Construindo ambientes resilientes

antecipando cenário de ameaças

alissonbaima

alisson.baima

Alisson Baima **Rebouças**

Enterprise Account Manager para o N/NE

alisson.reboucas@kaspersky.com

Geraldo-vasconcelos

geraldoff

Geraldo Vasconcelos

Pre-sales Manager para N/NE

Geraldo.vasconcelos@kaspersky.com

Threat landscape:
history of threats over the past 27 years

1994
Um virus
a cada hora

2006
1
Um virus
a cada minuto

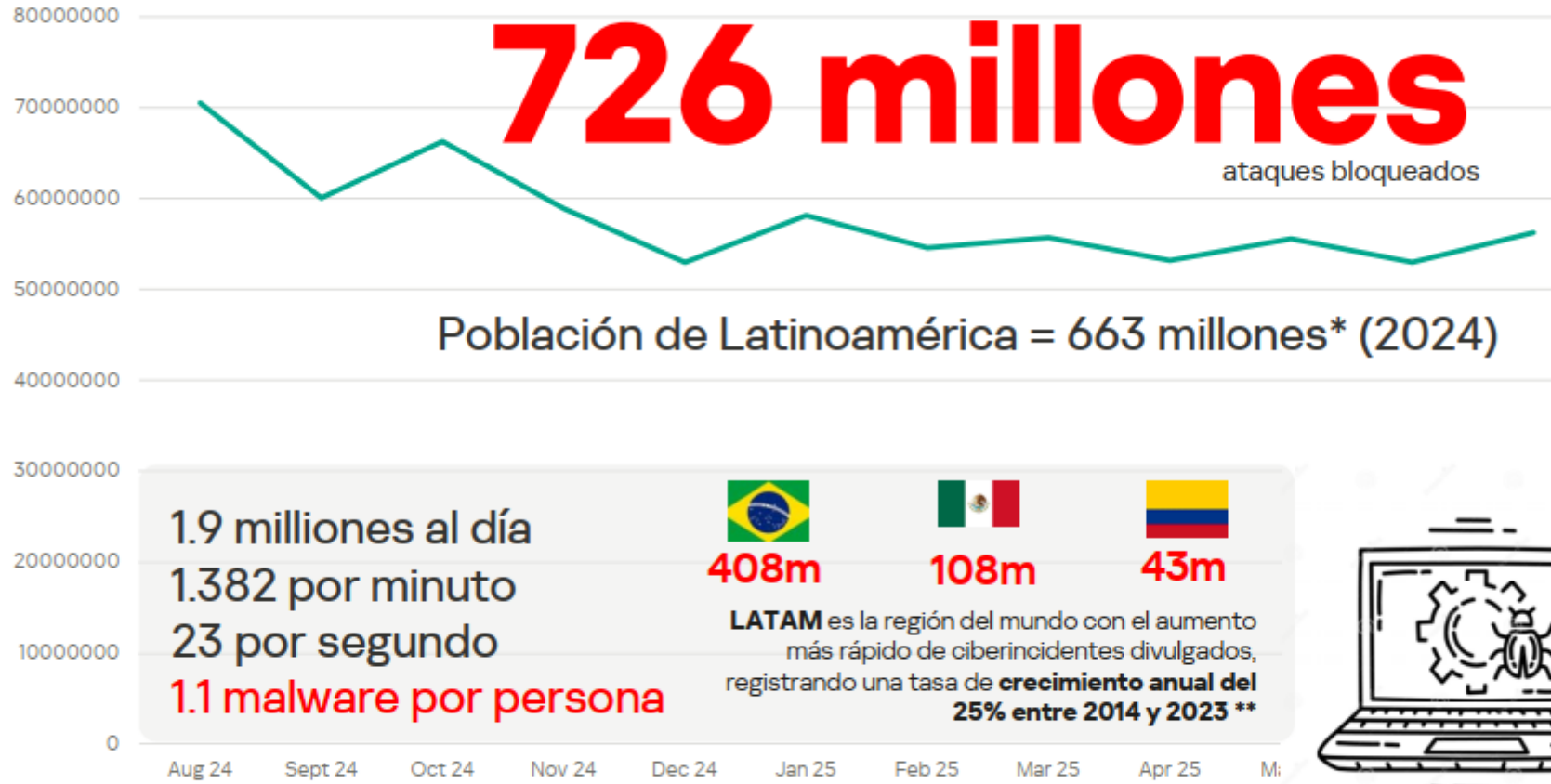
2011
1
Um virus
a cada segundo

2024
440 000
New threats
every day

kaspersky


kaspersky
CYBER SECURITY WEEK
Manaus
Brasil
8-11 de setembro de 2025
Cibersegurança
na Selva Digital

MALWARE (últimos 12 meses)



726 millones

ataques bloqueados

Población de Latinoamérica = 663 millones* (2024)

1.9 millones al día
1.382 por minuto
23 por segundo
1.1 malware por persona

408m

108m

43m

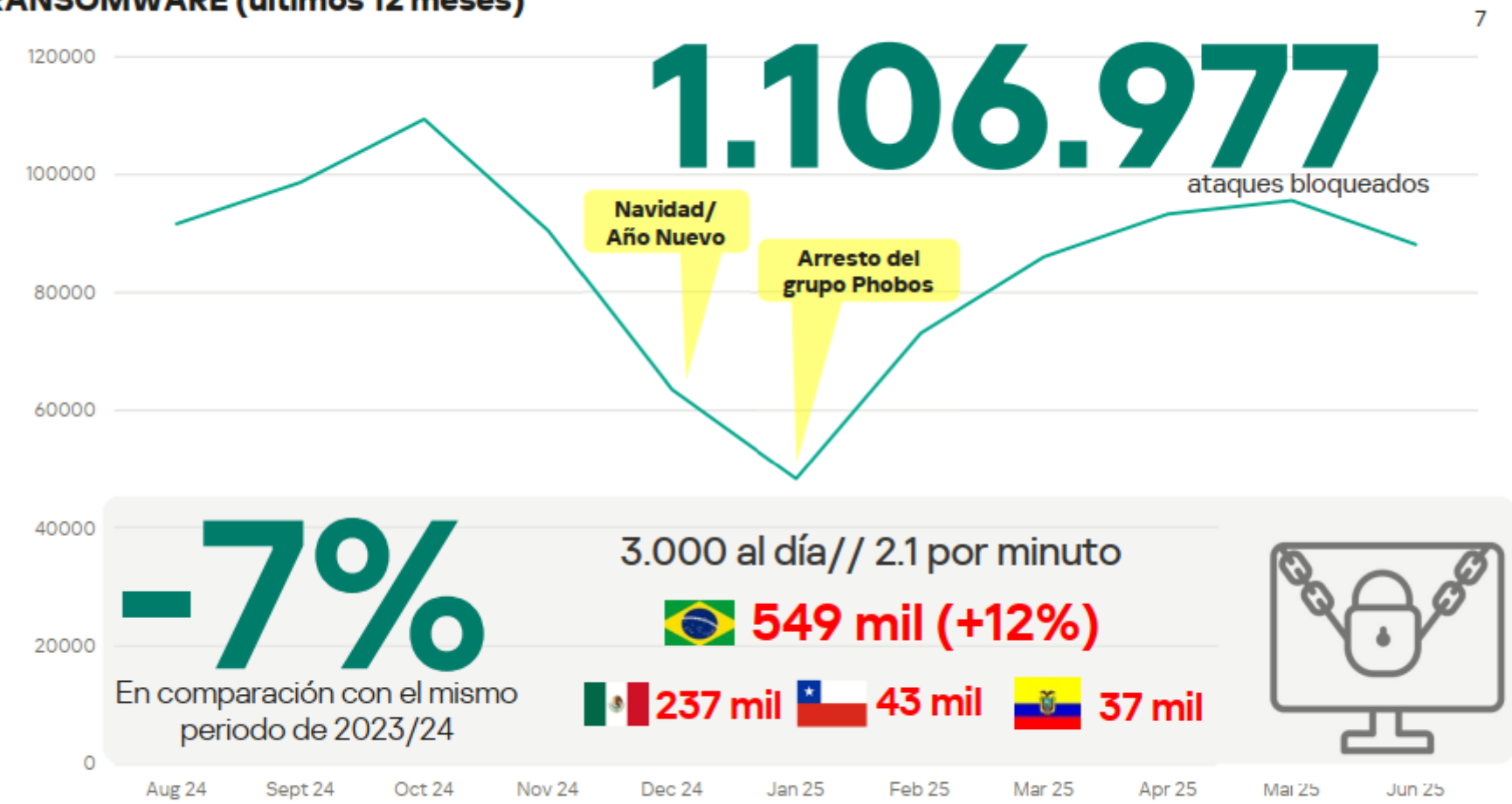
LATAM es la región del mundo con el aumento más rápido de ciberincidentes divulgados, registrando una tasa de **crecimiento anual del 25% entre 2014 y 2023** **

* Datos: CEPAL.org
** Datos Banco Mundial

PHISHING (últimos 12 meses)

5

RANSOMWARE (últimos 12 meses)



Fluindo pela Amazônia

Desvendando a situação das atividades na dark web no Brasil

A equipe do Kaspersky Digital Footprint Intelligence analisou a **situação das atividades na dark web no Brasil**

kaspersky

Today’s challenges

Os ataques estão se tornando mais sofisticado e destrutivos.

Increase in the number of threats

- The adversaries are very fast
- Interactive intrusions attack
- 440K new malwares everyday

Failure to process alerts quickly

- Data fatigue
- Unknown MTTD/MTTR
- Long response times due to manual and complex processes

Shortage of qualified specialists

- 4.8M cybersecurity professionals gap
- 47% of the global demand
- Challenges in hiring and retaining specialized talent

Today’s challenges

Afinal, se o antivirus não é mais suficiente.

O que devemos fazer, para nos anteciparmos, e nos proteger?

Contratar a melhor equipe de SOC?

Contratar o melhor XDR?

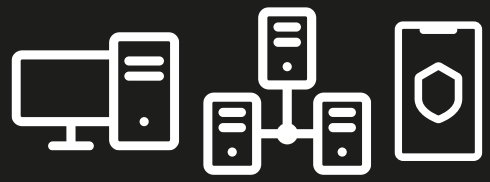
Gestão de Cibersegurança se faz com:
PPT

E na prática, o que realmente importa nesse jogo?
Ser mais rápido que os atacantes!

Então qual é o seu MTTR?

Atacante

70 minutos é o tempo médio de comprometimento de um ambiente
** Breakout time*



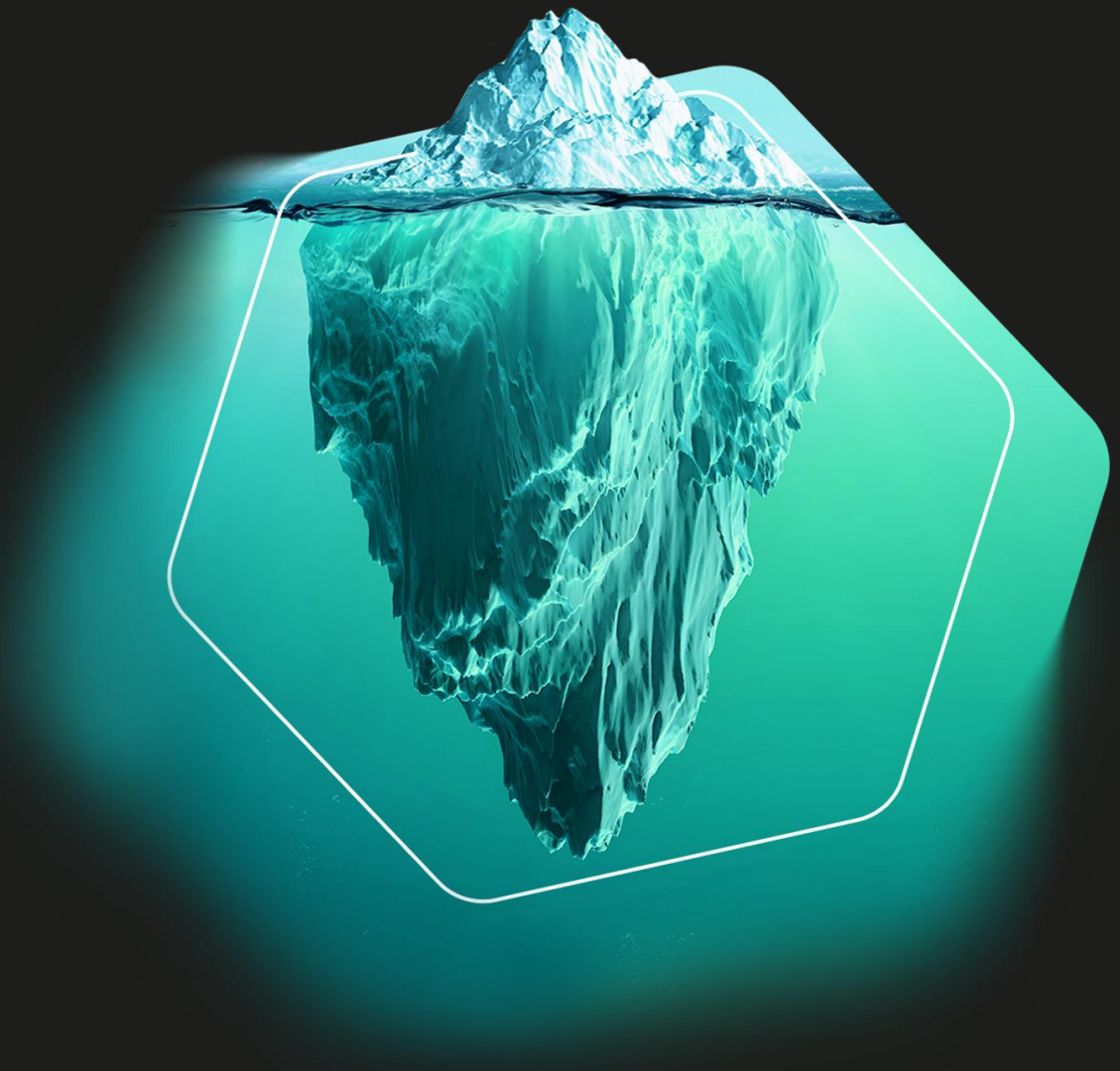
IT Industry

11 dias para responder a um ataque!

Mordenização de ESG SOC e o papel do XDR, 2024 | Resposta a incidentes da Kaspersky, 2024

kaspersky

O real custo da proteção



AQUISIÇÃO DE TECNOLOGIA DE SEGURANÇA DE ENDPOINT

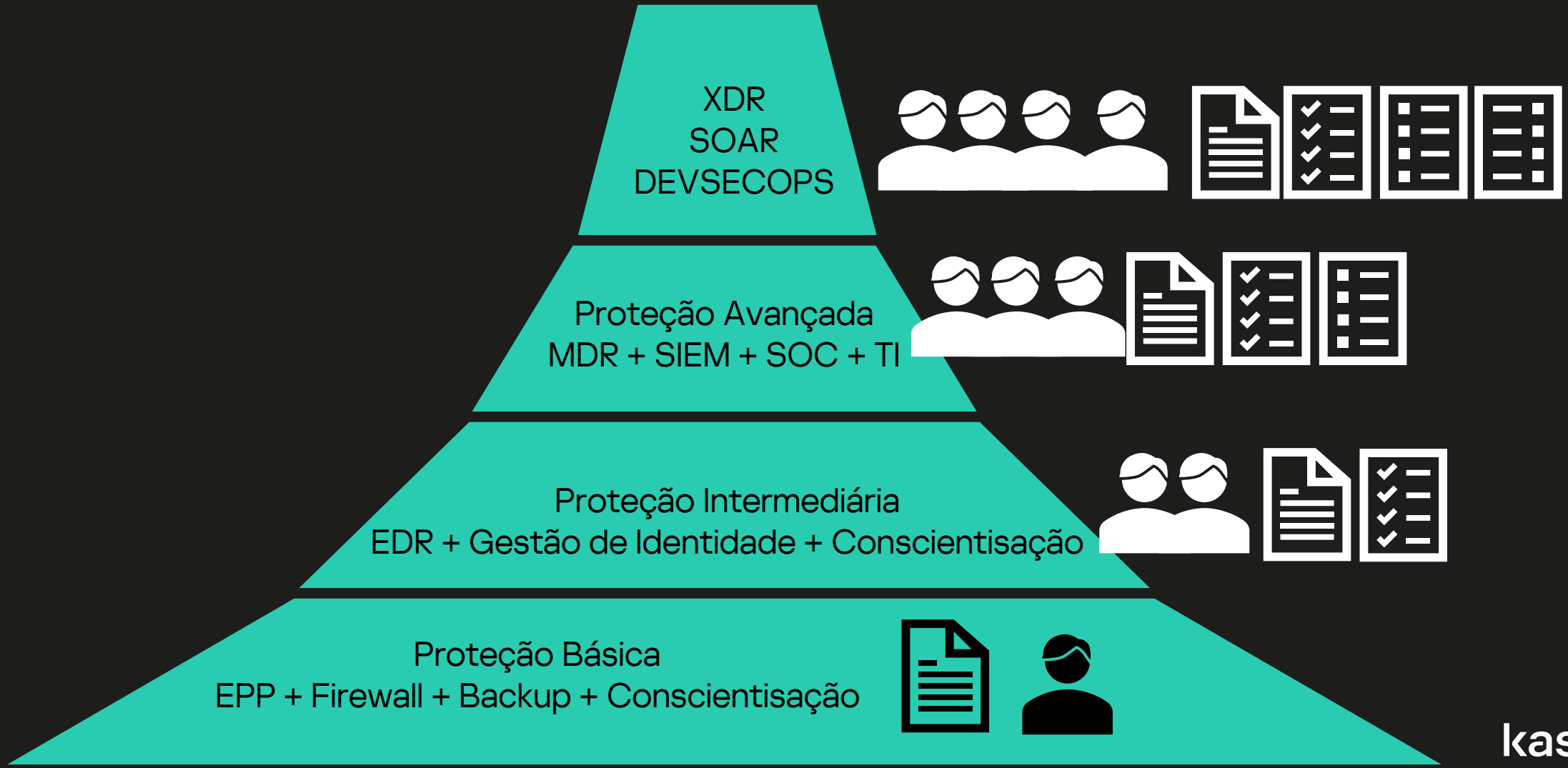
IMPLEMENTAÇÃO, CONFIGURAÇÃO E AJUSTE

MONITORAMENTO, TRIAGEM E ANÁLISE DE ALERTAS

RESPONDER A INCIDENTES E REALIZAR SUA REMEDIAÇÃO

O CUSTO DE UM ATAQUE

ETAPAS DE MATURIDADE DE CIBERSEGURANÇA



Mapeamento das ameaças nas ferramentas, tecnologias e conhecimentos necessários para mitigá-las

Complexidade crescente das ameaças	Ameaças em massa	Ameaças avançadas	Ataques cibernéticos complexos
Conhecimento necessário em segurança de TI	Especialistas de TI	Especialistas em segurança	Especialistas em segurança nível elevado
Conjunto de ferramentas necessário para defesa	Tecnologias automatizadas de prevenção de ameaças EPP FW BKP	+ Tecnologias de detecção e resposta automatizadas EDR MDR IR	+ Caça proativa a ameaças, enriquecimento de dados, investigação detalhada XDR CTI SOAR
% de ameaças	90%	9,9%	0,1%

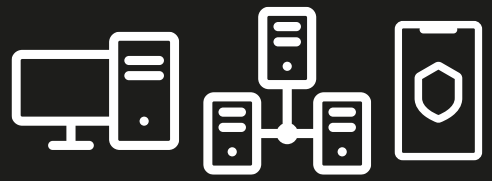
kaspersky

Desafios de hoje:
Qual é o seu MTTR?

Atacante

70 minutos é o tempo médio de comprometimento de um ambiente

** Breakout time*



IT Industry

11 dias para responder a um ataque!

Kaspersky

36 minutos é o MTTR do time da Kaspersky

Como?

Telemetria

Kaspersky AI

MDR Experts + Threat Hunting

kaspersky

Mordenização de ESG SOC e o papel do XDR, 2024 | Resposta a incidentes da Kaspersky, 2024

Enriquecimento de telemetria

Active industry contributor

As a key and active player in global threat intelligence, we work closely with the wider cybersecurity community to combat cybercrime worldwide

INTERPOL

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE 11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

We work alongside international organizations such as INTERPOL, law enforcement agencies, CERTs and the global IT security community on joint cybercrime investigations and operations.

MITRE | ATT&CK®

We contribute critical cyberthreat intelligence to global initiatives, including MITRE, to enhance the accuracy of the ATT&CK framework.

Our work is guided by the ethical principles of responsible vulnerability disclosure.

Kaspersky strengthens security across the industry by identifying and helping to fix zero-day vulnerabilities for leading companies such as Adobe, Microsoft, Google, Apple, etc.

kaspersky

Transparent & independently acknowledged

Proven.
Transparent.
Independent.

The Kaspersky Global Transparency Initiative is built on concrete, actionable measures that allow stakeholders to validate and verify the trustworthiness of our products, internal processes and business operations.

13

Transparency Centers across the world

Regular independent assessments

- SOC 2 audit
- ISO 27001 certification

Learn more

Bug bounty

Recognition that matters

Kaspersky products undergo regular independent assessments by leading research institutes, with our cybersecurity expertise consistently recognized by top industry analysts.

Most tested. Most awarded.

For over a decade, Kaspersky products have participated in 1022 independent tests and reviews, earning 771 first place results and 871 top-three finishes - testament to our industry-leading protection.

In 2024

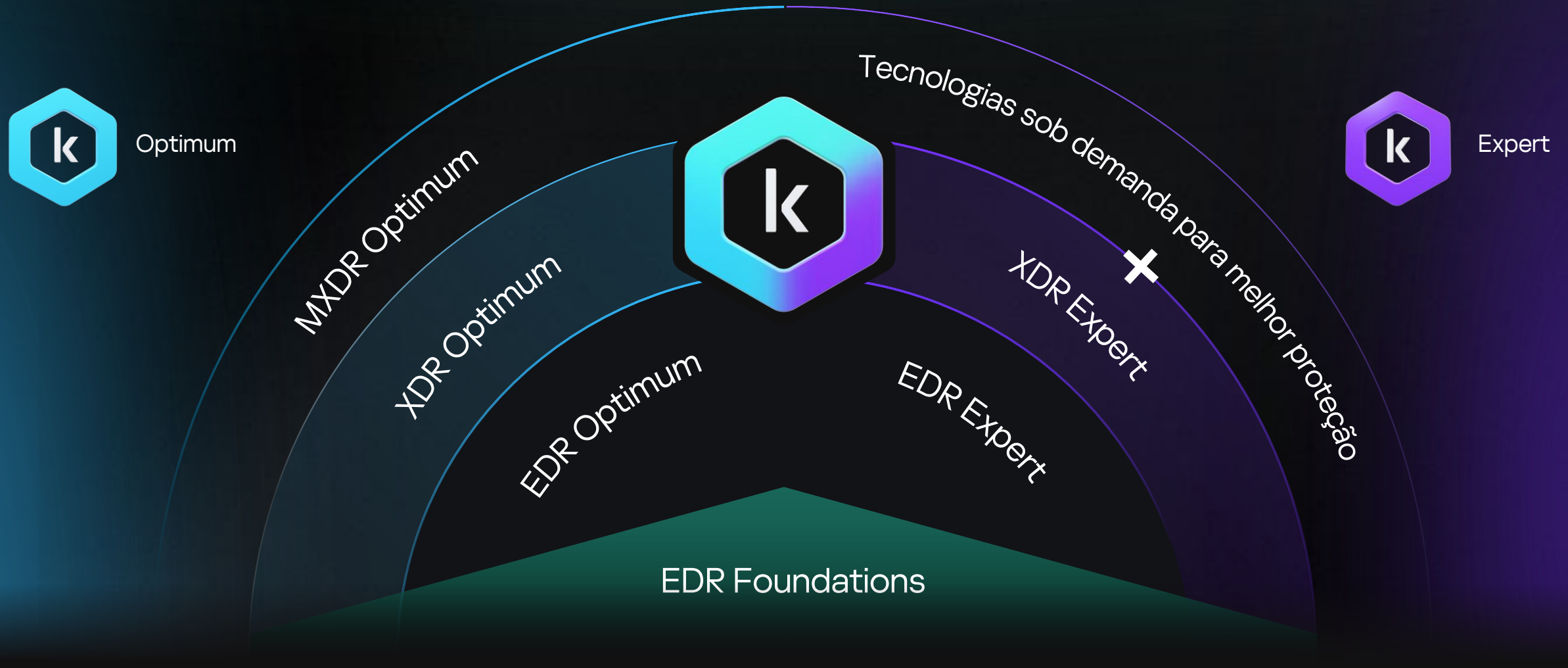
95	91	97%
Tests & reviews	First places	TOP3 places

Learn more

kaspersky

Kaspersky Next

Segurança personalizada para cada empresa



Camadas do Kaspersky Next MXDR Optimum

Recursos de proteção de endpoints

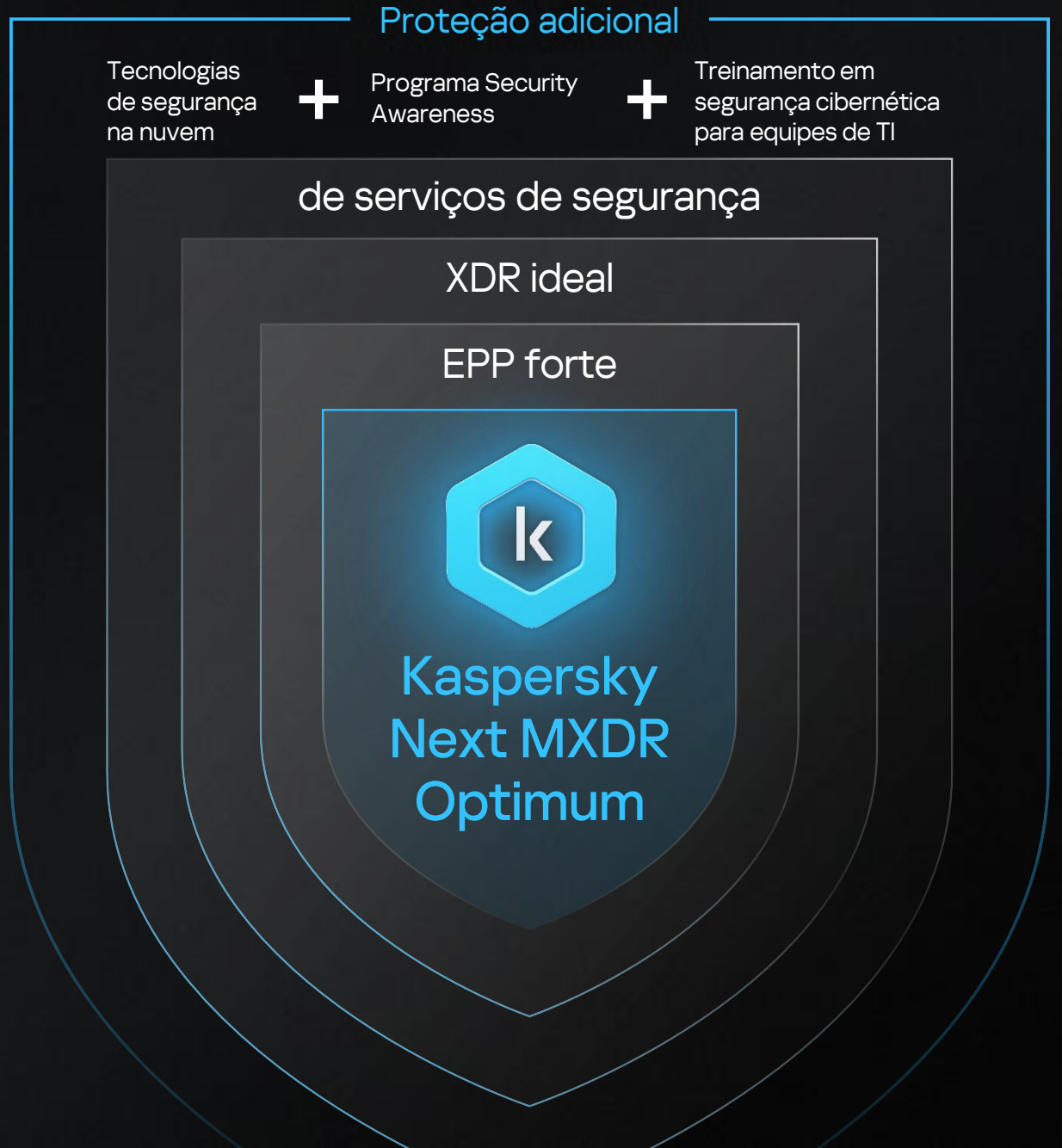
- Antimalware multicamadas
- Reforço reforço
- Verificação de vulnerabilidades
- Endpoint aplicativos
- Dados perímetro
- Gerenciamento de Correções

Detecção, análise e resposta

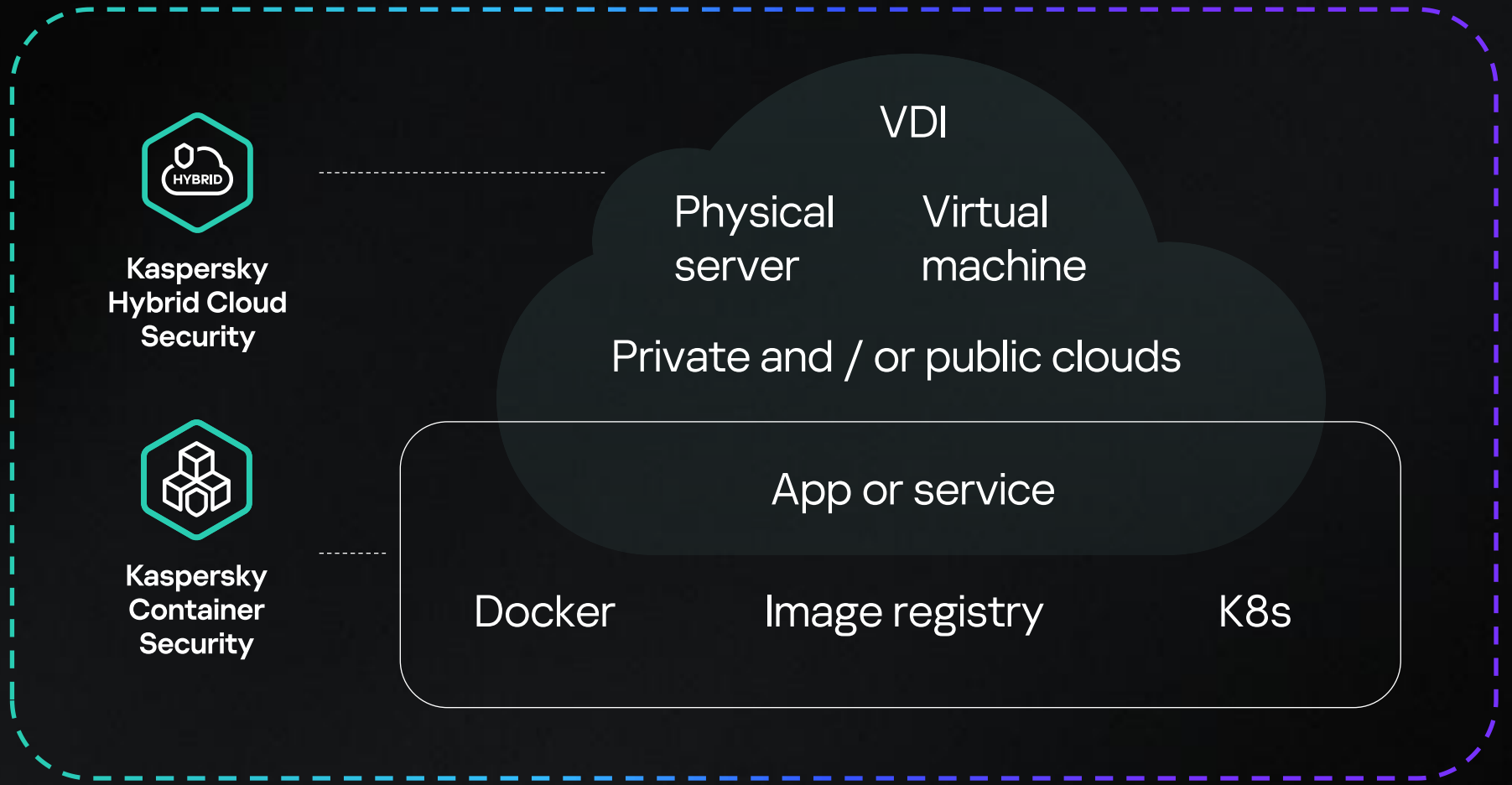
- Detecção comportamental
- Agregação de alertas
- Cloud Sandbox
- Descoberta de evidências de ameaças (IoCs) e IoCs personalizados
- Análise de causa-raiz
- Alcance das ações de resposta

Proteção gerenciada

- Monitoramento contínuo e busca de ameaças 24/7
- Visão geral de todos os recursos protegidos
- Armazenamento de telemetria bruta por 3 meses
- Comunique-se diretamente com a equipe do SOC sobre incidentes
- Envie incidentes
- Resposta orientada e automatizada



Kaspersky Cloud Workload Security



Developers rely on containerization, and businesses are scaling their cloud environments. However, the specific security risks of these environments can cause significant damage and require specialized protection solutions.

Kaspersky Cloud Workload Security is specifically designed to protect DevOps and cloud environments. It mitigates cloud risks with multi-layered threat protection and ensures full visibility across private, public, and hybrid clouds. It secures CI/CD pipelines and containerized applications by protecting key components throughout the development lifecycle.

Learn more

Kaspersky Threat Intelligence — stay ahead of your adversaries

Machine-readable Threat Intelligence

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Threat Intelligence expert support

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

Kaspersky Threat Intelligence

- Tactical
- Operational
- Strategic

Human-readable Threat Intelligence

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - Crimeware
  - ICS
- Kaspersky Threat Infrastructure Tracking

Kaspersky security services

Kaspersky Managed Detection and Response

Continuous monitoring, detection and response

Kaspersky Incident Response

Digital forensics, incident response and malware analysis

Kaspersky Compromise Assessment

Detection of compromise, and traces of past attacks

Kaspersky SOC Consulting

Establish your own SOC or enhance your existing security operations

Kaspersky Security Assessment

Practical exercises demonstrating how an adversary would breach your security

Kaspersky Digital Footprint Intelligence

Monitoring of your digital assets to detect external threats

Learn more

Anti-APT solution with NDR and EDR to enpower your SOC

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack is an advanced anti-APT solution that defends against sophisticated cyberthreats. It provides everything from Network Detection and Response (NDR) to native XDR capabilities, securing key attack entry points at network and endpoint levels. By delivering full visibility across your entire IT infrastructure, it strengthens your SOC's defenses against targeted attacks.

How we help

Defend your corporate infrastructure and your business against sophisticated attacks.

Simplify network traffic and endpoint control via a single interface.

All-in-one security across web traffic, emails, endpoints to protect your business.

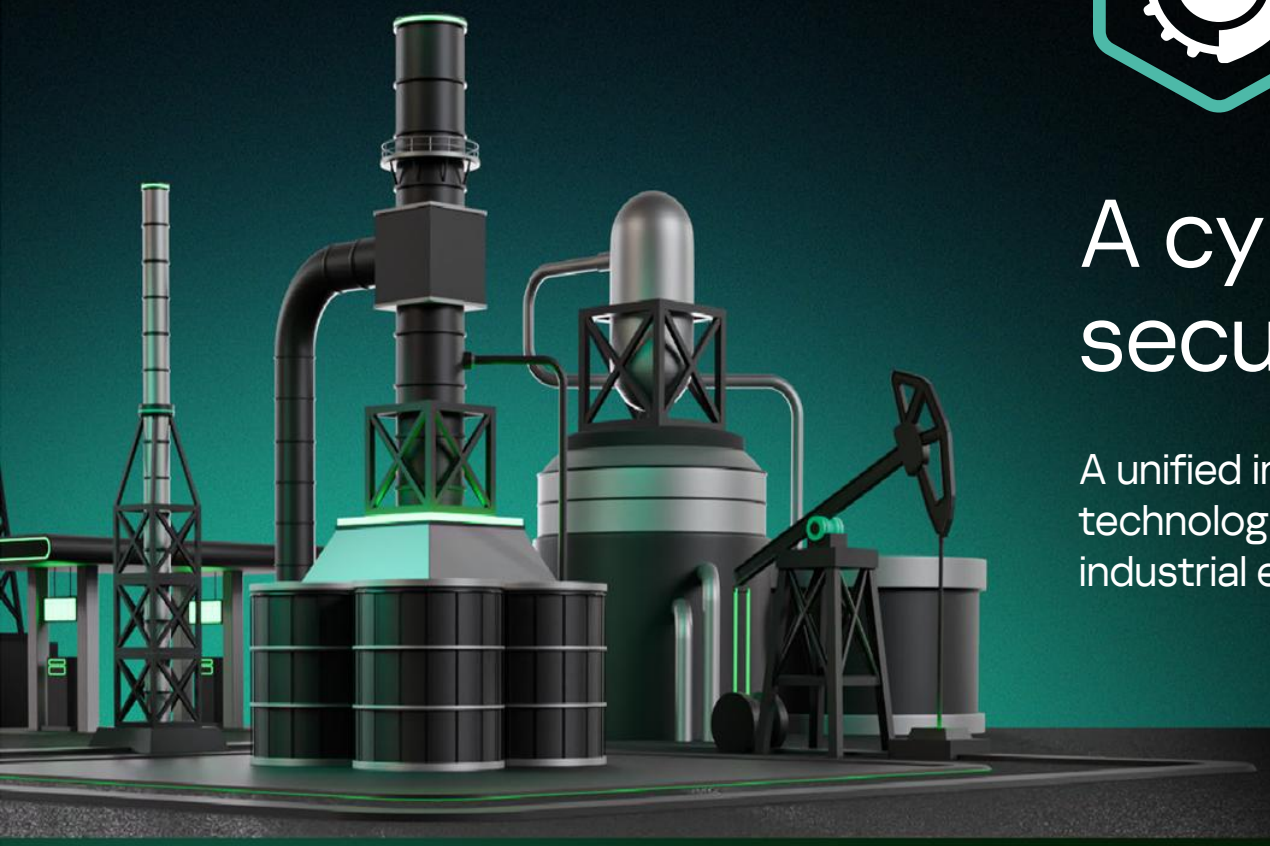
Automation of threat discovery and response tasks reduces incident detection and response times.

Learn more

Kaspersky security awareness

Our security awareness boosts cybersecurity culture inside organizations, engaging everyone from senior management to employees. Kaspersky-specific, game-based training helps executives and managers implement effective cyberdefense strategies while the automated platform empowers staff to proactively defend against threats. This approach reduces human-related incidents and enhances overall organizational resilience.

Kaspersky Automated Security Awareness Platform free trial



Kaspersky
OT CyberSecurity

A cyber-physical industrial security ecosystem

A unified industrial safety concept bringing together the technologies, knowledge and expertise needed to protect industrial enterprises at every level.

Learn more

kaspersky

Obrigado

Alisson Rebouças
Regional Account Manager

Geraldo Vasconcelos
Pre-Sales Manager