Miguel Díaz – Security Researcher

11/nov

- Threat Hunting -

A la caza de ciberamenazas

~$ whoami

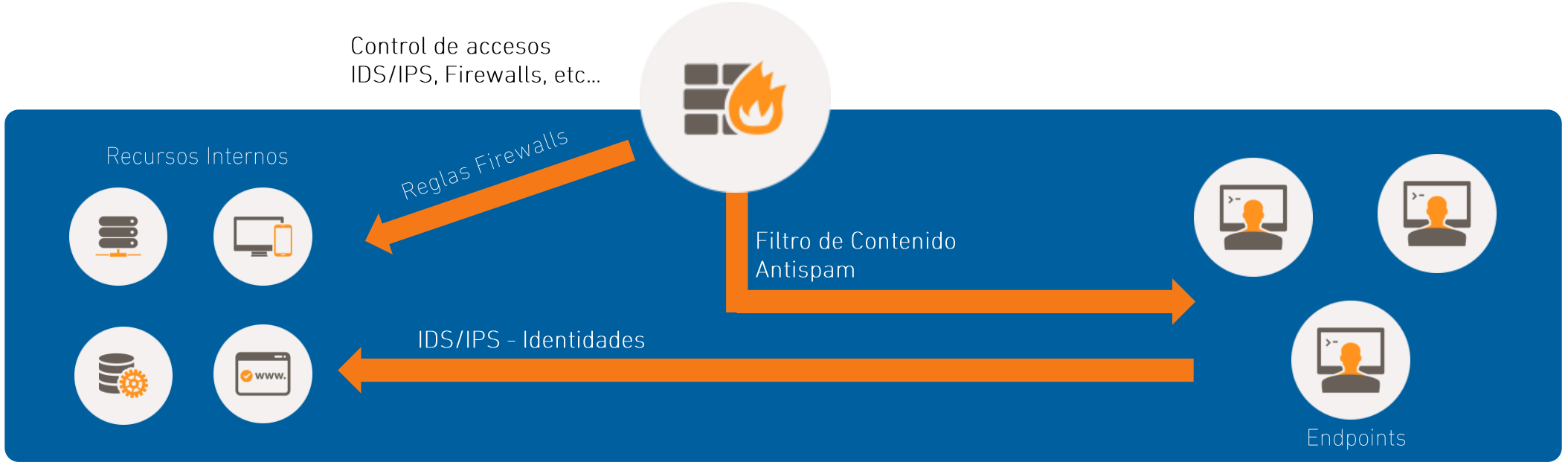
- Investigador de Ciber amenazas
- Consultor en Ciberseguridad
- Colaborador en Seguridad Informática Chile
- Certificado CEHv8
- Especialista Senior en ENTEL CyberSecure

- Habilidades:
  - Hacking a Infraestructuras fullstack
  - Hacking de Sitios Web
  - Scripting en Python

@mdiazcl

Hablemos del panorama de seguridad

Enfoque Tradicional



Componentes de la
seguridad tradicional

Infraestructura o "cajas"

- Antivirus
- Firewalls (L3 – L7)
- Filtro de Contenido
- IDS/IPS
- Data Loss Prevention
- AntiMalware
- Etc...

FIRMAS

Gestión

- Vulnerabilidades
- Pentesting
- Accesos e Identidades
- Parches y Hardening
- Eventos
- Incidentes
- Consultoría
- Normativas
- Etc...

CASOS DE USO

Enfoque pasivo de la ciberseguridad

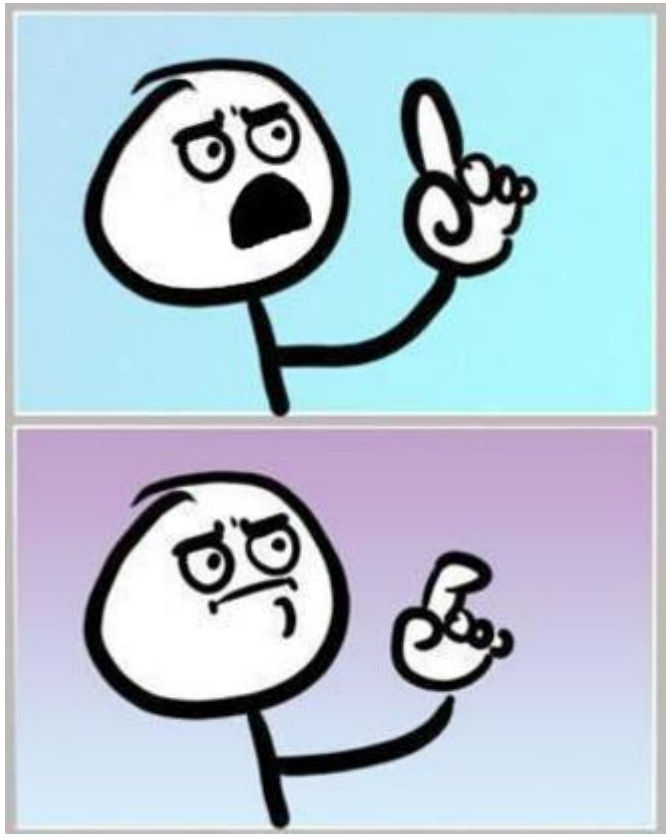
Antecedentes

- 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 disponble, struts2)
  - Suena wanna-cry?
- Deloitte – 2017
  - Clientes afectados: Gobierno USA, Naciones Unidas y Multinacionales
  - Robo de credenciales
  - Falta de controles

Las empresas están perdiendo frente a los ataques dirigidos

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)

Threat Hunting y como apoya a la seguridad tradicional

¿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 dejan las herramientas de seguridad.

Comencemos...

Conceptos clave

Threat Hunting

Como funciona la seguridad tradicional?

- Hashes maliciosos
- Listas negras de IP
- Listas negras de dominio
- Listas negras de emails
- Depende en su mayoría del vendor
- ....

Indicadores De compromiso

Como funciona el Threat Hunting?

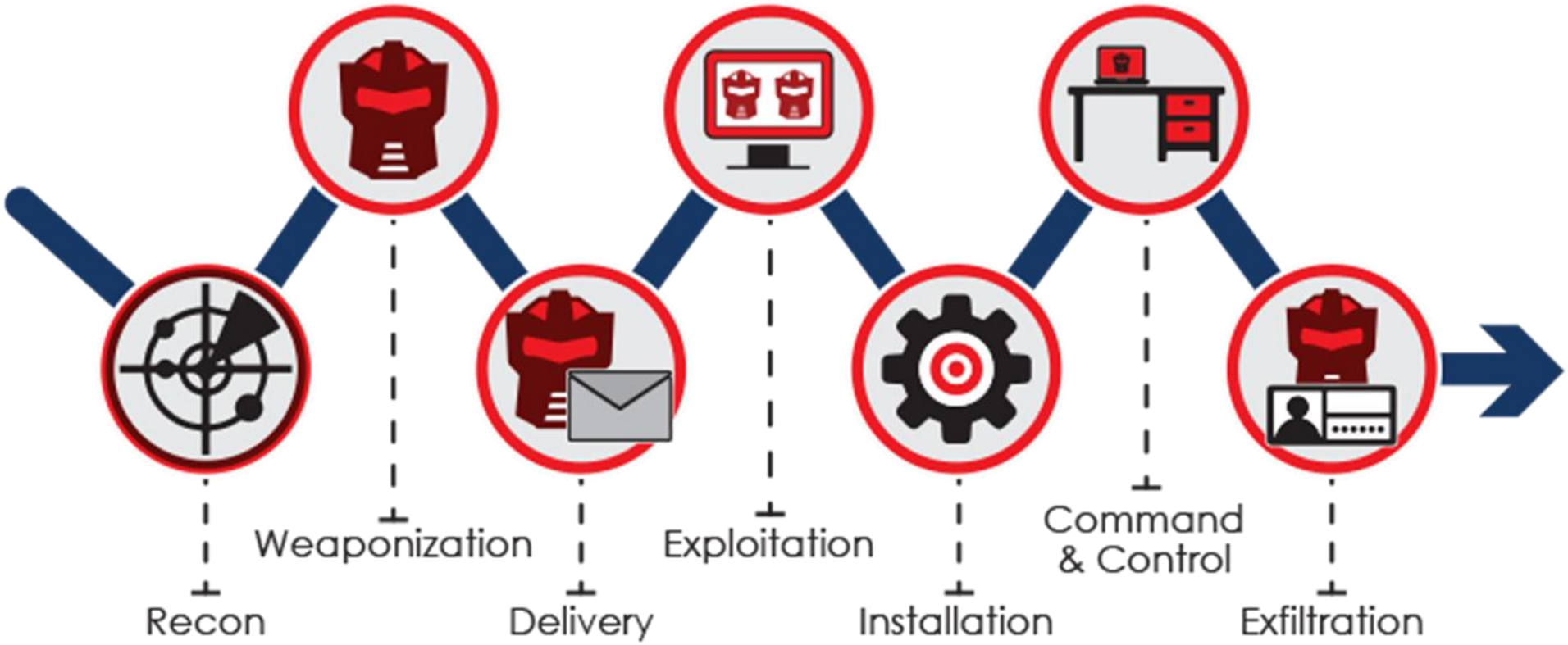
- Detección de lo **anormal****
- Asumir que ya hemos sido hackeados
- Levantar **visibilidad** y conocimiento
- Proactividad e investigación
- Fuerte alineamiento con el **negocio**
- Fuerte componente de Software
- Permanente **colaboración**
- ***Detectar ciberataques en progreso***

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.

Cybersecurity - Kill Chain

Diseccionando un ciberataque – Lockheed Martin

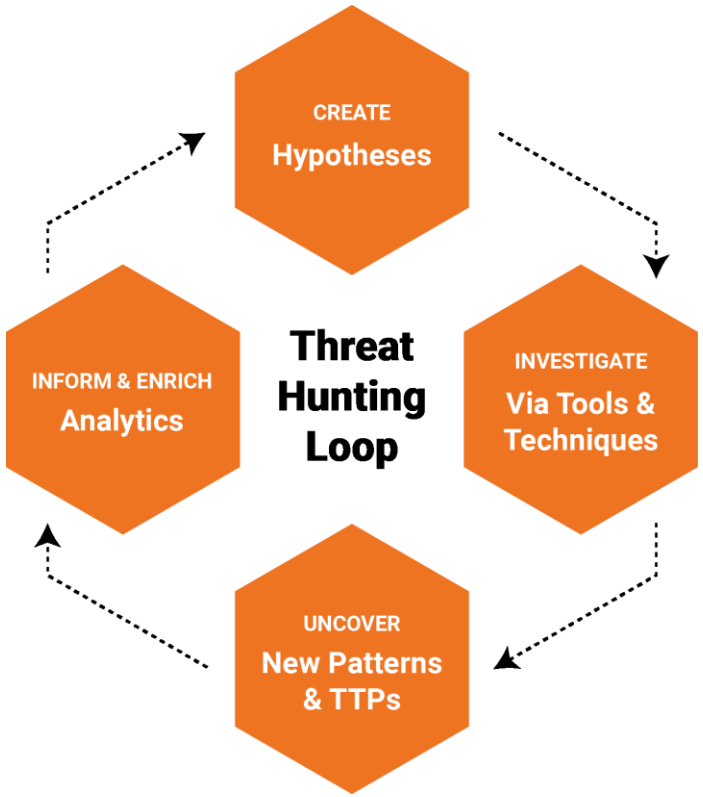


Source:
https://www.eventtracker.com

Como cazar estas amenazas

Como funciona?

Modelo de Threat Hunting



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

Crear una hipótesis

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

Investigar la hipótesis

- Recopilar la información necesaria
- Analizar y detectar

Descubrir patrones

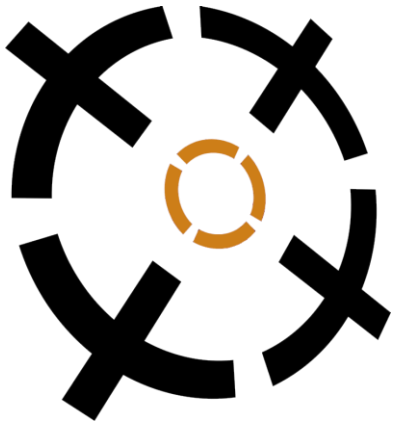
- Validar la hipótesis
- Declarar si existe o no amenaza
- Definir el KillChain

Informar y enriquecer

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

Creación de la hipótesis

Basados en Inteligencia

Powershell en máquinas	Requests DNS (TXT, Query's)	Conexiones de red hacia puertos con rangos extraños	Autenticaciones de usuarios desde IP's desconocidas
Proxy HTTP sitios no categorizados	Alta cantidad de conexiones únicas	Conexiones entre hosts extrañas	Accesos a FileServers fuera de lo común
	Navegación web excesiva	User Agents	Autenticaciones de usuarios desde IP's desconocidas

Técnicas para realizar

Investigación y Tratamiento de amenazas

Recolectar información

- Logs de eventos
- CMDBs
- Procesos de negocio
- Fuentes Externas (Threat Intelligence)

Procesar la información

- SIEM
- Análisis de Logs
- Herramientas de Visualizacion

Detección

- Análisis estadístico
- Análisis histórico
- Correlación de eventos

Notificación

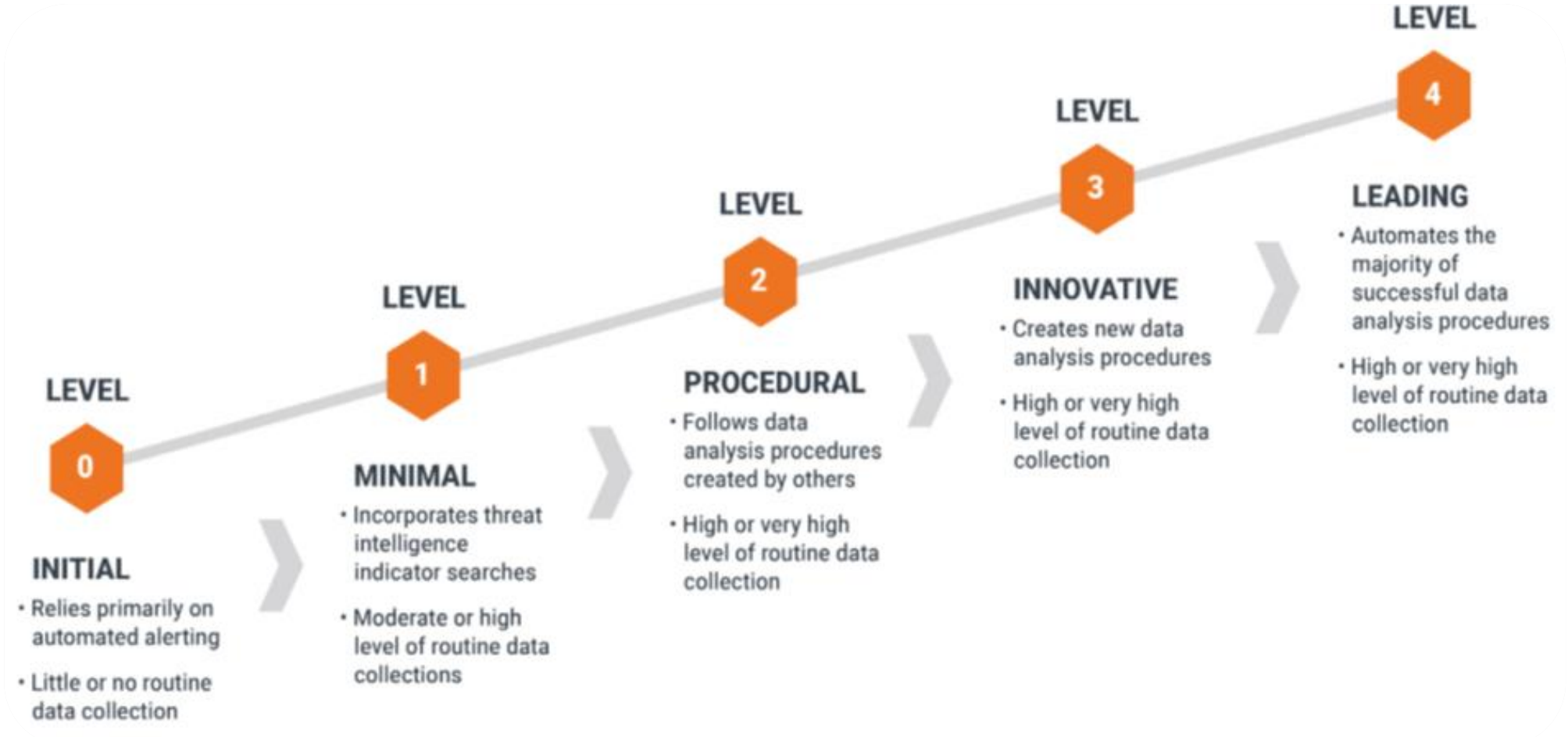
- Nuevos IoC / TTPs
- Alarmas de Seguridad
- Mejoras en la herramientas de seguridad

Principales fuentes de información

- Netflow
- Logs de aplicaciones
- Logs de máquinas de seguridad
- Eventos de sistemas operativos

Niveles de madurez

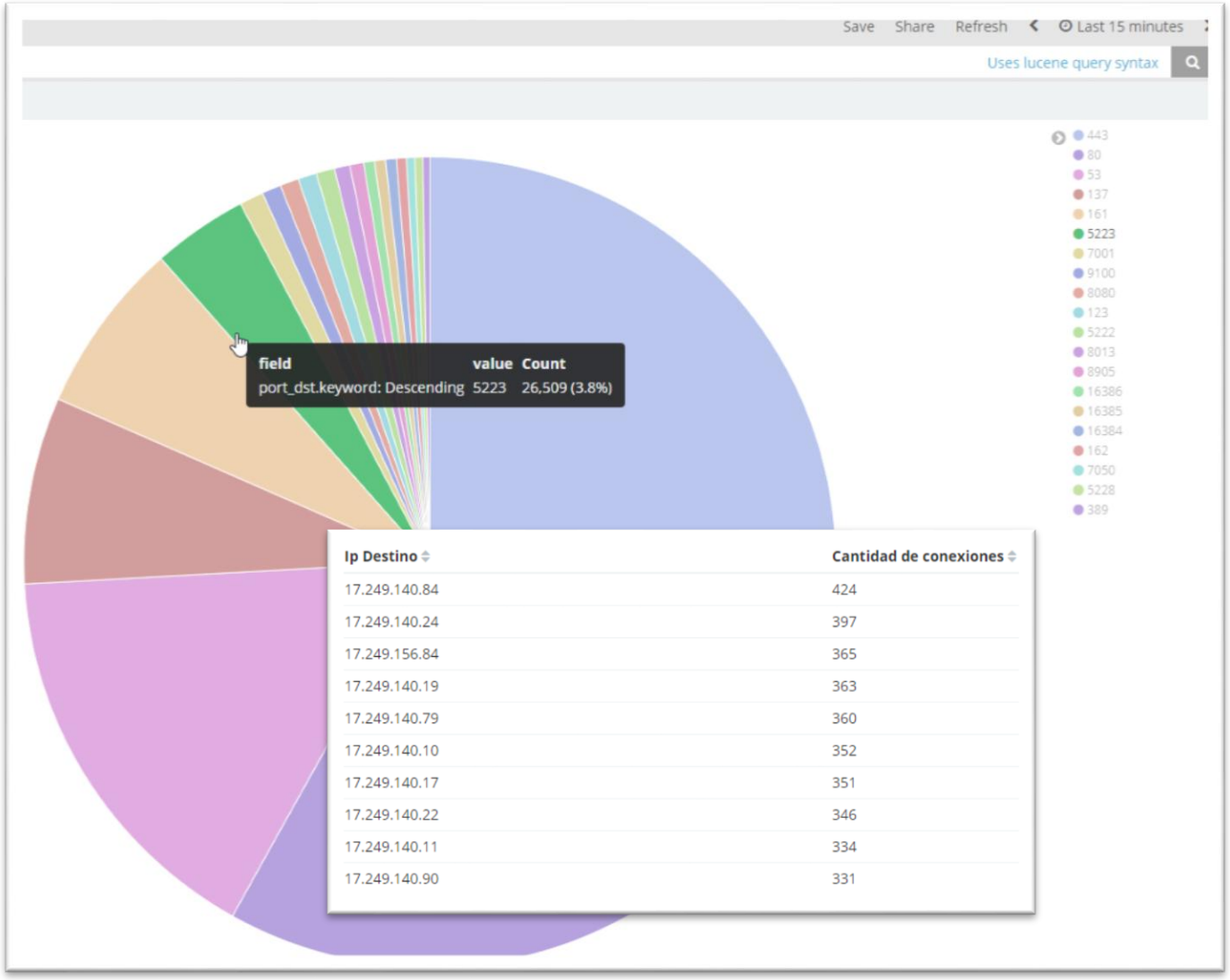
Cazando de 0 a 100



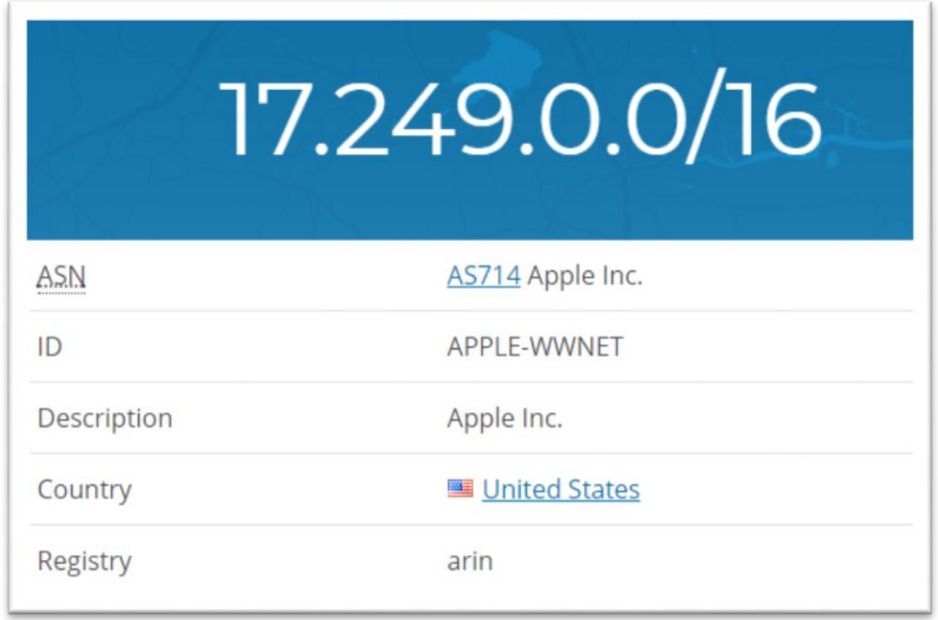
Modelo de Madurez
Source: https://sqrrl.com

Un caso simple

Basado en la hipótesis de puertos abiertos



Ip Destino	Cantidad de conexiones
17.249.140.84	424
17.249.140.24	397
17.249.156.84	365
17.249.140.19	363
17.249.140.79	360
17.249.140.10	352
17.249.140.17	351
17.249.140.22	346
17.249.140.11	334
17.249.140.90	331



¿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 desaparescan.
  - Los CISOs están presionados por demostrar que sus empresas son seguras.

La experiencia de cazar

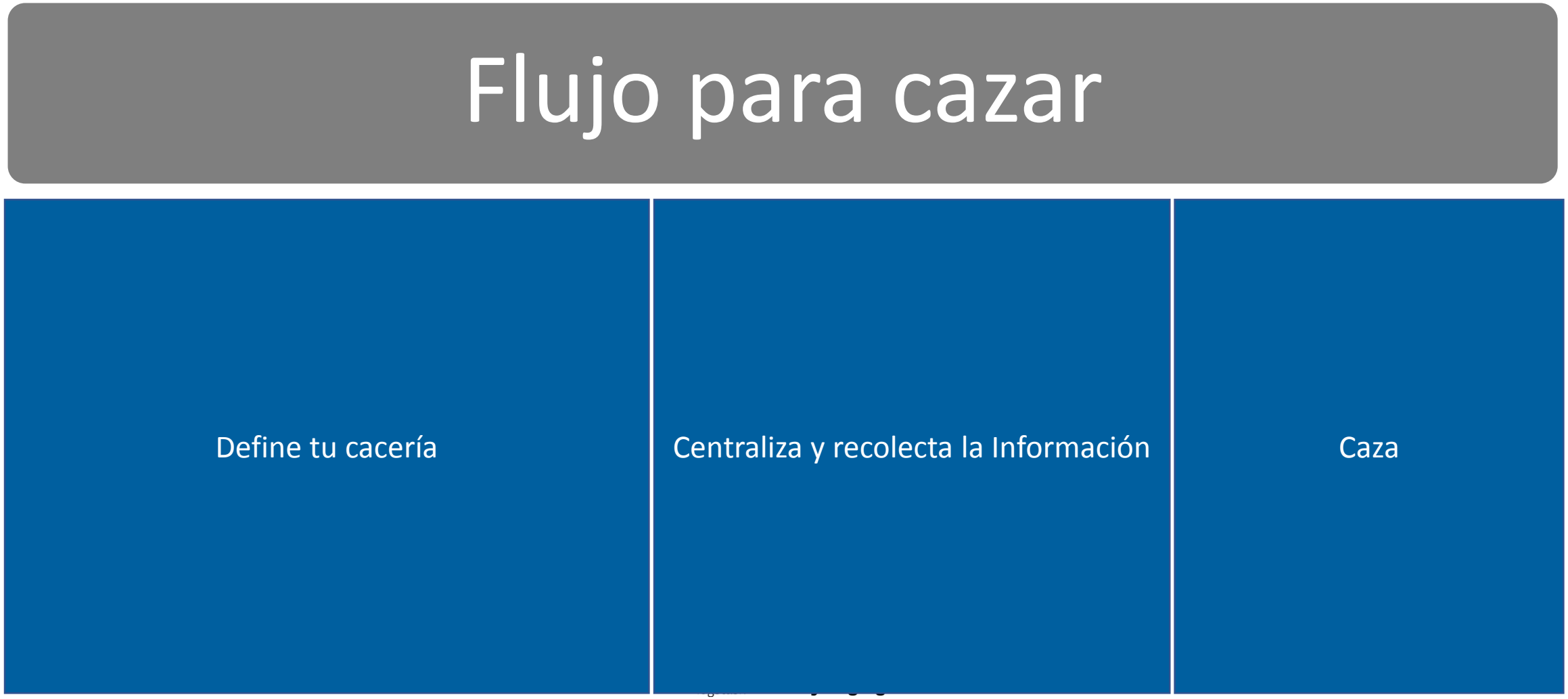
Lo que me ha ocurrido en estos 6 meses

- Negación de las herramientas
- Aceptación de las herramientas
- Fricción con algunas áreas TI
- Mucha, pero mucha programación
- Limitantes de Hardware/Software
- Toneladas de logs (parseo!)
- Normalización de los logs!
- Frustración durante la caza
- Falta de información (Threat Intelligence)
- Mucha, mucha lectura
- Difícil de explicar a la gerencia
- Es una visión de riesgo, no una visión de operación TI

¿Cómo comenzar?

Cómo comienzo?

Definiendo una cacería opensource



Consideraciones importantes

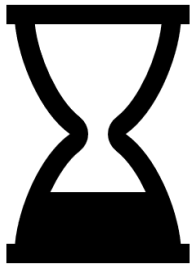
de una buena cacería

El Threat Hunting es una búsqueda iterativa

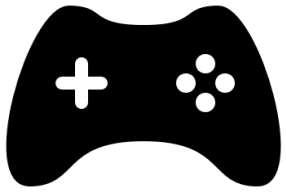
Requiere conocimiento específico en un área

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)