TI Safe

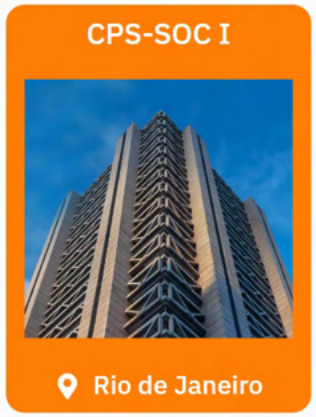
Segurança Cibernética Inteligente para CPS

Proteção e decisão em tempo real

29 de Abril de 2026

TI Safe: Liderando a Evolução da Segurança Cibernética de CPS no Brasil

2007	2008	2014	2017	2021	2022	2023	2024	2025	2026
•Fundação da TI Safe	•Foco em ICS •1ºformação em segurança para ICS	•1ª CLASS •1º Livro	•1º ICS-SOC do mundo	•2º livro	•1ª empresa das Américas certificada IEC 62443 •IA aplicada ao SOC	•Marca de 3000 pessoas treinadas pela Academia	•Safer – 1ª plataforma de IA para segurança de CPS	•3º livro	•4º livro •Plataforma Safer para o mercado



Nossos três compromissos técnicos

Cada colaborador da TI Safe tem, em seu plano de desenvolvimento individual, uma meta associada a um dos nossos três compromissos técnicos. Esses compromissos garantem o alinhamento entre nossa equipe, nossa missão e o que gera valor para nossos clientes.

Suportar a Continuidade do Negócio

Minimizar os Riscos Cibernéticos

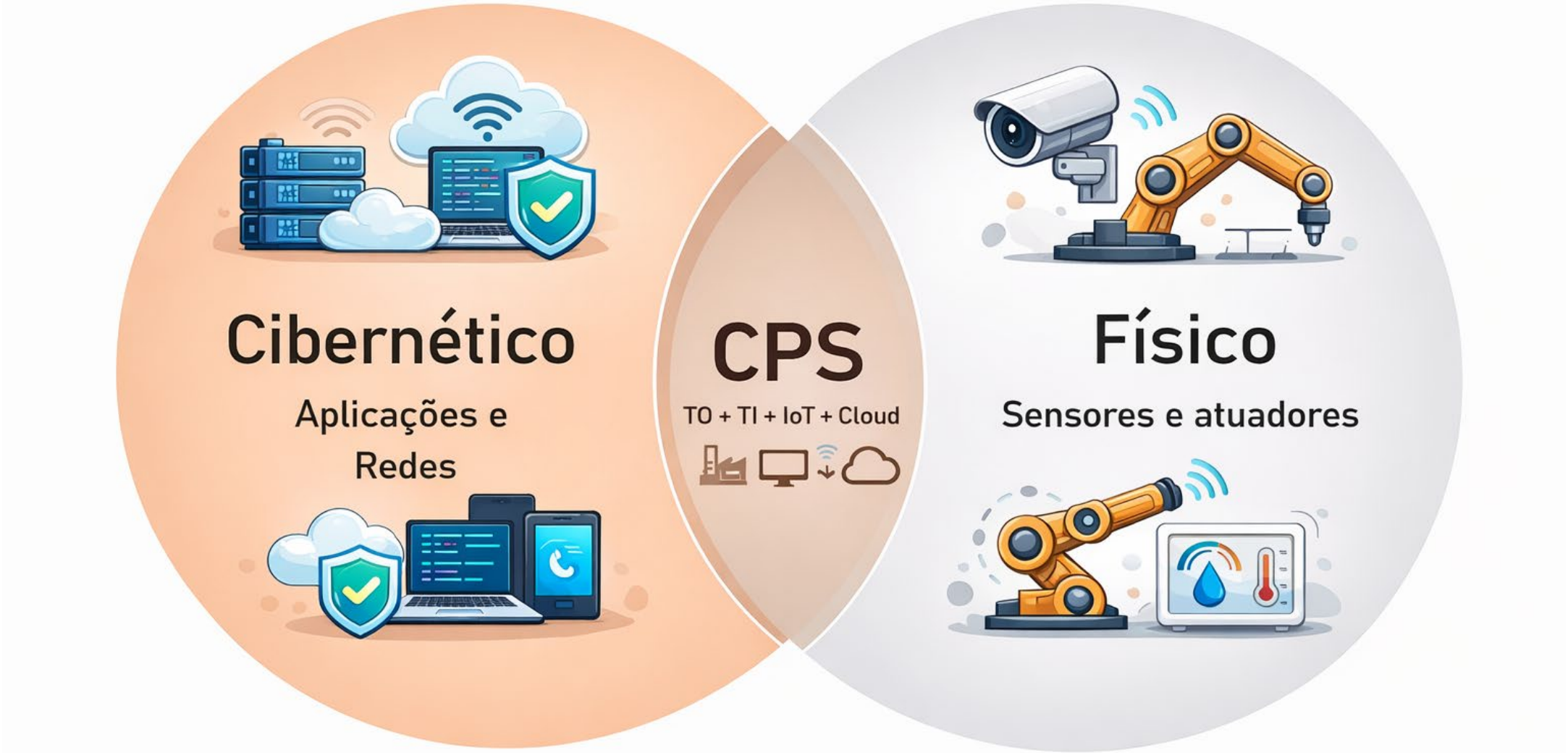
Estabelecer Conformidade com Normas e Melhores Práticas

Ti Safe

Um incidente cibernético hoje pode parar operações críticas e gerar prejuízos incalculáveis

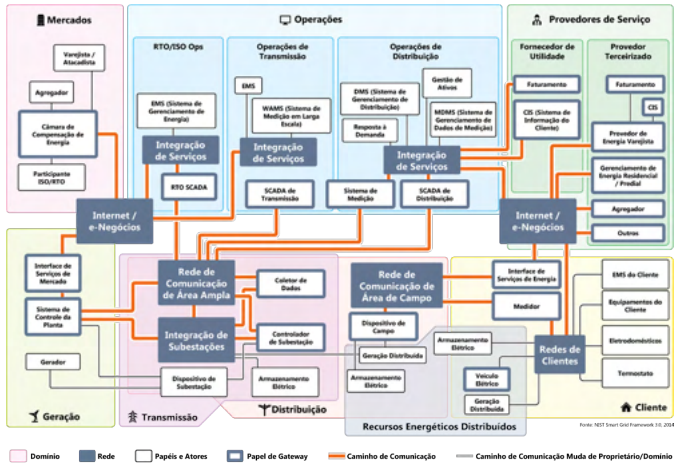
Interrupção operacional | Fraude em larga escala | Quebra de compliance | Perda de confiança

Sistemas Ciberfísicos (Cyber-Physical Systems – CPS)

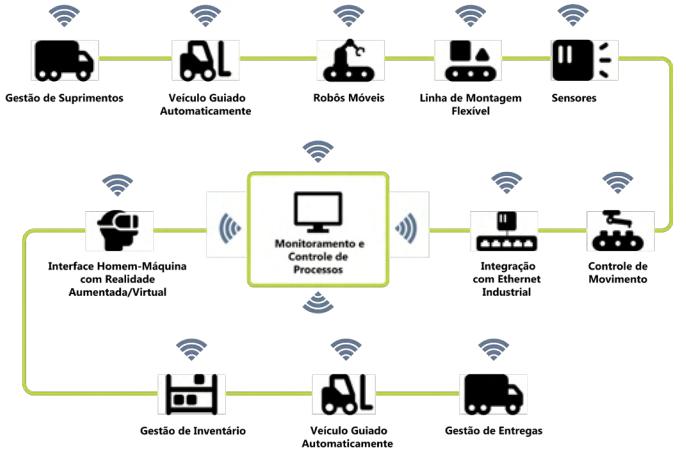


CPS tornam o mundo *smart* e cada vez mais conectado

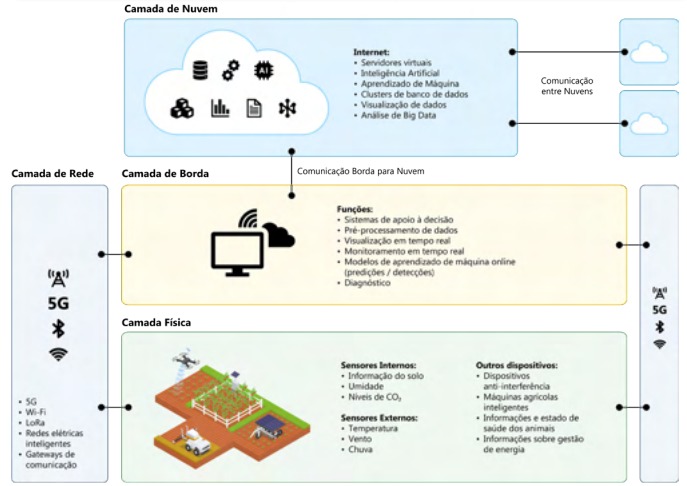
Smart Grid



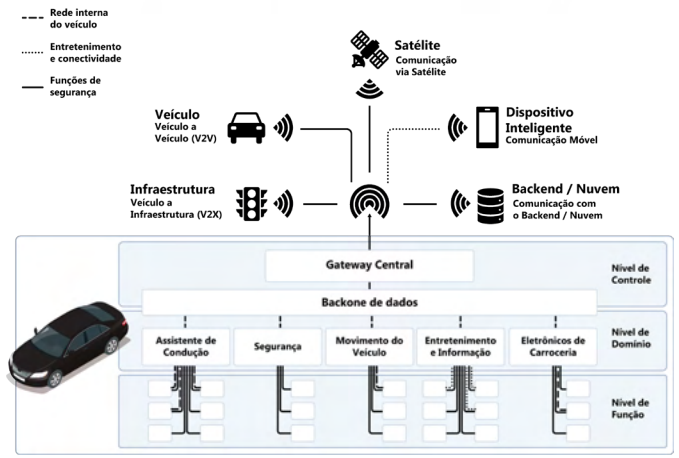
Smart Factory



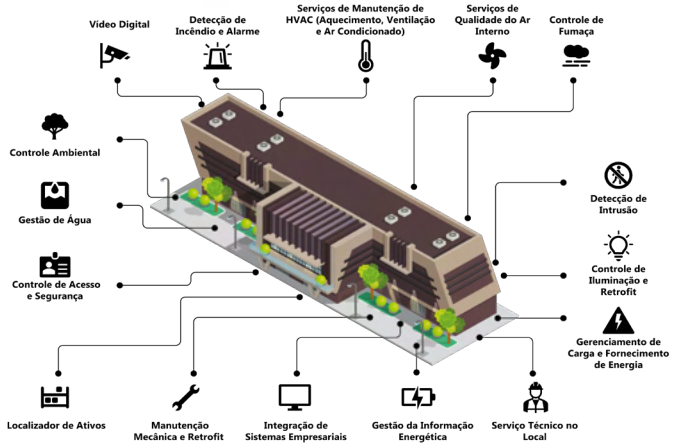
Smart Agriculture



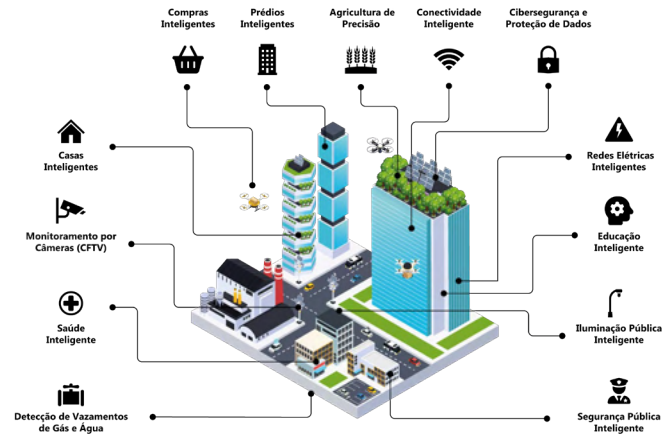
Smart Transportation



Smart Building



Smart City



Evolução das ameaças: do ataque clássico ao ataque por IA

Ataque Clássico

- Ataques manuais ou semi-automatizados
- Scripts estáticos
- Alto conhecimento técnico
- Baixa escala
- Longos ciclos de ataque

Automação Tradicional

- Ferramentas especializadas
- Exploração de vulnerabilidades conhecidas
- Engenharia social limitada
- Escala moderada

Ataque Baseado em IA

- Ataques adaptativos
- Geração dinàmica de conteúdo
- Aprendizado contínuo
- Redução da barreira técnica
- Escala algoritmica

Linha do Tempo

Anatomia de um ataque cibernético empoderado por IA

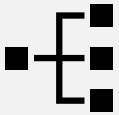
Planejamento

Reconhecimento de múltiplos alvos com suporte de IA

IA para a construção de ataques específicos

Intrusão

Entrega dissimulada por IA



Automação cognitiva de exploração

Instalação de artefatos gerados e em tempo real

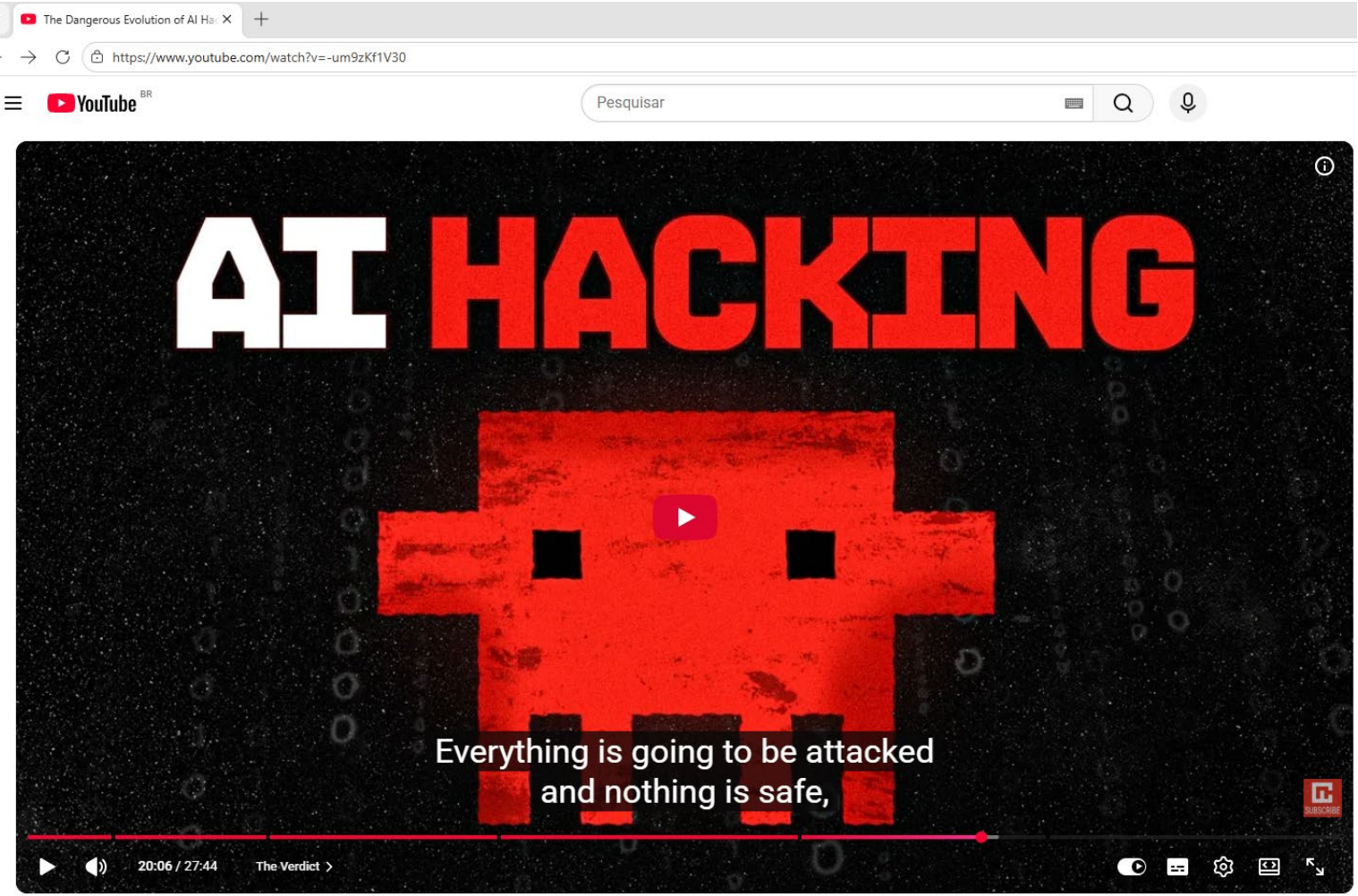
Execução

Comando e controle baseado em máquina

Realização de ações criminosas massificadas por IA

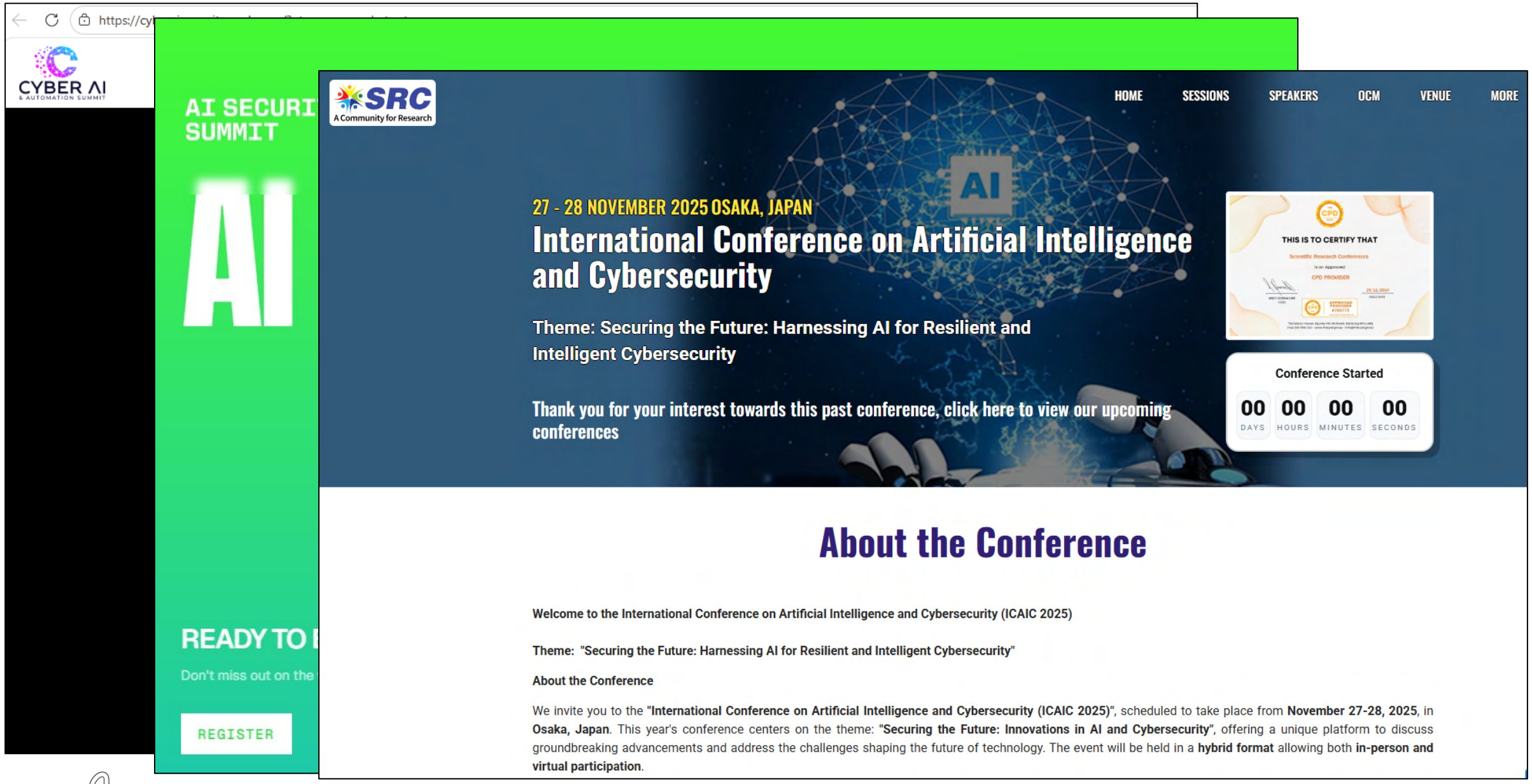
Assistam este vídeo

- The Dangerous Evolution of AI Hacking
- Este vídeo mostra a **evolução do uso de IA em hacking** e como ferramentas modernas podem automatizar técnicas de ataque.
- Explora casos reais e cenários de ataque em que **a IA participa ativamente do processo, incluindo fases como reconhecimento, geração de exploits e automação.**



The Dangerous Evolution of AI Hacking

Conferências de AI Hacking



Ataques empoderados por IA aumentam em escala, velocidade e precisão

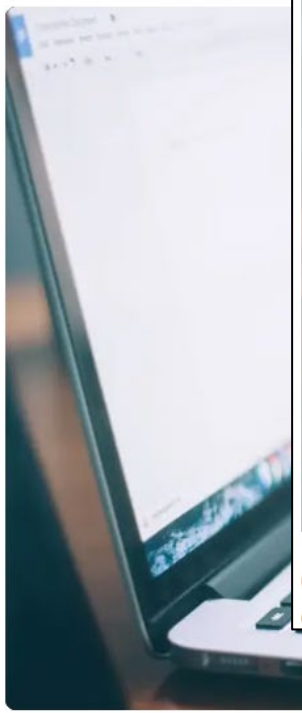
CNN BRASIL

Internacional

Funcionário golpista que

As autoridades estão cada
inteligência artificial

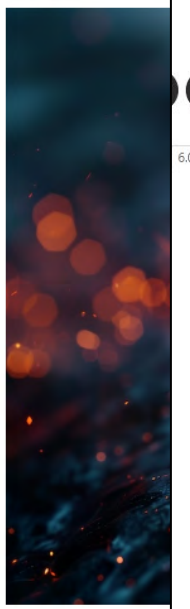
Heather Chen e Kethleen Magrar
04/02/24 às 10:02 | Atualizado 04



Hundreds of FortiGate Firewalls Hacked in AI-Powered Attacks: AWS

Threat actors re

By lo



6.009

Over 600 Fortine
exposed ports ar

Cyber Magazine

News & Articles | Magazines | Reports & Whitepapers | Topics | Webinars | LIVE Events

AI Agents Drive First Large-Scale Autonomous Cyberattack

By Georgia Collins

January 17, 2026 • 3 mins

Anthropic halted an AI-led cyber attack in 2025. Credit: Getty

Chinese state-backed hackers used Anthropic's Claude Code to carry out a largely AI-driven cyber espionage campaign targeting 30 organisations

CIODIVE

Deep Dive | Opinion | Library | Events | Press Releases | Topics

yees leaked corporate T: report

Share | License | Add us on Google

Company Portals

Anthropic

A Samsung flag flies outside the Samsung office on August 25, 2017 in Seoul, South Korea. *Chung Sung-Jun via Getty Images*

IA + Computação Quantica
O Próximo risco estrutural da segurança bancária

1. IA: AMEAÇA ATUAL

Automação e escala de ataques
phishing, engenharia social, malware

Descoberta acelerada
de vulnerabilidades

Ataques mais rápidos,
precisos e personalizados

Reduz o tempo entre exploração e impacto

2. COMPUTAÇÃO QUÂNTICA: AMEAÇA FUTURA

Algoritmos quânticos (Shor) podem quebrar:

- RSA
- ECC
- Diffie-Hellman

Impacto direto em:
TLS/HTTPS, VPNs,
assinaturas digitais e PKI

A base criptográfica atual tem prazo de validade

3. CONVERGÊNCIA CRÍTICA: IA + QUÂNTICO

IA acelera exploração e identificação de alvos

Computação quântica remove as barreiras criptográficas

ATAQUES MAIS INTELIGENTES + QUEBRA ESTRUTURAL DA PROTEÇÃO

4. RISCO JÁ EM CURSO: HARVEST NOW, DECRYPT LATER

Dados bancários capturados hoje → Armazenados por atacantes → Decifrados no futuro com quantum

Exposição retroativa de transações e informações sensíveis

5. IMPACTO PARA O BANCO

- Comprometimento de comunicações seguras (HTTPS, VPNs)
- Fraudes em larga escala
- Risco regulatório (BACEN / LGPD)
- Perda de confiança do cliente
- Risco sistêmico ao sistema financeiro

MENSAGEM ESTRATÉGICA

A QUESTÃO **NÃO É** "SE", MAS "QUANDO" A CRIPTOGRAFIA ATUAL SERÁ QUEBRADA.
A PREPARAÇÃO PARA O MUNDO PÓS-QUÂNTICO PRECISA COMEÇAR AGORA.

Os modelos tradicionais de cibersegurança não foram projetados para ataques baseados em IA

Limitações das Defesas Tradicionais

Dimensão	Defesas Tradicionais	Limitação Estrutural
Base de detecção	Assinaturas e regras	Dependem de conhecimento prèvio
Adaptabilidade	Estática	Incapaz de reagir a ataques mutáveis
Contexto operacional	Inexistente ou limitado	Não considera estado físico
Escalabilidade	Manual	Não acompanha volume e velocidade
CPS	Parcial	Incompatível com impacto físico

TI Safe

“Para proteger os CPS contra ataques com IA, precisamos de uma metodologia de segurança cibernética com IA”

Marcelo Branquinho, CEO da TI Safe

Quebra de Paradigma: Segurança Estática vs. Defesa Adaptativa com IA

Modelo Tradicional (Estático)

Regras Fixas • Assinaturas • Thresholds Estáticos • Resposta Reativa

Defesa baseada em conformidade técnica

Modelo Cognitivo (Adaptativo)

Defesa baseada em contexto, aprendizado e adaptação dinamica

A Metodologia iCPS Cybersecurity

Inteligência Artificial no Centro da Defesa

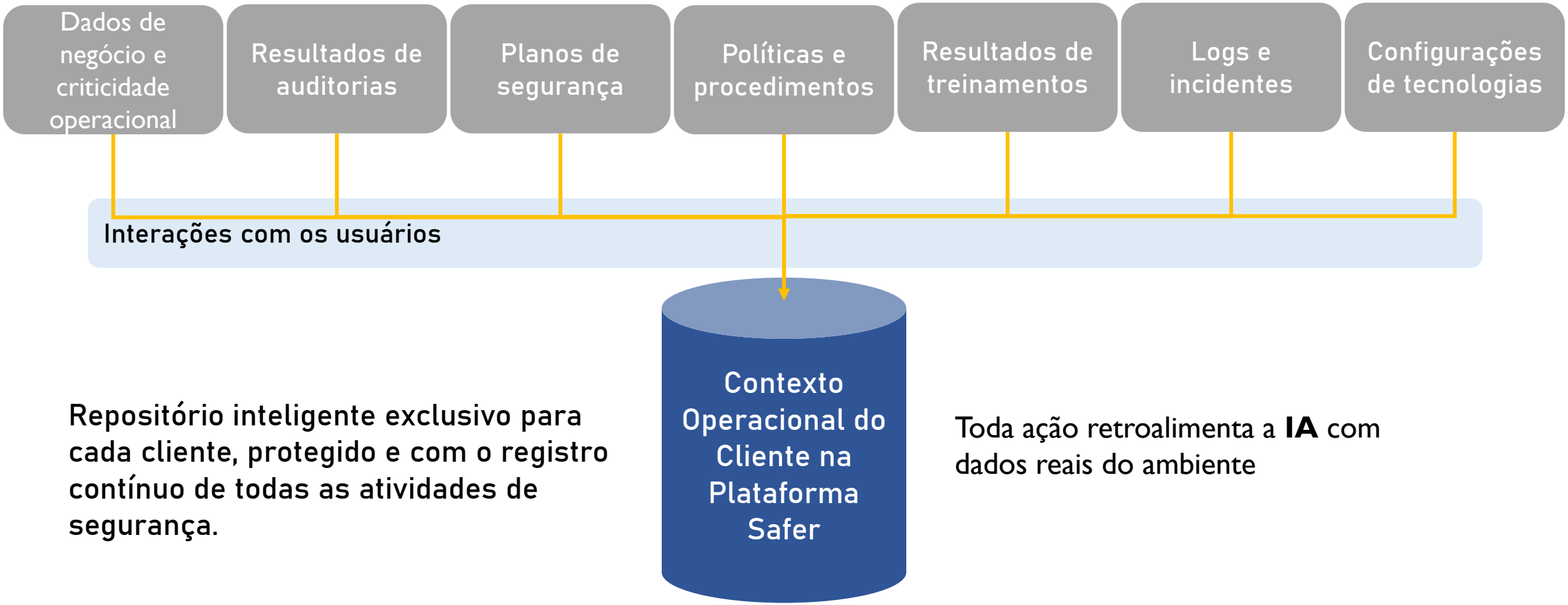
Arquitetura centrada em IA

Contexto Operacional seguro e personalizado

Resposta automatizada e rastreável

Defesa adaptativa e preditiva

A decisão em segurança só é eficaz quando baseada no contexto real do negócio



Repositório inteligente exclusivo para cada cliente, protegido e com o registro contínuo de todas as atividades de segurança.

Toda ação retroalimenta a **IA** com dados reais do ambiente

Com isso a inteligência da Plataforma Safer avalia, recomenda e reage com base no perfil, risco e maturidade reais de cada ambiente. Sem contexto operacional, não existe decisão de segurança eficaz.

O Conceito de Jornada de Segurança da Metodologia ¿CPS Cybersecurity

Bem vindos a Nova Era: Segurança Cibernética Inteligente

Soluções da TI Safe para a Jornada de Segurança Cibernética Inteligente

Plataforma Safer

- Porta de entrada para a segurança cibernética inteligente
- Centraliza contexto, riscos e decisões
- Ideal para iniciar a jornada com base estruturada

Início com inteligência e visibilidade

CPS-SOC Inteligente

- Monitoramento e resposta 24x7 conduzidos por especialistas
- Decisões mais rápidas com apoio de IA
- Implementação ágil de um SOC moderno

Operação contínua com inteligência e eficiência

Tecnologias integradas e orquestradas

- Implantação e integração de soluções líderes de mercado
- Arquitetura alinhada à Plataforma Safer
- Otimização contínua de desempenho e segurança

Integração que gera valor e resiliência

Projetos de Segurança Cibernética Inteligente

- Projetos estruturantes de segurança cibernética inteligente
- Construção completa da arquitetura de segurança
- Atendimento a requisitos regulatórios (IEC 62443, ONS, ANEEL)
- Evolução contínua da maturidade e governança

Segurança como vantagem competitiva

A TI Safe se adapta ao momento da organização, da primeira iniciativa à operação completa da segurança.

1. Plataforma Safer (o cérebro da segurança cibernética inteligente)

ARQUITETURA UNIFICADA

TI
Segurança de Tecnologia da Informação

TO
Segurança de Tecnologia Operacional

IoT
Segurança de Dispositivos e Conectividade

NUVEM
Segurança de Ambientes e Aplicações na Nuvem

PLATAFORMA SAFER

Inteligência Artificial no centro da defesa

Contexto do cliente • IA • Automação • Especialistas
Decisões mais rápidas, precisas e alinhadas ao risco real

CAPACIDADES POTENCIALIZADAS POR IA

Detecção precoce de ameaças
Análise contínua e inteligente de eventos

Resposta automatizada a incidentes
Ações orquestradas e rastreáveis

Conformidade contínua
Monitoramento e relatórios para auditorias e normas

APPLIANCES DEDICADOS

Escaláveis para cada necessidade

SFR-5

SFR-25

SFR-50

SFR-100

Desempenho, segurança e confiabilidade para proteger ambientes críticos.

OPERANDO COM CPS-SOC 24x7

Resiliência operacional
Monitoramento contínuo e resposta especializada

Governança em tempo real
Visibilidade completa do ambiente e dos riscos

Continuidade do negócio
Redução de impactos e garantia da operação crítica

2. CPS-SOC Inteligente:
Monitoramento e resposta 24x7 conduzidos por especialistas, IA e contexto

O PROBLEMA

SOCs tradicionais enfrentam limitações críticas:

- **Alertas em excesso** e ruído operacional
- **Dificuldade de priorização** e análise de contexto
- **Dependência de especialistas** escassos e caros
- **Tempo de resposta lento** e impacto maior nos negócios

A Solução: CPS-SOC Inteligente da TI Safe

IA aplicada para correlação, priorização e detecção de ameaças

Especialistas 24x7 com profundo conhecimento de CPS/ICS

Decisões mais rápidas e assertivas com base em risco e contexto operacional

Visibilidade completa do ambiente OT, ativos e ameaças em tempo real

Operação centralizada, inteligente e contínua, com foco em reduzir risco e garantir resiliência.

PARA QUEM É

- **Organizações** sem SOC estruturado
- Empresas que **desejam terceirizar** a operação
- **Ambientes críticos** que exigem monitoramento especializado

Segurança contínua, inteligente e alinhada ao contexto do negócio.

RESULTADOS QUE GERAM IMPACTO

- Resposta até **10x** mais rápida
- Até **90%** de redução de alertas irrelevantes
- Foco no que realmente importa: **risco crítico**
- Mais **resiliência** e continuidade das operações

3. Ecossistema de Tecnologias Integradas à Plataforma Safer

4. Projetos de Segurança Cibernética Inteligente
Transformação da segurança em capacidade estratégica do negócio

PARA QUEM SE DESTINAM

- Empresas com alta criticidade operacional
- Ambientes que precisam atender requisitos regulatórios (ONS, IEC 62443)

O QUE RESOLVE

- Ambientes fragmentados e sem arquitetura definida
- Dificuldade de atender compliance e operar com eficiência

COMO COMEÇA

- Projeto de segurança cibernética inteligente completo
- Definição, implantação e integração de toda a arquitetura com a Plataforma Safer

BENEFÍCIOS PARA O NEGÓCIO

Proteção integrada e inteligente
Cobertura completa da rede industrial com visibilidade e controle centralizados

Conformidade e redução de riscos
Atende normas como IEC 62443 e requisitos regulatórios

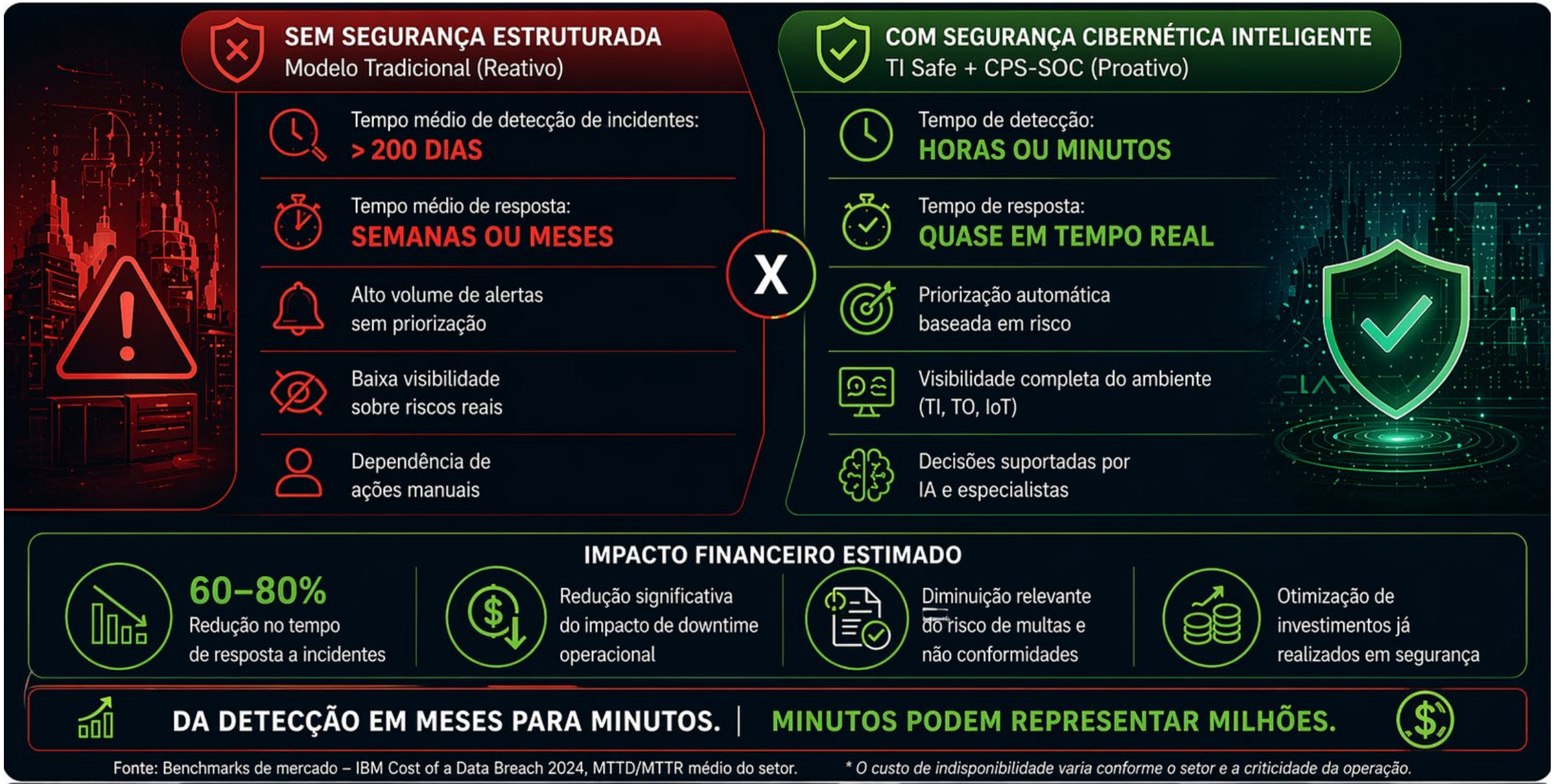
Decisões mais rápidas e assertivas
Inteligência aplicada para priorização e resposta eficaz

Operação contínua e resiliente
CPS-SOC Inteligente 24x7 e serviços especializados

Eficiência e retorno sobre o investimento
Redução de incidentes, multas e paradas não planejadas

O Impacto real da segurança cibernética no negócio

Velocidade e contexto na resposta definem o impacto financeiros de um incidente



Como a Segurança Cibernética Inteligente gera retorno financeiro mensurável

Redução estrutural de custos
Eliminação da necessidade de construir e operar um SOC próprio, incluindo operação 24x7 e alta dependência de especialistas.

Otimização dos investimentos
Maximiza o uso de tecnologias existentes e evita novas aquisições desnecessárias.

Aumento da produtividade operacional
Menor dependência de atividades manuais e melhor uso das equipes internas.

Redução do impacto financeiro de incidentes
Decisões mais rápidas e melhor priorização de riscos reduzem perdas e custos associados.

Diminuição do tempo de indisponibilidade
Menos paradas operacionais e perdas associadas a falhas de segurança.

Maior previsibilidade orçamentária
Modelo escalável e planejado de evolução da segurança traz controle e previsibilidade dos custos.

Redução de riscos regulatórios e financeiros
Menos exposição a multas, penalidades e não conformidades com normas e regulamentações.

Transformação da segurança em valor para o negócio
De um custo imprevisível para um modelo controlado, eficiente e com retorno financeiro mensurável.

Segurança cibernética inteligente não é custo.
É proteção, eficiência e retorno financeiro para o seu negócio.

Ti Safe

A questão não é se sua organização será impactada — é se estará preparada quando acontecer.

Estamos prontos para apoiar sua organização nessa transformação.

Contem conosco!

TiSafe

Obrigado!

Marcelo Branquinho, CEO

Querem conhecer a Plataforma Safer?