

Una visión proactiva de ciberdefensa



Miguel Díaz Lira, Ingeniero
Experto en Ciberseguridad



| CHILE

About: Miguel Díaz

- » Investigador de Ciberamenazas en tiempo libre
- » 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
 - > Ex-desarrollador de software



CHILE



Agenda

- » **Contexto:** Panorama de Ciberseguridad
- » Enfoques de Ciberseguridad
- » Visión proactiva
- » Cierre



| CHILE

Panorama de ciberseguridad 2019



| CHILE



Las grandes empresas están siendo afectadas



*MR: Millones de registros



Revisemos un par de casos

<https://www.zdnet.com/article/marriott-ceo-shares-post-mortem-on-last-years-hack/>
<https://www.zdnet.com/article/us-government-releases-post-mortem-report-on-equifax-hack/>



3 Años

- Se dieron cuenta el **8 de Septiembre 2018** (notificado por un tercero)
- Un “**query gigantesco**” alertó a la base de datos
- **10 de Septiembre** traen una empresa externa para **hacer el forense**
- Demoraron **1 semana** en encontrar un **equipo infectado con RAT**
- En octubre encontraron **evidencias de Mimikatz**
- **En noviembre** se dieron cuenta que los **hackers estaban dentro desde el 2014**
- **19 de Noviembre** finalmente encuentran evidencia de que se robaron la información.
- **500 millones de registros robados!**

- El 8 de marzo del 2017 se publica el CVE-2017-5638 (**RCE en Apache Struts**)
- **Equifax comunica** sobre la importancia del parchado, pero no les llega a todos (mail-lista estaba desactualizado).
- **El 10 de Marzo detectan** que uno de sus **servidores fue hackeado**, pero no se robaron nada.
- Luego de un scan masivo, el **servidor comprometido ya no aparece como vulnerable**.
- **El 13 de mayo**, los atacantes **comienzan a extraer información** sin ser detectados.
- **No fueron detectados** ya que el dispositivo que tenía que analizar no estaba revisando tráfico encriptado (**por que el certificado expiró**).
- El 30 de Julio dan de baja el servidor infectado, declarando incidente el 8 septiembre.
- **145.5 millones de registros robados** (y uno de los breaches más caros existentes).



76 días



Y la lista sigue...

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]
Mauritius International	2010	500,000,000	hotel	hacked	[183][184]



CHILE



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



Ganancias del Cibercrimen

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

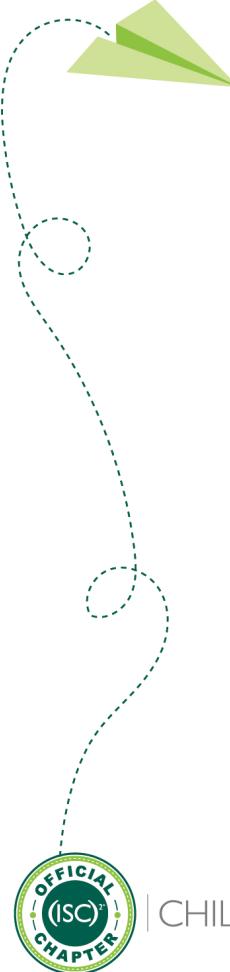
- Investigator Dr. Michael McGuire (2018)

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



CHILE



Algunos puntos clave que he rescatado con el tiempo

- » Los atacantes se preparan para evadir la seguridad tradicional.
- » Es imposible tener un control total de lo que ocurre, por lo que hay que ser estratégico.
- » El cambio tecnológico es más rápido que cualquier otro proceso de seguridad y el vendor no trabajará para ti.
- » Las herramientas de seguridad tienen sus “areas grises” y es importante identificarlas.
- » Es definitivamente un buen negocio.

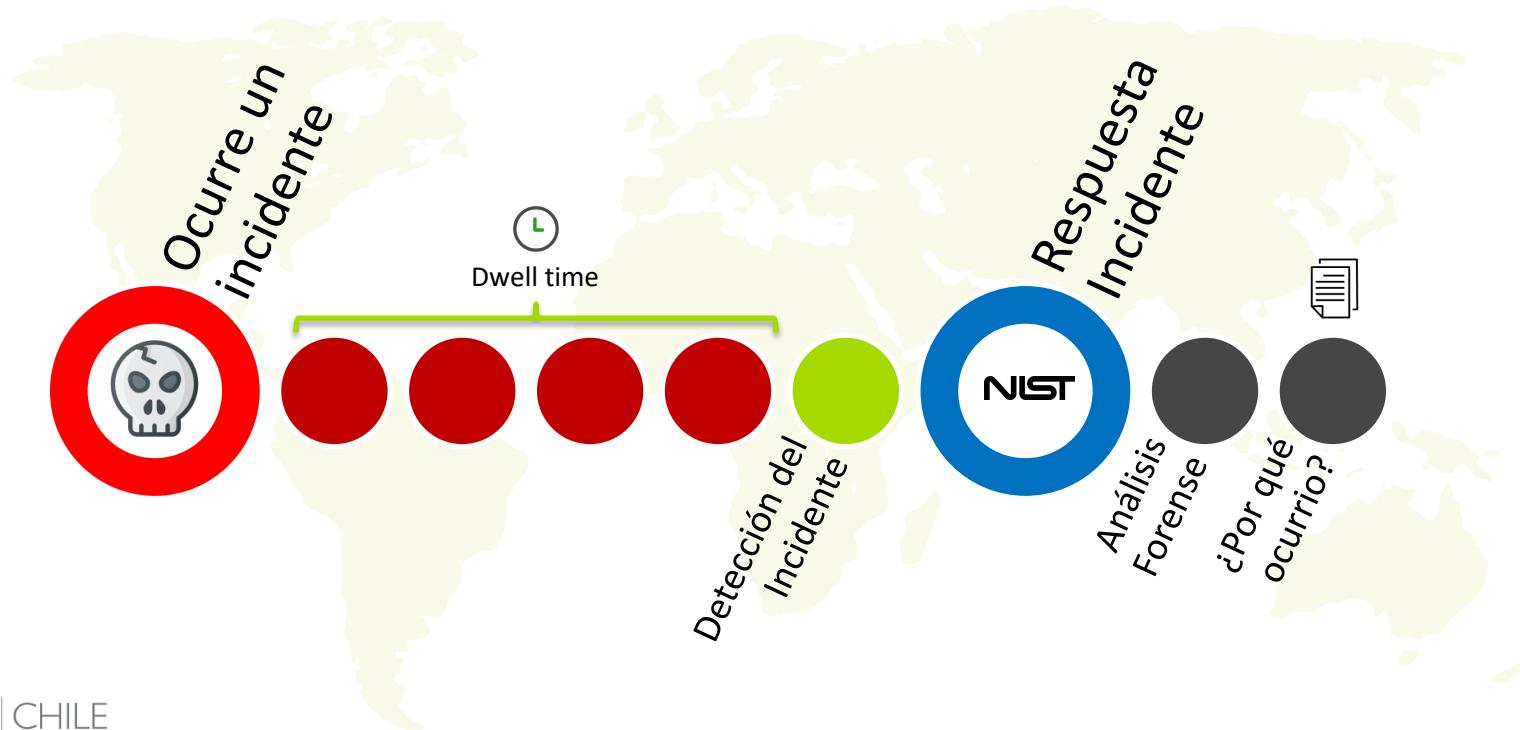


| CHILE

Estructura de un incidente



Línea de tiempo de un Incidente

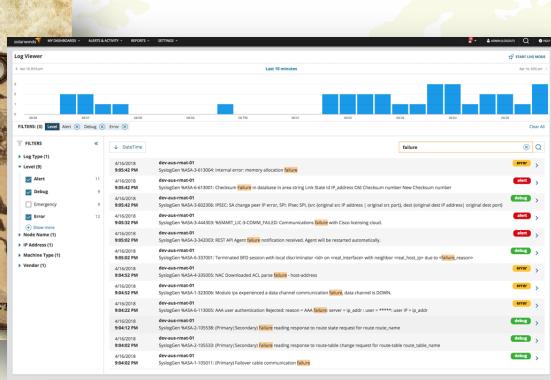




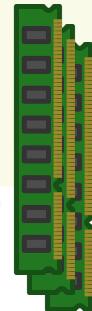
¿Qué se suele buscar durante una respuesta?



Análisis
artefactos
hosts



Análisis de Logs
de red, DNS y
ActiveDirectory



Análisis
dinámicos
de memoria



Cualquier
otra pieza
que sirva



| CHILE

Una pregunta: ¿y si vamos a buscar los incidentes antes que ocurran?

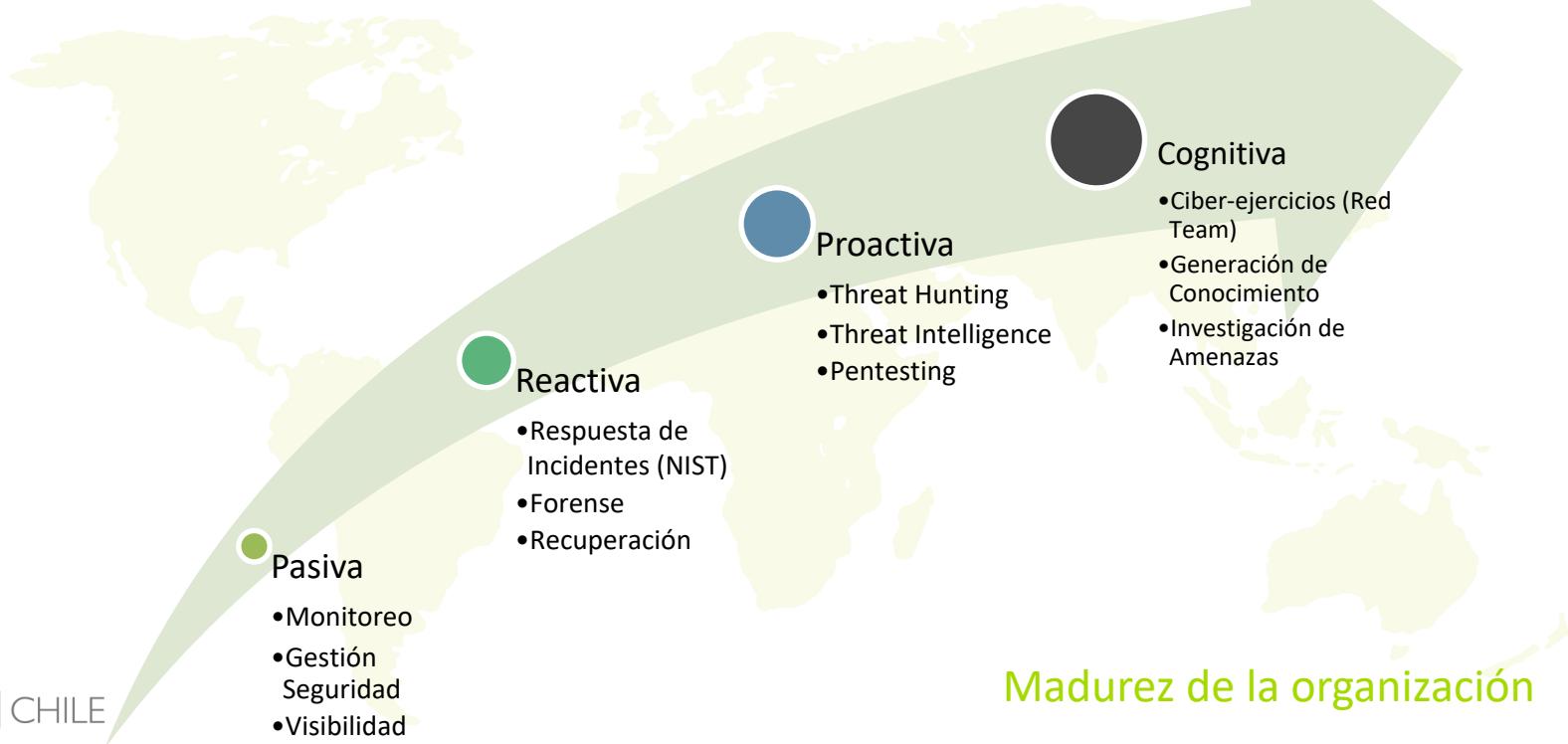


| CHILE

Evolución de Ciberdefensa



La evolución de la ciberdefensa



CHILE

Enfoque Proactivo



La postura proactiva nos presenta tres desafíos

THREAT
HUNTING



THREAT
INTELLIGENCE



PENTESTINGS



CHILE

1) Threat Hunting



Definición Threat Hunting

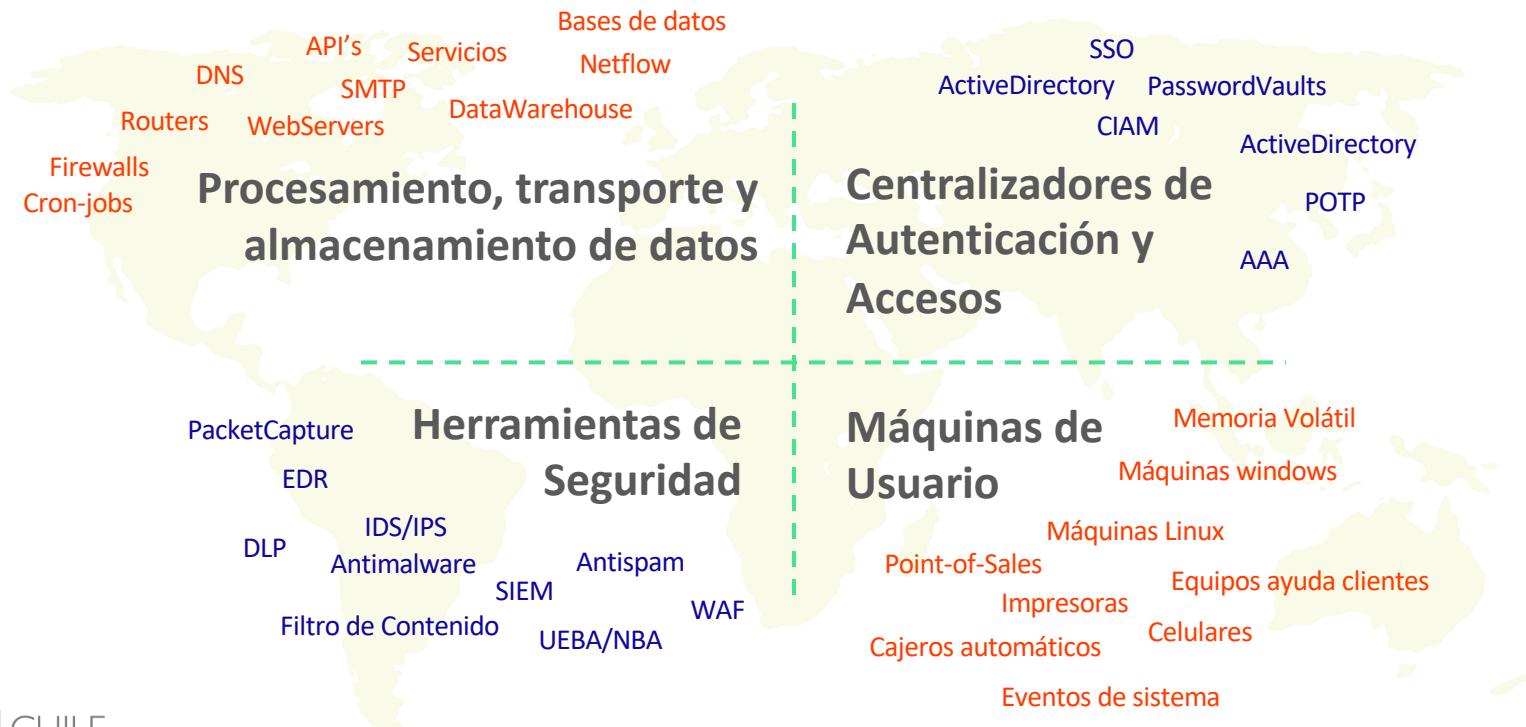


El proceso **proactivo e iterativo** de búsqueda de amenazas en la organización, asumiendo que **un atacante ya ha vulnerado** las medidas de seguridad implementadas.

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



¿Dónde participa?



CHILE



| CHILE



Fundamentos de hunting

Entender como funciona una intrusión.



Identificar información disponible



Entender ciclo de hunting



Herramientas y Coordinación entre áreas



Ejecución periódica estilo auditoria...

2) Threat Intelligence



Definición Threat Intelligence



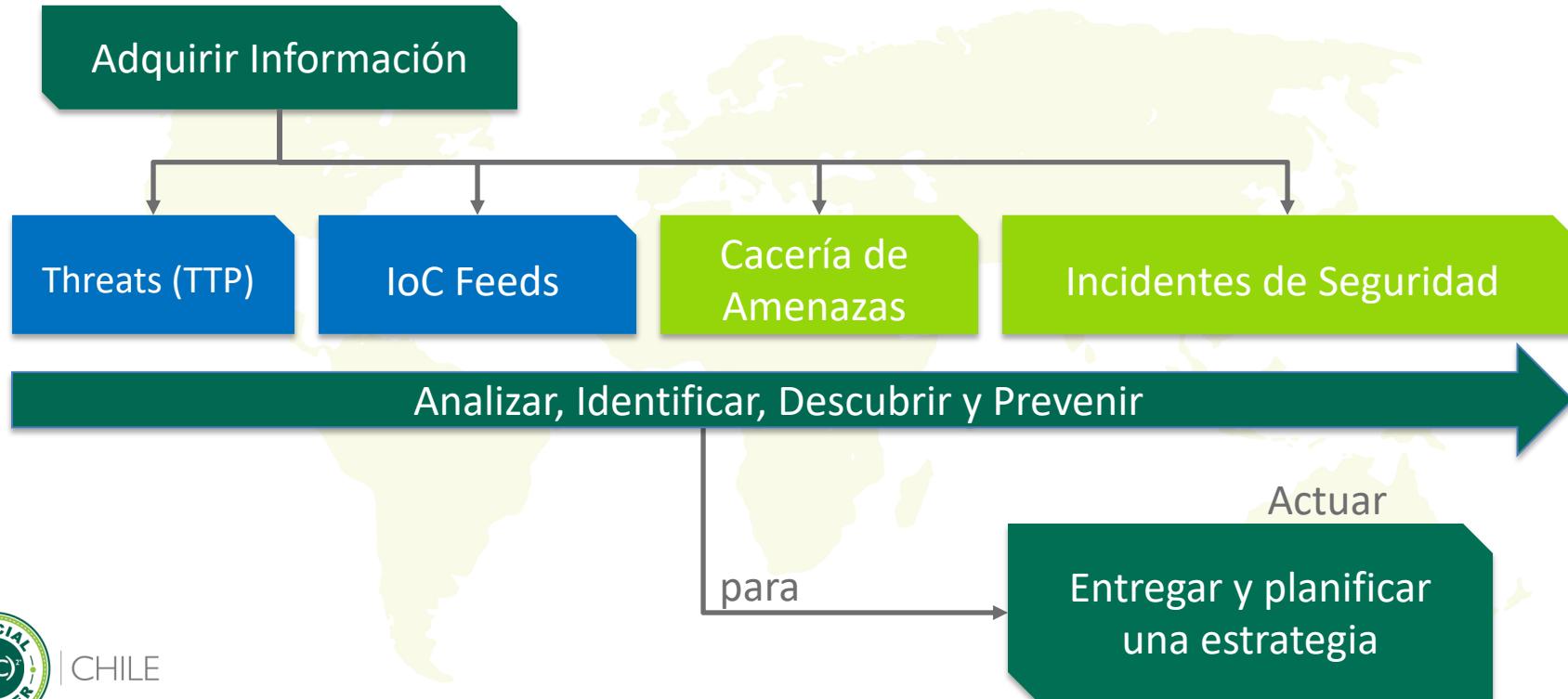
Es la capacidad que **permite adquirir, analizar, identificar y rastrear información** para gestionar medidas de protección **preventivas** y mejorar las **detectivas**.

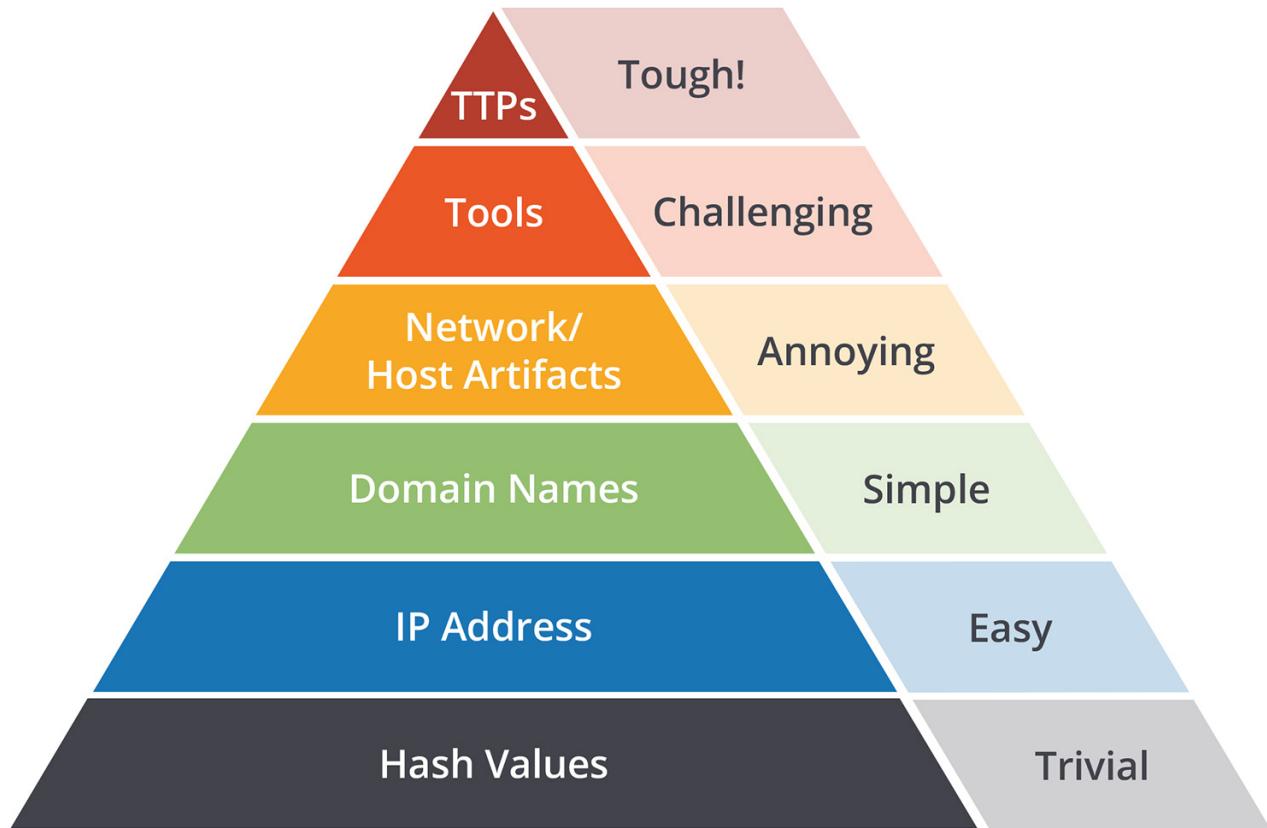
Threat Intelligence permite obtener y aplicar analíticas de comportamiento, mecanismos e indicadores de compromiso para prevenir y detectar ciberataques.

Fuente: Advancing Cyber Intelligence Practices
https://www.youtube.com/watch?v=S_W3pRNuXss



Modelo de Threat Intelligence

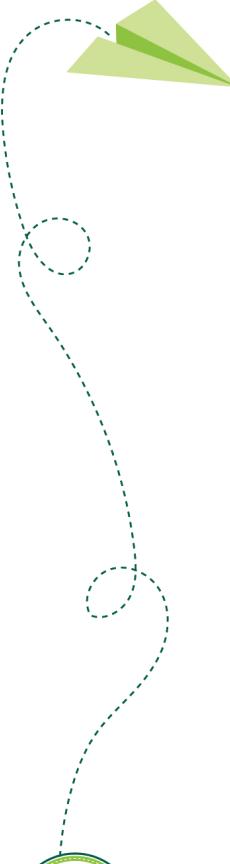




Source: David J. Bianco, personal blog



| CHILE



¿Dónde participa?

Nuevos vectores
de ataque

Gestionar los riesgos

Inteligencia sobre
herramientas

Apoyo en la toma de
decisiones

Conocimiento interno
de la organización

Descubrir APT

Apoyo estratégico en la
resolución de incidentes



| CHILE

3) Pentesting



Definición Pentesting



Es la **simulación de un ciberataque** real a la organización por un grupo de **hackers éticos** que tienen un **objetivo claro**.

Pentesting permite comprobar el nivel de preparación de la organización para detectar, responder y prevenir un ciberataque.



Conceptos importantes a considerar

- NO ES UN ANÁLISIS DE VULNERABILIDADES
- ES UN PROCESO MANUAL CON AUTOMATIZACIÓN
- LA CAJA NEGRA VS LA CAJA BLANCA
- LAS VULNERABILIDADES NO SOLO SON TECNOLÓGICAS
- DEBE EVALUAR LA CAPACIDAD DE DEFENSA, NO LA TECNOLÓGICA
- DEBE SER ENFOCADO EN LA ORGANIZACIÓN
- DEBE SER PERIÓDICO Y CON SEGUIMIENTO



CHILE



Es bueno hacer un pentesting, suele abrir presupuestos y entregar sensibilidad al tema de ciberseguridad.

Pero uno debe estar preparado como organización para solicitarlo.

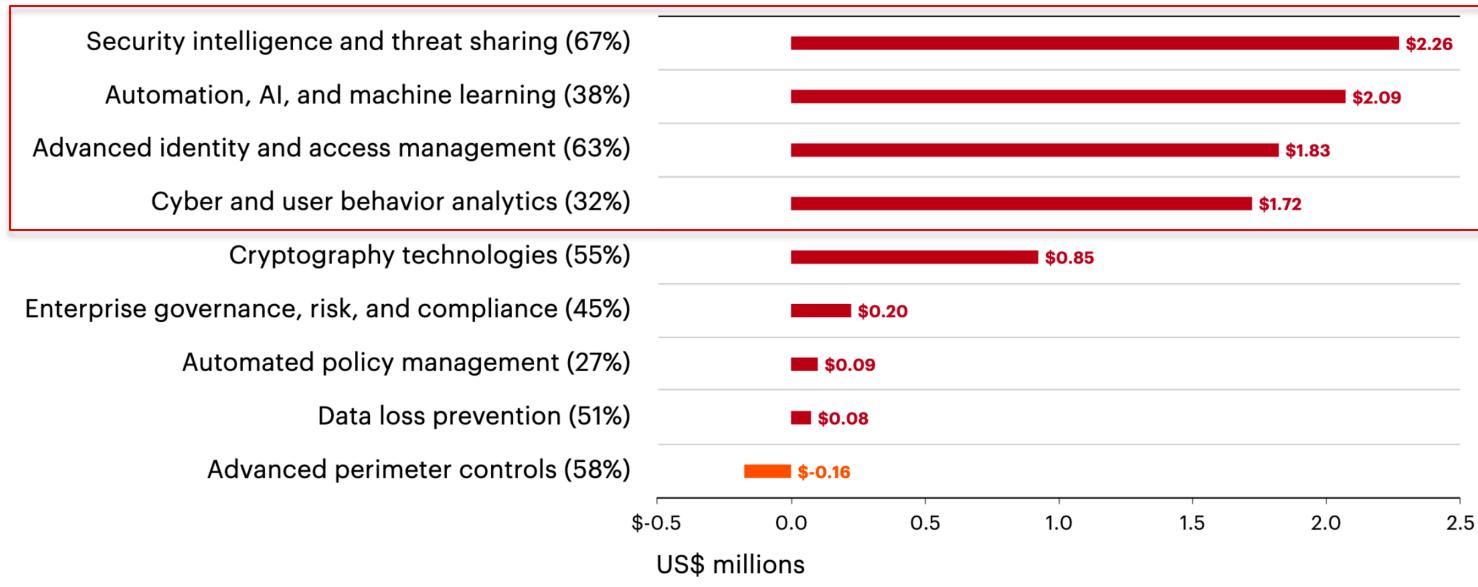


| CHILE

Resumiendo

Inversión neta en Ciberseguridad

Net technology savings
(Total technology savings minus total technology spend)



CHILE

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



Analizar la capacidad y construir desde ahí...

Pasivo

- Monitoreo
- Gestión Seguridad
- Visibilidad

Proactivo

- Threat Hunting
- Threat Intelligence
- Pentesting

Reactivo

- Respuesta de Incidentes (NIST)
- Forense
- Recuperación

Cognitivo

- Ciber-ejercicios (Red Team)
- Generación de Conocimiento
- Investigación de Amenazas



CHILE

Palabras finales

- » No basta con ganar batallas si no estamos avanzando en la guerra, ataquemos el 80/20!
- » El camino puede parecer abrumador, pero se puede ir avanzando por etapas.
- » **Hunting:** Los controles de seguridad son tan importantes como la inteligencia y análisis experto detrás de ellos!
- » **Intelligence:** El estudio de lo que está ocurriendo permite prevenir potenciales ciberataques y detectar nuevos riesgos.
- » **Pentesting:** Evaluar la capacidad de defensa permite descubrir y mejorar la falencia en los sistemas de implementados (no sólo tecnológicos).



| CHILE

Invitación de Cierre

- » Identificar el grado de madurez de la organización.
- » Revisión de los controles CIS, por último para comparar!
- » Realizar Threat Huntings y Pentestings de forma periódica en la organización.



| CHILE