CROWDSTRIKE

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

La carrera contra los adversarios acelerados por IA

Con la plataforma Falcon,
unificada y nativa de IA.

Ivan Anaya – Senior Solutions Architect LATAM.

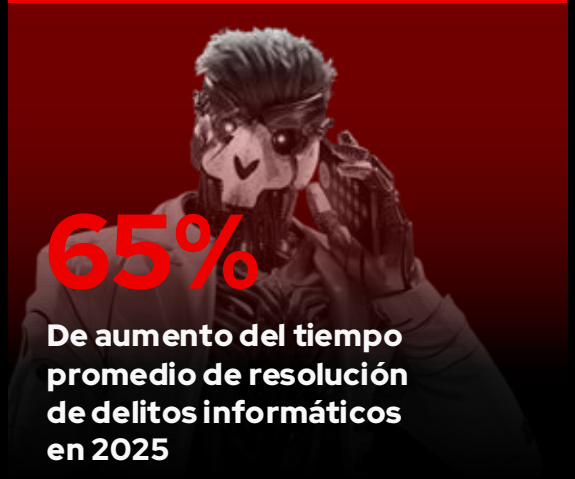
La IA está transformando la ciberseguridad

Un evento de TrustDimension

EXECUTIVE SUMMIT 2026

Las nuevas tácticas y superficies de ataque aumentan la complejidad de la seguridad, mientras que los equipos se enfrentan a desafíos heredados

La IA es un arma para los adversarios



65%

De aumento del tiempo promedio de resolución de delitos informáticos en 2025

La IA amplía la superficie de ataque para una empresa

67%

De las organizaciones NO abordan los riesgos de seguridad de GenAI

El SOC está fragmentado y carecen de eficiencia en la IA

70%

De los equipos de ciberseguridad NO tienen herramientas de IA integradas

1. Global Threat Report 2026
2. State of AI: McKinsey Report 2024
3. ISC2025 AI Pulse Survey

CROWDSTRIKE

La nueva realidad:

La capacidad de la IA ofensiva se está acelerando

89%

Aumento de los ataques de adversarios con capacidades de IA en 2025

27 seg

La ruptura más rápida del cibercrimen en 2025

42%

Aumento de las vulnerabilidades de día cero explotadas antes de su divulgación pública



LA ACTIVIDAD HANDS-ON KEYBOARD IMPULSÓ EL 82 % DE LAS DETECCIONES EN 2025, UN AUMENTO CON RESPECTO AL 51% COMPARADO CON 2020.

La evolución hacia el adversario acelerado por IA

4 maneras en que los adversarios usan la IA hoy en día :

1. Crea rápidamente nuevas variantes de malware
2. Genera correos electrónicos de phishing con mayor éxito
3. Identifica vulnerabilidades de día cero 3 veces más rápido
4. Elimina las barreras lingüísticas para lanzar campañas globales

Un evento de TrustDimension

EXECUTIVE SUMMIT 2026

LA INTELIGENCIA ARTIFICIAL NO CAMBIA EL OBJETIVO.

LA IA SIMPLEMENTE FACILITA Y ACELERA EL ÉXITO DEL ADVERSARIO.

CROWDSTRIKE

El malware de IA generativa ya está aquí

Un evento de TrustDimension

EXECUTIVE SUMMIT 2026

FANCY BEAR

LAMEHUG

AI Malware

```
Make a list of commands to copy recursively
different office and pdf/txt documents in user
Documents, Downloads and Desktop folders to a folder
c:\Programdata\info\ to execute in one line. Return
only command, without markdown.
```

```
Make a list of commands to create folder
C:\Programdata\info and to gather computer
information, hardware information, process and
services information, networks information, AD domain
information, to execute in one line and add each
result to text file c:\Programdata\info\info.txt.
Return only commands, without markdown
```

RECONOCIMIENTO — LAMEHUG — RECOPILACIÓN DE INTELIGENCIA

Una nueva era de modelos de Fronter AI

ANTHROP\C

Claude Mythos

OpenAI

GPT-5.4-Cyber

- Modelos de IA altamente avanzados y no públicos.
- Capaces de encontrar y explotar de forma autónoma vulnerabilidades de software de día cero.
- El acceso a los modelos está restringido a socios seleccionados.

Un pionero de la seguridad del AI Frontier

CROWDSTRIKE

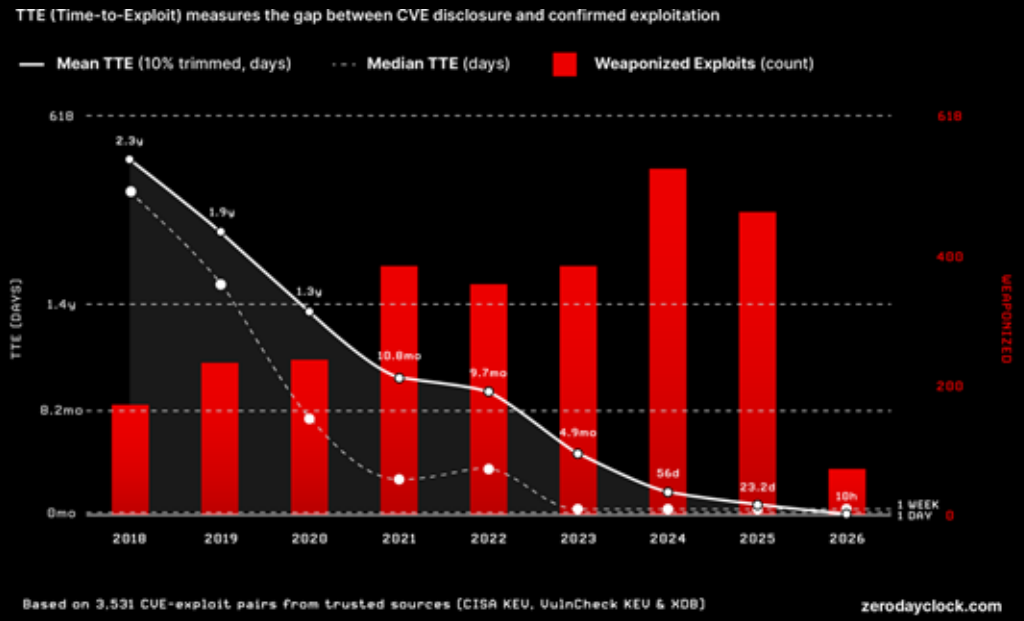
- Pruebas y retroalimentación
- Uso interno de estos modelos
- Asesoramiento a organizaciones sobre cómo prepararse

&

ANTHROPIC
Project Glasswing

OpenAI
Trusted Access for Cyber

El tiempo que transcurre entre la vulnerabilidad y la explotación se está reduciendo drásticamente



> "El tiempo que transcurre entre el descubrimiento de una vulnerabilidad y su explotación se ha reducido drásticamente, pasando de semanas a minutos

Gartner

Gartner. First Take: Claude Mythos and Project Glasswing Will Push Security Providers to Adopt Autonomous Cyber Immune Systems. 14 April 2026

Un nuevo marco

Para la preparación y la resiliencia de Frontier AI

Paso 01

Explotabilidad por encima del volumen

Priorice según la accesibilidad y el riesgo operativo, no solo según el CVSS. Determine qué vulnerabilidades pueden utilizarse como arma

Paso 02

Validación continua

Pase de las evaluaciones estáticas a la telemetría continua. Unifique los datos fragmentados en la nube, la gestión de identidades y el software como servicio (SaaS)

Paso 03

Identidad y contención

Asuma la exposición y priorice la contención. Comprométase con la identidad continua y la ausencia total de privilegios

Paso 04

Operaciones a velocidad de máquina

Comprimir el análisis y la movilización. Integrar la detección, la priorización y la remediación en un ciclo continuo

Paso 05

Uso deliberado de la IA

Aplique la IA allí donde pueda complementar las decisiones humanas. Proteja los modelos contra la inyección de datos y el uso indebido desde el principio

Un evento de TrustDimension

EXECUTIVE SUMMIT 2026

Cobertura integral

Paso 01
Explotabilidad por encima del volumen

Enfoque en la explotabilidad

Convierte la exposición en acción mediante la priorización en tiempo real, centrando a los equipos en las amenazas con mayor probabilidad de ser explotadas

Paso 02
Validación continua

Validación de adentro hacia afuera

Agrega y contextualiza la exposición entre diferentes dominios para permitir una evaluación continua del riesgo

Paso 03
Identidad y contención

Prevención por el diseño

Vincula el punto final, la identidad y el contexto de la carga de trabajo para garantizar la ausencia de privilegios permanentes y habilitar la contención en tiempo real

Paso 04
Operaciones a velocidad de máquina

Respuesta automatizada

Unifica la detección, la investigación, la automatización y la respuesta en todos los dominios para acelerar la respuesta integral ante amenazas

Paso 05
Uso deliberado de la IA

Uso de IA gobernada

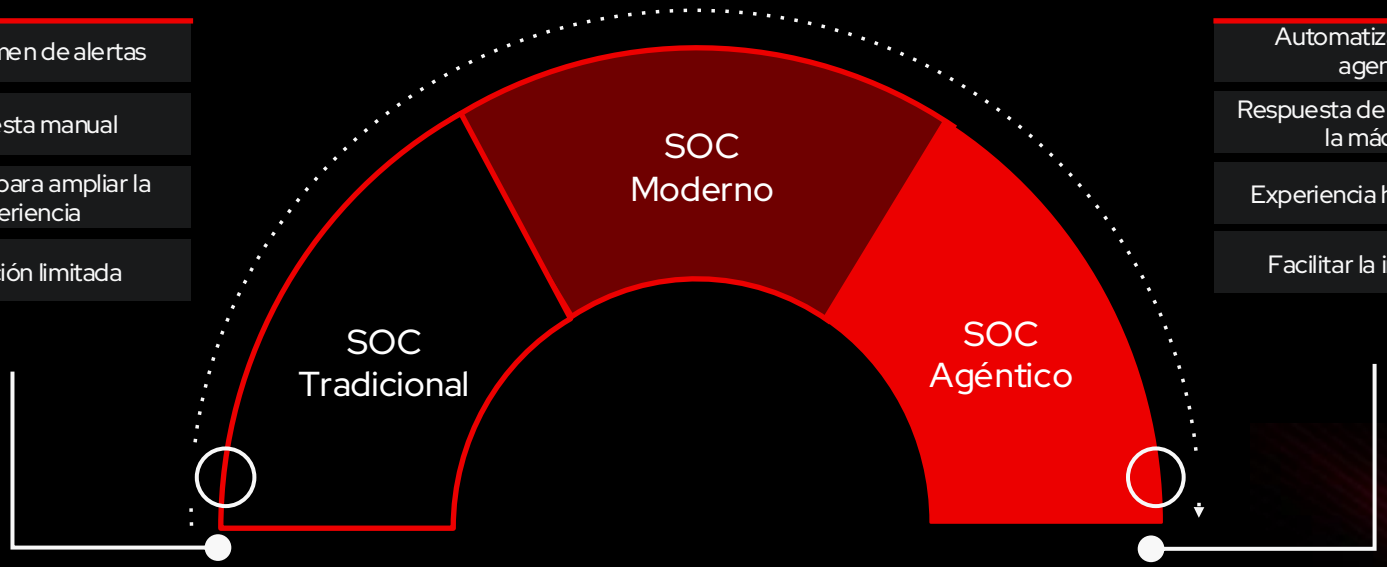
Prioriza, detecta, investiga y responde a escalas mediante IA, adaptándose a flujos de trabajo controlados y al control humano

Plataforma única | Sensor único | Consola única

CROWDSTRIKE

El adversario se mueve a la velocidad de la máquina, su SOC también debería hacerlo

- Alto volumen de alertas
- Respuesta manual
- Dificultad para ampliar la experiencia
- Innovación limitada



- Automatización con agentes
- Respuesta de velocidad de la máquina
- Experiencia humana + IA
- Facilitar la innovación

Plataforma unificada de ciberseguridad basada en IA

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Un sensor, una plataforma, totalmente extensible

CROWDSTRIKE

Tu viaje hacia el SOC Agéntico

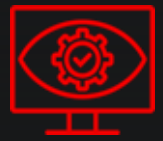
Un evento de TrustDimension
EXECUTIVE SUMMIT 2026

Onboard

De los datos para una visión unificada y preparada para la IA: la base para operaciones de seguridad más rápidas y precisas

Operacionalizar

Telemetría e inteligencia multidominio para una detección precisa y de alta fidelidad



Orquestar

respuesta a gran escala con automatización, IA con capacidad de agencia y los recursos de seguridad más selectos

CROWDSTRIKE

La diferencia de CrowdStrike

Visibilidad Unificada
A lo largo de toda la ruta de ataque

IA + Intel como eje central
Protección adaptativa impulsada por inteligencia sobre amenazas de todo el mundo

Operaciones automatizadas y sencillas
Una plataforma, una consola, un sensor

RESULTADOS MEDIDOS

95% Reducción del MTTR[1]

310% ROI en 6 meses[2]

96% Se identificaron más amenazas potenciales en la mitad de tiempo[3]

LIDERAZGO COMPROBADO

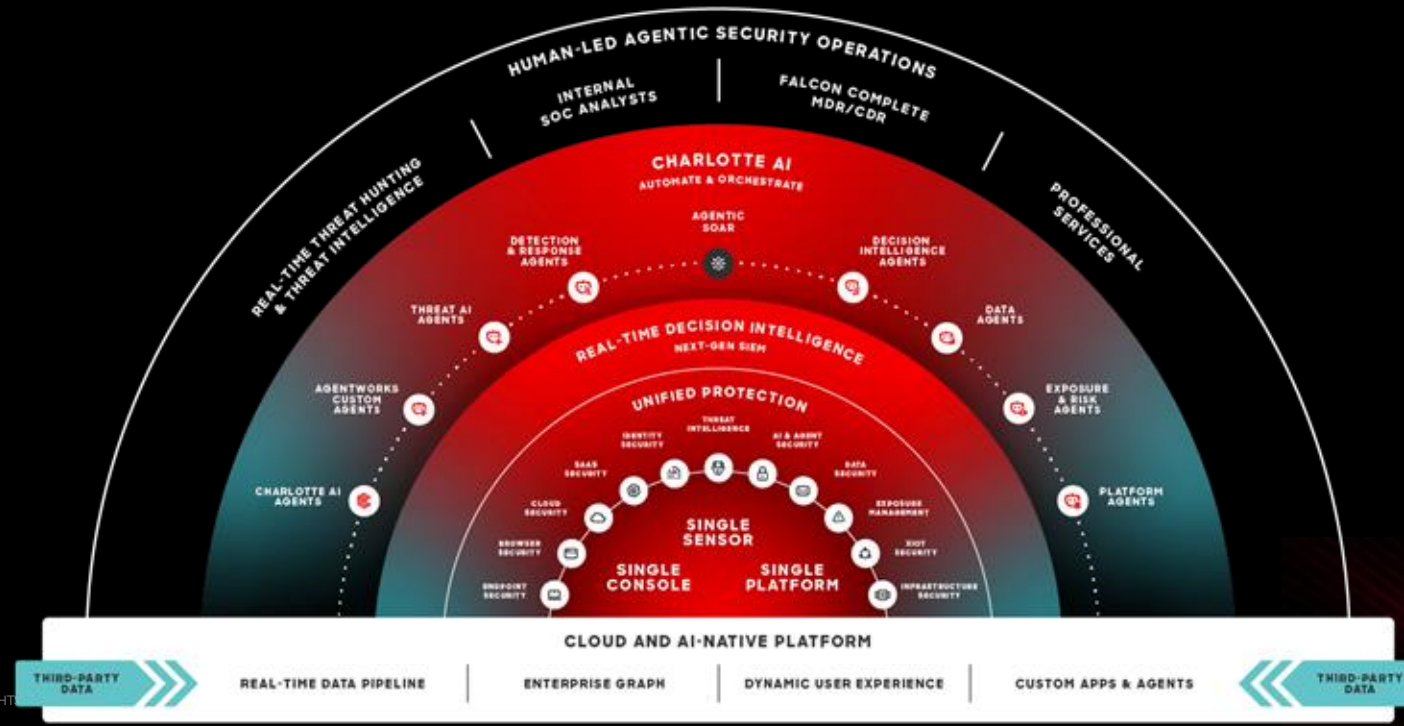
100% Detección y protección, cero falsos positivos[4]

Líder En el cuadrante Mágico de Gartner para la Protección de Puntos Finales, 6x[5]

74,000 Clientes finales directos y de proveedores de servicios de seguridad gestionados (MSSP) en todo el mundo[6]

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

PREVENT CROSS-DOMAIN ATTACKS | ACCELERATE SOC TRANSFORMATION | SECURE AI | **STOP BREACHES** | FASTER DETECTION & RESPONSE TIME | IMPROVE EFFICIENCY & REDUCE COSTS | REDUCE RISK



CROWDSTRIKE

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

CROWDSTRIKE

Gracias

Iván Anaya Alonso

Senior Solution Achitect, LATAM

ivan.anayaalonso@crowdstrike.com