inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Ciber ResiliencIA

Los Cabos, San Lucas, México 2026

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Bismarck Animas

Director de Ciber Resiliencia

CISSP, CSCP, CISM, CSX-P,CDSP, GCFE, GNFA, GCIH, GCTI, GDSA

Si no sabes nada ni del **enemigo** ni de ti mismo, sucumbirás en todas las batallas.

Si te conoces a ti mismo, pero **no** al enemigo, por cada victoria obtenida también sufrirás una derrota.

Si te conoces a tí mismo y conoces al enemigo, entonces serás **invencible**.

El supremo arte de la guerra es someter al enemigo **sin** luchar.

El arte de la guerra
Sun Tzu

Ciber Resiliencia

*La **capacidad** de una empresa de recibir un ataque y gracias a su preparación y precaución, poder **levantarse** tan rápido y con el menor daño como sea possible.*

Existe un suceso

¿Cómo reacciono?

¿Cómo me mantengo operando?

¿Salí fortalecido?

El problema que todos conocemos

Invertimos en herramientas...

...pero los incidentes se repiten.

Tenemos un SOC operando...

...pero no sabemos si está mirando lo correcto.

Apagamos incendios...

...sin eliminar lo que los provoca.

Hacemos reportes limpios...

...que generan complacencia, no inversión.

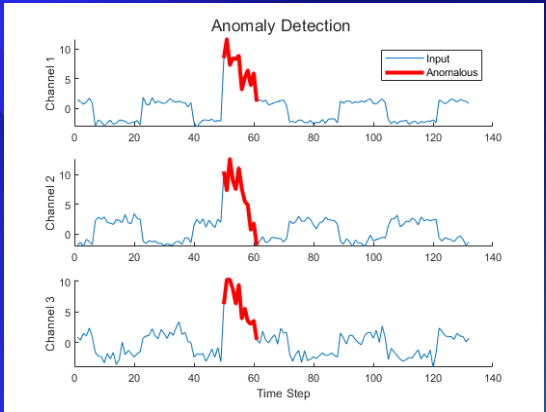
El CRoC nació para salir de ese ciclo — no con más herramientas, sino con más contexto y disciplina.

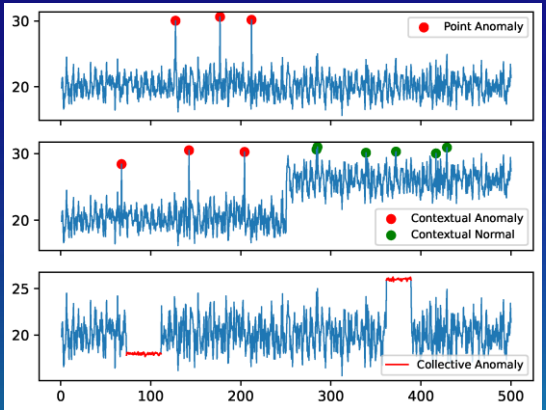
Lo que el CRoC responde para el negocio

¿Dónde estamos realmente expuestos?	El CRoC mapea la superficie de ataque real del negocio, integrando todos los assessments disponibles y correlacionándolos con los procesos que hacen ganar dinero a la empresa.
¿Estamos mirando lo que importa?	Valida que el modelo de monitoreo del SOC refleje el riesgo real del negocio — no las configuraciones por defecto del proveedor.
¿Qué hacemos cuando pasa algo?	Define procesos claros de respuesta con autoridad establecida, comunicación al comité directivo y gestión de causas raíz para que el evento no se repita.

Detecta lo Anormal via normalización

Tenemos que enfocarnos en la visibilidad, monitoreo y alerta de lo anormal





*Necesitas tener claro como **opera normalmente** tu operación.*

Debemos tener claro lo que conforma nuestra organización.

Inventario claro y en tiempo real de infraestructura, identidades, información y personal.

“Inteligencia” Artificial

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

¿Agilizar o asegurar?

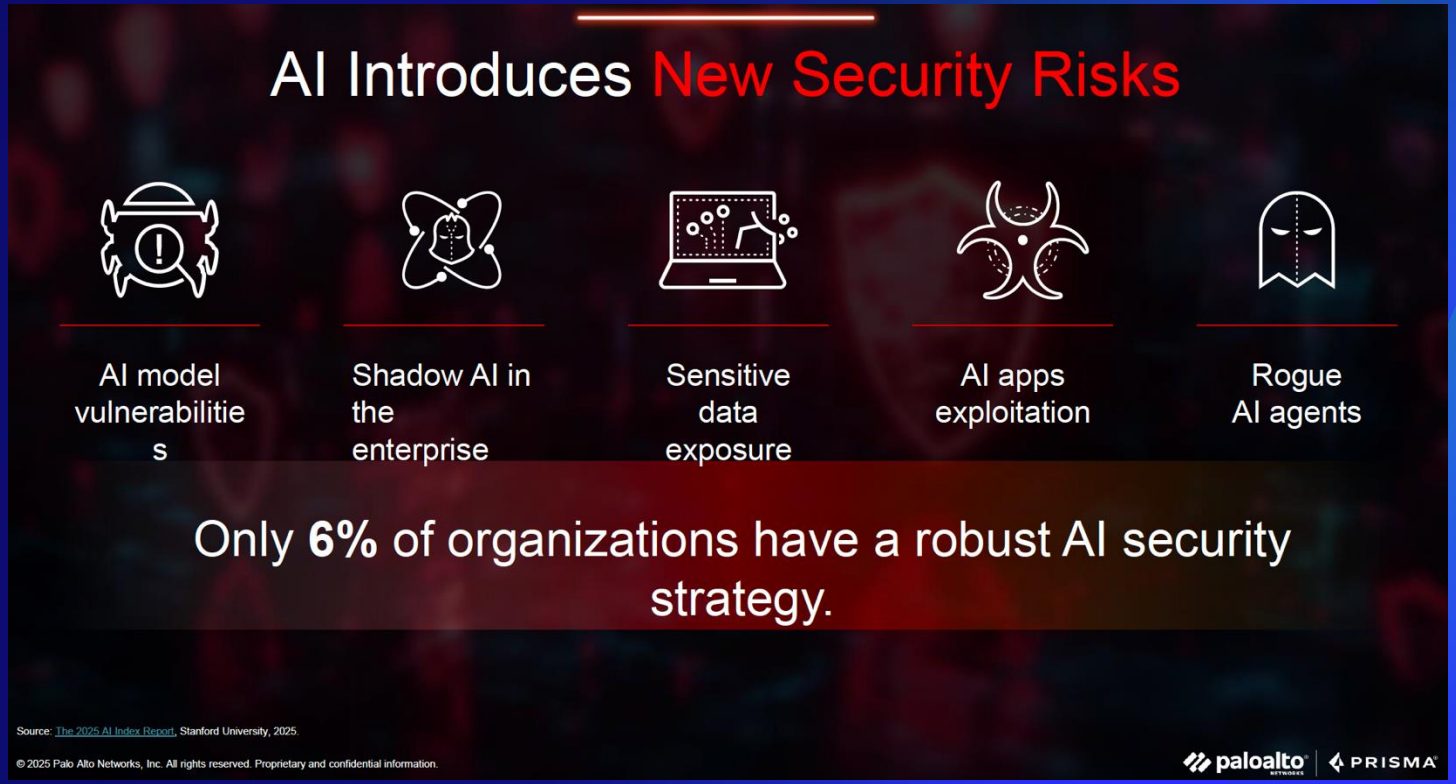
> Adoptar agentes de IA puede acelerar los tiempos de 40% a 50% y reducir los costos mas del 40% a la vez que mejora la Calidad de los resultados.

McKinsey, Dec 2024

> *Para el 2030, mas del 40% de las organizaciones globales sufrirán incidentes de seguridad o cumplimiento debido al uso de herramientas de IA no autorizadas.*

Gartner

Riesgos por IA



Riesgos por IA

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

Gartner Predictions for CISOs' Focus

Gartner

Top cybersecurity trends for 2026

Secure
new frontiers

Post-quantum moves from theoretical risk to action plans

IAM adapts to secure and enable AI agents

Transform
governance

AI and cyber resilience redefine the CISO's remit

Global regulatory volatility drives massive cyber resilience efforts

Normalize
AI adoption

GenAI breaks traditional cybersecurity awareness tactics

AI-driven SOC solutions destabilize operational norms

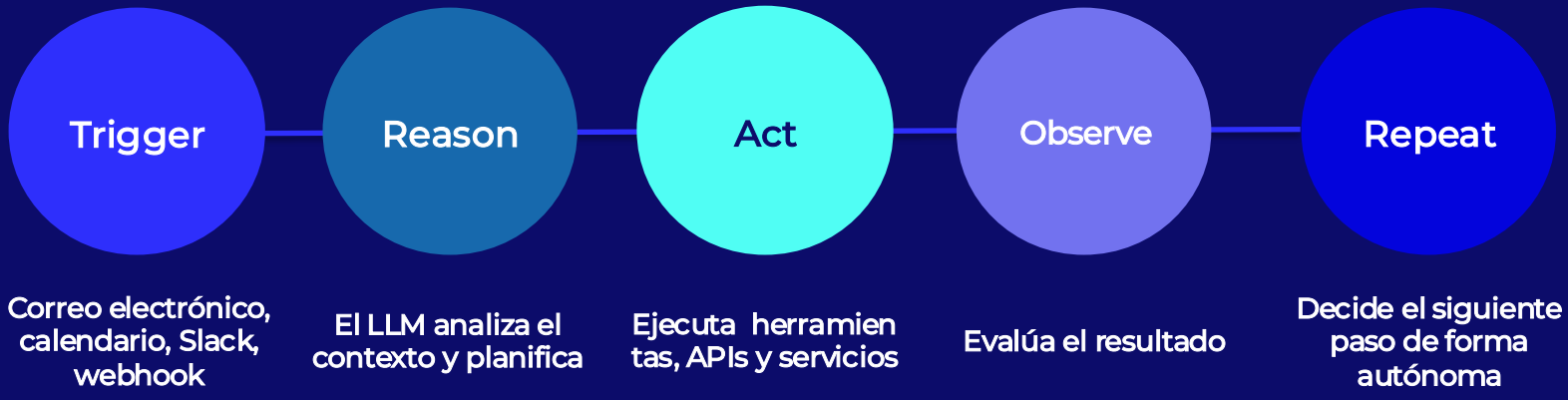
Agentic AI demands program oversight

AI democratization drives collaborative data security governance

Agentes “Inteligentes”

¿Qué son los Agentes?

Y por qué cambian fundamentalmente el modelo del riesgo



La gran diferencia entre LLM y Agentes, es que los agentes no solo responden preguntas. Ellos toman acciones de manera autónoma.
¡Ellos deciden los siguientes pasos!

La Trifecta Mortal

Tres capacidades de los agentes que, combinadas, rompen los modelos de seguridad tradicionales.

Acceso a Datos Privados

Lee archivos, bases de datos, repositorios de código y herramientas internas.

Exposición a Contenido No Confiable

Procesa páginas web, mensajes y documentos provenientes de fuentes no verificadas.

Capacidad de Exfiltrar Datos

Puede llamar APIs, publicar en Slack, hacer commits de código o compartir archivos externamente.

Cualquiera de las dos = riesgo manejable. Las tres juntas = la trifecta mortal.

Recomendaciones prácticas

1. Visibilidad

- Inventario de IAs internas y externas.
- Inventario de comunicaciones
- Inventario y clasificación de datos sensibles e identidades
- Redefinir el monitoreo, alerta y respuesta

2. Límites

- Definir Políticas de IA
- Herramientas aprobadas y prohibidas
- Uso aceptable
- Supervisión humana
- Definir niveles de riesgo a evitar
- Apegarse a frameworks existentes
- NIST AI RMF
- ISO 42001
- CSA AI-CM, AI-CAIQ

3. Responsabilidad

- Gobierno de Identidades (no solo gestión)
- Asignar propiedad
- Crear flujos de aprobación
- Registrar su uso
- Entrenar y concientizar usuarios

Estrategia a corto plazo

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026

1 VE LA IA

- Ten visibilidad, loggea todo uso de IA: apps, identidad, tráfico, intención, infraestructura on prem y on cloud, interna o con terceros y establece la norma para detectar anormalidades.
- *Sin esto, todo lo demás es solo adivinación*

2 MOLDEA LA IA

- Establece políticas, enruta inteligentemente, establece límites, protege los datos en ambos sentidos y participa desde el diseño.
- *Convierte la visibilidad en gobernanza*

3 PROVEE LA IA

- Conecta al gobierno con los resultados de la IA, Mapea las métricas que al negocio le interesan (Productividad, Velocidad, Producción y supervivencia de los modelos o agentes).
- *Rompe el ciclo de medidas sin sentido*

Mi recomendación como IRM

1. No gestiones las identidades y los accesos, *GOBIÉRNALOS*
2. Clasifica y gestiona tus datos, sus ubicaciones y quiénes los acceden
3. Inventario en tiempo real y claro de tus activos de información normales y usados por la IA.
4. Gestiona tu superficie de ataque: prueba como el enemigo, defiende según tu análisis de riesgo.
5. Gestiona la visibilidad, adecúa el monitoreo, define las alertas y practica la respuesta.

¡Gracias!

inception
Un evento de TrustDimension
EXECUTIVE SUMMIT
2026