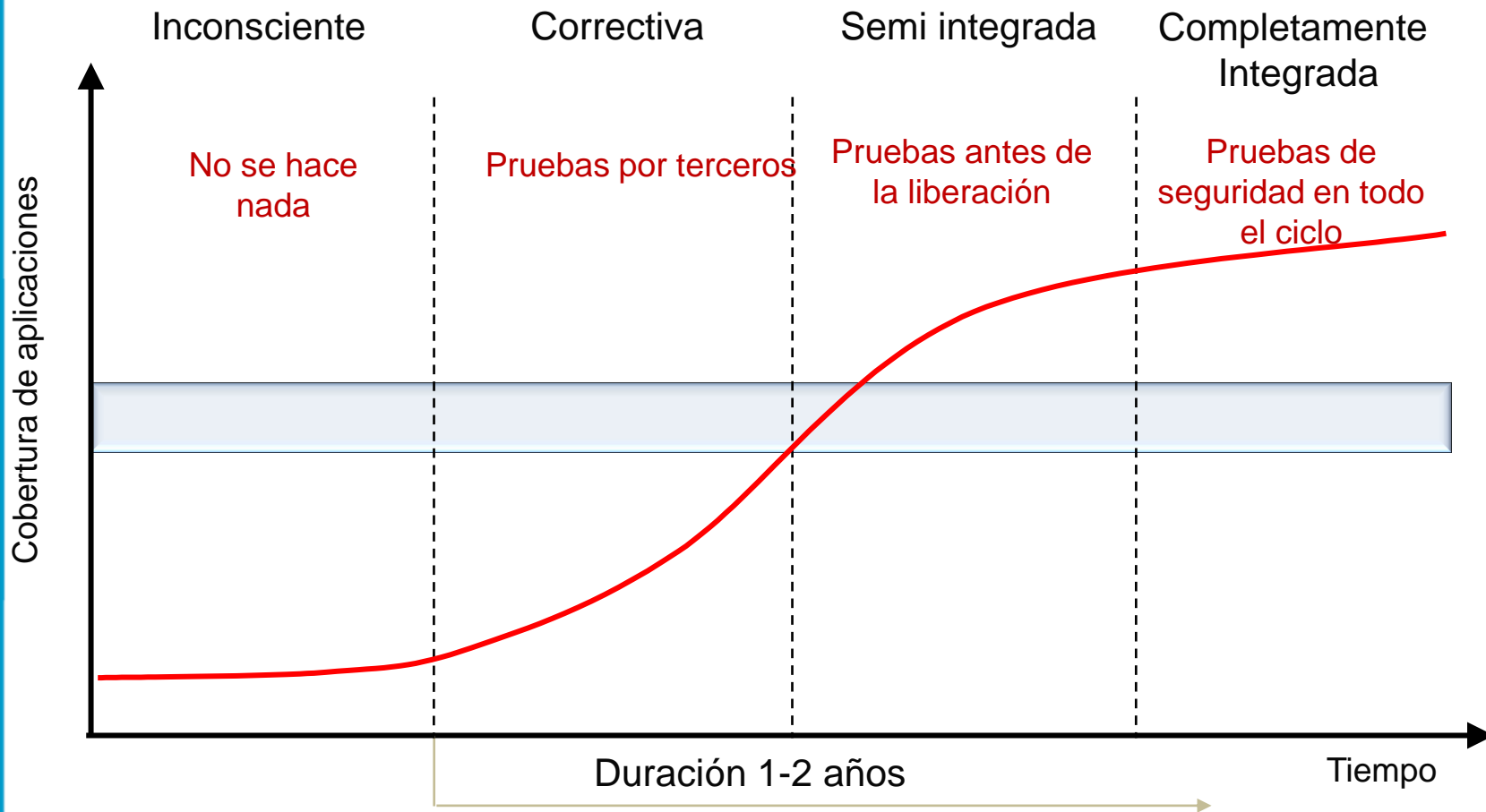


AppScan Source
(SAST desktop client)



AppScan Enterprise
Dynamic Analysis Scanners
(server-based DAST)

Modelo de madurez de seguridad de aplicaciones



SDLC

Código

Versión

QA

Seguridad

Producción

% de errores encontrados en el SDLC

La mayoría de los errores son encontrados antes de salir a producción.



Tipo	Vulnerabilidades por revisar
Críticas	1159
Altas	947
Medias	2529
Bajas	2091



SDLC

Código

Versión

QA

Seguridad

Producción

% de errores encontrados en el SDLC

Perfil deseado



AppScan Source



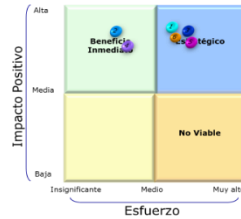
AppScan Standard



```

1: /
2: ..... TxnCSSFontStyle .....
3: constructor TxnCSSFontStyle.Create(aFontStyle: TxnCSSFontStyleEnum);
4: begin
5:   inherited Create(aFontStyle);
6:   FFontStyle := aFontStyle;
7: end;
8:
9: function TxnCSSFontStyle.GetStyleValue: string;
10: begin
11:   Result := nxCSSFontStyleToString(FFontStyle);
12: end;
13:
14: procedure TxnCSSFontStyle.SetFontStyle(Value: TxnCSSFontStyleEnum);
15: begin
16:   IF FFontStyle <> Value then
17:   begin

```



Tipo	Vulnerabilidades por revisar
Críticas	1
Altas	4
Medias	15
Bajas	21

SDLC

Código

Versión

QA

Seguridad

Producción

Desarrolladores

Desarrolladores

Desarrolladores



AppScan Build



Tipo	Vulnerabilidades por revisar
Críticas	1
Altas	4
Medias	15
Bajas	21

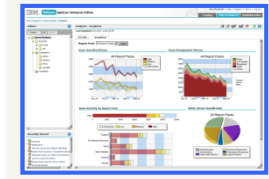


AppScan Standard

Tipo	Vulnerabilidades por revisar
Críticas	0
Altas	0
Medias	3
Bajas	12



AppScan Standard



```

1  ..... TuC3FFontStyle .....
2  constructor TuC3FFontStyle.Create(aFontStyle: TuC3FFontStyleEnum);
3  begin
4      inherited Create(aFontStyle);
5      FFontStyle := aFontStyle;
6  end;
7
8  function TuC3FFontStyle.GetStyleValue: string;
9  begin
10     Result := ucC3FFontStyleStrings[FontStyle];
11 end;
12
13 procedure TuC3FFontStyle.SetFontStyle(Value: TuC3FFontStyleEnum);
14 begin
15     if FFontStyle <> Value then
16     begin

```



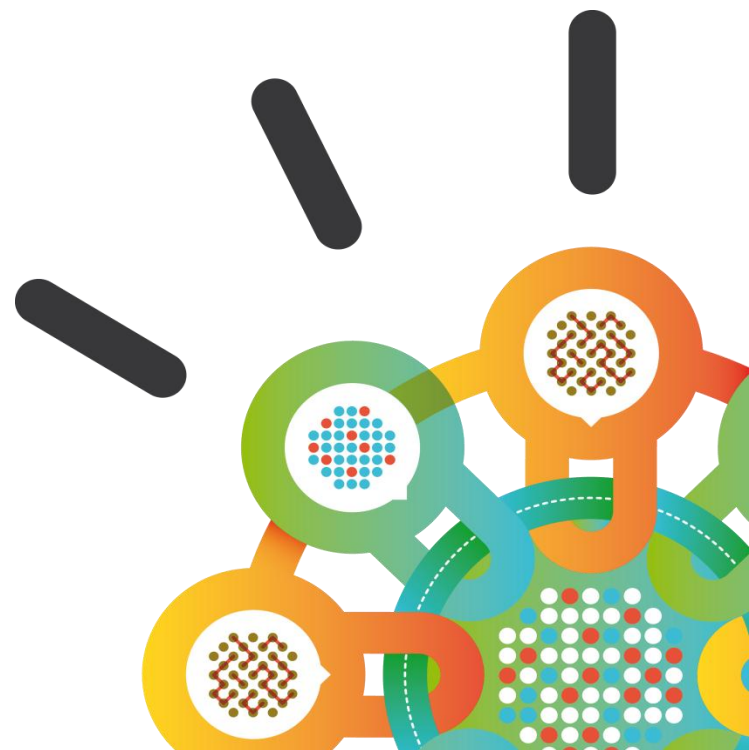
AppScan Source

Madurez en las pruebas de seguridad

Security Intelligence.
Think Integrated.

Novedades

Noviembre 2012



Agente para aplicaciones móviles

La mayoría de las aplicaciones WEB exponen una interface diferente para móviles y navegadores comunes.



- Simula cualquier tipo de navegador, sea móvil o normal
- La navegación se realiza en la plataforma seleccionada
- Se pueden seleccionar agentes predefinidos
- Soporta los métodos de exploración manual y automáticos

Security intelligence – Priorizando y mitigando el riesgo

Site protector correlaciona tráfico malicioso hacia un host con vulnerabilidades conocidas en aplicaciones

QRadar toma en cuenta las vulnerabilidades para calcular de manera mas precisa los niveles de riesgo para cada activo y los puntajes de cada incidente



SiteProtector



QRadar



AppScan



Políticas de protección de aplicaciones Web

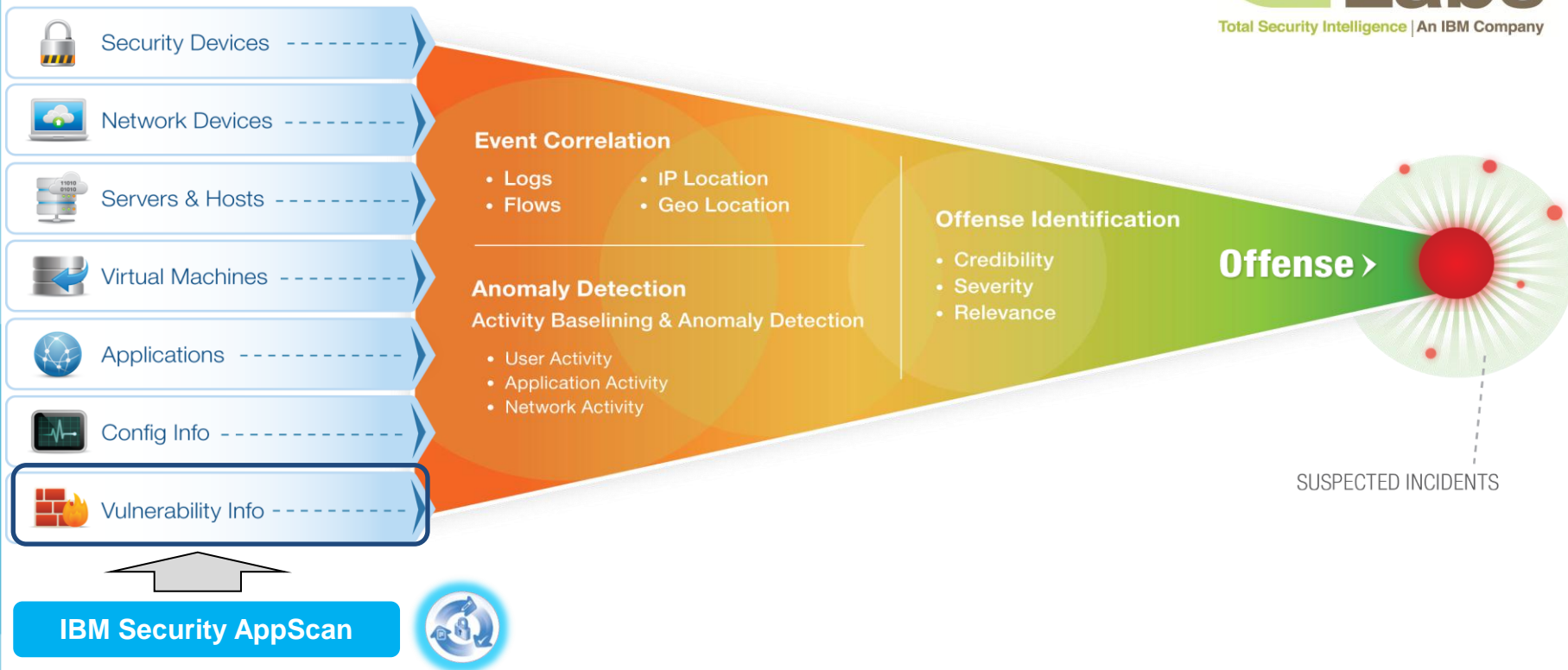


IPS



Applications

QRadar



IBM Security AppScan

Mas fuentes de datos



Profundidad



Precisión necesaria para decisiones inteligentes

DEMO



Seven has Arrived.

Meet the Most Advanced Ethical Hacking Training Program in The World



EC-Council NEWS

ACHIEVEMENT CERTIFICATION COURSES EVENTS FEATURED NEWS PARTNERS PRODUCTS UNCATEGORIZED

**Engineered by Hackers.
Presented by Professionals.**

IT Institute is committed to ethical hacking

IT Institute and Itara Process Consulting have gathered members of the most important technological enterprises in Spain for the launch of the 7th version of Ethical Hacker Certification.

EC-Council, from around the world, has chosen 25 training centers to launch the Ethical Hacker Certification, version 7. It Institute has been selected in Spain.

The certification was given at Itara's Process Consulting facilities located in Madrid's Technological Park.

At the closing event Ariel Súccar, General Manager, from Itara Spain, emphasize how important is to think the same way as hackers do, as an effective method to stop violations in the security systems of the organizations, as well as, the importance of rely on internationally accepted frameworks to manage the security priority and effectively.

After this, Anelio Rodríguez de Riva, Director of Security Information and IT Governance SGS, thanked the attendees for their participation and also explained the need of an appropriate training to ensure information security in the organizations.

The event concluded with the delivery of certificates to the first 17 Ethical Hackers in Portugal and Spain.



En un ataque,
sé capaz de
descifrar el qué,
cómo, quién y dónde

Computer Hacking Forensic Investigator CHFI



ECSA

EC-Council Certified Security Analyst
EC-Council Certified Security Analyst

Advanced Penetration Testing and Security Analysis

Plan and Design Networks.

**Implement Security Solutions. Analyze Security
Risks and Threats. Become an ECSA.**

ECSA

EC-Council Certified Security Analyst

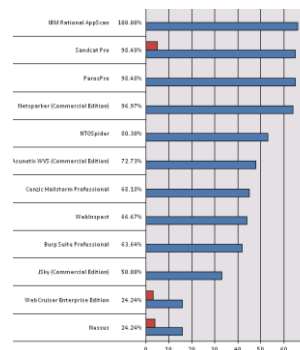
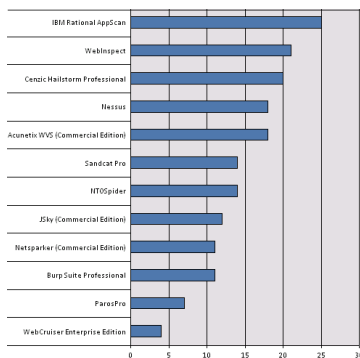


Añadiendo valor a las auditorías de seguridad con IBM Security Appscan

1. Necesidades identificadas por Gestión Canal.
2. Uso de la herramienta en Gestión Canal.
3. Beneficios aportados a Gestión Canal.

Necesidades identificadas por Canal de Isabel II Gestión, S.A.

- Con la creación de la División de Protección Informática en 2008, Gestión Canal establece una unidad con funciones específicas en el ámbito de Seguridad de la Información, reforzando de manera decidida la seguridad en este ámbito.
- Dentro de todas las vertientes relativas a la seguridad de la información, desde dicho área se identifica la necesidad de poder realizar **auditorías de seguridad técnicas y pruebas de penetración (pentesting)** en aplicaciones y servicios web de una manera sencilla, razonablemente completa y ágil, tanto en su vertiente de caja negra como de caja blanca.

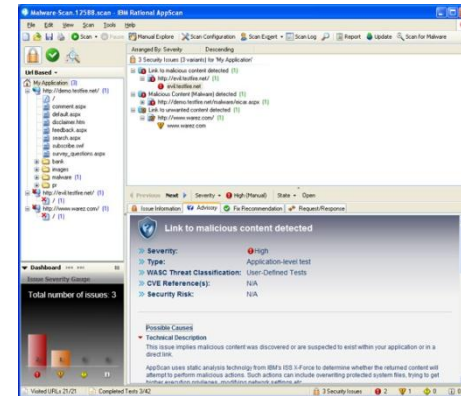


Necesidades identificadas por Canal de Isabel II Gestión, S.A.

- Es necesario por tanto que la aplicación cumpla con, al menos, los siguientes requisitos:
 1. Una alta capacidad de detección de vulnerabilidades, independientemente de su naturaleza.
 2. Una alta capacidad de actualización de la BBDD de vulnerabilidades.
 3. Minimizar el número de falsos positivos.
 4. Poder auditar contra estándares de seguridad (ISO 27001, ISO 27002, NIST 800-53, SANS/CWE, etc.) y normativas regulatorias (HIPAA, Basel II, SoX, PCI-DSS, etc.)
 5. Poder realizar pruebas de concepto de las vulnerabilidades encontradas (evidencias).
 6. Flexibilidad en la confección y presentación de informes de alto nivel y técnicos.
 7. Incluir recomendaciones para la resolución de las vulnerabilidades encontradas.
 8. Facilitar el seguimiento de las tareas de resolución (análisis Delta).
 9. Una implantación fácil y rápida
 10. Facilidad de uso y alto nivel de automatización y ejecución desatendida.

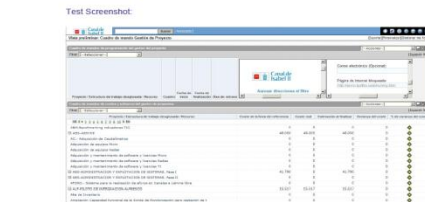
Uso de Rational AppScan en Gestión Canal

- **Análisis de seguridad** de aplicaciones tanto comerciales como desarrolladas internamente, en todo el ciclo de vida del proyecto de implantación.
- Presentación de **informes de resultados**
 - **Detallados** (vulnerabilidades + recomendaciones para su resolución).
 - **Ejecutivos** (estado de la seguridad de la aplicación)
- **Seguimiento** de los trabajos de subsanación de las vulnerabilidades encontradas como paquetes de trabajo dentro de una EDT.
- **Medición** de la calidad de los desarrollos (internos y externos) en cuanto a seguridad.
- **Pruebas de concepto.**
- Recolección de **evidencias.**



Validation in Response:
m&backAction=link/app?action=projectManagerDashboard&frame_id=502&R34.8>-iframe%20src=http://demo.testfire.net/publishing.html>&include=Content=TRUE&objectType=9&objectType=4&objectType=3&objec
ackAction=link/app?action=projectManagerDashboard&frame_id=502&R34.8>-iframe%20src=http://demo.testfire.net/publishing.html>&include=Content=TRUE&objectType=9&objectType=4&objectType=3

Reasoning:
The test response contained a link to the URL 'http://demo.testfire.net, which proves that the phishing attempt was successful.
CVE ID:
301

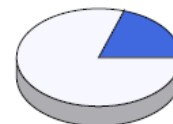


Beneficios aportados a Gestión Canal

- Agilidad a la hora de realizar auditorías de seguridad técnicas.
- Identificación de vulnerabilidades y seguimiento de su resolución a nivel de gestión del proyecto de implantación.
- Identificar el nivel de seguridad objetivo de una aplicación o servicio web.
- Falsos positivos mínimos.
- Facilidad de uso y automatización
- Garantizar un nivel de riesgo conocido y aceptado.
- Ahorro del gasto en las auditorías de seguridad técnicas (ROI en 4/6 meses, en el mismo año).
- Medición de la calidad de los desarrollos en cuanto a seguridad de los mismos (número de vulnerabilidades encontradas, criticidad de las mismas, nivel de riesgo, etc.)

Vulnerable URLs

20% of the URLs had test results that included security issues.



■ Vulnerable URLs (20%)
 Not vulnerable URLs (80%)

Compliance Scan Results

9 unique issues detected across 28 sections of the regulation.

Section	No. of Issues
1. The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. <small>(8.2.1)</small>	5
2. The Access control policy should cover the permitted access methods, and the control and use of unique identifiers such as user IDs and passwords. <small>(8.2.2 (8.1))</small>	-
3. The Access control policy should include an authorization process for user access and privileges. <small>(8.2.2 (8.2))</small>	-
4. The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement or adjusted upon change. <small>(8.3.3)</small>	-
5. The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. <small>(10.3.1)</small>	-
6. Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures designed to protect exchanged information from interception, copying, modification, misrouting, and destruction. <small>(10.8.1 (8))</small>	9
7. Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls should include: procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications. <small>(10.8.1 (8))</small>	7

Scan	Hosts	High	Medium	Low	Informational	Total
		56	11	17	12	96
		1	0	1	10	12

GRACIAS!!!

**Alberto Escribano García- Jefe De División De Protección Informática
Canal de Isabel II**

aescribano@gestioncanal.es

**Ariel Súcari – Country Manager
Itera**

ariel.sucari@iteraprocess.com