_ T H I N K A H E A D , A C T N O W .

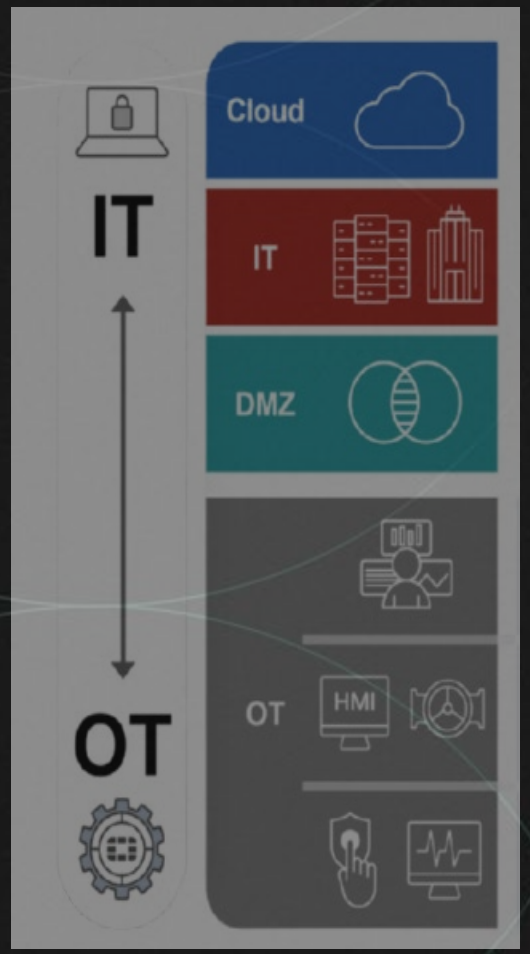
SEK Security Ecosystem Knowledge

MDR PARA OT:
PROTEGIENDO EL CORAZÓN DE TU OPERACIÓN.

UNA ALIANZA ESTRATÉGICA PARA PROTEGER SU EXCELENCIA Y A SUS PACIENTES

_ T H I N K A H E A D , A C T N O W .

EL PARADGMA



	IT	OT
Aspecto	**Paradigma IT (Tecnología de la Información)**	**Paradigma OT (Tecnología Operacional)**
Prioridad principal	Confidencialidad de los datos	Disponibilidad y continuidad operacional
Frecuencia de actualizaciones	Regular, con parches frecuentes	Limitada, debido a riesgos de interrupción
Tolerancia a fallas	Alta: se pueden reiniciar sistemas	Baja: reiniciar puede afectar producción o seguridad física
Protocolos de comunicación	Estándares (TCP/IP, HTTP, DNS)	Protocolos propietarios o industriales (Modbus, OPC, etc.)
Visibilidad de activos	Alta, herramientas bien establecidas	Baja, muchas veces sin inventario preciso
Respuesta ante incidentes	Automatizada, con uso de SOAR/SIEM	Coordinada y cautelosa, considerando seguridad física
Tipo de amenazas	Malware, ransomware, phishing	Ransomware, amenazas persistentes, manipulaciones físicas
Usuarios y endpoints	Humanos y endpoints tradicionales (PCs, móviles)	PLCs, sensores, actuadores, HMIs
Herramientas MDR tradicionales	SIEM, EDR, NDR	Requiere integración con plataformas OT-aware (ej. Claroty)
Regulaciones aplicables	GDPR, ISO 27001, LGPD	IEC 62443, NIST 800-82, ISA/IEC 61511

UTILITIES COMPANY

Challenge

- Equipos distintos IT/OT
- Partners distintos IT/OT
- Dificuldad em tener una
- gestion de riesgos unificada
- Falta de un plan de respuesta a incidente unificada

Solution

- Assessment de riesgos de IT y OT
- Diagnostico de Maturidad
- Consultoria para governança ITyOT
- SOC Convergente con las plataformas Qradar, Qualis y Claroty e Crowdstrike.
- MDR Operacion
    - 04 FORTIGATE 80F (2HA)
    - 01 FIREWALL CISCO
    - 7 SERVIDORES NA AZURE (2WINDOWS e 5 LINUX)
    - AZURE AD
    - CLOUD AZURE
    - IAM AZURE
    - AV/EDR MICROSOFT DEFENDER
    - O365
    - CLAROTY
    - CROWDSTRIKE

Resuts

- Gestion centralizada de todos los riesgos.
- Aumento de maturidad de lo ambiente de OT
- Plan de detecção y respuesta a incidentes unificada.
- Reducion en los costos de múltiplo partners,

_ T H I N K A H E A D , A C T N O W .

WHY SEK?

_ T H I N K A H E A D , A C T N O W ,

SEK Security Ecosystem Knowledge

Regional Service

Able to support multilanguage countries

Specialization in OT environments

- +1000 certifications in cybersecurity and +30 specific to the OT environment.
- Representation of the best brands in the OT industry, such as Tenable OT, Nozomi, Claroty, Fortinet among others.

Experience With OT Customers

- We understand the industry's challenges.
- We are able to combine IT/OT expertise to provide a single risk management approach.

_ T H I N K A H E A D , A C T N O W ,

_ T H I N K A H E A D , A C T N O W .

SEK Security Ecosystem Knowledge

MDR

MANAGED DETECTION RESPONSE

+200 CLIENTES
Tenemos el MDR más grande de América Latina.

+250 PROFESIONALES
dedicados.

98,7% DE AUTOMAÇÃO
De casos a través de la IA.

+500 MILLONES
de ataques detectados en 2024.

39,9 MIN
de medio tiempo para la resolución de incidentes críticos.

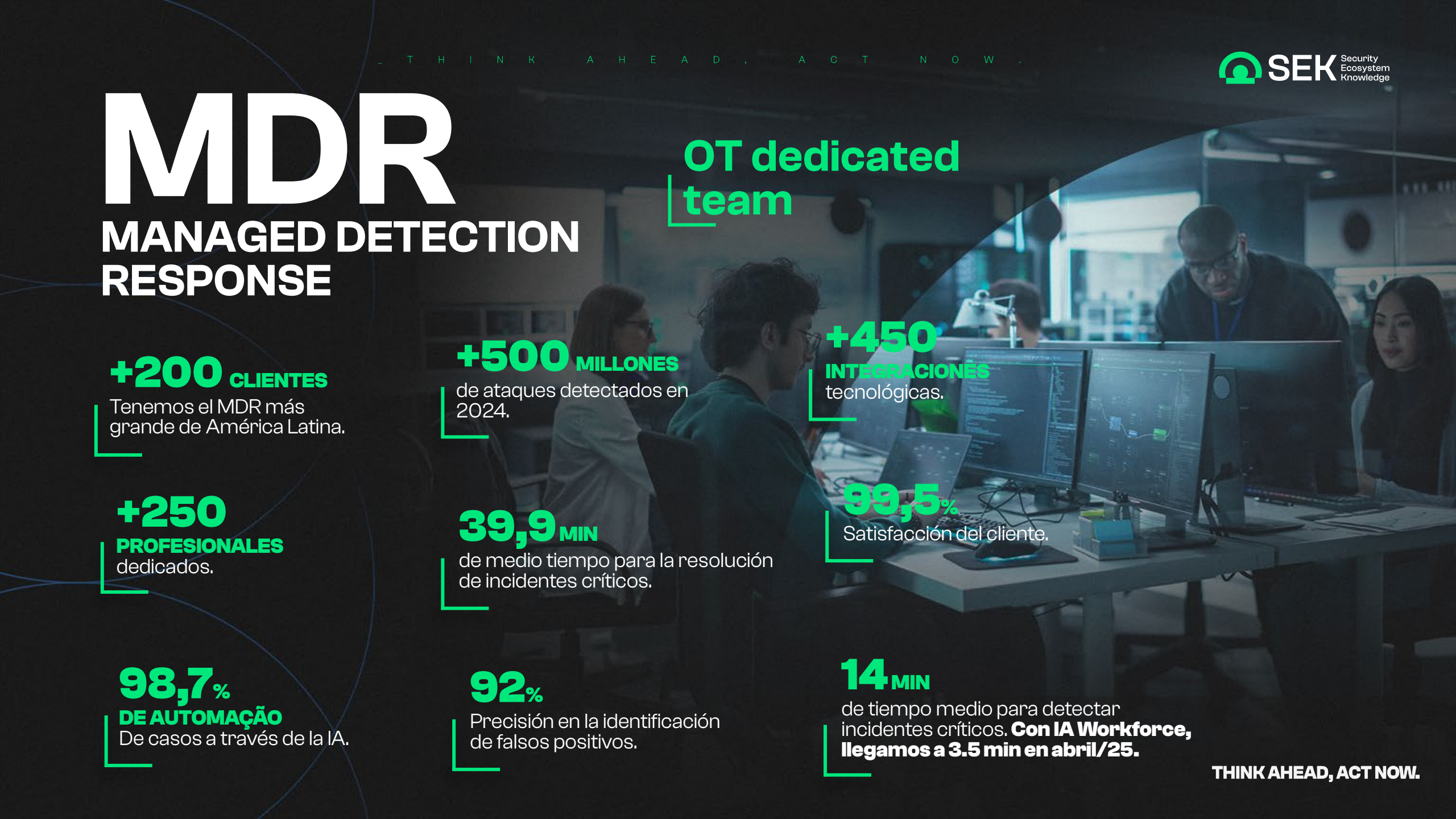
92%
Precisión en la identificación de falsos positivos.

OT dedicated team

+450 INTEGRACIONES
tecnológicas.

99,5%
Satisfacción del cliente.

14 MIN
de tiempo medio para detectar incidentes críticos. **Con IA Workforce, llegamos a 3.5 min en abril/25.**



THINK AHEAD, ACT NOW.


SEK
Security
Ecosystem
Knowledge