EL BRAZO TONTO DE LA INTELIGENCIA DE AMENAZAS

Quienes somos

Luciano Moreira: Con más de 15 años de experiencia en IT, de los cuales los últimos 10 años desempeñándose en el área de Seguridad de la Información.

Auditor Líder ISO/IEC 27001:2005, Auditor Interno ISO/IEC 9001, Certified Integrator in Secure Cloud Services-EXIN, MCSE+Security, MCP Azure Infrastructure Solutions, MCSE Private Cloud certification, MCSA: Office 365, CLODU - CLOUD UNIVERSITY, ITIL V3.

Miembro de ISSA, ISACA, OWASP. Así como de sus capítulos locales.

(miembro del board del capítulo Argentina de la CSA (Cloud Security Alliance)) Vice-Presidente

1

Leonardo Rosso: Profesional de IT desde fines de los años noventa, y de Seguridad de la Información desde el 2001.

CISSP, Auditor Líder ISO/IEC 27001:2005, MCSE + Security, MCITP: Virtualization, MCITP Enterprise Administrator 2008, MCSA: Windows Server 2008, MCSA: Office 365, MS Specialist: Azure Infrastructure Solutions,

Miembro de ISSA, ISACA, ISC2, OWASP y FSF. Así como de sus capítulos locales.

(miembro del board del capítulo Argentina de la CSA (Cloud Security Alliance)) Presidente

2

Agenda

- Introducción
- Motivadores y agentes
- Malware y la evolución de las amenazas
- Threat intelligence lifecycle
- Threat intelligence Plataform
- Threat Intelligence Team
- Threat Intelligence Plan

Introducción

Antes de empezar…..

Pensar…..

Nuevo Paradigma……

Tendencias y Innovaciones (The Big Five)


Mobile
Social Business
Cloud computing
Consumerization
Big data

Introducción

- Este nuevo paradigma trae consigo nuevos riesgos:
  - Nuevo canales, sin políticas definidas
  - Exposición de los datos
  - Perdida de la noción de privacidad
  - Dificultad de control y trazabilidad

Introducción

La inteligencia para la ciberseguridad nunca ha sido más necesaria de lo que es ahora porque las amenazas son cada vez más complicadas de combatir.

Introducción

Tendencias

Grupos organizados

La mayor parte de los ataques proviene de cibermafias

Malware avanzado

Las herramientas cada vez son más indetectables

Consumo: objetivo de 2015

El usuario final es el principal objetivo de la ciberdelincuencia

Un problema global

Todas las empresas usan nuevas tecnologías

Cambio de paradigma

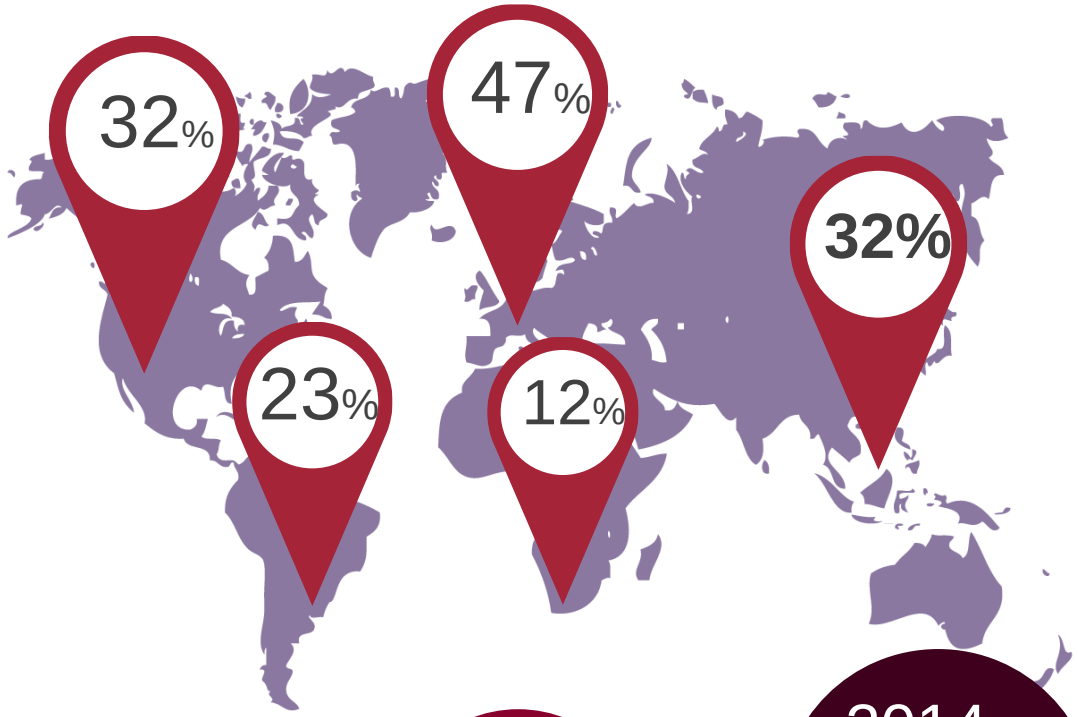
La seguridad de perímetro ya no es suficiente

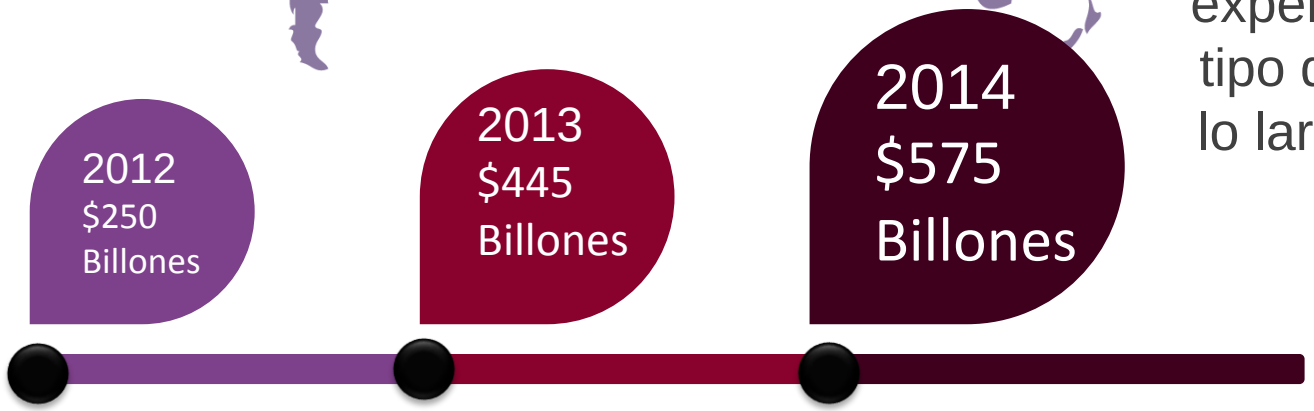
Consecuencias de un ataque

Pérdidas económicas y reputacionales de por vida.

Introducción

Situación Actual - Métricas





Evolución de Pérdidas por Cibercrimen/ amenazas

$575

Billones en pérdidas

69% víctimas

7/10 Adultos experimentarán algún tipo de ciberataque a lo largo de sus vidas.

Introducción

Víctimas del cibercrimen: pasado, presente y futuro

Ataques que ya se han producido

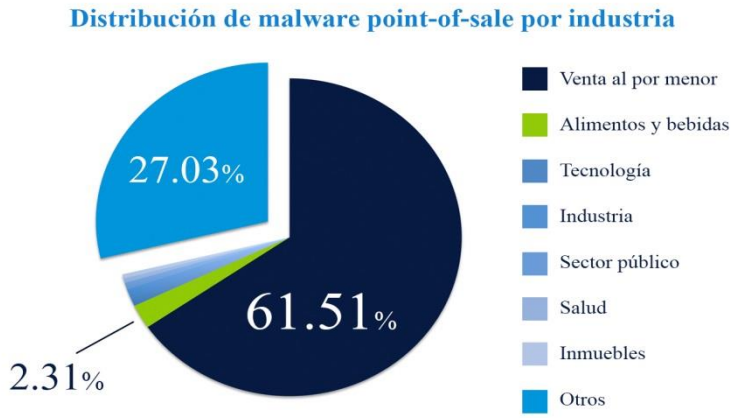
- 2014: más d 1.000 millones de datos robados
- Cada día:
  - 30.000 aplicaciones web vulneradas
  - 200.000 ciberataques

Nuevas víctimas día a día

- Más de un millón de víctimas al día:
  - 50.000 víctimas a la hora
  - 820 víctimas por minuto
  - 14 víctimas por segundo

Futuros objetivos

- Internet of things:
  - Coches
  - Alarmas
  - Casas
- Dispositivos móviles:
  - Smartphones
  - Tablets
  - Wereables
- Malware Point of Sale:
  - Datáfonos
- Drones



Motivadores y agentes

Motivadores

M – Money
I – Ideology
C – Coercion
E – Ego

Motivadores y agentes

Agentes

1. Ciberespionaje / Robo patrimonio tecnológico, propiedad intelectual

- China, Rusia, Irán, otros…
  Servicios de Inteligencia / Fuerzas Armadas / Otras empresas

2. Ciberdelito / cibercrimen

- HACKERS y crimen organizado

3. Ciberactivismo

- ANONYMOUS y otros grupos

4.Uso de INTERNET por terroristas

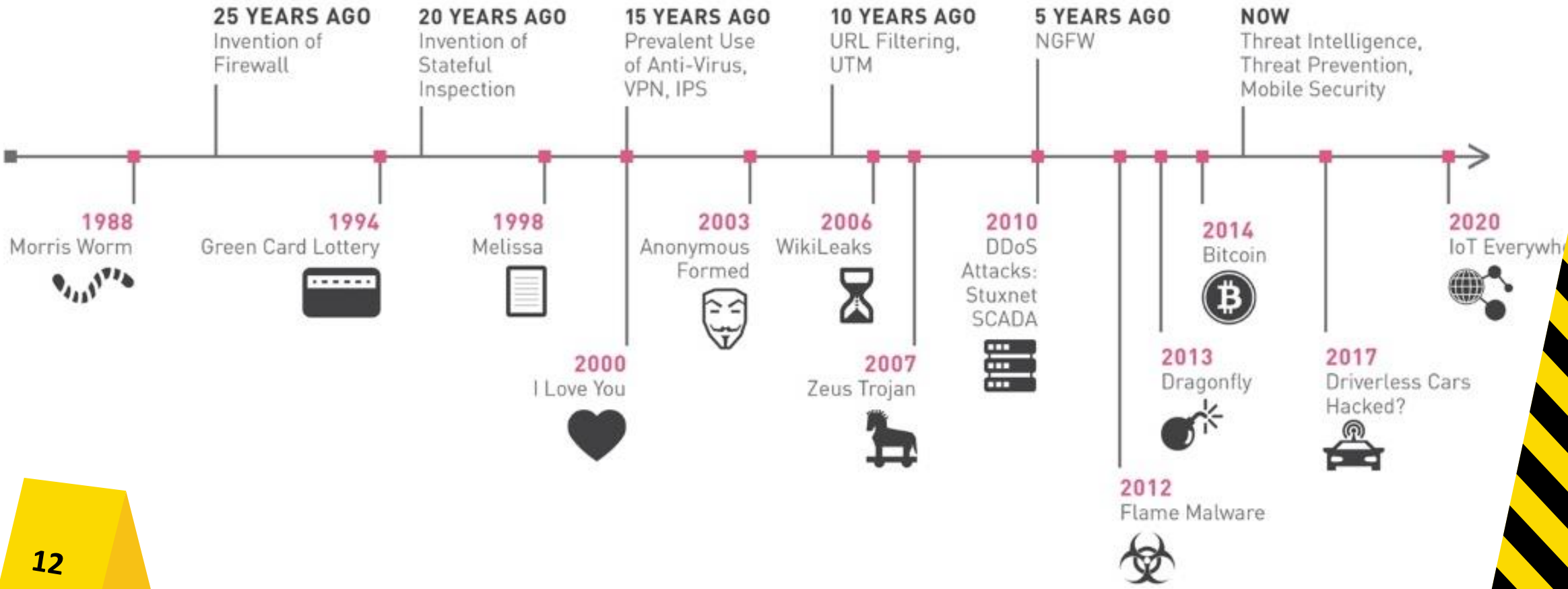
- Objetivo : Comunicaciones , obtención de información, propaganda, **radicalización** o financiación

5.Ciberterrorismo

- Ataque a Infraestructuras críticas y otros servicios

La evolución de las amenazas

La evolución de las amenazas



La evolución de las amenazas

Amenazas como servicio

La evolución de las amenazas

La seguridad Tradicional no es suficiente

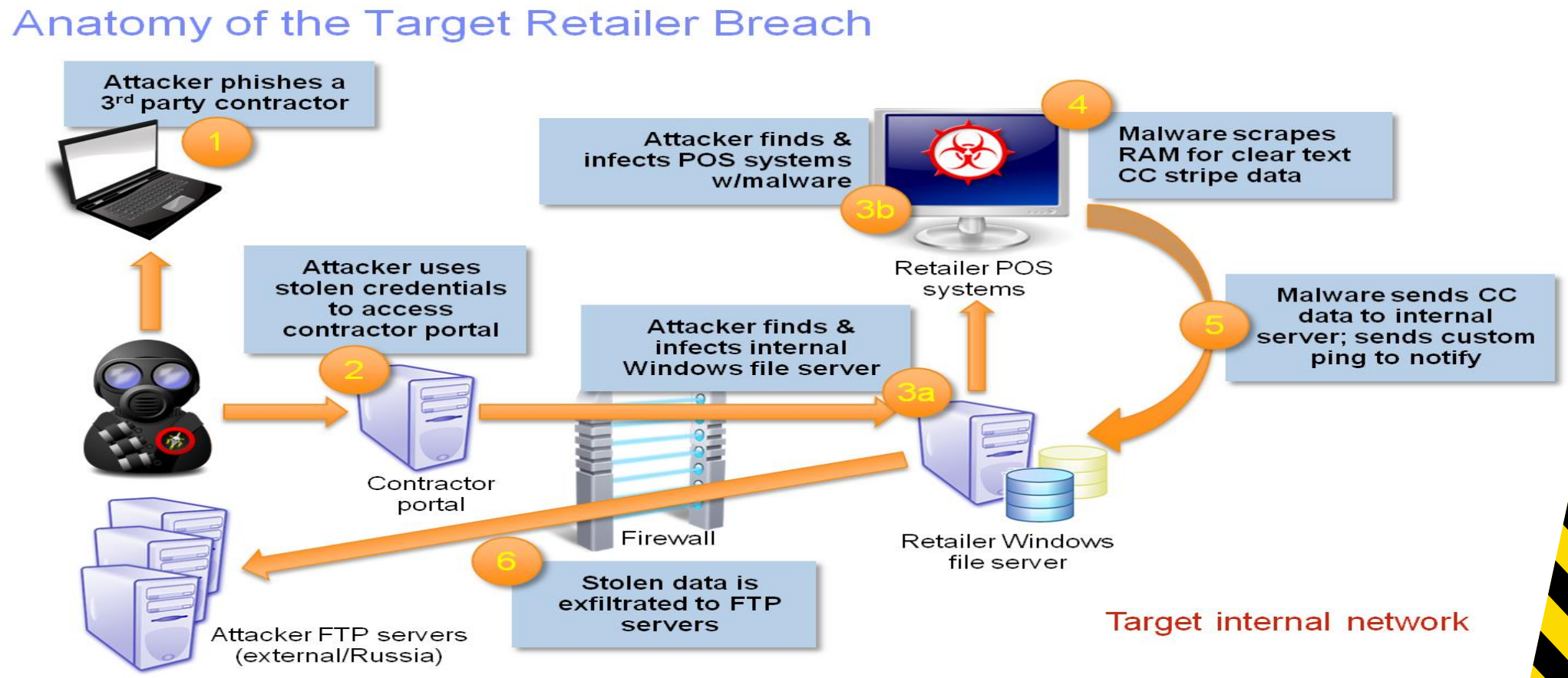
La evolución de las amenazas

La seguridad Tradicional no es suficiente

Permaneció oculto del 27 de Nov al 15 de Dic	10 a 20 veces más tarjetas disponibles en los mercados negros	40 millones de tarjetas comprometidas y la información personal de 70 millones de usuarios robada	110 millones de personas afectadas en total	140+ demandas contra Target
46% menos ingresos totales en el cuarto trimestre de 2013	13% cayó el precio de las acciones 6 meses después del ataque	3.8% menos ventas en el cuarto trimestre en comparación con 2012.	700 ofertas de trabajo no ocupadas	El CEO tuvo que presentar su renuncia
	us$170 millones de dólares invertidos para mitigar el ataque	us$1 billón de dólares será el costo total para Target según analistas	21.8 millones de tarjetas remitidas con un costo estimado de us$200 millones de dólares	

La evolución de las amenazas

La seguridad Tradicional no es suficiente



http://securityintelligence.com/wp-content/uploads/2014/01/TargetBreachAnatomy-v3.png

La evolución de las amenazas

La seguridad Tradicional no es suficiente

La evolución de las amenazas

Es imprescindible poder tomar decisiones ágiles y en tiempo real para combatir estas amenazas.

¿Qué recursos necesito para actuar eficazmente?

¿Supone esta amenaza un riesgo real para mis operaciones?

¿Como puede afectar lo que decida a otras áreas de mi organización?

¿Necesito un plan de contingencia con las medidas a aplicar?

¿Cuál podría ser el impacto real de esta amenaza?

¿A quién debo informar sobre esta amenaza?

¿Afectará esto a mi estrategia global?

¿Cuánto tiempo tengo para planificar una estrategia que me sirva?

¿Debo estar en contacto con mis aliados y competencia?

Threat intelligence

Muchas dudas?

No hay de que preocuparse pues tenemos un AS , en la materia para ayudarnos.

Threat intelligence

Resultados de Google para “threat intelligence” en los diferentes años

La inteligencia de amenazas se está convirtiendo rápidamente en una prioridad del negocio. Hay una conciencia general de la necesidad de "hacer" inteligencia de amenazas, y los vendedores están cayendo sobre sí mismos para ofrecer una gama diversa de productos de inteligencia amenaza.

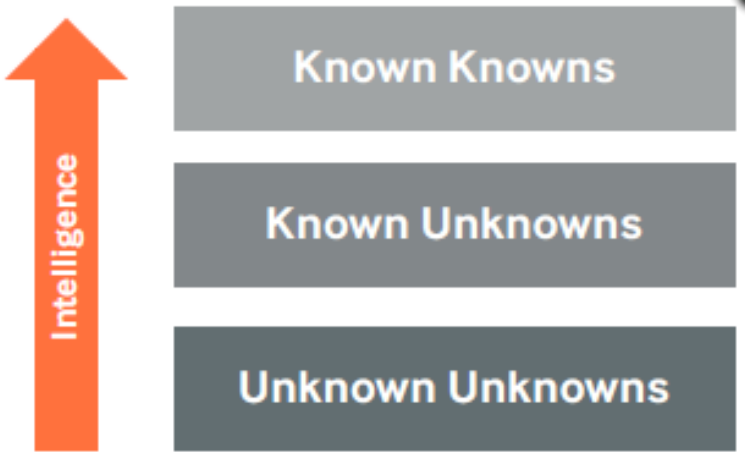
Threat intelligence

Objetivos de la inteligencia de amenazas

El objetivo es que la mayoría de las amenazas estén en la categoría **known knowns**

Mientras que algunas en la categoría **known unknowns**

Permitiendo que el menor numero de amenazas permanezcan en la categoría **unknowns unknowns**



Sin embargo, este es un reto considerable para la inteligencia tradicional y mas cuando se aplica a las nuevas amenazas cibernéticas.

Threat intelligence

El Análisis de Inteligencia es clave para la toma de decisiones, pero tiene que ser personalizado, oportuno y procesable

En mi experiencia, muchos enfoques para la generación y explotación de inteligencia no cumplen con los requisitos más importantes para facilitar la buena toma de decisiones:

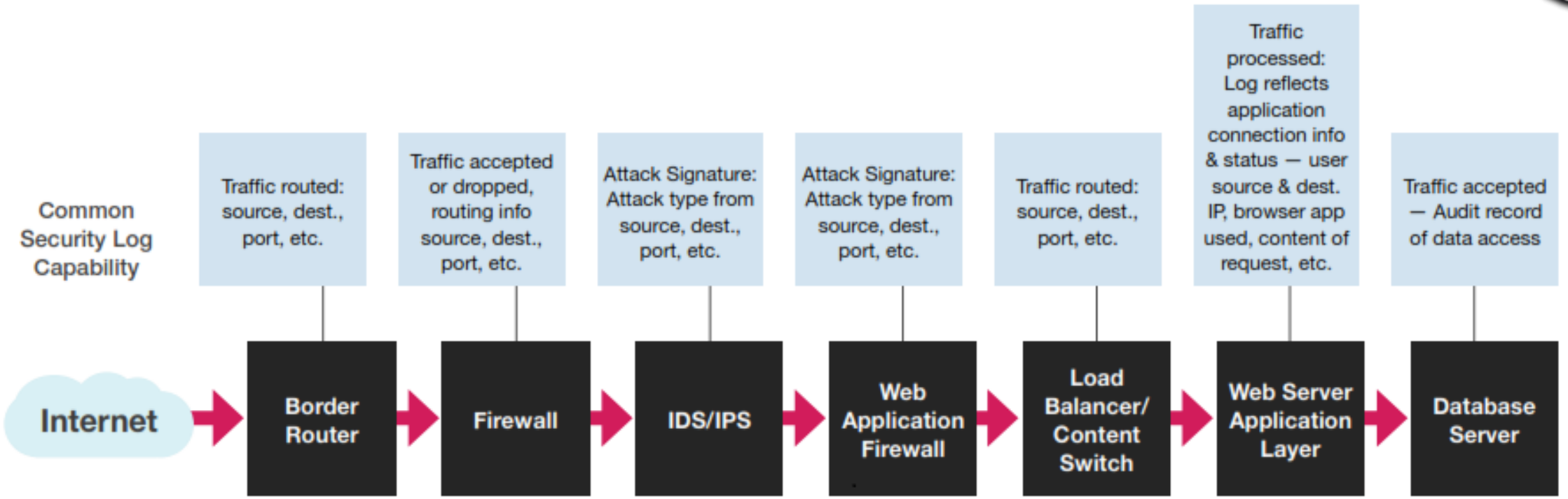
Debilidades	Ejemplos	Impactos	Buenas prácticas
Información obsoleta	Los metadatos no muestran información real	Los analistas de Inteligencia pierden tiempo buscando información inútil	Filtrado cuidadoso de los datos
Demasiados datos irrelevantes	Difícil procesar la información de modo integrado	Fallos al reconocer el escenario real.	Configuraciones adecuadas de listas blancas y listas negras
Gran cantidad de datos para procesar	No se detectan ataques de hacktivistas	La organización es atacada en su conjunto	Búsqueda proactiva para ese propósito
Insuficientes parámetros de seguridad	Ataque organizado utilizando los Social Media	La red de la organización es atacada y bloqueada	Medidas de seguridad dinámicas
Demasiada información nueva para decidir cuál es útil	Se reciben alertas inútiles que no contemplan todas las perspectivas	Desbordamiento de alertas de seguridad	Seguimiento y conocimiento de eventos específicos

Threat intelligence lifecycle

Un programa de inteligencia de amenazas efectivo (TI) tendrá una serie de áreas de enfoque.

La separación de inteligencia de amenazas con relación a las funciones específicas es más escalable, ya que es probable que su personal sea más hábil en aspectos específicos de la inteligencia de amenazas.

Threat intelligence lifecycle



Convertir los datos en inteligencia es una práctica que está lejos de ser fácil, pero se puede hacer, se requiere un proceso integral, robusto y en fases

Convertir los datos en inteligencia es una práctica que está lejos de ser fácil, pero se puede hacer, se requiere un proceso integral, robusto y en fases

Localizar información relevante en tiempo real es fundamental

Monitorización

¿Qué es lo más importante en esta fase?
Ejecutar una <u>búsqueda exhaustiva</u> de las fuentes externas de información, incluyendo la “deep web”

¿Cuáles son los retos para conseguirlo?	¿Cómo superar estos desafíos?
La localización de ciertos contenidos puede ser compleja	Usando diferentes soluciones para cada contexto y necesidad
Veracidad de la información	Colaboración integral entre unidades multidisciplinares
Información en constante cambio y evolución	Utilizando diferentes soluciones de software para cada recurso de información
Los datos están encapsulados en múltiples formatos	Búsqueda de otros sistemas para almacenaje y gestión de la documentación

Al igual que los análisis automáticos son esenciales, el elemento humano también es indispensable

Análisis

¿Qué es lo más importante en esta fase?
El análisis de Inteligencia <u>suministra información de valor</u> para la toma de decisiones

¿Cuáles son los retos para conseguirlo?	¿Cómo superar estos desafíos?
Como procesar/modelar los datos	Diseñando herramientas para unidades específicas
Un mismo riesgo tiene diferentes significados para la toma de decisiones	Escalar la amenaza recibida a la persona adecuada para su valoración
Como extrapolar los resultados a la organización global desde información tan específica	Establecer un proceso de colaboración estrecha con todas las partes
Qué medidas internas tomar después de recibir el análisis (por ejemplo, alertas)	Incorporación de procesos /reacciones internas a las amenazas alineadas con el análisis recibido

Los datos deben gestionarse adecuadamente para dirigirlos hacia las necesidades requeridas

Gestión

¿Qué es lo más importante en esta fase?
Filtrar y organizar la información en formatos cómodos para la consulta

¿Cuáles son los retos para conseguirlo?	¿Cómo superar estos desafíos?
Incomprensión de las necesidades de los distintos stakeholders	Trabajando estrechamente para una compresión mutua
Decidir qué es relevante	Proporcionar los indicadores adecuados a las personas adecuadas
Información en tiempo	Comprensión eficiente de las acciones en fuentes abiertas
Cómo justificar la calidad de la información	Comprensión eficiente de la estructura y trabajos en la organización

Sistema de información eficaz y eficiente que suministre información sobre amenazas y oportunidades

Informes

¿Qué es lo más importante en esta fase?	
Conseguir el <u>mensaje necesario</u> para los que toman las decisiones	
¿Cuáles son los retos para conseguirlo?	**¿Cómo superar estos desafíos?**
Los analistas necesitan tiempo para evaluar toda la información	Diseño de herramientas que ayuden a priorizar
Cómo conseguir que la información sea confiable	Inclusión de analistas de Inteligencia especialistas en todas las partes del proceso
Cómo conseguir que la información sea útil y vaya directa al grano	Desarrollar heramientas de visualización

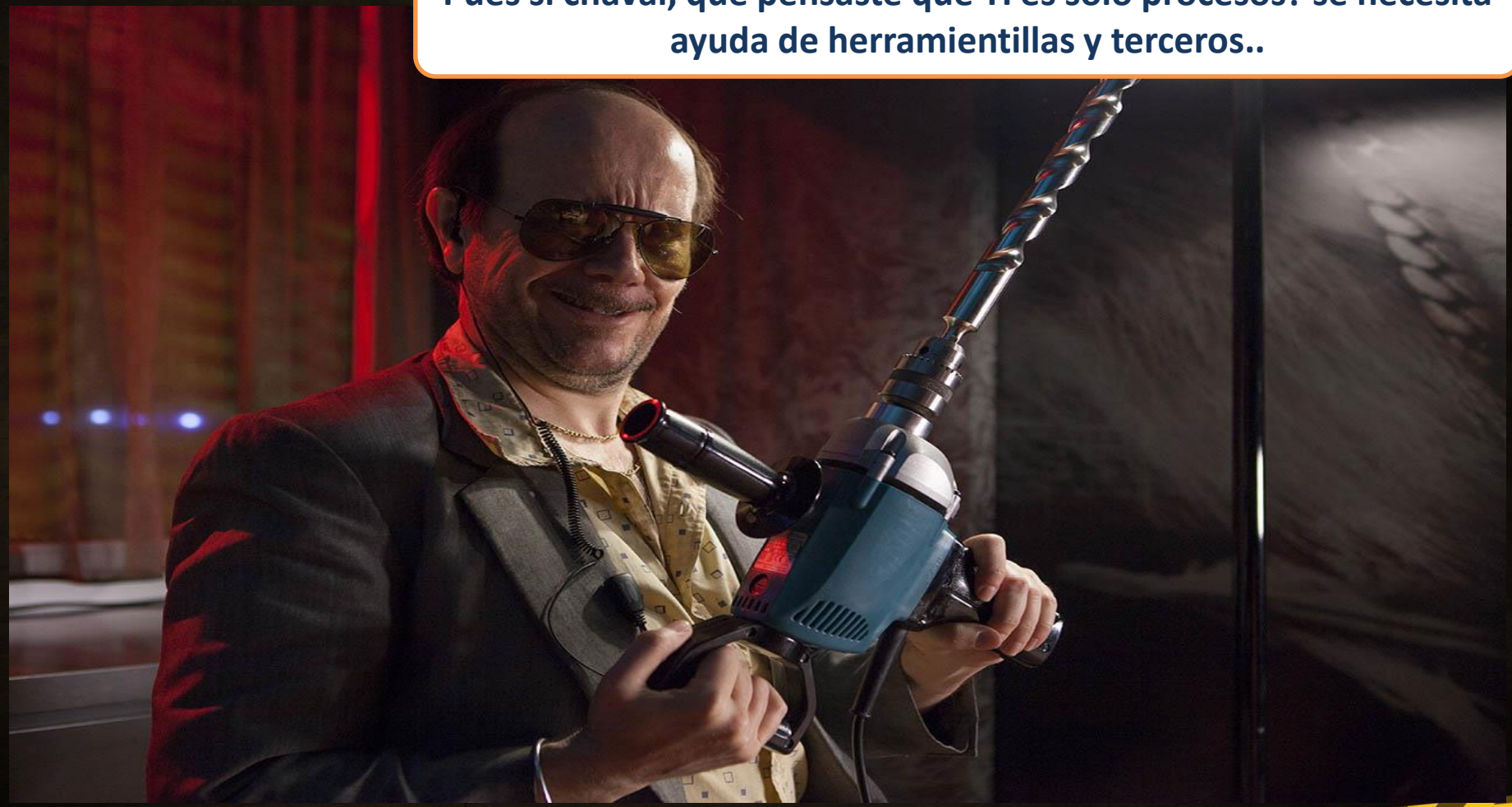
Para explotar con éxito la inteligencia se requiere de una profunda alineación e integración de los procesos internos

Explotación

¿Qué es lo más importante en esta fase?	
Convertir la información en <u>información de valor</u>	
¿Cuáles son los retos para conseguirlo?	**¿Cómo superar estos desafíos?**
Cómo educar a las unidades de Inteligencia	Procesos de comunicación interna adecuados
Cómo gestionar las diferentes necesidades	Comprendiendo los “puntos negros”
Cómo involucrar a los que toman las decisiones en todo el proceso	Mostrando resultados tangibles que les afecten
Cómo automatizar ciertas decisiones cuando ser recibe el aviso	Diseñando procesos robustos

Threat Intelligence Plataform

Pues si chaval, que pensaste que TI es solo procesos? se necesita ayuda de herramientillas y terceros..



Threat Intelligence Plataform

Pues si chaval, que pensaste que TI es solo procesos? se necesita ayuda de herramientillas y terceros..

Intelligence Sources

- Commercial
- Open Source
- Communities
- Sharing
- Internal

Actionable Integrations

- SIEM
- IPS/IDS, Firewalls
- Gateways
- Endpoint, Response
- DLP, NAV

Threat intelligence Team

Pero no se vive solo de procesos y herramientas chaval, vas a tener que buscar a los mejores.

Threat intelligence Team

Hay que entrenarlos en varios aspectos (Seguridad o no seguridad).

Threat intelligence Team

Hay que entrenarlos en varios aspectos (Seguridad o no seguridad).

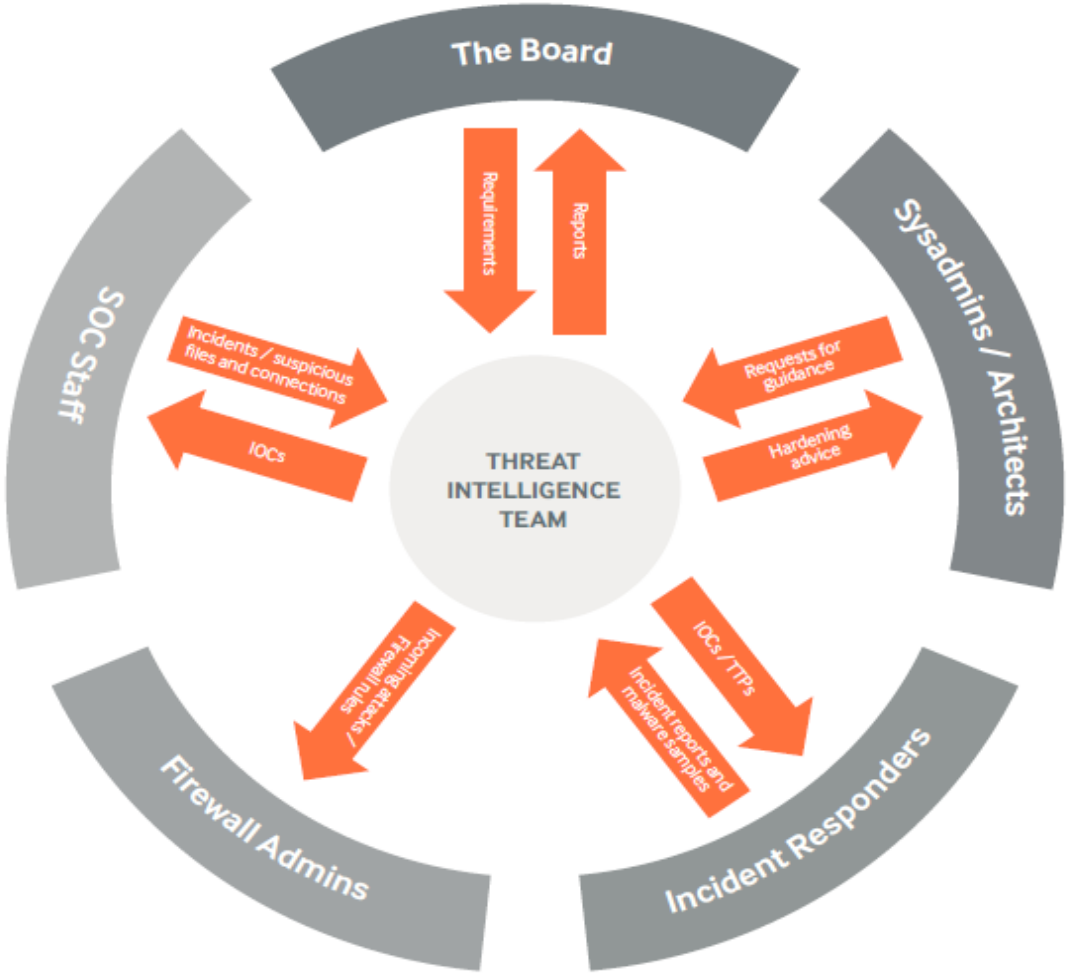
Threat intelligence Team

Hay que entrenarlos en varios aspectos (Seguridad o no seguridad).

- Identificar las necesidades.
- Usar los distintos frameworks y practicas.
- Identificar los recursos.
- Entender su organización de datos y entorno.
- Recolectar datos.
- Analizar datos.
- Colaborar.
- Tomar acción.
- Repetir.
- Automatizar.
- Compartir conocimiento.

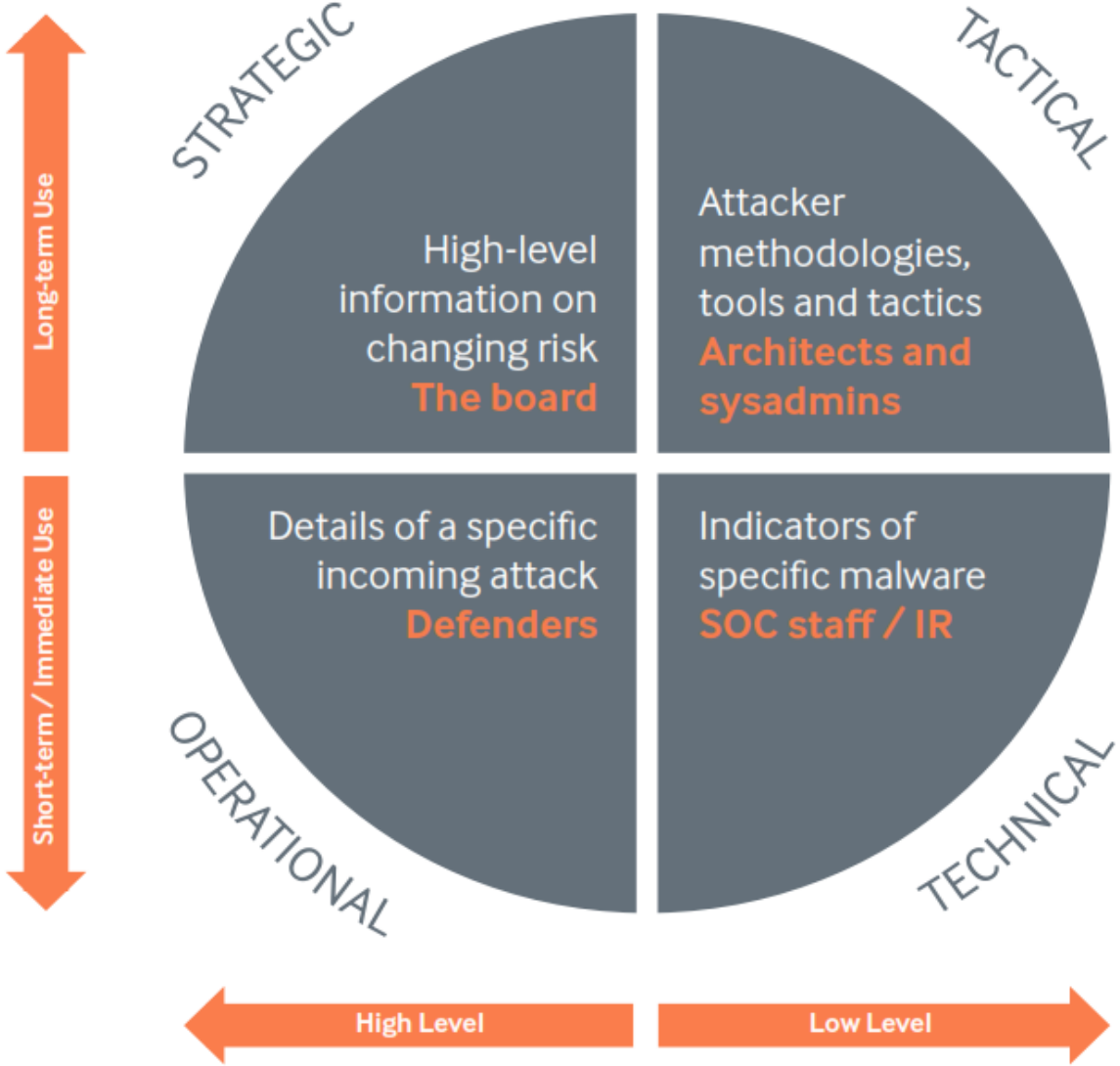
Threat intelligence Team

Completando los paso anteriores lograremos formar nuestro propio “Threat intelligence Team”



Threat Intelligence Plan

Tenéis un equipo preparado, tienes procesos y herramientas ahora necesitas un plan.



Threat Intelligence Plan

Strategic

- Trabajar con los seniority mas altos para identificar las amenazas informáticas actuales.
- Servir de enlace con las organizaciones en el mismo sector de la industria para determinar si hay otras amenazas que su organización aún no ha reconocido.
- Con la ayuda de la alta dirección, crear una lista de todos los actores (empresas, grupos de campaña, países, etc.) que se beneficiarían de acceso a sus datos sensibles - o de su incapacidad para funcionar con eficacia.

Operational

- Prepare una lista de nombres y datos de contacto (incluyendo detalles de fuera de horas) para ponerse en contacto con las personas por si su organización recibió el aviso de un ataque inminente.
- Si se están siendo victimas de ataques de DDoS, use Google para buscar el nombre de su organización, pero limitado con aquellas fechas que inmediatamente preceden a los ataques.
- El objetivo es determinar si la cobertura negativa está dando lugar a los ataques. Si no es así, tratar de identificar otros factores que podrían estar provocando los ataques

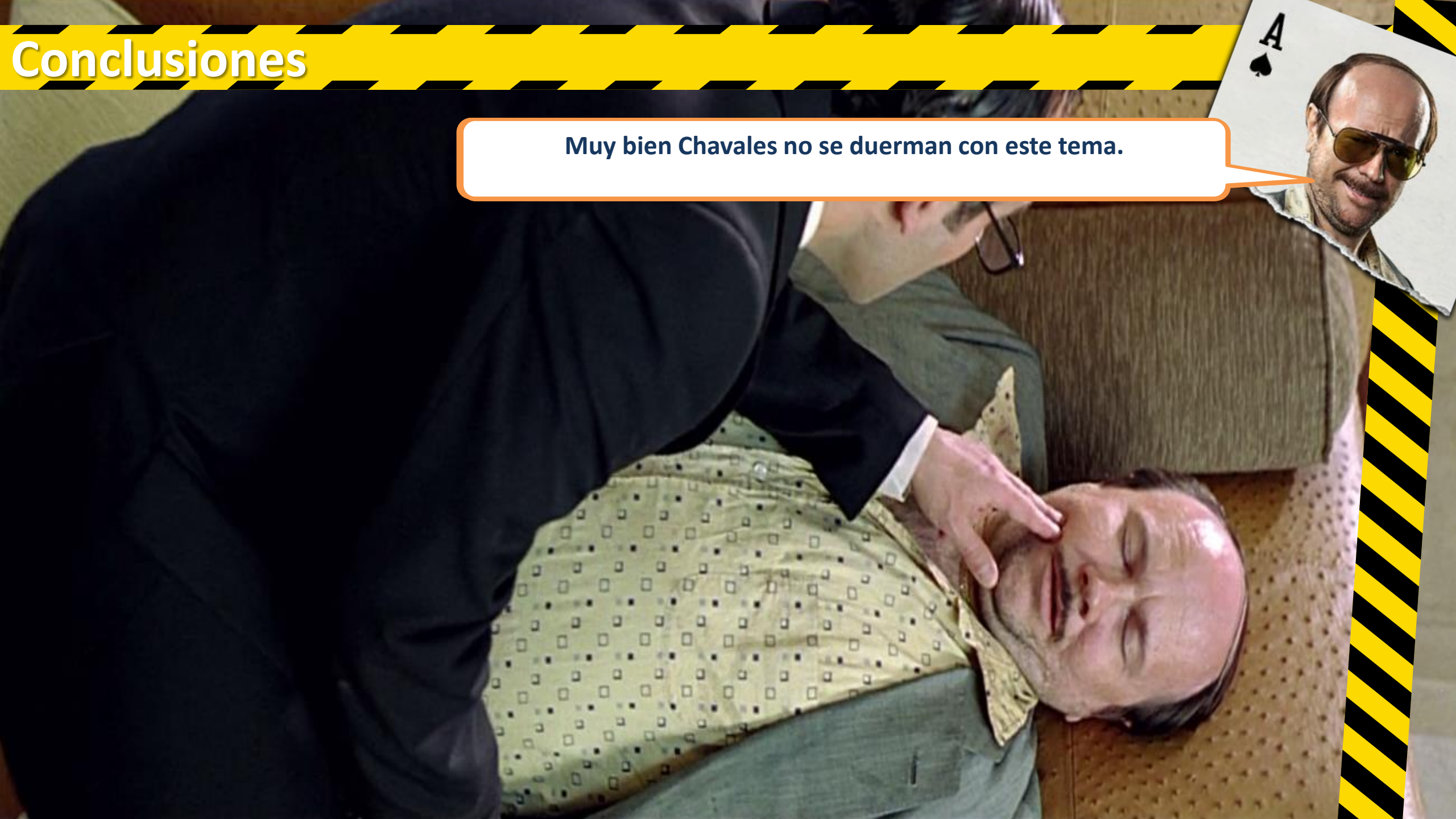
Tactical

- Identificar las organizaciones que están produciendo informes de respuesta a incidentes y white papers o grupos sobre amenazas.
- Establecer alertas de RSS Feed sobre nuevos documentos publicados por estas organizaciones.
- Cuando se da a conocer un documento, extraer del mismo indicadores tácticos y claves, como el mecanismo inicial de entrada a la red, herramientas o técnicas utilizadas para moverse por la red, y los mecanismos utilizados para la exfiltración.
- Llevar a cabo un ejercicio teórico para determinar la susceptibilidad de su organización a esas técnicas, y los cambios que se necesitan para reducir la susceptibilidad a estas técnicas.
- Consulte a arquitectos y administradores de sistemas para identificar y planificar una actualización de tecnologías, ambientes o sistemas clave.

Technical

- Obtener acceso a la listas por ejemplo CISP o Una al Día u otros Feeds libres, y colocar las direcciones IP malintencionadas en una lista de "alerta" en el firewall primario o IDS.
- Revise periódicamente para determinar si las conexiones salientes se realizan desde adentro de su organización y - en caso afirmativo - iniciar la respuesta a incidentes.

Conclusiones



Conclusiones

Conclusiones

Conclusiones

Pónganse en el lugar del otro para entender sus necesidades y sus problemas

Conclusiones

Conclusiones

https://ar.linkedin.com/in/lucianomoreiradacruz

lucianomoreira9@hotmail.com

@luciano_m_cruz

lucianomoreiradacruz

https://www.linkedin.com/in/lrosso/es

leonardo.federico.rosso@gmail.com

leonardo.rosso

Gracias!

Referencias: http://www.threatconnect.com/