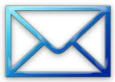

CIBERDEFENSA
PROGRAMA DE VINCULACIÓN Y DIFUSIÓN
CIBERDEFENSA
JORNADA REGIONAL EN ROSARIO
11 DE AGOSTO DE 2014
UTN Rosario - Zeballos 1341 - Salón de usos múltiples
inscripción e informes www.mindef.gob.ar
ORGANIZAN:
Facultad Regional Rosario
Universidad Tecnológica Nacional
AGASSI
CUANDO UN PAÍS SE JUNTA.
HAY FUERZA.
Ministerio de
Defensa
Presidencia de la Nación

Ministerio de Defensa
Presidencia de la Nación

Fernando A. Corvalán

Coordinador Técnico del Comité de Ciberdefensa

Jefatura de Gabinete de asesores



fernando.corvalan@mindef.gov.ar

@fercorvalan

Ataques persistentes (APT)

Ciberdefensa inteligente vs tecnología basada en firmas

Que es un APT

- El término APT se suele asociar erróneamente al uso de malware dirigido, pero es algo más.
- APT es el grupo de gente que esta detrás del ataque, no la operación y mucho menos el malware.
- El malware es como “una bomba”. Es lo que “mata”, pero para lanzar una bomba hace falta un avión, hacen falta pilotos, hacen falta ingenieros que diseñen la bomba, gente de inteligencia y medios de reconocimiento que digan donde hay que dejar caer la bomba

Que es un APT

Además no cualquier grupo de “ciber-agresores” entra dentro del término APT si no cumplen las condiciones básicas del término:

- ***Avanzado:*** En el sentido de que los atacantes tienen recursos técnicos, económicos y de inteligencia amplios.
  Son grupos poderosos o naciones.
- ***Persistente:*** Es decir los ataques no son únicos y se suelen mantener a largo plazo.
- ***Amenaza:*** Al estar realizados de forma organizada (Las herramientas de seguridad tradicionales están diseñadas para evitar ataques puntuales y por lo tanto son previsibles y fáciles de evadir si se realizan los ataques de manera planificada).

Cronologia de ataques APT

- 1999 Moonlight Maze - http://en.wikipedia.org/wiki/Moonlight_Maze
- 2005 Titan Rain - http://en.wikipedia.org/wiki/Titan_Rain
- 2008 Buckshot Yankee - http://en.wikipedia.org/wiki/2008_cyberattack_on_United_States
- 2009 Byzantine Hades / Gh0stNet - http://en.wikipedia.org/wiki/GhostNet
- 2010 Stuxnet - http://en.wikipedia.org/wiki/Stuxnet
- 2010 Aurora / Hydraq - http://en.wikipedia.org/wiki/Operation_Aurora

Cronologia de ataques APT

2011

- Night Dragon - http://www.mcafee.com/us/about/night-dragon.aspx
- Duqu - http://en.wikipedia.org/wiki/Duqu
- Shady RAT - http://en.wikipedia.org/wiki/Operation_Shady_RAT
- Sykipot - http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
- RSA SecurID Breach - http://www.zdnet.com/nation-state-behind-rsas-securid-breach-2062302463/
- Black Tulip / Diginotar Hacking - http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

Cronologia de ataques APT

2012

- Flame - http://en.wikipedia.org/wiki/Flame_(malware)
- Mahdi - http://en.wikipedia.org/wiki/Mahdi_(malware)
- Red October - http://en.wikipedia.org/wiki/Red_October_(malware)

Cronologia de ataques APT

2013

- Icefog - http://www.securelist.com/en/analysis/204792307/The_Icefog_APT_Frequently_Asked_Questions
- Bit9 Break-in - http://petehoang.blogspot.com.es/2013/02/bit9s-apt-hacker-break-in.html
- DeputyDog - http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
- NetTraveler - https://www.securelist.com/en/blog/8105/NetTraveler_is_Running_Red_Star_APT_Attacks_Compromise_High_Profile_Victims

Cronologia de ataques APT

- Careto / Mask - http://www.securelist.com/en/blog/208216078/The_Careto_Mask_APT_Frequently_Asked_Questions

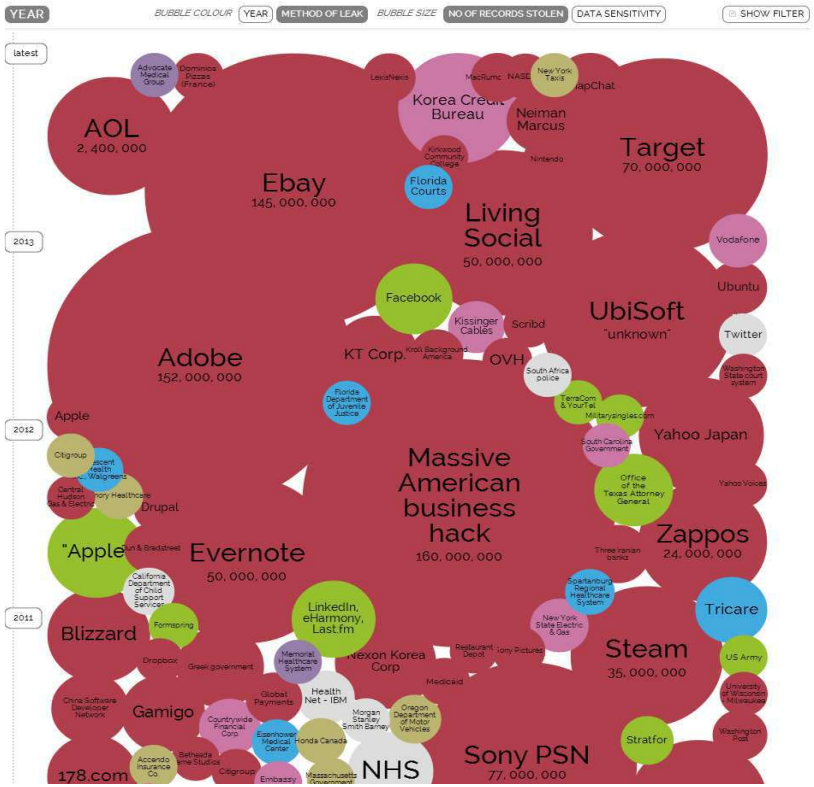
- Snake - http://www.baesystems.com/what-we-do-rai/the-snake-campaign

Podemos estar seguros siendo simples mortales?

Grandes empresas han sufrido APT

- Symantec
- RSA
- Adobe
- Sony
- Redes sociales (Linkedin, Facebook, Twitter)

Algunos TARGET's de APT



METHOD OF LEAK

- All
- Accidentally published
- Hacked
- Inside job
- Lost / stolen computer
- Lost / stolen media
- Poor security

Etapas de un APT (ejemplo)

- 1- El atacante envía un phishing de correo electrónico para obtener la entrada al objetivo.
- 2- Cuando la víctima abre el archivo adjunto, se instala el malware personalizado (Exploit 0-Day)
- 3- El malware personalizado enlaza un sitio web de mando y control y descarga malware adicional.
- 4- El atacante establece múltiples puertas traseras para asegurar el acceso si se encuentran los otros sistemas.
- 5- El atacante tiene acceso al sistema y vuelca los nombres de cuenta y contraseñas del controlador de dominio.

Etapas de un APT (ejemplo)

- 6- El atacante obtiene las contraseñas y ahora tiene acceso a las cuentas de usuarios legítimos para continuar el ataque sin ser detectado.
- 7- El atacante realiza de reconocimiento para identificar y recopilar datos.
- 8- Los datos se recogen en un servidor de ensayo.
- 9- Los datos se exfiltraron desde el servidor de ensayo.
- 10- El atacante cubre sus pistas mediante la eliminación de archivos, pero puede volver en cualquier momento para llevar a cabo actividades adicionales.

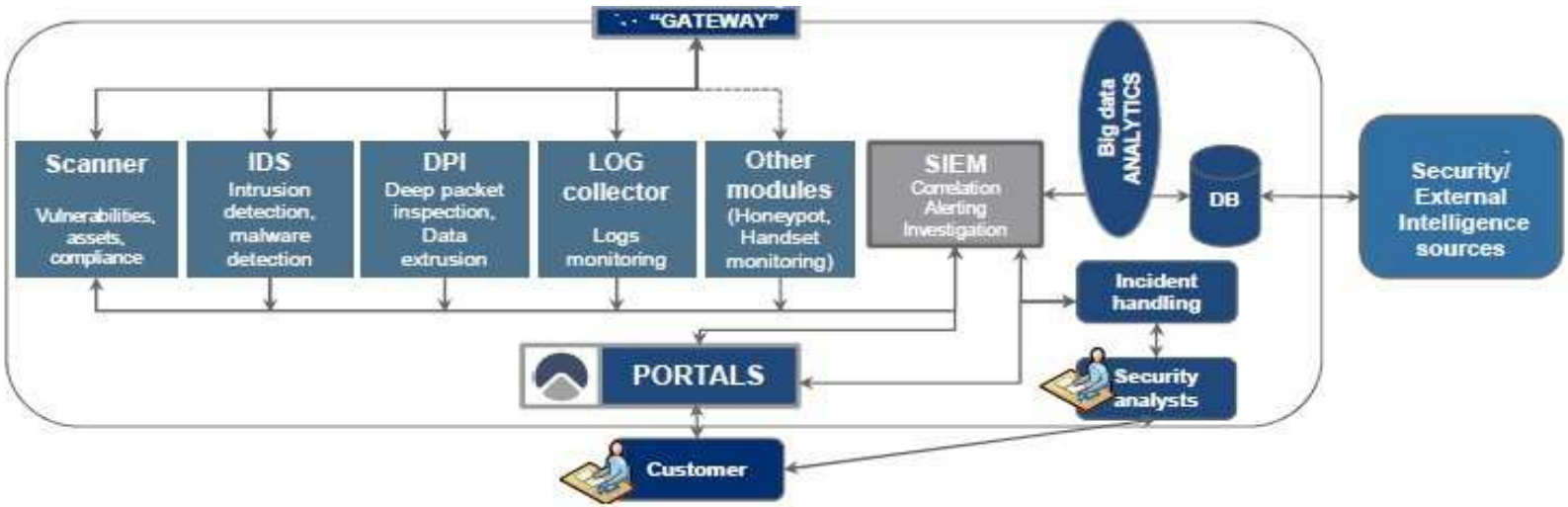
Métodos de protección estandar

- Firewall de borde
- Software Antivirus
- IDS / IPS
- SIEM / LOG’s centralizados

Métodos efectivos

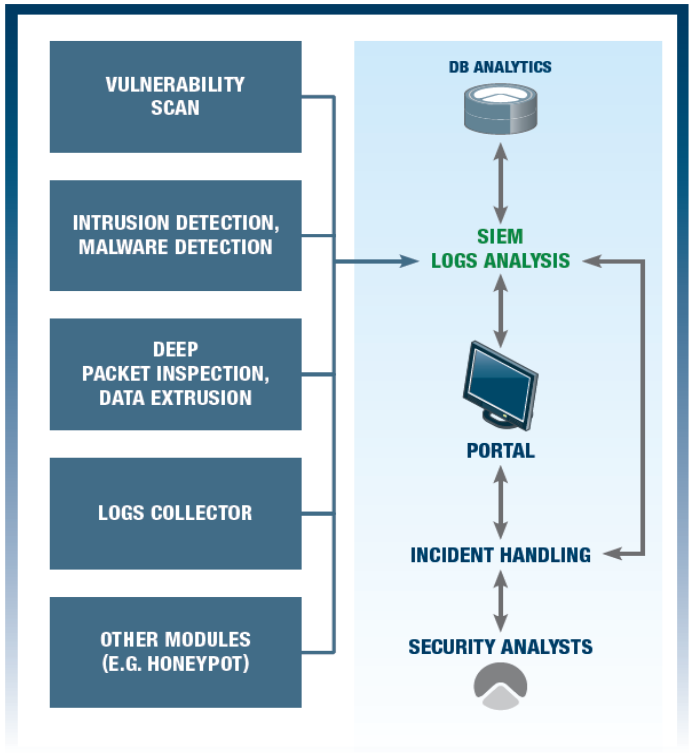
- BIG Data
- Almacenamiento de trafico en tiempo real y TAG’s (metadatos)
- Analisis de comportamiento
- Ciberinteligencia basada en cloud y Honeynets

SOC FUNCTIONAL ARCHITECTURE



SOC FUNCTIONAL ARCHITECTURE

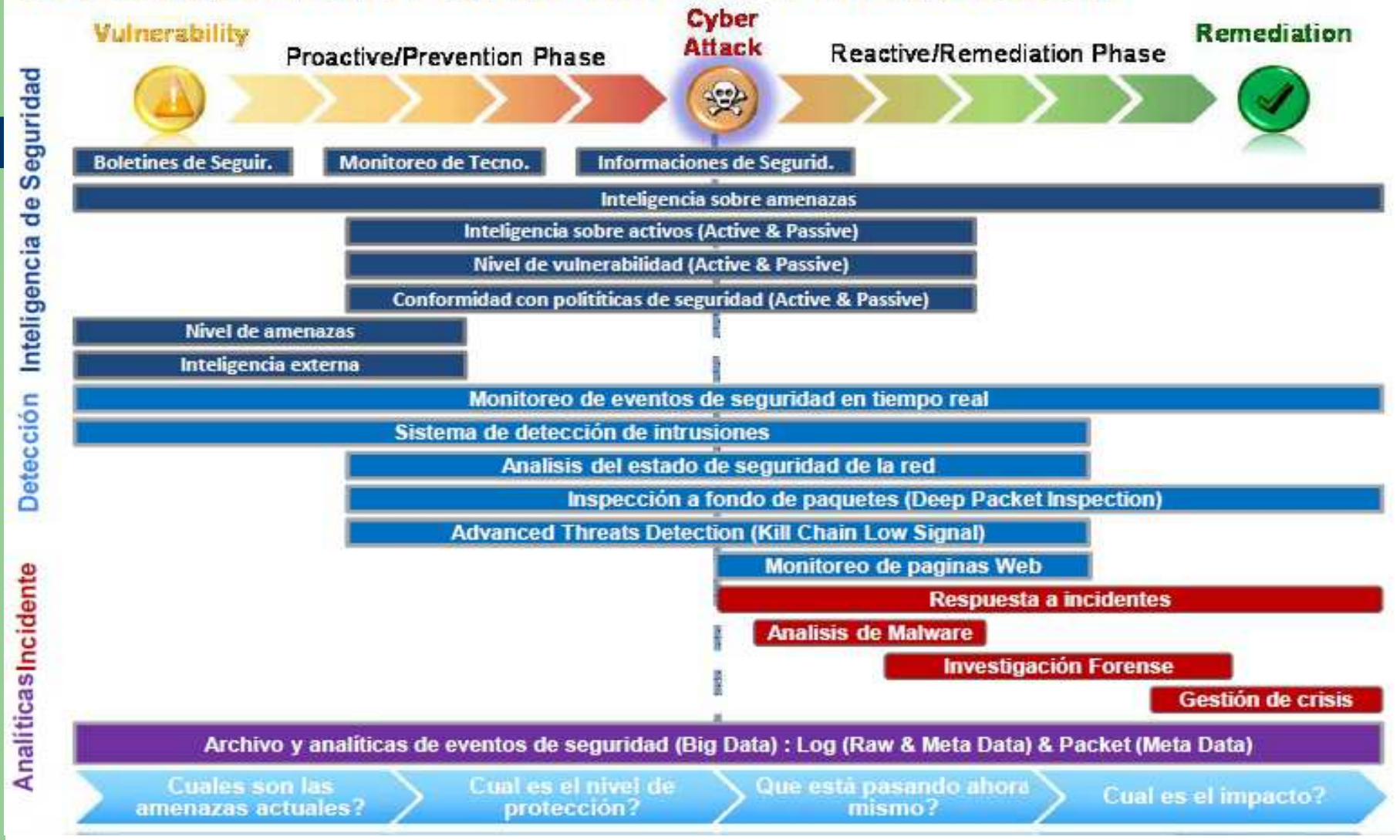
- Specific **threat monitoring tools** activated as per customer requirements (IDS/IPS,DPI…)
- Data collected, post processed, analyzed, **classified and correlated**
- **Big data analytics and SIEM** to enable automatized processes for incident management security analysts can focus on relevant threats and avoid unnecessary emergencies and fire drills
- **Advanced reporting and recommendations** to anticipate security issues
- **Incident response and recovery support**



Modulos de un SOC

- **Perimeter monitoring**
- Continuous assessment & service discovery
- Intrusion detection
- Web service monitoring
- **Intrusion detection**
- Service intrusion detection
- Web service protection
- E-mail flow security
- Advanced Persistent Threat (APT) detection
- **Extrusion detection**
- C&C connection detection
- Data Leak Prevention (DLP)
- Advanced Persistent Threat (APT) detection
- **Internal services monitoring**
- Assets discovery
- Logs monitoring
- Security controls monitoring
- **Threat intelligence**
- Intelligence feeds
- Reputation and brand monitoring

SOC: ACCIÓN PREVENTIVA Y REACCIÓN



Contexto Tecnológico

Volumen – Velocidad – Variedad

EVENTOS -- TRÁFICO

- Múltiples Sistemas Operativos
- Dispositivos móviles
- Dispositivos de seguridad e infraestructura
- Cloud - Virtualización

Contexto humano:

Ante el contexto tecnológico …

- Equipos de trabajo acotados
- Falta de conocimiento/experiencia
- Procesos inadecuados
- Baja visibilidad/control

Contexto Seguridad

Ante el contexto tecnológico y humano…

- Atacantes motivados económicamente
- Atacantes motivados políticamente
- Ataques sofisticados
- Crecimiento exponencial del malware
- Perímetro indefinido

BIG DATA + CONTEXTO

(HUMANO x TECNOLOGIA x SEGURIDAD)

...Algunas consecuencias...

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

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 el 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 de los jugadores sino en presumir y mostrar la escasa seguridad del sistema de Sony.

Symantec verifies stolen source code posted by Anonymous is "legitimate"

Symantec concerned that Anonymous group will also now post other stolen source code

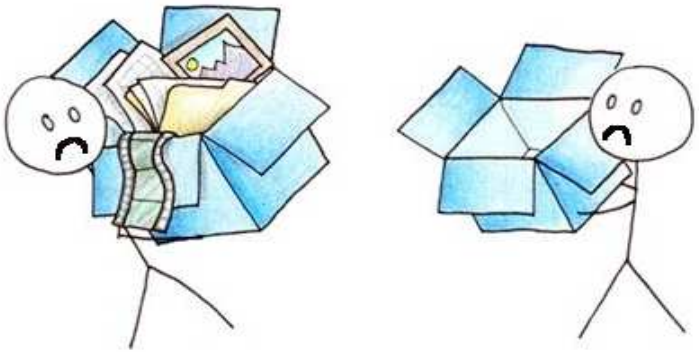
By Ellen Messmer, Network World
February 07, 2012 01:20 PM ET

Network World - Symantec is in an ongoing fight against hackers in the group Anonymous that last January attempted to extort a payment of around $50,000 from Symantec in exchange for not publicly posting stolen Symantec source code they had stolen for various older Symantec security products dating to 2006.

More on high-tech crime: From Anonymous to Hackerazzi: The year in security mischief-making

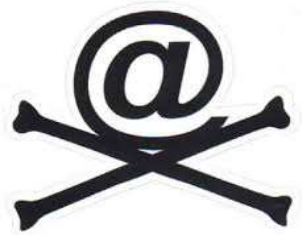
Dropbox admite el hackeo de sus cuentas y anuncia nuevas medidas de seguridad

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.

¿Quién puede generar un ataque ante este contexto?



-Cyber-Criminales

-Cyber-terroristas

-Estado

¿Que sabe el atacante acerca de mi organismo?

- Que dispone de pocos recursos
- Que usa tecnología tradicional
- Que está desbordado de información
- Que tiene un eslabón débil

¿Cuales son las fases de un ataque?

¿Cuales son las fases de un ataque?

1

Recopilación de información:

Se trata de adquirir información estratégica sobre el entorno de TI objetivo y la estructura de la organización.

¿Cuales son las fases de un ataque?

2

Punto de entrada:

Las APTs buscan lograr entrar en la red a través del correo electrónico, mensajería instantánea o redes sociales, explotando en su mayoría vulnerabilidades de día 0 de diferentes desarrolladores de software y sistemas.

3

Explotación

Ejecutan un exploit 0 Day para tomar control del equipo y evadir contramedidas

4

Movimiento lateral:

Localizan los hosts que alojan información sensible dentro de la red objetivo.

5

Descubrir activos y datos:

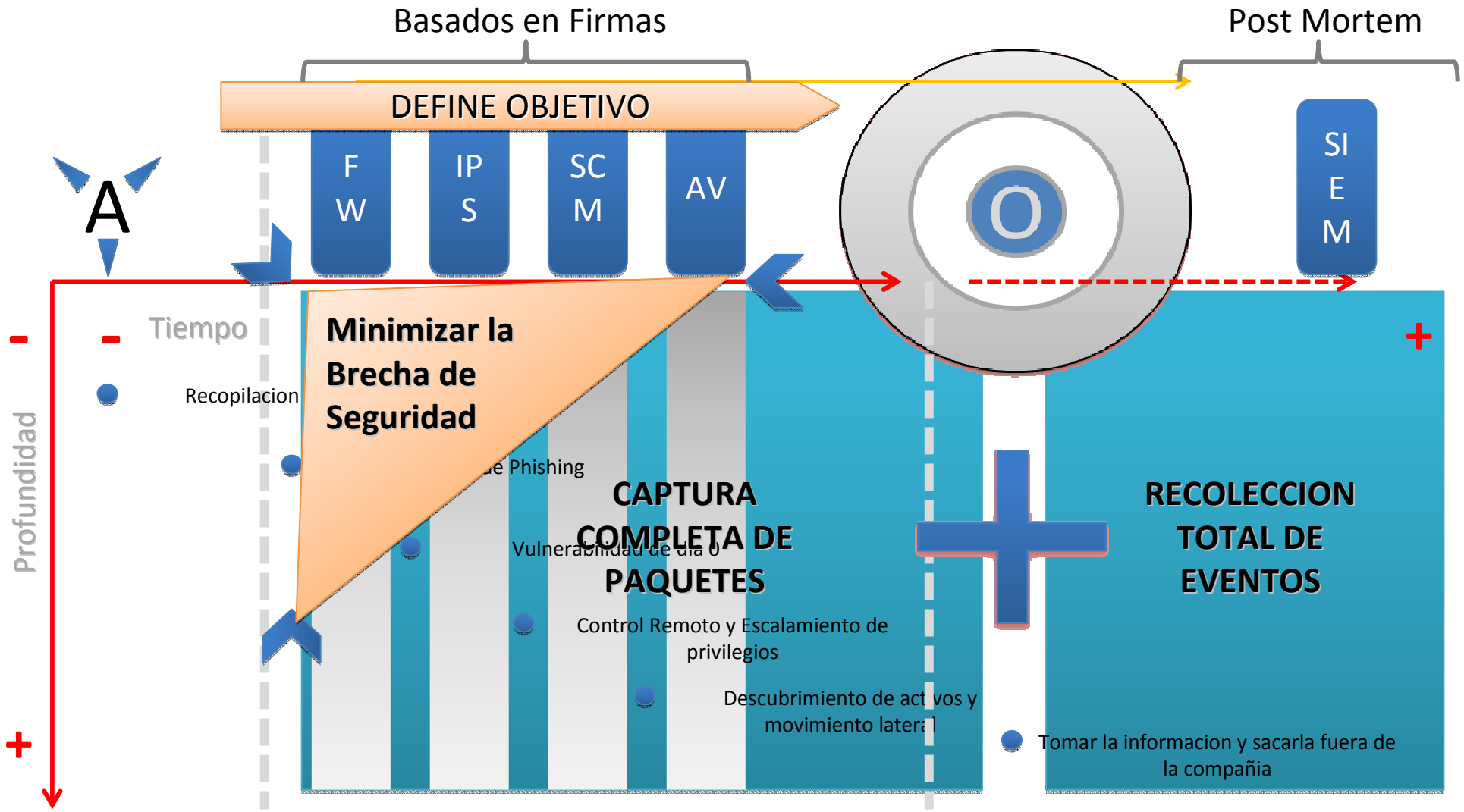
Identificar los datos valiosos para aislarlos con el fin de proceder a futuras sustracciones de información.

6

Extracción de datos:

En esta etapa se procede a transmitir la información a un lugar controlado por los responsables de las amenazas.

Solo un ataque…



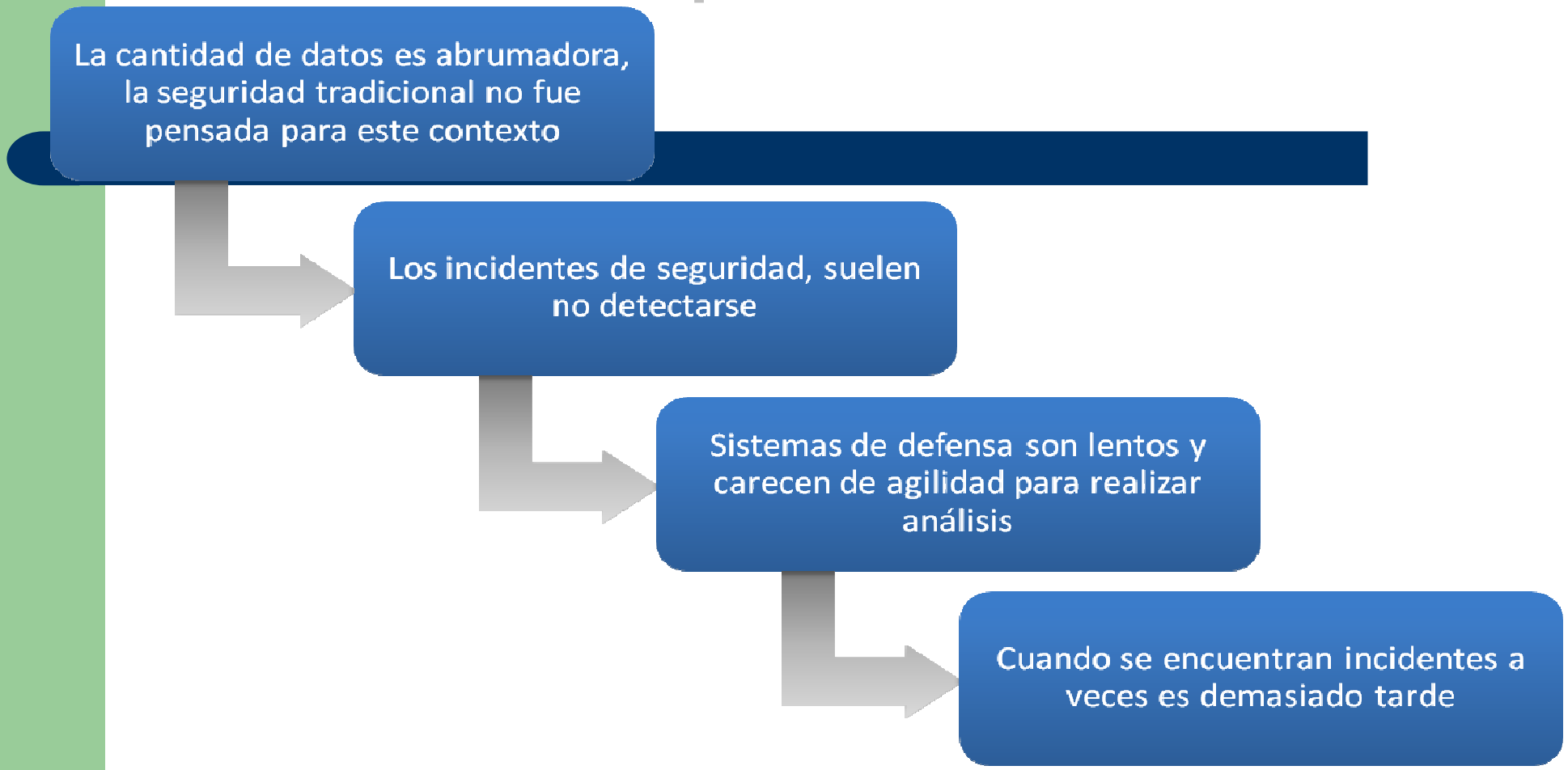
El enfoque tradicional de Seguridad
NO ES SUFICIENTE

99% de las brechas comprometen en “días” o menos tiempo, un 85% de estas conduce a una ex filtración de datos

85% de las brechas lleva semanas a meses para ser descubiertas

Source: Verizon 2012 Data Breach Investigations Report

El problema..


La cantidad de datos es abrumadora, la seguridad tradicional no fue pensada para este contexto
Los incidentes de seguridad, suelen no detectarse
Sistemas de defensa son lentos y carecen de agilidad para realizar análisis
Cuando se encuentran incidentes a veces es demasiado tarde

Requerimientos ante este contexto

Requerimientos de Seguridad HOY

Infraestructura de Big Data

"Rápida y escalable infraestructura que permita el análisis a corto y largo termino"

Mayor Visibilidad

"Debe permitir ver todo lo que esta pasando en mi ambiente"

Gran Capacidad Analítica

"Debe brindar la velocidad e inteligencia para descubrir e investigar amenazas potenciales en tiempo real"

Inteligencia Integrada

"Debe ayudar a entender y priorizar sobre el todo e informarme de hallazgos realizados por otros"

Una solución unificada que nos permita:

- Monitoreo de la Seguridad
- Investigación y gestión de incidentes basados en la criticidad de los activos a proteger
- Generación de reportes
- Análisis de APTs por comportamiento
- Armar cubos complejos a partir de metadatos
- Reconstruir sesiones completas mediante el tráfico capturado
- Que combine SIEM, Monitoreo de la seguridad de las redes, Administración y Análisis de Big Data
- Automatización de alertas y reportes

Una solución unificada que nos permita:

- Correlación de eventos
- Preferentemente que sea una única plataforma para la captura y análisis de largas cantidades de datos y trafico de red
- Arquitectura Distribuida y Escalable
- Repositorio de datos de seguridad para retención a largo término permitiendo análisis y cumplimiento regulatorio/normativo que almacene Metadatos de Paquetes y Logs, Crudo de Logs, Payload Específicos y permita el procesamiento de eventos complejos sobre los mismos.

Una solución unificada que nos permita:

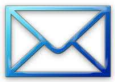
- Que se integre con otras herramientas de seguridad tales como SIEM, IDS/IPS, Firewalls, DLPs, WAFs, Honeypots, Antivirus, etc.
- Que posea una API (Interfaz de Programación) flexible para integrarla a soluciones de código abierto
- Que tenga una interface abierta para acceso y transformación de la información colectada
- Que permita integrar la clasificación de activos mediante su criticidad y contexto de producción para priorizar las investigaciones y el despliegue del plan de respuesta ante incidentes
- Gestión automática de workflow para el manejo de incidentes, seguimiento de progreso y visibilidad a responsables de cada unidad

Situación del mercado actual

- Tecnologías
- Experiencia
- Soluciones comerciales

Ministerio de Defensa
Presidencia de la Nación

Muchas gracias!


fernando.corvalan@mindef.gov.ar


@fercorvalan