2023 CELAES
Congreso Latinoamericano de Seguridad Bancaria

Un viaje a través del Managed Detection and Response

ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

SOFISTIC
CYBERSECURITY

Agenda

- Introducción a Managed Detection and Response (MDRServicio SOC MDR Sofistic
- Desafíos Actuales en Ciberseguridad
- Los Pilares Fundamentales del MDR
- Beneficios Estratégicos del MDR
- Claves para Implementación Exitosa del MDR
- El Rol de la Inteligencia Artificial y Machine Learning
- Preguntas

¿QUE ES UN MDR?

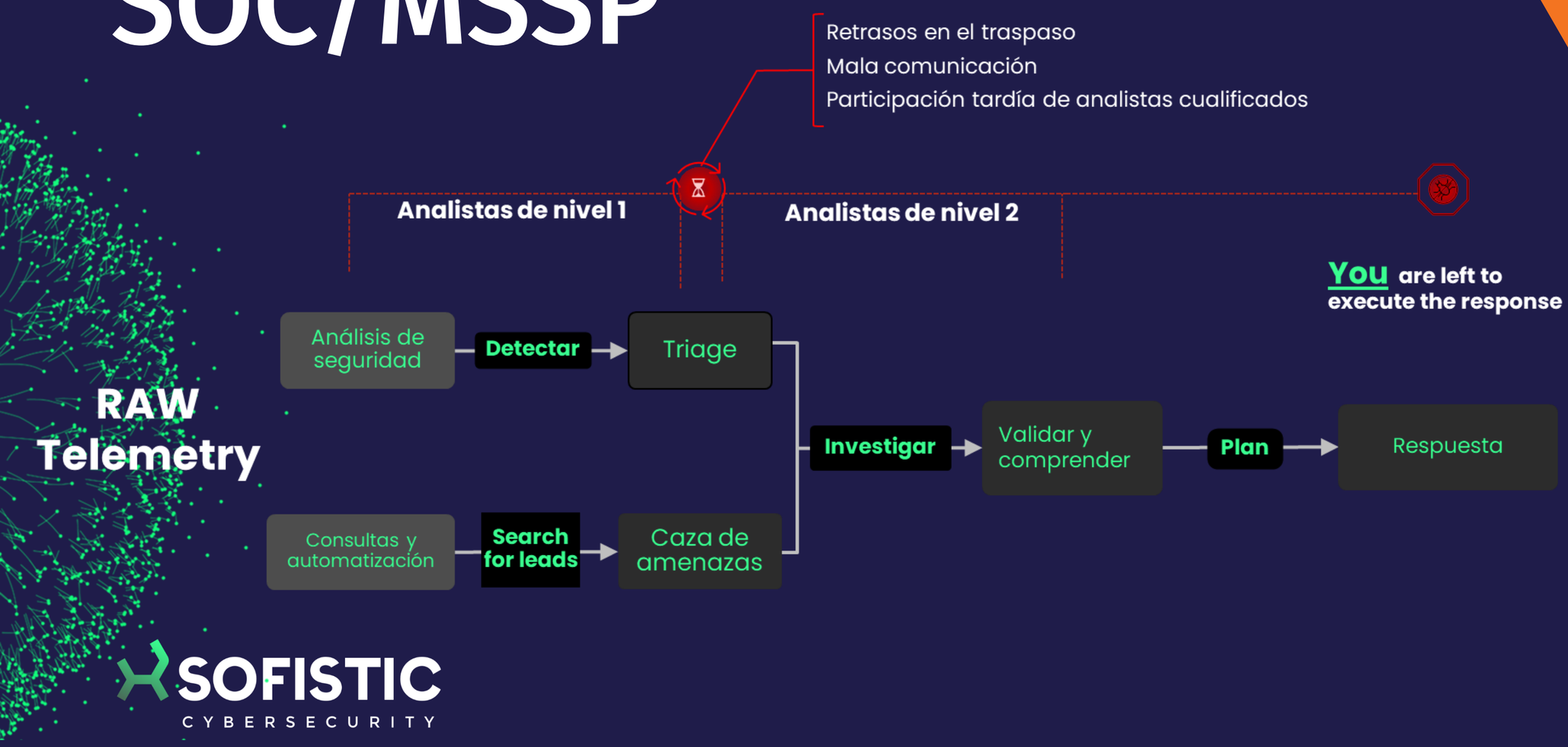
- Servicio administrado de detección y respuesta
- Un servicio provisto por el SOC de forma remota.
- Permite a las organizaciones detectar, analizar, investigar y responde activamente mediante la interrupción y contención de amenazas .

Gartner®

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Flujo de trabajo típico de SOC/MSSP



SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

La situación del sector

CRIME

IFX Networks Cybersecurity Breach: A Stark Reminder of Digital Infrastructure Vulnerabilities

By Salman Khan • 3 weeks ago

Casino giant MGM expects $100 million hit from hack that led to data breach

Reuters
Published 9:40 PM EDT, Thu October 5, 2023

Report: Sony Under Cyber Attack, Ransomed.vc Successfully Breaches Company With Intent to Sell Data

MOVEit, the biggest hack of the year, by the numbers

At least 60 million individuals affected, though the true number is far higher

More than 3.8 billion records exposed in DarkBeam data leak

Billions of login credentials were available online after a database was left unprotected

Add bookmark

Did a Cyberattack Cause the FAA System Outage in January 2023?

Thousands of flights were delayed on Jan. 11, 2023.

By Nur Ibrahim

Updated Jan 12, 2023 Published Jan 11, 2023

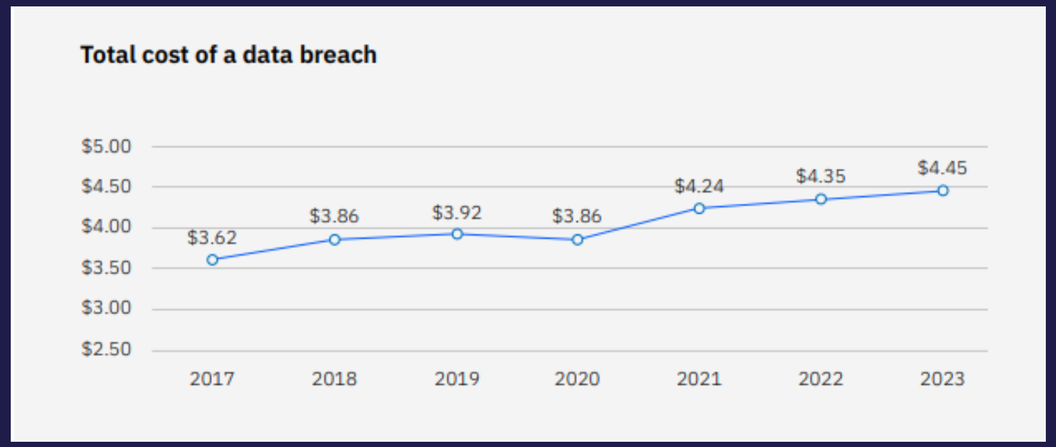
Ransomware Attack Hits Japan's Biggest Port, Delaying Cargo

- Port of Nagoya container terminal suffered outage on Tuesday
- Operations are expected to resume Thursday morning in Japan

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Panorama de amenazas



A nivel mundial, el coste medio de una filtración de datos ascendió a USD 4,45 millones, unos USD 100.000 aumento desde 2022. Esto representa un Aumento del 2,3% respecto al coste medio de 2022 de 4,35 millones de dólares. Desde 2020, cuando el costo total promedio de una violación de datos fue USD 3,86 millones, el costo total promedio ha aumentó un 15,3%.

* Fuente: data breach report

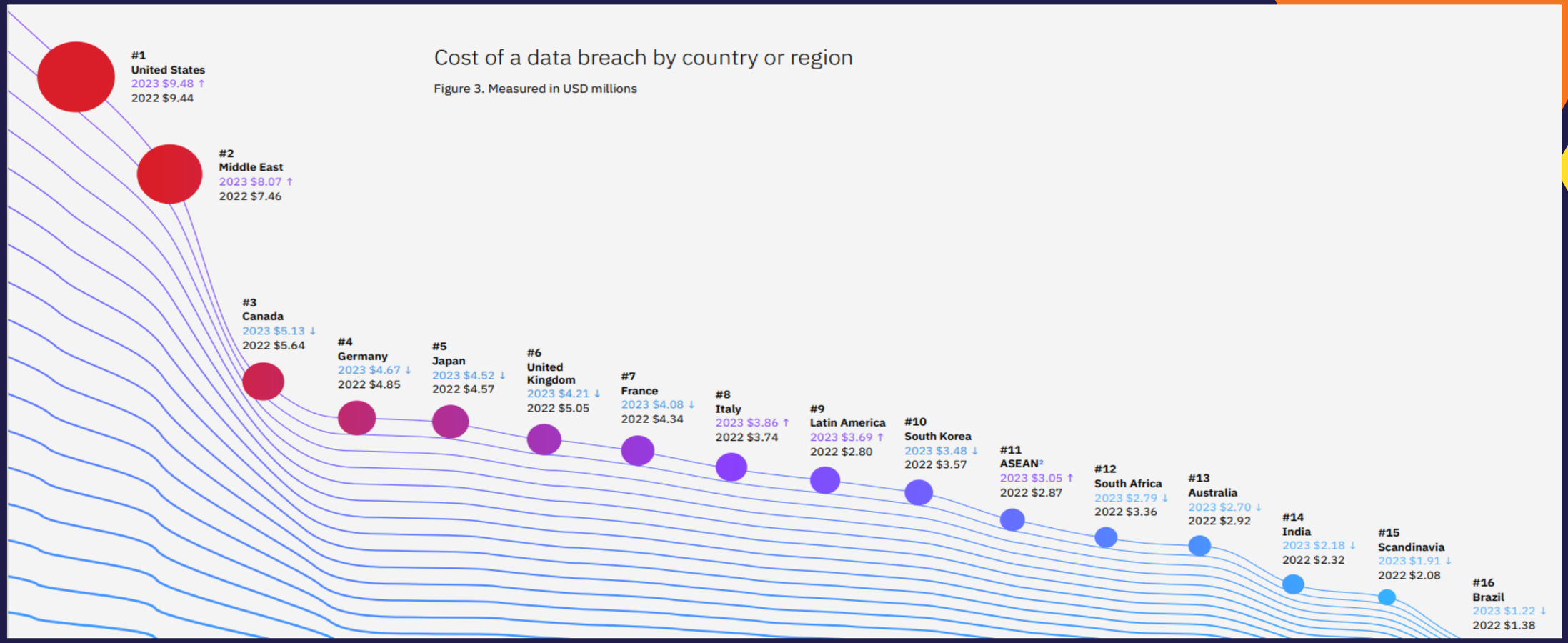
*Fuente: Cybercrime Magazine

* Fuente: 2021 CROWDSTRIKE GLOBAL THREAT REPORT

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

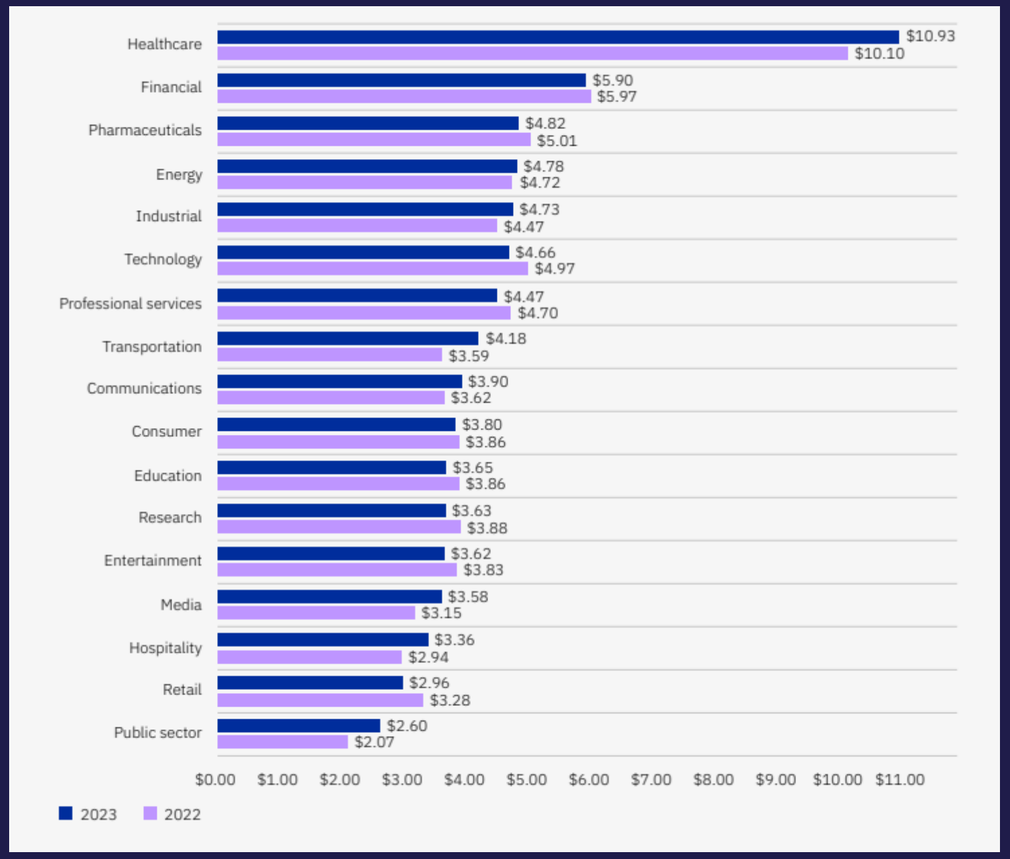
Panorama de Amenazas

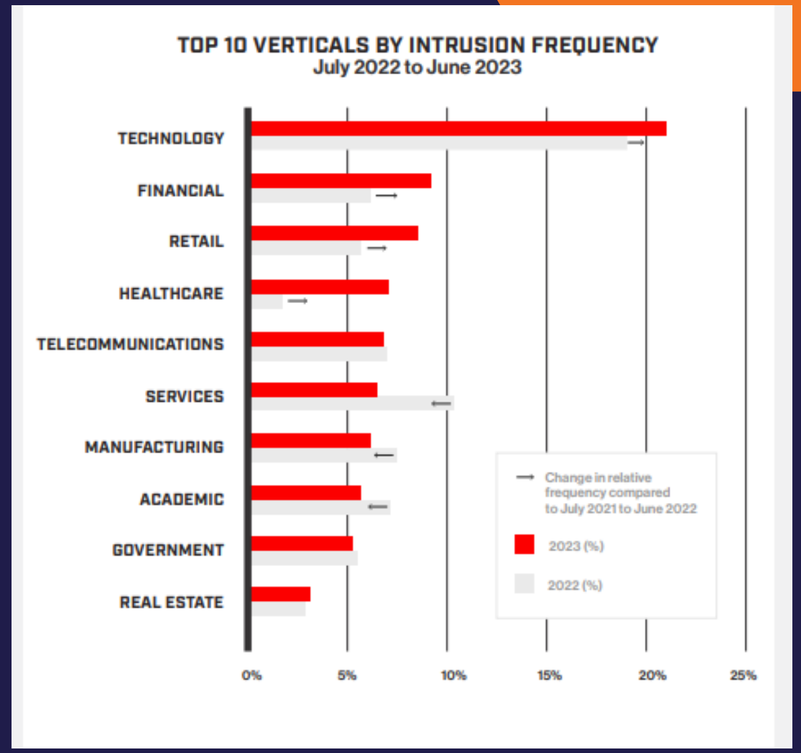


SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Algunos datos de interés

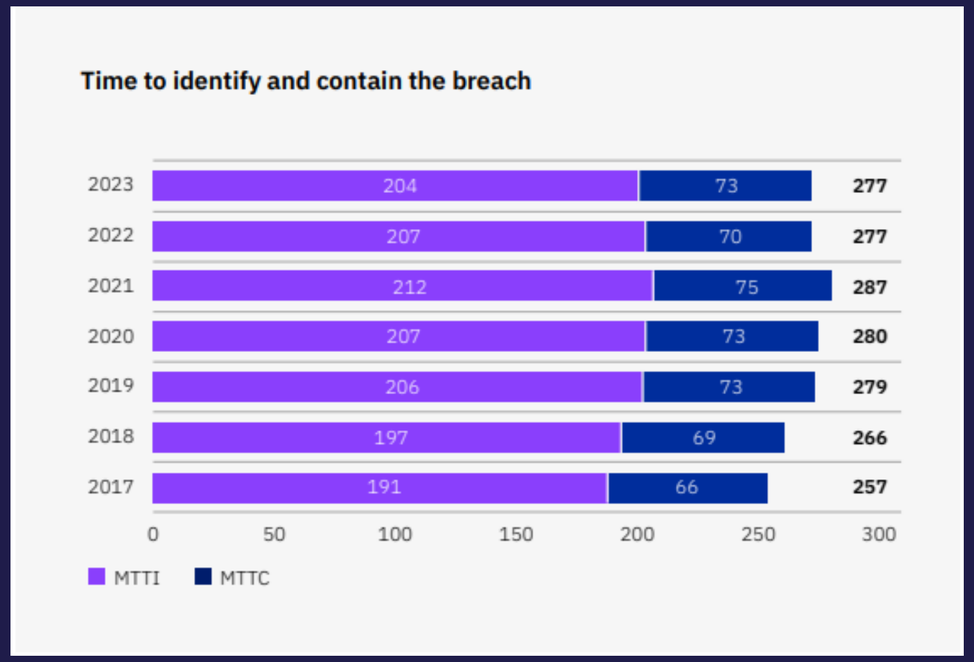




SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Algunos datos de interés



En 2022, las organizaciones tardaron 207 días para identificar una infracción. En 2023, solo hizo falta 204 días. Por otra parte, las organizaciones requirieron un promedio de 73 días para contener infracciones en 2023, mientras exigían sólo 70 días en promedio en 2022. Tiempos medios más altos para contener e identificar ambas infracciones ocurrieron en 2021, en 212 y 75 días, respectivamente.

- Fuente: data breach report

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Aceleración del panorama amenazas

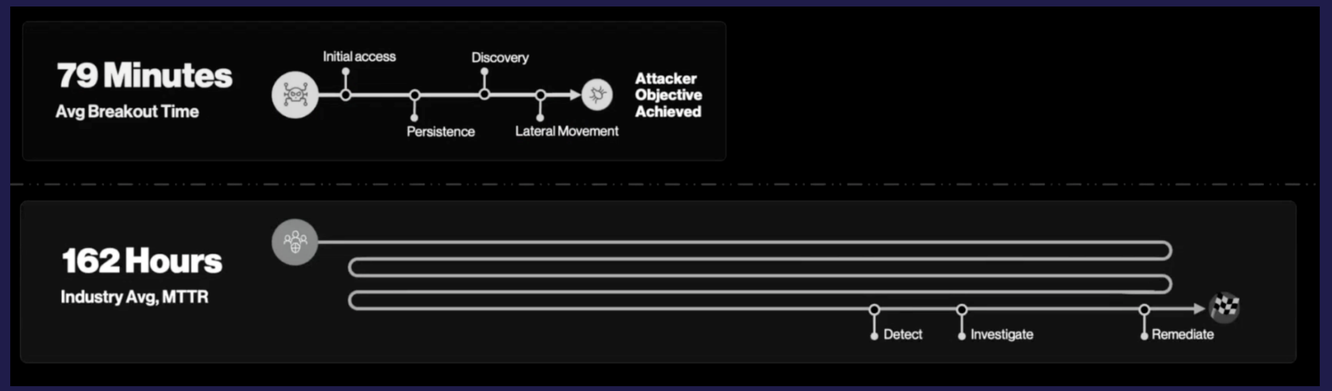
SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Breakout Time

El tiempo promedio de ruptura (breakout time) de la actividad de intrusión de delitos electrónicos interactivos disminuyó de 84 minutos en 2022 a **79 minutos** en 2023.

Mientras, el tiempo de respuesta medio en el que las organizaciones responden a una amenaza, es de **162 horas** en 2023.



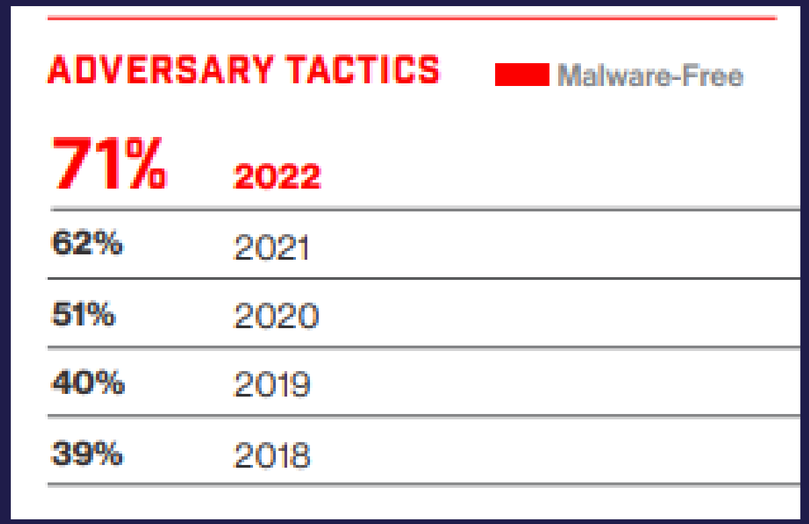
* Fuente: Global Threat report

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Tácticas de ataque

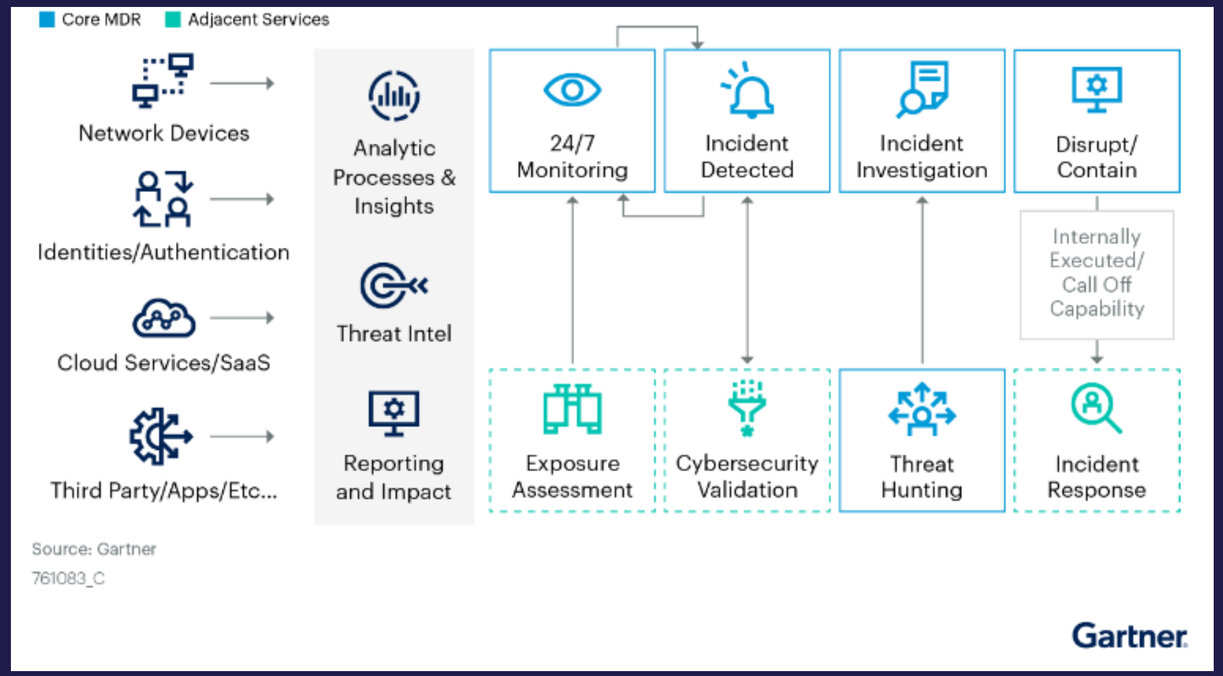
La actividad libre de malware representó el 71 % de todas las detecciones en 2022 (frente al 62 % en 2021). Esto se relacionó en parte con el prolífico abuso de credenciales válidas por parte de los adversarios para facilitar el acceso y la persistencia en los entornos de las víctimas.



SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

MDR | Servicios



Funciones Core

- Combinación de tecnologías
- contenido y análisis centrados en amenazas.
- Threat intelligence
- Threat Hunting

Servicios Adjacentes

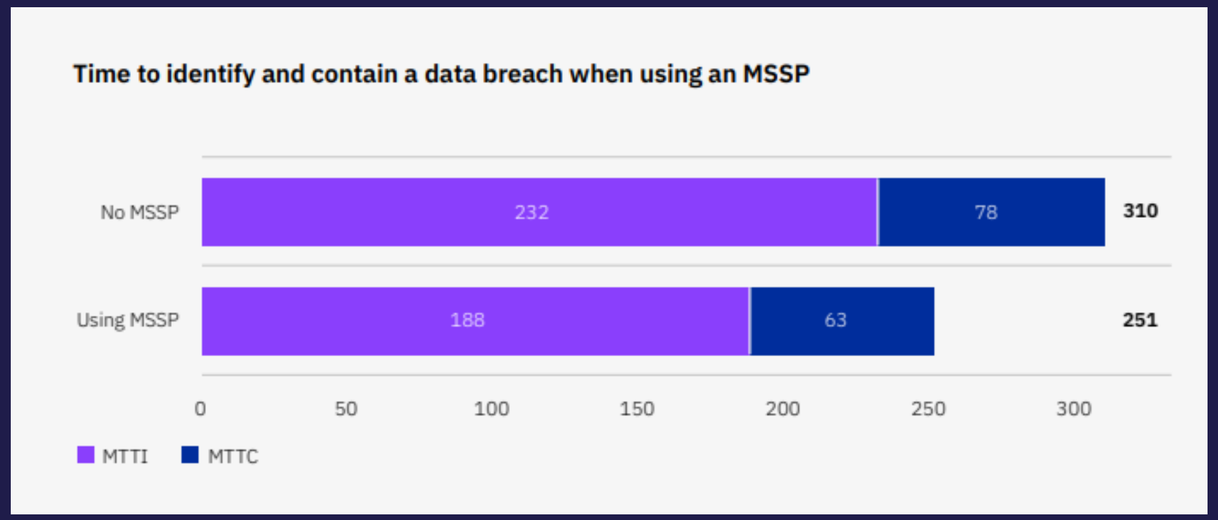
- Analisis forense
- Respuesta de incidente
- Breach attacks validations (BAS)

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

MDR | Servicios

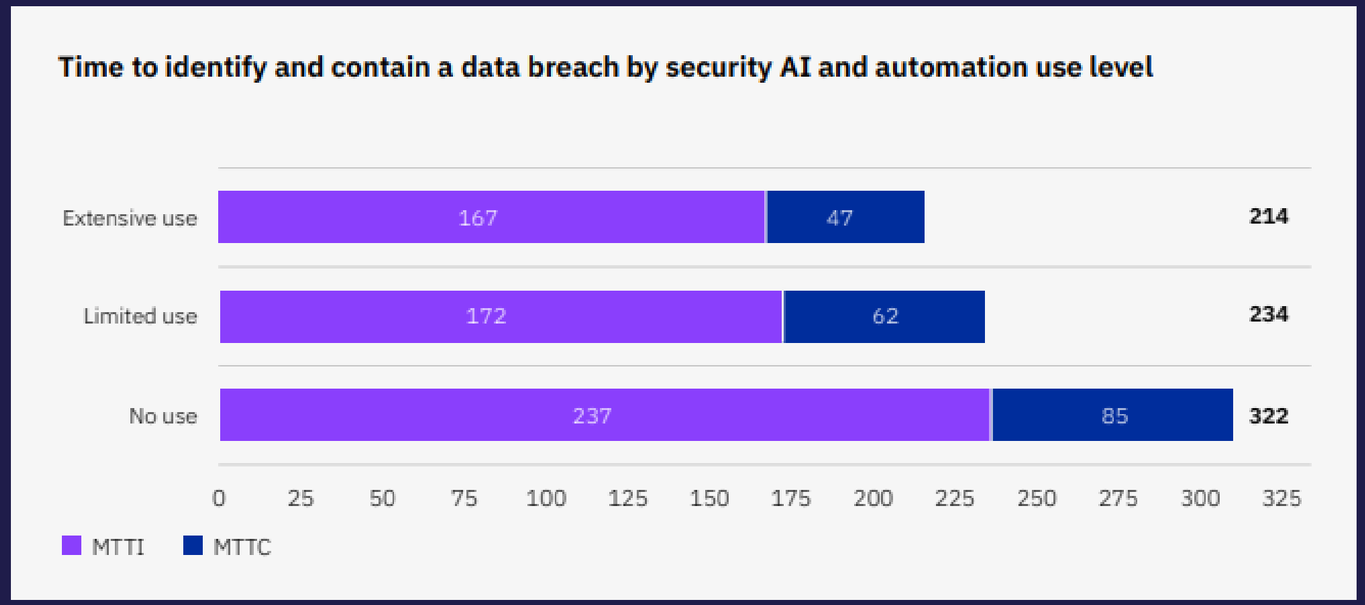
- En el informe de 2023, las organizaciones que tenían un MSSP pudieron identificar y contener incumplimientos en el 80% del tiempo.
- Las organizaciones que trabajaron con un MSSP identificaron infracciones 16 días más rápido o un tiempo de identificación de un 8,2% más corto que el promedio mundial de 204 días.
- Los que no lo hicieron tardaron 28 días más o 12,8% más.
- Los tiempos de contención sin ningún MSSP duraron cinco días más o el 6,6% más que el global reportado para 2023 (promedio de 73 días).
- Los tiempos de contención con la asistencia del MSSP fueron 10 días más rápidos o un 14,7% más rápidos.



SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

MDR | Servicios



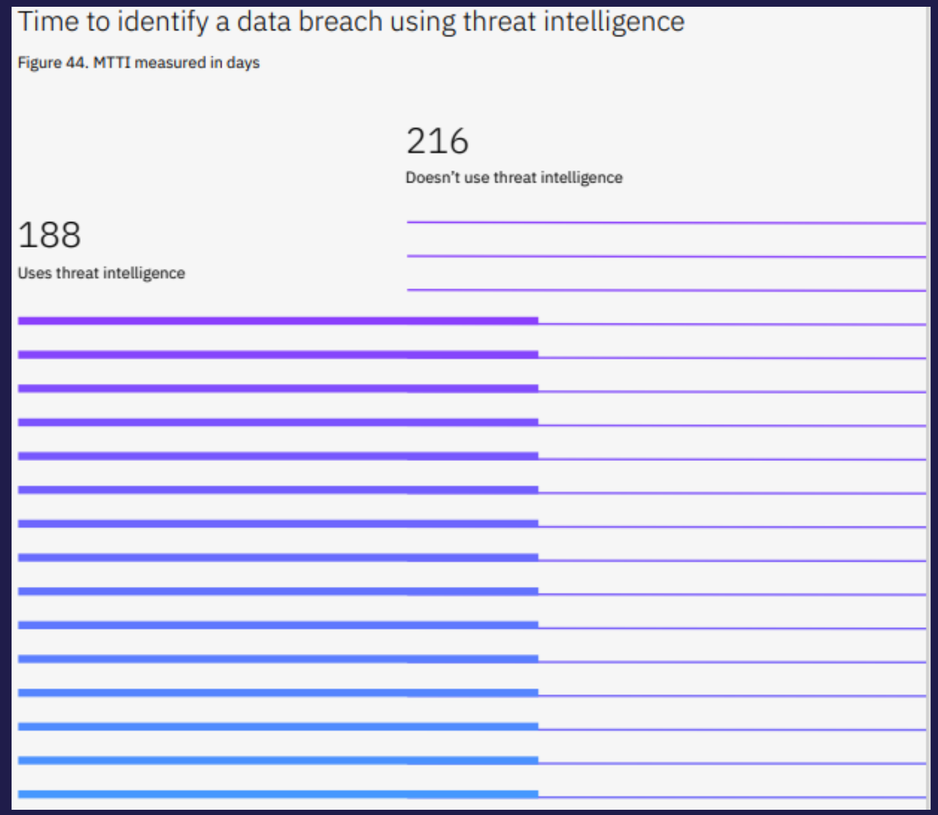
La automatización e inteligencia artificial de seguridad redujeron el tiempo para identificar y contener una infracción en más de 100 días.

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

MDR | Servicios

Inteligencia de amenazas reducida tiempo de identificación de incumplimiento



SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

Implementación existosa de MDR

- Evaluación de necesidades y objetivo.
- Selección del proveedor de MDR
- Definición de roles y responsabilidades
- Proceso de mejora continua

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

El rol de la inteligencia Artificial

Solo el 28% de las organizaciones utilizaron ampliamente la inteligencia artificial y la automatización de seguridad en sus operaciones.

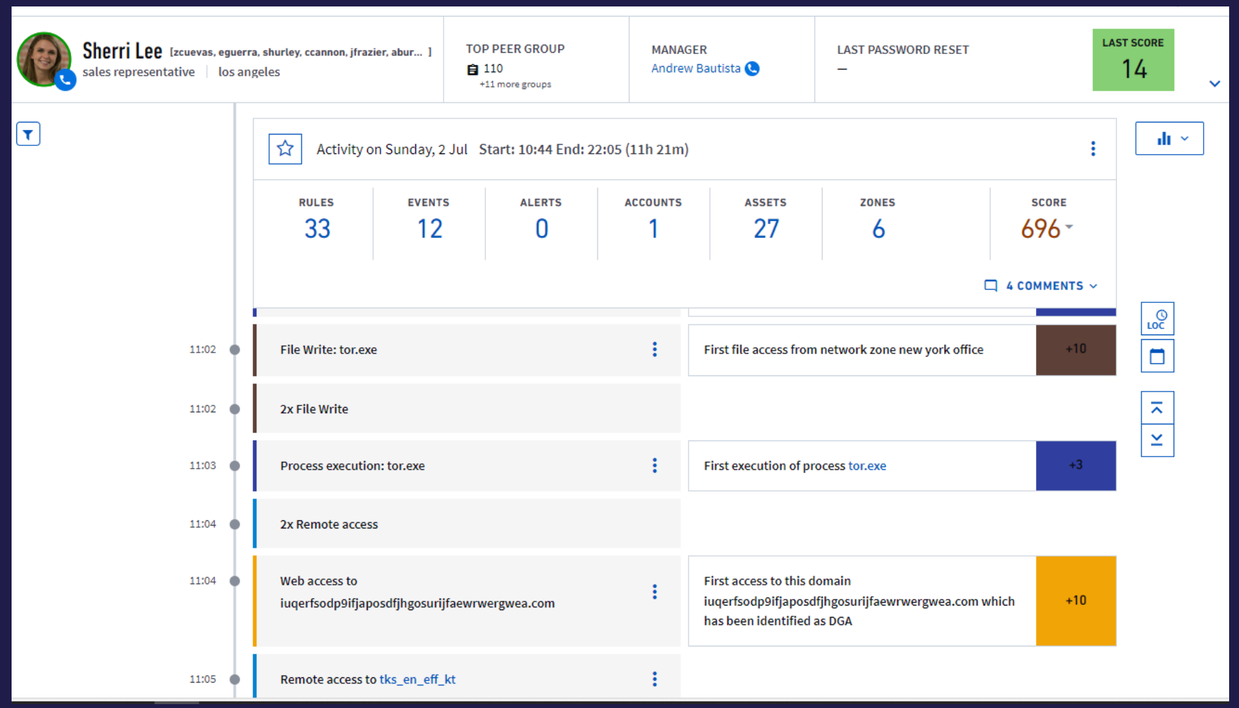
El uso extensivo de la IA de seguridad y la automatización generó un ahorro de casi 1,8 millones de dólares en costos de violación de datos.

Aceleró el tiempo para identificar y contener una infracción en más de 100 días en comparación con organizaciones sin uso.

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

El rol de la inteligencia Artificial



- Ayuda a los analistas a detector nuevas amenazas con mayor precision.
- Contexturalizar y clasifcar las alertas de Seguridad de manera mas efectiva
- Automatizar el proceso de investigacion
- Recomendar acciones para acelerar la respuesta

SOFISTIC CYBERSECURITY

2023 CELAES Congreso Latinoamericano de Seguridad Bancaria

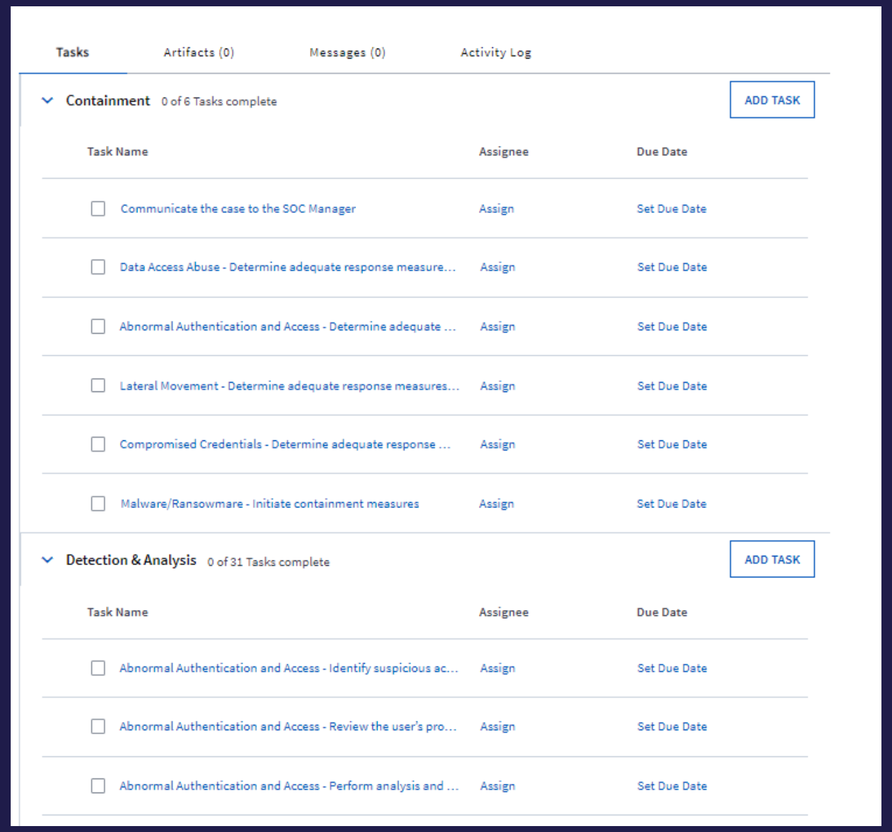
El rol de la inteligencia artificial

Behavioral Analytics

Sequence Type:	session	Sequence ID:	slee-20230702154400
User ID:	slee	Asset ID:	—
User Page:	Go to page	Asset Page:	—
Timeline Page:	Go to page	Exabeam Risk Score:	696
Rule Count:	33	Event Count:	12
Alert Count:	0	Asset Count:	27
Zones Count:	—	Location Count:	6

Risk Reasons:

Email received from competition domain
Exabeam detected a suspicious command that was issued to delete shadow copies on the system, this activity is common for malware/ransomware to hide its tracks and therefore this event is notable
Exabeam detected a suspicious command that was issued to disable recovery mode on this host. This may be an indicator of a malicious process such as Ransomware preventing the computer from recovering from a previous state, therefore this event is notable.
WannaCry is ransomware. Known command line artifacts or known processes were detected. This event is notable as Wannacry is a dangerous worm that can quickly spread through networks on it's own. Reference: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_malware_wani
A file has been written and is suspected of Ransomware on host
First file access from network zone for user.
Boot configuration data was deleted using the bcdedit command. This is a destructive technique used by malware or an attacker which can prevent the machine from being used. Reference: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_bootconf_moc
Exabeam detected that this user has attempted to access a web domain that seems to be DGA (Domain Generating Algorithm) generated. It is a common practice for malware to establish communications over a pseudo random domain name that is generated by an algorithm, an access to such domain be indicative of malware communicating outside of the network.
First time this user has logged onto a network zone
First time the user communicated from this network zone
First time user has accessed this asset
First time a user is accessing an internet IP address in this country
This is the first time Exabeam has seen this user running this process. Users normally run the same processes to perform their tasks, a first time appearance of a process is therefore notable since it may be an indicator of malicious activity
Risk transfer from past sessions.



Tasks | Artifacts (0) | Messages (0) | Activity Log

Containment 0 of 6 Tasks complete — ADD TASK

Task Name	Assignee	Due Date
Communicate the case to the SOC Manager	Assign	Set Due Date
Data Access Abuse - Determine adequate response measure...	Assign	Set Due Date
Abnormal Authentication and Access - Determine adequate ...	Assign	Set Due Date
Lateral Movement - Determine adequate response measures...	Assign	Set Due Date
Compromised Credentials - Determine adequate response ...	Assign	Set Due Date
Malware/Ransowmare - Initiate containment measures	Assign	Set Due Date

Detection & Analysis 0 of 31 Tasks complete — ADD TASK

Task Name	Assignee	Due Date
Abnormal Authentication and Access - Identify suspicious ac...	Assign	Set Due Date
Abnormal Authentication and Access - Review the user's pro...	Assign	Set Due Date
Abnormal Authentication and Access - Perform analysis and ...	Assign	Set Due Date