Deloitte.

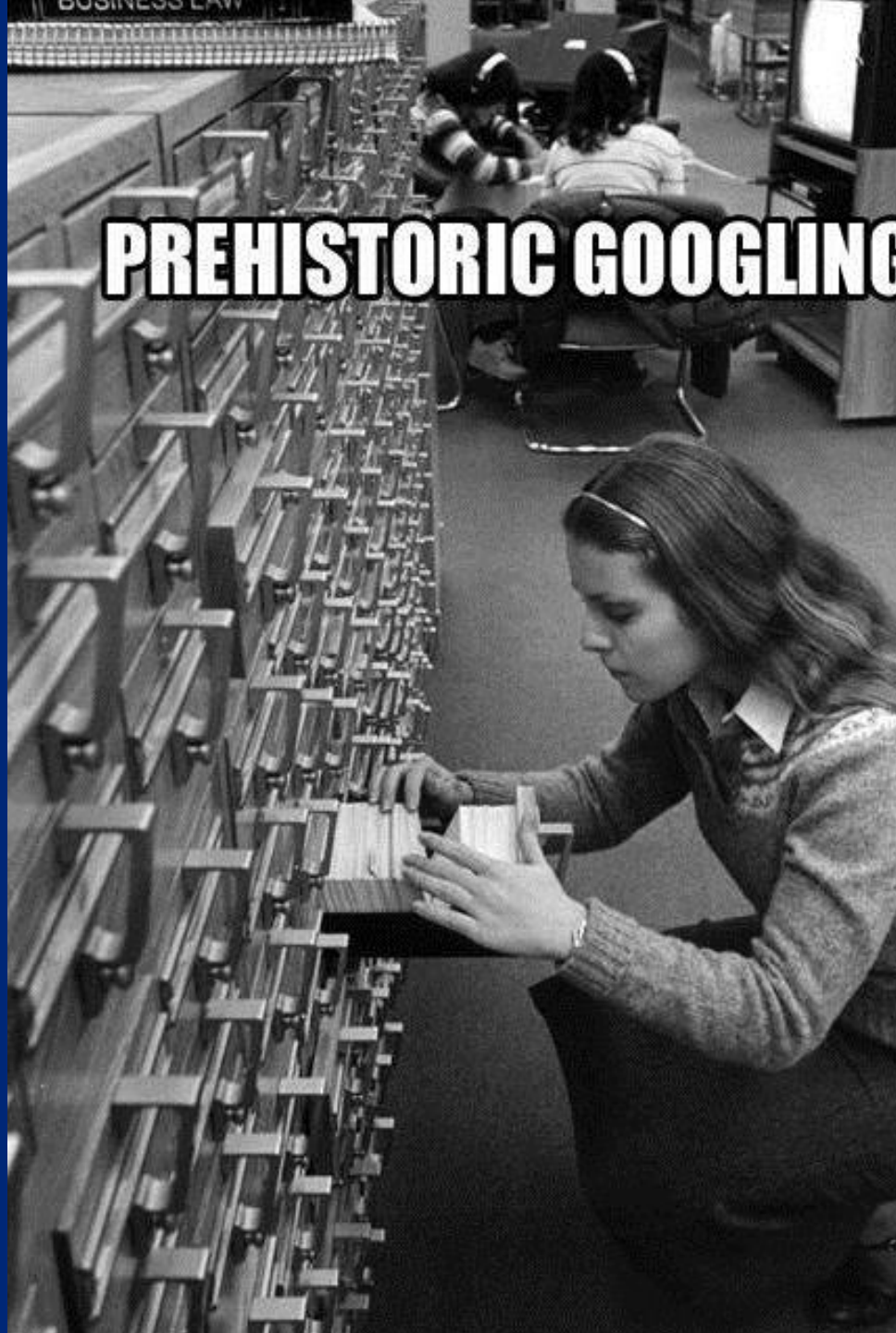
Cyber SOC
IT-ERS Services
Ciberinteligencia

Febrero 2014

Situación actual

Evolución histórica

Hace 40 años el 99% de las empresas almacenaba la información en archivadores, lo cual implicaba que las búsquedas fueran manuales.

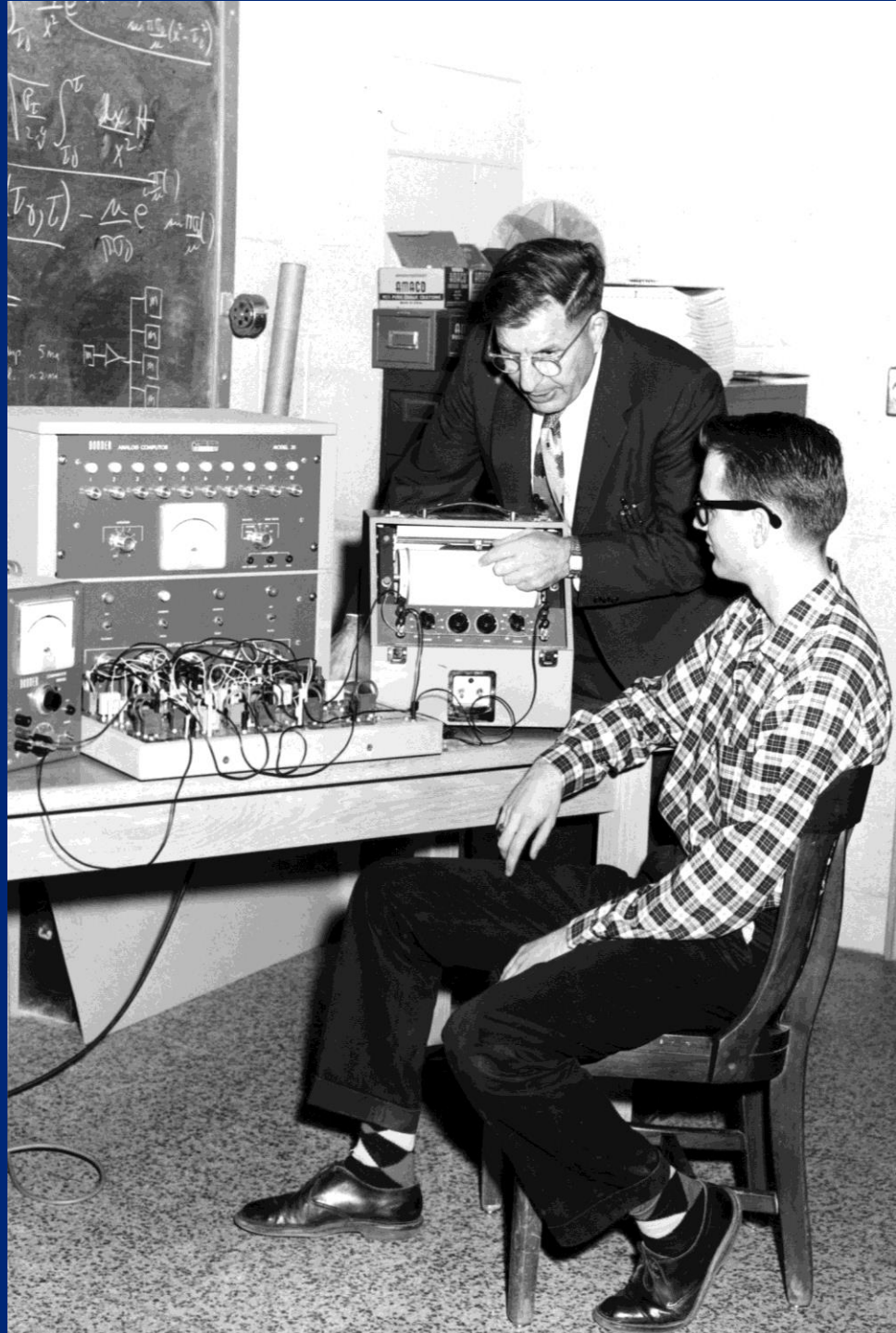


Evolución histórica

Las comunicaciones se realizaban a través de telefonía analógica, controladas por las compañías telefónicas

Evolución histórica

Las computadoras se usaban con fines académicos, educativos y militares



Evolución histórica

En la actualidad hemos mejorado la productividad y la forma de comunicarnos, alcanzando unos niveles impensables hace 40 años

Pero también nos hemos vuelto tecnológicamente dependientes, y esta dependencia conlleva riesgos

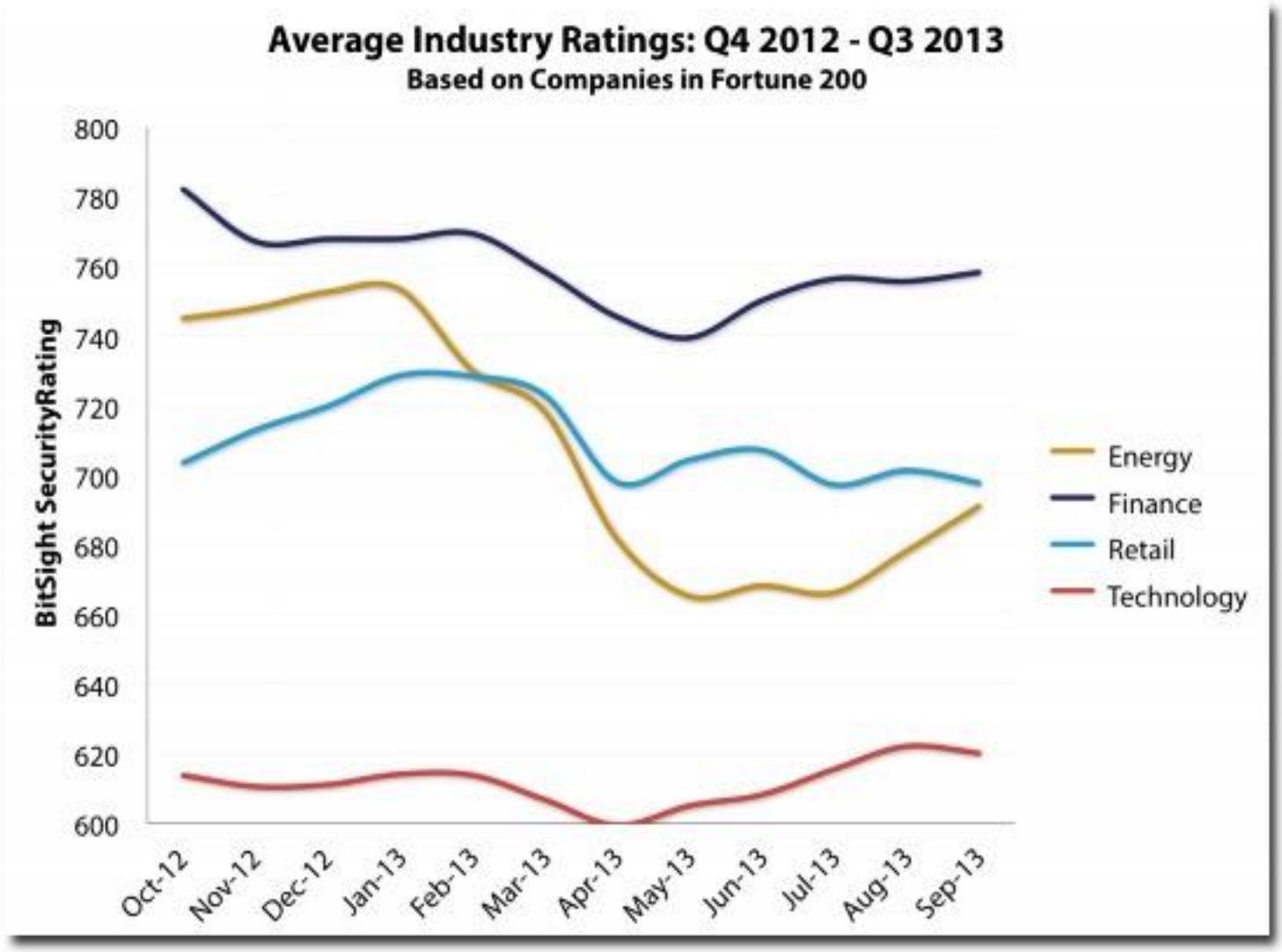
Situación actual
Algunos datos

Al analizar los incidentes de seguridad reportados en 2013 (la referencia es de The Fortune 200 companies), existe un descenso en sectores tradicionales y un ligero incremento en empresas tecnológicas.

Esto no quiere decir que las empresas estén ganando la batalla contra el cibercrimen, sino que se están trabajando nuevos vectores de ataque más sofisticados, desde los puntos de vista: objetivo y tecnológico.

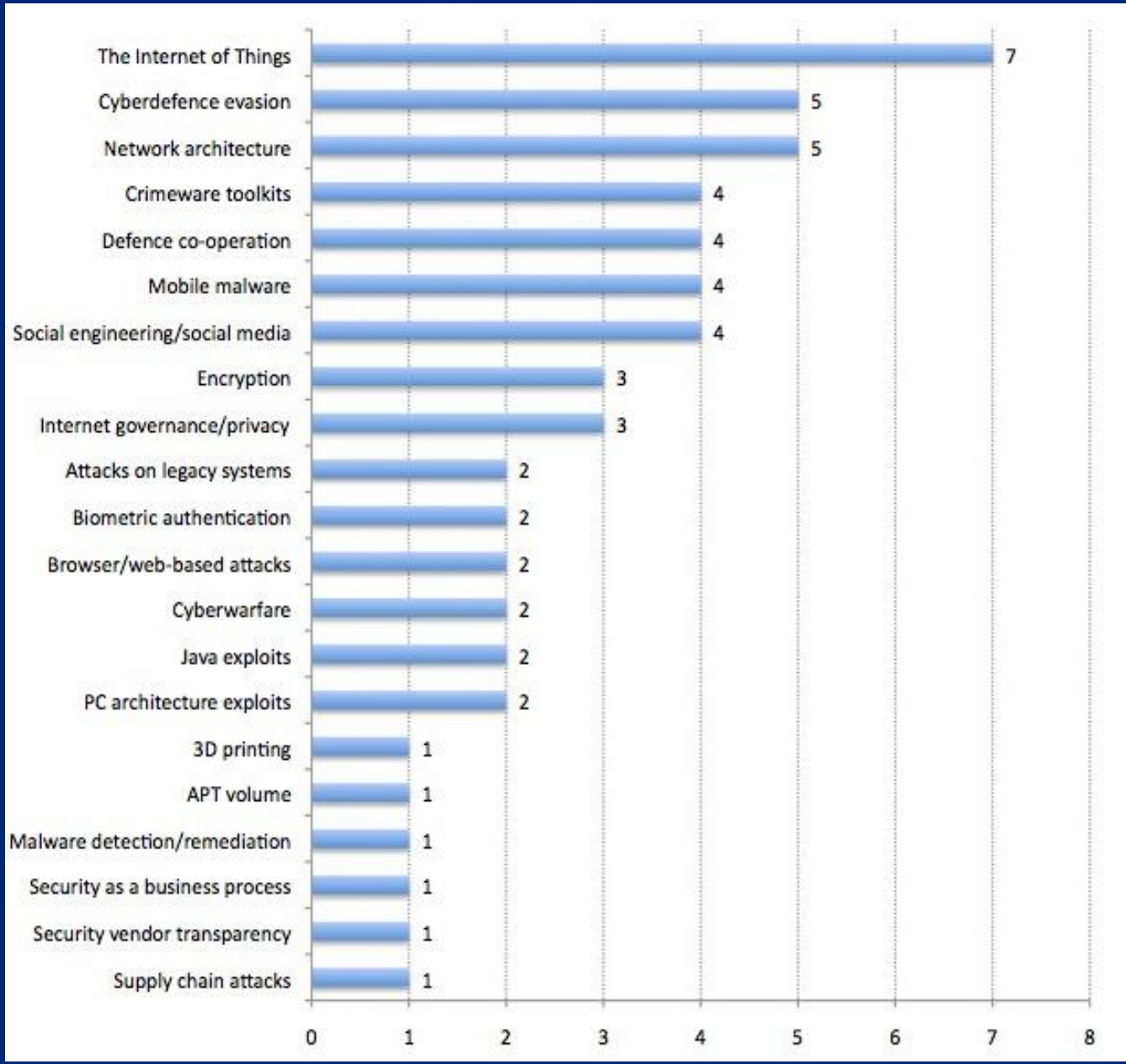
No podemos olvidar que el sector vulnerable sigue siendo el mismo para un mayor número de delincuentes informáticos.

Situación actual
Algunos datos (2)



Predicciones 2014

Predicciones 2014



* Compendio de predicciones de FireEye, Fortinet, Lancope, Neohapsis, Symantec, Websense and Zscaler

Internet de las Cosas

Se incrementarán los ataques dirigidos contra los dispositivos tanto domésticos como empresariales que estén conectados a Internet

Los delincuentes informáticos buscan hallar nuevas formas de fraude, como el ataque contra la domótica inteligente

Además, la tendencia es encontrar alternativas para atacar infraestructuras críticas nacionales a través de componentes secundarios conectados a Internet

Evasión de ciberdefensa

Nuevos métodos para ocultar *malware* con códigos de autenticación válidos, mediante la corrupción de los protocolos o el robo de firmas

Desarrollo de formas para librar los sistemas automatizados de análisis de *malware* (*Sandbox*)

Ataques contra entornos *cloud* y virtuales

Incremento de ataques informáticos dirigidos contra entornos en la nube con el objetivo de robar información

Los sistemas en *cloud* disponen de mayor accesibilidad y disponibilidad que los sistemas informáticos tradicionales, pero suponen también una mayor exposición de ataques externos

Aumento de ataques contra sistemas de máquinas virtuales, ya que con un solo ataque se pone en riesgo a un número importante de organizaciones que comparten recursos de computación

Gobierno de Internet
OSINT

Uso por parte de entidades públicas de sistemas de cibervigilancia y gestión de amenazas, reduciendo los derechos de privacidad de la ciudadanía a cambio de mayor seguridad en la red

En el caso de OSINT se trata de integrar los sistemas informáticos tradicionales de las fuerzas y cuerpos de seguridad con herramientas automatizadas de inteligencia de red y monitoreo de amenazas en Internet.

Ejemplos: Policía Federal de Brasil y la Policía Montada de Canadá

Malware contra dispositivos móviles

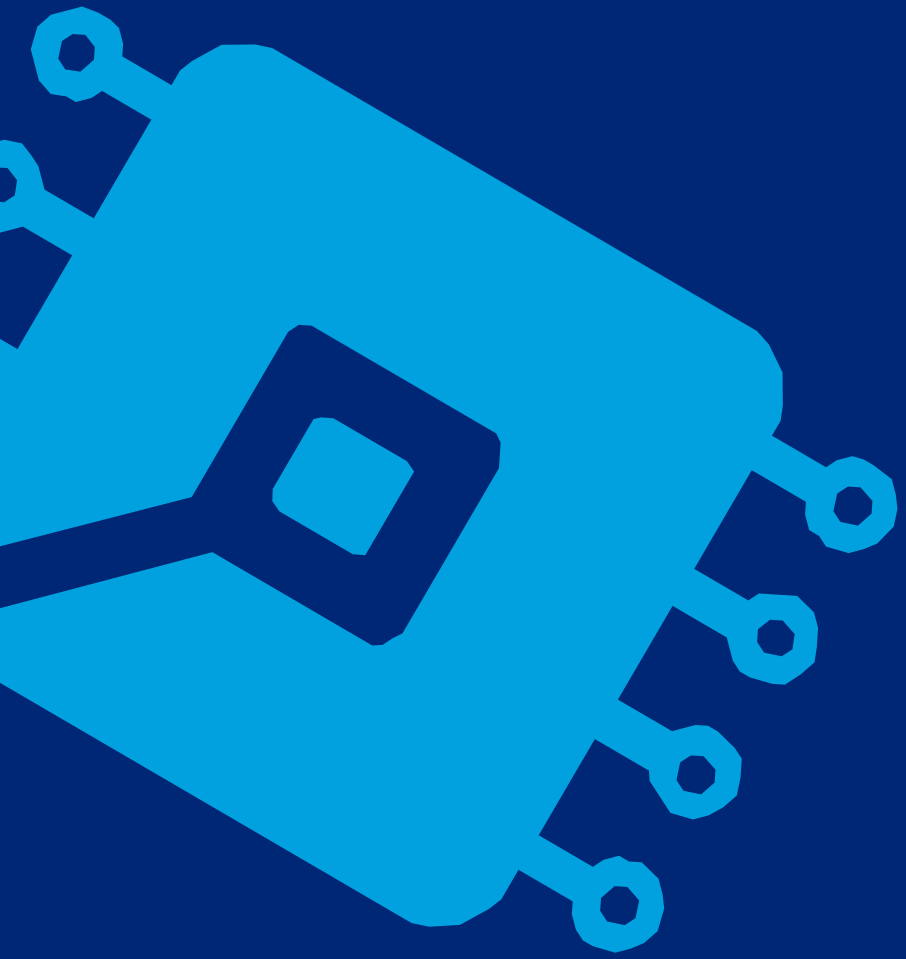
Incremento del *malware* contra dispositivos móviles

Modificación de *malware* tradicional
para el entorno móvil. Ejemplo: Zeus

Aumento de la productividad y uso de dispositivos móviles, como mayores transacciones bancarias, compras en comercio electrónico.
Como resultado hay un mayor interés
de los delincuentes por estas plataformas.

La ciberinteligencia como valor diferenciador

Motivación



Tener acceso a información de ciberinteligencia ayuda a la organización a entender su perfil de amenazas y los riesgos de negocio derivados.

Con la información facilitada, las empresas pueden abordar planes de acción y gestionar eficazmente los riesgos identificados.

Respuesta de 10 preguntas clave

1 ¿Qué tipo de ciberamenazas afectan a su organización?

2 ¿Qué clase de información sensible puede filtrarse en Internet?

3 ¿Cuáles son las credenciales que pueden estar en manos de hackers?

4 ¿Cuáles de sus sistemas pueden haber sido comprometidos?

5 ¿Qué tipo de sitios web pueden estar suplantando su identidad?

Respuesta de 10 preguntas clave

6 ¿Qué clase de información publican sus empleados?

¿Qué virus y malware está diseñado para atacar a su organización o a sus clientes? 7

8 ¿Actualmente, existen documentos sensibles publicados en Internet?

¿Qué bases de datos pueden haber sido robadas? 9

10 ¿Qué amenazas en redes sociales afectan a su organización?

Detectar un amplio abanico de amenazas

- Phising
- Malware
- Credenciales robadas
- Configuración de seguridad de sistemas críticos
- Robo de datos personales
- Planificación de ataques DDoS
- Vulnerabilidades específicas de sus sistemas
- Información sobre sistemas comprometidos

Detectar un amplio abanico de amenazas (2)

- Fuga de información de bases de datos
- Registro de dominios fraudulentos
- Publicación de documentos confidenciales
- Perfiles falsos en redes sociales
- Información publicada por empleados
- Estafas relacionadas con puestos de trabajo

Detectar un amplio abanico de amenazas (3)

- Mercado de imitaciones
- Incumplimiento de copyright
- Promociones fraudulentas
- Menciones negativas en medios o foros
- Menciones negativas sobre directivos clave

Inteligencia de clientes
Ejemplos

Ejemplo 1: Inteligencia de servidores C&C

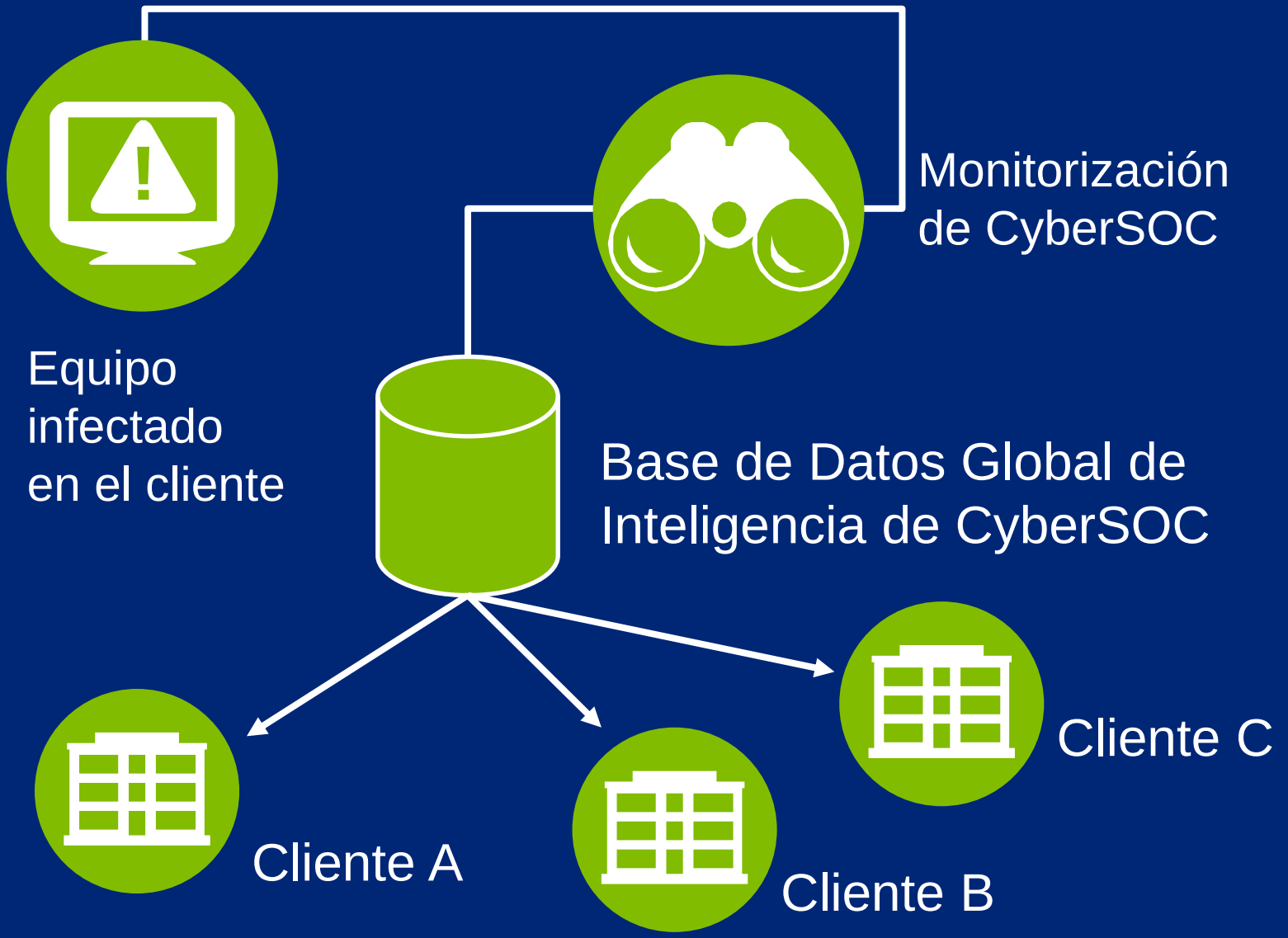
01/ Nuestro equipo de MSS detecta la activ ad sospechosa de varias estaciones de tra o en una red interna del cliente

02/ Estas estaciones de trabajo intentan en información robada a un servidor C&C

03/ Las direcciones IP del servidor C&C so ingresadas en la plataforma de inteliger para poder reconocer este malware en resto de los clientes

Inteligencia

Ejemplo 1: Inteligencia de servidores C&C (2)



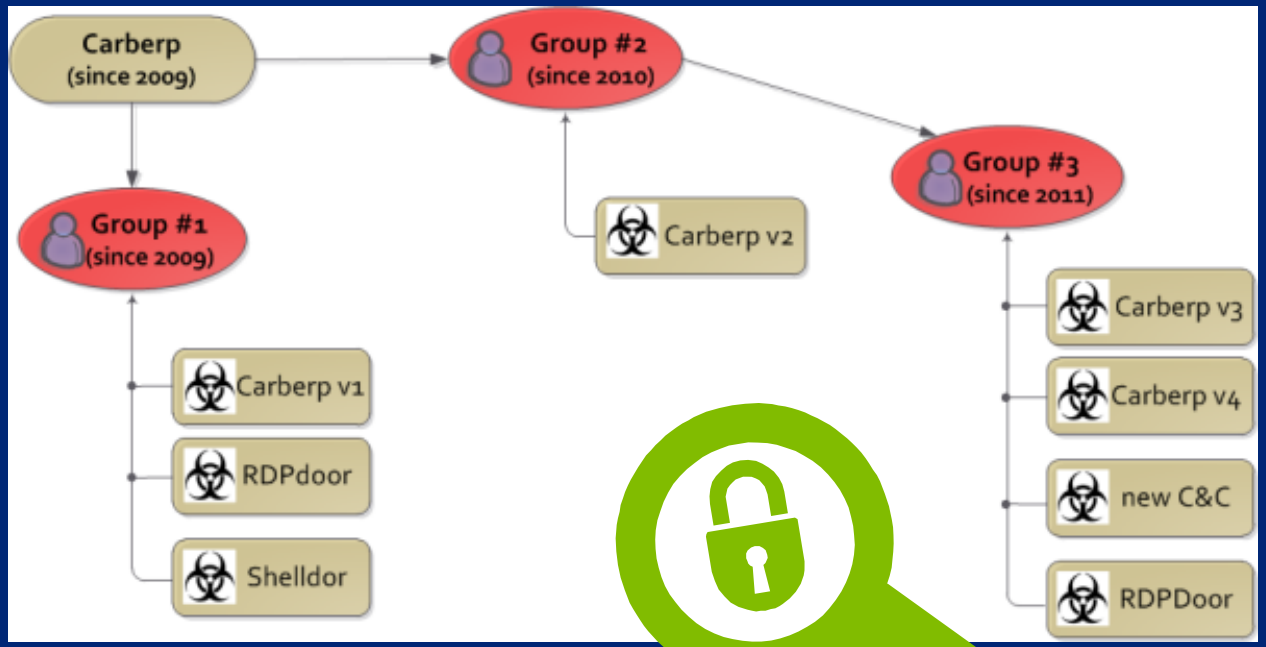
Ejemplo 2: Información robada

01/ Nuestro equipo de inteligencia recoge información robada de un cliente de *bot*

02/ Los datos recogidos de *botnet* se analiz se descubre otra información

03/ Esos clientes adicionales se benefician nuestro análisis y se informa a ellos tam sobre la información robada

Ejemplo 2: Información robada (2)



Cliente afectado

Análisis
en profundidad

Cliente A también afectado

Cliente B también afectado

Ejemplo 3: Inteligencia de intrusión

01/ Nuestro equipo de pruebas de intrusión realizó una evaluación de vulnerabilidades para un cliente y se encontró un escenario de intrusión

02/ El escenario detectado se aplica a todas las organizaciones que reúnen ciertas condiciones

03/ Todos los clientes que reúnen dichas condiciones son informados de dicha amenaza y se comparte información de detección con ellos

Ejemplo 3: Inteligencia de intrusión (2)

Estudios de caso
Ejemplos

Institución financiera con presencia en todo el mundo

Escenario

La empresa sufrió una incidencia de fuga de información crítica debida a la publicación de las credenciales del usuario en un foro de cibercrimen.

La publicación no se identificó, por lo que las cuentas asociadas al usuario no se bloquearon a tiempo.

Institución financiera con presencia en todo el mundo (2)

Solución propuesta

Se ejecutó el servicio de CyberWatch para el alcance definido por el cliente, teniendo en cuenta los requisitos descritos anteriormente.

Ya que Deloitte era el proveedor de anti-*phishing*, algunos de los procedimientos establecidos eran también válidos para este servicio, acelerando el proceso de provisión.

Institución financiera con presencia en todo el mundo (3)

62 incidentes relevantes informados en el último año (2012)

Asistencia 24x7 para llevar a cabo análisis forenses y otras investigaciones en los datos proporcionados por el servicio

Proveedor de software con oficinas en 24 países

Escenario

La empresa requirió una solución de monitorización de seguridad de Cyber Intelligence combinando datos internos con información recogida de fuentes externas, para detectar información de las IPs que se estaban fugando.

Proveedor de software con oficinas en 24 países (2)

Solución propuesta

Deloitte propuso implantar y operar una solución SIEM, así como crear un *feed* personalizado de ciberinteligencia, tomando como entrada activos del cliente, marcas y palabras clave relacionadas.

Las alertas personalizadas que vengan de la plataforma de ciberinteligencia se insertarán como alertas SIEM y serán gestionadas por nuestro equipo como parte de la operación 24x7.

Proveedor de software con oficinas en 24 países (3)

124 eventos relevantes de **seguridad interna** informados en 6 meses de servicio

12 alertas externas, incluyendo credenciales, recogidas por la Plataforma de Inteligencia

Institución financiera que opera en 19 países

Escenario

La empresa requirió un programa de gestión de vulnerabilidades para descubrir debilidades en activos tecnológicos críticos.

Institución financiera que opera en 19 países (2)

Solución propuesta

Se realizó una huella digital de la presencia en Internet del cliente y descubrió una serie de amenazas críticas que no habían sido identificadas por ninguna evaluación de vulnerabilidades realizada en los últimos 19 años.

A continuación, se propuso implantar una función de ciberinteligencia junto con un programa de gestión de vulnerabilidades para asegurar que las amenazas posteriores serán también identificadas.

Institución financiera que opera en 19 países (3)

98 vulnerabilidades de alto riesgo informadas tras 3 meses de servicio

57 amenazas externas que pudieran afectar activos críticos del cliente probadas