LOS LIMITES DE LA SEGURIDAD TRADICIONAL EN BIG DATA

Francisco Medero
Sr. Systems Engineer SoLA & Brazil

RSA EMC²

¿Cuál es el contexto tecnológico actual?

BILLONES
DE USUARIOS

3RA PLATAFORMA

2010

Móviles Nube Big Data Social

DISPOSITIVOS MOVILES

MILLONES
DE APLICACIONES

CIENTOS DE MILLONES
DE USUARIOS

2DA PLATAFORMA

1990

LAN/Internet Cliente/Servidor

PC

CIENTOS DE MILES
DE APLICACIONES

MILLONES
DE USUARIOS

1RA PLATAFORMA

1970

Mainframe, Mini Computadoras

Terminales

MILES
DE APLICACIONES

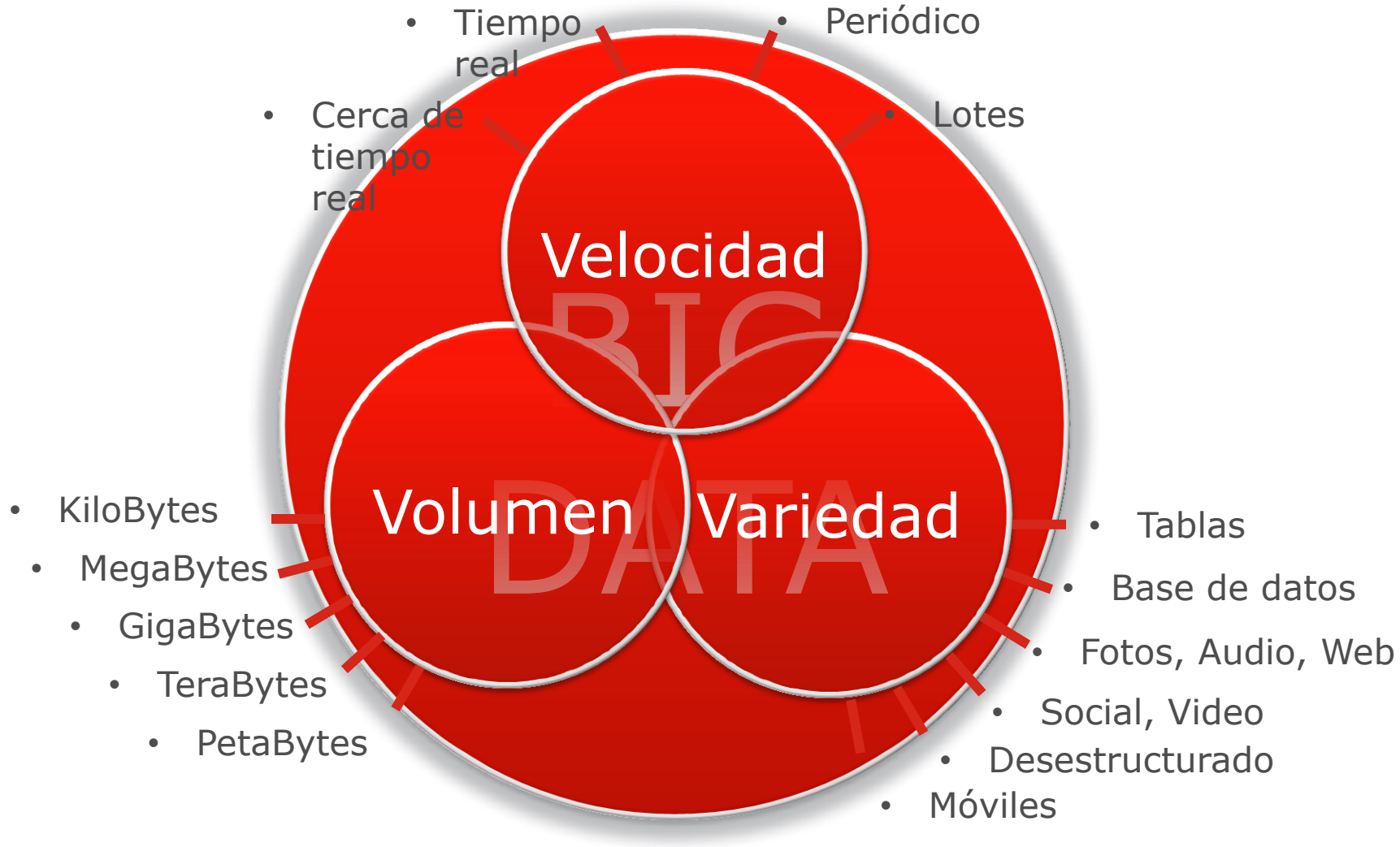
Fuente: IDC, 2012

¿Qué es el BIG DATA?

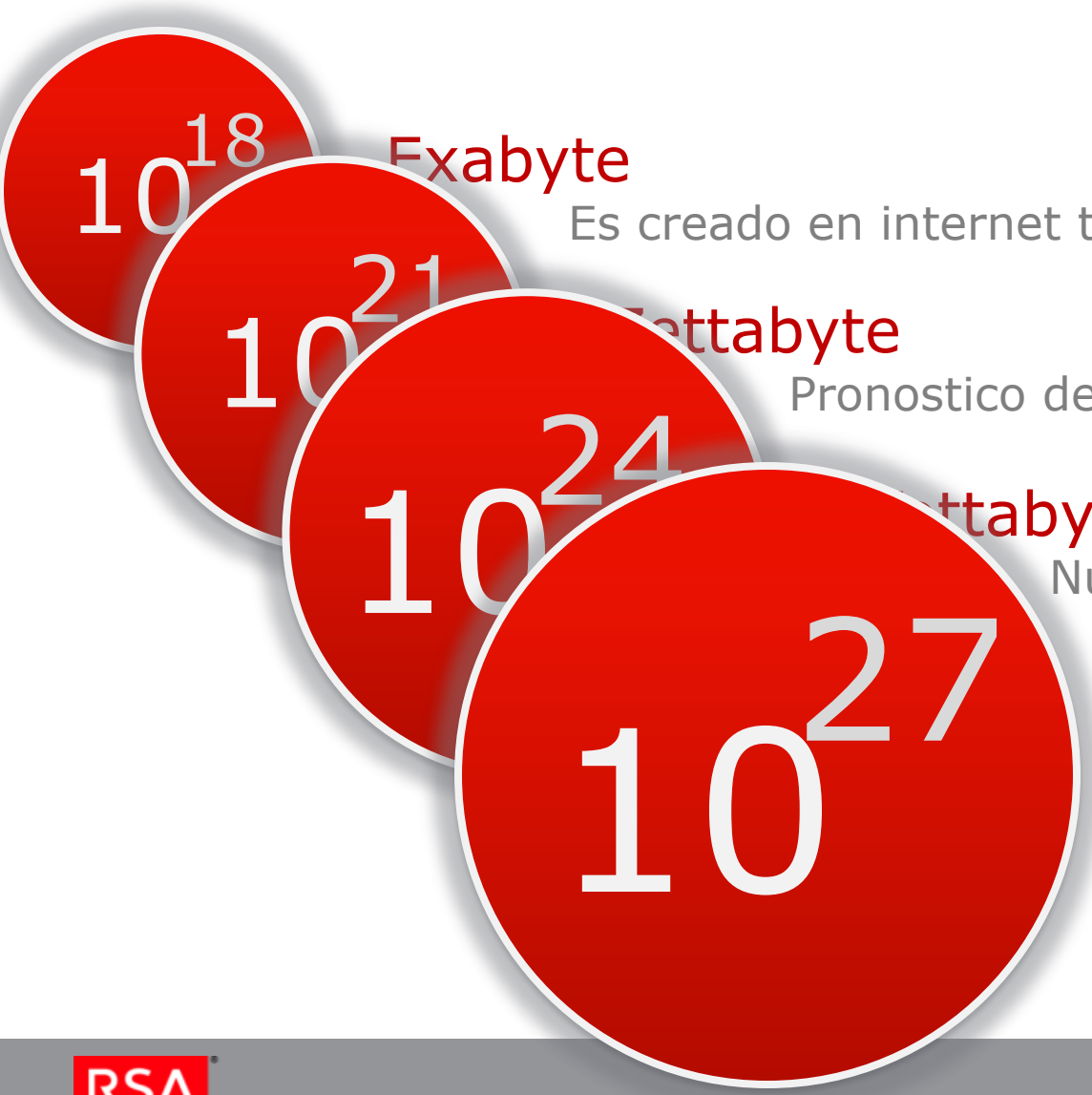
Definición:

"Big data" es un término aplicado a conjuntos de datos cuyo tamaño va más allá de la capacidad de captura, almacenado, gestión y análisis de las herramientas de base de datos actuales".

Las 3V…



BIG DATA en números



Exabyte
Es creado en internet todos los días

ttabyte
Pronostico de trafico de red anual para 2016

ttabyte
Nuestro Universo digital hoy

Brontobyte
Nuestro Universo digital del mañana

Quien los genera y consume?

Persona a Persona

- Blogs
- Comunidades virtuales
- Redes sociales
- E-mail
- Mensajería instantánea

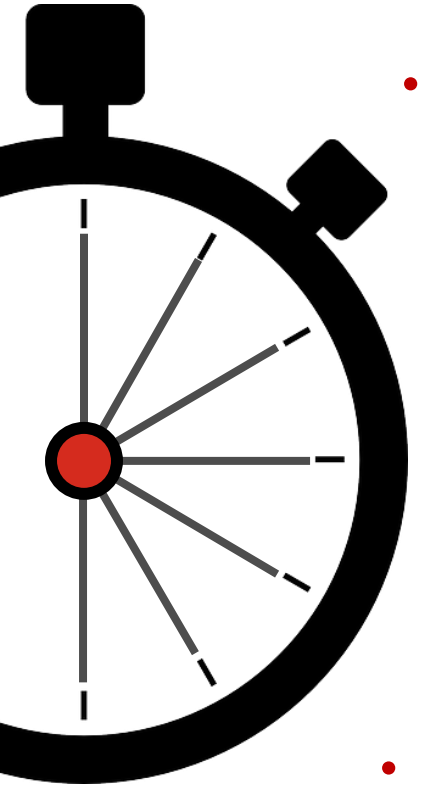
Persona a Maquina

- Repositorio de datos
- Dispositivos Médicos
- TV Digital
- Comercio Digital
- Tarjetas inteligentes
- Computadoras
- Móviles

Maquina a Maquina

- Sensores
- Dispositivos GPS
- Códigos de barra
- Escáneres
- Cámaras de Vigilancia
- Investigación científica

Un minuto de Big Data



- 347.222 imágenes son compartidas en Whatsapp
- 48.000 descargas de aplicaciones de Itunes
- 72 horas de video son subidas a Youtube
- 4.000.000 de búsquedas en Google
- 204.000.000 de emails son enviados
- 571 nuevos sitios son creados
- 70 dominios nuevos son registrados
- 278.000 tweets son generados en Twitter
- 2.460.000 posts compartidos en Facebook
- 1.400.000 minutos de conexión de usuarios de Skype

¿Cuál es el contexto de seguridad?

Contexto seguridad

INFRAESTRUCTURA

- Múltiples S.O
- Dispositivos Móviles
- Múltiples Dispositivos de Seguridad
- Nube
- Virtualización

PERSONAS

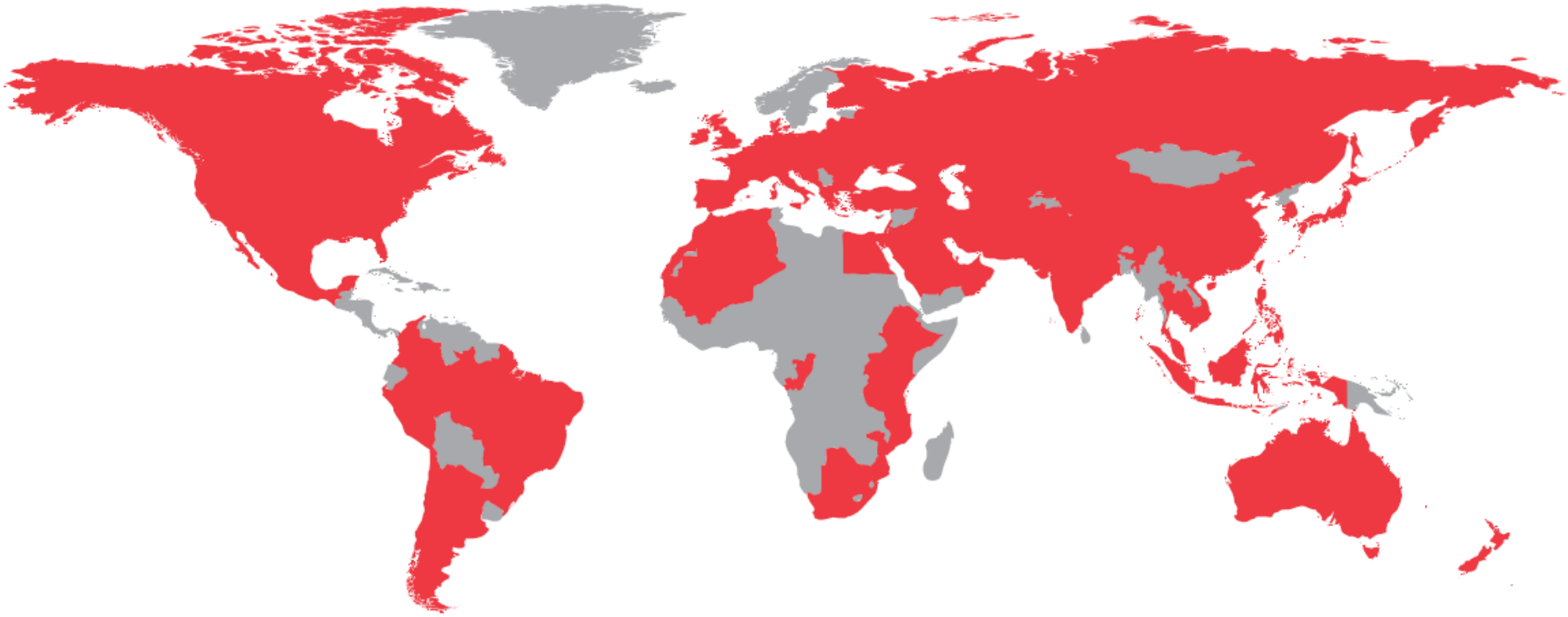
- Equipos Reducidos
- Falta de conocimiento / Inexperiencia
- Procesos obsoletos
- Baja Visibilidad y Control

AMENAZAS

- Atacantes motivados económicamente y políticamente
- Ataques sofisticados y más efectivos
- Crecimiento exponencial del malware

Estadísticas

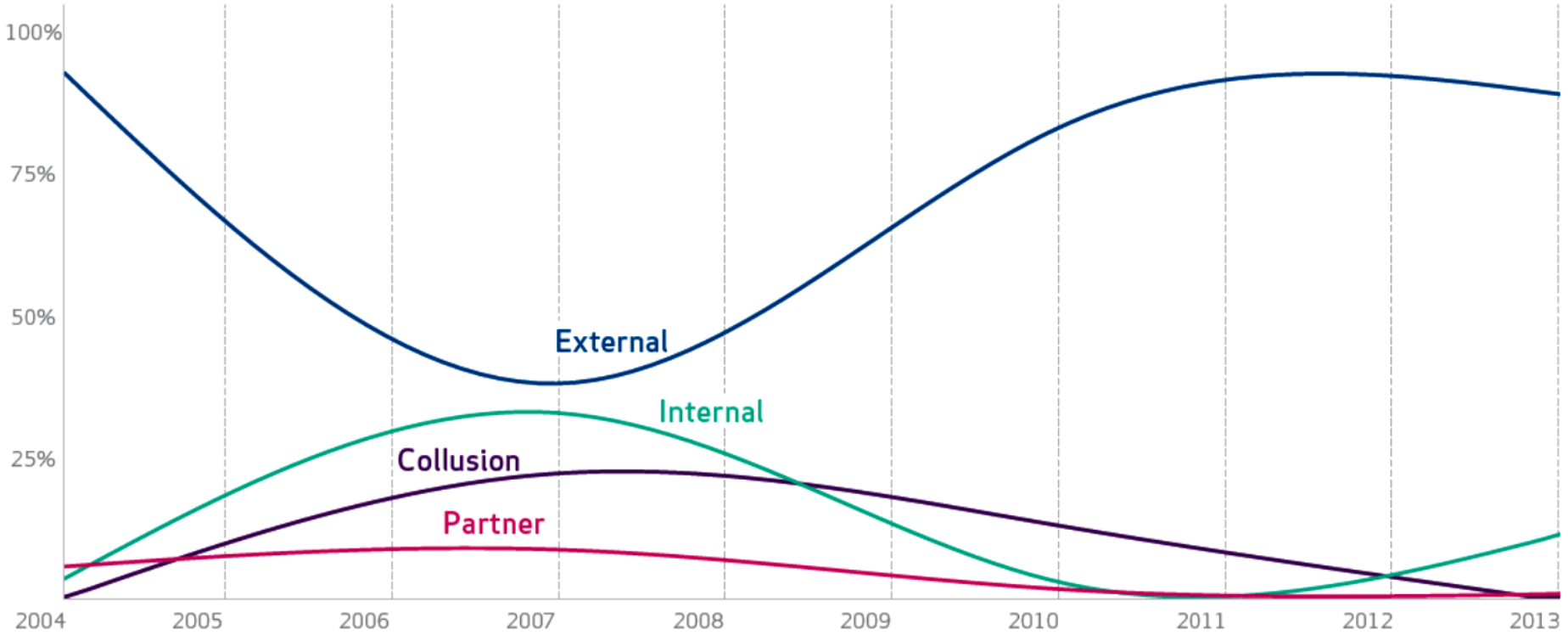
Mapa global de brechas de seguridad



Durante 2013 solo **27** países representaron el mapa de victimas de brechas de seguridad. Durante 2014 se encuentran **95** países representados. Un **350%** de incremento.

FUENTE: VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

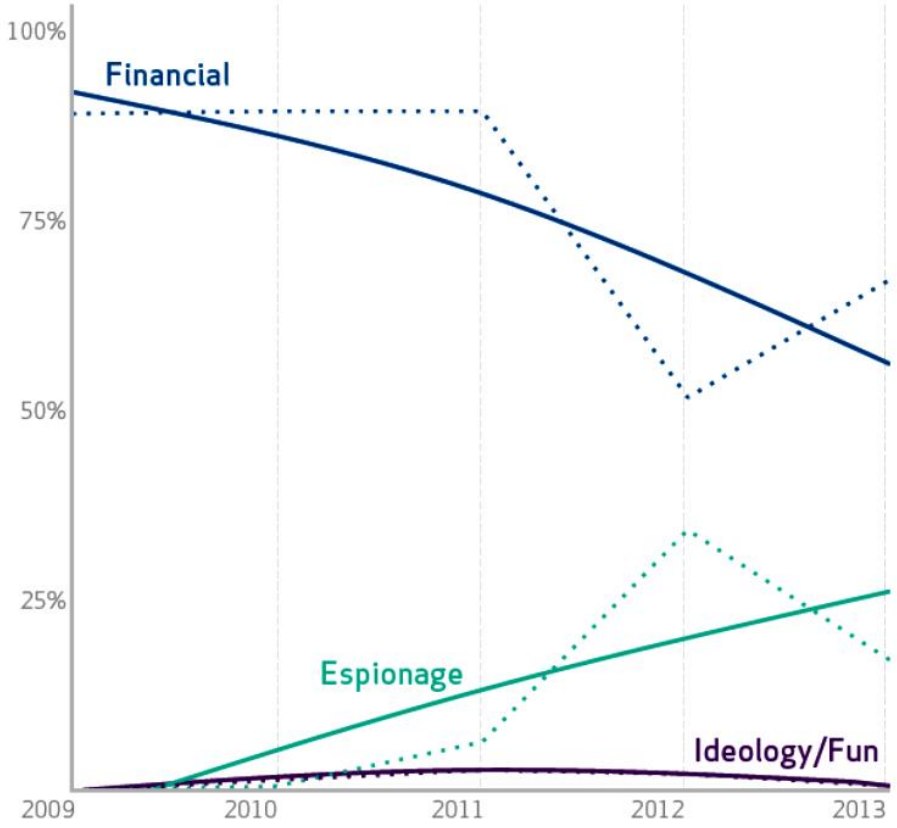
Porcentaje de brechas por tipo atacante…

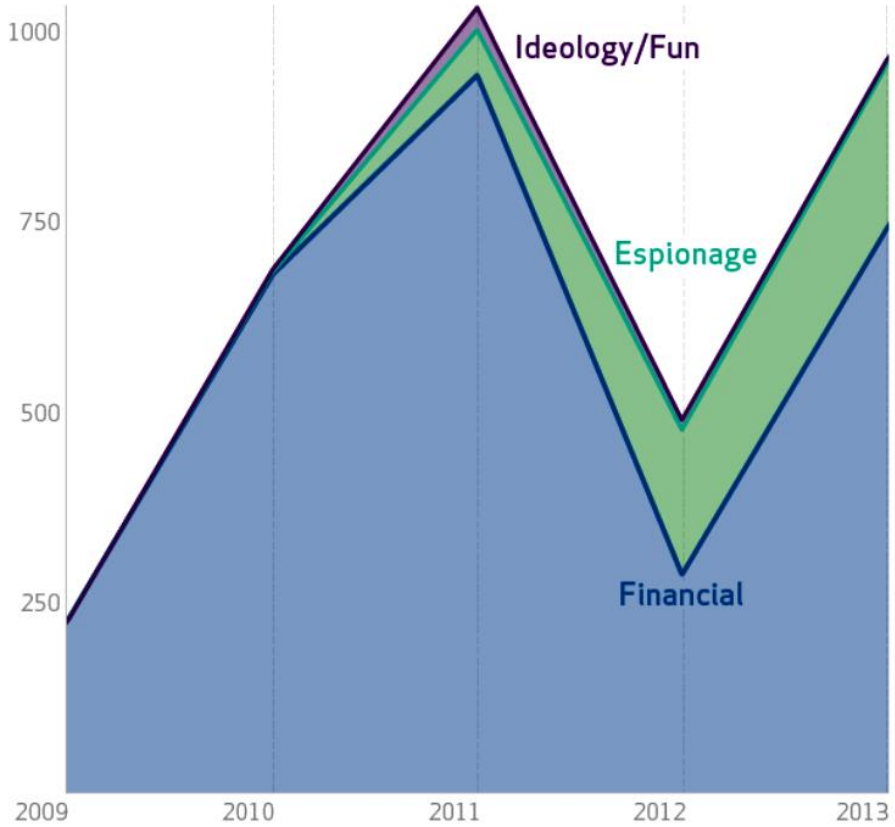


El mayor porcentaje de la brechas fueron ocasionadas por **ataques externos** y en menor medida por **usuarios internos**.

FUENTE: VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

Motivo de las brechas de seguridad

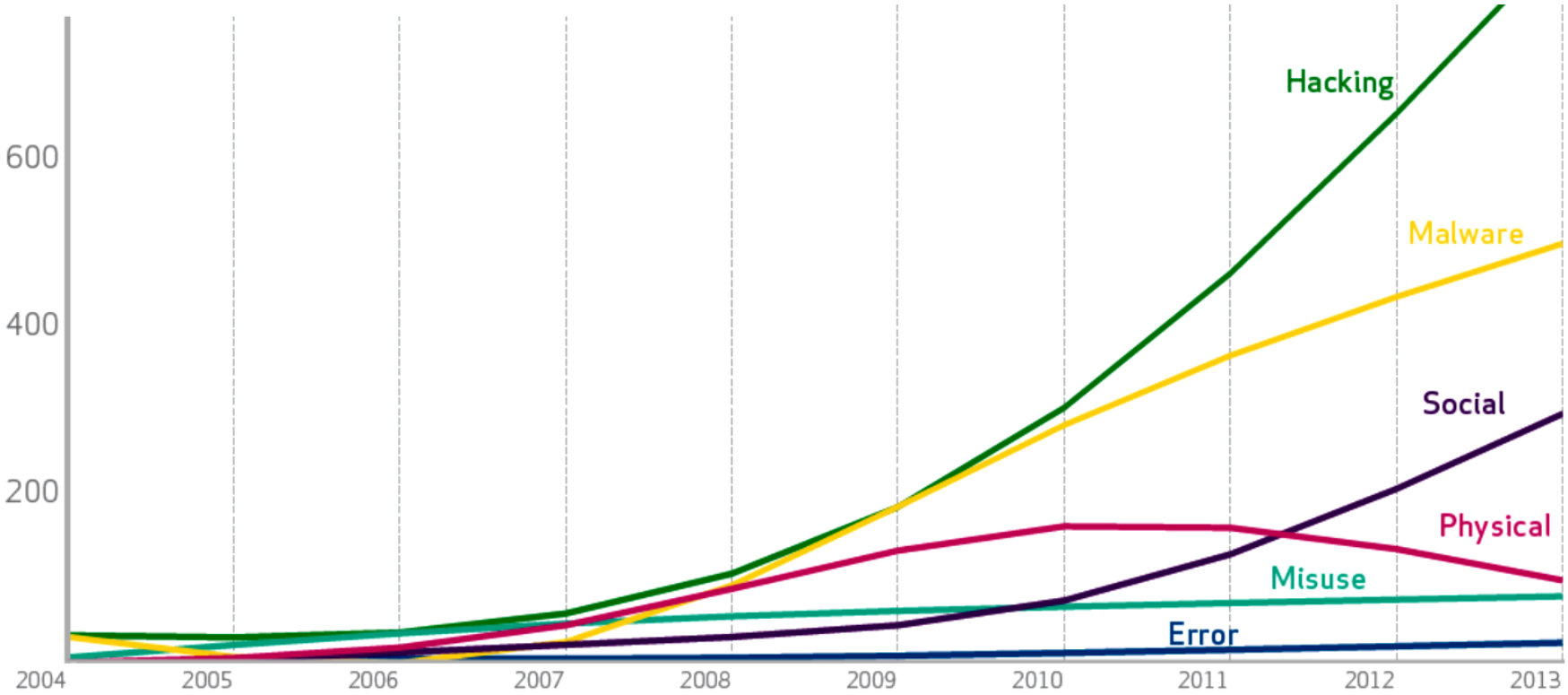




El principal motivo de las brechas de seguridad en porcentaje y volumen es el redito **Financiero**, seguido del **Espionaje**.

FUENTE: VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

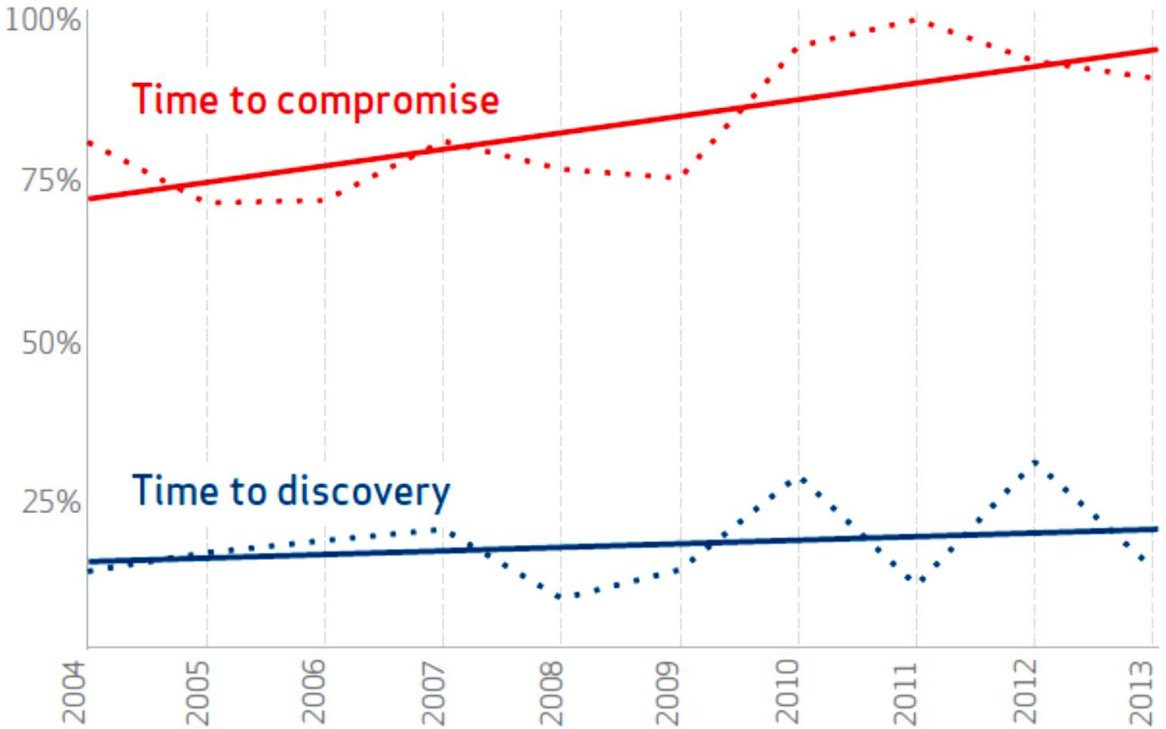
Tipo de amenazas utilizadas



El **Hacking**, **Malware** y los **Ataques de ingeniería social** son los principales mecanismos utilizados para concretar una brecha.

FUENTE: VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

Tiempo de compromiso vs tiempo de descubrimiento



El **99%** de las veces el atacante puede generar una brecha en días o menos. En el **70%** de los casos a las compañías les lleva semanas o más tiempo detectar las mismas.

FUENTE: VERIZON 2014 DATA BREACH INVESTIGATIONS REPORT

Adaptación de los ataques

2011 – Presente
Era de las redes de negocios y organizacionales
Motivación: Sabotaje, espionaje, ganancias, agenda política
Comportamiento: Persistir en la red
Virus: 2012 - Luckycat

2010 - Presente
Era de los dispositivos móviles
Motivación: Ganancias
Comportamiento: Abuso de servicio
Virus: 2011 DroidSMS

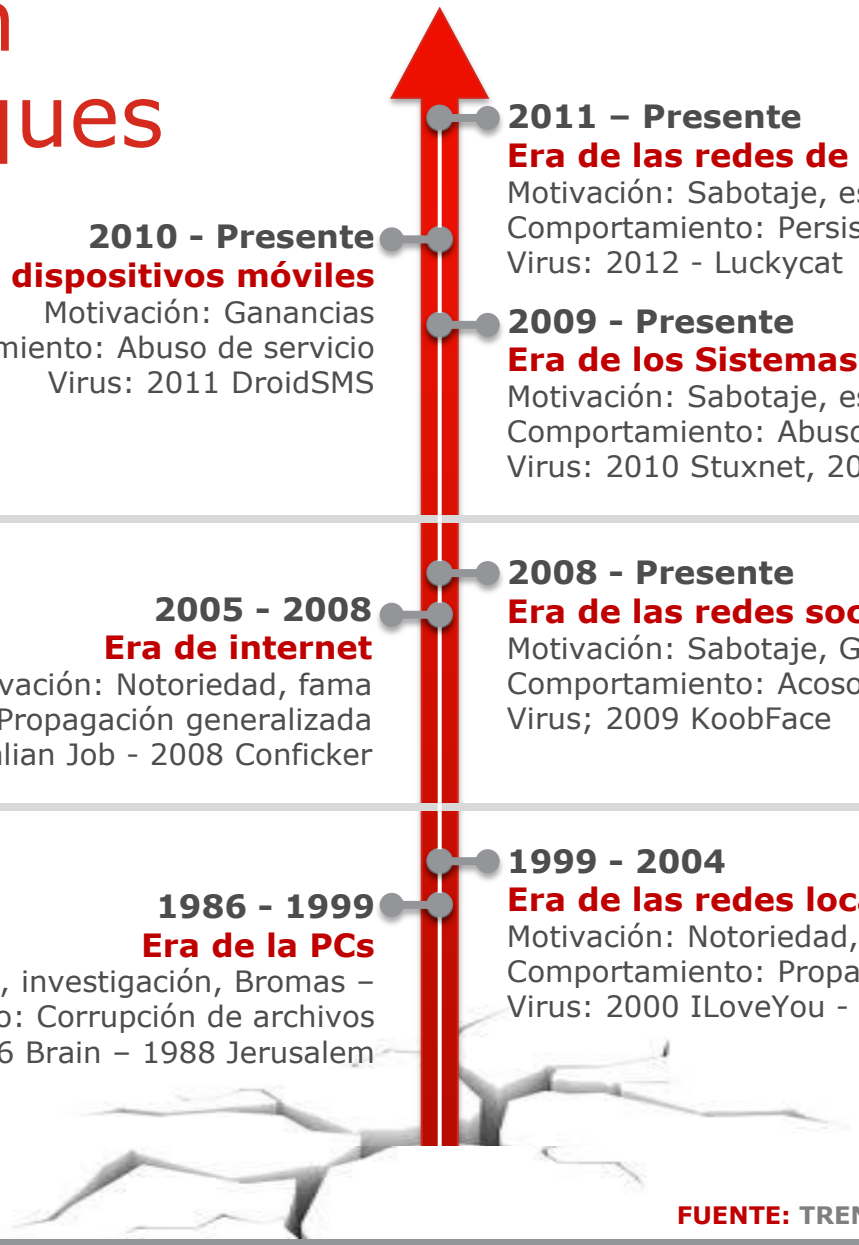
2009 - Presente
Era de los Sistemas de control industrial (ICS)
Motivación: Sabotaje, espionaje
Comportamiento: Abuso de infraestructura
Virus: 2010 Stuxnet, 2012 Flame

2008 - Presente
Era de las redes sociales
Motivación: Sabotaje, Ganancias
Comportamiento: Acoso social
Virus; 2009 KoobFace

2005 - 2008
Era de internet
Motivación: Notoriedad, fama
Comportamiento: Propagación generalizada
Virus: 2007 The Italian Job - 2008 Conficker

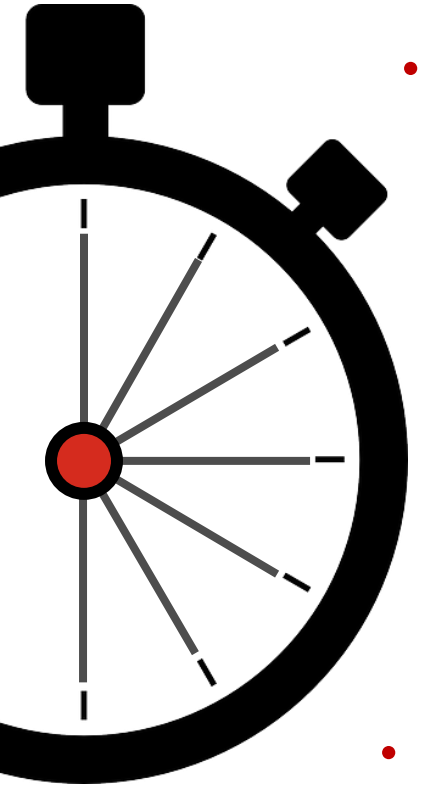
1999 - 2004
Era de las redes locales
Motivación: Notoriedad, fama
Comportamiento: Propagación generalizada
Virus: 2000 ILoveYou - 2001 Nimda – 2004 Blaster Sasser

1986 - 1999
Era de la PCs
Motivación: Vandalismo, investigación, Bromas –
Comportamiento: Corrupción de archivos
Virus : 1986 Brain – 1988 Jerusalem



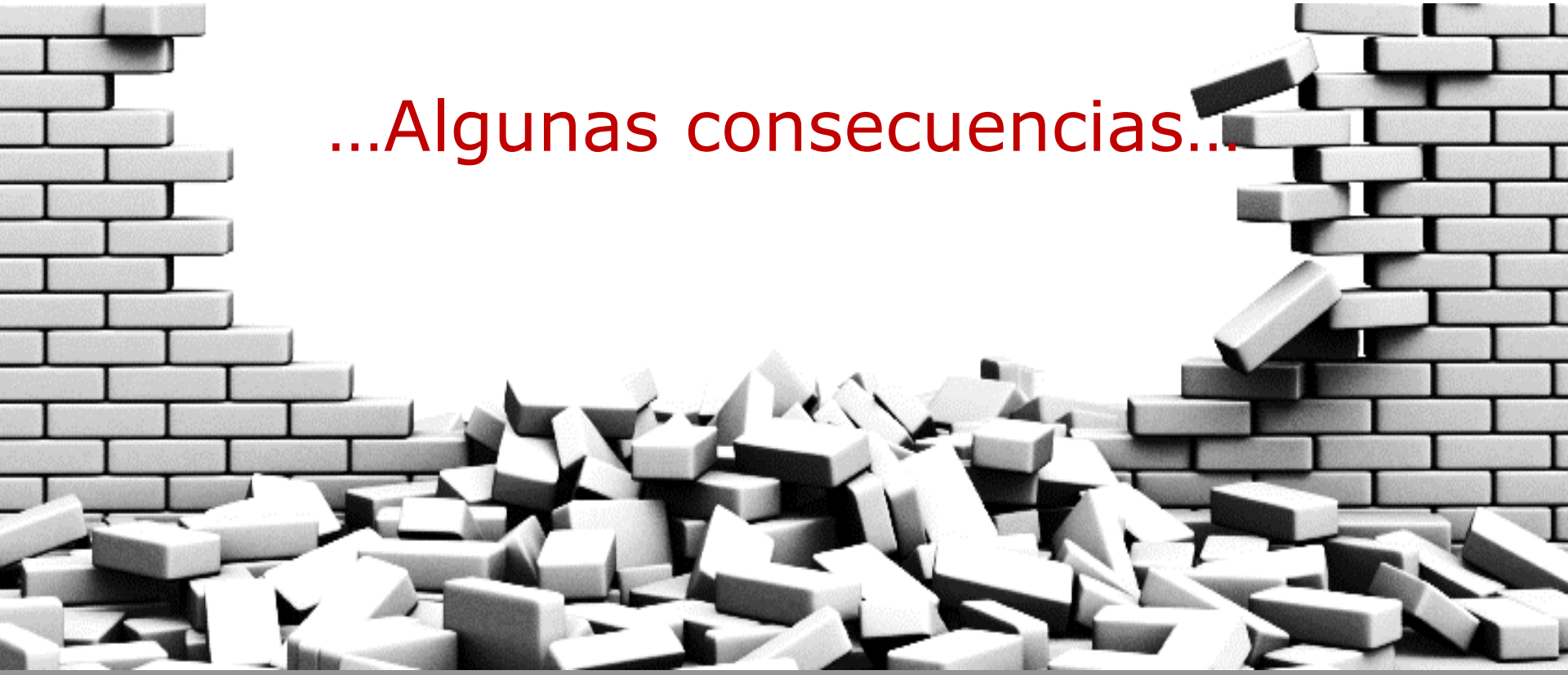
FUENTE: TREND MICRO HOW ATTACKS ADAPT 2013

Un minuto de inseguridad



- 240 nuevas variantes malware son generadas
- 5 nuevas variantes de malwares Android
- 5.700 ataques de malware a usuarios
- 90 cyber ataques son generados
- 1.080 infecciones de botnets
- 20 sitios son comprometidos
- 1 ataque de phishing es concretado
- 1 nuevo rasonware es dectectado
- 146.880.000 de correos spam son generados
- 20 nuevas victimas de suplantación de identidad

BIG DATA + CONTEXTO
(TECNOLOGIA x PERSONAS x SEGURIDAD)



Evernote sufre ataque cibernético a su seguridad

Sábado, 2 de marzo de 2013

La empresa de almacenamiento de información en línea, Evernote, pidió a todos sus usuarios que cambien sus contraseñas, a raíz de un ataque a su seguridad por parte de piratas cibernéticos.

La compañía -con sede en California- permite almacenar y organizar los datos personales en un servidor externo. Se cree que tiene cerca de 50 millones de usuarios.

Según el comunicado publicado por la empresa, los intrusos pudieron ver los nombres de usuario, las direcciones de correo electrónico y las contraseñas encriptadas.

Sin embargo, insistió en que "no hay evidencia" de que se cambiara o perdiera la información referente a información financiera o el contenido almacenado.

Evernote 2013
50 Millones de usuarios afectados

Linkedin 2012
6 Millones de usuarios afectados

LinkedIn es hackeado y más de 6 millones de contraseñas son filtradas

Hasta ahora sólo se han publicado las contraseñas, sin entregar datos de los usuarios vulnerados. LinkedIn no ha confirmado el ataque.

Emol — Miércoles, 6 de Junio de 2012, 09:46

Twittear 287 | +1 8 | Me gusta 269

MOSCÚ.- Según informa The Verge, la red social de "currículums" LinkedIn habría sido hackeada y más de seis millones de contraseñas habrían sido publicadas en un foro ruso por el mismo atacante.

Hasta ahora no hay mayor información, y LinkedIn no ha confirmado el ataque. A través de su cuenta en Twitter la empresa afirmó que "están revisando reportes de contraseñas robadas". La cifra exacta de cuentas vulneradas sería 6.458.020.

Sony se hará cargo de las pérdidas económicas del ataque a PSN

Se prevé que actuará de la misma forma en Europa.

Mireia Fernández | 27 de abril del 2011 varios GBA GameBoy Advance

El analista Michael Patcher ha informado que es muy probable que la situación europea de los usuarios de PSN sea la misma que los ubicados en Norteamérica, donde **Sony ha prometido reembolsar cualquier uso fraudulento de las tarjetas de crédito.**

*"En los Estados Unidos, **ningún cliente de PSN tendrá que pagar por el uso fraudulento de la tarjeta de crédito**, así que Sony trabajará con las entidades financieras para cubrir cualquier pérdida […] Por descontado, Sony se hará también responsable de reembolsar el coste de PlayStation Plus a sus subscriptores durante e tiempo en que el sistema permanezca inactivo […]"*

Patcher prevé que Europa recibirá un tratamiento parecido, sino igual, a éste y también quiere tranquilizar a los usuarios de PSN haciéndoles saber que muy probablemente, el hacker no esté interesado en el dinero ni en las tarjetas de crédito los jugadores sino en presumir y mostrar la escasa seguridad del sistema de Sony.

Sony 2011
25 Millones
de usuarios afectados
y tarjetas de crédito

Target Corp 2013
40 Millones
de usuarios afectados
y tarjetas de crédito

Hackean 40 millones de cuentas de Target en Estados Unidos

Target confirmó que alrededor de 40 millones de cuentas de tarjetas de crédito y débito quedaron comprometidas tras un ataque cibernético a la cadena de tiendas.

Compartir 0 Twittear 7 +1 0 Pin it Deja tu comentario

Target confirmó el hackeo de alrededor de 40 millones de cuentas. Foto: AP.

Target informó que las cuentas pueden haber sido afectadas entre el 27 de noviembre y el 15 de diciembre. Los datos robados incluyen nombres de clientes, **números de tarjetas de crédito y débito**, fechas de vencimiento y los códigos de seguridad de tres dígitos en el reverso de las tarjetas.

La compañía, con sede en **Minneapolis**, dijo que informó de inmediato a las autoridades e instituciones financieras una vez que conoció de la penetración, y que trabaja con una firma externa de pesquisas forenses para investigar lo sucedido. Dijo que está dedicando todos los "recursos apropiados" para resolver el problema.

Target Corp. dijo que los clientes que hicieron **compras** en sus **tiendas en Estados Unidos** durante el período en cuestión y sospechan de alguna actividad no autorizada en sus cuentas deben llamar al teléfono 866-852-8680. El robo de identidad también se puede denunciar a la policía o a la

La empresa Global Payments, encargada de procesar pagos en Estados Unidos, fue hackeada, poniendo en riesgo a millones de clientes de tarjetas de crédito.

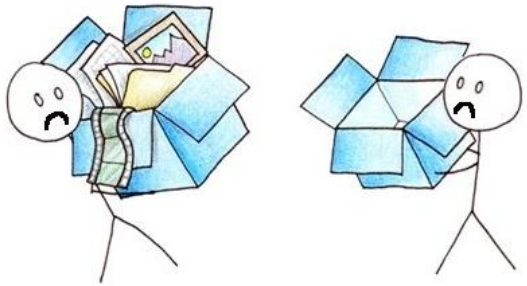
Visa y MasterCard están alertando a los bancos que trabajan con sus tarjetas sobre un ataque a uno de los sistemas de procesamiento de pagos en Estados Unidos. Unas 10 millones de tarjetas podrían estar afectadas, según reportó KrebsonSecurity. De acuerdo a la información entregada por el Journal, en tanto, la empresa encargada del procesamiento que sería *Global Payments*.

Visa Mastercard 2012
10 Millones
de usuarios afectados
y tarjetas de crédito

Dropbox 2012
7 Millones
de usuarios afectados

Dropbox admite el hackeo de sus cuentas y anuncia nuevas medidas de seguridad

por Drita 01 / 08 / 2012



Está claro que los hackers nunca dan tregua. El famoso servicio de almacenamiento en la nube, Dropbox, ha sufrido un importante ataque que ha puesto al descubierto las cuentas y contraseñas de numerosas personas. Tras los avisos de varios usuarios que ponían en alerta a la compañía sobre la recepción masiva de spam sospechosos, el equipo comenzó una investigación gracias a la cual han descubierto que efectivamente fueron hackeados y ya se han puesto en contacto con los afectados para ayudarles a proteger nuevamente sus cuentas -la mayoría se encuentran ubicados en Reino Unido, Alemania y Holanda-. Gran parte del origen del ataque parece estar en el robo de cuenta de un empleado de la propia compañía, lo que habría dado acceso a una gran cantidad de emails de usuarios -se desconoce el número concreto- a través de los cuales comenzó el envío indiscriminado de spam.

Adobe hack: At least 38 million accounts breached

Adobe has confirmed that a recent cyber-attack compromised many more customer accounts than first reported.

The software-maker said that it now believed usernames and encrypted passwords had been stolen from about 38 million of its active users.

It added that the attackers had also accessed details from an unspecified number of accounts that had been unused for two or more years.

The firm had originally said 2.9 million accounts had been affected.

Adobe has also announced that the hackers stole parts of the source code to Photoshop, its popular picture-editing program.

Adobe said source code fo
had been stolen

Adobe 2013

38 Millones de usuarios afectados, tarjetas de crédito y código fuente

Edward Snowden NSA 2013

200 Mil documentos afectados

CIBERESPIONAJE

Snowden denunció un nuevo programa de bloqueo y ataques cibernéticos

El ex técnico de inteligencia denunció que la NSA está desarrollando "MonsterMind", un sistema que podría neutralizar posibles ataques cibernéticos contra Estados Unidos y, a su vez, lanzar represalias a otros países.

Recomendar 33 Tweet 41 +1 0 ACCESIBLE

¿Quiénes toman ventaja de esta situación?

Cyber-Criminales

Motivos: Redito Económico, Espionaje Industrial

Nivel de conocimiento: Experto

Cyber-terroristas

Motivos: Ideología diferente

Nivel de conocimiento: Medio pero en volumen

Estado

Motivos: Espionaje

Nivel de conocimiento: Experto

Insiders

Motivos: En desacuerdo con la compañía

Nivel de conocimiento: Básico

¿Cómo evaden mi seguridad tradicional?

Un poco de sentido común…

- Saben que dispone de pocos recursos
- Saben que utiliza tecnología tradicional
- Saben que esta desbordado de tareas
- Saben que siempre hay un eslabón débil

Preparando un ataque

1

Reconocimiento:

- Obtener la foto global del ambiente, red, estaciones de trabajo, móviles, y virtualización, incluyendo tecnologías implementadas para asegurar el mismo

2

Programación:

- Crear malware dirigido y contextualizado, codificándolo para que no sea detectado por los mecanismos habituales.

3

Testeo:

- Asegurar que el malware funciona como se espera, específicamente si evade mecanismos de seguridad tradicionales

4

Ejecución:

- Iniciar el ataque de acuerdo a lo planeado

Ejecutando el ataque

1

Punto de entrada:

- Buscar a través de la explotación de vulnerabilidades de día cero evadir los mecanismos de control a través de correo electrónico, mensajería instantánea, redes sociales

2

Control remoto:

- Una vez ejecutado la rutina del malware asegurar la comunicación continua entre el host comprometido y el servidor C2

3

Movimiento Lateral:

- Localizar los host que alojan la información sensible de la red objetivo

4

Descubrimiento de activos:

- Identificación de los datos valiosos para aislarlos preparándolos para su futura sustracción

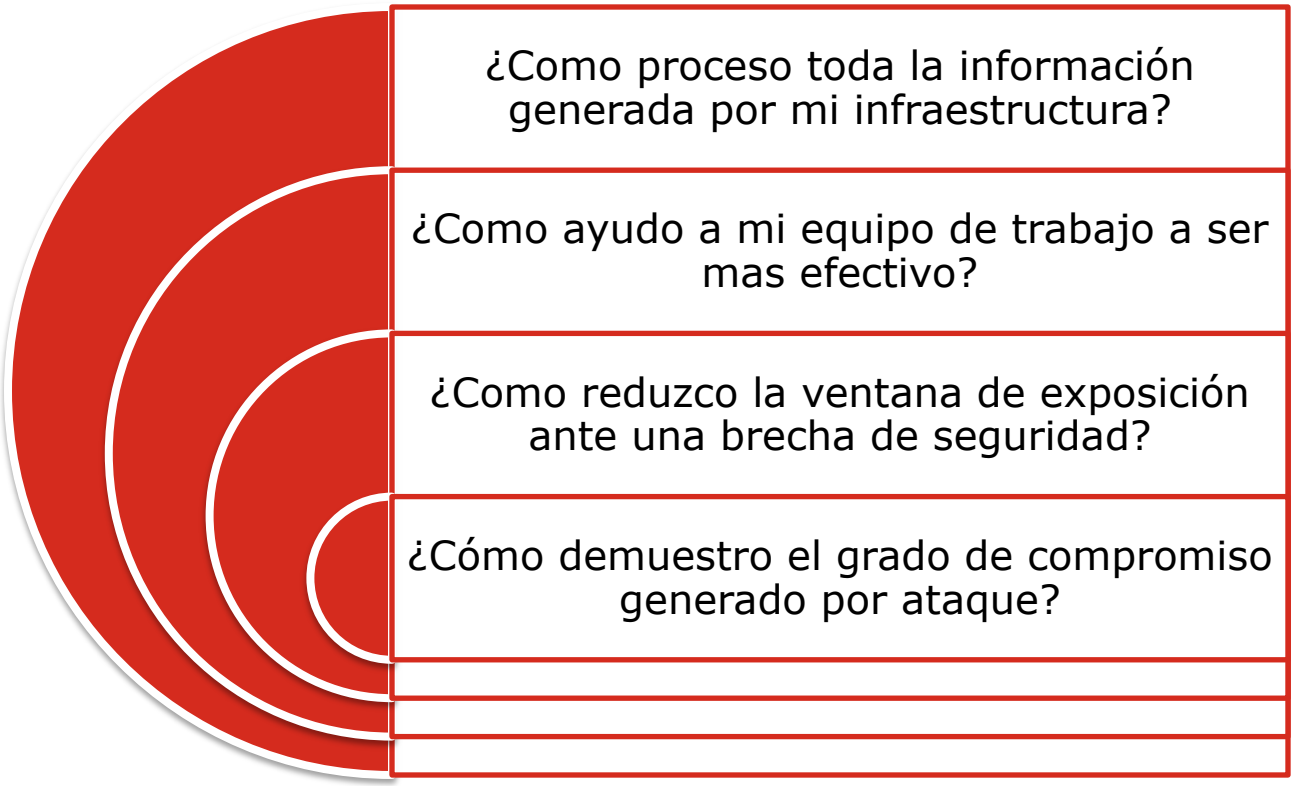
5

Extracción de datos:

- Transmitir la información fuera de la organización afectada

¿Qué desafíos surgen a partir de esta problemática?

Desafíos de seguridad en Big Data



¿Cómo minimizar el impacto?

Un Nuevo Enfoque de Seguridad es necesario

CONTROLADO POR TI
BASADO EN PERIMETRO

PREVENCION
BASADO EN FIRMAS

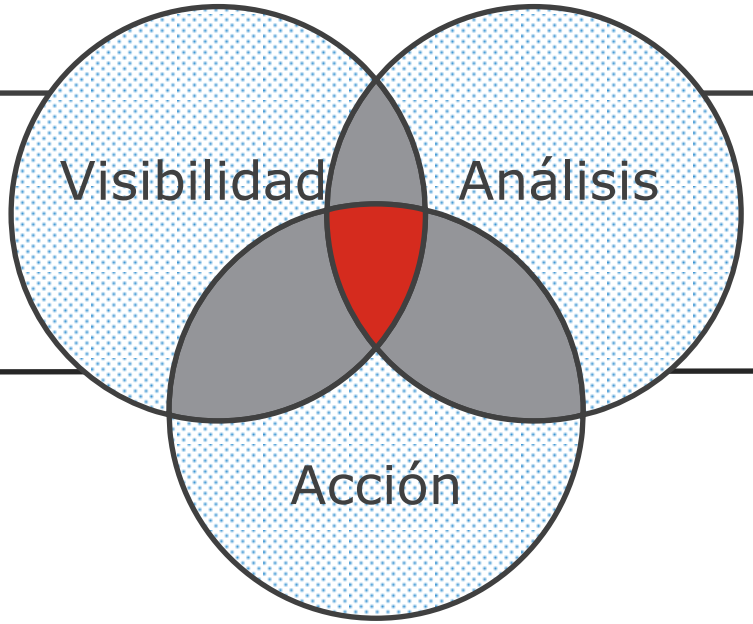
CENTRALIZADO EN EL USUARIO
SIN PERIMETRO

DETECCION
IMPULSADA POR
INTELIGENCIA

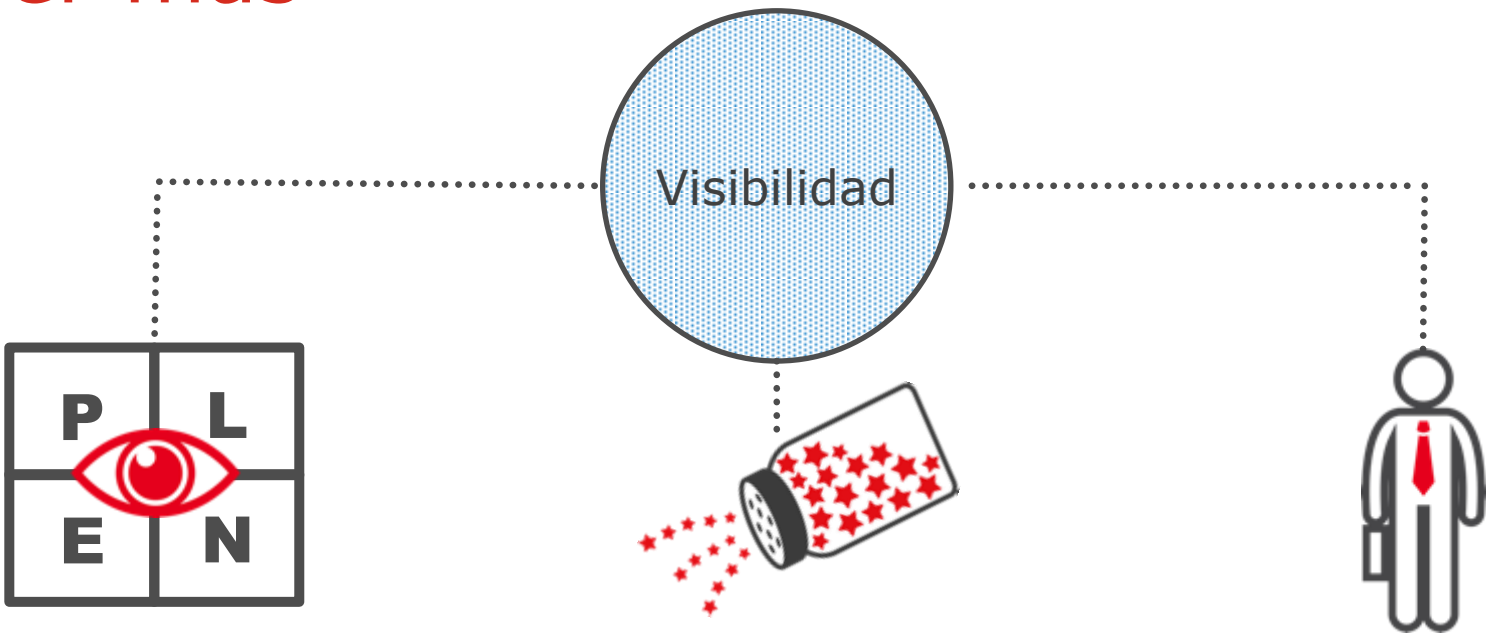
Solo un ataque…

TRANSFORMA

Seguridad impulsada por Inteligencia



Ver más

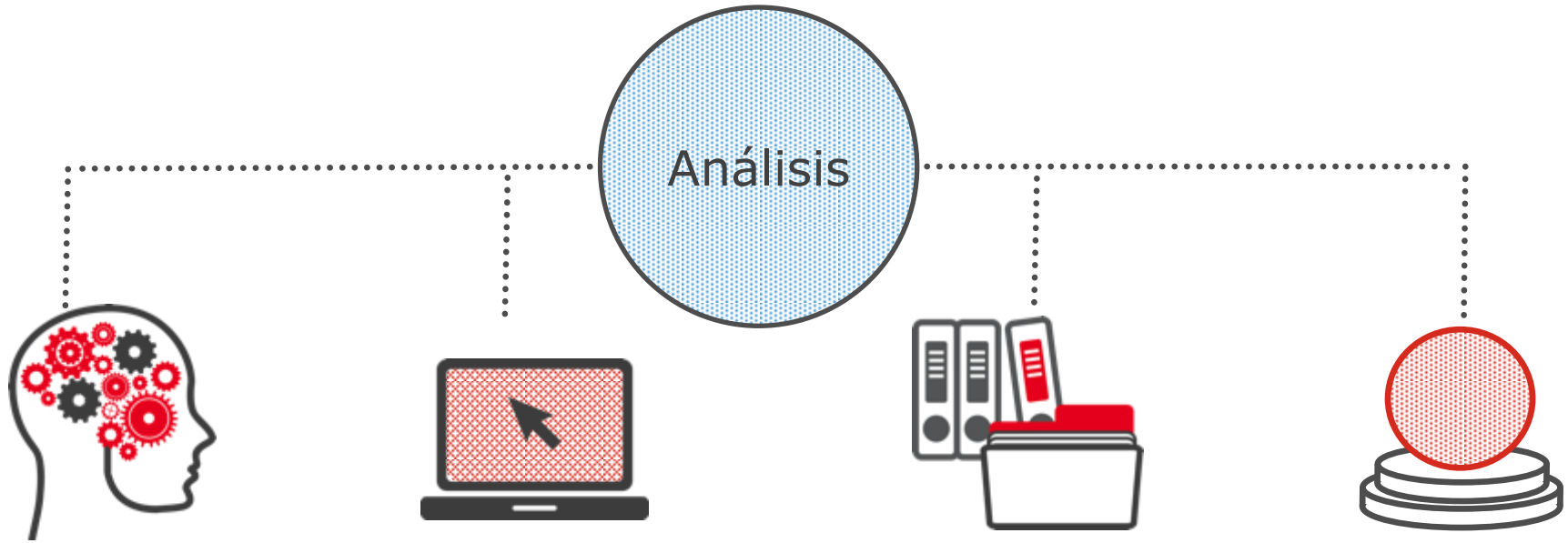


Paquetes, Logs, Estación de trabajo, Flujos de red

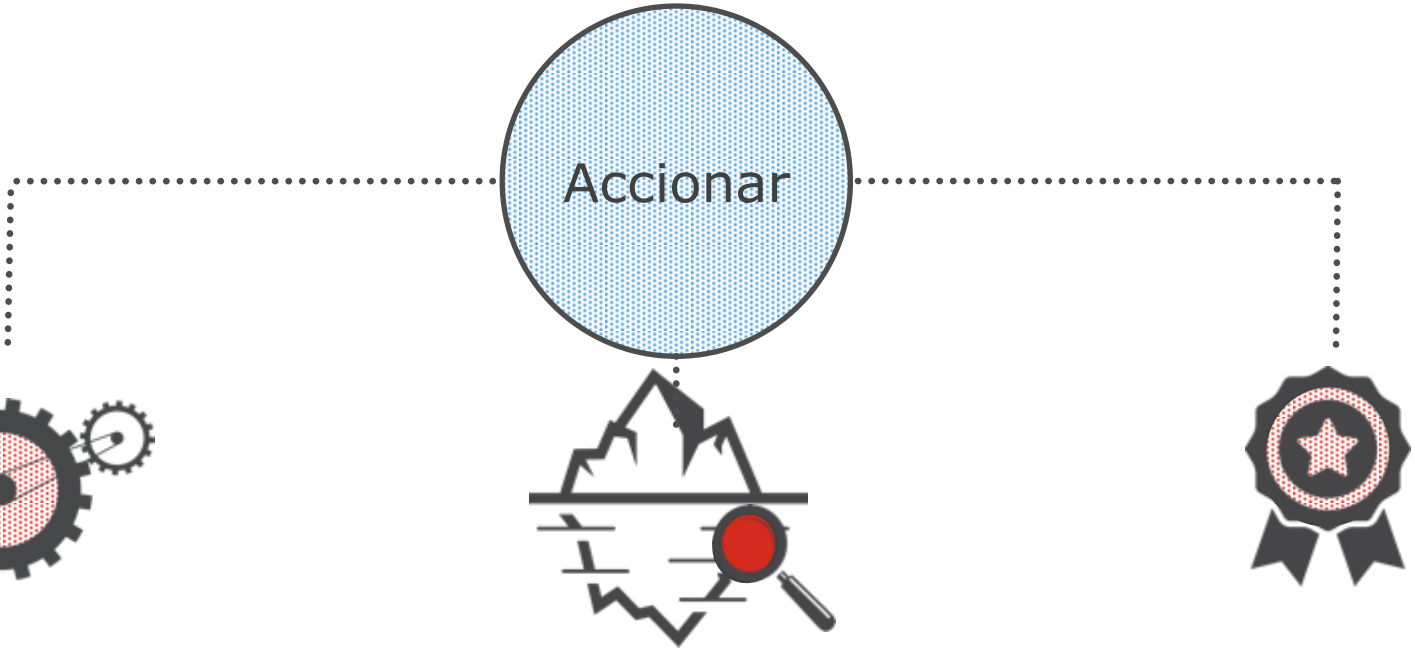
Enriquecimiento en el momento de la captura

Contexto del negocio y Cumplimiento normativo

Entender todo



Investigar y Remediar más rápido



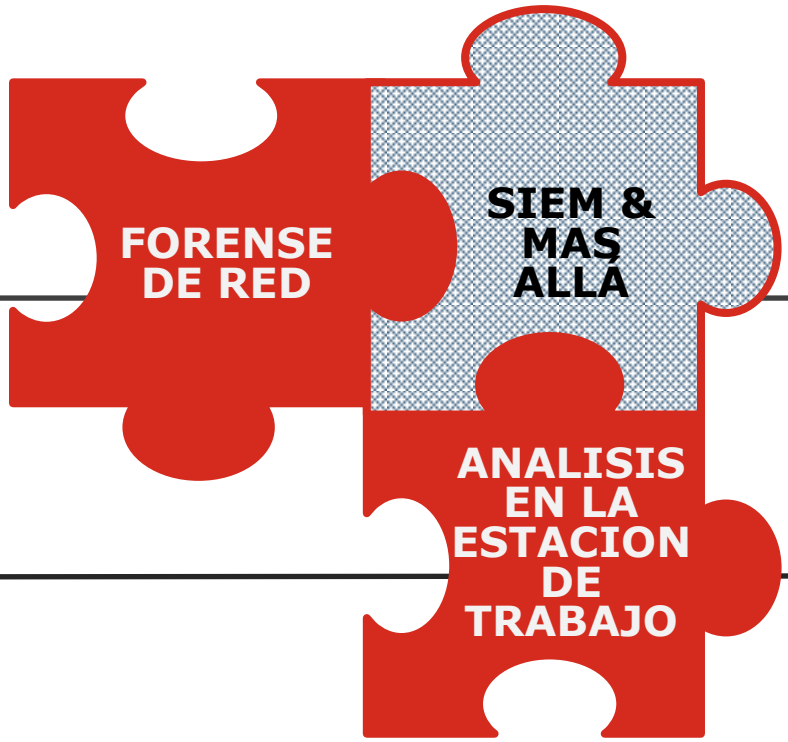
Flujo de trabajo
del analista
Priorizado y unificado

Investigar en
profundidad
al más mínimo detalle

Integración de
mejores Practicas
de SOC

Modular

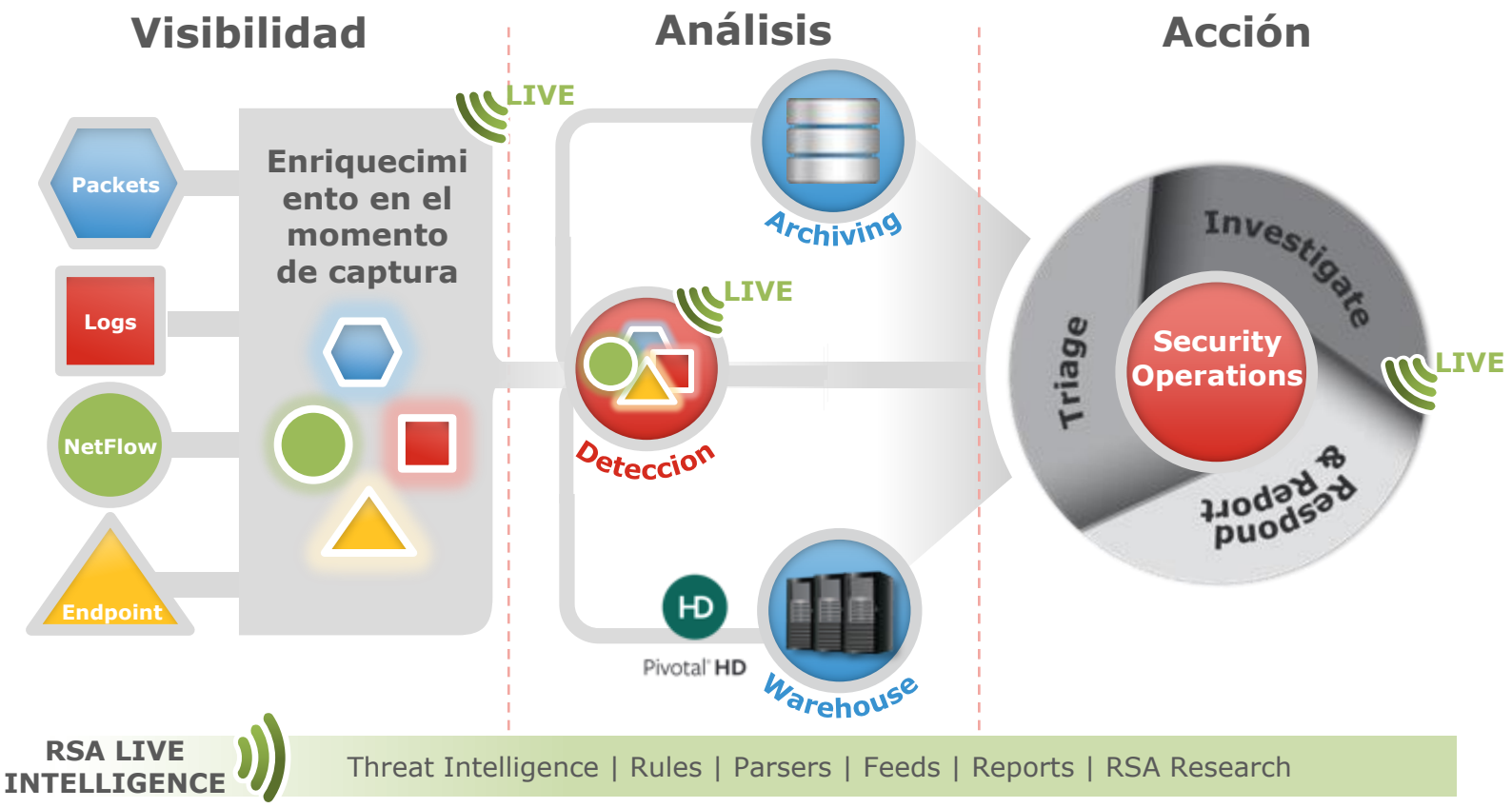
RSA Advanced SOC Solution



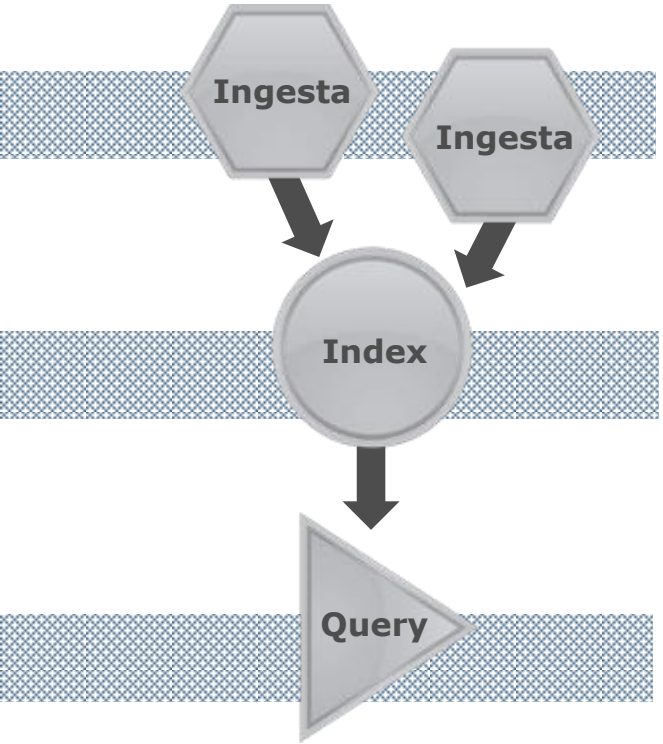
A medida que su departamento de seguridad crece, la solución crece con usted

¿Qué es una plataforma de Security Analytics?

Security Analytics Architecture

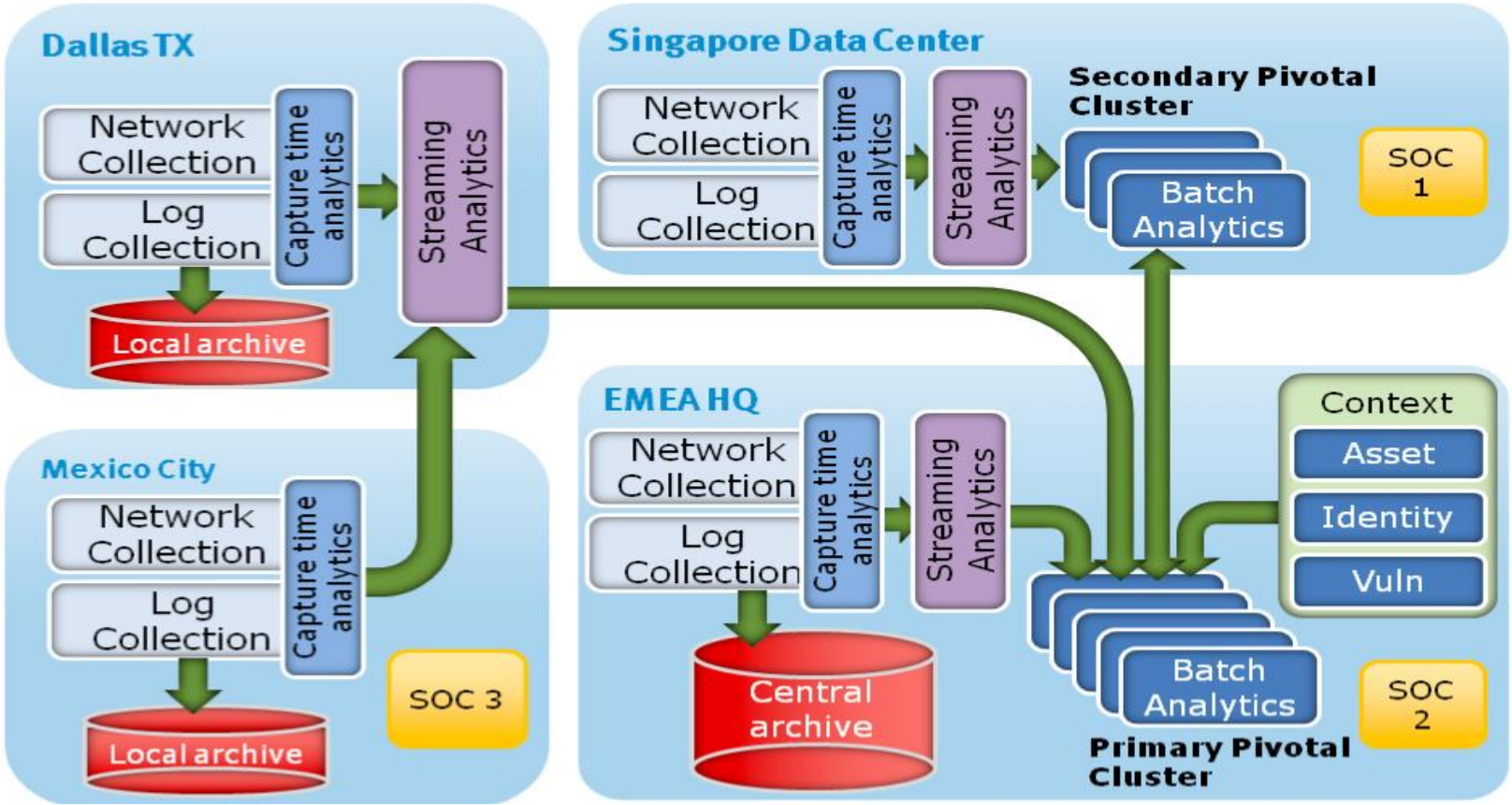


Arquitectura distribuida escalable

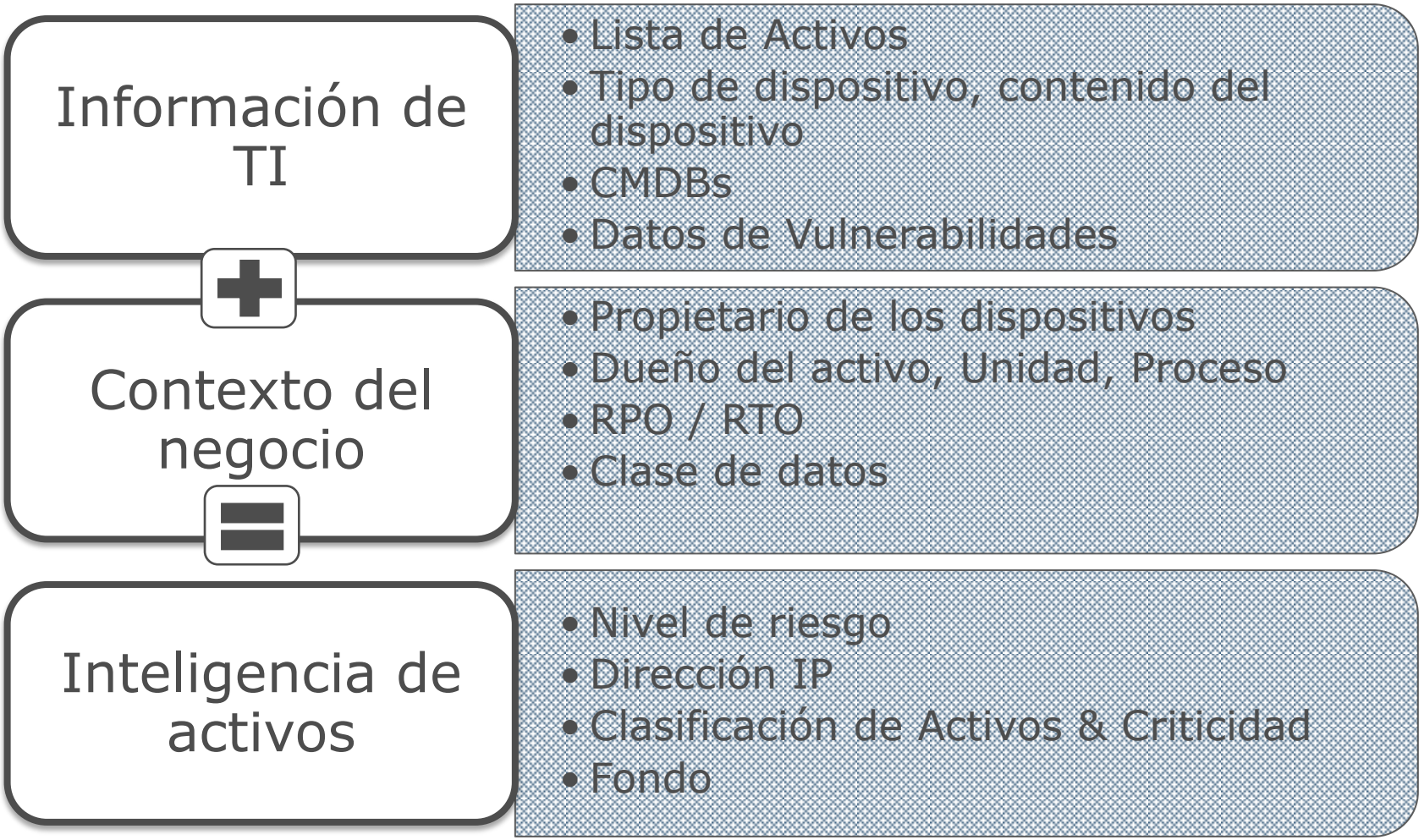


- Recopilar y analizar grandes cantidades de datos
- Infraestructura federada permite a las empresas escalar linealmente
- Capacidad para analizar y consultar sin problemas en todo el sistema

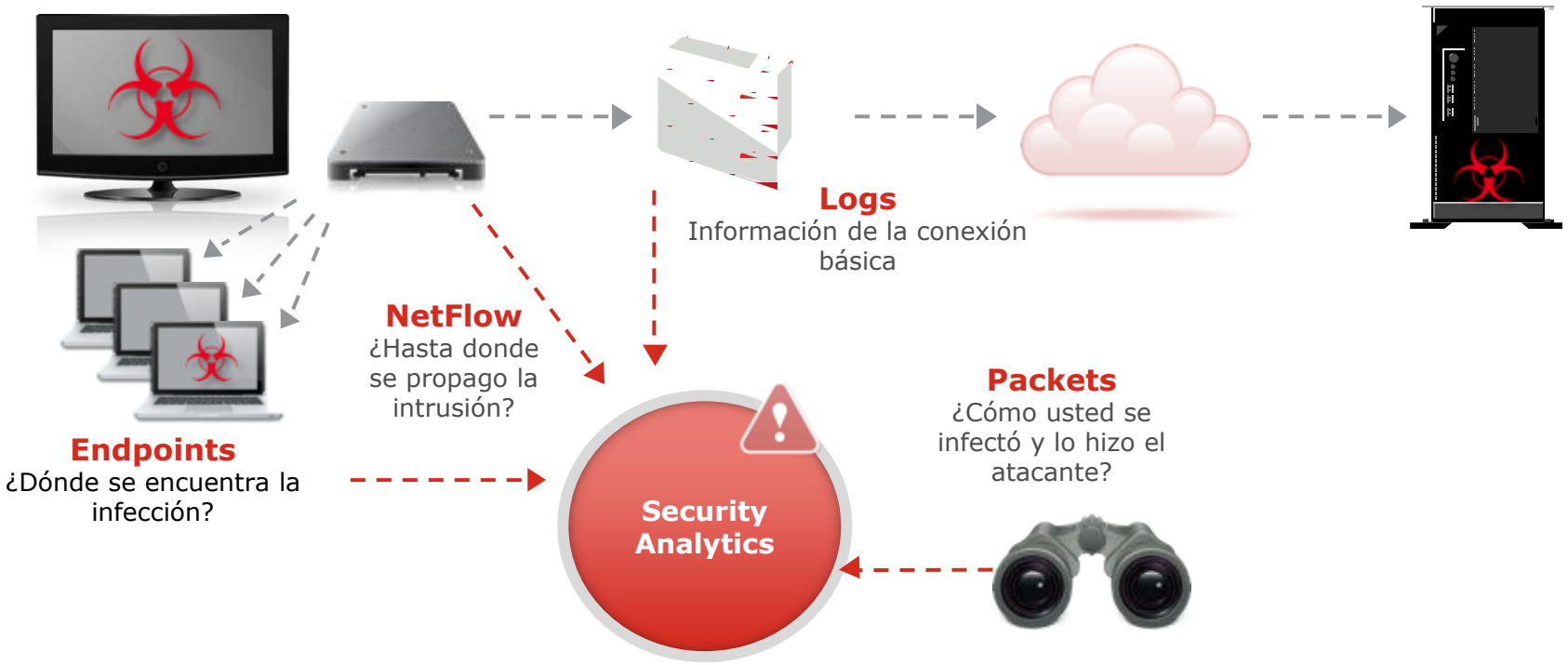
Ejemplo de arquitectura de referencia



Añadir Cumplimiento & Contexto de negocio

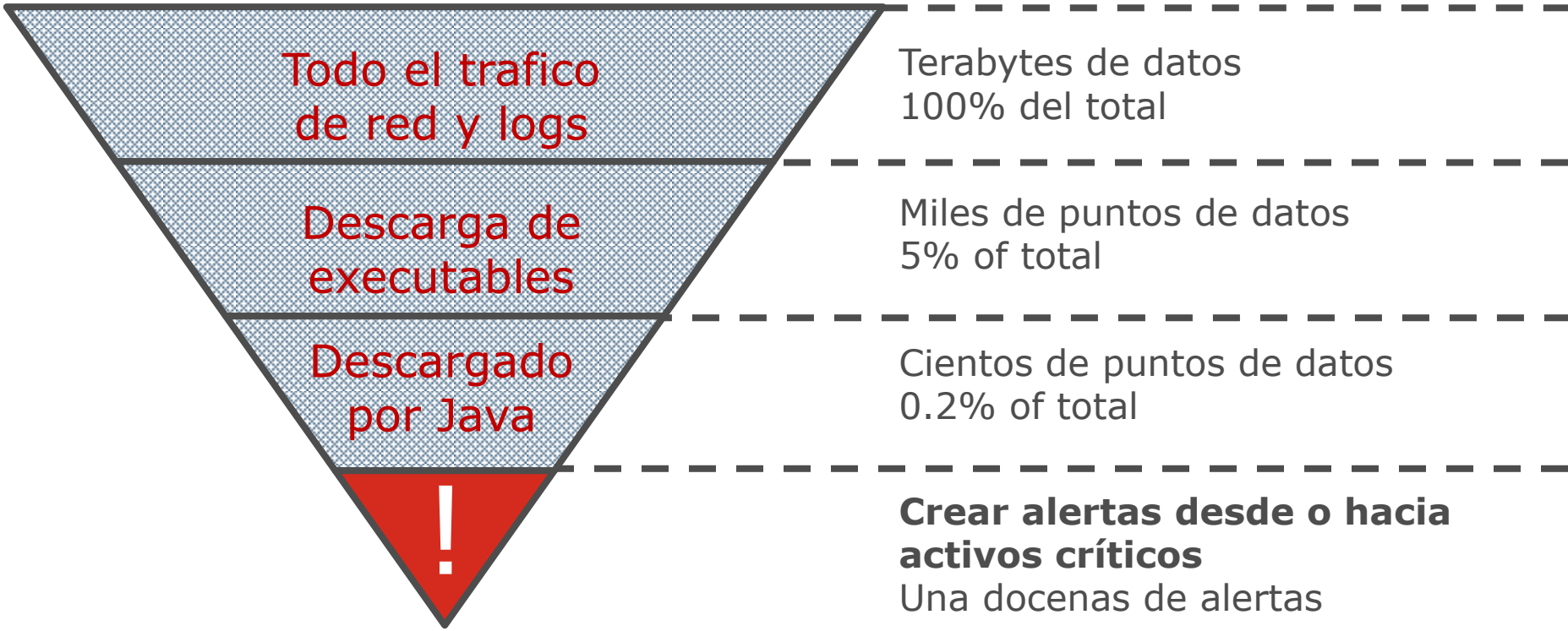


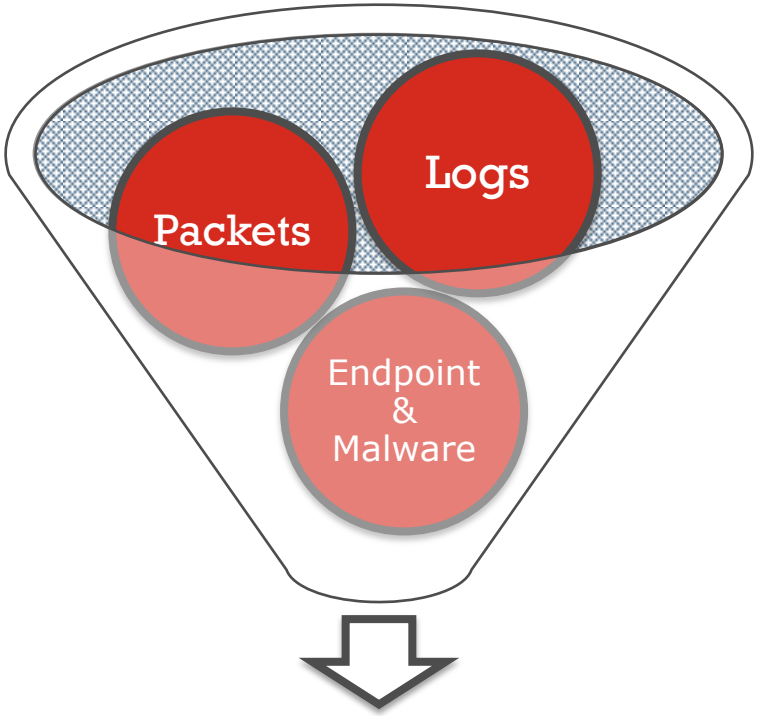
The Power Of A Risk-Based Approach



Investigación con profundidad en segundos

Removiendo la paja y buscando la aguja





Punto de partida del analista

Gestión de Incidentes Nativa

Incidentes y flujos unificados


RSA


EMC²