



THREAT HUNTING

Tras la cacería de amenazas



Líder de operaciones de
Ciberinteligencia en ENTEL

Miguel Díaz | CEHv8

- Investigador de ciberamenazas.
- CEHv8.
- Colaborador en Seguridad Informática Chile.
- Consultor en ciberseguridad.

@mdiazcl – <https://mdiazlira.com>



- 1. Contextualización**
- 2. Qué es Threat Hunting?**
- 3. El camino del hunter**
- 4. Cierre**

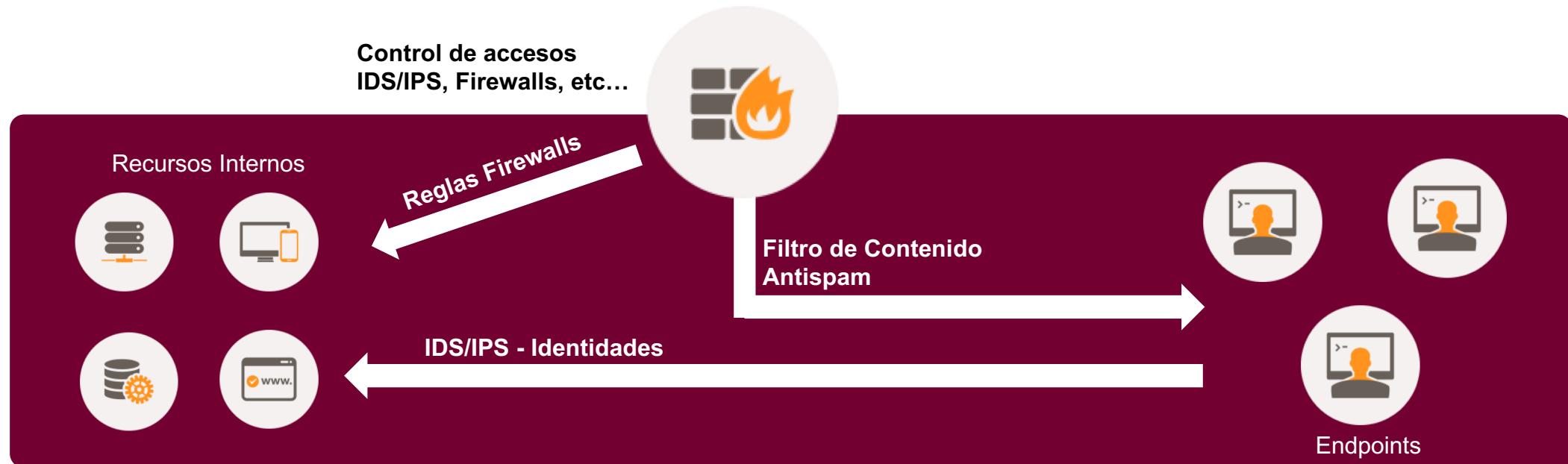


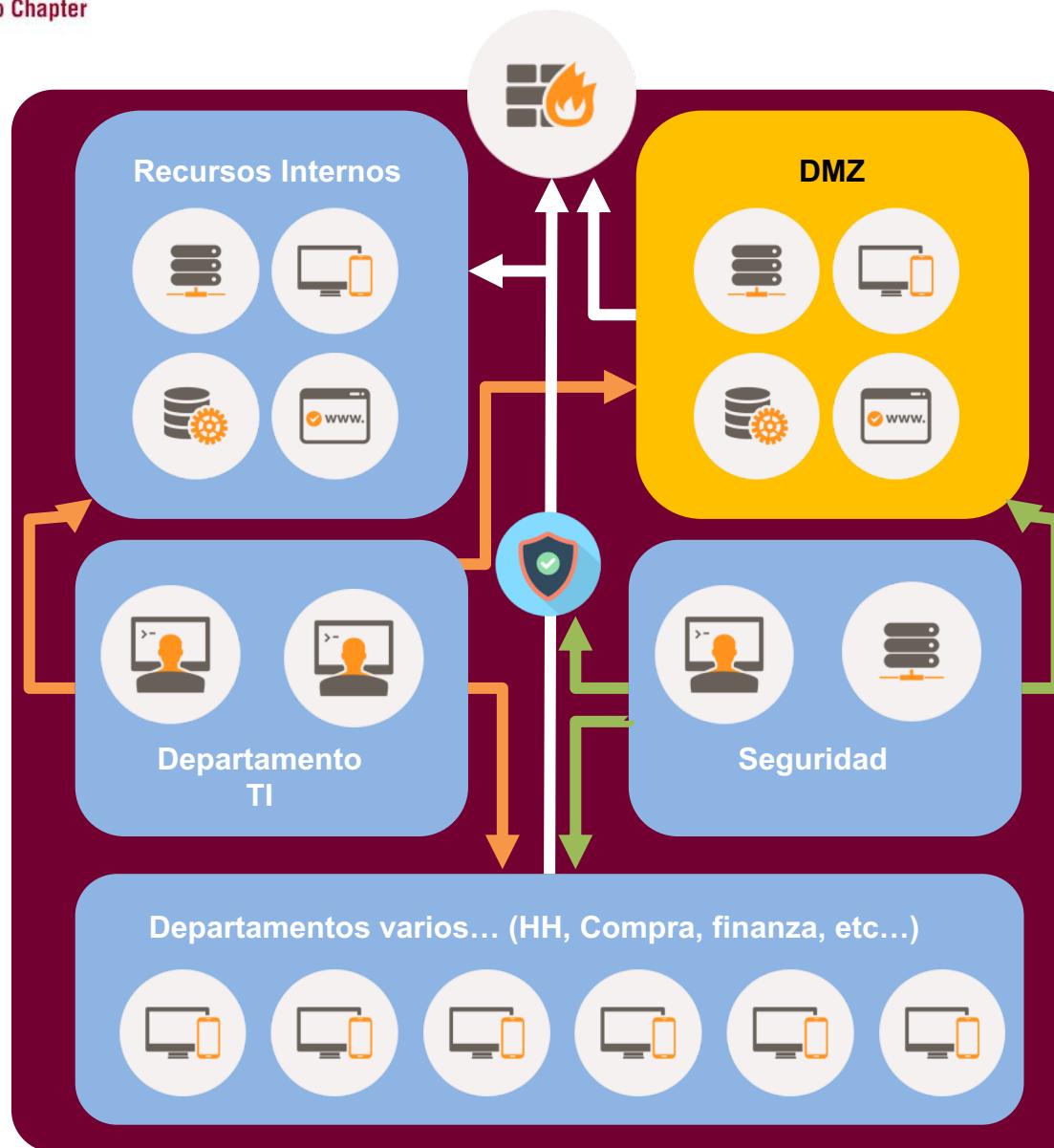
“La información aprendida en esta charla la podrán utilizar al momento de volver a sus oficinas”

- LA PROMESA SANS

CONTEXTUALIZACIÓN

Enfoque Tradicional





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)

LOS HACKEOS OCURREN...

EQUIFAX



YAHOO!

Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked
MyHeritage	2018	92,283,889	genealogy	unknown
BMO and Simplii	2018	90,000	banking	poor security
Orbitz	2018	880,000	web	hacked
Popsugar	2018	123,857	fashion	hacked
Under Armour	2018	150,000,000	Consumer Goods	hacked
Defense Integrated Data Center (South Korea)	2017	235 GB	military	hacked
Deloitte	2017		consulting, accounting	poor security
Erie County Medical Center	2017	unknown	healthcare	poor security
Equifax	2017	143,000,000	financial, credit reporting	poor security
Grozio Chirurgija	2017	25,000	healthcare	hacked
Heathrow Airport	2017	2.5GB	transport	lost / stolen media
Taringa!	2017	28,722,877	web	hacked
Uber	2017	57,000,000	Web	hacked

https://en.wikipedia.org/wiki/List_of_data_breaches

“LAS EMPRESAS SON HACKEADAS DE TODAS FORMAS”

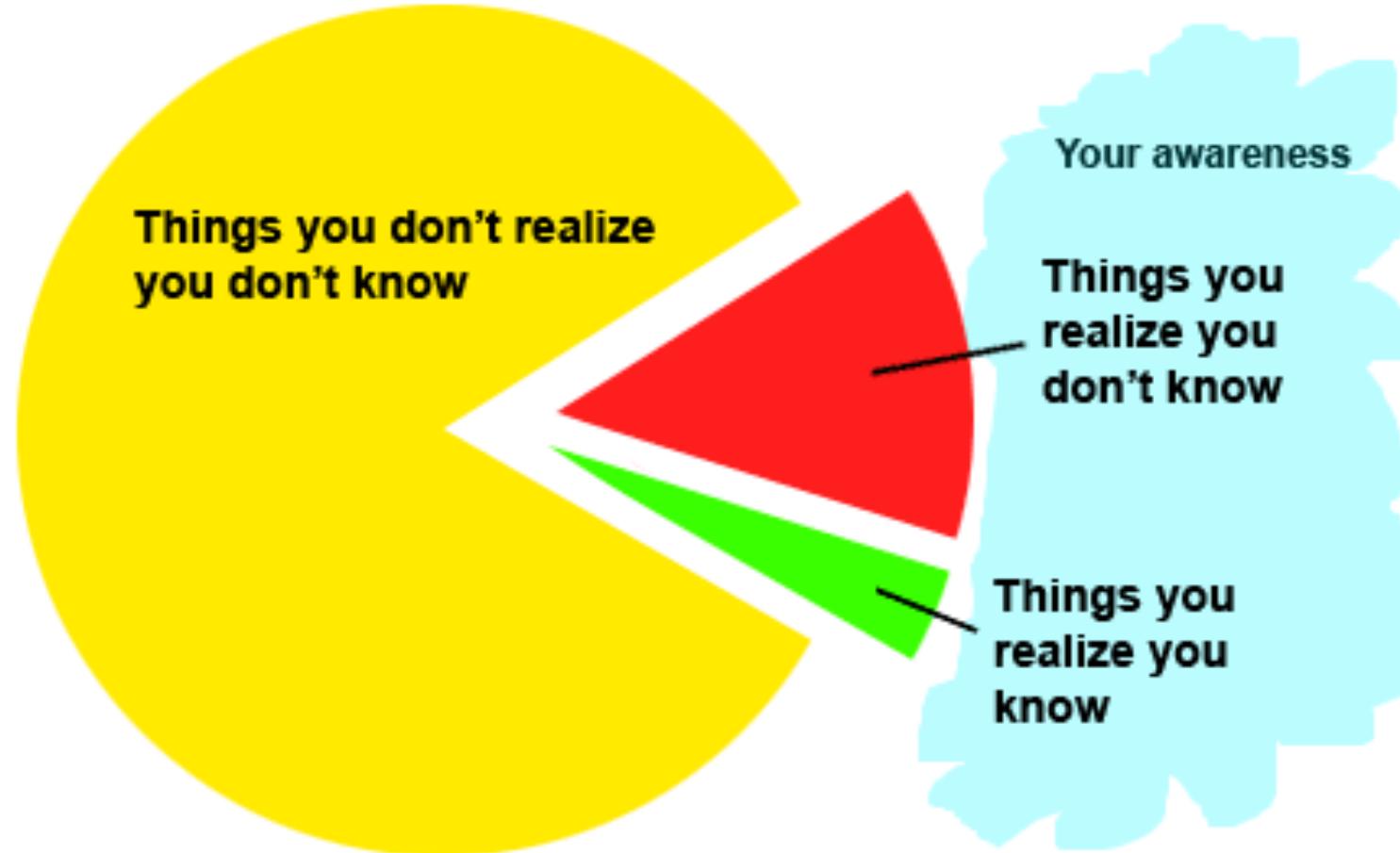
**PERO... QUE PASA CON LAS HERRAMIENTAS
DE SEGURIDAD INSTALADAS?**



Las herramientas de seguridad sufren de...

- Reducción de falsos positivos...
- Configuraciones no-apropiadas...
- Trabajan (principalmente) en base a firmas, las cuales dependen del vendor...

Body of all possible knowledge

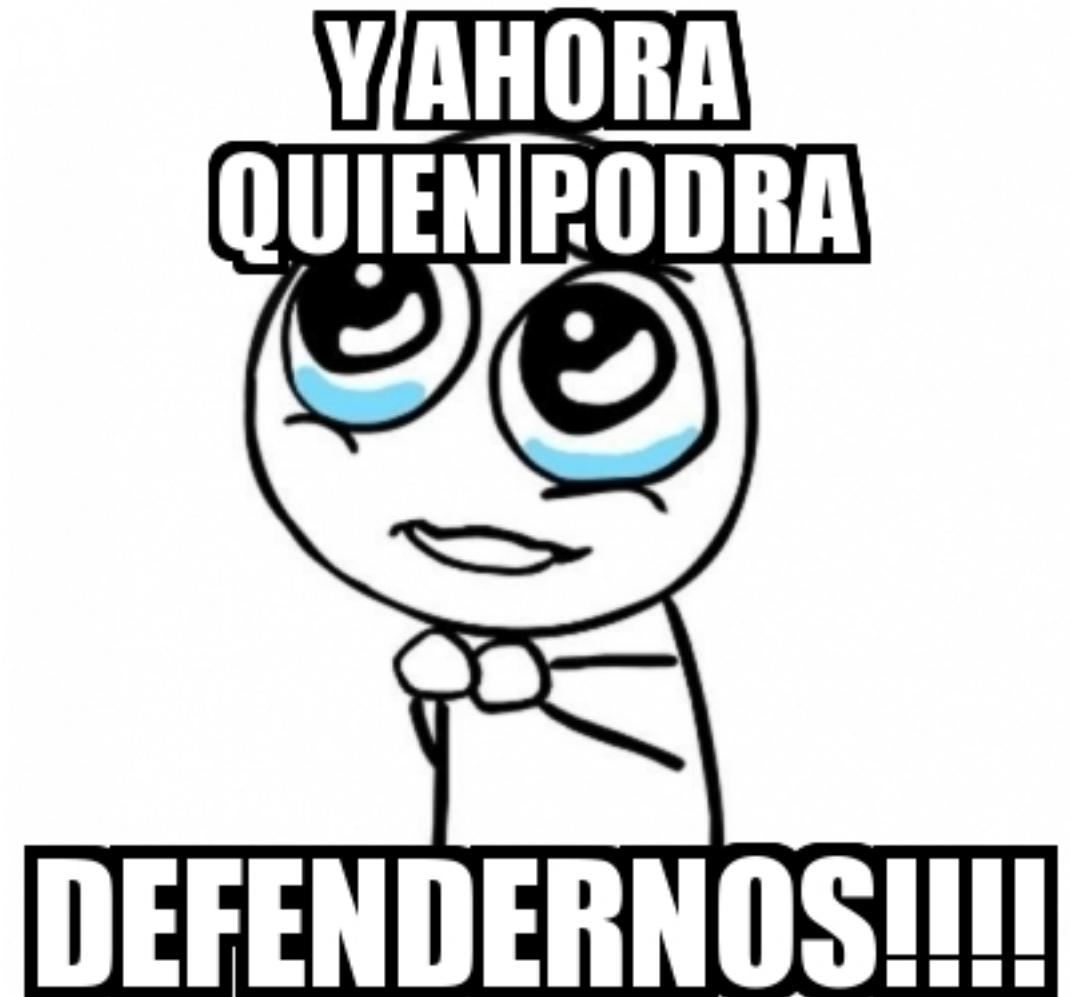


ÁREAS GRISES EN LAS HERRAMIENTAS...

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 “vulnerable” (*)
Control de accesos	Credenciales robadas
Parches y Hardening	Procesos de empresa lentos y complejos (factor de riesgo)

Recapitulando:

- Las cajas de seguridad no son suficientes...
- Los hackeos van a pasar igual... tarde o temprano
- Debí haber estudiado medicina....
- Entonces....



THREAT HUNTING

PROACTIVO

INCIDENT RESPONSE TEAM

REACTIVO

QUÉ ES THREAT HUNTING?



*El proceso **proactivo e iterativo** de búsqueda de amenazas en la red asumiendo que **un atacante ya ha vulnerado** las medidas de seguridad implementadas.*

CÓMO FUNCIONA?



Proceso de Threat Hunting
Source: <https://sqrrl.com>

Crear una hipótesis

- Threat Intelligence (Externa)
- Análisis de activos críticos
- Análisis de anomalías (UBA, NBA, SBA)
- Qué podría buscar un hacker (EH)

Investigar la hipótesis

- Recopilar la información necesaria
- Analizar y detectar

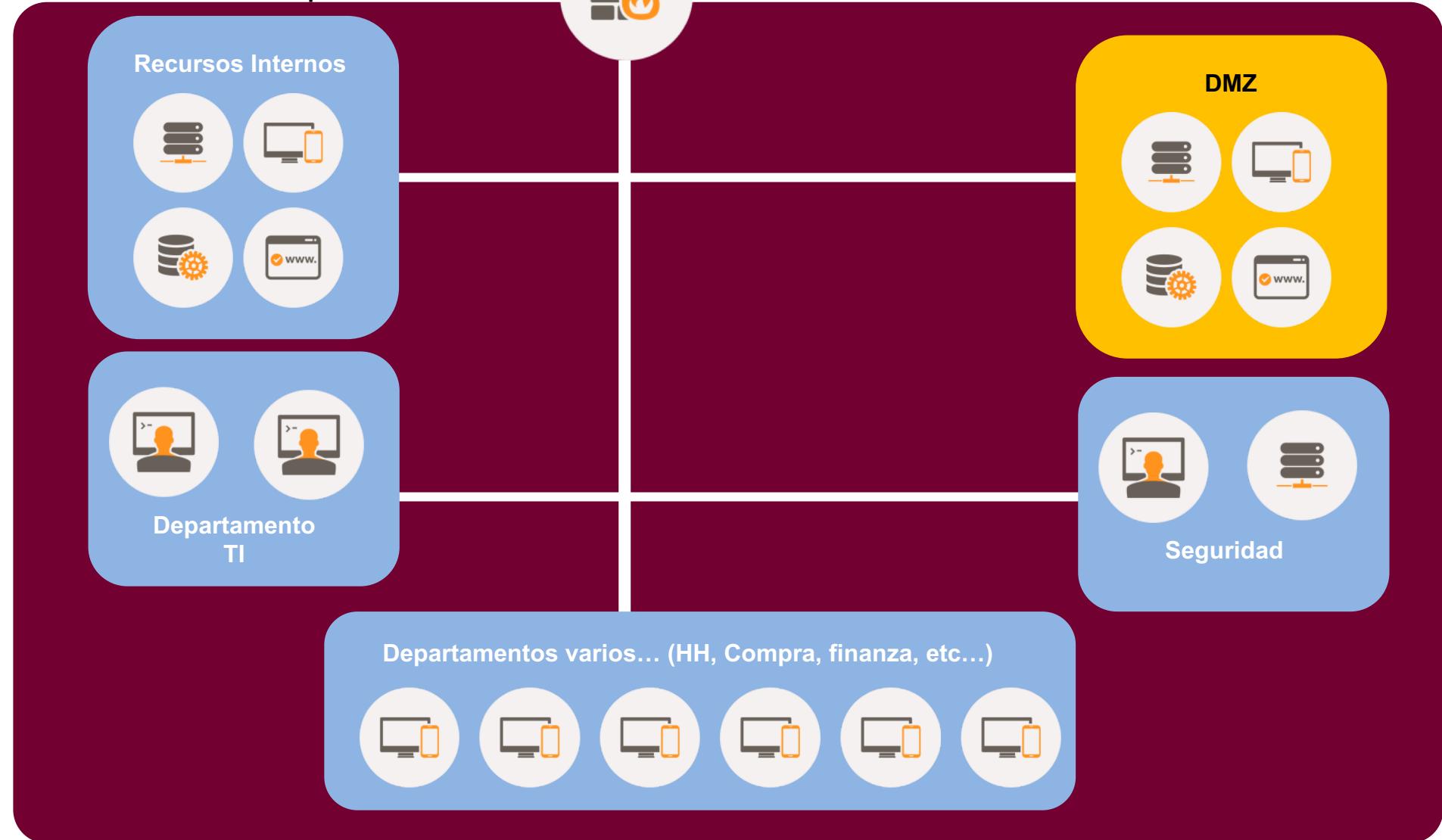
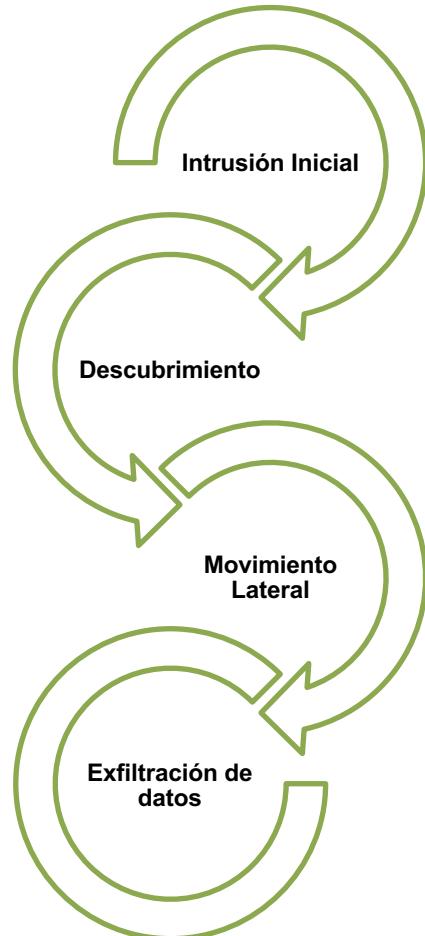
Descubrir patrones

- Validar la hipótesis
- Declarar si existe o no amenaza
- Definir si hay intrusión

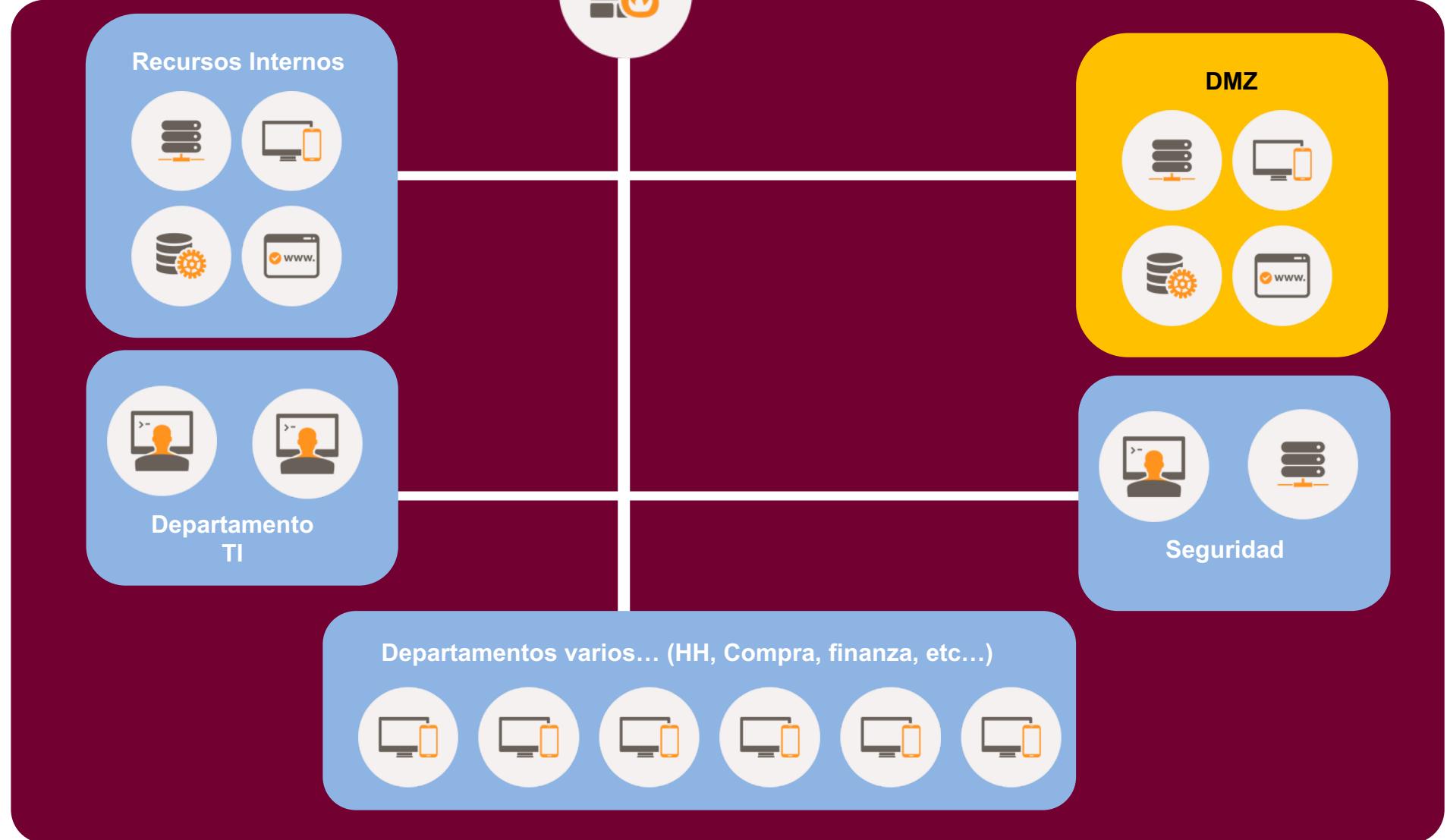
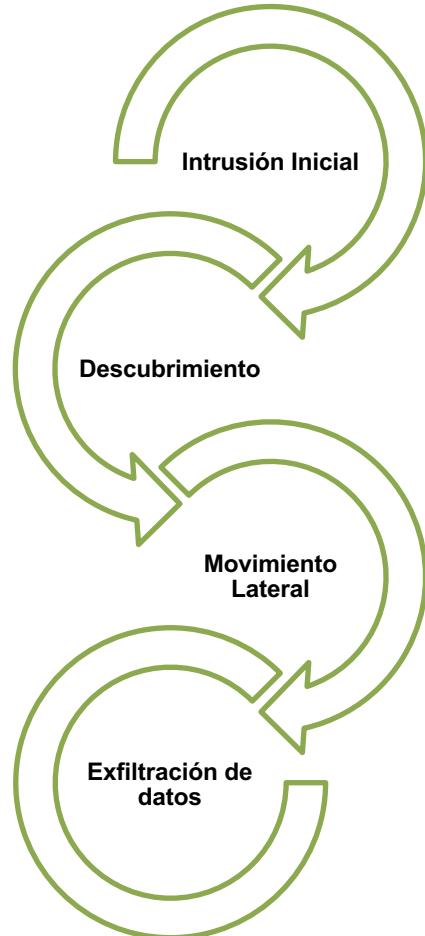
Informar y enriquecer

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

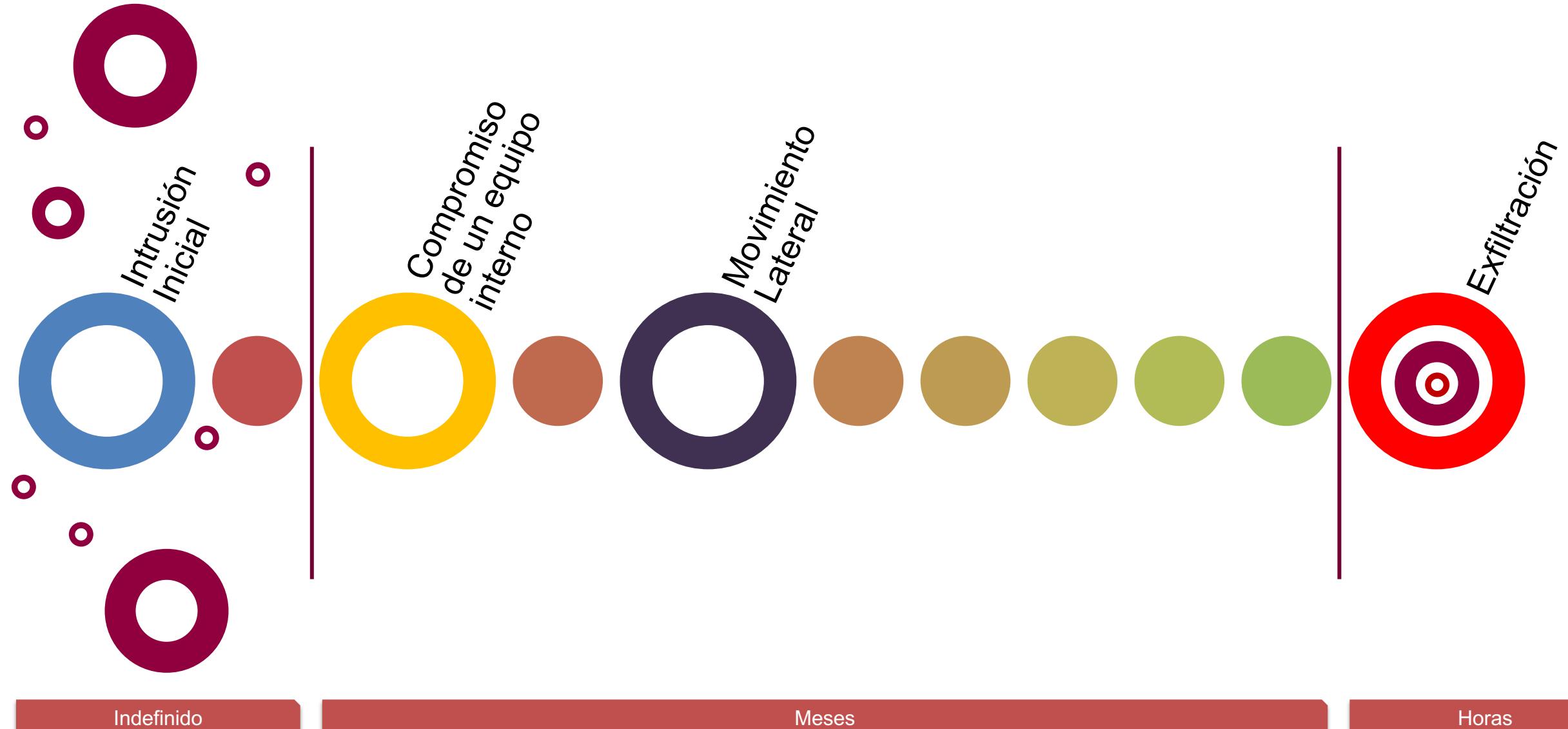
Intrusión servicio expuesto



Intrusión vía phishing



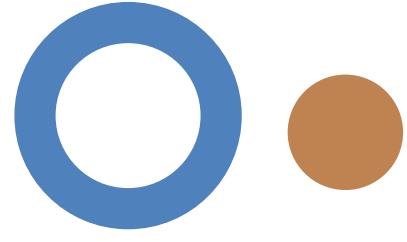
UNA INTRUSIÓN COMPLETA



EN QUÉ PUNTO BUSCAMOS?



Intrusión inicial



Movimiento Lateral



Exfiltración

ALGUNAS IDEAS PARA DETECTAR MOVIMIENTO LATERAL...

Powershell en máquinas

Utilización anormal de puertos

Conexiones de red hacia puertos con rangos extraños

Autenticaciones de usuarios desde IP's desconocidas

Solicitudes de Kerberos
Tickets excesivos

Actividad de antivirus

Conexiones entre zonas fuera de lo común

Accesos a FileServers fuera de lo común

Servicios, WMIC,
SchTasks, PSEnc (??)...

Ratio consumidor
productor distinto de 1

Escaneos de red Internos

Utilización explícita de credenciales



Fork de David J. Bianco (@DavidJBianco)
<https://github.com/mdiazcl/ThreatHunting>

INVITACIÓN AL PÚBLICO

Hipótesis

- Credencial de domain admin comprometida utilizada

Investigar la hipótesis

- Revisar logs en DC (4624, 4648, 4768, 4672).
- Comprobar que los usuarios estén siendo usados en horas lógicas y una cantidad de eventos razonable.

Descubrir patrones

- Descubrir cómo fue comprometida.
- Detectar qué acciones ha realizado.

Informar y enriquecer

- Detectar que herramientas han fallado y por qué.
- Crear regla de SIEM con listado de administradores y horarios de uso.

Hipótesis

- Malware propagándose por la red.

Investigar la hipótesis

- Revisar los logs de antivirus buscando infecciones (limpiadas y las que no).
- Actividad entre equipos que no debiesen comunicarse.
- Puertos inusuales en la red.

Descubrir patrones

- Descubrir por donde entró el malware.
- Detectar cuales son los IoC del malware para prevenir.

Informar y enriquecer

- Detectar que herramientas han fallado y por qué.
- Cargar (y compartir) los IoC detectados.

¿Por qué Hacer hunting?

- **Monetario:** Pérdidas por ciberataques son devastadoras
- **Profesional:** No podemos tomar una perspectiva pasiva frente a los desafíos de seguridad
- **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.



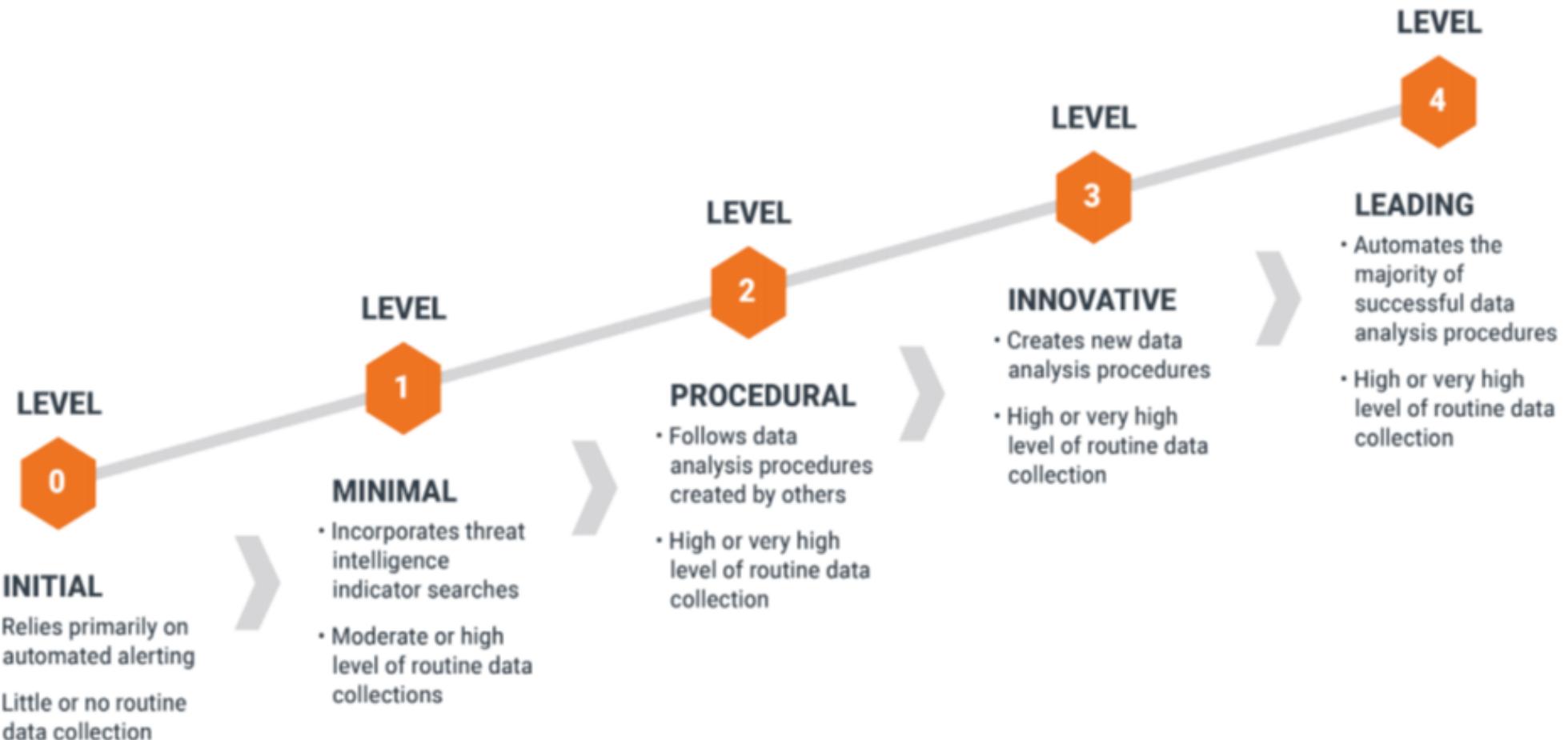
"60% of those who hunt for threats reported measurable improvements in their InfoSec programs based on their hunting efforts, and 91% report improvements in speed and accuracy of response." - ESTUDIO SANS 2018

EL CAMINO DEL HUNTER

HABILIDADES A DESARROLLAR

- Desarrollar un muy buen conocimiento de redes.
- Buen manejo de eventos de Windows.
- Conocimiento del entornos de seguridad Microsoft y empresariales.
- Conocimientos y herramientas forenses
- Reversing de malware
- Scripting en algún lenguaje (python, bash, etc...)
- Conocimientos de Data Science
- Experiencia en pentesting
- Buen manejo del inglés

NIVELES DE MADUREZ



Modelo de Madurez Threat Hunting
Source: <https://sqrrl.com>

CIERRE E INVITACIÓN



**CARBON
BLACK**



Google