

Threat Hunting:

Enfoque proactivo de
ciberdefensa



e) corp

mdiazcl ~ \$: whoami

- Investigador de Ciberamenazas
- Security Advisor Entel Cybersecure Perú
- 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
 - Ex-desarrollador de software



Panorama de Ciberseguridad 2019

Casos de Brechas

Las grandes empresas están siendo afectadas



2 casos interesantes

Para discutir

<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/>



- 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 ven evidencia de hackeo.
- 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 expiro**).
- El 30 de Julio dan de baja el servidor infectado, declarando incidente el 8 septiembre.
- **145.5 millones de registros robados**



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



Realidad frente a los ciberataques

Encontré 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 y el vendor no trabajará para ti.

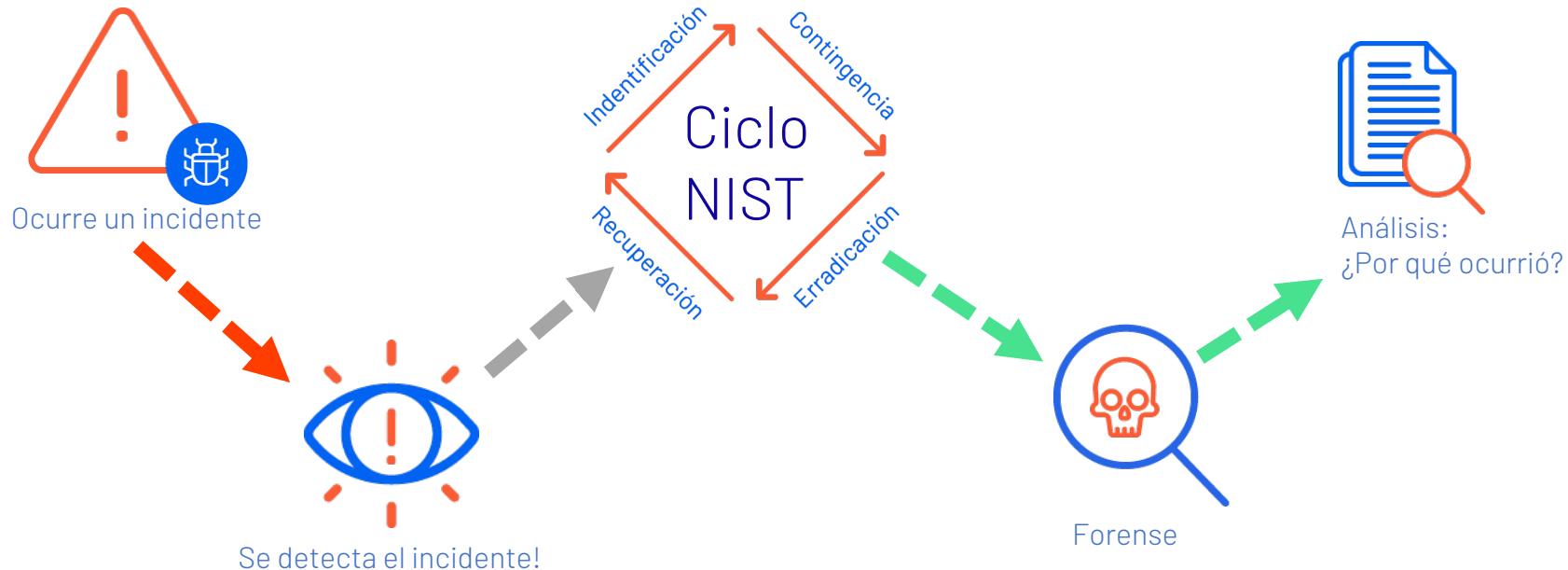
Las herramientas de seguridad tienen grietas y no son capaces de proteger de forma íntegra



Hablemos
de la respuesta
al incidente

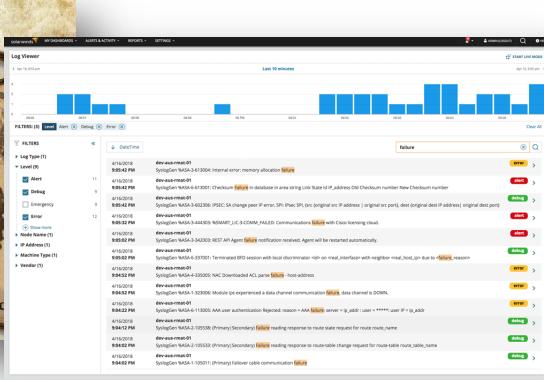
Línea de tiempo de un IR

Simplificada



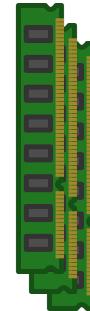
Forense post-respuesta

Etapa de Análisis Forense



Análisis
artefactos
hosts

Análisis de Logs
de red, DNS y
ActiveDirectory



Análisis
dinámicos
de memoria

Cualquier
otra pieza
que sirva

Finalmente buscamos huellas de qué fue lo que pasó!

**“¿Por qué tenemos que esperar a que
haya un incidente... para ir a cazarlo?”**

Threat Hunting

¿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 que dejan las herramientas de seguridad.

Postura de ciberseguridad

SEGURIDAD
TRADICIONAL

PASIVO

INCIDENT
RESPONSE
TEAM

REACTIVO

THREAT
HUNTING

PROACTIVO

Hablemos
de hunting!

Vamos a repasar los siguientes tópicos

- 1. Fundamentos de Threat Hunting**
- 2. Ejemplos de una cacería**
- 3. El perfil del hunter**

1. Fundamentos de Threat Hunting

Cuatro pilares fundamentales

Entender como
funciona *una intrusión*



Identificar *información*
y *herramientas*
disponibles



Entender *ciclo*
de hunting

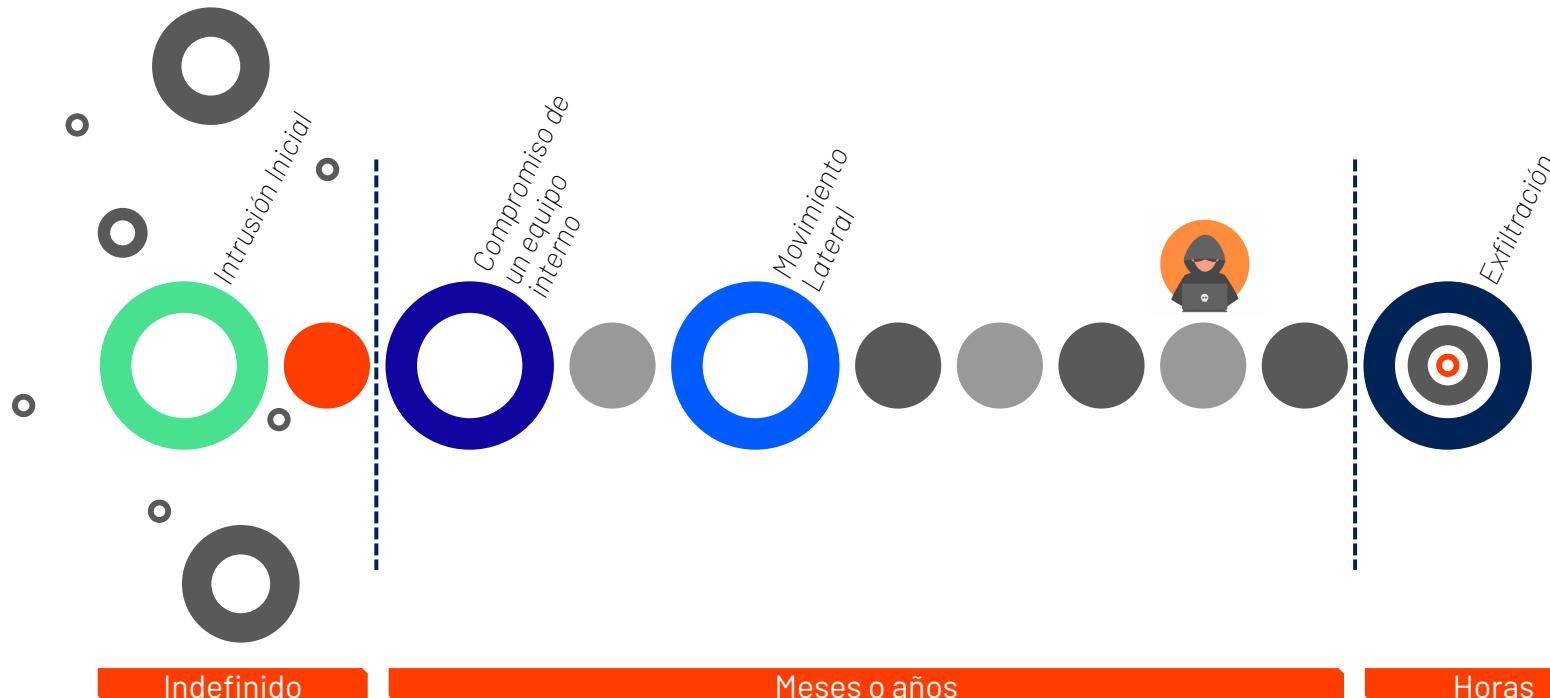


Herramientas y
Coordinación
entre áreas



Como podría ser una intrusión

Línea de tiempo de una intrusión



Indefinido

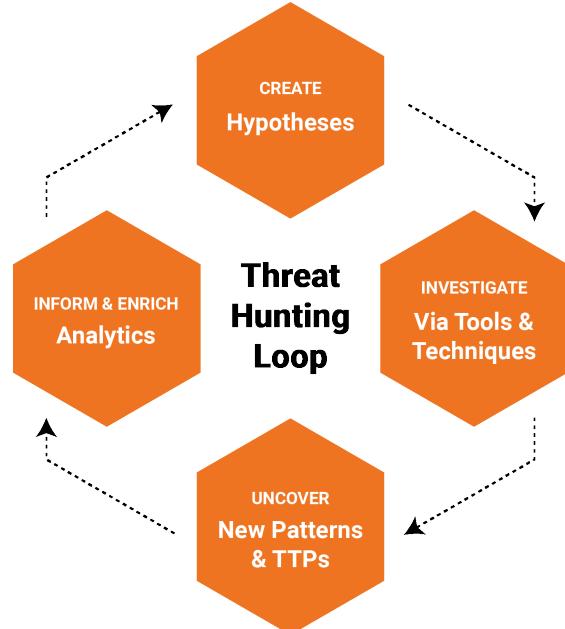
Meses o años

Horas

Identificar información disponible



Ciclo de 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

Mindset del Hunter

“No tengas miedo a equivocarte... Caza rápido, descarta pronto ya que no hay peor cacería que la que no se realiza”

Herramientas y Coordinación entre áreas



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 (*)

Adicional a las herramientas es fundamental tener **coordinación entre áreas!**

Esto permitirá enfocar mejor las búsquedas y descartar rápidamente falsos positivos.

2. Ejemplos de una cacería

Algunas ideas

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

Invitación a cacerías locales

Cazando Webshells

Una webshell es un trozo de código que se inyecta en un sitio web para tomar control de la máquina que hostea el sitio.

Muy común en penetraciones perimetrales!

- **Hipótesis:** Utilización de un Webshell en un webserver
- **Información a recolectar:**
 - Historial de procesos del servidor
 - Evento 4688 si es un IIS (creación de nuevo proceso)
 - Access log del servidor
- **Comportamientos observables:**
 - Alta cantidad de peticiones desde una misma fuente
 - URLs "semi-únicas" en un path
 - URLs que contienen comandos de Linux / Windows
 - Base64 presente en la URL
 - Creación de archivos comprimidos en el servidor.
- **Técnicas de Análisis**
 - Procesamiento estadístico de logs (GoAccess, ELK)
 - Análisis visual de procesos en el sistema

Export: Raw [Raw](#) Formatted [Formatted](#)

Response Codes

Top 20 response Q	Count d
200	143,837
304	7,706
404	827
301	633
206	162
302	69
405	24
400	?

Temporary Redirects

Top 5 response Q	Top 10 request Q	Count d
302	/wp-admin/	14
302	/wp-admin/options.php	12
302	/wp-admin/post.php	12
302	/wp-login.php	11
302	/wp-signup.php	8
302	/wp-admin/admin.php	6
302	/wp-admin/user-edit.php	4
302	/wp-admin/admin.php?screen=wp-rrr&post=1778	1

5XX Responses

No results found

Real-Time Website Visitor Distribution

Legend [Q](#)

- 200
- 304
- 404
- 301
- 206
- 302
- 405
- 400
- 403
- 402
- 401
- 406
- 407
- 408
- 409
- 410
- 411
- 412
- 413
- 414
- 415
- 416
- 417
- 418
- 421
- 422
- 423
- 424
- 425
- 426
- 427
- 428
- 429
- 430
- 431
- 432
- 433
- 434
- 435
- 436
- 437
- 438
- 439
- 440
- 441
- 442
- 443
- 444
- 445
- 446
- 447
- 448
- 449
- 450
- 451
- 452
- 453
- 454
- 455
- 456
- 457
- 458
- 459
- 460
- 461
- 462
- 463
- 464
- 465
- 466
- 467
- 468
- 469
- 470
- 471
- 472
- 473
- 474
- 475
- 476
- 477
- 478
- 479
- 480
- 481
- 482
- 483
- 484
- 485
- 486
- 487
- 488
- 489
- 490
- 491
- 492
- 493
- 494
- 495
- 496
- 497
- 498
- 499
- 500
- 501
- 502
- 503
- 504
- 505
- 506
- 507
- 508
- 509
- 510
- 511
- 512
- 513
- 514
- 515
- 516
- 517
- 518
- 519
- 520
- 521
- 522
- 523
- 524
- 525
- 526
- 527
- 528
- 529
- 530
- 531
- 532
- 533
- 534
- 535
- 536
- 537
- 538
- 539
- 540
- 541
- 542
- 543
- 544
- 545
- 546
- 547
- 548
- 549
- 550
- 551
- 552
- 553
- 554
- 555
- 556
- 557
- 558
- 559
- 560
- 561
- 562
- 563
- 564
- 565
- 566
- 567
- 568
- 569
- 570
- 571
- 572
- 573
- 574
- 575
- 576
- 577
- 578
- 579
- 580
- 581
- 582
- 583
- 584
- 585
- 586
- 587
- 588
- 589
- 590
- 591
- 592
- 593
- 594
- 595
- 596
- 597
- 598
- 599
- 500+

Response Code Distribution

Legend [Q](#)

- 200
- 304
- 404
- 301
- 206
- 302
- 405
- 400
- 403
- 402
- 401
- 406
- 407
- 408
- 409
- 410
- 411
- 412
- 413
- 414
- 415
- 416
- 417
- 418
- 421
- 422
- 423
- 424
- 425
- 426
- 427
- 428
- 429
- 430
- 431
- 432
- 433
- 434
- 435
- 436
- 437
- 438
- 439
- 440
- 441
- 442
- 443
- 444
- 445
- 446
- 447
- 448
- 449
- 450
- 451
- 452
- 453
- 454
- 455
- 456
- 457
- 458
- 459
- 460
- 461
- 462
- 463
- 464
- 465
- 466
- 467
- 468
- 469
- 470
- 471
- 472
- 473
- 474
- 475
- 476
- 477
- 478
- 479
- 480
- 481
- 482
- 483
- 484
- 485
- 486
- 487
- 488
- 489
- 490
- 491
- 492
- 493
- 494
- 495
- 496
- 497
- 498
- 499
- 500
- 501
- 502
- 503
- 504
- 505
- 506
- 507
- 508
- 509
- 510
- 511
- 512
- 513
- 514
- 515
- 516
- 517
- 518
- 519
- 520
- 521
- 522
- 523
- 524
- 525
- 526
- 527
- 528
- 529
- 530
- 531
- 532
- 533
- 534
- 535
- 536
- 537
- 538
- 539
- 540
- 541
- 542
- 543
- 544
- 545
- 546
- 547
- 548
- 549
- 550
- 551
- 552
- 553
- 554
- 555
- 556
- 557
- 558
- 559
- 560
- 561
- 562
- 563
- 564
- 565
- 566
- 567
- 568
- 569
- 570
- 571
- 572
- 573
- 574
- 575
- 576
- 577
- 578
- 579
- 580
- 581
- 582
- 583
- 584
- 585
- 586
- 587
- 588
- 589
- 590
- 591
- 592
- 593
- 594
- 595
- 596
- 597
- 598
- 599
- 500+

Bots Getting Error Response Codes

Time d	response Q	name	message
December 10th 2015, 06:20:19.351	Slurp		2015-12-10T04:20:19.351803Z production-site-lb 68.180.231.51:54776 172.31.62.236:80 0.000039 0.179046 0.000039 200 200 0 20075 "GET http://production-site-lb-1166584198.us-east-1.elb.amazonaws.com:80/blog/5-logstash-pitfalls-and-how-to-avoid-them/ HTTP/1.1" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/search/slurp)" - -
December 10th 2015, 06:20:19.023	Slurp		2015-12-10T04:20:19.023859Z production-site-lb 68.180.231.51:34989 172.31.62.236:80 0.000038 0.071004 0.000033 200 200 0 35 "GET http://production-site-lb-1166584198.us-east-1.elb.amazonaws.com:80/robots.txt HTTP/1.1" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/search/slurp)" --

4XX Responses

Top 5 response Q	Top 10 request Q	Count d
404	/httpptest.php	87
404	/manager/html	31
404	/index.html	27
404	/index.php	21
404	/index.htm	17

Invitación a cacerías locales

Honeypot

Un honeypot es una máquina especialmente preparada para que el hacker “se tiente” a escanearla o comprometerla.

Cuando lo hace (o intenta), es evidente la intrusión!

- **Hipótesis:** Hacker está en la red y esta buscando máquinas con información.
- **Información a recolectar:**
 - Actividad del Honeypot (ej: cowrie)
 - Logs de servicios vulnerables
- **Comportamientos observables:**
 - Cualquier tipo de interacción de una estación de trabajo o servidor con esta máquina.
 - Actividad SSH, FTP, Carpetas compartidas, etcétera
- **Técnicas de Análisis**
 - Análisis de logs
 - Análisis de tráfico de red

[<https://github.com/Hackinfinity/Honey-Pots->]



3. Perfil del Hunter

Perfil del Hunter

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

Cierre



¿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

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!**

Invitación y literatura



CARBON
BLACK

Google



e) corp