VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA
Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

segura

Identidades Blindadas:

Protegiendo las 'Llaves del Reino' en la Era de la IA

Ivan Rosales

Territory Manager LATAM – Segura®

VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PREVENCIÓN
DE FRAUDES Y SEGURIDAD FÍSICA

CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA
Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

segura

Identidades Blindadas

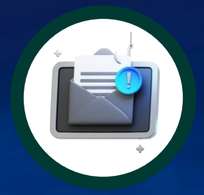
Protegiendo las 'Llaves del Reino' en la Era de la IA

La Anatomía de la Brecha Moderna

Identity Kill Chain: El nuevo vector de ataque

Los atacantes ya no hackean, inician sesión

Movimiento lateral automatizado



INGENIERÍA SOCIAL / PHISHING

Phishing por correo electrónico, suplantación o phishing.

Atacantes engañan a empleados para robar credenciales iniciales.

COMPROMISO DE CREDENCIALES

Acceso exitoso usando credenciales robadas o adivinadas.

Cuentas de servicio no gestionadas.

ESCALAMIENTO DE PRIVILEGIOS

Uso de credenciales iniciales para obtener accesos más altos.

Búsqueda de permisos excesivos o vulnerabilidades.

MOVIMIENTO LATERAL

Navegación por la red buscando activos críticos y bases de datos.

Aprovechamiento de la confianza entre sistemas.

EXFILTRACIÓN / RANSOMWARE

Robo de información sensible y encriptación de sistemas esenciales.

Impacto masivo en el negocio.

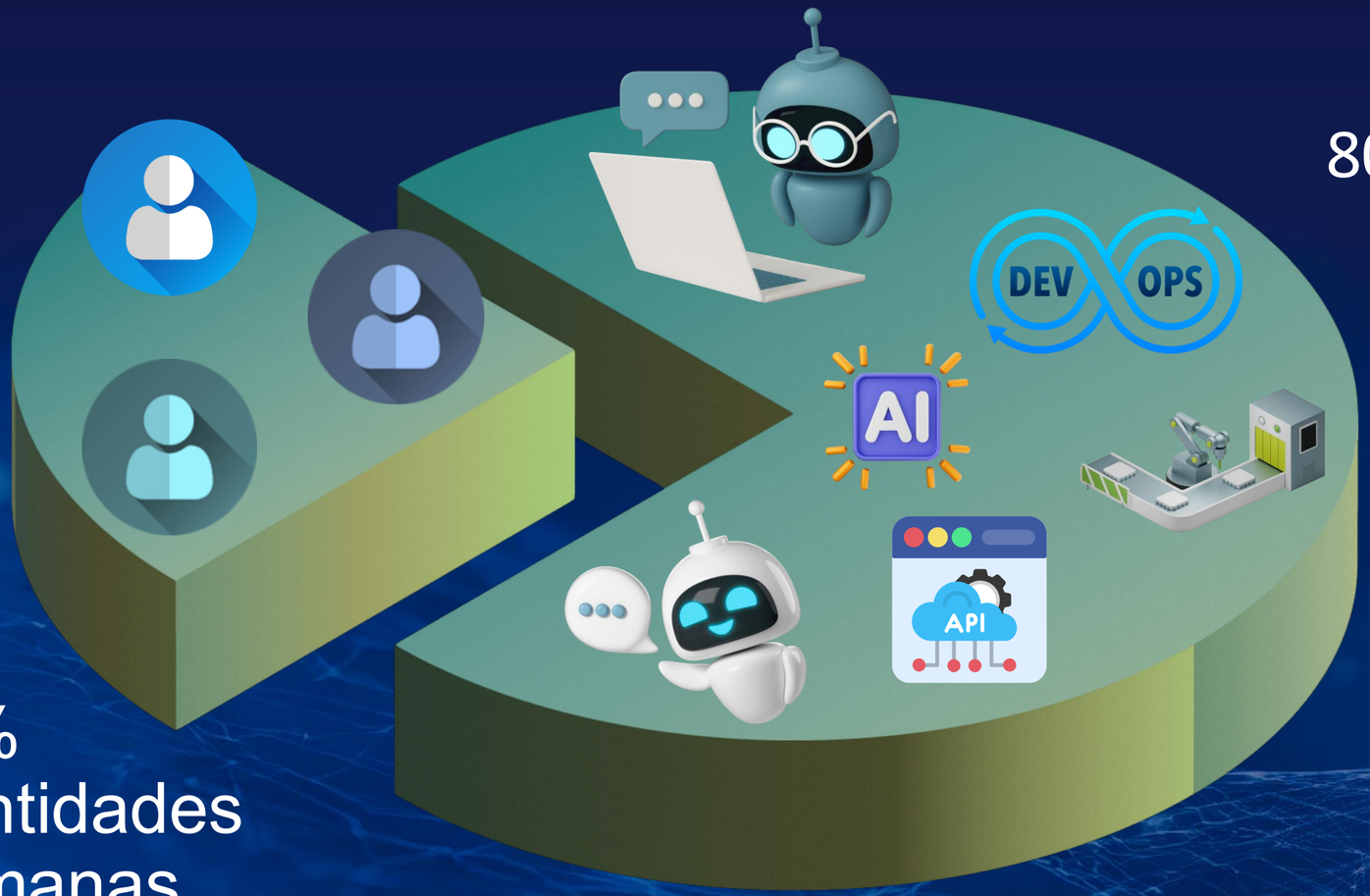
Cumplimiento Normativo y Riesgo Financiero

Regulaciones actuales: ISO 27001, PCI-DSS, Leyes Locales

Trazabilidad irrefutable como mandato legal

Impacto financiero de la falta de gobernanza

La Expansión de la Superficie de Ataque



80% Identidades de Máquina

Riesgo ciego en RPA, APIs, DevOps y Cloud

20% Identidades Humanas

Privilegios perpetuos: el mayor punto de falla

Evolución de la Estrategia PAM

- De Bóvedas de Contraseñas a Zero Trust
- Zero Standing Privileges (ZSP)
- El poder del acceso Just-in-Time (JIT)

PRIVILEGIOS PERMANENTES	DIMENSIÓN / CATEGORÍA.	ACCESO JUST-IN-TIME (JIT)
24/7/365, Perpetuo	DURACIÓN	**Temporal** (Minutos/Horas)
Procesos Manuales Aprobación Heredada	SOLICITUD	**Flujos Automatizados** Justificación Explícita
Alto Riesgo (Standing Privileges)	EXPOSICIÓN	**Mínima Superficie de Ataque**
Logs Vagos Difícil Trazabilidad	GOBERNANZA	**Grabación de Sesiones** Trazabilidad Completa
Estático Confianza Implícita	POSTURA	**Dinámico,** Basado en Zero Trust y Contexto
Fricción Operativa Retrasos	IMPACTO	Agiliza Procesos Frictionless

DevSecOps: Seguridad sin Fricción

Integración transparente mediante APIs

Asegurando el pipeline CI/CD

Habilitando al negocio sin frenar el desarrollo

Gobernanza de Terceros (Supply Chain Risk)

Eliminación de VPNs abiertas para proveedores

Accesos granulares y sin agentes

Aislamiento y grabación de sesiones

La IA en el Arsenal Ofensivo

- Deepfakes y suplantación de identidad C-Level
- Automatización de escaneo de vulnerabilidades
- Asimetría de velocidad: MTTR humano vs. IA atacante

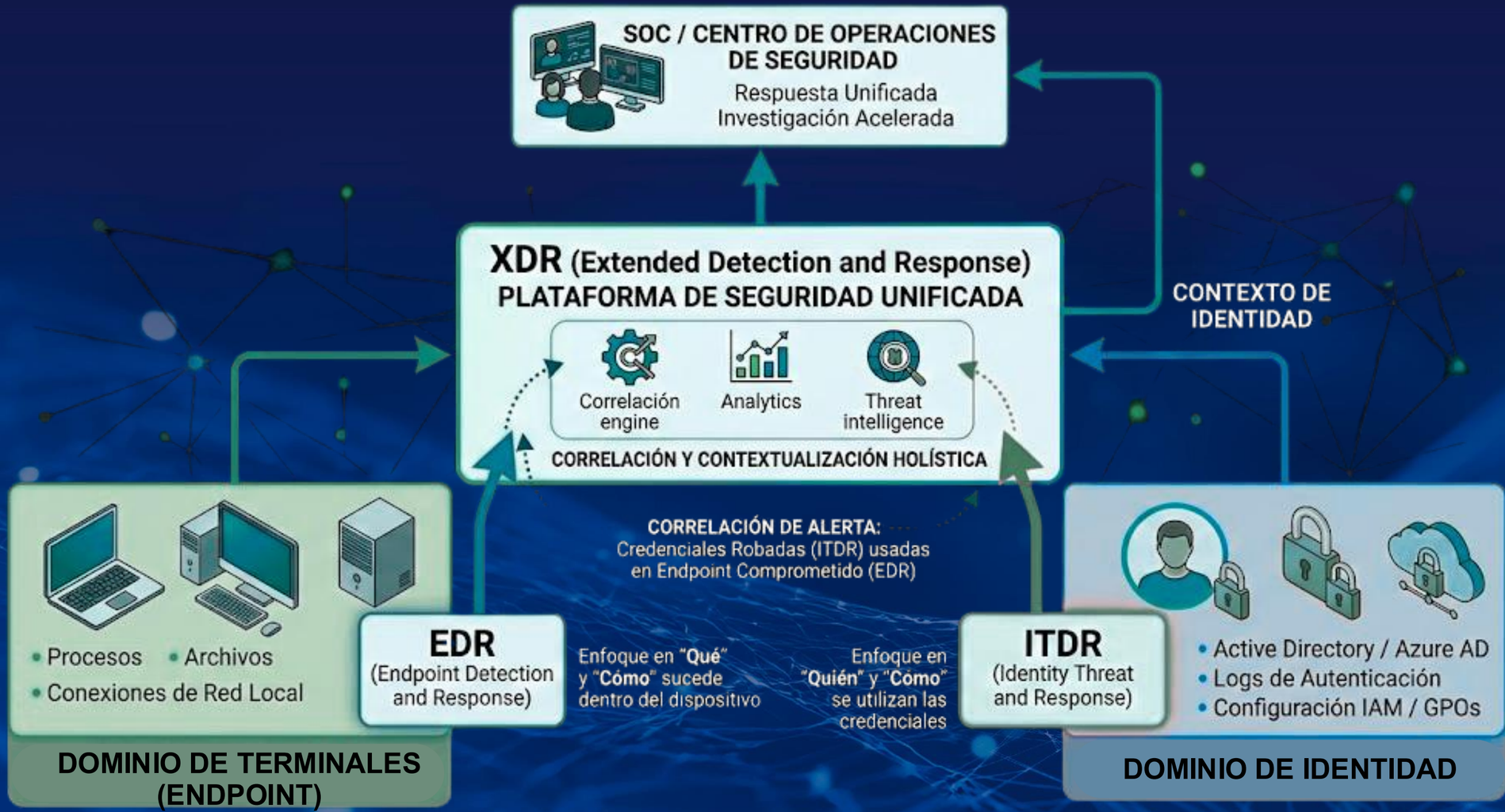
1. Recopilación masiva de datos

2. Síntesis de identidad por IA (Deepfakes)

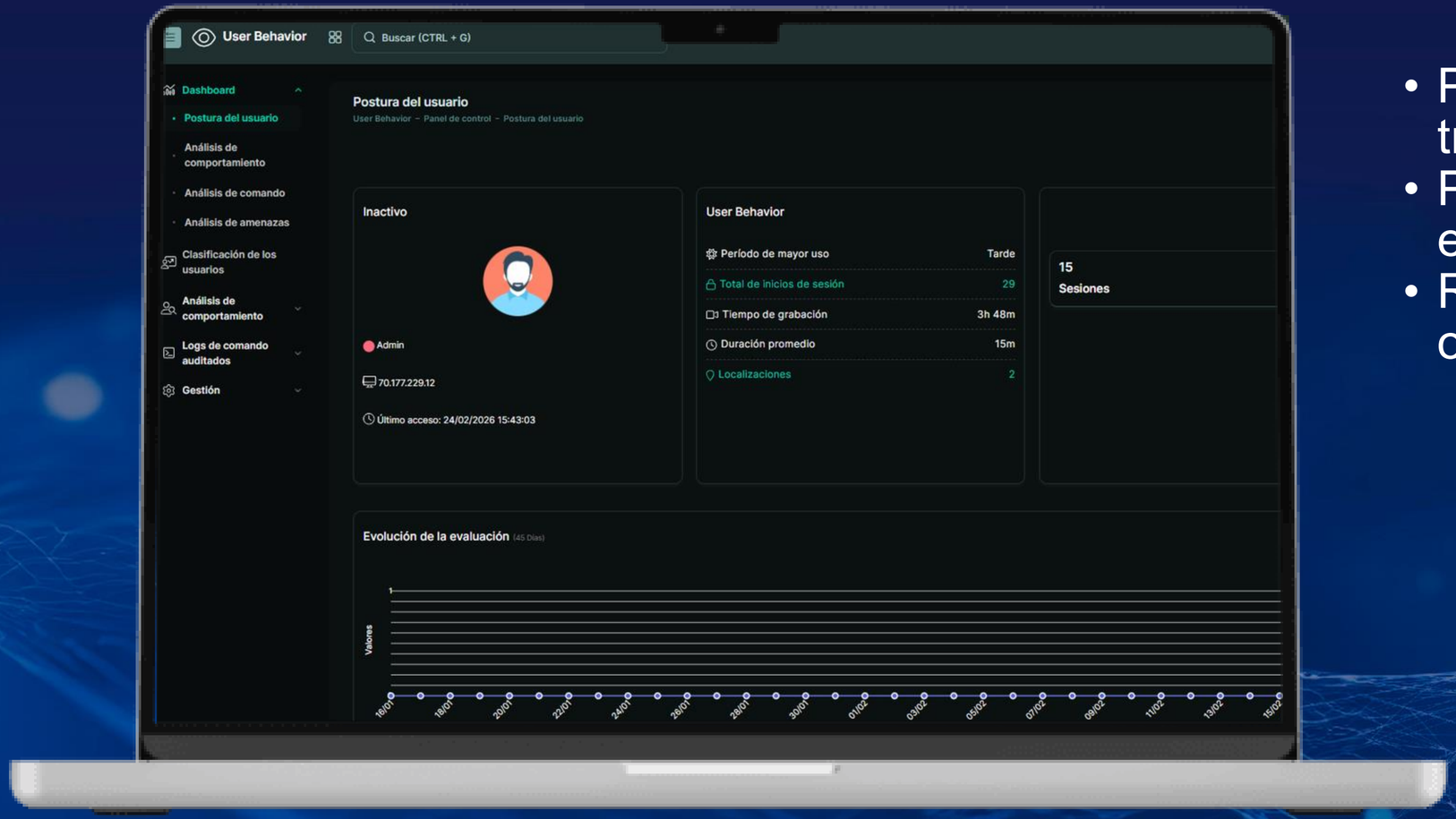
3. Ataque de 'Phishing' dirigido

4. Robo de cuentas y fraude

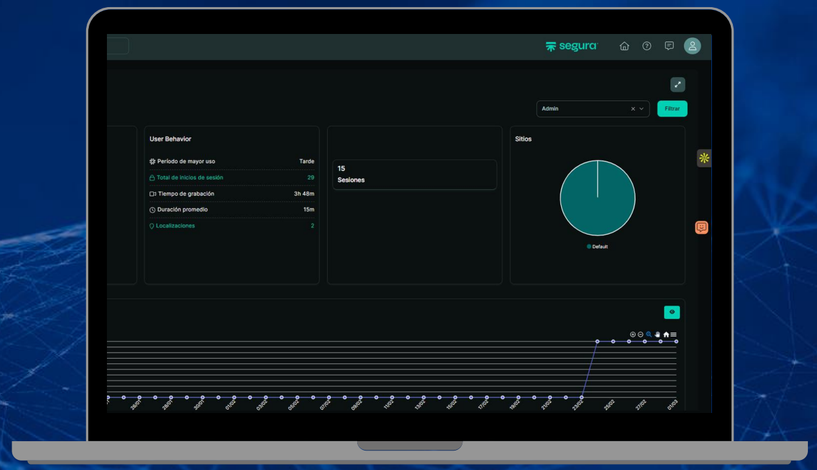
El Surgimiento del ITDR



IA Conductual (UEBA) y Riesgo Dinámico



- Perfilado de comportamiento transaccional
- Puntuación de riesgo (Risk Score) en tiempo real
- Respuesta autónoma: aislamiento o mitigación adaptativa



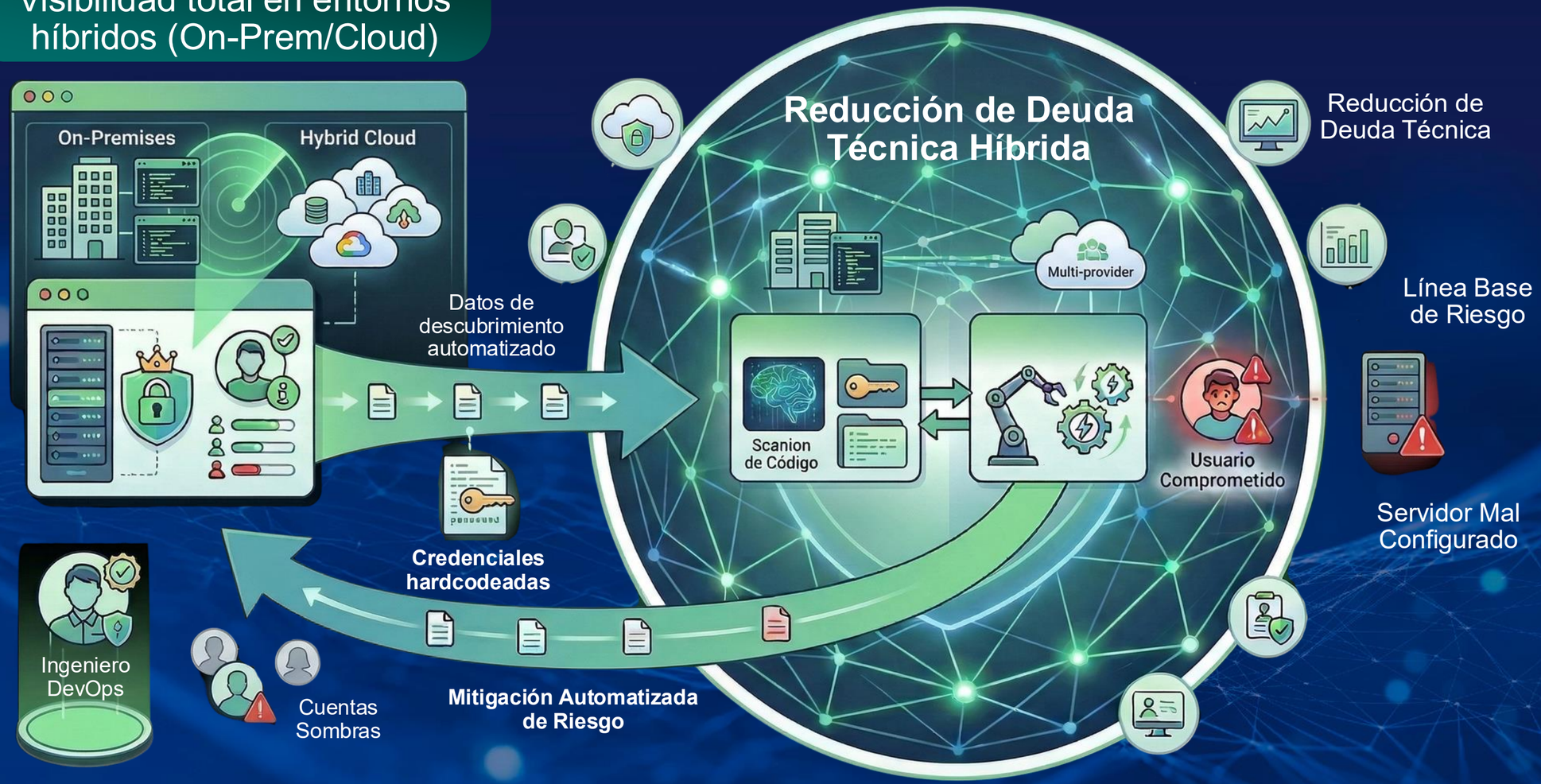
Integración con el SOC

- Telemetría enriquecida hacia el SIEM
- Orquestación de respuestas con SOAR
- Creación de una Malla de Ciberseguridad resiliente

Descubrimiento y Reducción de Deuda Técnica

Visibilidad total en entornos híbridos (On-Prem/Cloud)

- Identificación de cuentas sombra
- Mitigación de credenciales hardcodeadas



VI CONGRESO INTERNACIONAL DE CIBERSEGURIDAD, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

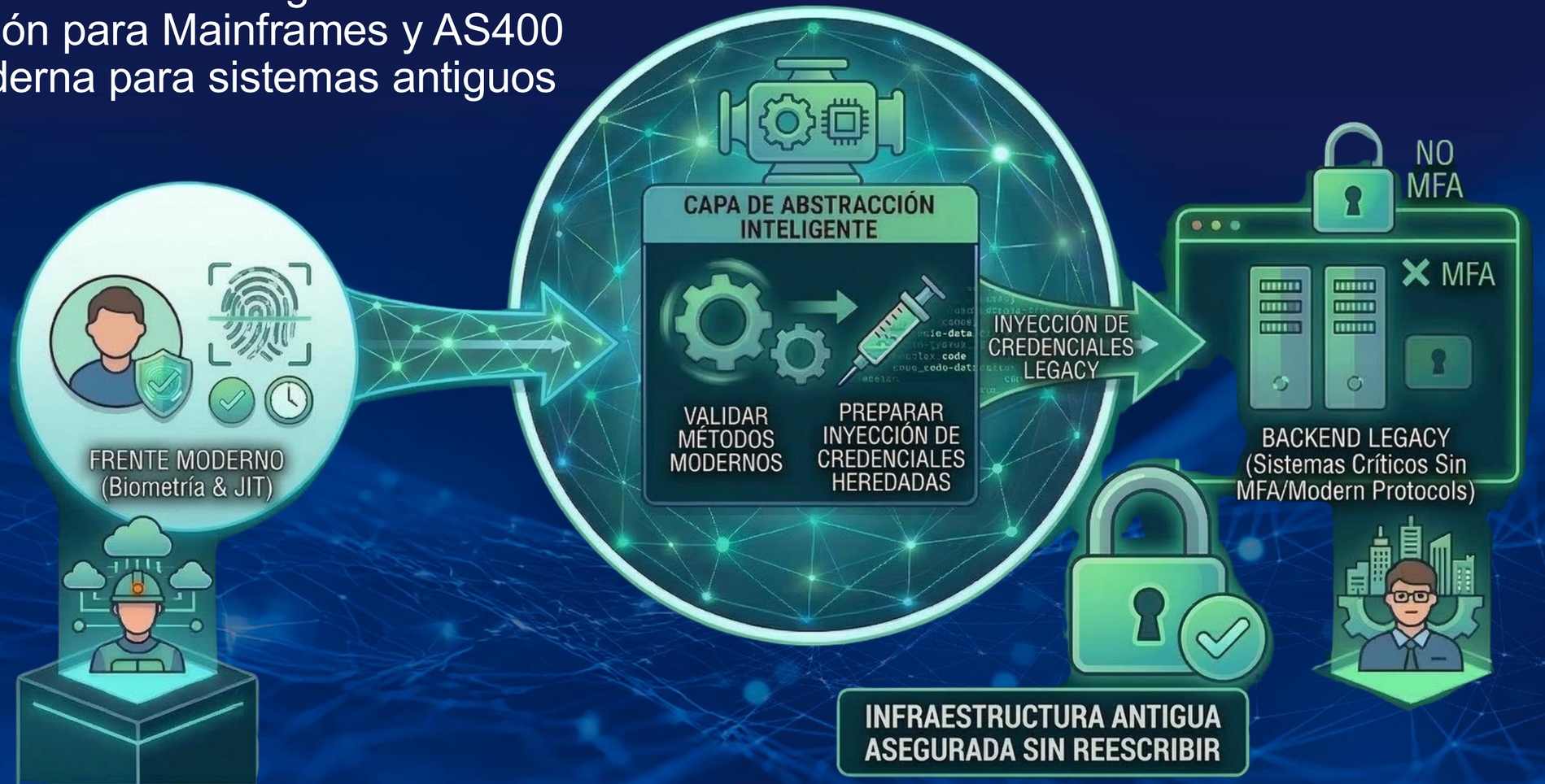
CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO

segura

El Tablero del CISO: Métricas para la Junta

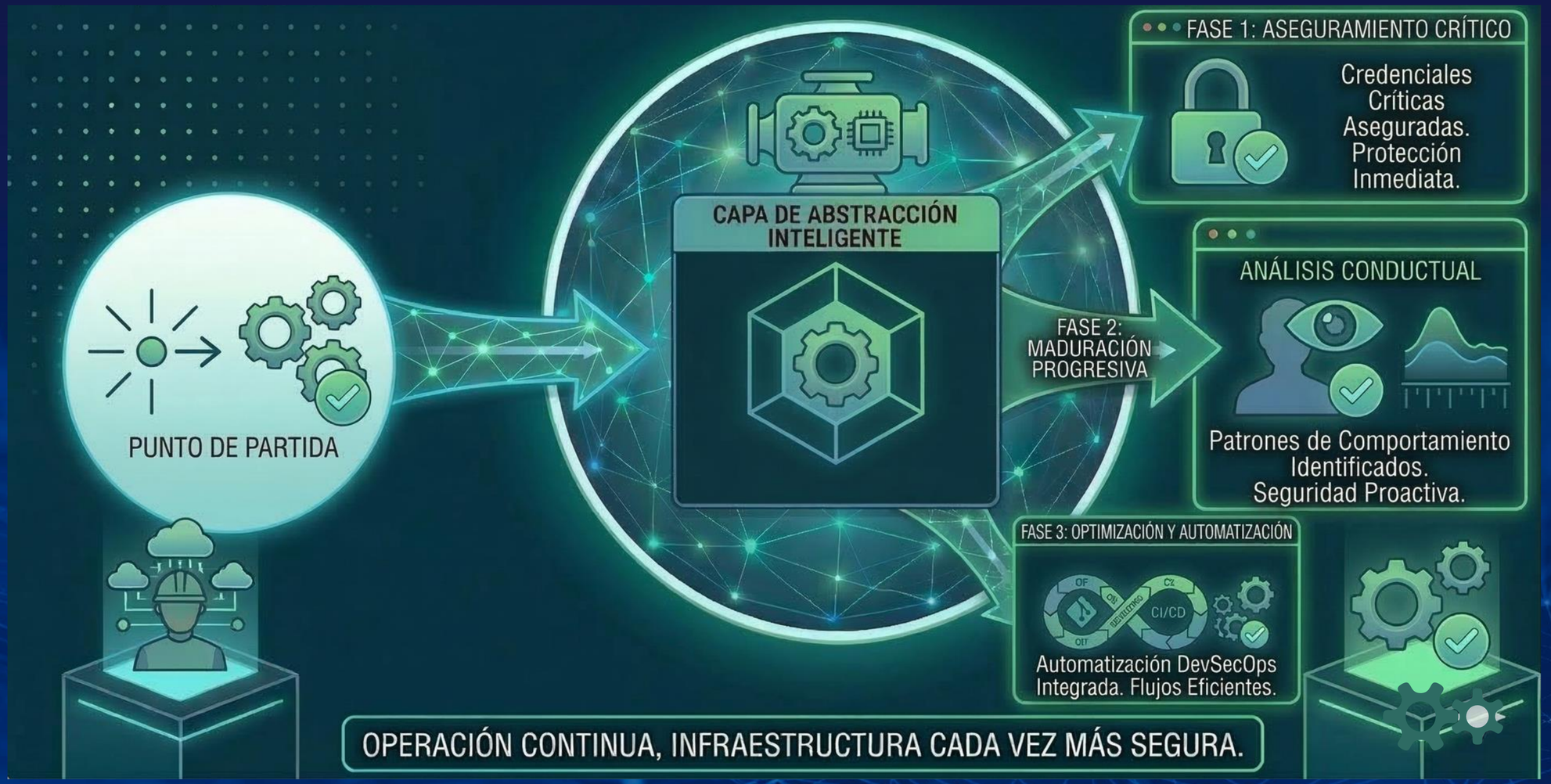
Superando la Deuda Heredada (Sistemas Legacy)

- Modernización sin reescribir código
- Capa de abstracción para Mainframes y AS400
- Autenticación moderna para sistemas antiguos



El Framework de Implementación Ágil

- Fases basadas en el nivel de riesgo
- Día 1-30: Visibilidad y control de terceros
- Madurez hacia DevSecOps y análisis conductual



segura

Próximos Pasos

- Programa un Identity Risk Assessment
- Visítanos en el nuestro Stand

segura®

Solicítalo hoy

¡GRACIAS POR TU ATENCIÓN!