CASOS PRÁCTICOS DE INVESTIGACIÓN FORENSE

XXIX Congreso Nacional

Jess García

email: jess@one-esecurity.com

Sígueme en twitter: @j3ssgarcia

(one) eSecurity

(one) eSecurity

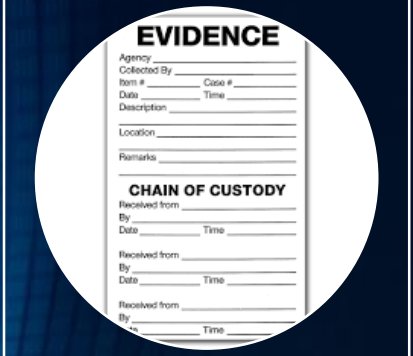
Investigadores Forenses Digitales

- Incident Response, Digital Forensics & Investigations (DFIR) Service
- DFIR Emergency Onsite Service
- DFIR Interim & Support Service
- DFIR Assessment & Dry-Run Exercises
- DFIR Training and Skills Development Service
- DFIR Up-to-Date Service
- DFIR Infrastructure Service
- CyberThreat Intelligence (CTI) Infrastructure Service
- FaaS / SKaaS – Forensics as a Service / SKY as a Service

(one) eSecurity

CIBERSEGUROS

CIBERSEGURIDAD PARA CIBERSEGUROS



Litigio

- Triage
- Análisis
- Preservación
- Adquisición
- Evidencia física

Investigación

- APT
- Fraude
- Grandes incidentes
- Empleados
- Análisis
- Fuga información
- Perfilado
- eDiscovery

Ciberseguridad

- Threat analysis
- Threat hunting
- Respuesta incidentes
- Cyber threat intelligence
- Restablecimiento

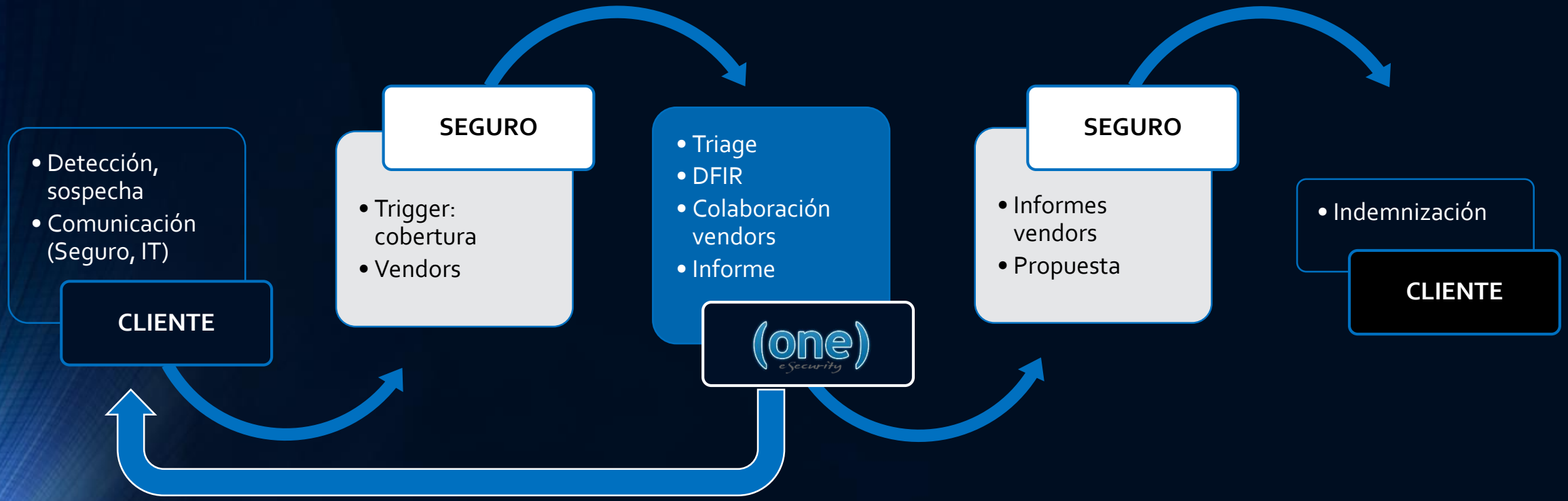
Equipo técnico → **+10 años de experiencia cualificada**

Herramientas → **+Procesos automatizados**
- Tiempos de respuesta

Gestión → **24/7**
KPIs
SLAs

CIBERSEGUROS

TIMELINE: CIBERINCIDENTE



CIBERSEGUROS

CASOS REALES

NUESTROS RESULTADOS

(one) eSecurity

CIBERSEGUROS

Case A: INSIDER FRAUD

VICTIMA: **Sector Retail**

TIPO INCIDENTE: **Fuga de información**: venta de miles de tarjetas y datos de clientes en Deep Web → GDPR!!!

RIESGO:

- Desconocimiento de clientes afectados → Sanciones: GDPR, NIS, recl.3os
- Impacto en imagen corporativa → Reputacional
- Pérdida económica debido al fraude → Lucro cesante

OBJETIVOS:

- ¿Cómo ha ocurrido la fuga?
- Minimizar impacto (fraude/imagen)
- ¿Responsable?

CIBERSEGUROS

Case A: INSIDER FRAUD

INVESTIGACIÓN:

DURACIÓN:
4 meses

RECURSOS:
- 4 ONE
- 2 eq.Audit.
- 3 eq.ciberseg.

Análisis flujo transaccional y aplicativo → Seguimiento ventas / movimientos perfil en deep web → Identificación de información filtrada
- Capacidad de detección y bloqueo de tarjetas vendidas

Identificación de metodología de exfiltración → Identificación de interno culpable de la fuga y venta → Colaboración con fuerzas del orden
- Bloqueo de mecanismo de fuga de datos
- Detención

CIBERSEGUROS

Case B: MALWARE

VICTIMA: **Sector energético**

TIPO INCIDENTE: **Malware** destruye +30.000 equipos cliente (85% del HW)
(Generación no se ve afectada)

RIESGO:

- Tecnológicamente la empresa deja de funcionar → Lucro cesante
- Caos en la organización → Reputacional, RRHH
- Empresa no preparada para este tipo de incidentes → DM, Mercado

OBJETIVOS:

- ¿Qué ha pasado?
- Identificación de riesgos (además de la destrucción de equipos, ¿hay algo más?)
- ¿Responsable?
- ¿Motivaciones?

CIBERSEGUROS

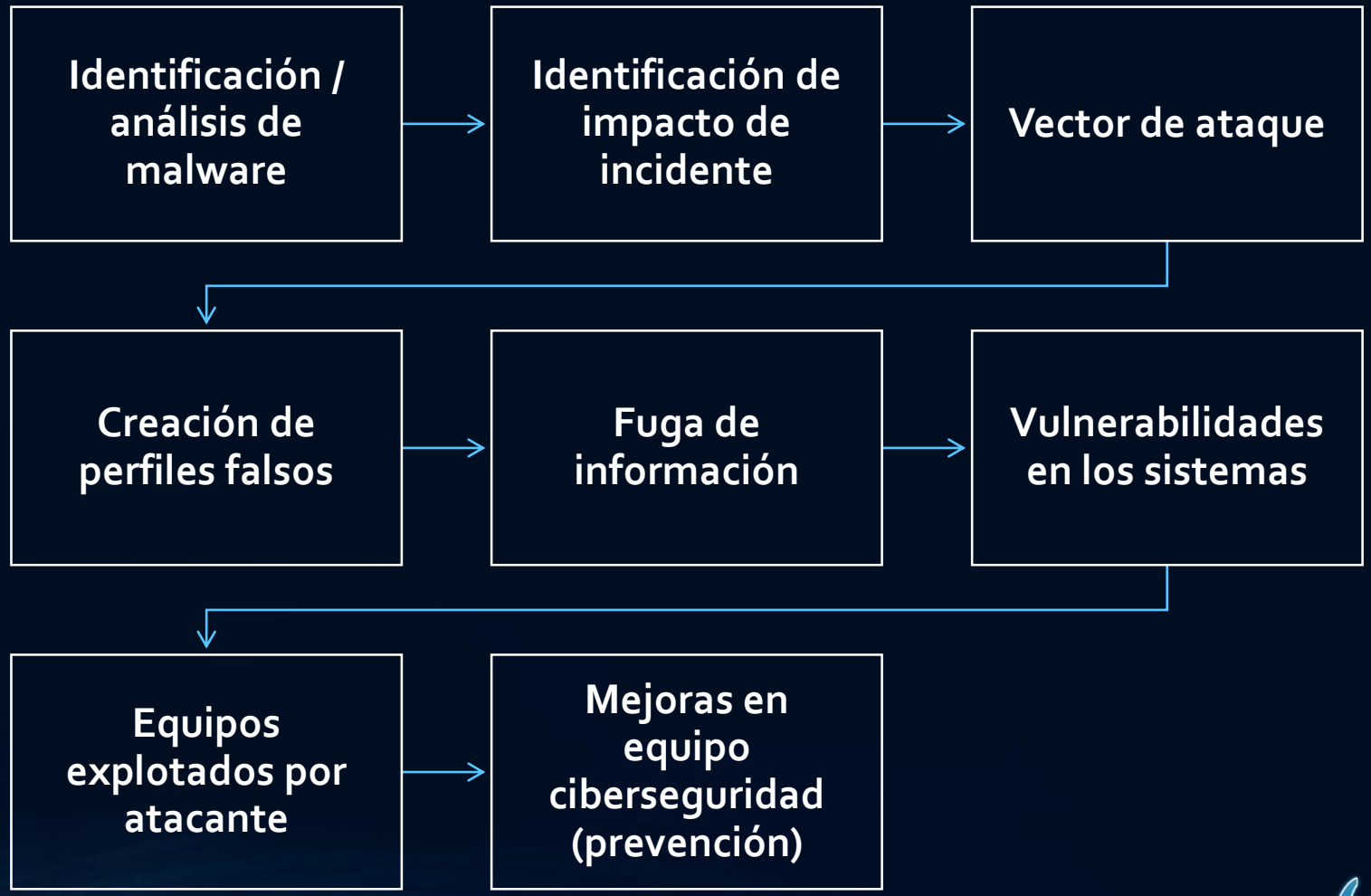
Case B: MALWARE

INVESTIGACIÓN:

DURACIÓN:
6 meses

RECURSOS:
- 7 ONE
- 6 forenses colab.
- 3 eq.ciberseg.

Cliente desconectado completamente de internet



CIBERSEGUROS

Case C: ATM JACKPOTTING

VICTIMA: **Sector financiero**

TIPO INCIDENTE: **Fraude en ATM**: extracción de +5M € en cajeros de todo el país

RIESGOS:

- Desconocimiento de por qué ATM daba dinero "gratis" → DM
- Pérdida económica debido al fraude → Lucro cesante

OBJETIVOS:

- Minimizar impacto fraude
- ¿Cómo ha ocurrido?
- ¿Personal interno involucrado?

CIBERSEGUROS

Case C: ATM JACKPOTTING

INVESTIGACIÓN:

DURACIÓN:
3 meses

RECURSOS:
- 3 ONE
- 4 eq.ciberseg.