IBM Security Systems

Herramientas de securización de Centros de Proceso de Datos de alta criticidad.

AGENDA

- La nueva división de seguridad
- Principios de la seguridad inteligente
- Como proteger nuestros centros de procesos de datos

El mundo cada vez está más digitalizado e interconectado, abriendo la puerta a nuevas amenazas y filtraciones emergentes…

EXPLOSIÓN DE DATOS

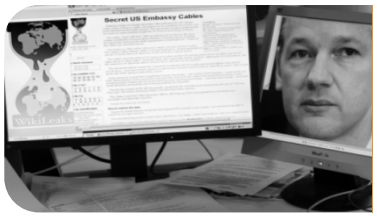
La edad de Big Data – la explosión de la información digital – ha llegado y se amplia por la extensión de aplicaciones accesibles desde cualquier lugar.

UTILIZACIÓN DE LOS RECURSOS IT

La linea entre los horarios personales y profesionales ha desaparecido.

TODO ESTÁ EN TODAS PARTES

Las organizaciones continuan migrando a nuevas plataformas, incluyendo los servicos en la nube, virtualización de sistemas y aumento del uso de dispositivos moviles.

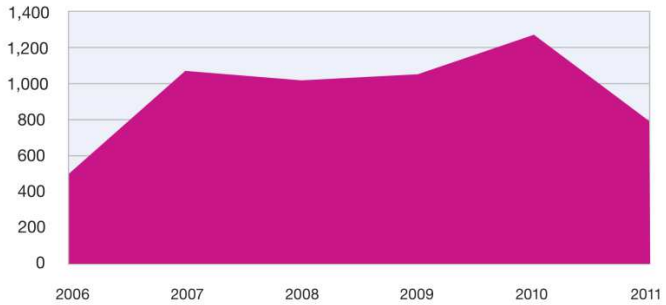


SOFISTIFICACIÓN DE LOS ATAQUES

La velocidad y sofisticación de los ataques ha aumentado. Aparecen nuevos actores, con nuevas motivaciones, que van desde el ciber crimen a las intrusiones de estado

Datos principales del estudio IBM X-Force® 2011

Vulnerabilidades públicas 2006-2011

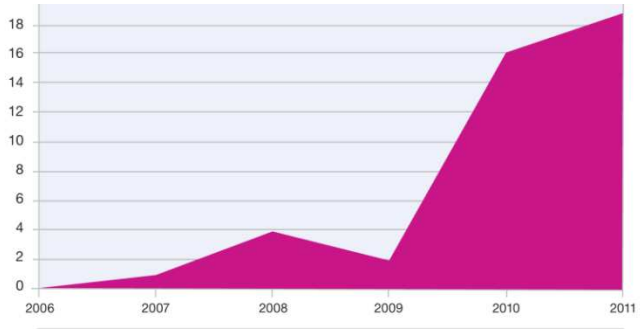


Avances en la seguridad de Internet

- Menos programas maliciosos
- Menos vulnerabilidades de aplicaciones web
- Mejora de los parches

Pero…

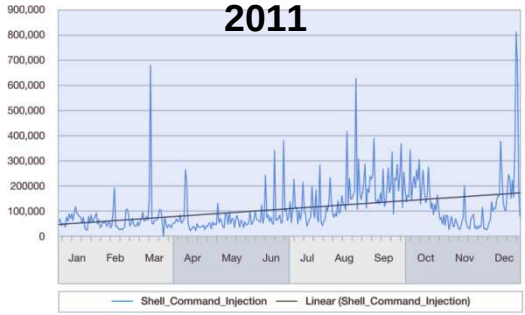
Vulnerabilidades en sistemas operativos móviles 2006-2011



Movilidad y la *nube* representan nuevos desafíos

- Crece el número de vulnerabilidades móviles
- Las arquitecturas cloud desafían los desarrollos de seguridad
- Redes sociales más vulnerables por la proliferación de medios sociales

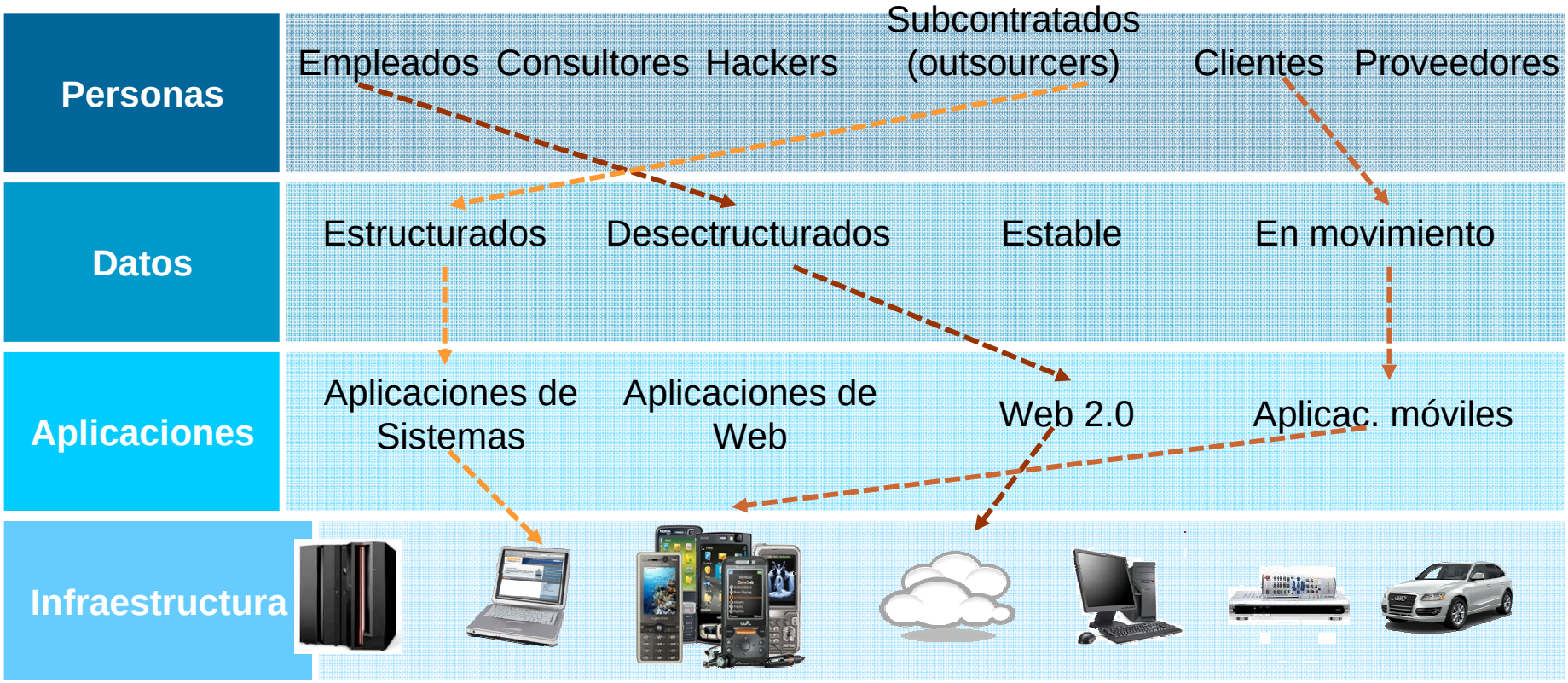
Top MSS High Volume Signatures & Trend Line Shell Command Injection 2011



Creciente sofisticación de los ataques

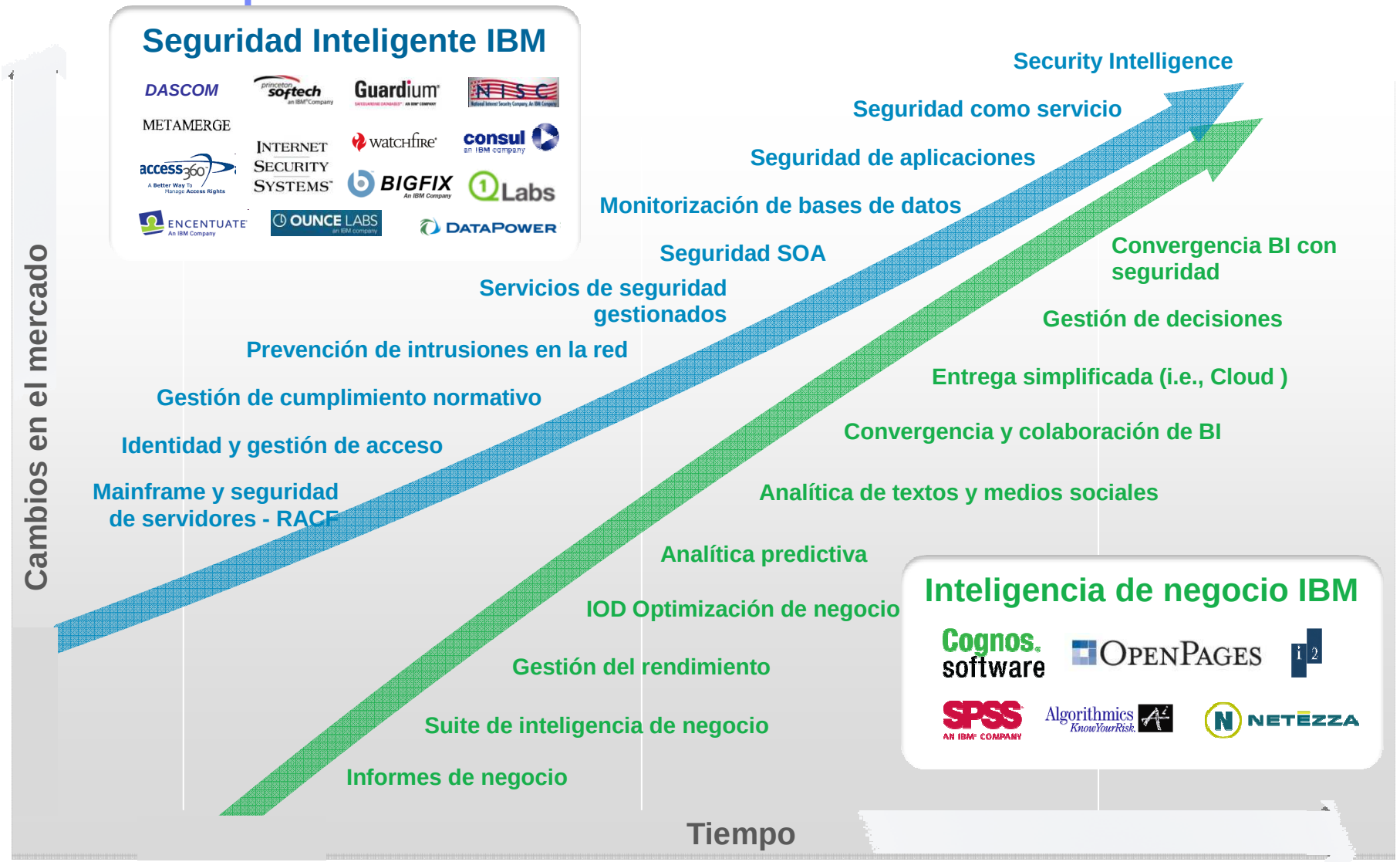
- Ataques Shell Command Injection
- Aumento de ataques contra contraseñas
- Incremento de la distribución de malware basado en phishing y fraude por “clic”

Resolver los temas de seguridad es un puzzle complejo y cuatridimensional



Ya no es suficiente la seguridad perímetral. Las soluciones aisladas y localizadas en un solo punto para proteger la empresa de las amenazas de seguridad es insuficiente

Para IBM, seguridad e inteligencia de negocio ofrecen una visibilidad paralela

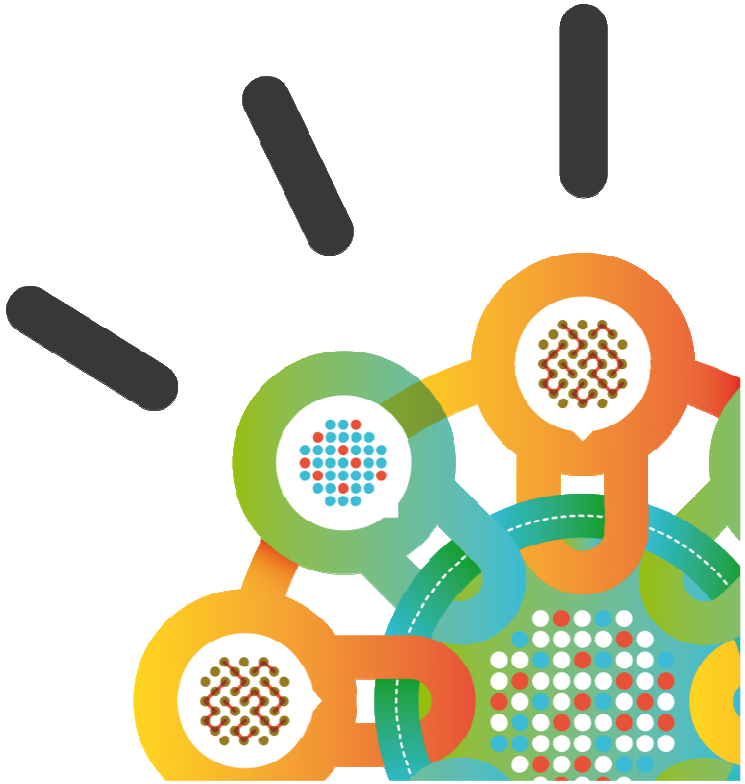


“Secure by Design”

Seguridad desde el Diseño, *ha sido el punto de partida de la nueva División de Seguridad de IBM (“Security Systems”).*

I*BM considera que la manera de ayudar a nuestros clientes a estar por delante de las amenazas de seguridad, consiste en unir nuestras capacidades analíticas y de inteligencia de nuestras diferentes áreas de I+D en una única organización, que sea capaz de mejorar la predicción y detección de amenazas y riesgos para la seguridad*

*La consolidación de las diferentes compañías de seguridad nos permiten trabajar en una línea estratégica “****Security Intelligence****”*



Definición de Seguridad Inteligente

Security Intelligence (SI) *es la obtención en tiempo real, normalización y análisis de los datos generados por los usuarios, las aplicaciones y la Infraestructura que impacta en la seguridad de los sistemas de información y en la estrategia de la compañía.*

Objetivo*: Proporcionar el conocimiento y su comprensión, de manera que puedan reducir riesgos y optimizar el esfuerzo operacional para cualquier tipo de organización, independientemente de su tamaño.*

Resultado*: Security Intelligence proporciona información analítica para contestar a las preguntas fundamentales que cubren el antes, durante y después del momento en el que se producen riesgos y amenazas.*

Security Intelligence *proporciona una visión unificada de la seguridad y la postura de riesgo de una organización, atravesando los cuatro dominios de riesgo primarios:*

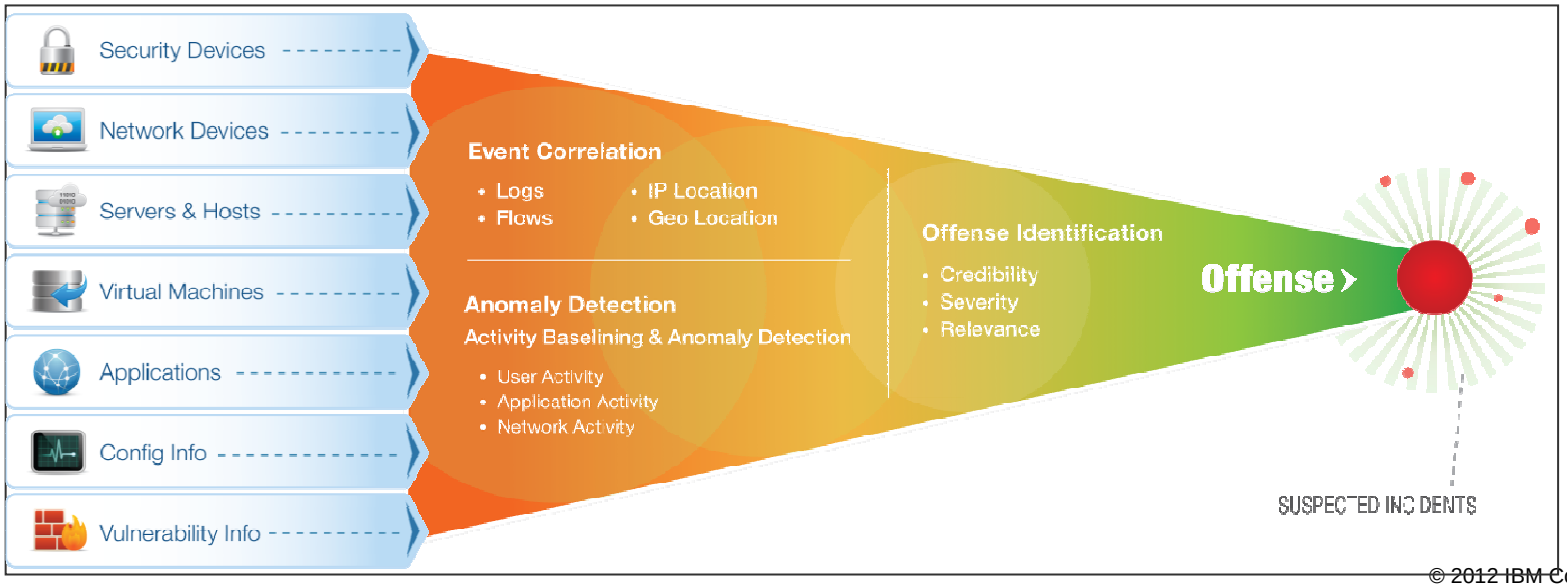
Personas, Datos, Aplicaciones, e Infraestructura

Principios de Seguridad Inteligente

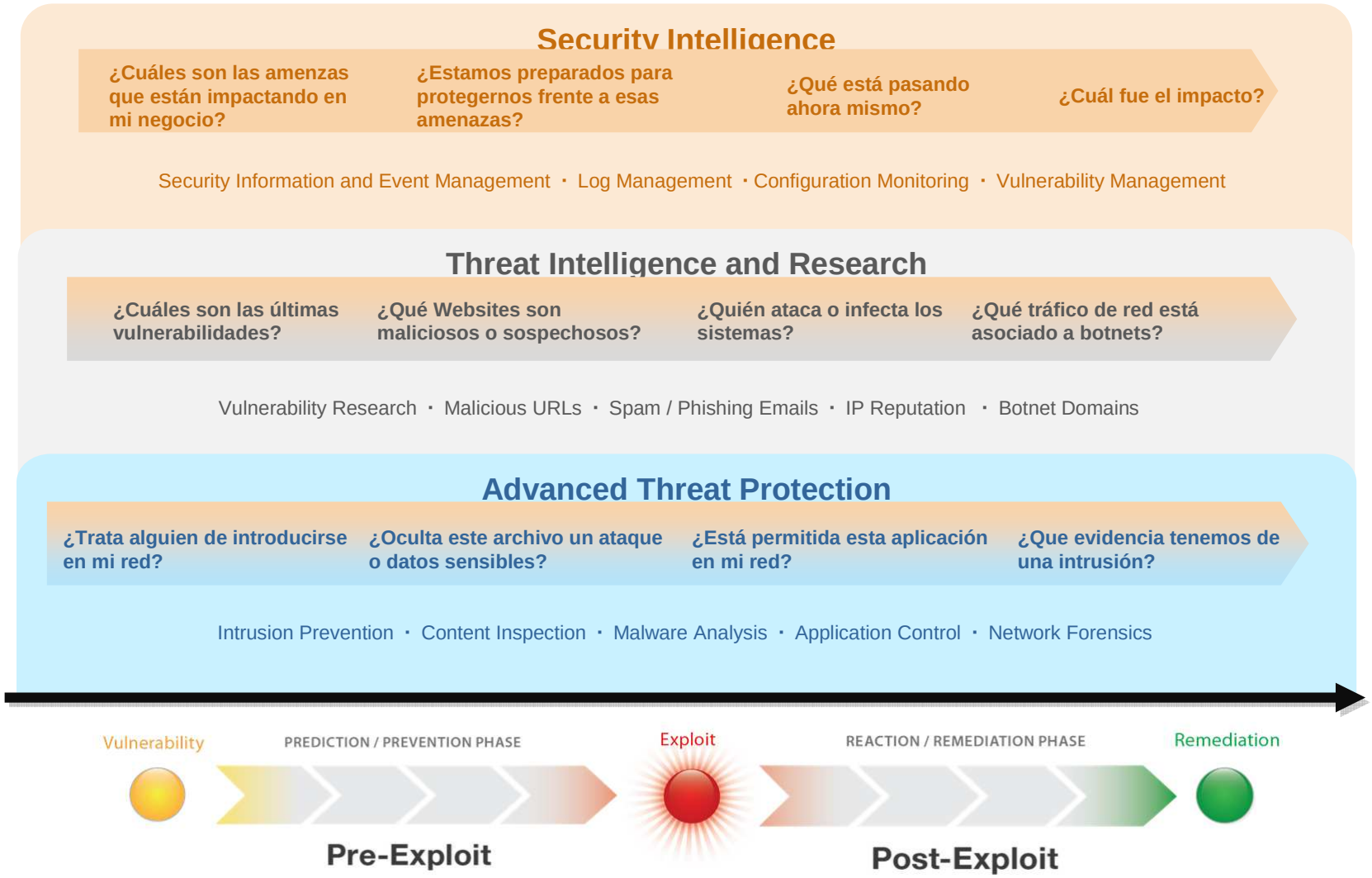
*1. **Integración**: Este proceso permite análisis constante de la información, normalizando así datos dispares.*

*2. **Inteligencia**: La capacidad de dar sentido a la gran cantidad de información relevante tanto en seguridad como cumplimiento normativo. Esto significa almacenar, correlacionar, reportar y buscar en una amplia variedad de información a gran escala. Esta capacidad ofrece comprensión y facilita la toma de decisiones.*

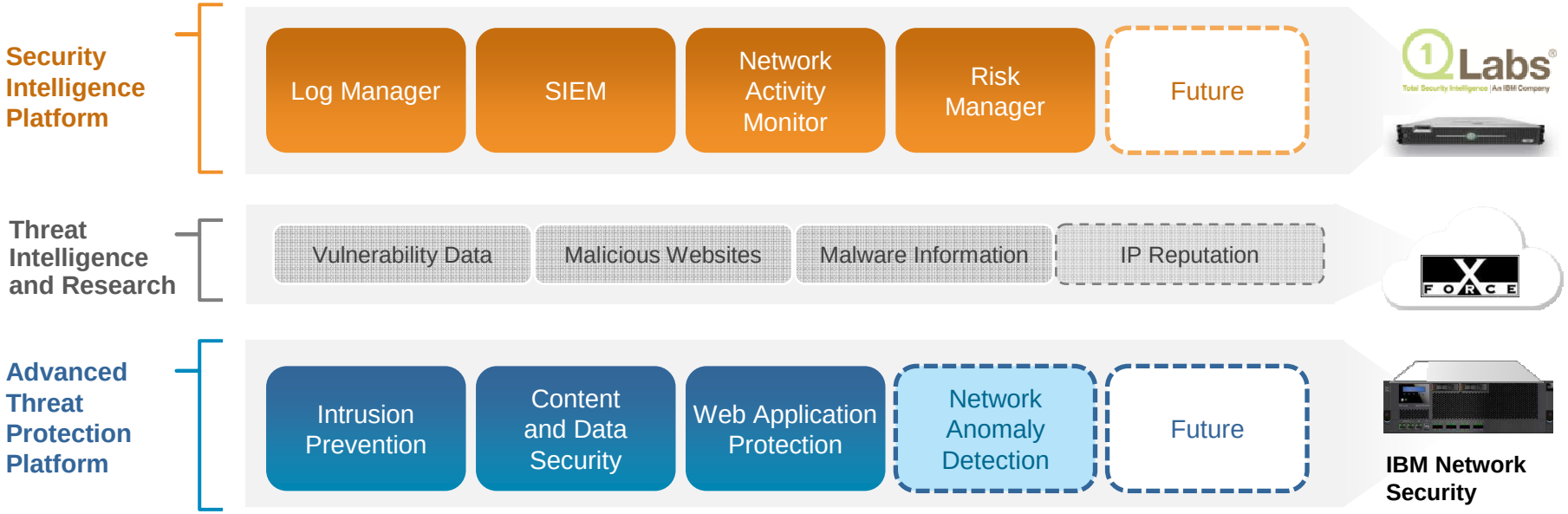
*3. **Automatización**: La automatización es el elemento que posibilita el concepto de Security Intelligence hoy en día, puesto elimina la complejidad innecesaria y reduce el coste total de propiedad (TCO).*



Requerimientos para una Plataforma de Seguridad Avanzada



Visión de IBM para proteger la infraestructura frente a amenazas



Advanced Threat Protection Platform

La capacidad de prevenir amenazas sofisticadas y descubrir el comportamiento anómalo de la red. Todo ello gracias a la combinación de las capacidades de análisis de información en tiempo real con las herramientas de Security Intelligence.

Expanded X-Force Threat Intelligence

Cobertura incrementada de las capacidades del grupo X-Force para analizar datos y tomar decisiones más ágilmente en el portfolio de soluciones de seguridad de IBM

Security Intelligence Integration

La integración entre Advanced Threat Protection Platform y QRadar Security Intelligence proporciona un modo único y significativo para detectar, investigar y remediar amenazas.

Capacidades de IBM Security en detección de intrusiones

Aspectos destacados

- Proporciona seguridad manteniendo el rendimiento de las aplicaciones de negocio
- Proporciona protección ante amenazas y vulnerabilidades antes de su publicación gracias la tecnología “Virtual Patch” ofrecida por X-Force
- Reduce el coste y la complejidad de securizar las infraestructuras

Capacidades

Mas allá que un IPS tradicional proporciona Security Intelligence incluyendo:

•Web application protection (WAF)
•Protección a la Web 2.0
•Data Loss Prevention (DLP)
•Motor SNORT. Además de la potencia del motor PAM permite trabajar con el motor SNORT de forma simultánea.
•Application Control
•Protección a sistemas de control (SCADA)

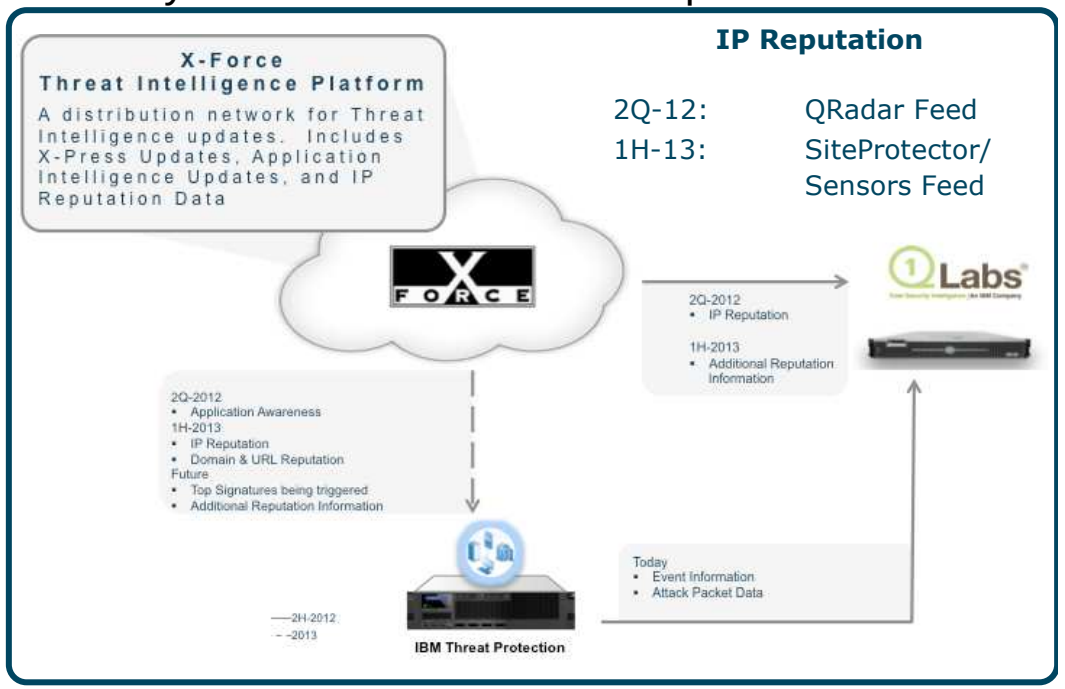
Rendimiento. Un único dispositivo es capaz de analizar tráfico de red a 23Gb por segundo en modalidad IPS con conectividad 10G.

Protección efectiva proporcionada por el equipo de i+D de X-Force, que posibilita estar “ahead of the threat”

Reduce y coste y la complejidad puesto que consolida en un mismo dispositivo varias soluciones de seguridad y se integra con el resto de herramientas de seguridad de la compañía.

X-Force IP Reputation Feed for QRadar

- X-Force proporciona desde 2012 dos contenidos recurrentes:
  - Security Content X-Press Updates (XPUs;)
  - URL & IP Reputation Data & Application Awareness.
- IBM X-Force proporciona a través de QRadar, IP Reputation, lo cual facilita disponer de información de entidades sospechosas en Internet , proporcionando una correlación fácil e inteligente.
- Supervisión continua de la Internet para evaluar direcciones IP nuevas y existentes y Dominios para continuamente madurar calidad y exactitud de la lista de Reputación IP
- Más de 14B URLs Monitorizadas y clasificadas
- IP Reputation Data contiene información sobre Malicious IPs, Malware hosts, SPAM sources e información detallada para cada uno de ellos (incluido geo information)



Capacidades Globales de IBM Security Systems

IBM pone a disposición de sus clientes las capacidades globales tanto en materia tecnológica como humana.

Las capacidades globales de IBM Security Systems producen ingentes cantidades de información en materia de Seguridad:

X-Force Investigación

14B páginas Web analizadas

40M spam & phishing

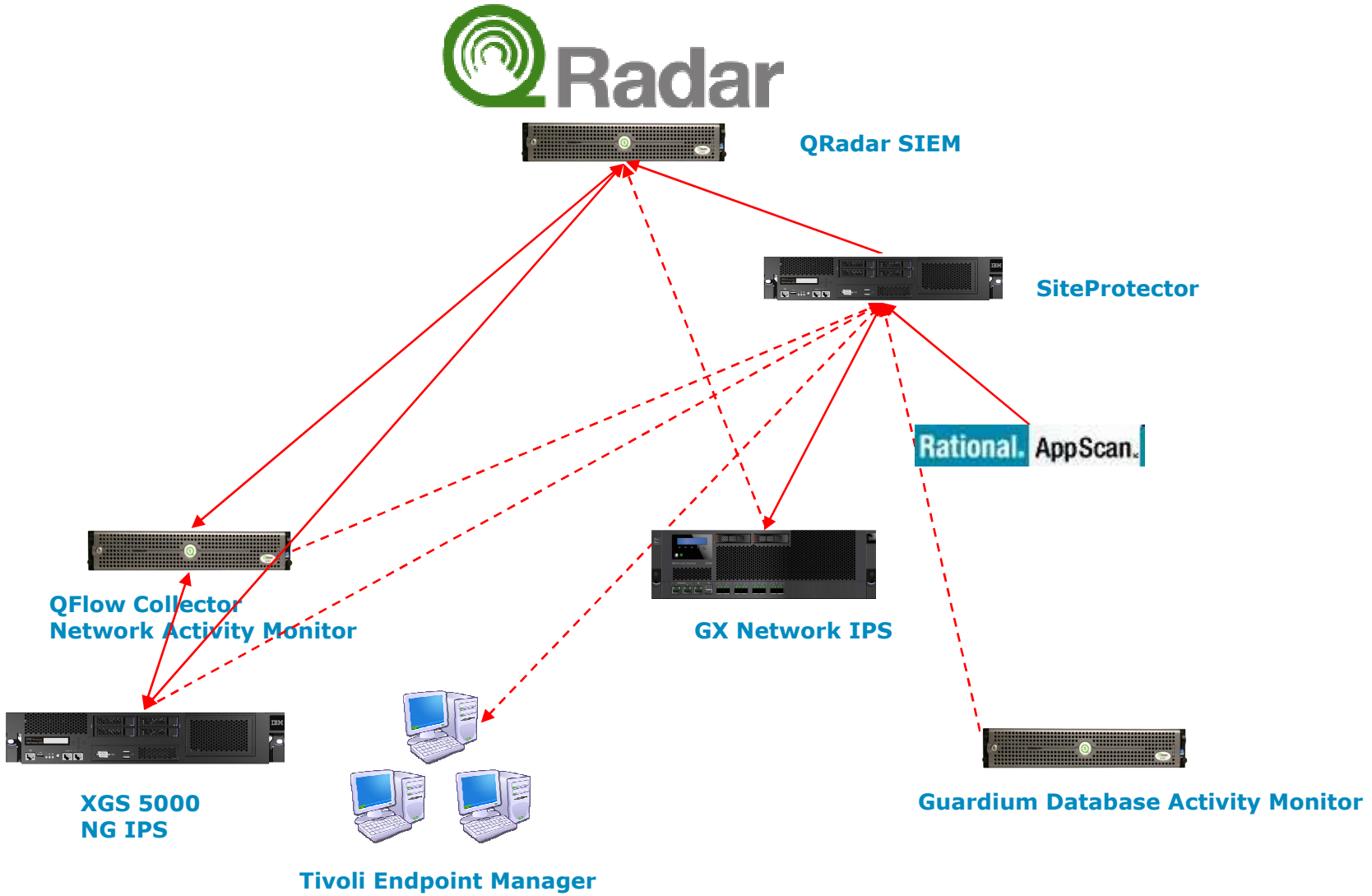
54K vulnerabilidades documentadas

13B eventos de seguridad diarios

Proporciona análisis específico de:

- Vulnerabilidades & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Otras amenazas emergentes

Network Security Product Interconnectivity



Thank You- Q&A