



- Threat Hunting -

There is more than meets the eye

Miguel Díaz – Security Researcher

31/oct

~\$ whoami

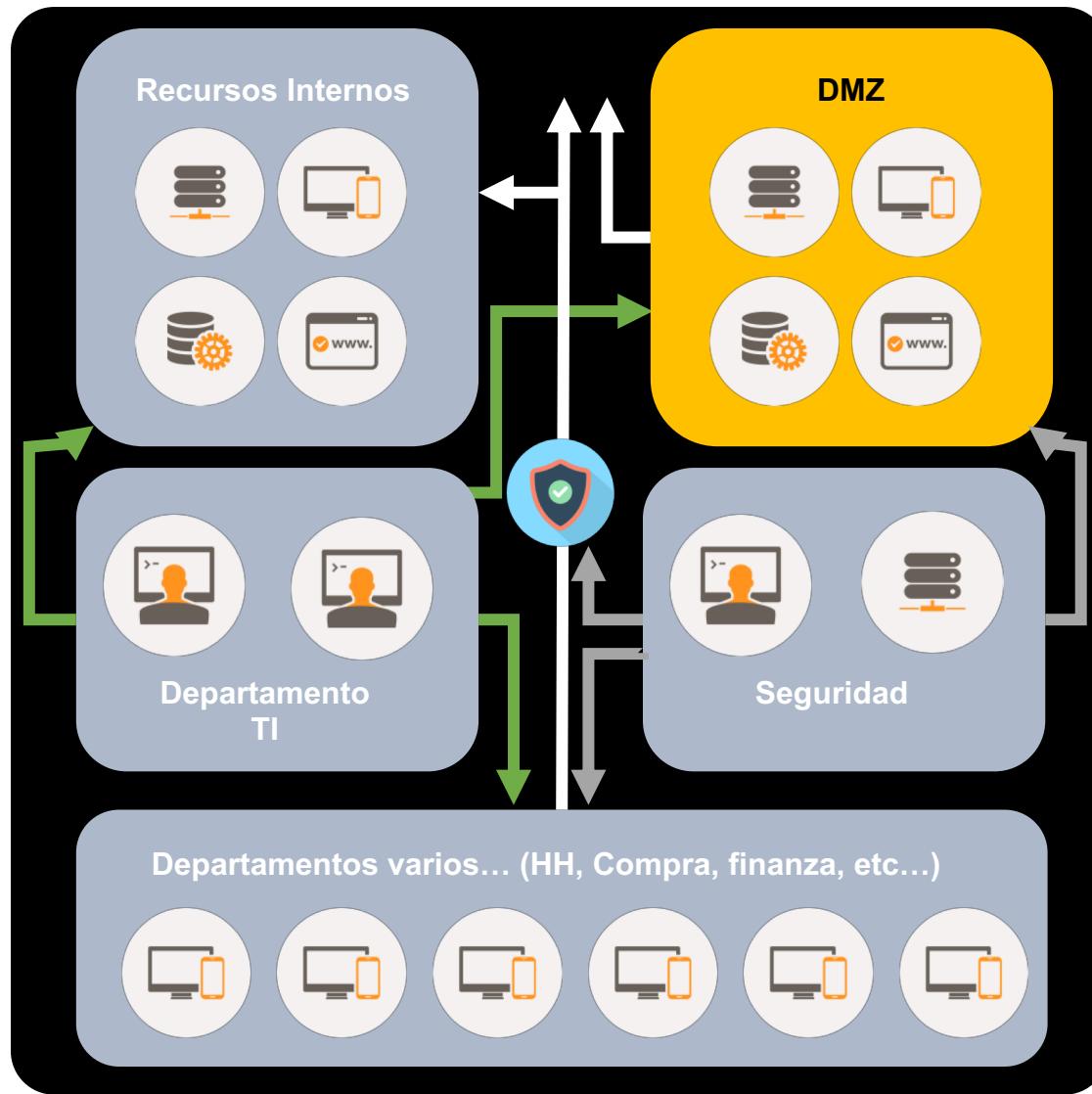
- Investigador de Ciberamenazas
- Consultor en Ciberseguridad
- Líder equipo de Ciberinteligencia en ENTEL
- Certificado CEHv8
- Entrenamiento en Threat Hunting Avanzado (FOR508)
- Habilidades:
 - Hacker Ético
 - First-responder
 - Ex-desarrollador de software

@mdiazcl



**Hablemos del panorama de
seguridad**

Una sistema de seguridad (simplificado)



Dispositivos de seguridad:

- 📦 IPS/IDS
- 📦 Network profilers
- 📦 Firewalls
- 📦 Endpoints (Consolas)
- 📦 SIEM
- 📦 Antispam
- 📦 Filtro de Contenido
- 📦 WAF
- 📦 Gestor de Identidades
- 📦 DLP (???)
- 📦 ACL
- (y cuanta caja nos venden)

Hoy en día no es posible esperar a que las cajas nos alerten algo.

Qué es lo que se escucha normalmente...

Operaciones

“El IPS ha bloqueado 6.780 firmas de intrusos”

“El AntiSPAM ha bloqueado satisfactoriamente una campaña de fraude”

“Anti-Malware ha bloqueado 3.405 virus este mes”

Auditoria

“Somos ISO 27001”

“Contamos con PCI Compliance”

“Cumplimos la norma NCH 498123”

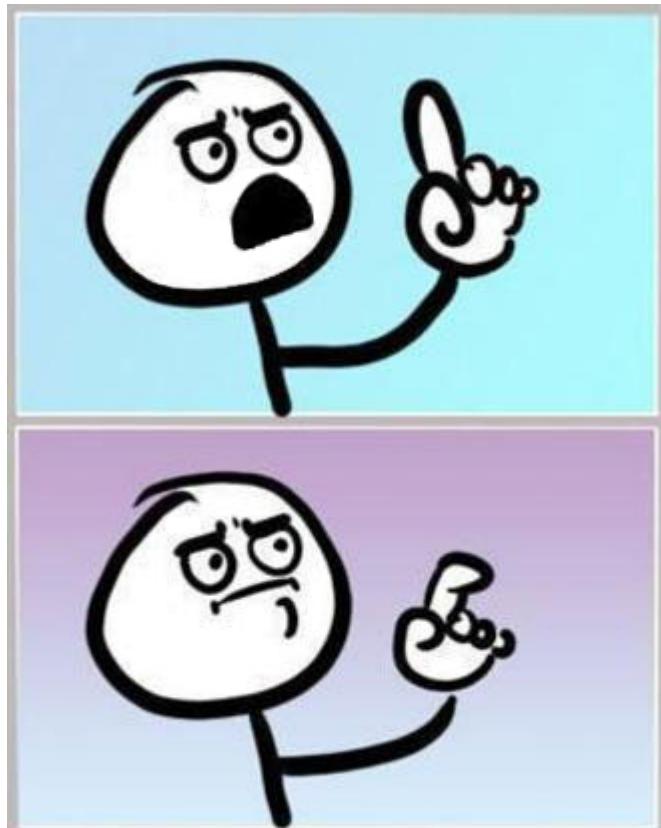
Antecedentes



- Target - 2014
 - Gestión de Alarmas
 - Análisis de comportamiento
 - Credenciales comprometidas (Phishing)
 - Compliance PCI
- Equifax – 2017
 - No solo lo hackearon una, si no que múltiples veces
 - Explotación de una vulnerabilidad (con parche disponible, struts2)
- Deloitte – 2017
 - Clientes afectados: Gobierno USA, Naciones Unidas y Multinacionales
 - Robo de credenciales
 - Falta de controles
- Incidentes de este año
 - Bancos
 - Redes SCADA
 - Filtraciones de data

Conclusiones (?)

- ¿Hay que parchar?
- ¿Hay que gestionar las alarmas?
- ¿Usar doble-factor de autenticación?
- ¿Las cajas no sirven?



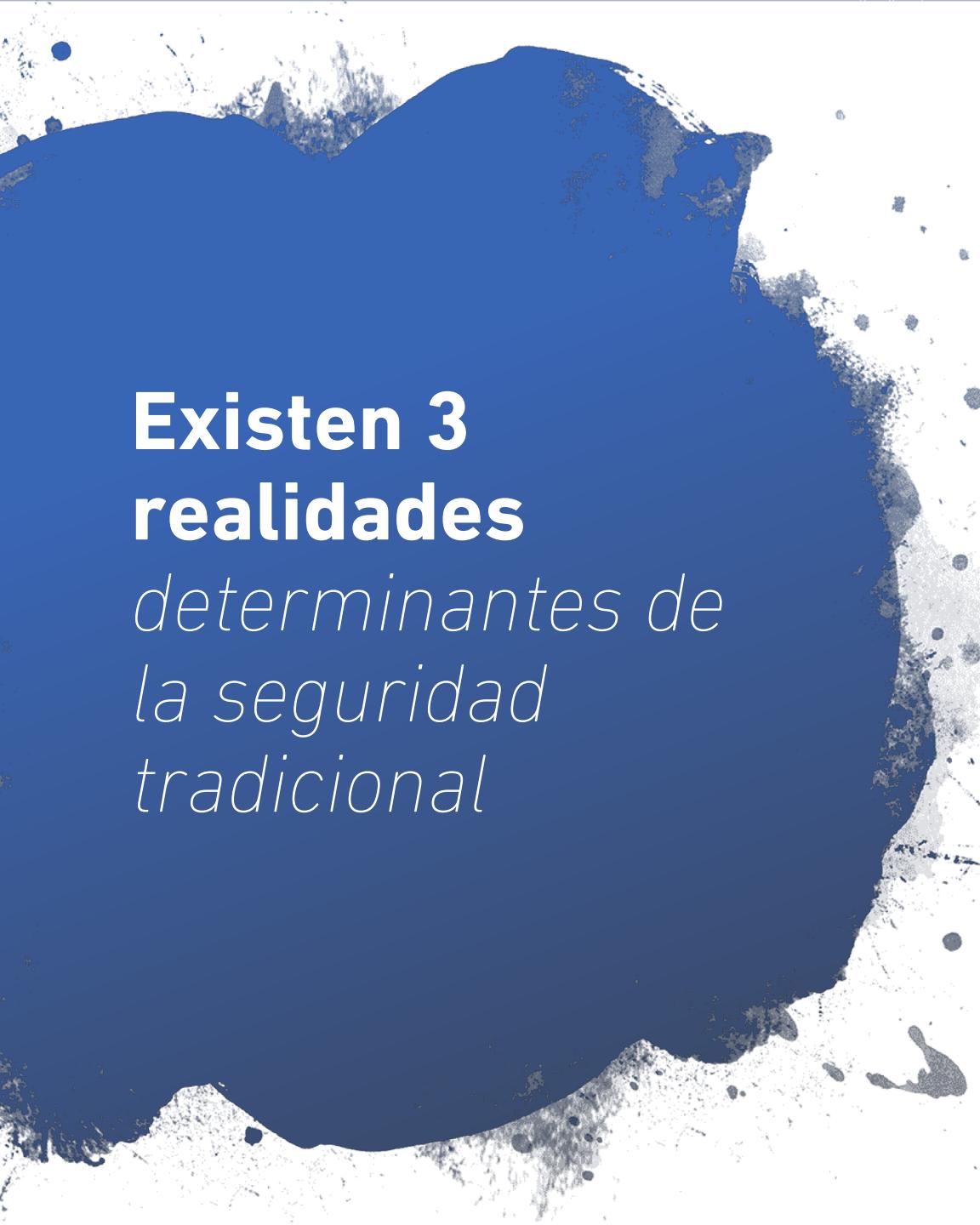
Existen grietas en los controles de seguridad. La seguridad tradicional si bien es necesaria, no es suficiente.

Hablemos de las grietas

Ejemplos

Herramienta	Grieta
Antivirus	Powershell, comandos elevados
Firewalls (c4)	Puertos conocidos
Filtro de Contenido	Webs no categorizadas
Antispam	Borde del sistema de scoring
Escáner de vulnerabilidades	Webs no “vulnerables” (*)
Control de accesos	Credenciales robadas
Parches y Hardening	Procesos de empresa lentos y complejos (factor de riesgo)





Existen 3 realidades

*determinantes de
la seguridad
tradicional*

- 🎃 Los atacantes se preparan para evadir la seguridad.
- 🎃 Es imposible tener un control total de lo que ocurre (ni en la guerra).
- 🎃 El cambio tecnológico es más rápido que cualquier otro proceso.



Sin embargo... el panorama no es tan pesimista como se cree...



Hablemos de
hunting...

¿Qué es *Threat Hunting?*

Es la cacería proactiva e iterativa de amenazas que evaden las herramientas automáticas de seguridad.

Es el complemento de la seguridad tradicional. Tiene por objetivo llenar aquellas grietas que dejan las herramientas de seguridad, en ningún caso reemplazar.

Conceptos:

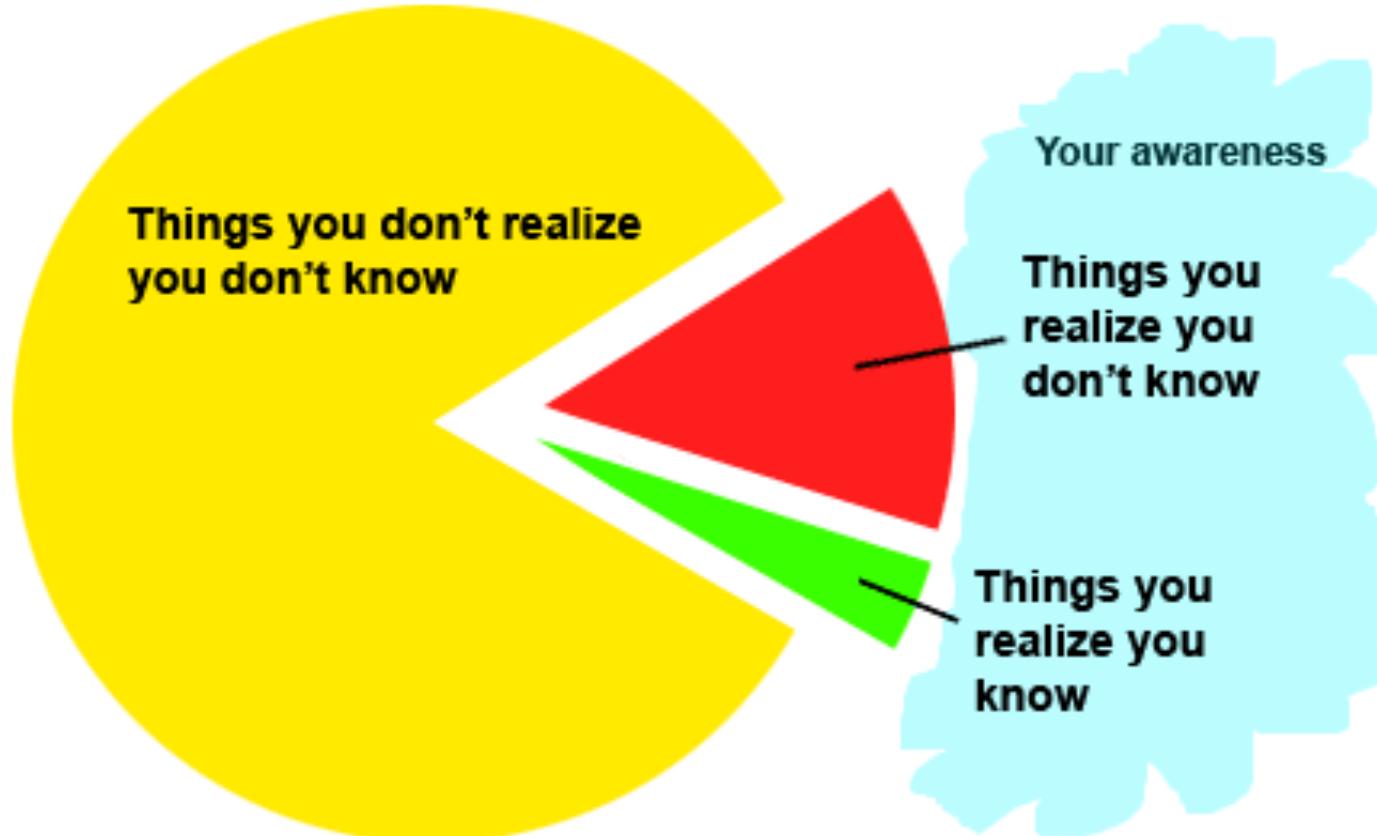
- Detección de lo **anormal****
- Asumir que ya hemos sido hackeados
- Ser proactivo
- Fuerte alineamiento con el **negocio**
- Fuerte componente de Software
- Permanente **colaboración**

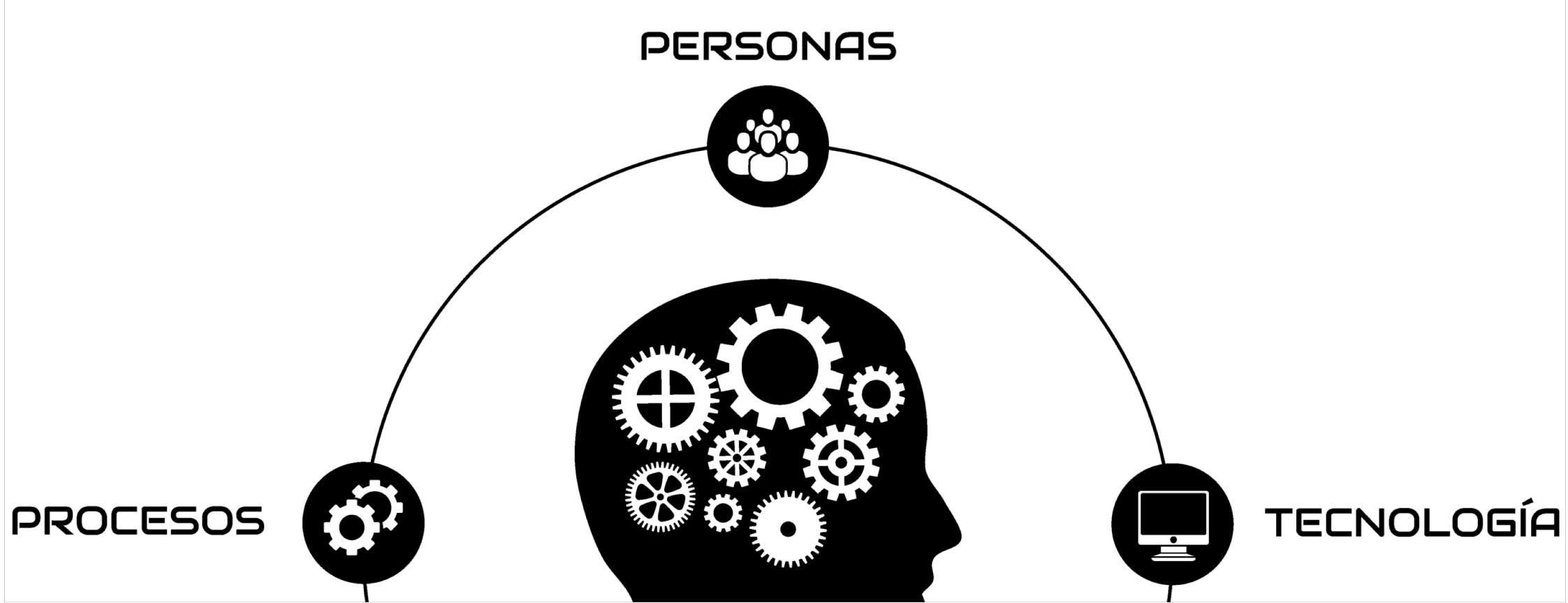
Componente humano

■ No es algo nuevo! de hecho es algo que se lleva haciendo durante años por distintos profesionales, y en muchos lo hacen sin saber.

¿Dónde
ubicamos el
Threat
Hunting?

Body of all possible knowledge

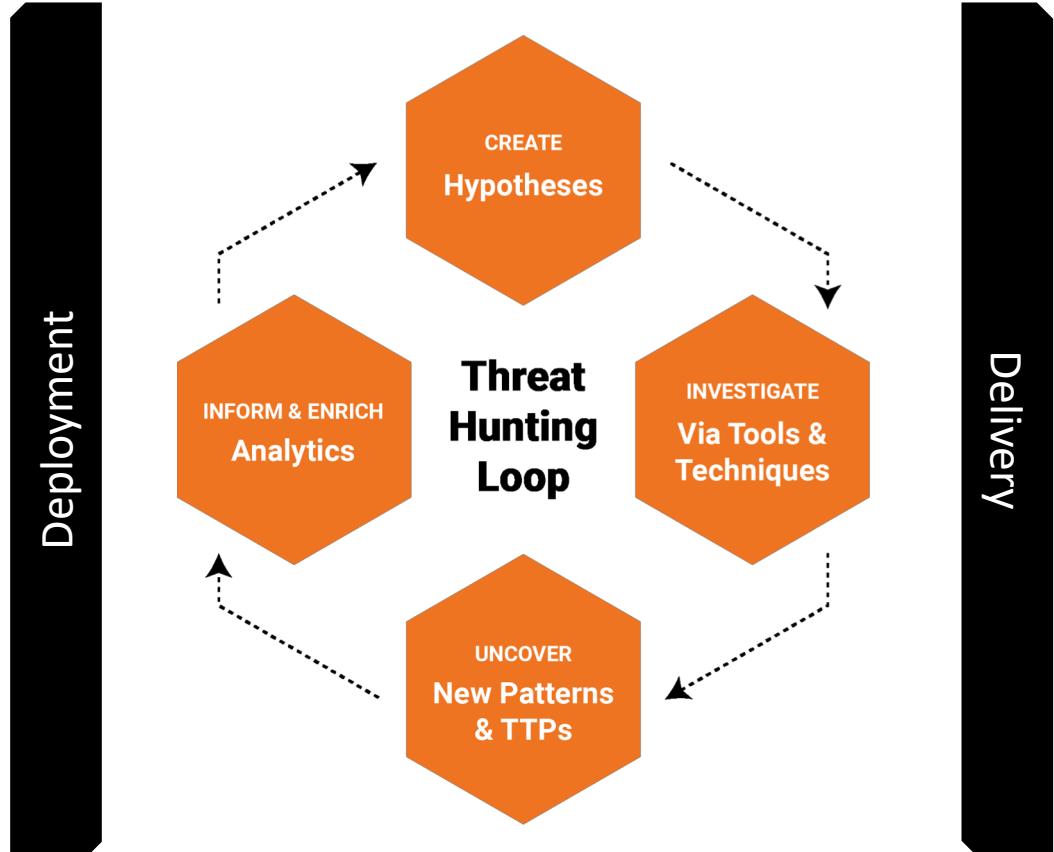




Los 3 pilares del Hunting

Como funciona?

Modelo de Threat Hunting



Crear una hipótesis

- Threat Intelligence (Externa)
- Análisis de activos críticos
- Análisis de anomalías

Investigar la hipótesis

- Recopilar la información necesaria
- Analizar y detectar
- Validar la hipótesis

Descubrir patrones

- Validar la hipótesis
- Declarar si existe o no amenaza
- Definir el KillChain

Informar y enriquecer

- Mejorar los sistemas de protección
- Reportar hallazgos
- Generar inteligencia

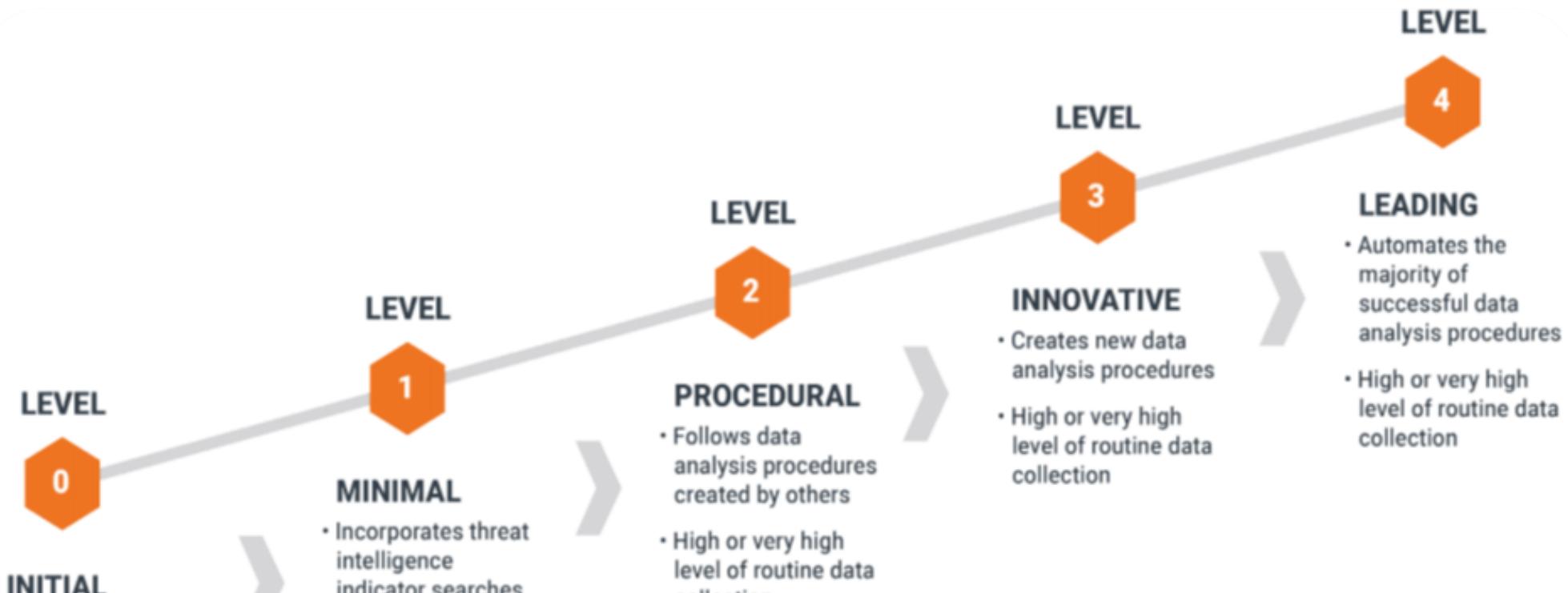
¿Por qué *Hacer hunting?*

- **Monetario:** Pérdidas por ciberataques son devastadoras
- **Profesional:** No podemos tomar una perspectiva pasiva frente a los desafíos de seguridad.
- **Negocio:** Apetito de riesgo
- **Técnico:** Los ataques dirigidos son efectivos
 - **Verizon:** 23% de los recipientes abren el phishing y 11% hace click en los adjuntos.
 - **Symantec:** Los ataques utilizando credenciales comprometidas están en aumento
 - Las defensas tradicionales no son capaces de detectar ataques dirigidos.
 - Cloud, BYOD y ShadowIT hacen que las fronteras de seguridad desaparezcan.
 - Los CISOs están presionados por demostrar que sus empresas son seguras.



Proceso de madurez

Cazando de 0 a 100



Source: <https://sqrrl.com>

La experiencia de cazar
Lo que he vivido en este
2018



Consideraciones importantes

de una buena cacería

El Threat Hunting es
una búsqueda
iterativa



Requiere
conocimiento
específico en un área

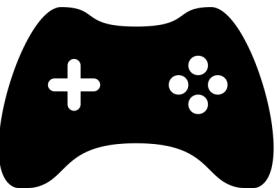


Suele generar
fricción con las
otras áreas



Es un trabajo de
paciencia

Se puede comenzar
de a poco



La motivación es más
importante que la
tecnología

Palabras de Cierre

Y preguntas! (espero)

