INSIGHT

SOFTWARE DONE RIGHT

BEST PRACTICES | TOOLS | TEST AUTOMATION | SECURITY | TRAINING

BOGOTA | MEXICO | MONTEVIDEO

Seguridad de Aplicaciones NOV 2014

Insight se especializa en mejorar la forma de desarrollar software. Mediante capacitación, consultoría, incorporación de mejores prácticas y herramientas del Ciclo de Vida del Software, su equipo de desarrollo se transformará en un pilar para la innovación de sus productos y servicios.

Agenda

- 8:30 Registro y desayuno
- 9:00 Bienvenida
- 9:05 Estado de la seguridad
- 9:30 Introducir la seguridad en el ciclo de vida
- 10:00 Experiencia ANCAP con APPSCAN
- 10:45 Preguntas y respuestas
- 10:55 Cierre

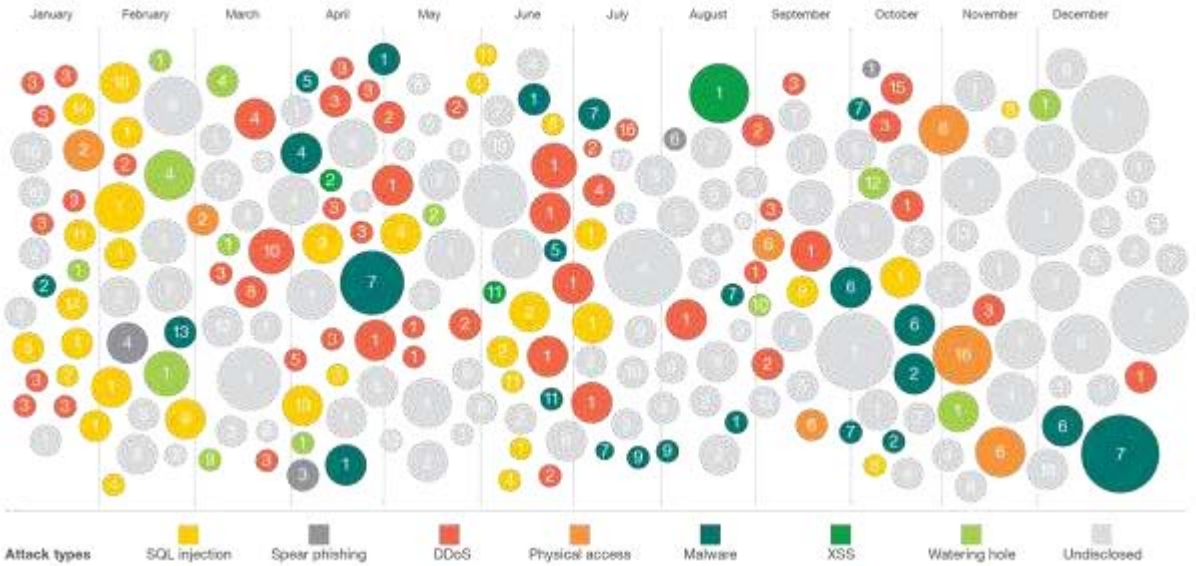
The OWASP Top Ten and Beyond

16 de oct de 2014 | 375 | 36 | 3

Application security problems are not only the most common type of vulnerability, they also lead to the majority of breaches. In 2003, I wrote the first Top Ten Application Security Risks for the Open Web Application Security Project (OWASP). Our goal at the time was to raise awareness and improve software security through the establishment of free and open industry standards.

In case you are wondering, OWASP is an open-source community comprised of software developers from corporations, educational organizations, and other interested individuals from around the world.

Vulnerabilidades de Aplicaciones 2013



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types

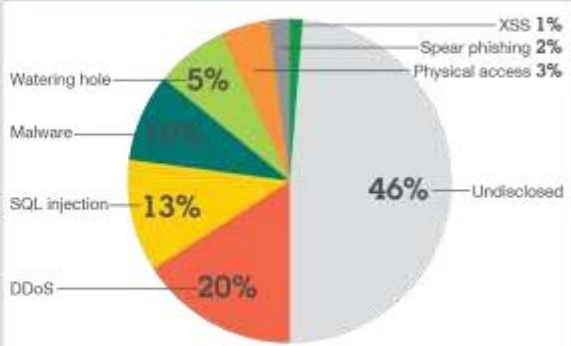
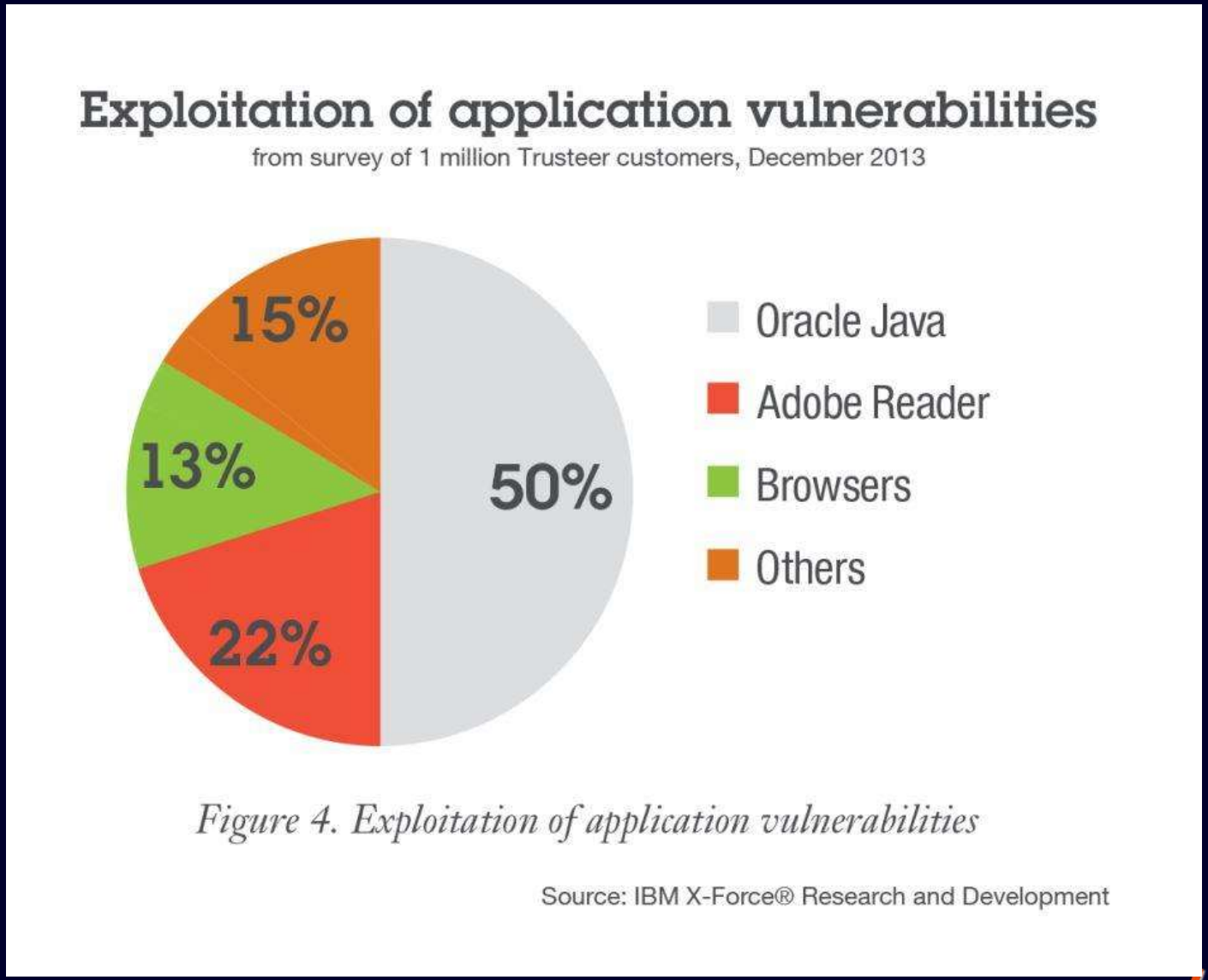


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

Vulnerabilidades de Aplicaciones 2013



Tendencia vulnerabilidades Java 2010-2013

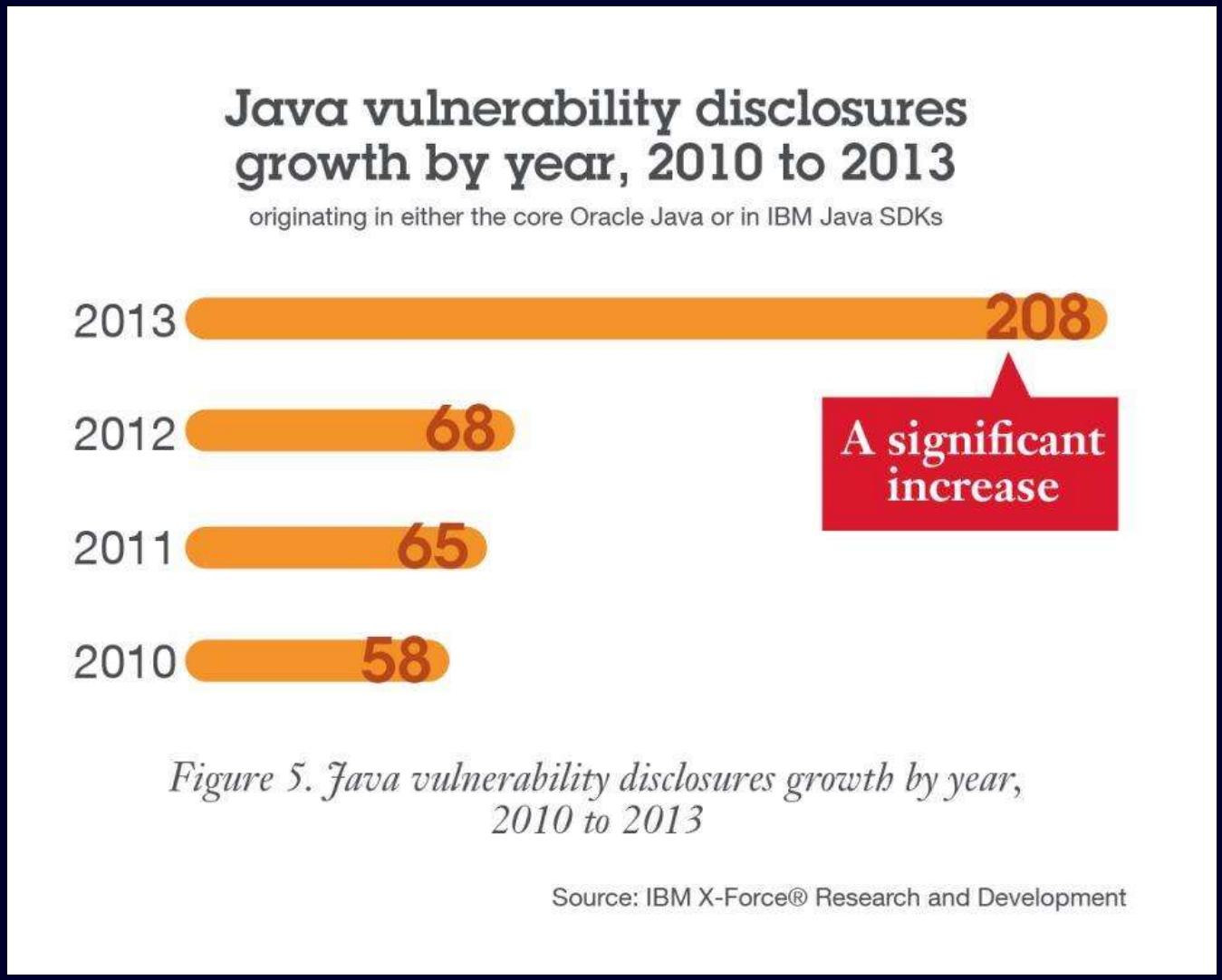


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

Source: IBM X-Force® Research and Development

Tendencia vulnerabilidades 2012-2013

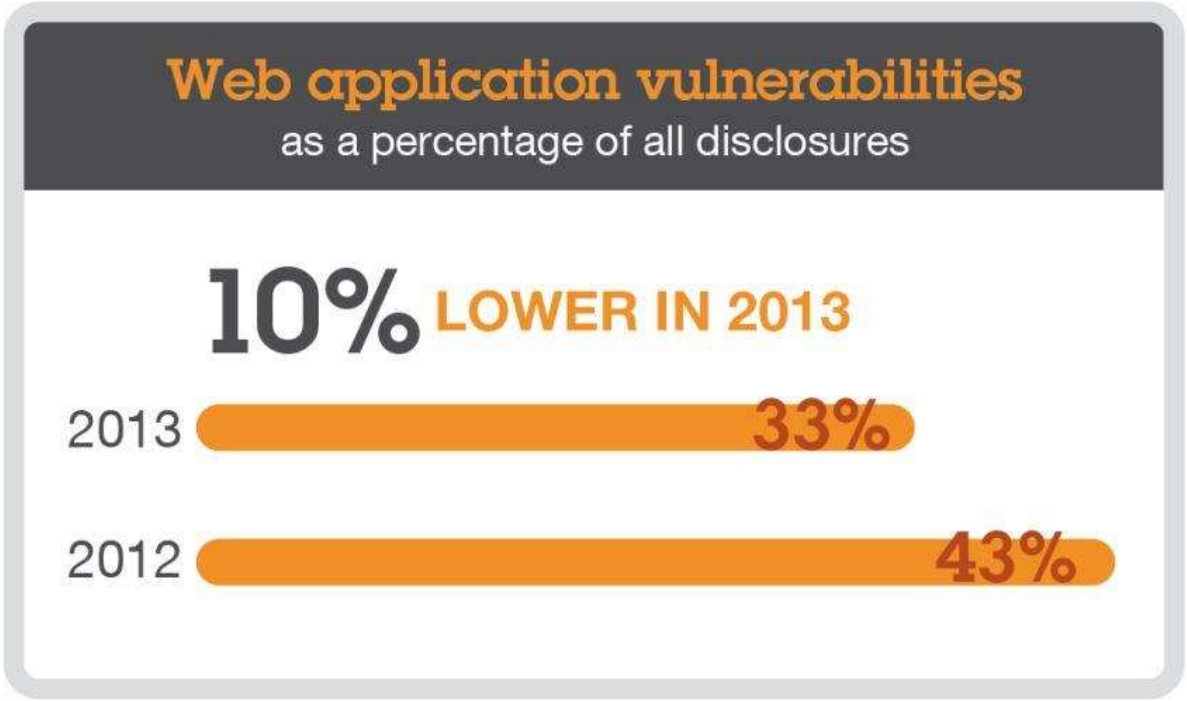


Figure 9. Web application vulnerabilities as a percentage of all disclosures, 2012 to 2013

Source: IBM X-Force® Research and Development

Vulnerabilidades por tipo de ataque 2009-2013

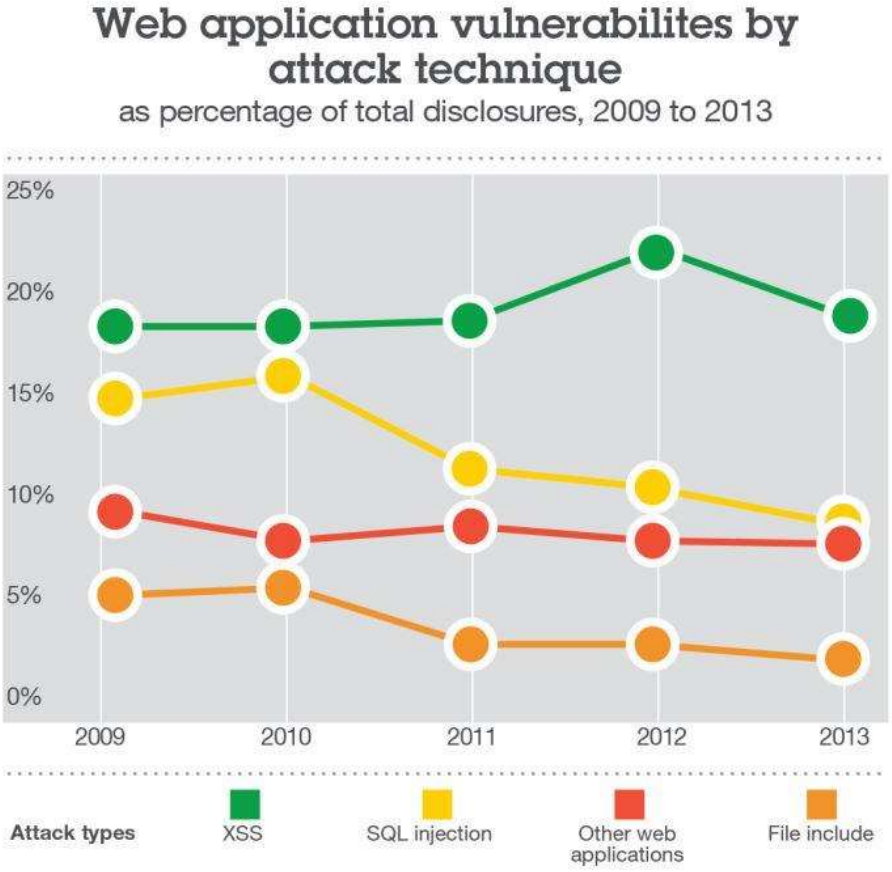


Figure 11. Web application vulnerabilities by attack technique, 2009 to 2013

Source: IBM X-Force® Research and Development

SQL INJECTION representa el 33% del total de vulnerabilidades reportadas pese a la facilidad con que se puede prevenir y detectar

2014

Ataques

EBAY

REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

EBay asks 145 million users to change passwords after cyber attack

BY JIM FINKLE, SOHAM CHATTERJEE AND LEHAR MAAN

BOSTON/BANGALORE | Wed May 21, 2014 4:

12 COMMENTS | Tweet

John Donahoe, chief executive of eBay, speaks

CREDIT: REUTERS/STEPHEN LAM

The eBay data breach led to a huge amount of sensitive user data to be compromised.

Image from Leon7 via wikimedia.org

The occurrence of security breaches at large companies appears to be on the rise. Last year, we saw massive data breaches at Target and Adobe affecting millions of customers. The personal data of many people were at stake as a result of the incidents. Data breaches are the stuff of nightmares for any enterprise. They not only suffer huge financial loss, but also lose the trust of their customers. Recently, eBay became the latest victim of a major data breach, with a database containing encrypted passwords and other personal data becoming compromised. The hacker followed the usual practice of using employee credentials to gain access to the eBay network and steal the personal details of millions of eBay customers. Last week, the company notified users via email to change their passwords in order to prevent further damage due to the breach.

TARGET

Se infiltró la red con **malware** el que fue detectado por el servicio de seguridad externo pero la **alarma** no fue atendida por el equipo de seguridad interno.

El acceso se produjo por credenciales robadas a un **proveedor** de **servicios de limpieza** y mantenimiento

JP MORGAN

TECHNOLOGY | After Breach, JPMorgan Still Seeks to Determine Extent of Attack

patched so they can regain access.

Hackers may potentially have a window into how the bank's individual computers work, people said.
Mike Segar/Reuters

A fourth person with knowledge of the matter, also speaking on condition of anonymity, said hackers had not gained access to account holders' financial information or Social Security numbers, and may have reviewed only names, addresses and phone numbers.

The hack began in June and was not detected until late July. JPMorgan briefed financial regulators on the extent of the damage last week. Investigators say they believe that at least four other banks or financial institutions into JPMorgan's internal systems. Ultimately, the hackers found multiple entry points, the people said, but the race website was not among them. One route that proved somewhat successful was through an older human resources system at the bank.

The White House

The New York Times

U.S. Fines Automakers Hyundai and Kia for Misstating Mileage

Angry Voters and Piles of Money Put Control of Senate in Play

In States Voting on Minimum Wage, Even Critics Sound Like Supporters

U.S.

White House Cites a Breach by Hackers

By THE NEW YORK TIMES OCT. 29, 2014

MILWAUKEE — Hackers recently breached an unclassified computer network used by President Obama's senior staff, a White House official said Tuesday night, prompting countermeasures by the administration that caused temporary system outages.

Administration officials said the attack did not appear to be aimed at destruction of either data or hardware, or to take over other systems at the White House. That strongly suggests that the hackers' intention was either to probe and map the unclassified White House system, find entry points where they connect to other system or conduct fairly standard espionage.

That means it would be different from the kind of attack that Iran launched two years against the computer systems of Saudi Aramco and would be more in the style of the kind of attacks that Russia and China have used over the years against United States government targets.

Some White House staff members lost their connections to the system "as a result of measures we have taken to defend our networks," the official said.

URUGUAY también está en el radar

Perú.com CLASIFICATORIAS 2014

INICIO | ESTADISTICAS | EQUIPOS | F

PERU.COM › ELIMINATORIAS AL MUNDIAL BRASIL 2014 › WEB DEL MINISTERIO DEL URUGUAY FUE HACKEADA

Web del Ministerio del Deporte de Urugua hackeada

Hacked by H4x0rs Perú

Uruguayos de mierda ganaron solo porque el puto arbitro Cabricio Loustau los ayudó. No e

TE AMOOOOOO PERÚ

GRACIAS FARFAN Y GUERRERO QUE LA LUCHARON HASTA EL FINAL, YOSHIMAR YOTUN ERES UN WEON xD

AUMENTO DE TECNOLOGÍA DEJA A URUGUAY MÁS EXPUESTO A LOS ATAQUES CIBERNÉTICOS

AGOSTO 1, 2014 0

Like Share 2 Twittear 1

Así lo afirmó el director de Agesic, José Clastornik, en la apertura del ejercicio de simulación de ataques informáticos con el objetivo de capacitar especialistas en la materia.

Destacó, además, que el país es líder en telecomunicaciones, conectividad de escolares en línea, gobierno electrónico y servicios en línea.

La Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento) abrió este jueves un ejercicio de dos días de simulación de ataques informáticos.

2014

Vulnerabilidades

Heartbleed

Error de Aplicación – Clásico Buffer Overrun

Se pudo haber detectado con un análisis de código fuente

tls1_process_heartbeat (/col5/ddehaas/CSOINDIRECT/tmp/openssl-1.0.1f/ssl/t1_lib.c)

```
2554  tls1_process_heartbeat(SSL *s)
2555          {
2556          unsigned char *p = &s->s3->rrec.data[0], *pl;
2557          unsigned short hbtype;
2558          unsigned int payload;
2559          unsigned int padding = 16; /* Use minimum padding */
2560
2561          /* Read type and payload length first */
2562          hbtype = *p++;
2563          n2s(p, payload);
2564          pl = p;
2565
2566          if (s->msg_callback)
2567                  s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
2568                          &s->s3->rrec.data[0], s->s3->rrec.length,
2569                          s, s->msg_callback_arg);
2570
2571          if (hbtype == TLS1_HB_REQUEST)
2572                  {
2573                  unsigned char *buffer, *bp;
2574                  int r;
2575
2576                  /* Allocate memory for the response, size is 1 bytes
2577                   * message type, plus 2 bytes payload length, plus
2578                   * payload, plus padding
2579                   */
2580                  buffer = OPENSSL_malloc(1 + 2 + payload + padding);
2581                  bp = buffer;
2582
2583                  /* Enter response type, length and copy payload */
2584                  *bp++ = TLS1_HB_RESPONSE;
2585                  s2n(payload, bp);
2586                  memcpy(bp, pl, payload);
```

Tainted Buffer Access

This code could read past the end of the buffer pointed to by s2 memcpy.c:41

- The code reads from the buffer pointed to by s2 memcpy.c:41 at a position tainted by a file descriptor.
  - payload is derived from n memcpy.c:41
  - payload is tainted by a file descriptor.

The issue can occur if the highlighted code executes.

See related event 70

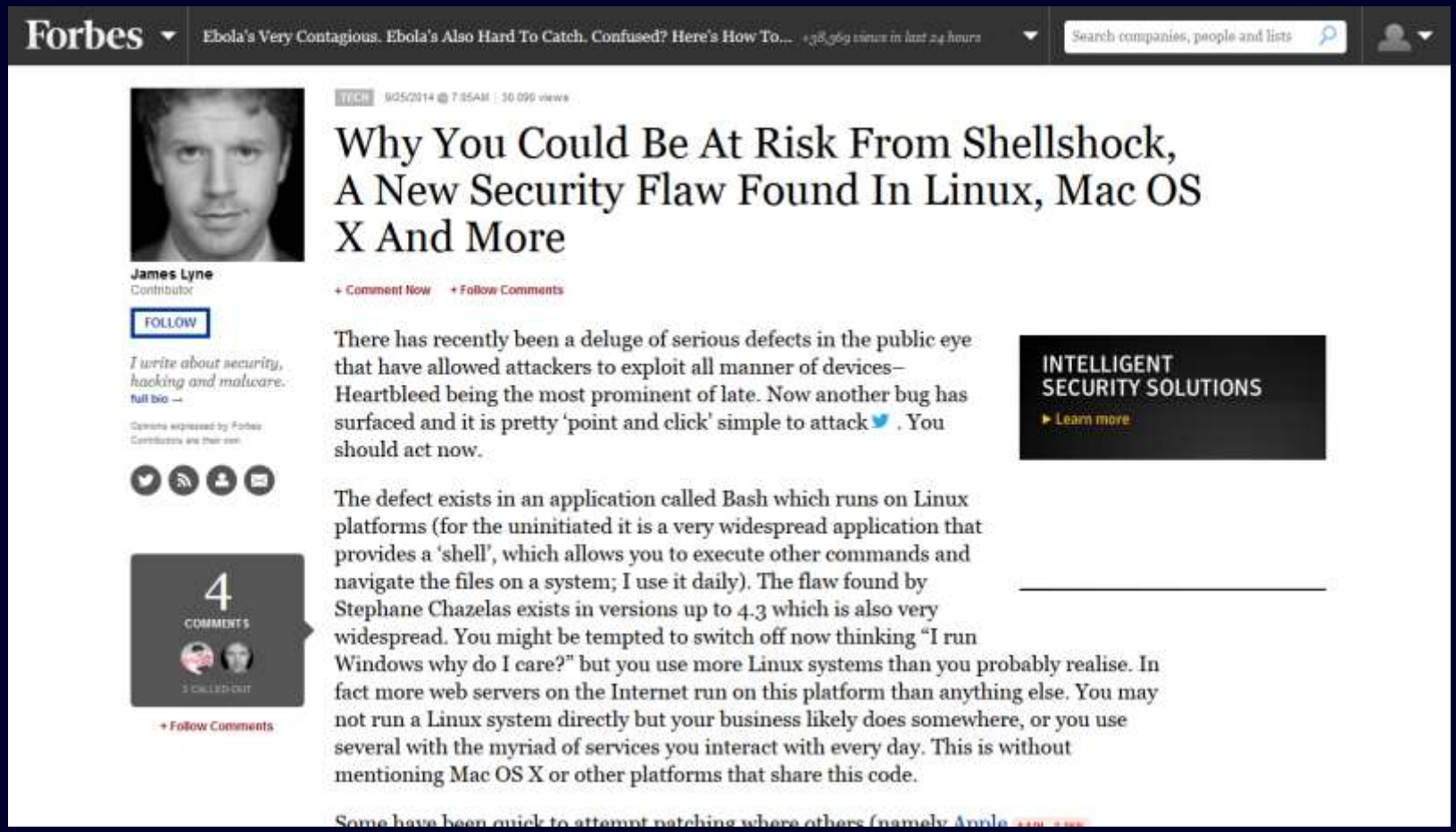
Show: All events | Only primary events

INSIGHT

SOFTWARE DONE RIGHT

SHELLSHOCK - BASH

Error de Aplicación



Forbes ▾ Ebola's Very Contagious. Ebola's Also Hard To Catch. Confused? Here's How To... 438,369 views in last 24 hours ▾ Search companies, people and lists

James Lyne
Contributor

FOLLOW

I write about security, hacking and malware.
full bio →

Opinions expressed by Forbes Contributors are their own.

4
COMMENTS

+ Follow Comments

TECH 9/25/2014 @ 7:35AM | 30,096 views

Why You Could Be At Risk From Shellshock, A New Security Flaw Found In Linux, Mac OS X And More

+ Comment Now + Follow Comments

There has recently been a deluge of serious defects in the public eye that have allowed attackers to exploit all manner of devices– Heartbleed being the most prominent of late. Now another bug has surfaced and it is pretty 'point and click' simple to attack . You should act now.

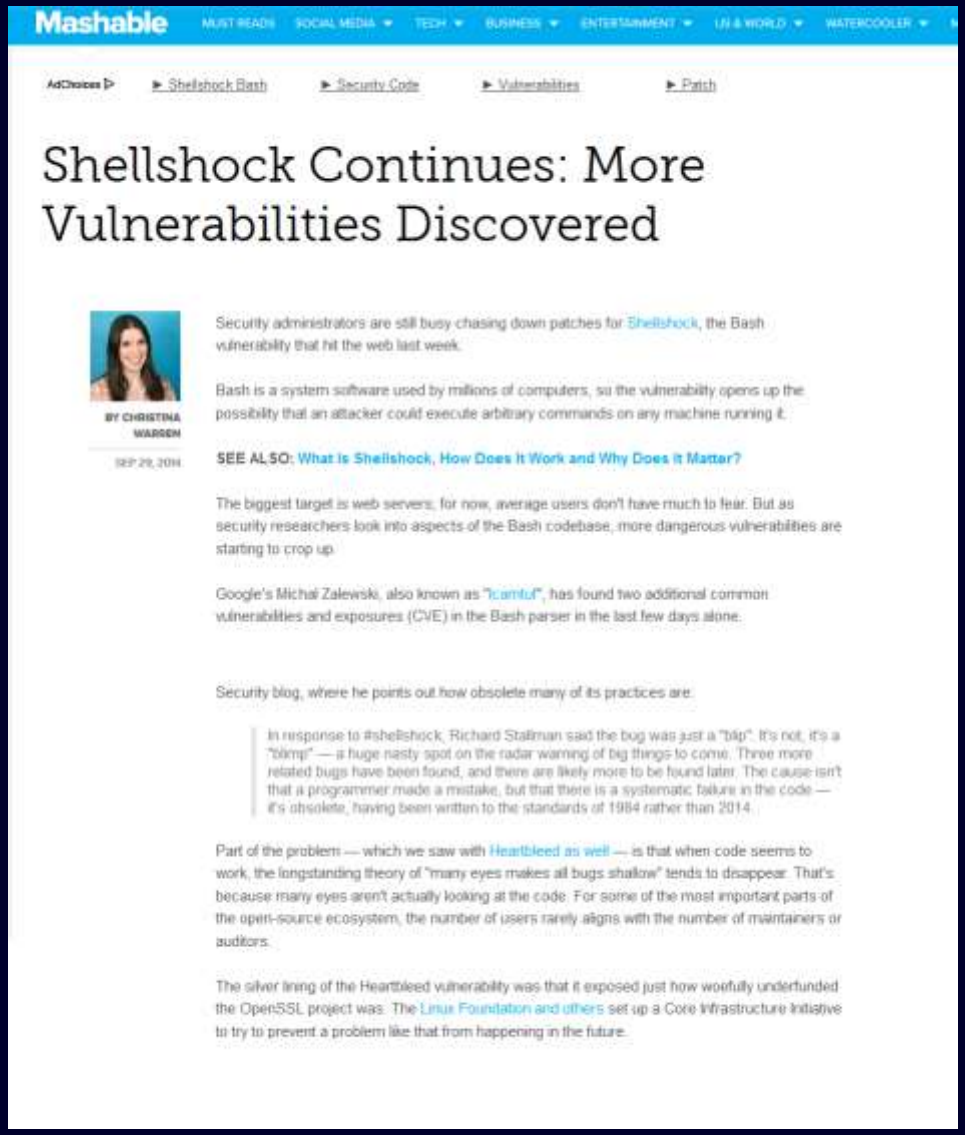
The defect exists in an application called Bash which runs on Linux platforms (for the uninitiated it is a very widespread application that provides a 'shell', which allows you to execute other commands and navigate the files on a system; I use it daily). The flaw found by Stephane Chazelas exists in versions up to 4.3 which is also very widespread. You might be tempted to switch off now thinking "I run Windows why do I care?" but you use more Linux systems than you probably realise. In fact more web servers on the Internet run on this platform than anything else. You may not run a Linux system directly but your business likely does somewhere, or you use several with the myriad of services you interact with every day. This is without mentioning Mac OS X or other platforms that share this code.

Some have been quick to attempt patching where others (namely Apple

INSIGHT
SOFTWARE DONE RIGHT

SHELLSHOCK
Error de Aplicación

Luego que la vulnerabilidad inicial fue detectada y se liberó un parche con su corrección otras dos vulnerabilidad es fueron detectadas en el código que no fueron solucionadas por el parche liberado



Mashable

MUST READS SOCIAL MEDIA TECH BUSINESS ENTERTAINMENT LIFE & WORLD WATERCOOLER

AdChoices ▷ ▶ Shellshock Bash ▶ Security Code ▶ Vulnerabilities ▶ Patch

Shellshock Continues: More Vulnerabilities Discovered

BY CHRISTINA WARREN

SEP 29, 2014

Security administrators are still busy chasing down patches for Shellshock, the Bash vulnerability that hit the web last week.

Bash is a system software used by millions of computers, so the vulnerability opens up the possibility that an attacker could execute arbitrary commands on any machine running it.

SEE ALSO: What is Shellshock, How Does It Work and Why Does it Matter?

The biggest target is web servers; for now, average users don't have much to fear. But as security researchers look into aspects of the Bash codebase, more dangerous vulnerabilities are starting to crop up.

Google's Michal Zalewski, also known as "lcamtuf", has found two additional common vulnerabilities and exposures (CVE) in the Bash parser in the last few days alone.

Security blog, where he points out how obsolete many of its practices are.

> In response to #shellshock, Richard Stallman said the bug was just a "blip". It's not, it's a "blimp" — a huge nasty spot on the radar warning of big things to come. Three more related bugs have been found, and there are likely more to be found later. The cause isn't that a programmer made a mistake, but that there is a systematic failure in the code — it's obsolete, having been written to the standards of 1984 rather than 2014.

Part of the problem — which we saw with Heartbleed as well — is that when code seems to work, the longstanding theory of "many eyes makes all bugs shallow" tends to disappear. That's because many eyes aren't actually looking at the code. For some of the most important parts of the open-source ecosystem, the number of users rarely aligns with the number of maintainers or auditors.

The silver lining of the Heartbleed vulnerability was that it exposed just how woefully underfunded the OpenSSL project was. The Linux Foundation and others set up a Core Infrastructure Initiative to try to prevent a problem like that from happening in the future.

2014

Tendencias

Velocidad en Aumento – Ataque Java 2012

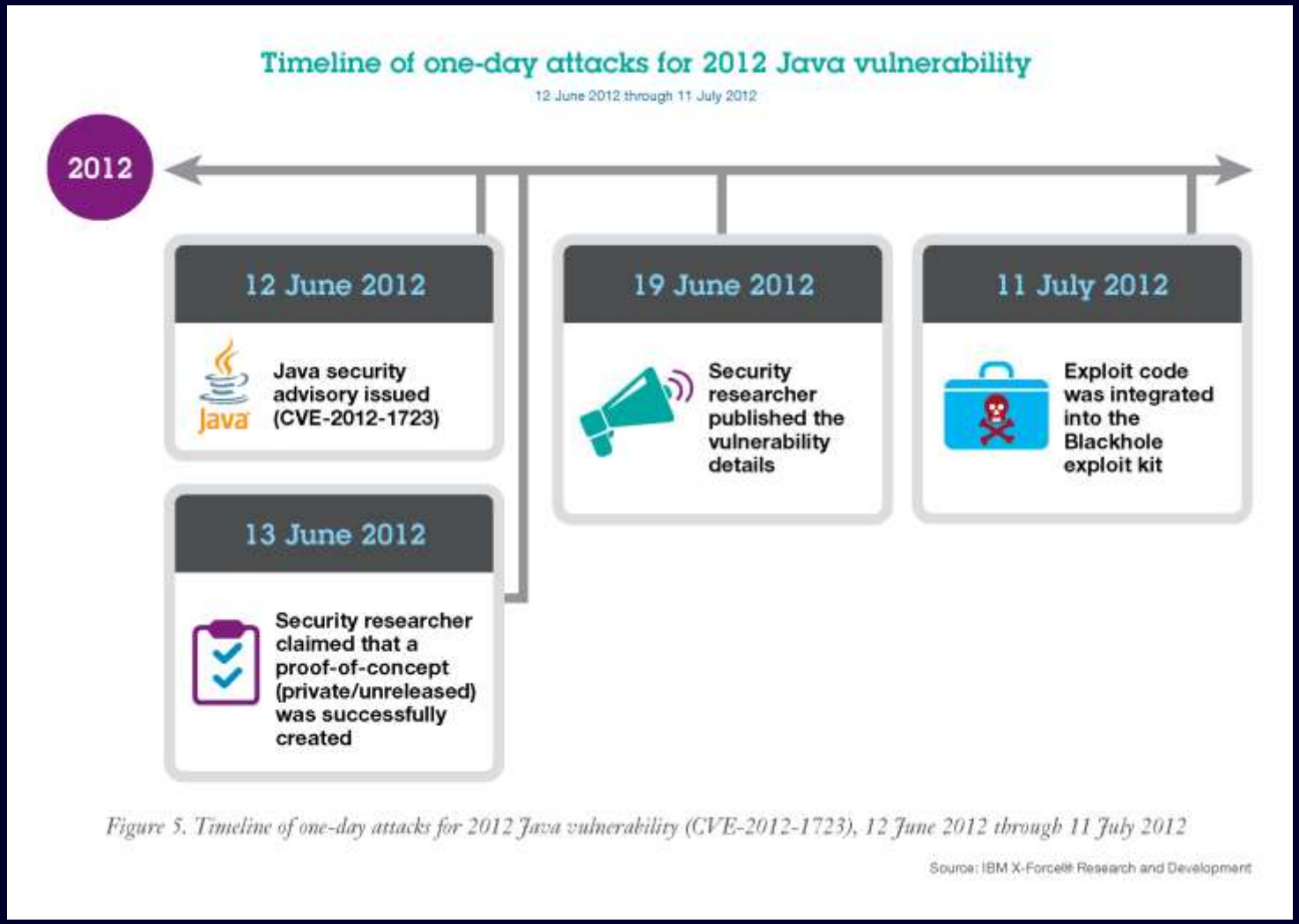


Figure 5. Timeline of one-day attacks for 2012 Java vulnerability (CVE-2012-1723), 12 June 2012 through 11 July 2012

Source: IBM X-Force® Research and Development

Velocidad en Aumento – Heartbleed 2014

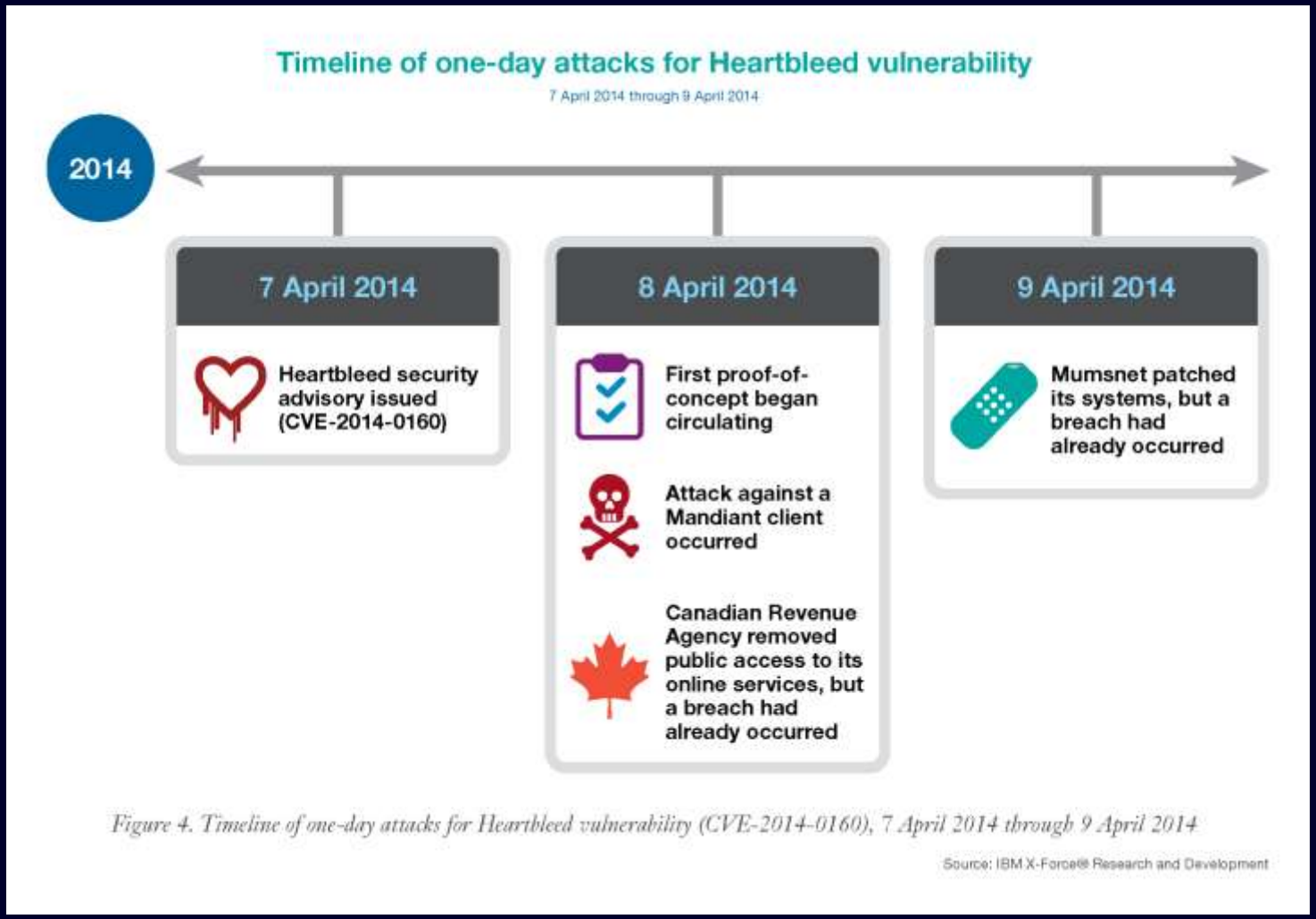


Figure 4. Timeline of one-day attacks for Heartbleed vulnerability (CVE-2014-0160), 7 April 2014 through 9 April 2014

Source: IBM X-Force® Research and Development

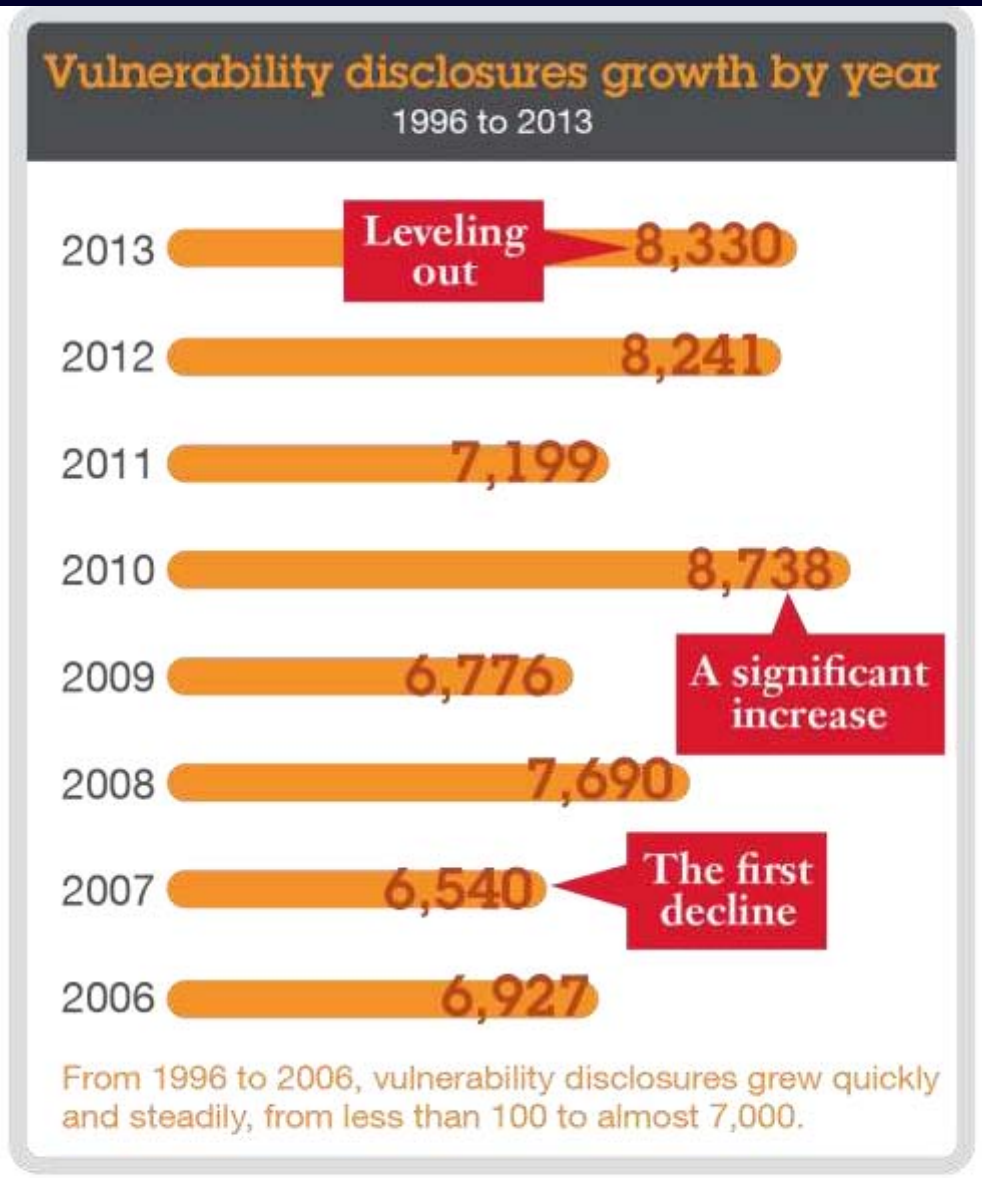


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development

TENDENCIA 2014

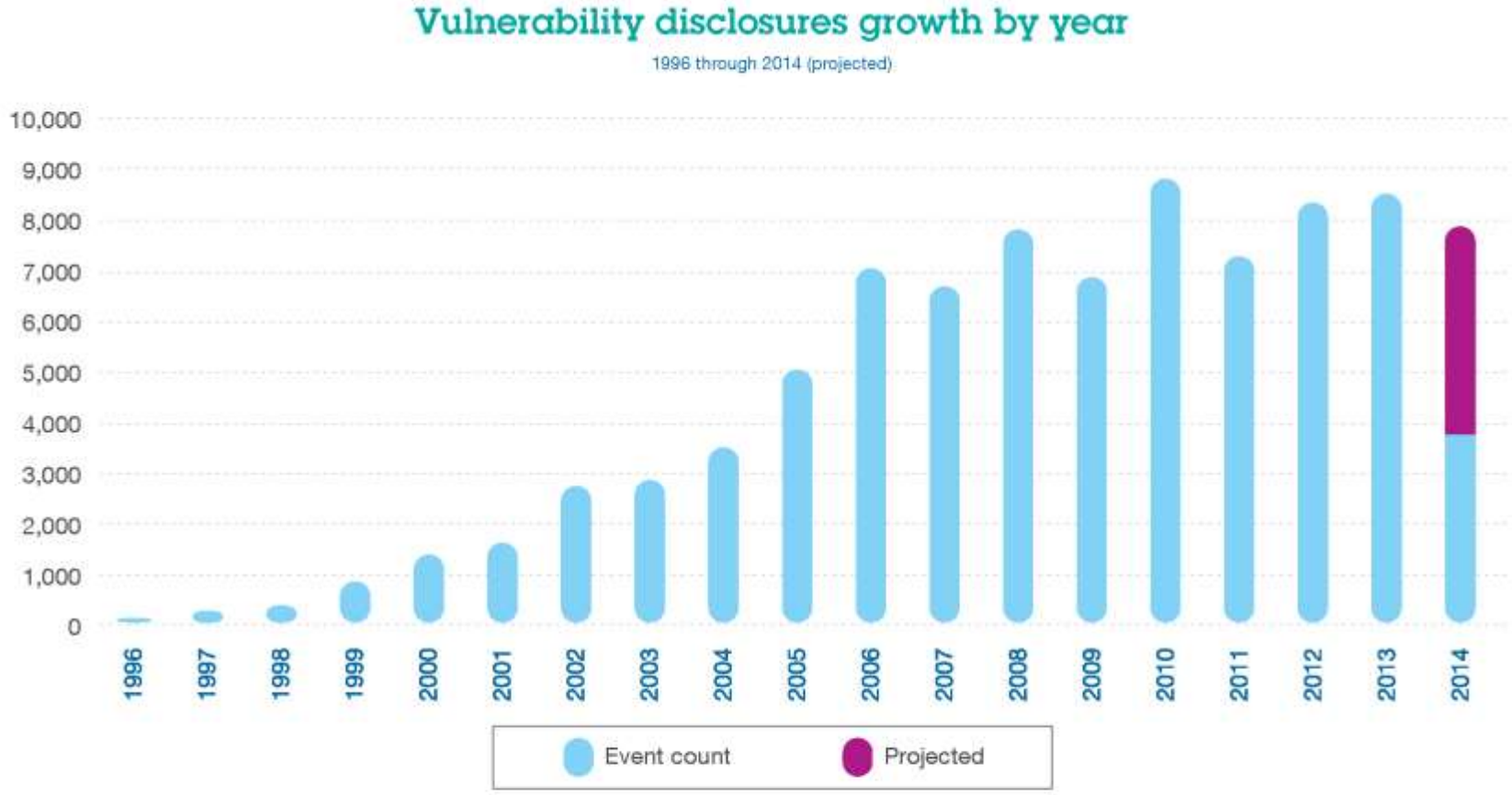


Figure 6. Vulnerability disclosures growth by year, 1996 through 2014 (projected)

Source: IBM X-Force® Research and Development

INSIGHT

SOFTWARE DONE RIGHT

BEST PRACTICES | TOOLS | TEST AUTOMATION | SECURITY | TRAINING

BOGOTA | MEXICO | MONTEVIDEO

seguridad en el ciclo de vida de software

appScan

SEGURIDAD en el CICLO de VIDA

porqué es importante ?

la seguridad es importante

se requiere infraestructura dinámica adaptándose a novedades en ambiente de negocio enfocando:

dinámica de negocio

- **servicio**

  dar respuesta ágil a oportunidades y desafíos, exige modelos escalables, de alta visibilidad, control y nivel de automatización y conectividad en múltiples plataformas y dispositivos.

dinámica de negocio

- **costo**

  competencia GLOBAL, servicios a demanda variable, complejidad creciente, exigencias de clientes crecientes, factor crítico en velocidad en cambios y eficiencia.

dinámica de negocio

- **riesgo**

  diversidad de información, dispositivos, conexiones en red de clientes y servicios de terceros, multiplica riesgo en **integridad**, **disponibilidad**, **confidencialidad** en sistemas de información

la seguridad es importante

- autenticación, firma, sesión, autorización, auditoría, adopción de credenciales, exposición de datos, inyección & corrupción datos,...

SEGURIDAD en el CICLO de VIDA

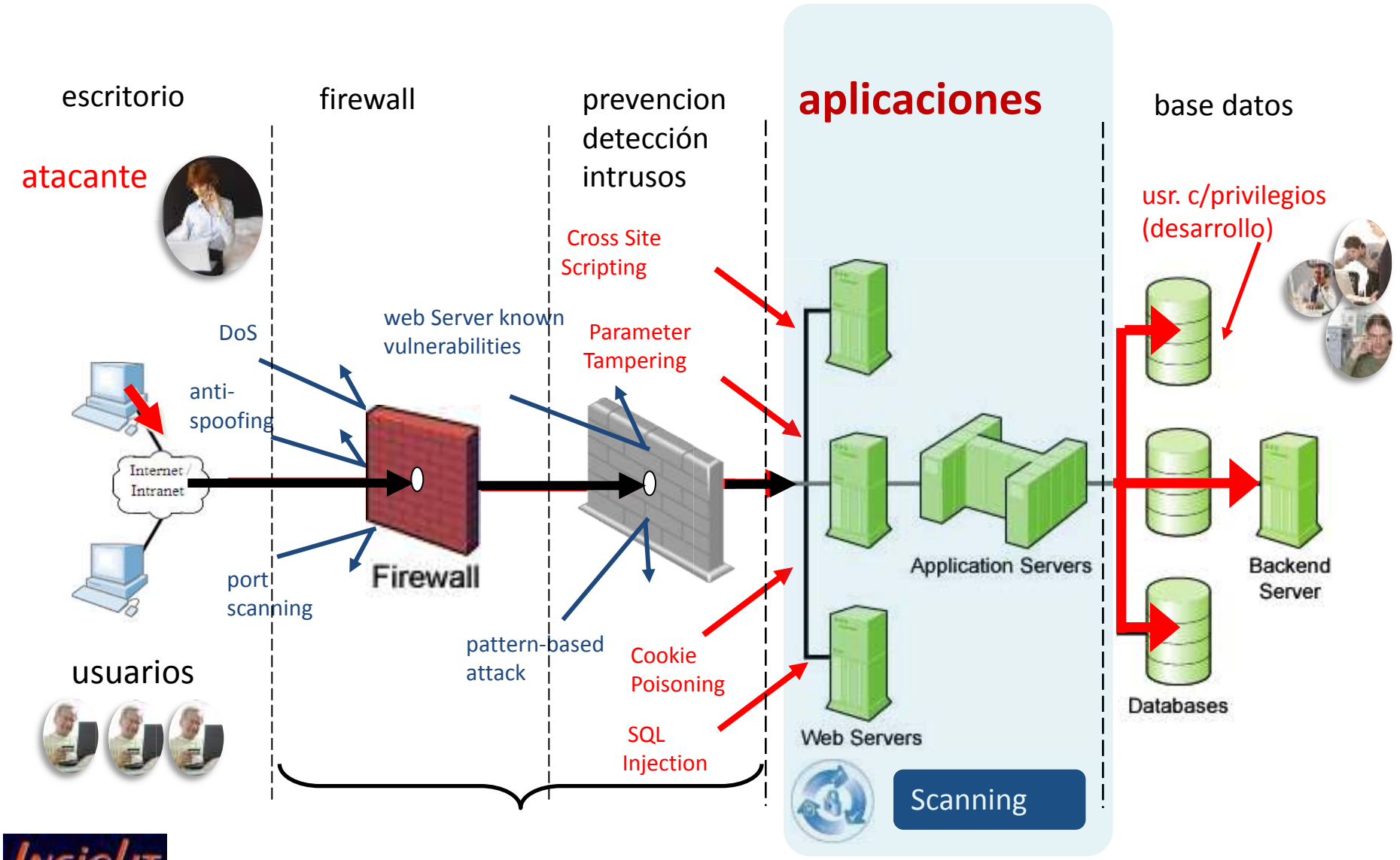
asuntos de seguridad

son requerimientos, que merecen ser contemplados en fase desarrollo de sistemas y en ciclo de vida.

SEGURIDAD en el CICLO de VIDA

CONTEXTO de APLICACIONES

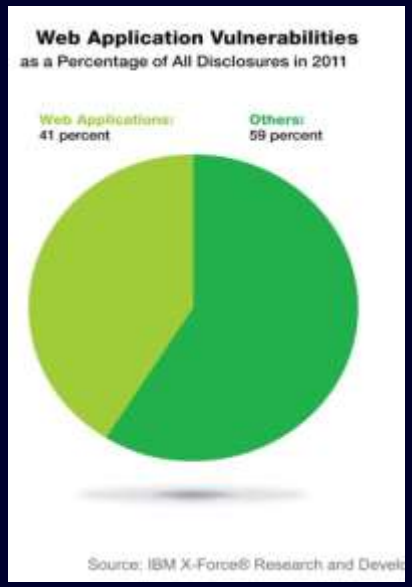
CONTEXTO SEGURIDAD



SEGURIDAD en el CICLO de VIDA

RIESGOS ?

RIESGOS en APLICACIONES



hoy

- **impacto tecnología móvil**
- **creciente detección fallas de seguridad de aplicaciones**
- **mas de 1/3 de violaciones registradas, relacionadas a inyección SQL**

https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report

INSIGHT

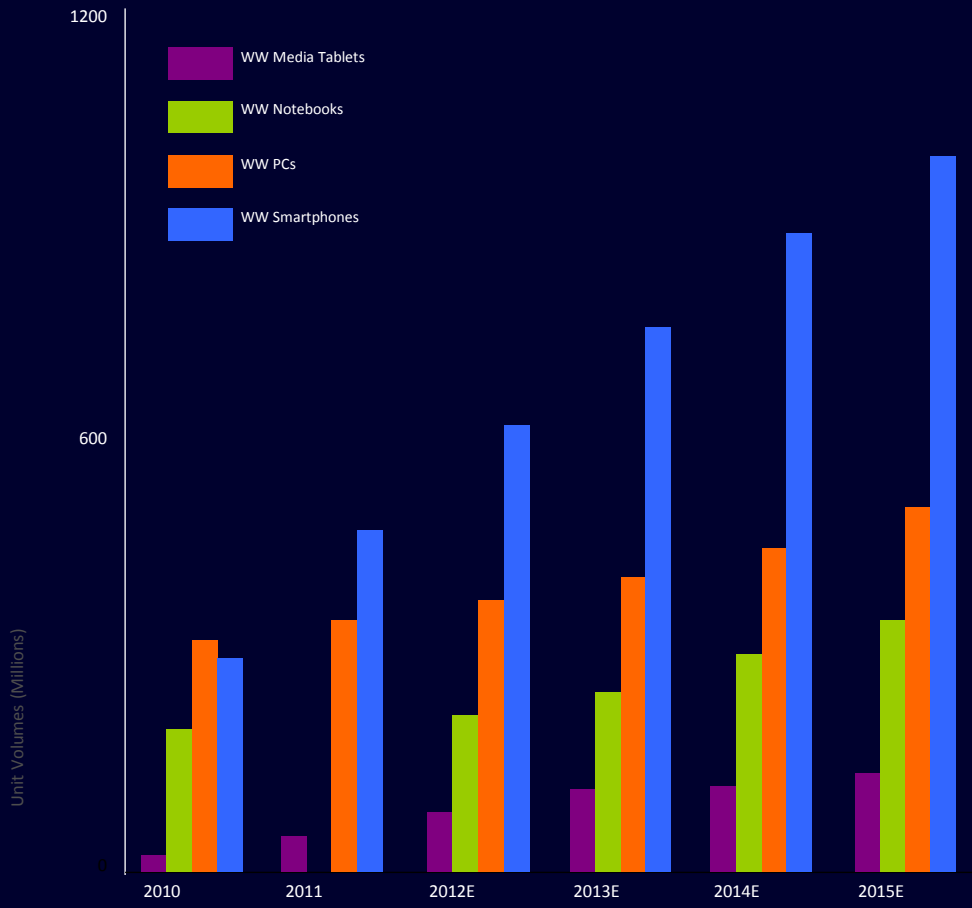
APP & DISPOSITIVOS PERSONALES

dentro de organización:

- **dificultad en sostener políticas para dispositivos personales fuera de red empresa**

soporte de organización:

- **movilidad es estrategia de negocio: "asegurar dispositivos móviles”**



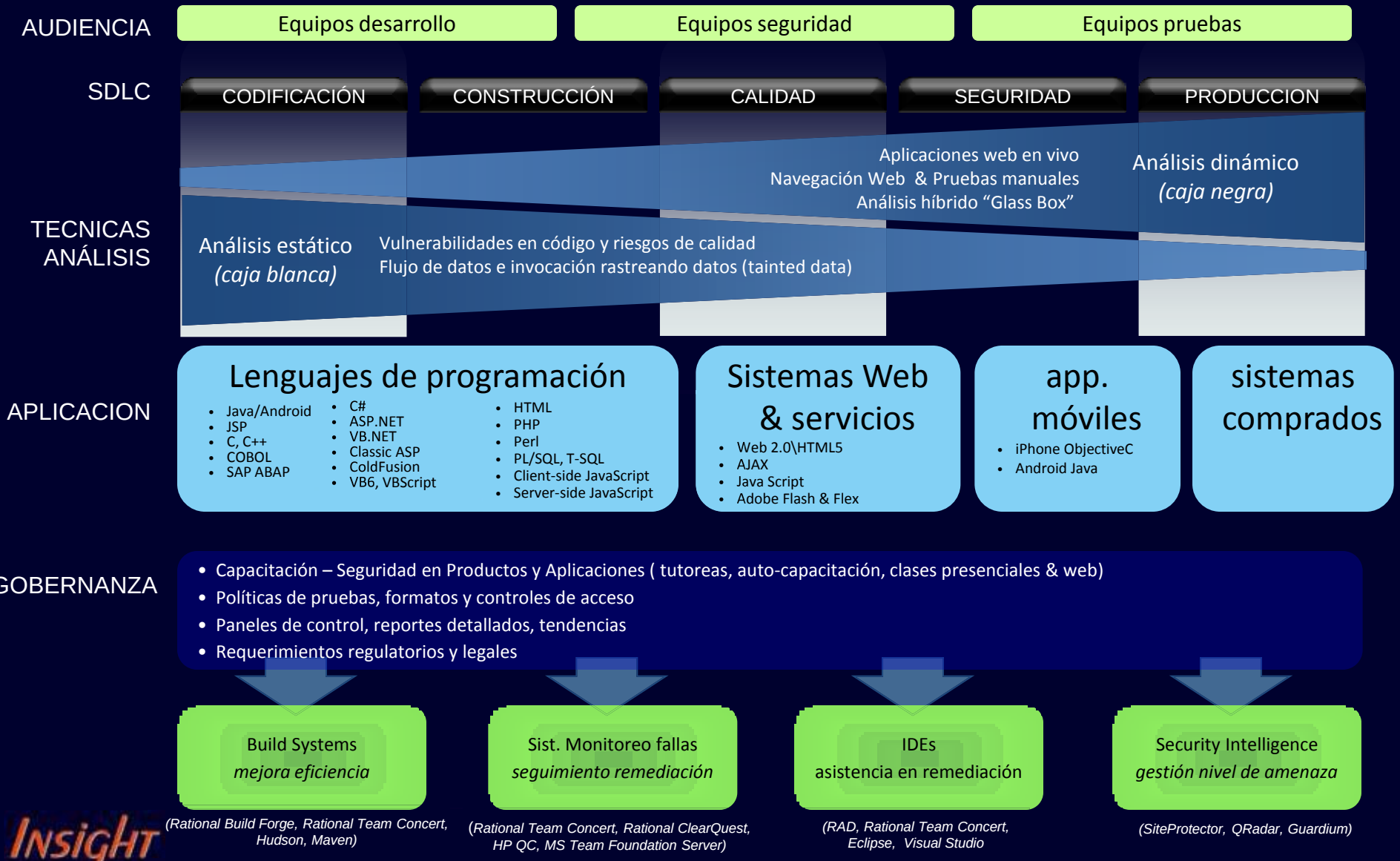
Fuente: *“Fostering the People: The Shift to Engagement Apps ”,* Wells Fargo Securities, January 23, 2012

INTERÉS ESTRATÉGICO

Seguridad institucional

- Conformidad: auditorías, consultoría, QA
- CISO - Oficial de seguridad de información
  - políticas: definición, implementación, supervisión
  - respuesta a incidentes, investiganción forense
  - arquitectura de seguridad
  - planes: recuperación desastres, continuidad opr.

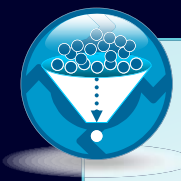
alcance


AUDIENCIA
Equipos desarrollo
Equipos seguridad
Equipos pruebas
SDLC
CODIFICACIÓN
CONSTRUCCIÓN
CALIDAD
SEGURIDAD
PRODUCCION
TECNICAS ANÁLISIS
Aplicaciones web en vivo
Navegación Web & Pruebas manuales
Análisis híbrido "Glass Box"
Análisis dinámico
(caja negra)
Análisis estático
(caja blanca)
Vulnerabilidades en código y riesgos de calidad
Flujo de datos e invocación rastreando datos (tainted data)
APLICACION
Lenguajes de programación
Java/Android
JSP
C, C++
COBOL
SAP ABAP
C#
ASP.NET
VB.NET
Classic ASP
ColdFusion
VB6, VBScript
HTML
PHP
Perl
PL/SQL, T-SQL
Client-side JavaScript
Server-side JavaScript
Sistemas Web & servicios
Web 2.0\HTML5
AJAX
Java Script
Adobe Flash & Flex
app. móviles
iPhone ObjectiveC
Android Java
sistemas comprados
GOBERNANZA
Capacitación – Seguridad en Productos y Aplicaciones (tutoreas, auto-capacitación, clases presenciales & web)
Políticas de pruebas, formatos y controles de acceso
Paneles de control, reportes detallados, tendencias
Requerimientos regulatorios y legales
Build Systems
mejora eficiencia
(Rational Build Forge, Rational Team Concert, Hudson, Maven)
Sist. Monitoreo fallas
seguimiento remediación
(Rational Team Concert, Rational ClearQuest, HP QC, MS Team Foundation Server)
IDEs
asistencia en remediación
(RAD, Rational Team Concert, Eclipse, Visual Studio
Security Intelligence
gestión nivel de amenaza
(SiteProtector, QRadar, Guardium)

contexto de seguridad

capacitación &
concientización

programación segura



planificación
de proyectos

pruebas y evaluaciones
de vulnerabilidades

framework
ingeniería

evaluación
de riesgo

documentacion

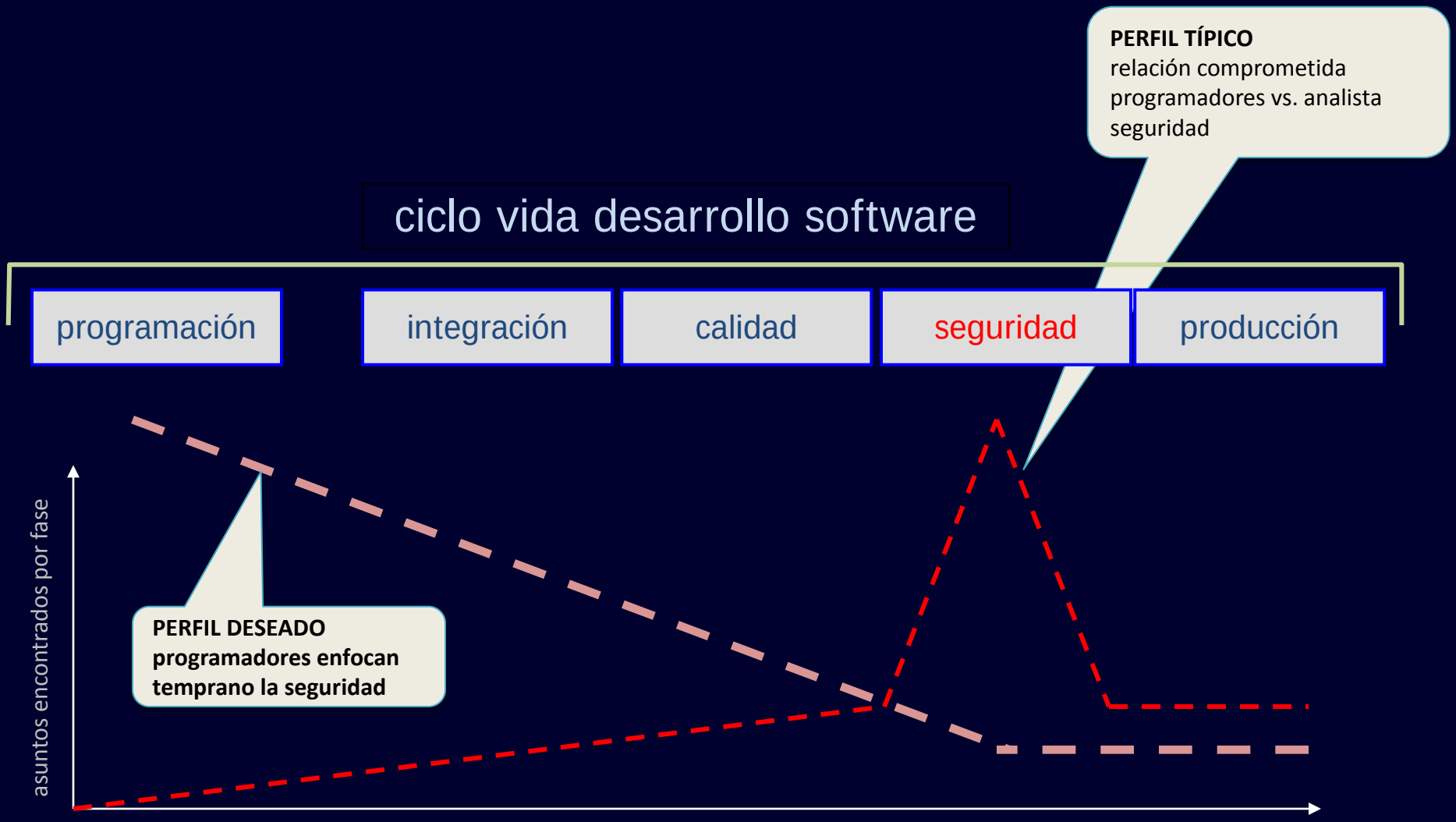
requerimientos
de seguridad

respuesta a
incidentes

SEGURIDAD en el CICLO de VIDA

IMPACTO
& COSTO

CICLO de VIDA de APLICACIONES



CICLO de VIDA de APLICACIONES

ciclo vida desarrollo software

programación	integración	calidad	seguridad	producción

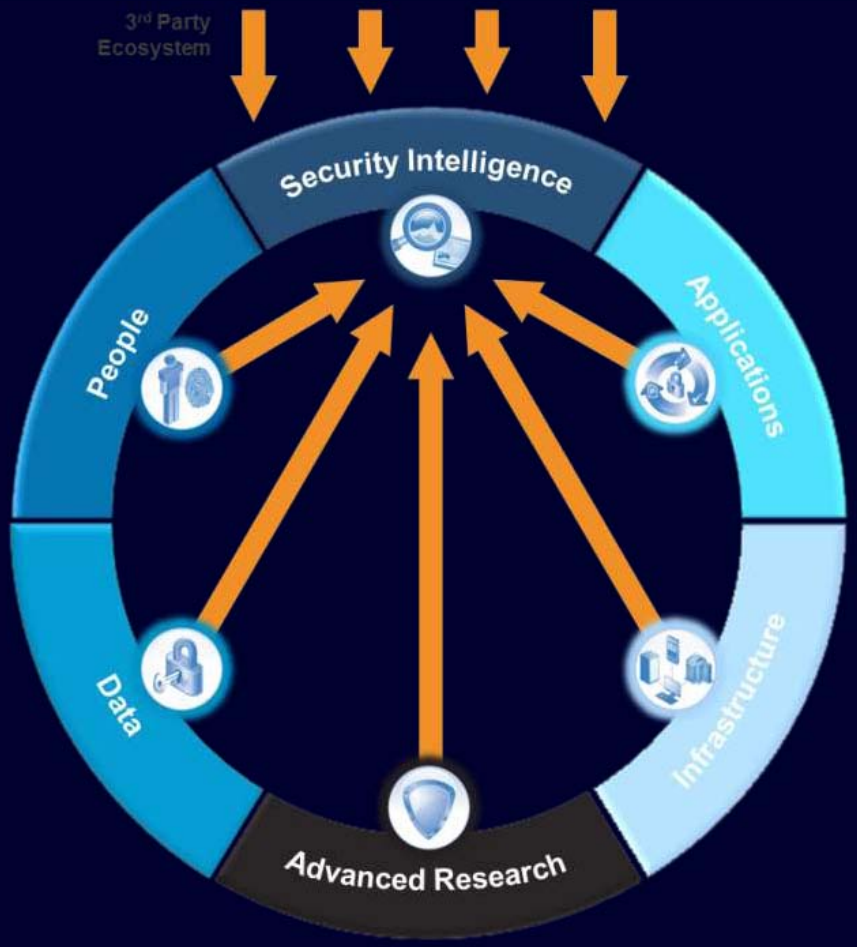
COSTO por DEFECTO encontrado en cada FASE

80 USD	**240 USD**	**960 USD**	**7.600 USD**
1	**x 3**	**x 12**	**x 95**

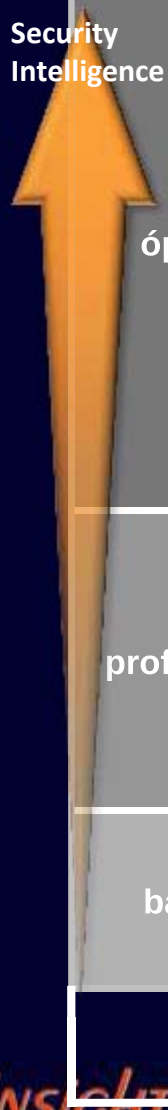
*Based on X-Force analysis of 100 vulnerabilities per application

contexto seguridad: aplicaciones ++

- arquitectura
- personal
- datos
- **aplicaciones**
- infraestructura
- investigación



contexto : optimización en fases



	Contexto de seguridad: gestión de información y eventos, correlacionamiento y profundidad en análisis, investigación en amenazas externas			
óptimo	Análisis basado en roles Gobernanza en identidad Controles de usuarios con privilegios	Análisis de flujo de datos Gobernanza de datos	Procesos de ingeniería seguros Detección de fraudes	Monitoreo de red avanzada Forense / minería de datos Sistemas de seguros
profesional	Gestión de usuarios y acceso Autenticación fuerte	Monitoreo vulnerabilidad base datos y de acceso Prevención pérdida de datos	Escaneo Glass box Análisis estático	Seguridad en virtualización Gestión de activos Gestión de seguridad en redes
básico	Gestión centralizada	Encriptado Control de acceso	Análisis dinámico	Seguridad perimetral Anti-virus
	personal	**datos**	**aplicaciones**	**infraestructura**

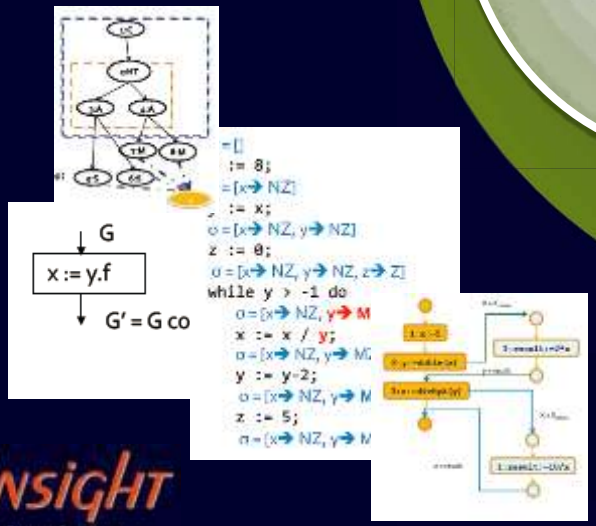
SEGURIDAD en el CICLO de VIDA

ANÁLISIS de SEGURIDAD

PROGRAMCIÓN: análisis seguridad

análisis código fuente:
datos, punteros,
vectores, flujo,
expresiones, …

análisis caja blanca
casos desde código fuente
análisis caja negra
casos desde especificación



"Static Analysis can reduce defects by up to a Factor of six!"
(Capers Jones, Software Productivity Group)

INSIGHT
Software Code Root

Análisis de código

- **Problema de halting**

  Alan Turing proved in 1936 that a general algorithm to solve the halting problem for *all* possible program-input pairs cannot exist.

  http://en.wikipedia.org/wiki/Halting_problem

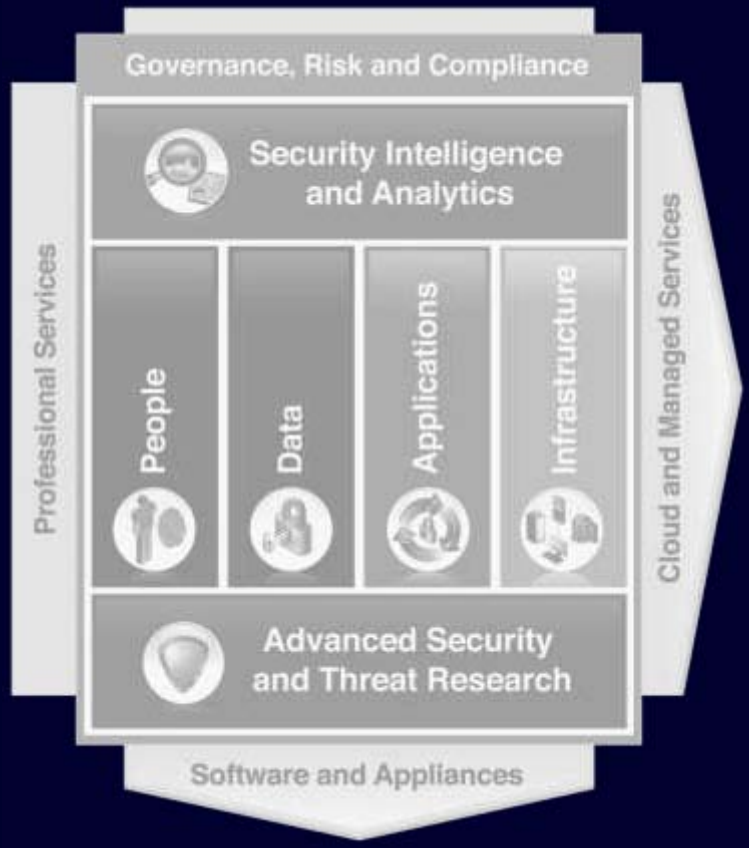
- **Métodos heurísitcos**

  análisis automático: criterios inteligentes

HERRAMIENTAS: análisis de código

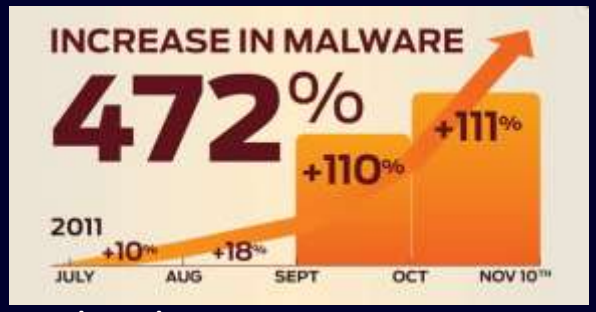
inspección

- **manual**
  auditorías de calidad vs. políticas
- **asistida por software**
  appScan, otros.



alcance

- integrar análisis **estático** & **dinámico** de código en evaluación de seguridad, mejorando cobertura.
- incluir pruebas de vulnerabilidades, por plataforma y arquitectura donde se libera produtco (client, server, mobile, web,…)



android

CICLO de VIDA

desarrollo de aplicaciones seguras

requerimientos

- **pre-liberación software**
  (diseño, programación, construcción, prueba)

  - políticas de riesgo: evaluación riesgo
  - definición de requerimientos de seguridad
    (accseso, auditoría, multi-sesión, trazabilidad, ...)
  - ciclo de iteración: revisión vulnerabilidades en código y revisión vulnerabilidades en aplicativo funcionando
  - auditoría de seguridad

requerimientos

- **software en producción**
  - monitoreo recursos ambiente de producción
  - control de acceso e identificación *(usuarios privilegiados, restricciones en horarios, dispositivos, etc.)*
  - protección de aplicaciones y servicios (servers app, sist. web, web-services)

SEGURIDAD en el CICLO de VIDA

- **herramientas**

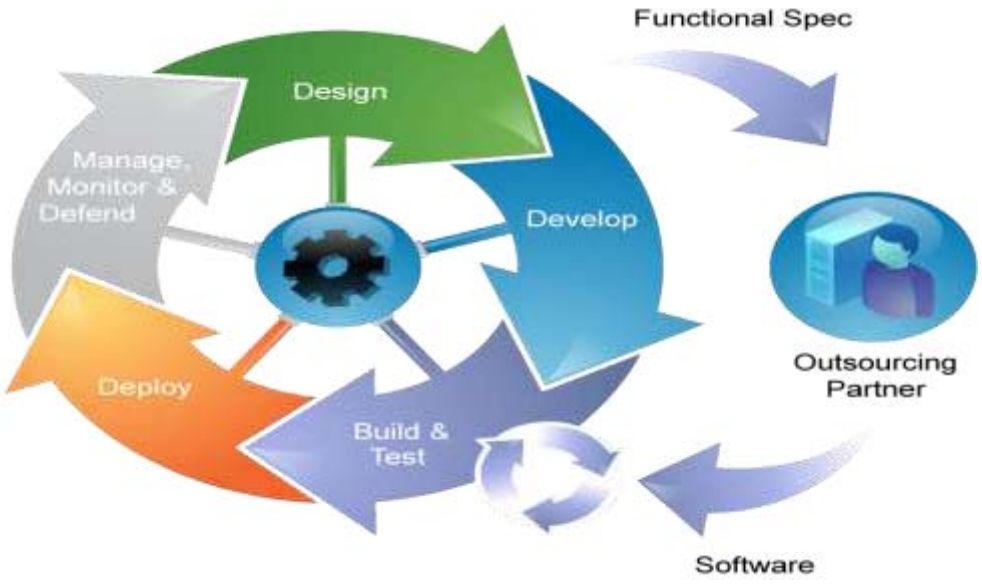
  uso de herramientas de gestión, análisis y control, asistiendo en el ciclo de desarrollo y liberación de software, es cada vez más una necesidad

  (costo fixes, pérdidas vs. costo herramientas)

integración !

Conectar áreas/silos en la organización

- Expertos en seguridad establecen políticas de pruebas de seguridad
- Equipos de desarrollo prueban temprano en ciclo vida
- Tratar vulnerabilidades como defectos de desarrollo

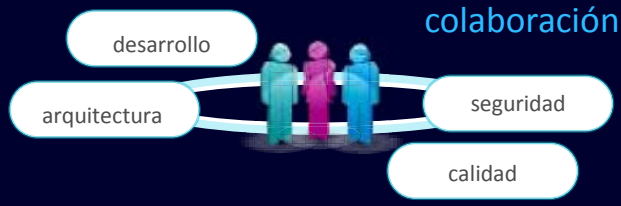


SEGURIDAD en el CICLO de VIDA

- **criterio**

  adoptar enfoque de asegurar desde el diseño, para generar aplicaciones y servicios más confiables y eficientes.

  vincular & comunicar estrechamente a desarrollo, calidad y seguridad, y dar visibilidad a gerencia por resultados



SEGURIDAD en el CICLO de VIDA

es buena idea, hacer el ejercicio de cuantificar cuanto cuesta invertir en seguridad !

INSIGHT

SEGURIDAD en el CICLO de VIDA

gracias

INSIGHT

SOFTWARE DONE RIGHT

BEST PRACTICES | TOOLS | TEST AUTOMATION | SECURITY | TRAINING

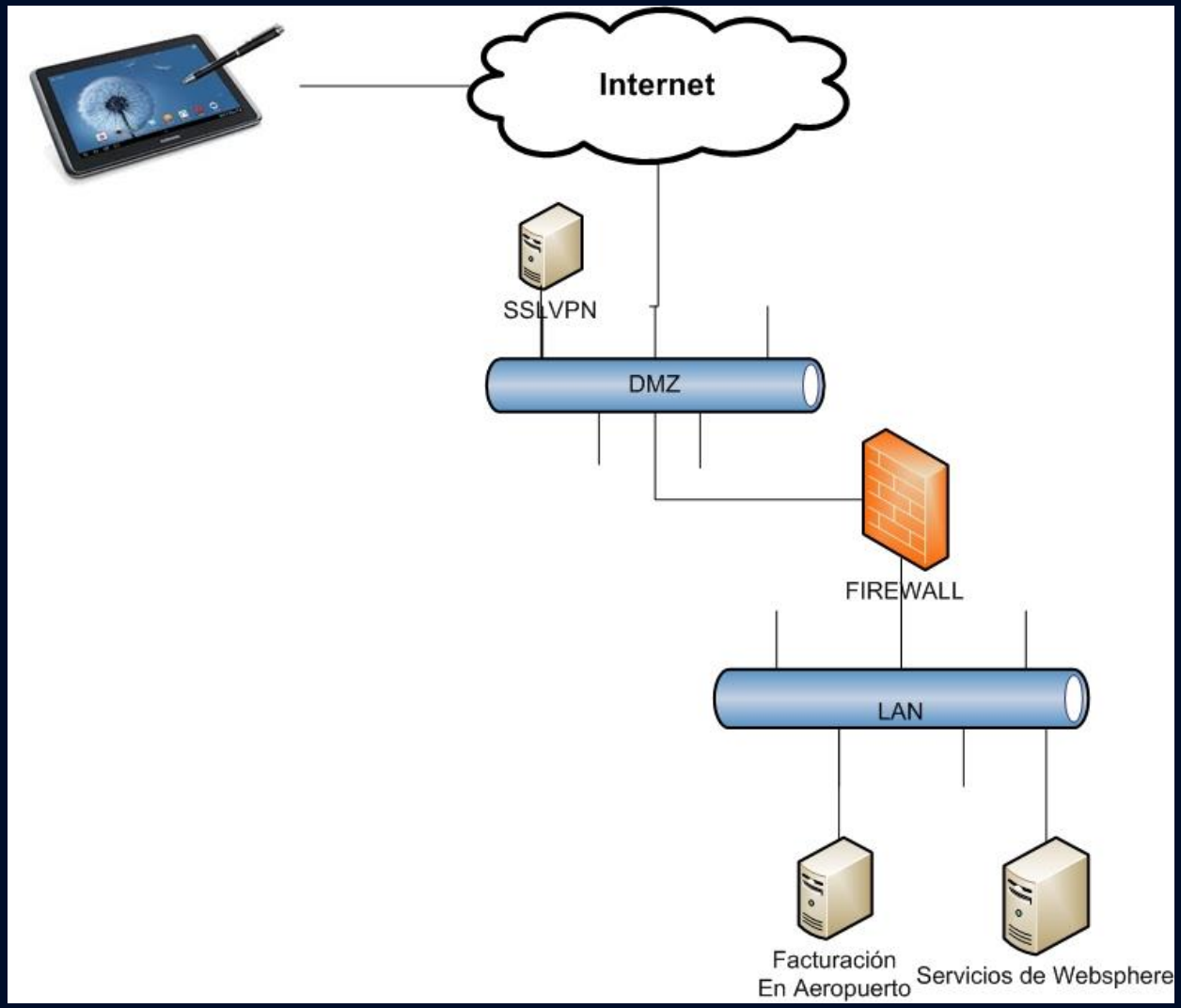
BOGOTA | MEXICO | MONTEVIDEO

Experiencia de ejecución APPSCAN en ANCAP

Criticidad y arquitectura de las aplicaciones

- Facturación en Aeropuertos
  - Permite incluir el requerimiento de la DGI en la facturación en Aeropuertos
  - Sustitución de Facturas en papel e incorporación de ticket electrónico (salvo contingencia)
  - Minimizar pérdida o daño de facturas en papel
  - Facturación desde la pista sin necesidad de dirigirse a una oficina.

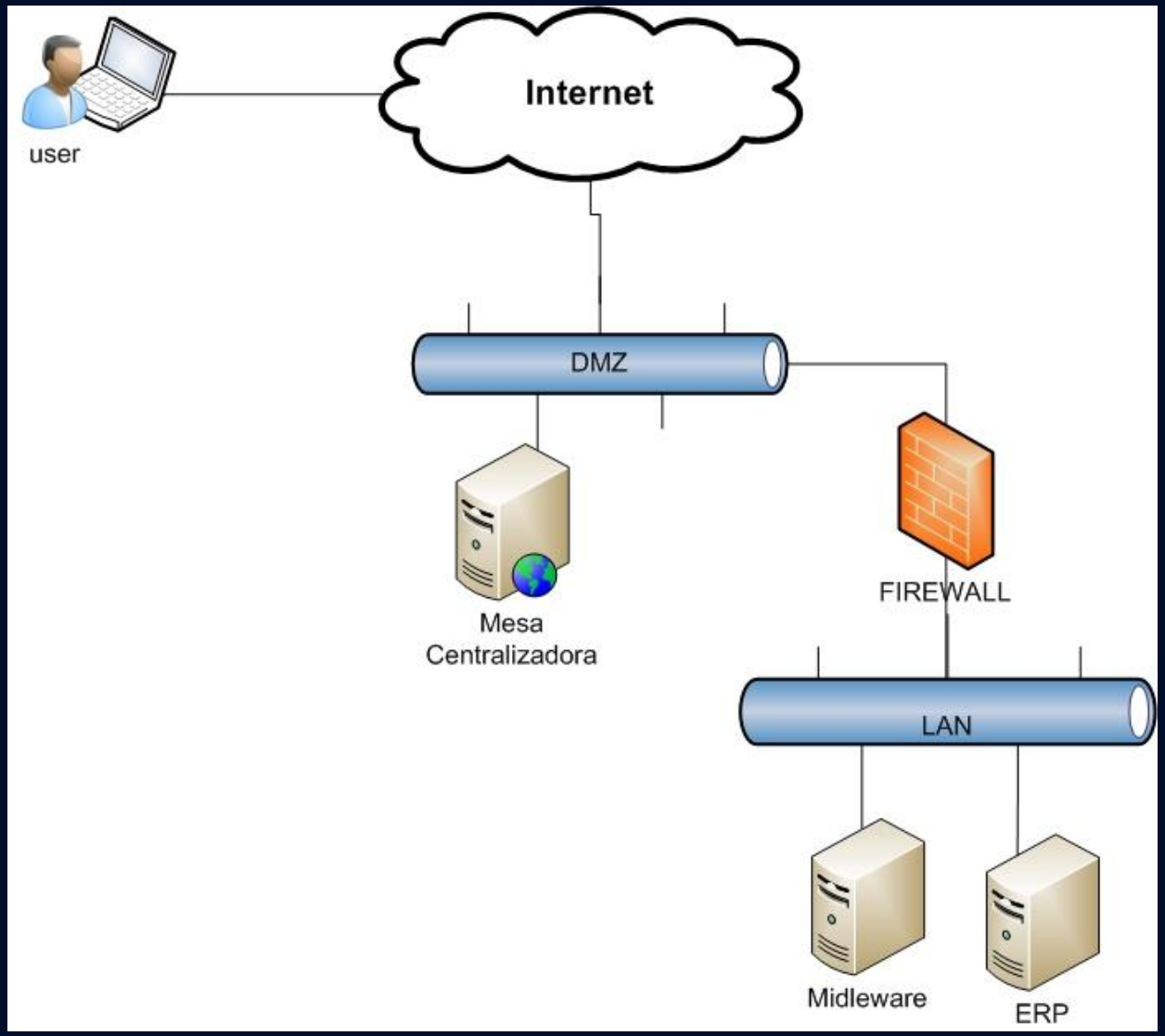
Criticidad y arquitectura de las aplicaciones



Criticidad y arquitectura de las aplicaciones

- Mesa Centralizadora
  - Permite el ingreso de facturas a proveedores que no poseen facturación electrónica
  - Único punto de acceso para dichos proveedores
  - Mitigar la pérdida o daño de facturas en papel
  - Menor costo operativo a nivel empresarial

Criticidad y arquitectura de las aplicaciones



Criticidad y arquitectura de las aplicaciones

- Portal SAP
  - Permite la gestión de clientes y proveedores
  - Aplicativo que utiliza la empresa vinculada para publicar información del ERP de la misma empresa.

Planificación de las ejecuciones

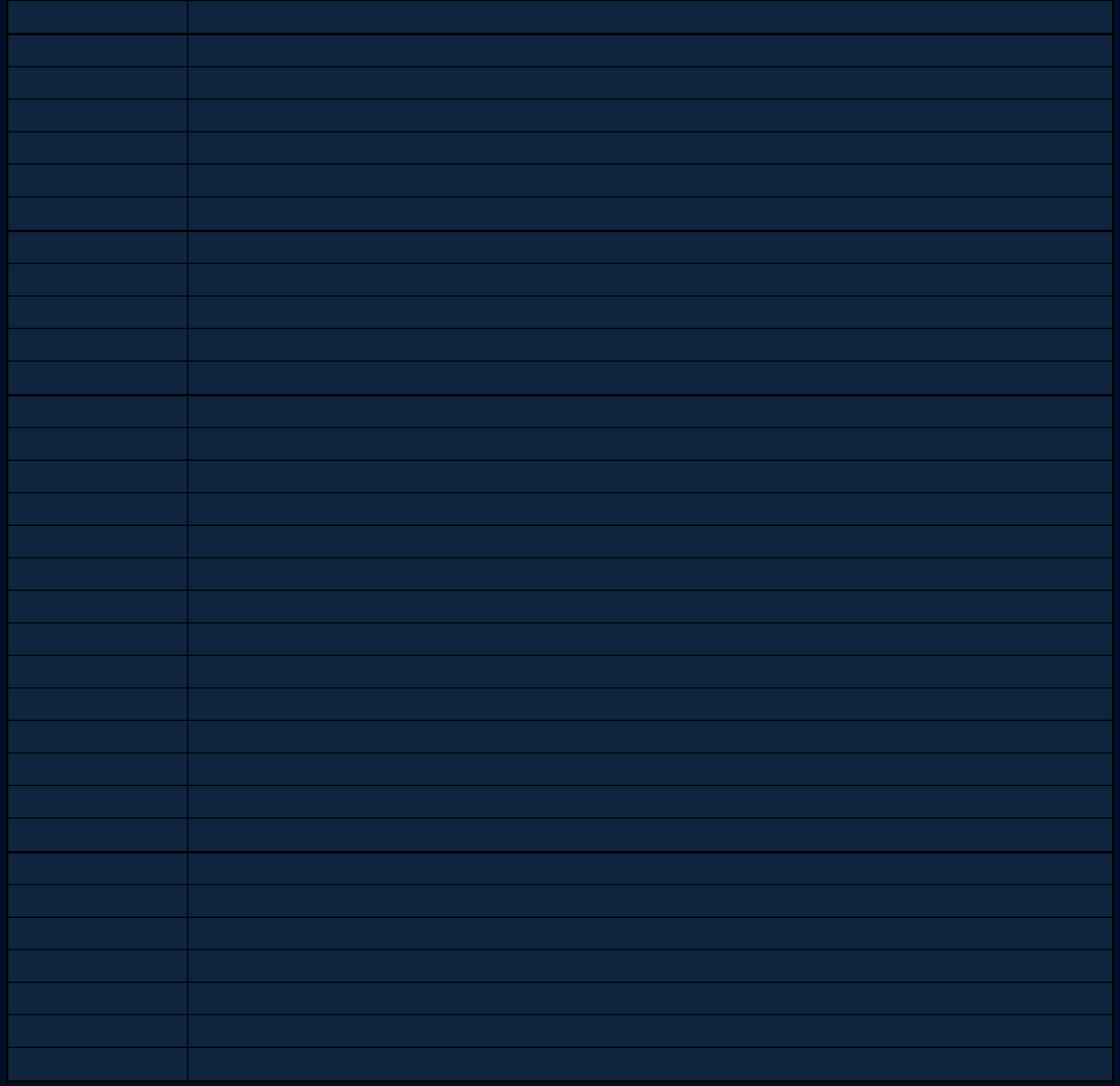
- ¿En qué componente se apuntó a ejecutar la herramienta?
  - Facturación en Aeropuerto: En los servicios web publicados desde Websphere
  - Mesa Centralizadora: En el Portal de la DMZ
  - Portal de SAP: En el primer componente desde el lado de ANCAP disponible en la DMZ

Planificación de las ejecuciones

- ¿Cuántas horas de esfuerzo se necesitaron?
  - Facturación en Aeropuerto: 25 horas totales
  - Mesa Centralizadora: 7 horas totales
  - Portal de SAP: 13 horas totales
- ¿Qué Skills se necesitan para realizar la ejecución y cuáles para el análisis?

Resultados de las ejecuciones

- Facturación en Aeropuertos:
  - 2 High
  - 2 Medium
  - 1 Low
  - 7 Informational
- Mesa Centralizadora:
  - 7 High
  - 6 Medium
  - 41 Low
  - 9 Informational
- Portal de SAP:
  - 0 High
  - 7 Medium
  - 38 Low
  - 33 Informational



Metodología de trabajo

- ¿Cuál sería la metodología de trabajo luego de las ejecuciones?
  - Analizar los resultados que forman parte de falsos positivos y descartarlos
  - Mitigación de vulnerabilidades detectadas luego del filtro de falsos positivos previa salida a producción
  - Analizar si dichas mitigaciones eliminan varias vulnerabilidades que suelen ser repetidas en distintos Webservices (módulo de acceso a la base de datos)
  - Volver a realizar una nueva ejecución de forma corroborar la mitigación de las vulnerabilidades subsanadas

Metodología de trabajo

- ¿Cuál sería la metodología de trabajo luego de las ejecuciones?
  - Contar con Análisis Delta que compara las ejecuciones y muestra los resultados obtenidos en base a la primera ejecución
  - Proponer de incorporar la ejecución de la herramienta en cada liberación de la aplicación
  - Adopción de la herramienta por el equipo de testing (Área de Desarrollo) y un apoyo del Área de Seguridad Informática
  - Adoptar criterios de desarrollos más seguros y que contemplen ciertos riesgos conocidos.

Ventajas de contar con APPSCAN

- Herramienta que automatiza las pruebas y de fácil ejecución
- Los resultados deben ser tomados como un insumo del análisis, dado que pueden dar falsos positivos.
- Es un software por lo que se puede ejecutar en diversos ambientes.
- Permite hacer testeos manuales y visualización de resultados.

Desafíos

- Ejecutar la herramienta en ambientes no Web (Tablet, Smartphone, etc)
- Incorporar la herramienta en el ciclo de vida del desarrollo.
- Exigir a empresas vinculadas que en sus aplicaciones se ejecute la herramienta
- Armar un Equipo de testing con especialistas para el análisis de resultados.

¿Preguntas?

Gracias

Contacto:
Victor Tassino
vtassino@ancap.com.uy