FORTINET

IA en Ciberseguridad: Multiplica el Impacto, Minimiza el Riesgo

Jorge Miranda

Sr. Country Manager

Forbes

“Sean Parker: agente disruptivo”

LAS MEJORES HISTORIAS DE LA DÉCADA

“Nuevo modelo de negocio en la industria musical”

¿Qué impacto quieres causar?

Impacto ≠ **Funcionalidad**

Impacto de la Inteligencia Artificial

1960s

Algoritmo “minimax”
Búsqueda de fuerza bruta
Evaluar posibles movimientos

Juegos de ajedrez

2010s

Procesamiento lenguaje natural
Aprendizaje automático
Aprendizaje profundo

Asistentes Inteligentes para tareas predefinidas

HOY

Inteligencia
Artificial Generativa
Modelo Lenguaje Largo (LLM)

Creación de contenido nuevo, cómo voz, texto, imágenes y videos

Impacto de la Inteligencia Artificial

1960s

Algoritmo “minimax”
Búsqueda de fuerza bruta
Evaluar posibles movimientos

Nueva forma de jugar y ejercitar nuestra mente

2010s

Procesamiento lenguaje natural
Aprendizaje automático
Aprendizaje profundo

Nueva forma de comunicarse con las máquinas

HOY

Inteligencia
Artificial Generativa
Modelo Lenguaje Largo (LLM)

Nueva forma de conseguir resultados más rápidos

¿Qué impacto quieres causar?

Impacto = Resultados

Impacto de la Inteligencia Artificial en Ciberseguridad

Nueva forma de comunicarse con las máquinas

Nueva forma de conseguir resultados más rápidos

Dos perspectivas de IA en Ciberseguridad

La Mala

Puede empoderar más a los intrusos, Los cibercriminales ahora utilizan herramientas con inteligencia artificial disruptivas

La Buena

Los proveedores Ciberseguridad están proporcionando a los equipos de TI soluciones integradas con Inteligencia Artificial

“Toda batalla es ganada antes de que inicie”

El arte de la guerra - Sun Tzu

Objetivo

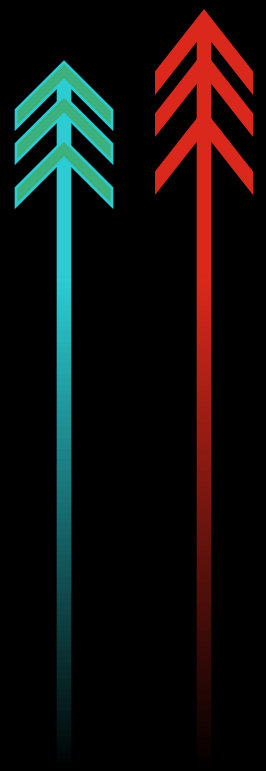
Proteger Activos Digitales de Alto Valor

Aquellos que tienen IMPACTO directo en el CRECIMIENTO del negocio

Proteger Activos Digitales de Alto Valor

Directamente Proporcional

Valor del activo digital de la empresa con impacto en crecimiento de negocio



Monto extorsión de los ciberdelincuentes luego de “secuestrar” el activo digital

10.5 T USD para 2025

11,4 M USD por minuto recibió el cibercrimen en 2024

Identificar los posibles vectores de ataque con acceso a los activos digitales

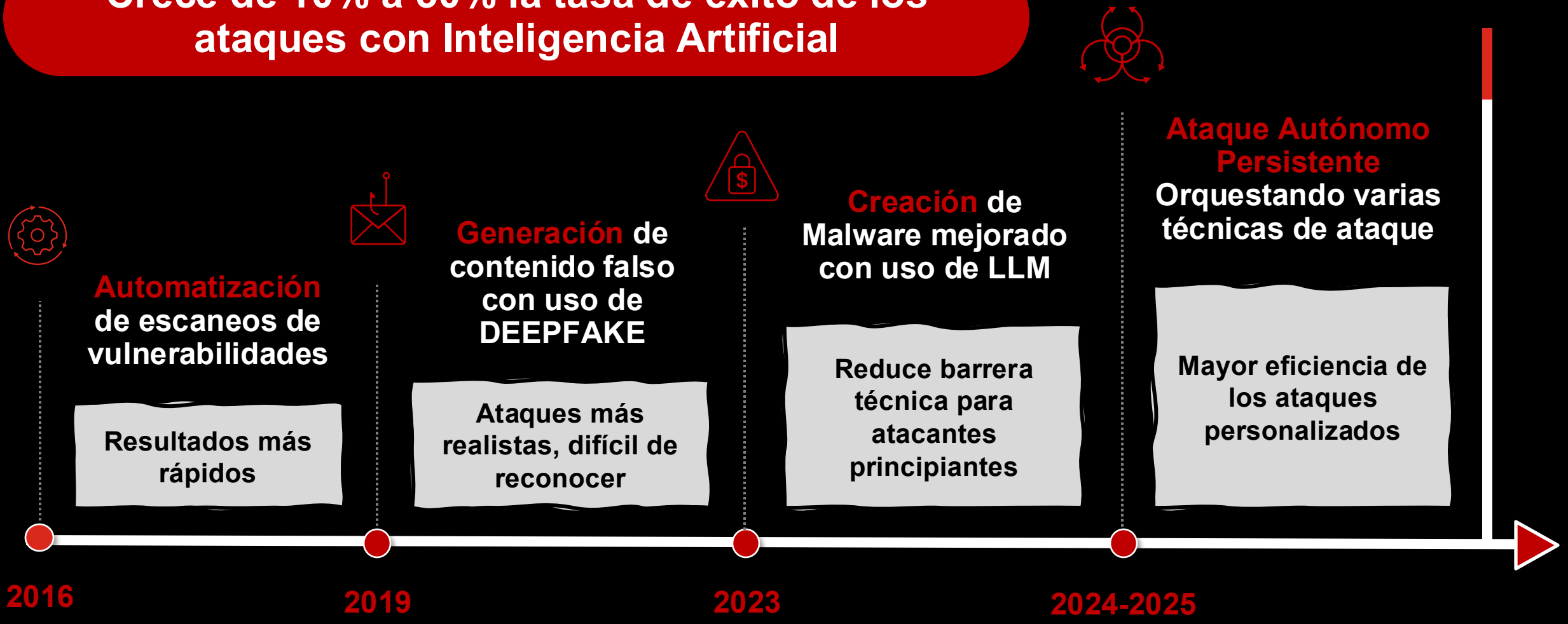
Toda batalla es ganada antes de que inicie

El arte de la guerra - Sun Tzu

4 Fases de Evolución de Ciberataques con IA

Crece de 10% a 50% la tasa de éxito de los ataques con Inteligencia Artificial

IMPACTO en tasa de conversión



Generación de contenido falso con uso de DEEPFAKE

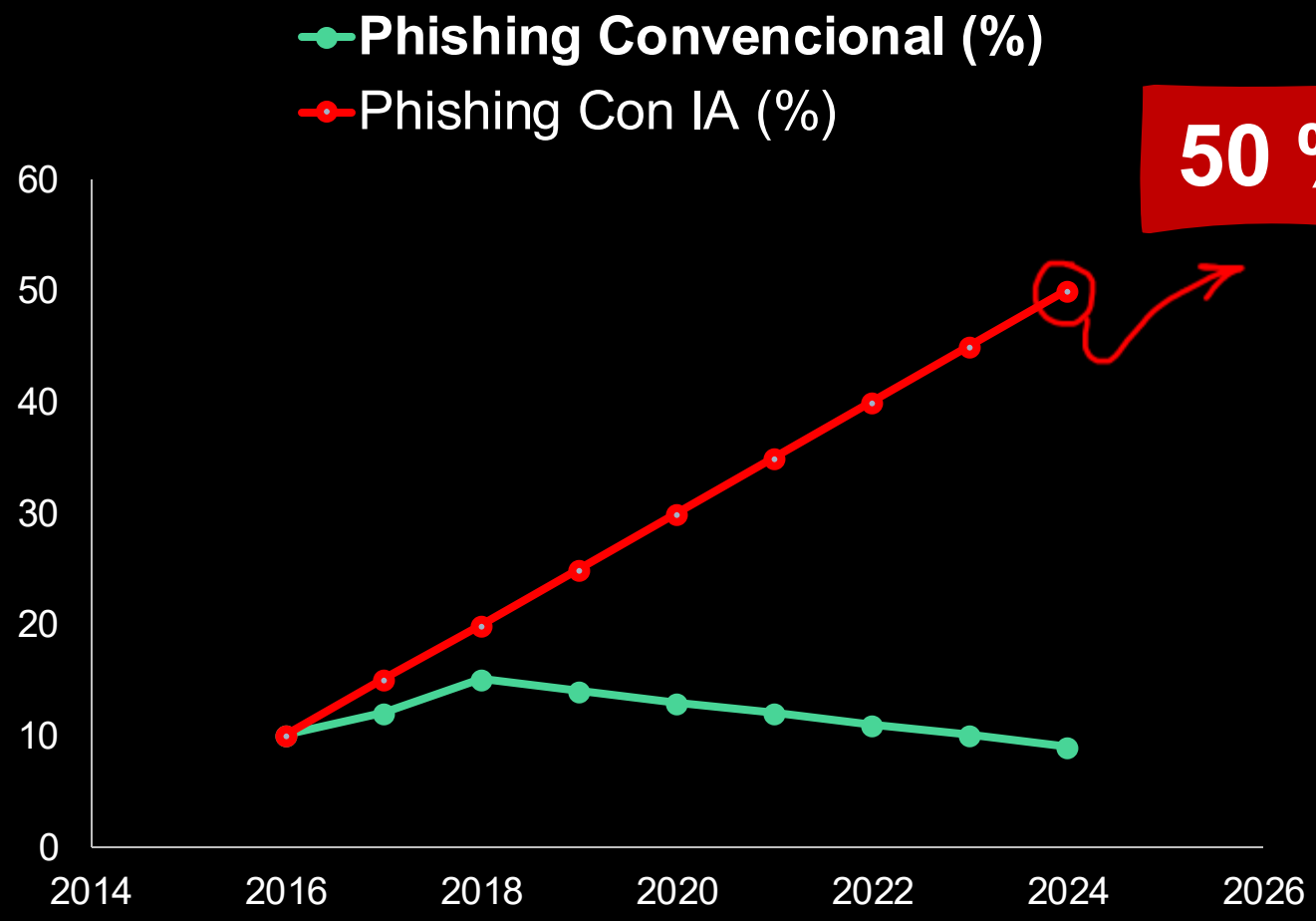
La Buena

¿Cuál fue el libro que me recomendaste la semana pasada?, y de repente la llamada se cortó.

La Mala

El trabajador fue engañado para que asistiera a una videollamada, todos los personajes eran recreaciones ultra falsas de directivos de la empresa, dijo la policía de Hong Kong es una sesión informativa.

Crece a 50% la tasa de Éxito de Ataques con IA



Fuente: ChatGPT Analizando técnicas de ataques con IA en Latinoamérica

Consideraciones

- ❑ Correos personalizados por GenAI
- ❑ Análisis de grandes cantidades de datos para escoger víctimas específicas

“Errores humanos”

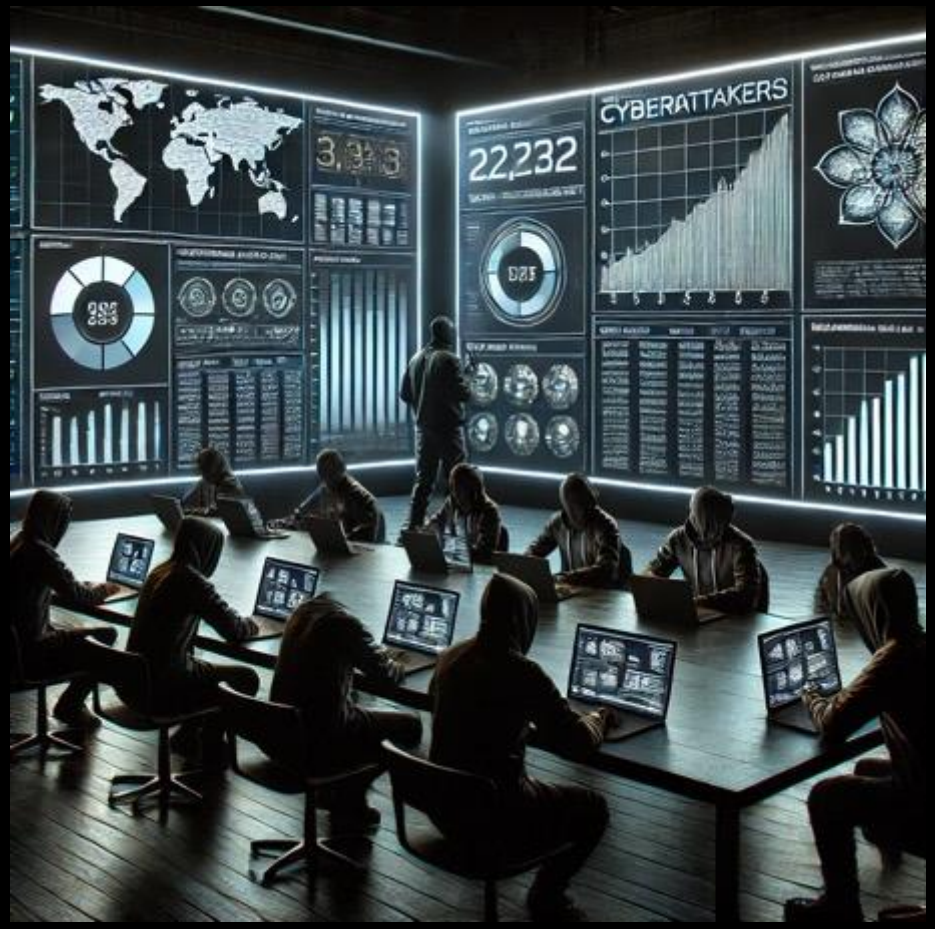
Toda batalla es ganada antes de que inicie

El arte de la guerra - Sun Tzu

4 Debilidades que conocen los Ciberdelincuentes

Falta de integración de Inteligencia Artificial	**Lentitud en identificar comportamientos anómalos**
Uso de muchas herramientas y consolas de seguridad dispares	**Aumenta el tiempo de respuesta a incidentes**
Falta de políticas centralizadas y coordinadas	**Incoherencia en la gestión de riesgos**
700,000 Puestos “Vacíos” en equipo de ciberseguridad TI LATAM	**Baja experiencia en herramientas avanzadas**

Su “Dashboard” de resultados de negocio ilícito va en aumento (IMPACTO)

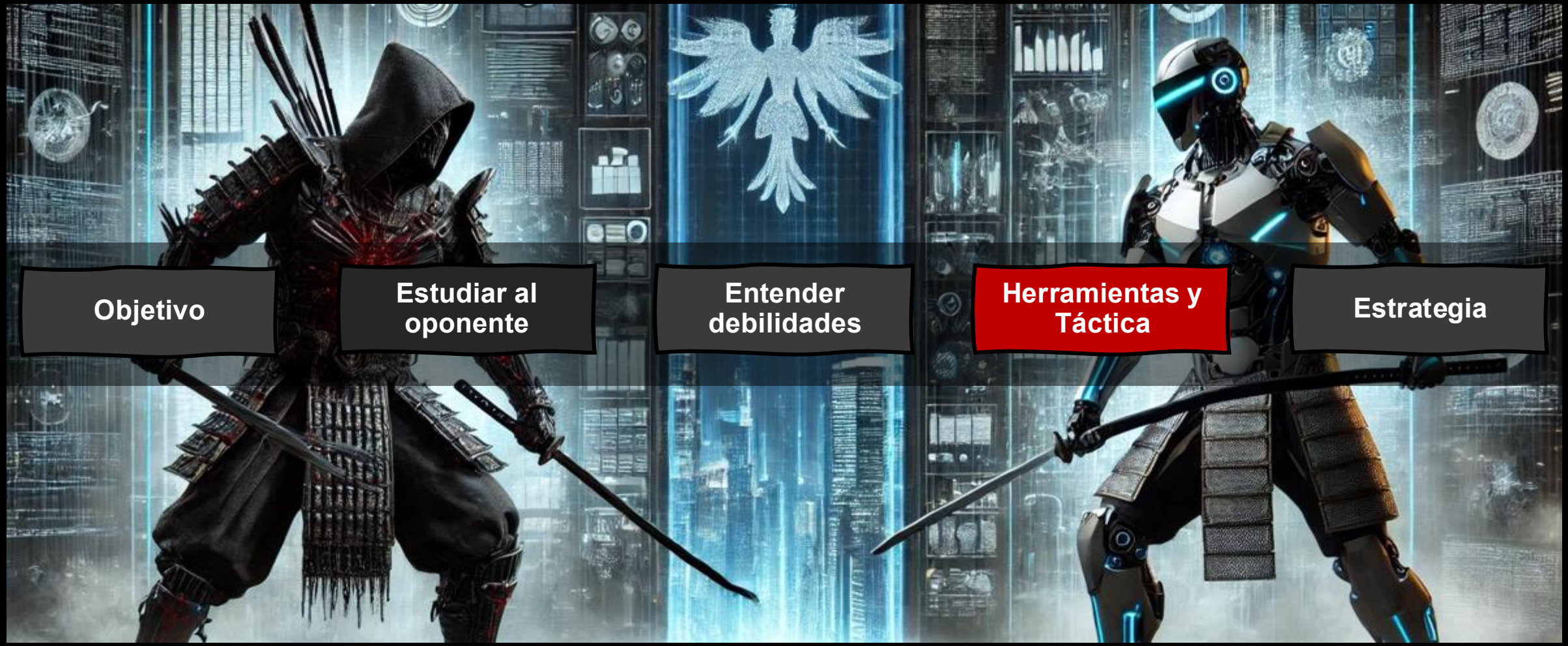


50%	Tasa de Éxito de ataques con IA
94%	Amenazas cibernéticas desapercibidas
70%	Empresas que reportan aumento de complejidad de amenazas
240 B	Intentos de Ciberataques en México 2024

Fuente: FortiGuard LABs – Panorama de amenazas 2024

Toda batalla es ganada antes de que inicie

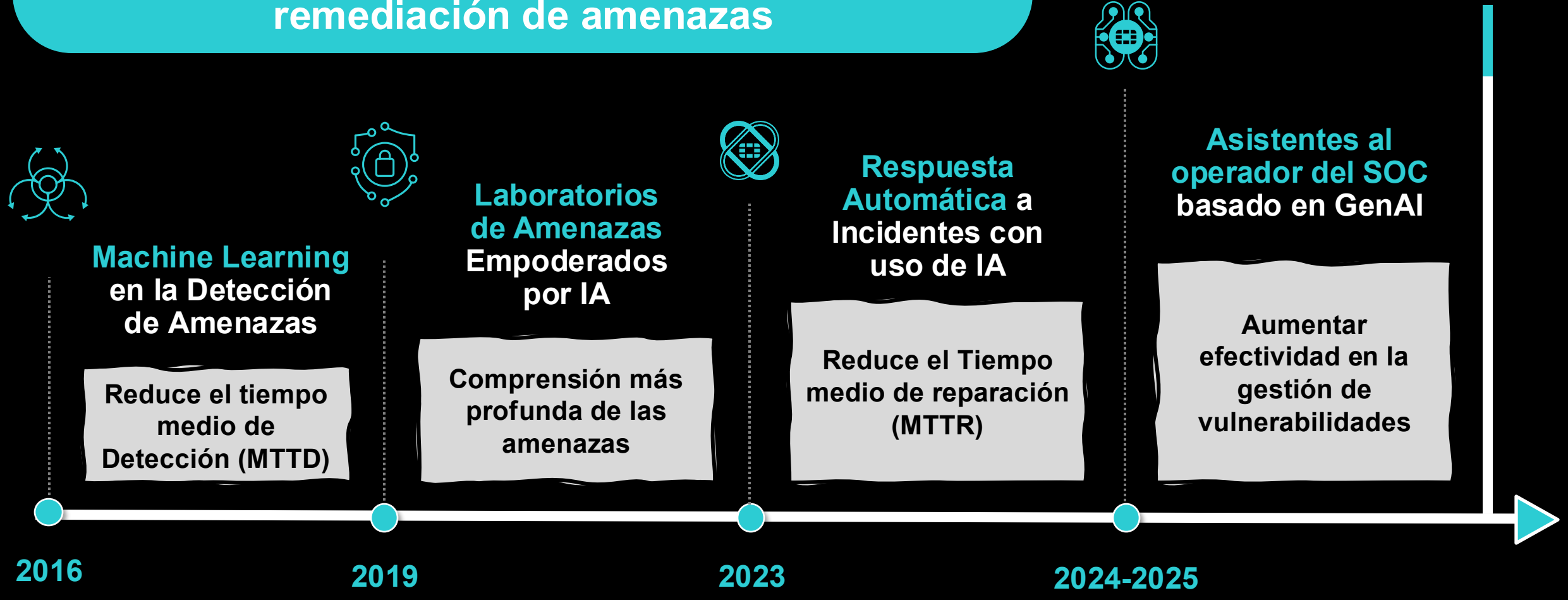
El arte de la guerra - Sun Tzu



4 Fases de Evolución de Ciberseguridad con IA

Se reduce en un 99 % los tiempos investigación y remediación de amenazas

IMPACTO en mitigación de amenazas



Laboratorios de Amenazas Empoderados por IA

6M
Firewalls

3M
Web Gateways

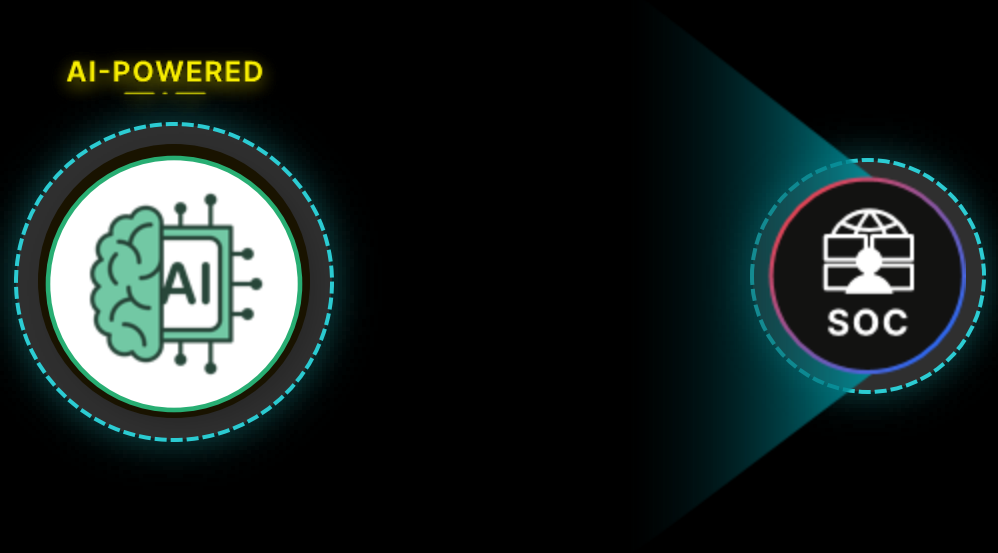
20M
Emails

10M
Endpoints

5M
Sandbox

LABS

+ 5 MM Logs / Día



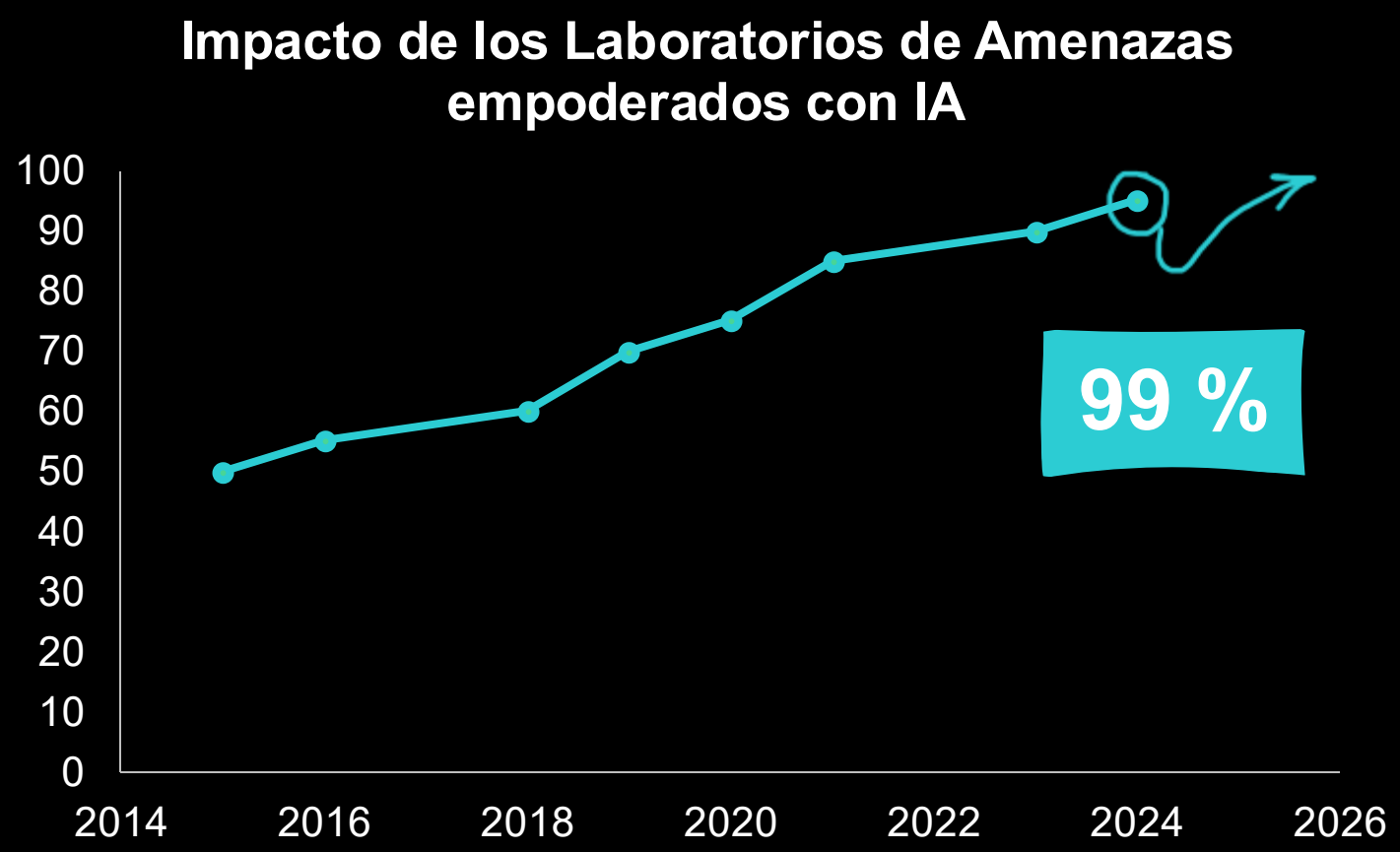
Habilita a las Operaciones con la inteligencia de amenazas más reciente

- **Detecta comportamientos anómalos**
- **Identifica amenazas desconocidas, de día cero y otras basadas en archivos**
- **Alerta sobre nuevos dominios y URL maliciosos**

By FortiGuard Labs

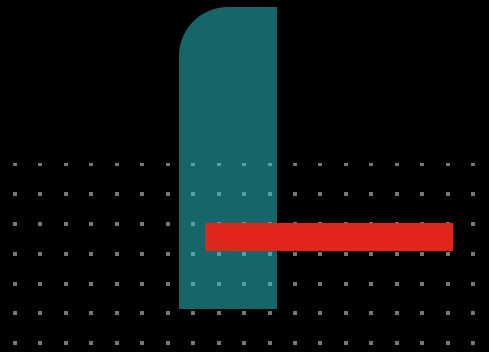
LABS

Los laboratorios impactan de 50% a 99% en Mitigación



Comprensión más profunda de las amenazas emergentes y la creación de firmas y soluciones en un tiempo récord…

¿Cómo optimizamos los resultados de las operaciones de Ciberseguridad?



GenAI en Ciberseguridad

Asistencia al operador basada en IA que pueden apoyar a los equipos de seguridad en

- Mejorar las políticas
- Reducir tiempos de detección de amenazas
- Aumentar efectividad en la gestión de vulnerabilidades

La IA no reemplaza puestos de trabajo….
pero los que dominen la IA si…

Resolviendo un Incidente con el soporte de GenAI

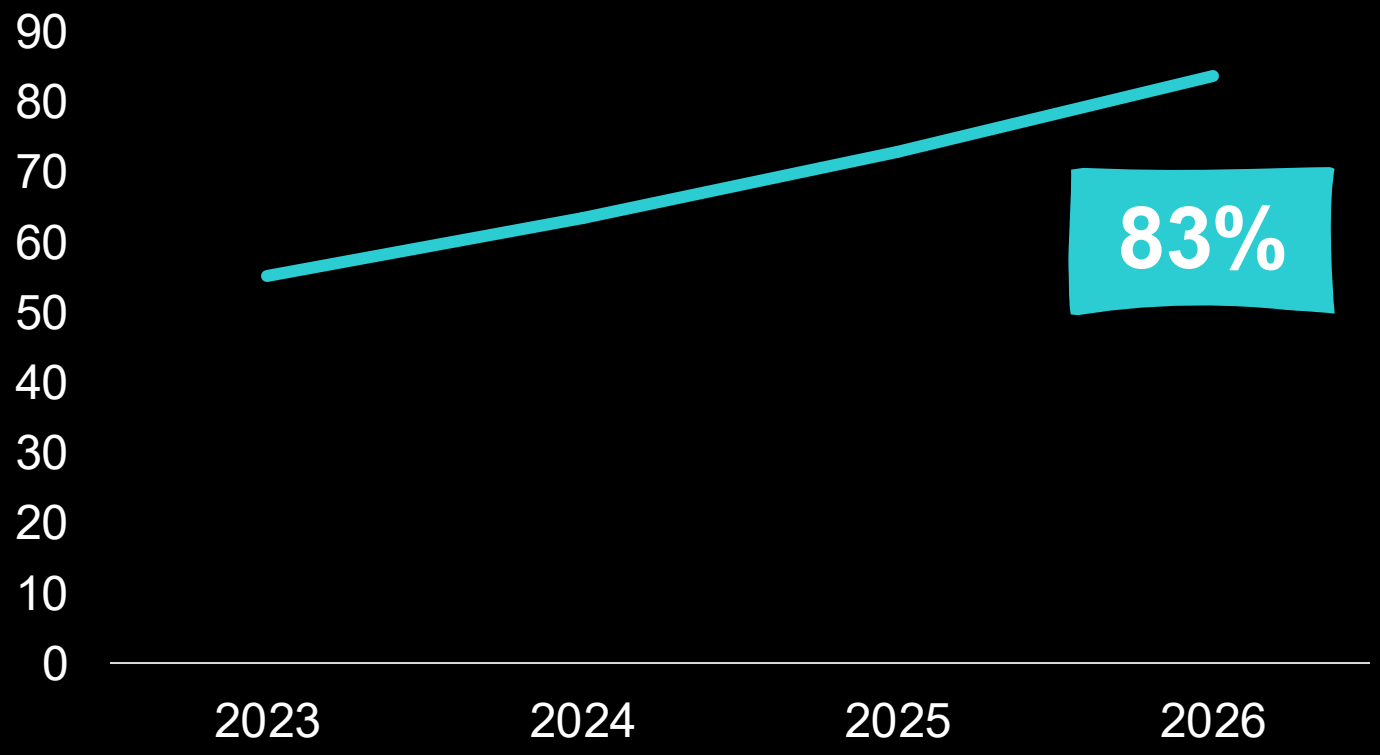
Analiza este incidente

¿Qué acción debo tomar?

Crea un reporte de IoC de esta semana y compáralo con resultados de la semana pasada

De 55% a 83% de Eficiencia Operativa con GenAI

Proyección de Eficiencia Operativa con GenAI



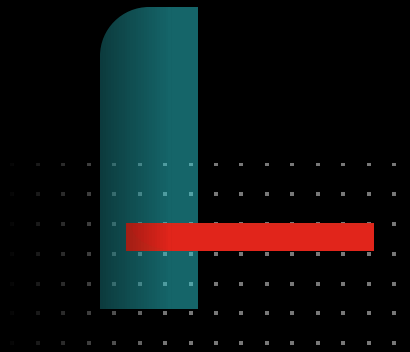
Para 2026, más del 80% de las empresas tendrán implementada soluciones con GenAI en sus entornos de ciberseguridad

Aumento exponencial con respecto a menos del 5% a principios de 2023

Toda batalla es ganada antes de que inicie

El arte de la guerra - Sun Tzu

La táctica sin estrategia es el Ruido antes de la Derrota



El arte de la guerra - Sun Tzu

Táctica sin estrategia

→ Los “mejores productos” de forma Independiente

Laboratorio 1	Laboratorio 2	Laboratorio 3	Laboratorio 4	Laboratorio 5	Laboratorio 6
Políticas 1	Políticas 2	Políticas 3	Políticas 4	Políticas 5	Políticas 6
Gestión 1	Gestión 2	Gestión 3	Gestión 4	Gestión 5	Gestión 6
Proveedor 1	Proveedor 2	Proveedor 3	Proveedor 4	Proveedor 5	Proveedor 6
Conectividad	Branch	Data Center	Public Cloud	SaaS	Dispositivos Remotos

Táctica sin estrategia
→ Los “mejores productos” de forma Independiente

Pesadilla Operativa
(Administración | Cambios | Integraciones | Actualizaciones)

Crea complejidad y desacelera la innovación

67%

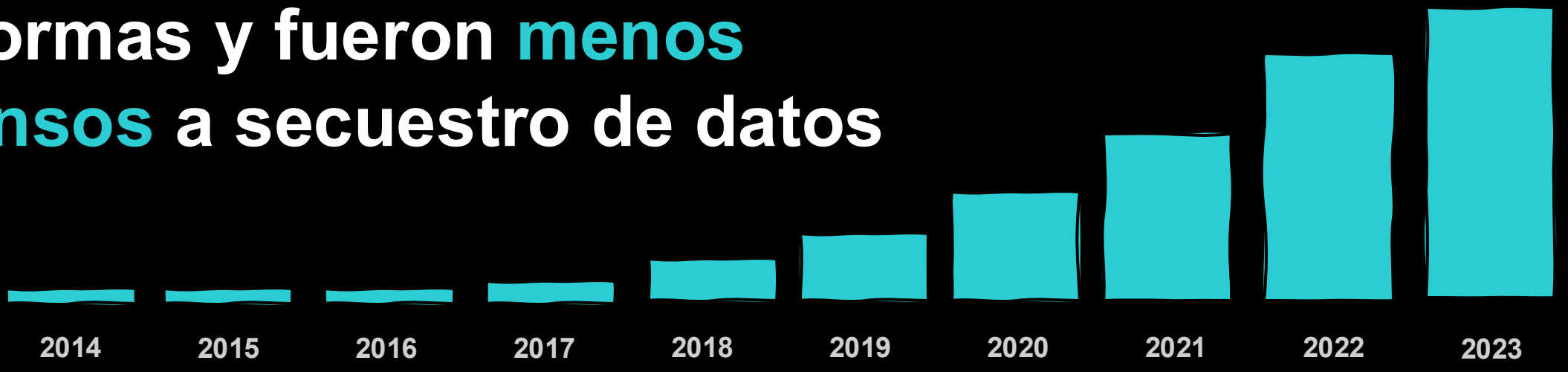
De las empresas que apostaron por 'mejores productos' fueron más vulnerables al ransomware

Empresas paralizadas entre 48 horas y más de 12 meses por secuestro digital

Source: FortiGuard Labs | 2023 Global Ransomware Report

38%

De los Clientes adoptaron plataformas y fueron menos propensos a secuestro de datos



Empresas que NO ha sido paralizadas

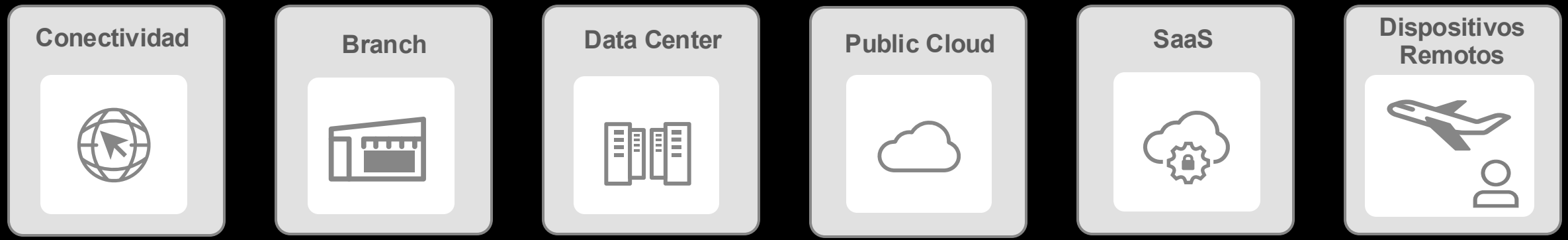
Source: FortiGuard Labs | 2023 Global Ransomware Report

De Productos a Plataformas en Ciberseguridad

75% de las organizaciones están buscando activamente evolucionar a una estrategia de consolidación de proveedores (1)

Inteligencia Artificial

Ciberseguridad en Plataforma con Integración Nativa



1 - Gartner, Top Trends in Cybersecurity 2023, March 2023

“Dashboard” de Resultados de Ciberseguridad con Plataformas (IMPACTO)

90% Eficiencia operativa con Plataformas

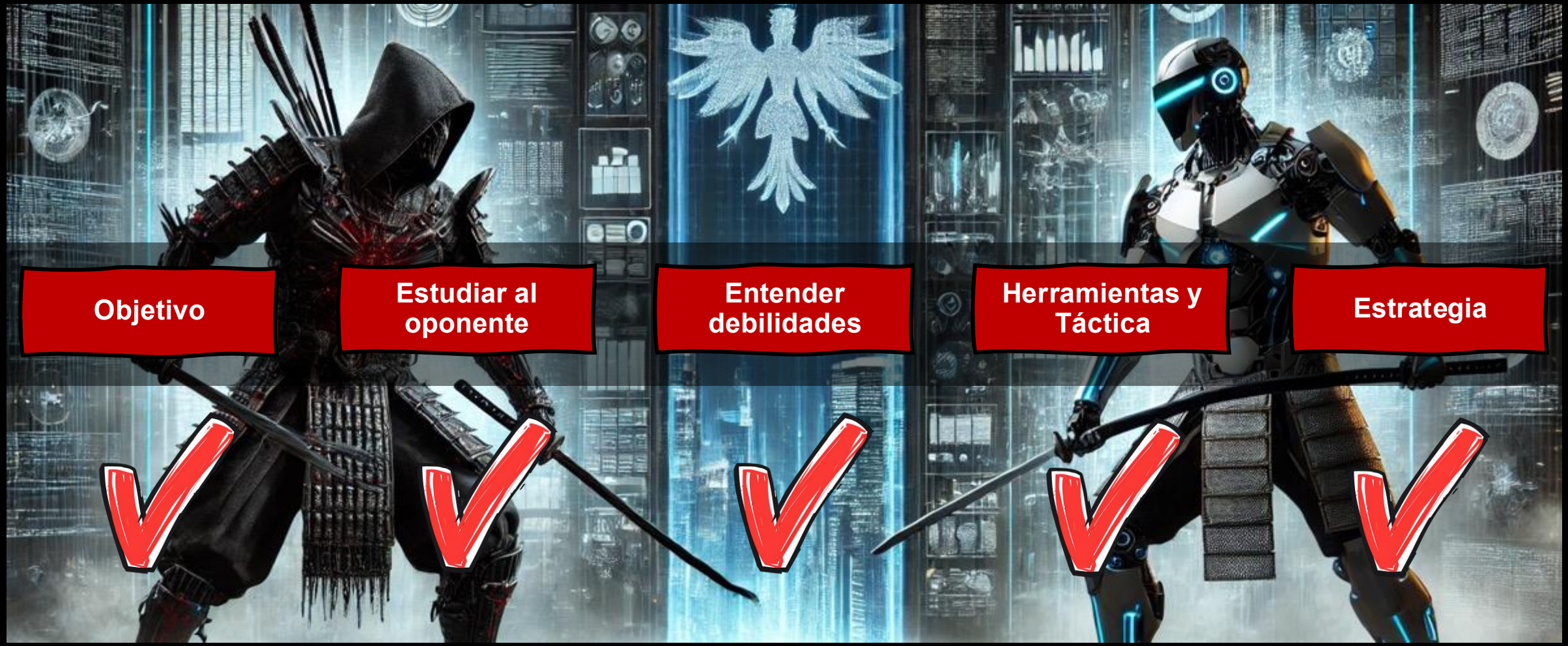
90% Reducción del impacto financiero de incidentes de ciberseguridad

99% Mitigación de nuevas amenazas

99% Disminución de tiempos de detección y respuesta

Toda batalla es ganada antes de que inicie

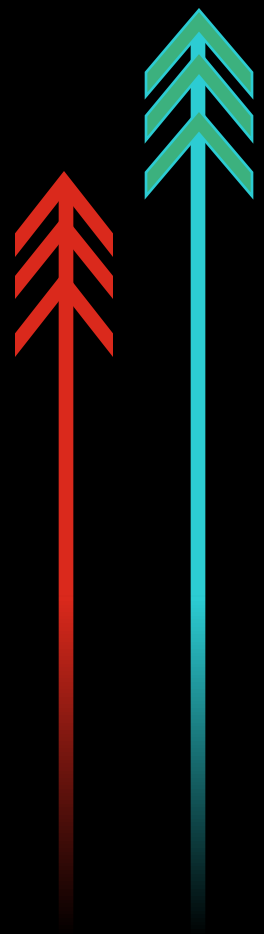
El arte de la guerra - Sun Tzu



Empieza con el fin en mente (Resultados)

Libro: Los 7 Hábitos de las personas altamente efectivas
Dr. Stephen R. Covey.

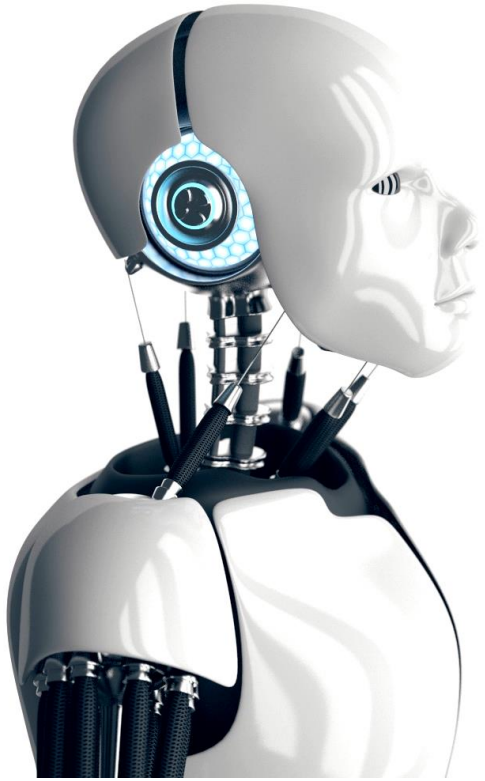
50%	Éxito de Ataques con IA
94%	Amenazas cibernéticas desapercibidas
70%	Empresas que reportan aumento de complejidad de amenazas
240 M	Intentos de Ciberataques LATAM en 2024



Eficiencia operativa con Plataformas	90%
Reducción del impacto Financiero	90%
Reducción de tiempos en atención de incidentes	93%
Eficiencia Operativa	90%

IA en Ciberseguridad

Multiplica el Impacto, Minimiza el Riesgo



Eficiencia operativa con Plataformas — 90%

Reducción del impacto Financiero — 90%

Reducción de tiempos en atención de incidentes — 93%

Eficiencia Operativa — 90%

© Fortinet Inc. All Rights Reserved.

FORTINET