

# Threat Hunting:

Enfoque proactivo de  
ciberdefensa



e) corp

# mdiazcl ~ \$: whoami

- Investigador de Ciberamenazas
- Consultor en Ciberseguridad
- Líder de Investigación y Desarrollo en ENTEL
- Certificado CEHv8
- Entrenamiento en Respuesta de Incidentes y Threat Hunting Avanzado (FOR508)
- Experiencia en múltiples incidentes de Ciberseguridad
- **En progreso:** Master en Data Science

- Habilidades:
  - Hacker Ético
  - First-responder
  - Ex-desarrollador de software



# Panorama de Ciberseguridad 2018 - 2019

# El costo de las brechas aumenta

Y seguirá aumentando!

# 130

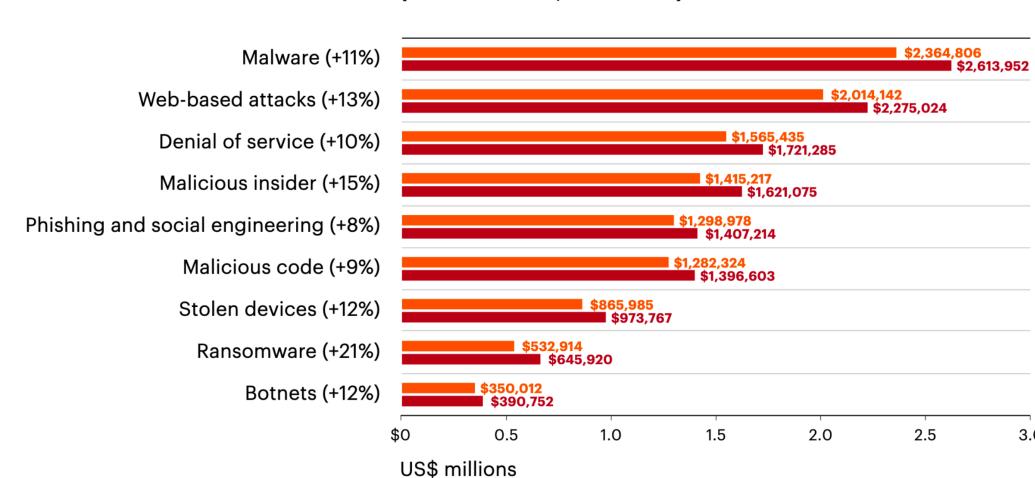
Average number of security  
breaches in 2017



# 145

Average number of security  
breaches in 2018

**Average annual cost of cybercrime by type of attack  
(2018 total = US\$13.0 million)**

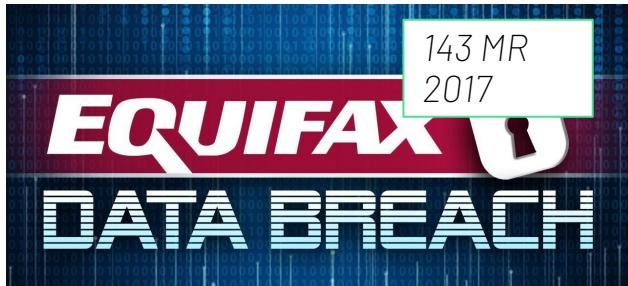


**Legend**

- 2017
- 2018

# Casos de Brechas

Las grandes empresas están siendo afectadas



# Casos de Brechas

Las grandes empresas se ven afectadas

Entity	Year	Records	Organization type	Method	Sources
First American Corporation	2019	885,000,000	financial service company	poor security	[120]
Facebook	2019	540,000,000	social network	poor security	[117]
Truecaller	2019	299,055,819	Telephone directory	unknown	[272][273]
Canva	2019	140,000,000	web	hacked	[54][55][56]
Justdial	2019	100,000,000	local search	unprotected api	[166]
Quest Diagnostics	2019	11,900,000	Clinical Laboratory	poor security	[219]
Desjardins	2019	2,900,000	financial	inside job	[85]
Facebook	2019	1,500,000	social network	accidentally uploaded	[118]
Health Sciences Authority (Singapore)	2019	808,000	healthcare	poor security	[147]
Westpac	2019	98,000	financial	hacked	[324]
Ministry of Health (Singapore)	2019	14,200	healthcare	poor security/inside job	[192][193]
Australian National University	2019	19 years of data	academic	hacked	[325]
Woodruff Arts Center	2019	unknown	arts group	poor security	[309]
Marriott International	2018	500,000,000	hotel	hacked	[183][184]

FUENTE: [https://en.wikipedia.org/wiki/List\\_of\\_data\\_breaches](https://en.wikipedia.org/wiki/List_of_data_breaches)



# Detrás de cámaras: Ganancias del Cibercrimen



Cybercrime will generate at least \$1.5 trillion this year—and that's conservative

- Investigator Dr. Michael McGuire (2018)

At <https://www.rsaconference.com/speakers/michael-mcguire>

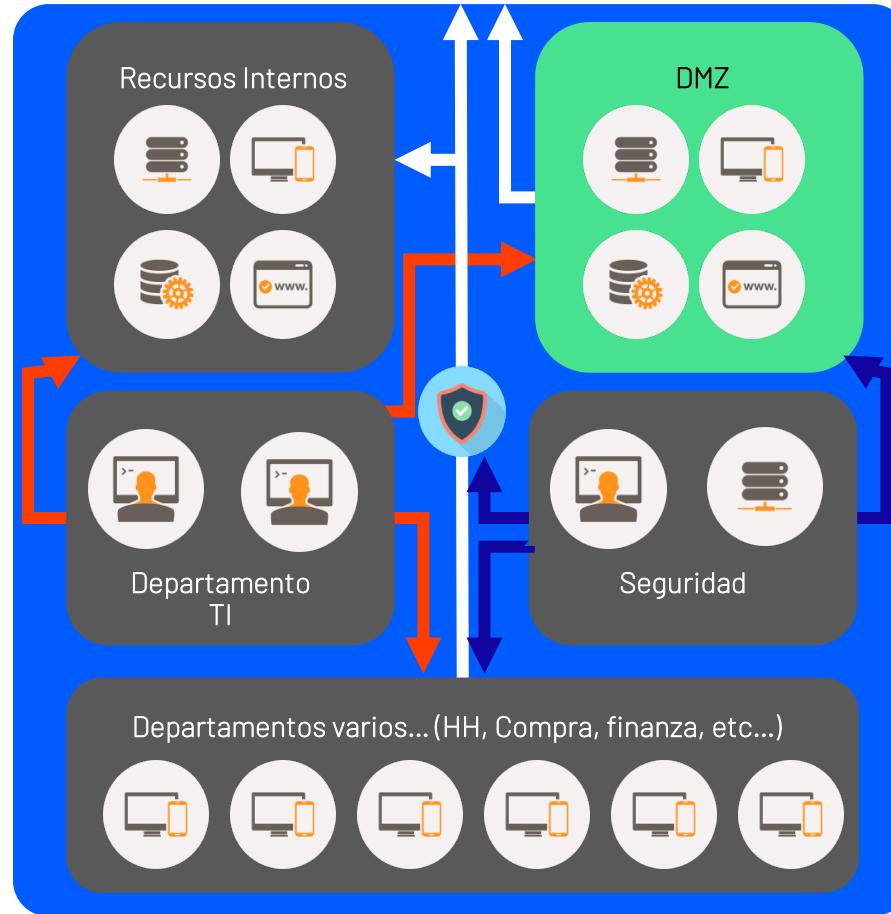
- \$860 billion – Illicit/illegal online markets
- \$500 billion – Theft of trade secrets/IP
- \$160 billion – Data trading
- \$1.6 billion – Crimeware-as-a-Service
- \$1 billion – Ransomware

# Enfoque tradicional ciberseguridad

# Enfoque tradicional de Ciberseguridad

## Dispositivos de seguridad:

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



## Realidad frente a los ciberataques

**Existen 4  
realidades**  
*determinantes de  
la seguridad  
tradicional*

Los atacantes se preparan para evadir la seguridad tradicional.

Es imposible tener un control total de lo que ocurre (ni en la guerra).

El cambio tecnológico es más rápido que cualquier otro proceso de seguridad.

La seguridad las están haciendo las áreas de ciber, y no la compañía completa.

# Controles Tradicionales



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

# Postura de ciberseguridad

SEGURIDAD  
TRADICIONAL

PASIVO

INCIDENT  
RESPONSE  
TEAM

*REACTIVO*

THREAT  
HUNTING

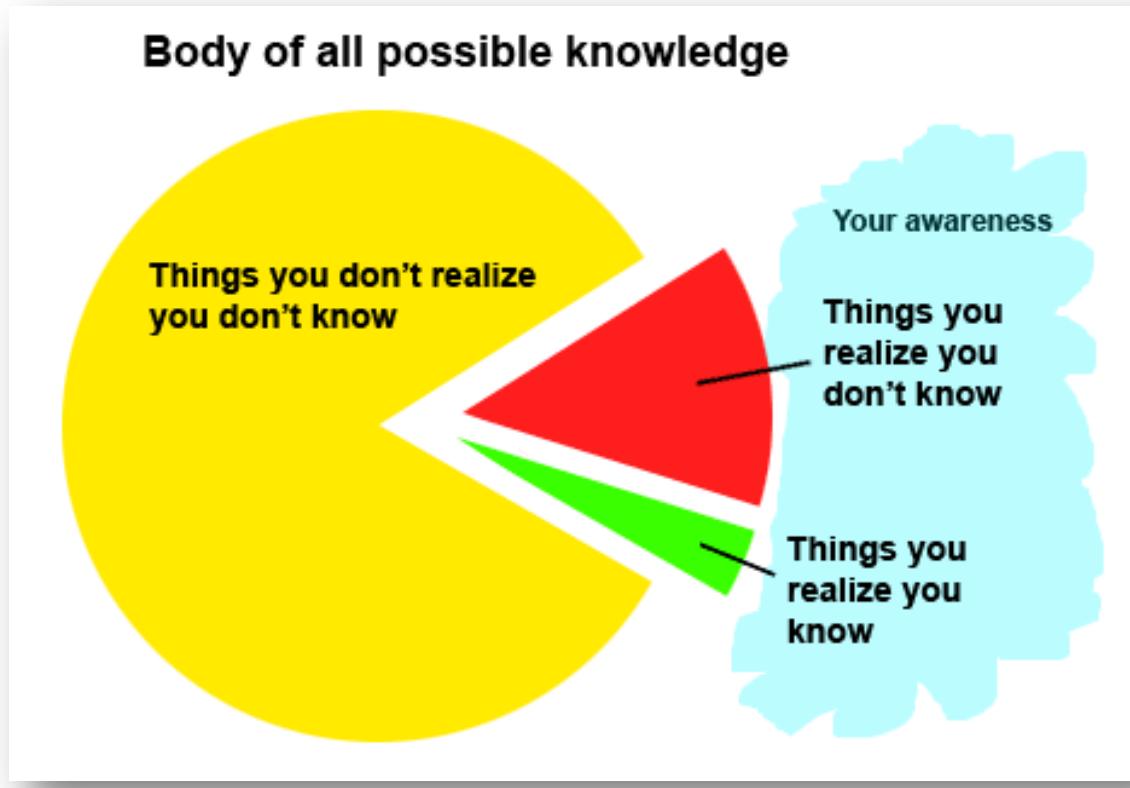
*PROACTIVO*

# Threat Hunting

(por fin eh...)



# Diagrama del Conocimiento



# ¿Qué es el Threat Hunting?

## Definición

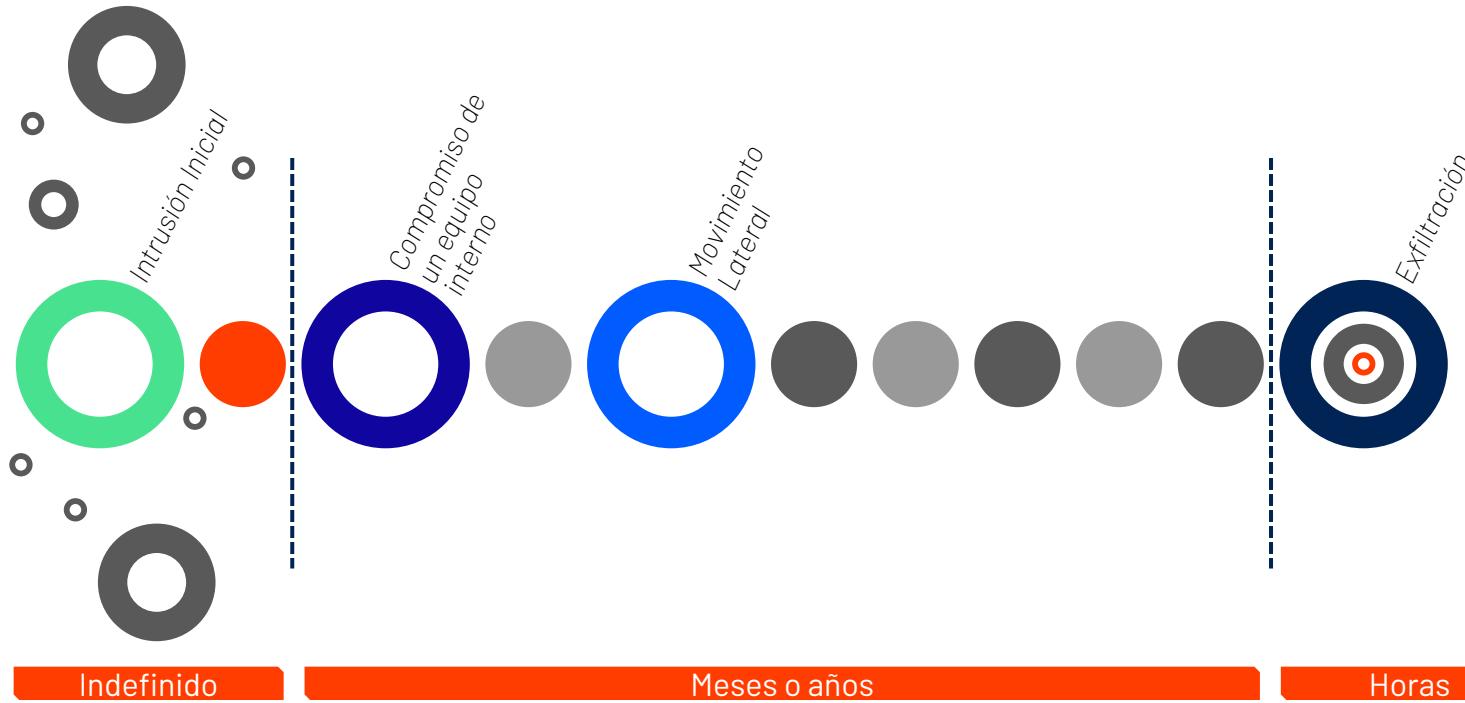
El proceso **proactivo e iterativo** de búsqueda de amenazas en la red asumiendo que **un atacante ya ha vulnerado** las medidas de seguridad implementadas.

Threat Hunting es un complemento a la seguridad tradicional. Tiene por objetivo llenar aquellas grietas dejadas las herramientas de seguridad.

## Killchain - Lockheed Martin



# Diagrama de una intrusión



Los logs  
Nos cuentan  
cosas

## Quick Values for port\_dst

Add to dashboard ▾ Customize ▾ x



Value

%

Count

## Quick Values for result

Add to dashboard ▾ Customize ▾ x



Value

%

Count

Previous

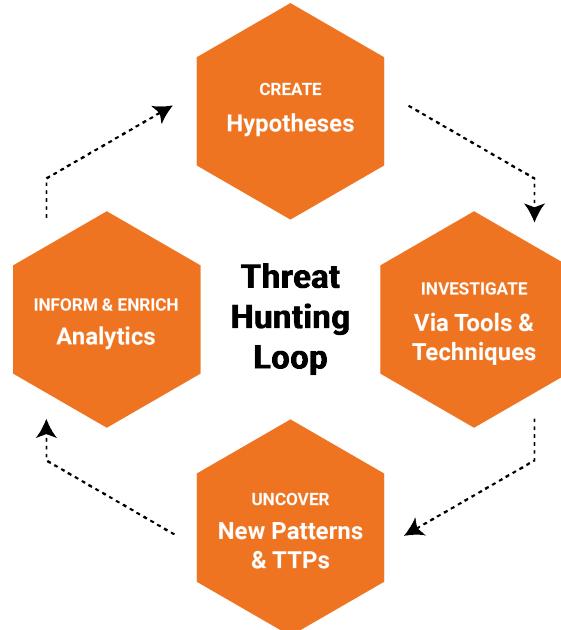
1

Next

## Messages

Timestamp <span style="color: #0070C0;">↑</span>	source	ip_mac	logon_name
2017-12-07 09:44:42.526	mapache	34-02-86-9A-95-CA	admin_pc
2017-12-07 09:44:42.525	mapache	34-02-86-9A-95-CA	admin_pc
2017-12-07 09:44:42.525	mapache	34-02-86-9A-95-CA	jpjil
2017-12-07 09:44:42.524	mapache	34-02-86-9A-95-CA	admin_pc
2017-12-07 09:44:42.524	mapache	34-02-86-9A-95-CA	admin_pc
2017-12-07 09:44:42.522	mapache	34-02-86-9A-95-CA	SYSTEM
2017-12-07 09:44:42.519	mapache	34-02-86-9A-95-CA	jpjil

# ¿Cómo hacer hunting?



## Proceso de Threat Hunting

FUENTE: <https://sqrrl.com>

### Crear una hipótesis

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

### Investigar la hipótesis

- Diseñar la cacería (trampas, registros, etc)
- Recopilar la información necesaria
- Analizar y detectar

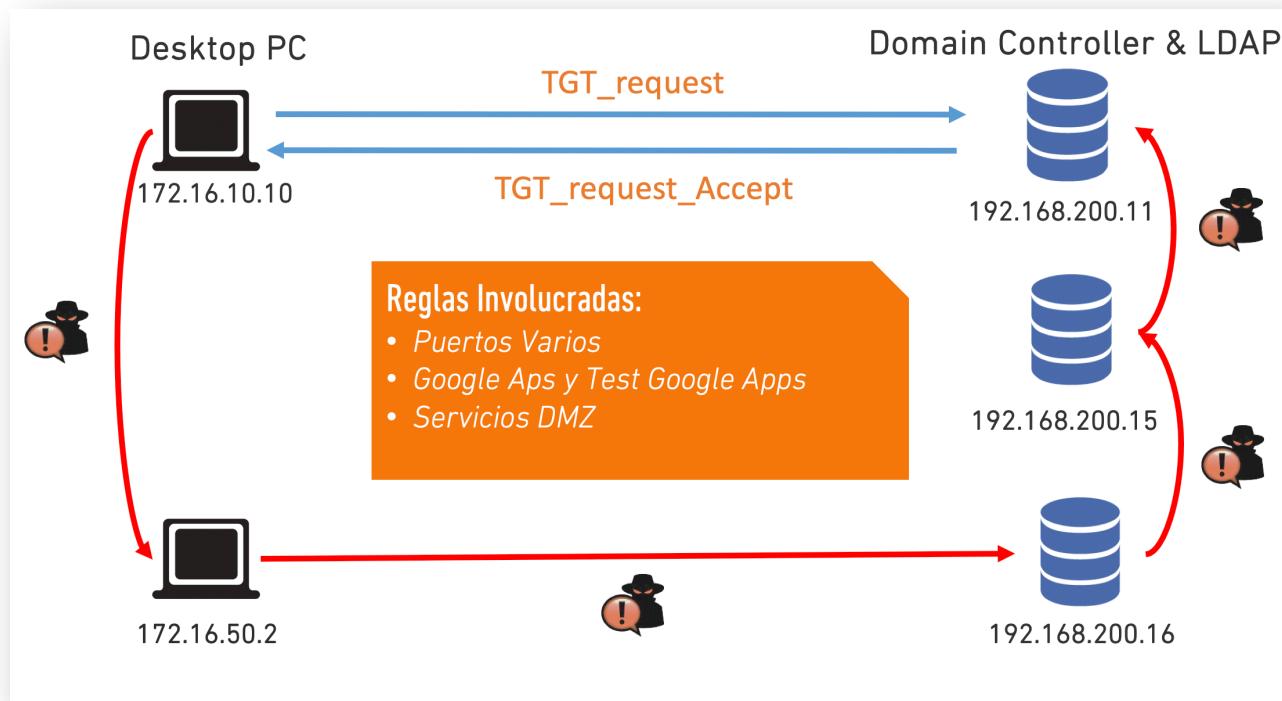
### Descubrir patrones

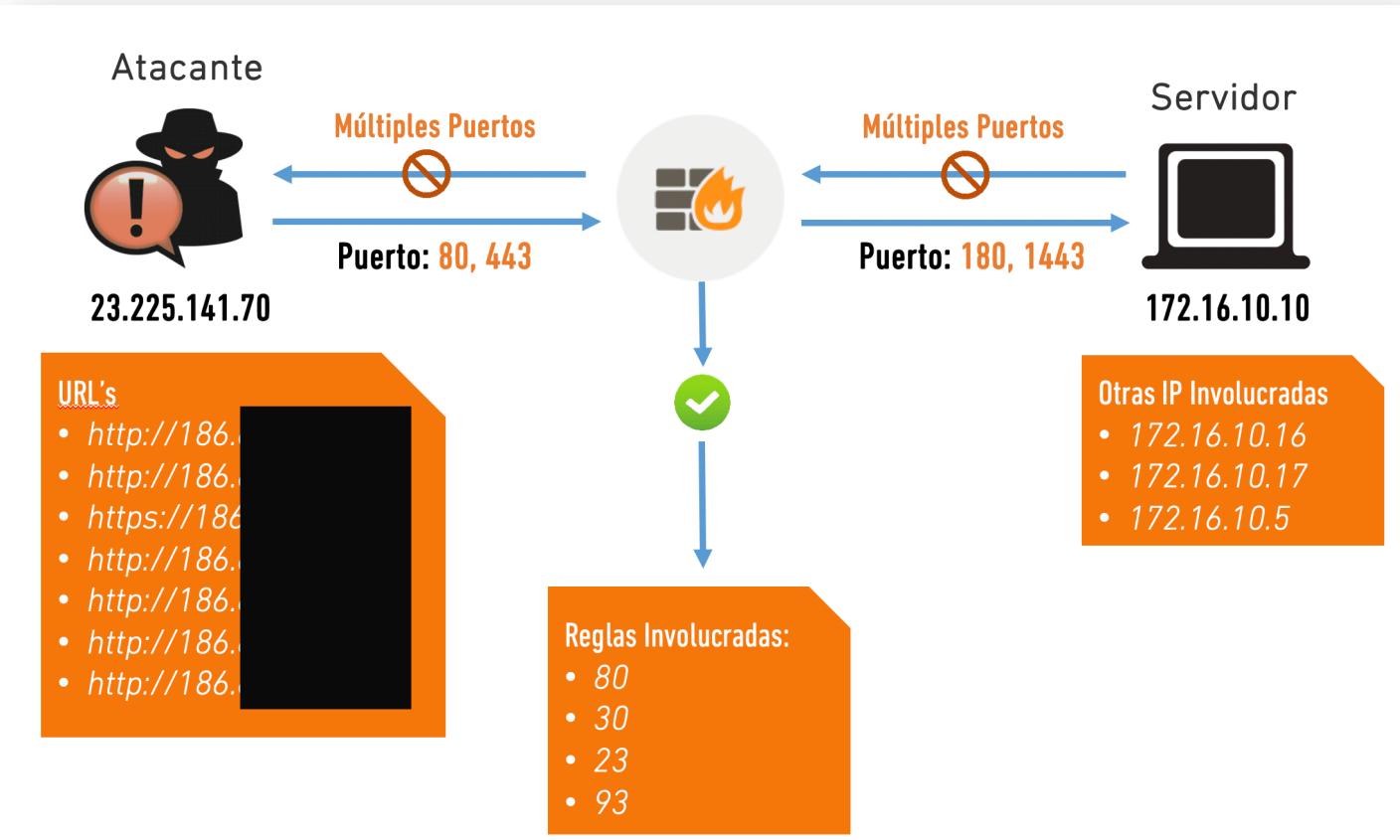
- Validar la hipótesis
- Declarar si existe o no amenaza
- Definir si hay intrusión

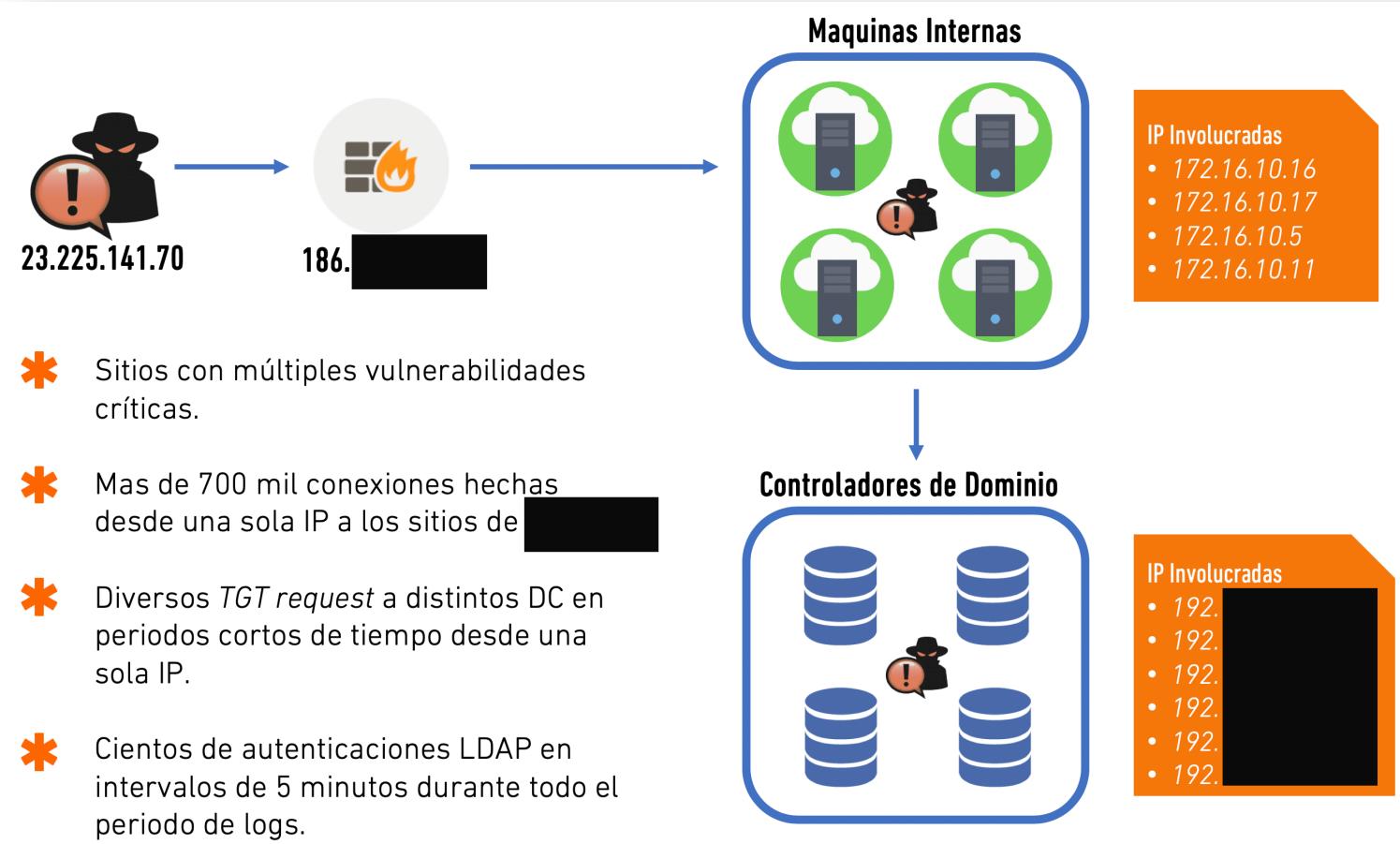
### Informar y enriquecer

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

# Una Cacería exitosa







# ¿De dónde sacar información?

## Fuentes relevantes:

- Resoluciones DNS
- Actividad de Antimalware
- Filtro de Contenido
- Netflow (ESTE-OESTE, NORTE-SUR)
- Active Directory
- IPS/IDS
- Honeypots

## Herramientas útiles:

- Analizadores de data
- Sistemas de profiling de red, usuarios y entidades
- SIEMs que permitan hacer consultas
- EDRs en los Endpoints
- Diagrama actualizado de comunicaciones
- Un responsable identificable (\*)

# Ejemplos de cacerías

Powershell en máquinas

Utilización anormal de puertos

Conexiones de red hacia puertos con rangos extraños

Autenticaciones de usuarios desde IPs 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

Honeypots  
Docker Traps

Escaneos de red Internos

Utilización explícita de credenciales

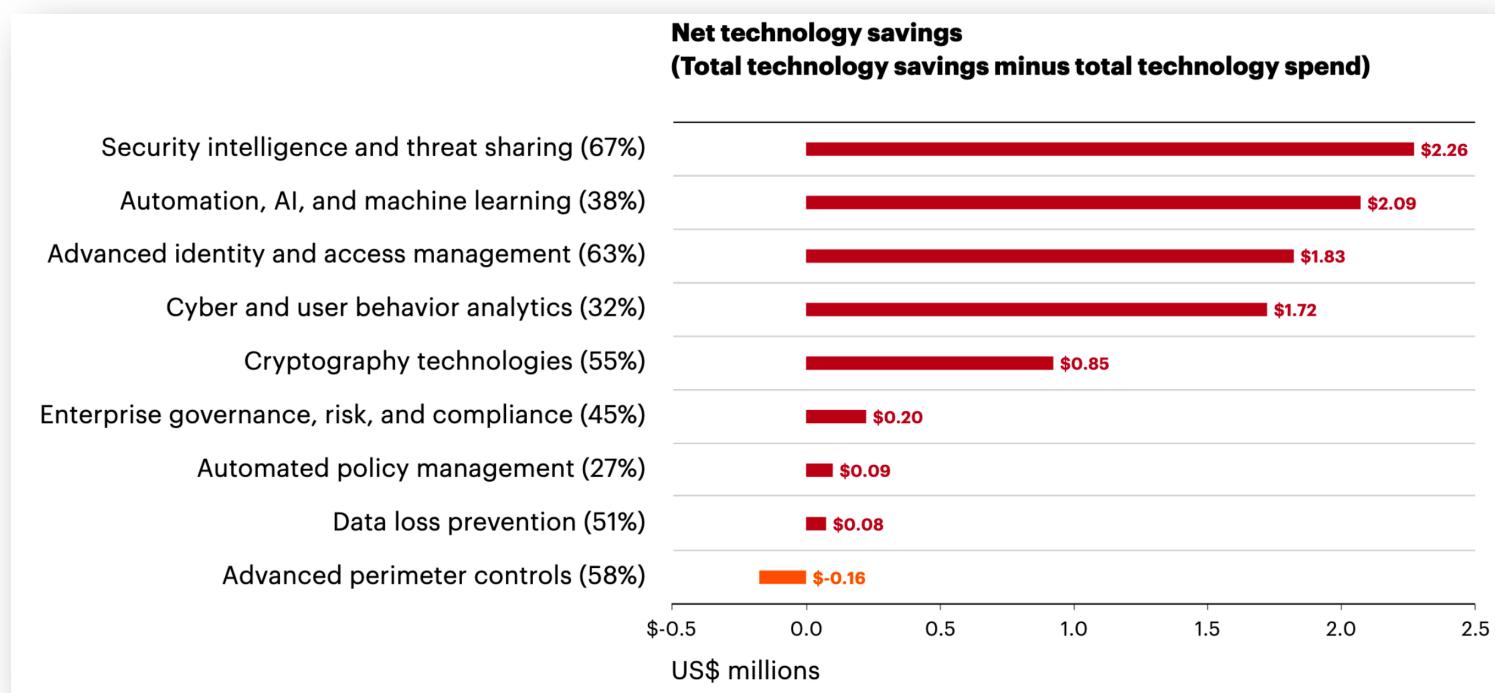
# ¿Por qué realizar Threat Hunting?

- **Monetario:** Pérdidas por ciberataques son devastadoras.
- **Estratégico:** No podemos tomar una perspectiva pasiva frente a los desafíos de seguridad, no con un cibercrimen que invierte en atacar.
- **Técnico:** Esperar a que los *vendedores* tengan las firmas y los parches específicos para nuestra empresa específica es imposible.
- Los hackeos ocurrirán, y no son evidentes. Es necesario ir a buscarlos dentro de la compañía.
- Mejoran considerablemente los procesos de búsqueda y en algunos casos de auditoría interna.

*"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."*

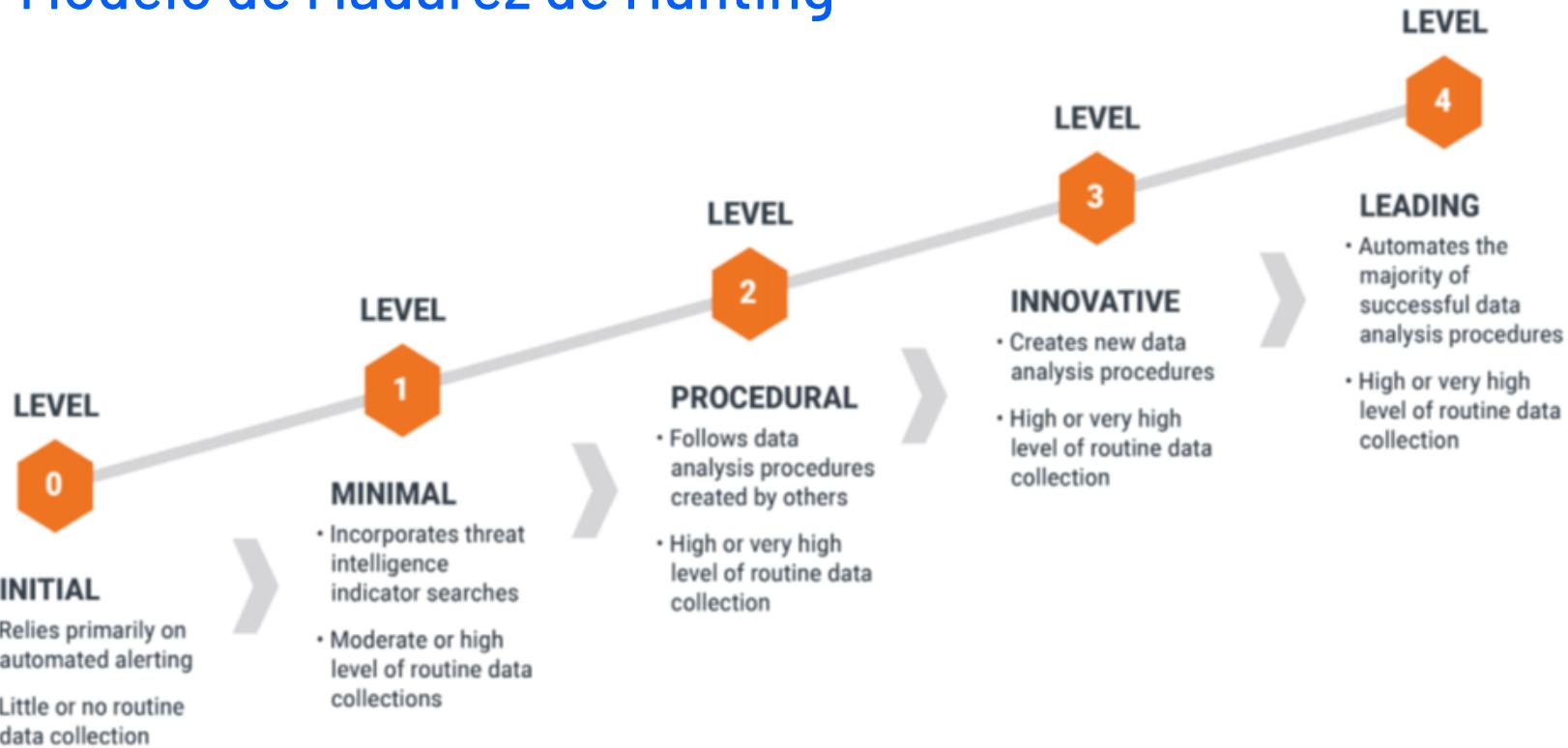
- ESTUDIO SANS 2018

# La inversión en Ciberseguridad



FUENTE: NINTH ANNUAL COST OF CYBERCRIME STUDY  
Accenture y Ponemon Institute

# Modelo de Madurez de Hunting

Fuente: <https://sqrrl.com>

## Invitación y literatura



CARBON  
**BLACK**

Google



# Cierre



# Cierre

- Los **ciberataques no son evidentes**, pero dejan muchas señales y huellas que se pueden perseguir.
- Es necesaria **gente capacitada y un buen nivel de madurez** para implementar Threat Hunting como cultura. Primero lo pasivo, luego avanzamos.
- Si no existe la madurez, se recomiendan **Threat Hunting estilo auditorias** de ciberseguridad similar a los pentesting.
- La adquisición de **inteligencia accionable** es la clave para realizar una buena cacería.
- Tecnologías como **Machine Learning e Inteligencia artificial** permiten tener un enfoque proactivo, siempre y cuando existan analistas capacitados detrás.
- **La ciberseguridad la hacemos todos!**

e) corp