INVESTIGACIONES DIGITALES COMPLEJAS EN ENTORNOS FINANCIEROS

Jess Garcia - @j3ssgarcia

$whoami

Jess Garcia
@j3ssgarcia

- Fundador y CEO de One eSecurity, una compañía global de Digital Forensics and Incident Response (DFIR) (~15 años)
- Líder del proyecto DS4N6.
  Visita: **www.ds4n6.io**
- Instructor Senior en el Instituto SANS (~20 años)

AGENDA

- PANORAMA DE AMENAZAS
- METODOLOGÍA Y CASO DE USO
- EXPERIENCIAS Y MEJORAS
- Q&A

PANORAMA
DE AMENAZAS

THREAT LANDSCAPE - ACTORS

ORGANIZACIONES
CRIMINALES

ACTORES
GUBERNAMENTALES

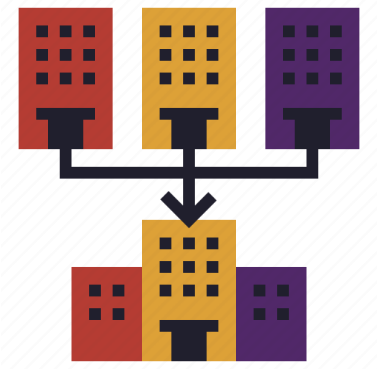
IDEOLOGICOS
O HACKTIVISMO

LABORALES
O PERSONALES

THREAT LANDSCAPE - CASOS

Exfiltración o Fraude

Insiders



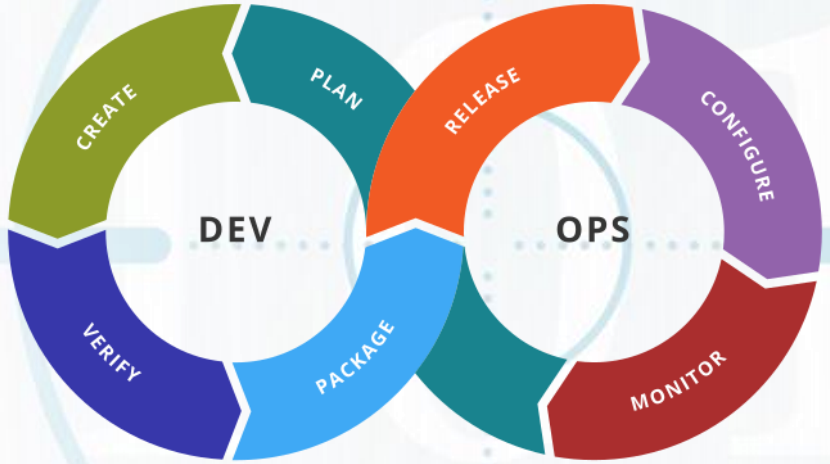
Terceros, fusiones y adquisiciones

Cibercrimen

THREAT LANDSCAPE – EXFILTRACION O FRAUDE

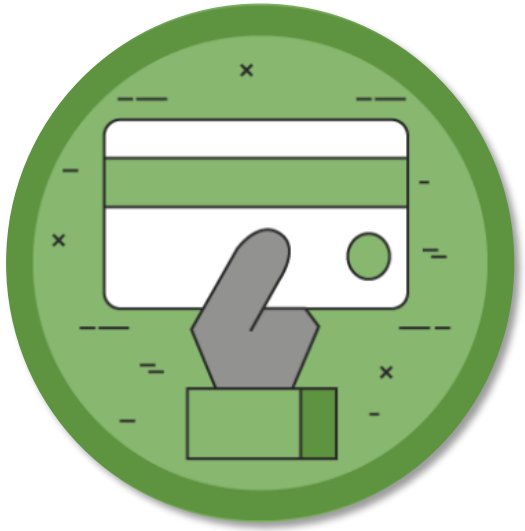
Personal interno

Sistemas mal configurados



Fallos en software por malas prácticas

THREAT LANDSCAPE - INSIDERS

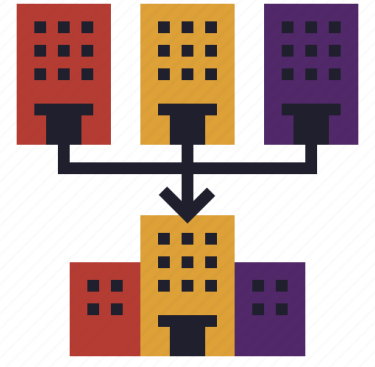


Robo de tarjetas

Ataques de falsa bandera

Extorsión

THREAT LANDSCAPE - TERCEROS



Empresas adquiridas

Proveedor de servicios

THREAT LANDSCAPE – CIBERCRIMEN

centro de cooperación interbancaria

Hackers "bandidos revolution team" siguen trabajando.

Nación viernes 14 de agosto de 2020 - 00:55

Por Martha Bautista

Una banda de ciber ladrones fueron capturados en León, Guanajuato en mayo de 2
recluidos en varios penales del Estado de México; su líder Héctor Ortiz solares "el Hr" y
Lemus alias "el Lemus" se encuentran en el penal de Tenango del Valle; sin embargo, aún
dejado de trabajar, ya que se sabe que los abogados que llevan su defensa, han logr
celulares hasta computadoras, para que sigan trabajando.
No todos los integrantes de esta organización fueron detenidos, ahora existe una

Bank Security
@Bank_Security

Revil Ransomware hit BancoEstado Bank in Chile

BancoEstado @BancoEstado · 6 Sep
Información de Prensa
Show this thread

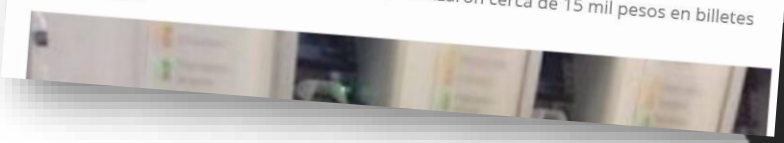
BancoEstado

INFORMACIÓN DE PRENSA

Durante este fin de semana, BancoEstado detectó en sus sistemas operativos un software malicioso. Apenas fue descubierto este problema, nuestros equipos de operaciones y de ciberseguridad se desplegaron para localizar, contener y solucionar esta situación.

¡Dinero, dinero, dinero! Falla en cajero automático provoca que "llueva" billetes

Al momento del arribo de los uniformados, localizaron cerca de 15 mil pesos en billetes de 500 pesos



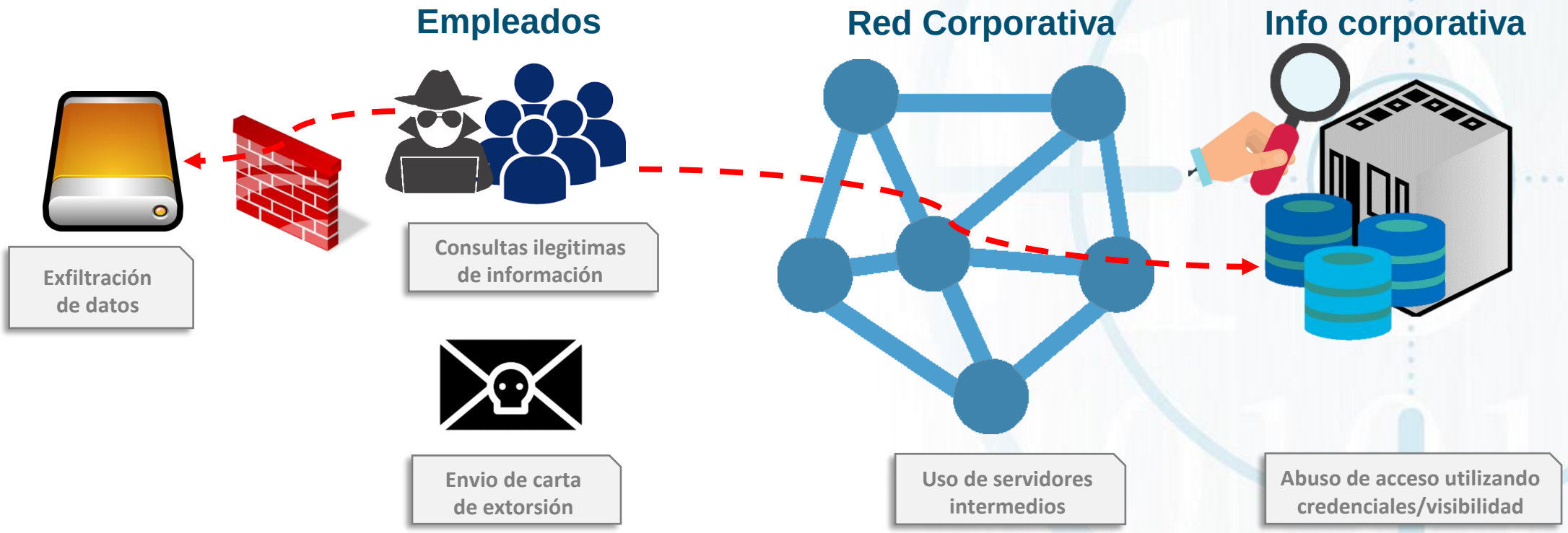
THREAT LANDSCAPE – CIBERCRIMEN

ATAQUES DIRIGIDOS

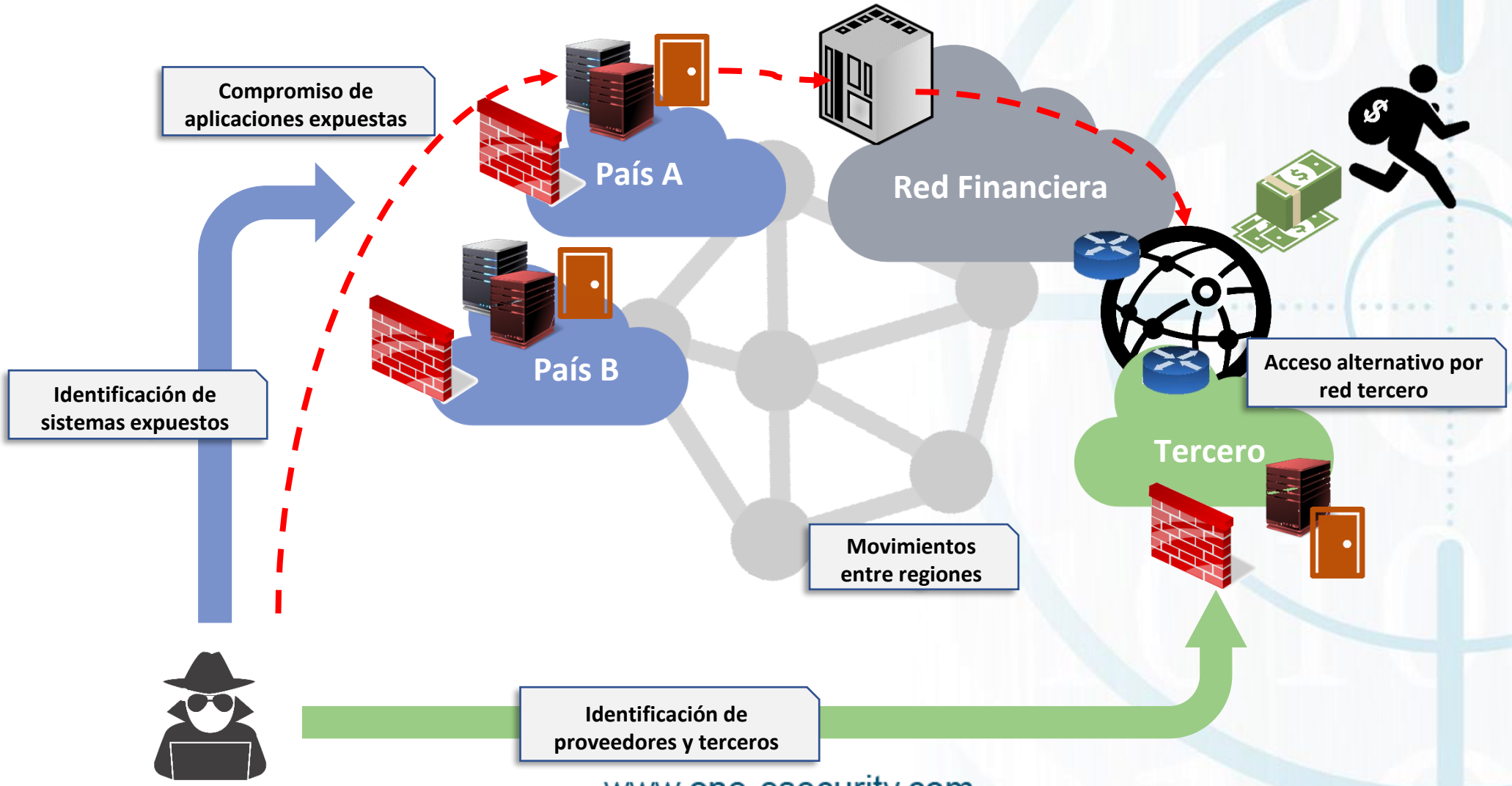
ATAQUES FORTUITOS

PASTEBIN

THREAT LANDSCAPE – FUGAS DE DATOS



THREAT LANDSCAPE – ABUSO ATMs



METODOLOGÍA
Y CASO DE USO

METODOLOGIA - CAPACIDADES

Equipo de respuesta:

- Reduce el coste por brecha de seguridad.

Prueba de planes de respuesta:

- Reduce el tiempo de gestión por brecha de seguridad.

Planes de concienciación y ciberejercicios.

- Reduce el riesgo por brecha de seguridad

Servicios Proactivos.

- Reduce el tiempo de detección de una brecha de seguridad

METODOLOGIA - CAPACIDADES

Protección

- Gestión de Identidades Privilegiadas
- Microsegmentación ágil
- Herramientas de protección activos críticos (checkers/whitelisting)

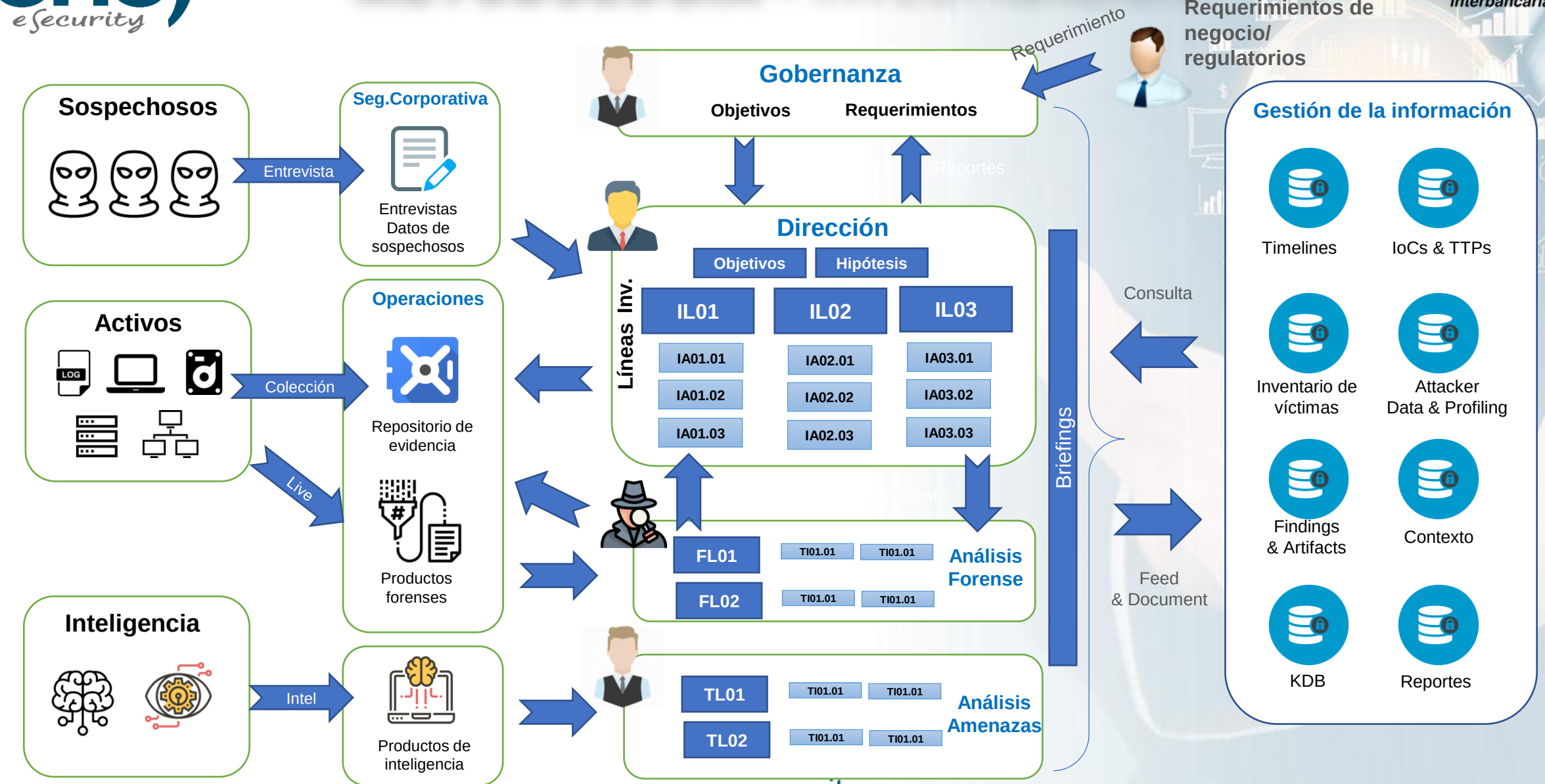
Detección

- Lagos de datos y plataformas de correlación de eventos
- Plataformas Avanzadas de Detección y Respuesta
- Caza de amenazas (Threat Hunting & Compromise Assessment)
- Detección de anomalías en sistemas y tráfico de red

Respuesta

- Plataformas forenses corporativas

METODOLOGIA - INVESTIGACIÓN



METODOLOGIA - INVESTIGACIÓN

Analysis of competing hypotheses (ACH)

Evidence	Evidence Type	Credibility	Relevance	H1	**H2**	H3
				1	**9**	3
Usage of Equation Group Exploit	Assumption	Low	High	+	**+**	-
Unpatched servers	Assesment	High	Medium	+	**+**	-
Ransomware Note	Artifact	Low	Low	+	**+**	-
Remote Acces off hours	Artifact	Low	Medium	--	**+**	+
Remote Acces off hours	Log	High	High	--	**+**	+
Creation dump files	Artifact	High	High	-	**++**	+
Usage of third admin account	Artifact	High	High	+	**-**	+
Hacking Tools in the laptop	Artifact	High	Medium	+	**++**	+
Bad feeling with the Manager	Assumption	Low	Medium	+	**+**	+

H1 External Threat Actor
H2 Insider from IT + External Threat Actor
H3 Insider from IT

METODOLOGIA – LINEA TEMPORAL

Contención
Lecciones aprendidas
Traspaso de la investigación

1-3 semanas

Threat Hunting

Hunting/monitorización
Traspaso operacional

1-3 Meses

Investigación Forense

Auditoría, lecciones aprendidas
Planes de mejora

1-6 Meses

Aseguradoras

Sanciones y
aprobación de ciberseguros

2-3 Meses

Arrestos potenciales

Fase Judicial

2-N Años

METODOLOGIA – EVOLUCION EIR

METODOLOGIA – ESTADÍSTICAS

ESTADISTICAS EJEMPLO

+2.500.000 Host analizados anualmente

+120.000 Falsos positivos anuales

+150 Gb Netflow diario

+8.000 Assets diarios

La Prevención es **IDEAL**

La Deteción es **OBLIGATORIA**

La Detección sin respuesta es **INSERVIBLE**

EXPERIENCIAS
Y MEJORAS

MEJORAS

Contrata un retainer

Entrena a tu equipo a lo grande

Conoce tu preparación ante incidentes

Conoce tus capacidades de visualización y detección

Mejora tus capacidades remotas

Mantén buenos periodos de retención

Crea un plan de recuperación ante desastres

Adopta un enfoque proactivo

All the details about this talk:

one-esecurity.com/cci21

INVESTIGACIONES DIGITALES COMPLEJAS EN ENTORNOS FINANCIEROS

Jess Garcia
@j3ssgarcia

Thanks!

one eSecurity

www one-esecurity.com

One_eSecurity

One eSecurity

www.one-esecurity.com | www.ds4n6.io