Seguridad e Integridad en el ámbito digital

Diego Oviedo

Associate Partner – IBM Security Services

MBA, CISA, CRISC, ISO27001 LA

Agenda

- Contexto actual de la seguridad
- Enfoque proactivo
- Recomendaciones

O > D

"En el ciber espacio, la ofensa lleva la ventaja."
Deputy Secretary of US Defense, William Lynn, 2010

¿Estamos siendo exagerados?

- Stuxnet
- Target
- World's Biggest Data Breaches
- Ataques en vivo! (¿en serio?)
- WannaCry
- GoT

WannaCry

EL MUNDO
TECNOLOGÍA

Hackean la red interna de Telefónica y de otras grandes empresas españolas

theguardian

Massive ransomware cyber-attack hits nearly 100 countries around the world

BBC NEWS
Technology

More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA

The ransomware causing chaos globally

emol. Tecnología
Santiago: Sábado 13 de mayo del 2017 | Actualizado 01:00

Hackeo mundial a empresas: Confirman 150 detecciones de virus en Chile y Gobierno monitorea efectos

Hasta ahora se registran más de 57 mil detecciones del virus en 74 países, aunque la cifra crece constantemente.

12 de Mayo de 2017 | 14:10 | Por Javier Neira R., Emol

Qué sucedió

Anuncio de hacking a la NSA con robo de ciberarmas. Ofrecimiento a 1.000.000 de bitcoins

Se publica la vulnerabilidad CVE-2017-0143. Vulnerabilidad sobre SMBv1, descubierta por la NSA, no publicada.

Edward Snowden anuncia que Shadow Brokers ha liberado las ciberarmas de la NSA.

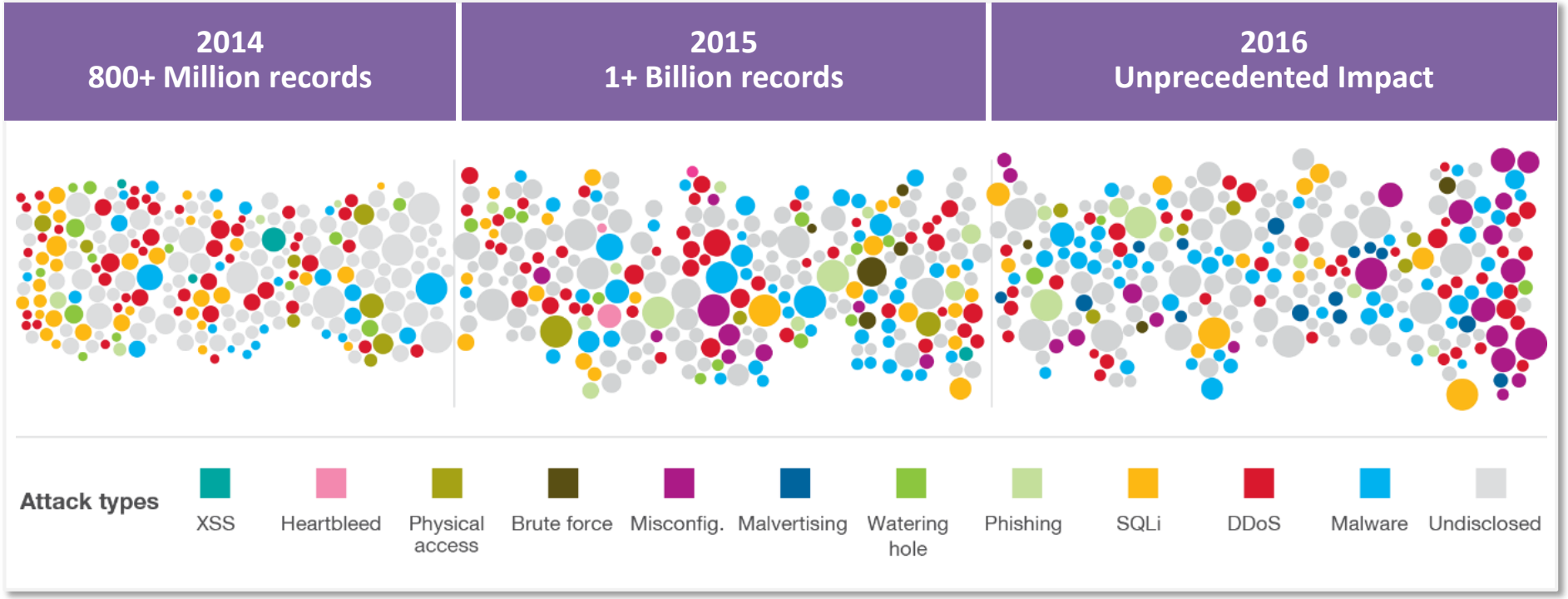
15-ago-16 | 7-ene-17 | 13-mar-17 | 14-mar-17 | 8-abr-17 | 14-abr-17 | 12-may-17

Ofrecimiento por twitter del framework **Fuzzbunch.** Incluye los exploits Eternalblue y Doublepulsar

Se publica el parche MS17-010 que resuelve la vulnerabilidad expuesta.

Se libera Fuzzbunch al público.

Se rompen las barreras de seguridad todos los días



Tiempo promedio detección APTs

200 días

Costo promedio por registro comprometido

$158

Sources: IBM® X-Force® Threat Intelligence Report 2016, Ponemon Institute Cost of Data Breach Study 2016

Economía de la Cyber Seguridad compleja

Perspectiva: Estado Actual de la Seguridad

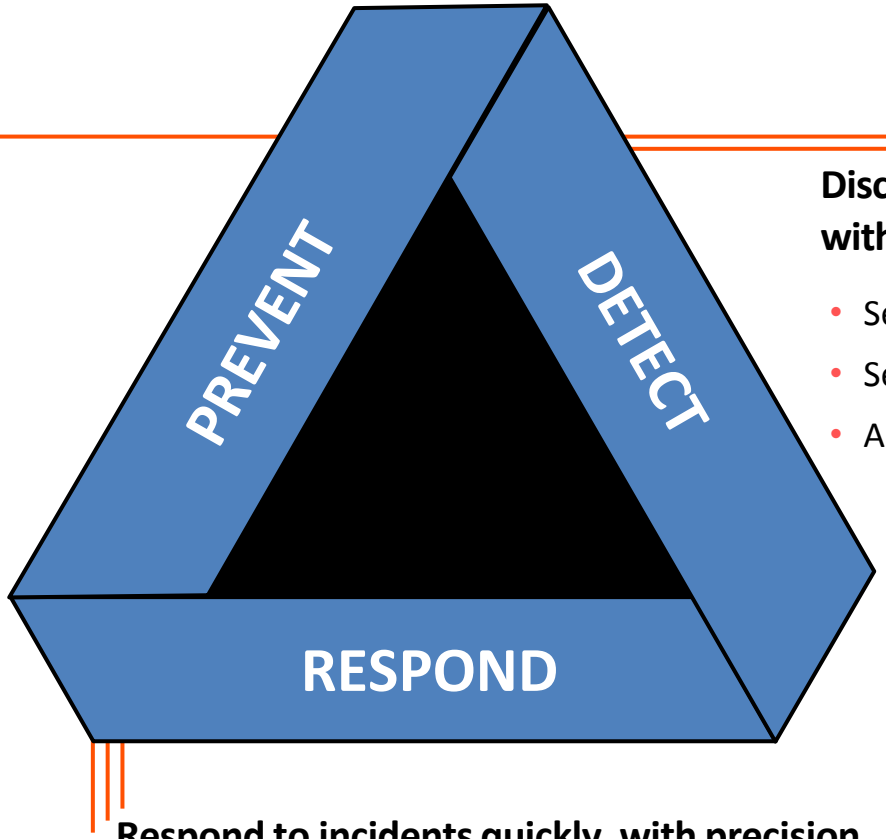
- Defenderse contra múltiples amenazas
- Constantemente mantener y monitorear las medidas defensivas
- Mayor demanda por recursos especializados incrementan los costos
- La Precisión y la capacidad de respuesta son esenciales

- Puede apuntar a múltiples organizaciones vulnerables
- Identificar y explotar un fallo en las medidas defensivas
- Las herramientas y servicios reducen las habilidades requeridas para realizar actividades maliciosas
- Opción de emplear múltiples métodos de ataque en un periodo de tiempo

Enfoque proactivo

Continuously stop attacks and remediate vulnerabilities

- Disrupt malware and exploits
- Discover and patch endpoints
- Automatically fix vulnerabilities



Discover unknown threats with advanced analytics

- See attacks across the enterprise
- Sense abnormal behaviors
- Automatically prioritize threats

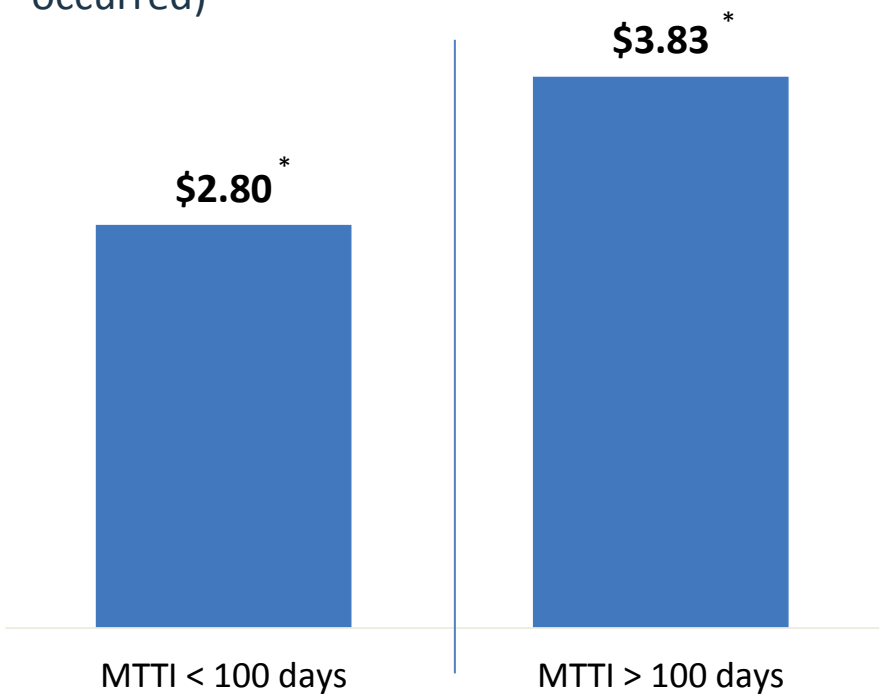
Respond to incidents quickly, with precision

- Orchestrate and automate incident response
- Hunt for indicators using deep forensics

Detección temprana reduce costos y tiempo

Mean time to identify (MTTI)

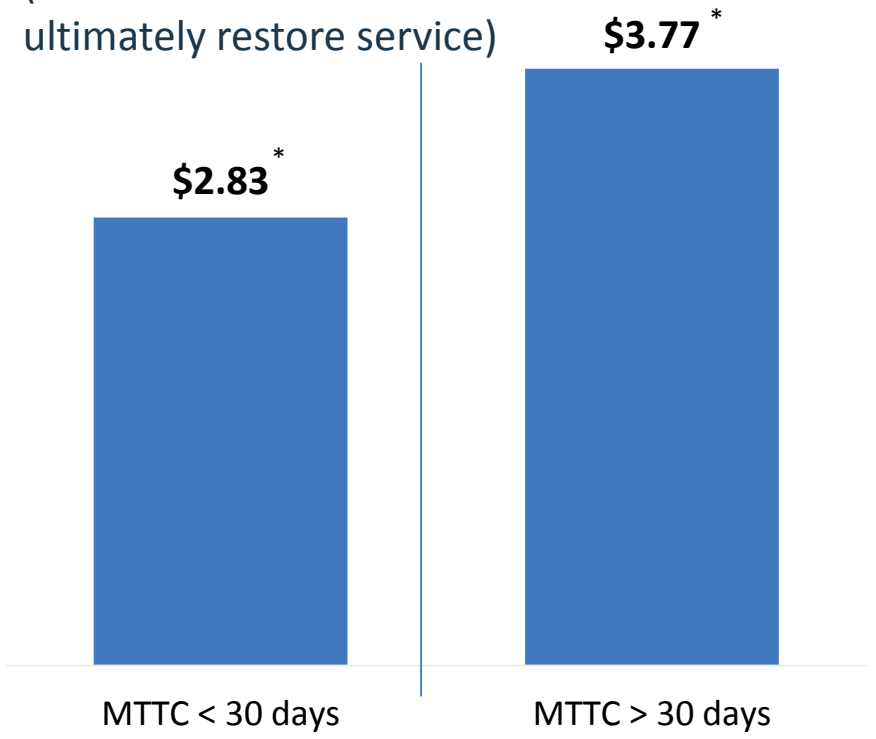
(The time it takes to detect that an incident has occurred)



Total cost, in millions

Mean time to contain (MTTC)

(The time it takes to resolve a situation and ultimately restore service)



Total cost, in millions

FY 2017

Average total breach cost includes investigation, remediation, third parties, notification and business impact - "2017 Cost of Data Breach Study," Ponemon Institute, May 2017, Currencies converted to USD (covered 1,900 individuals across 419 companies in 13 countries or regions and 17 industries)

¿Nos estamos enfocando en lo realmente importante?

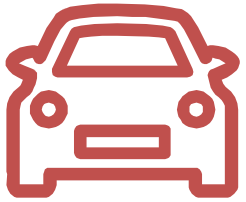
La probabilidad de que…

¿Gane la lotería (Powerball)?

1 en 292,201,338

¿Le caiga un rayo?

1 en 960,000



¿Tenga un accidente vehicular en un viaje de 1000 millas?

1 en 366

¿Salga con un millonario?

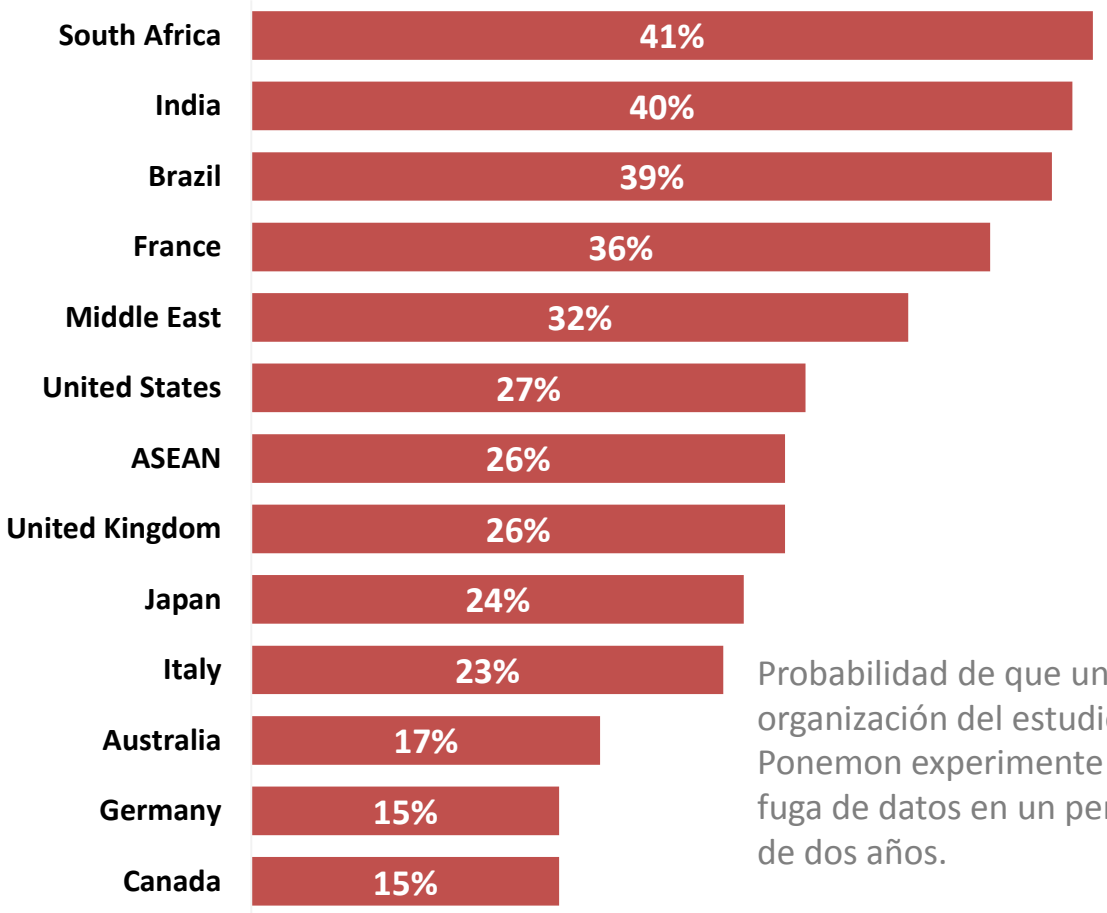
1 en 220

La probabilidad de que experimente una fuga de datos son mayores

¿Experimentar una fuga de datos?

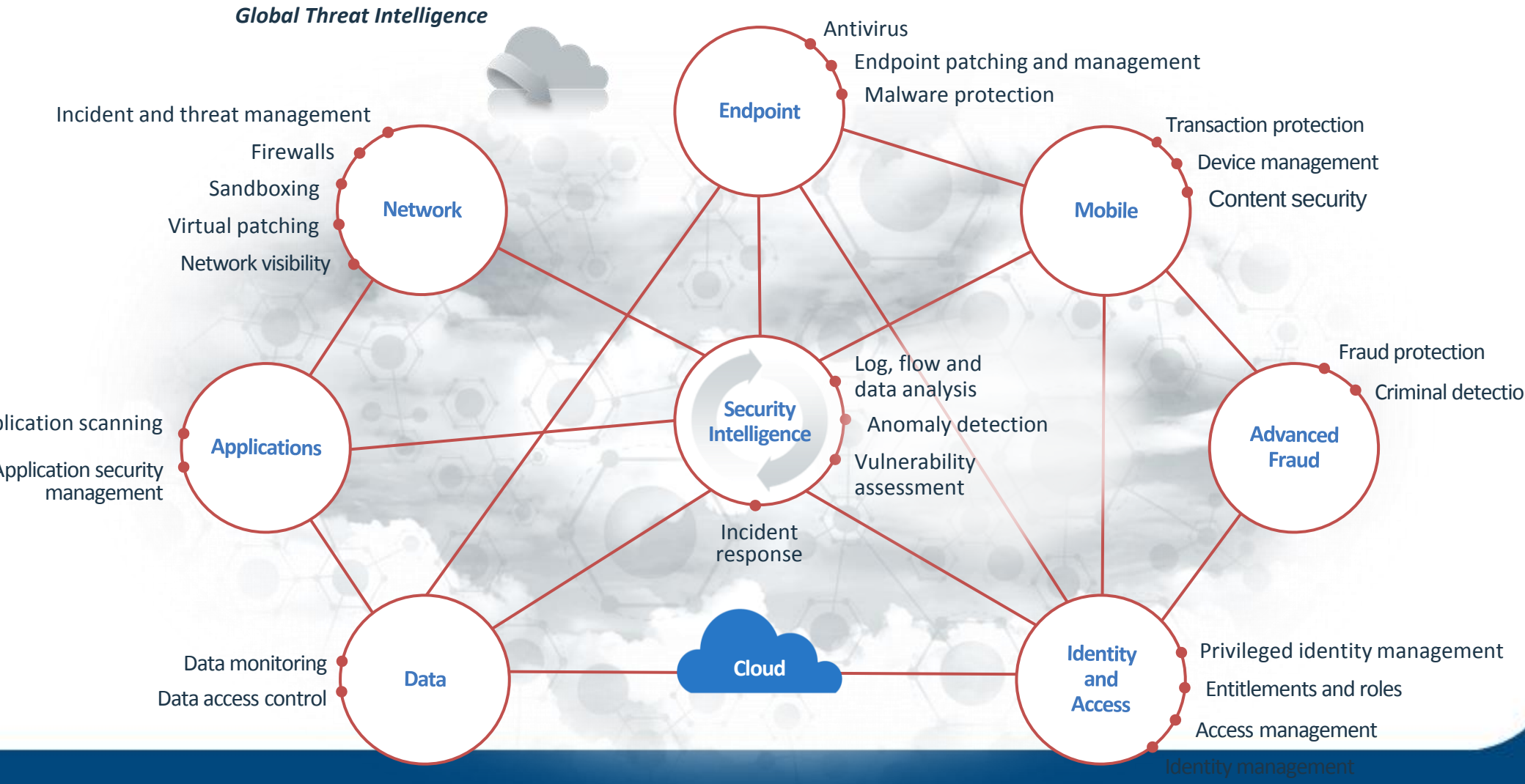
1 en 4

(Global average 28%)



Probabilidad de que una organización del estudio Ponemon experimente una fuga de datos en un periodo de dos años.

Mejorar la seguridad mediante inteligencia e integración



Controles Críticos de seguridad

- CSC 1: Inventario de dispositivos autorizados y no autorizados.
- CSC 2: Inventario de software autorizado y no autorizado.
- CSC 3: Configuración segura de HW y SW en: Móviles, Laptops, Servidores, etc.
- CSC 4: Evaluación continuación vulnerabilidades y remediación.
- CSC 5: Uso controlado de privilegios administrativos

Fuente: The Center for Internet Security (CIS) – Critical Security Control v6.0 - SANS

Lecciones aprendidas de los últimos ciber ataques

1	Reduzca su superficie de ataque asegurando que todos los sistemas son escaneados y parchados de manera regular
2	Despliegue tecnologías de bloqueo de puertos para host externos y desde la red local a la WAN
3	Asegúrese de que existe segmentación de la red y que las políticas se cumplen
4	Respalde la información crítica de manera frecuente y asegúrese de que los mismos funcionan (restaure data)
5	Tenga un plan de ciber resiliencia que sea probado regularmente
6	Eduque a sus empleados a no hacer clic en adjuntos sospechosos
7	Realice regularmente pruebas internas y externas de penetración
8	Monitoree las cuentas con acceso privilegiados

Finalmente:

No se puede proteger lo que no se conoce; identifique los activos críticos y protéjalos

GRACIAS

Diego Oviedo
diego.oviedo@pe.ibm.com