TiSafe

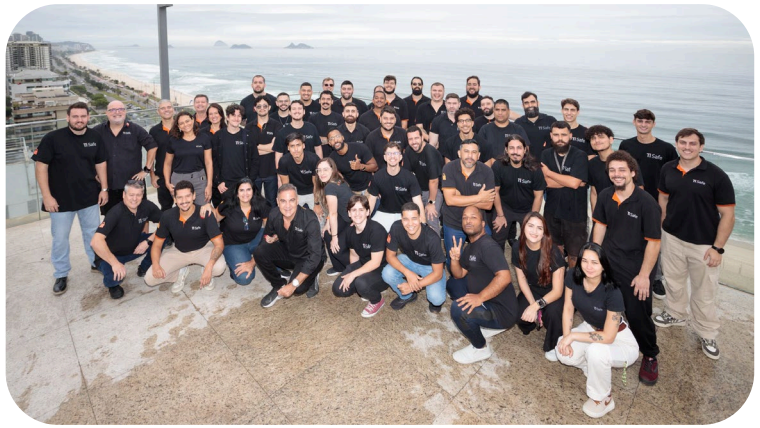
CPS-SOC Inteligente

Next Generation SOC para CPS

CPS (Cyber-Physical Systems) — ambientes industriais, operacionais e infraestruturas críticas onde sistemas digitais impactam diretamente o mundo físico.

Maio de 2026

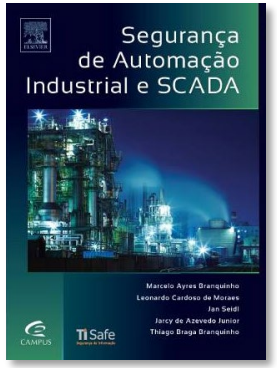
TI Safe: Liderando a Evolução da Segurança Cibernética de CPS no Brasil



2007
- Fundação da TI Safe

2008
- Foco em ICS
- 1ºformação em segurança para ICS

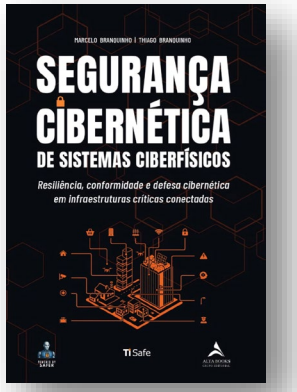
2014
- 1ª CLASS
- 1º Livro



2017
- 1º ICS-SOC do mundo

2021
- 2º livro

2022
- 1ª empresa das Américas certificada IEC 62443
- IA aplicada ao SOC



2023
- Marca de 3000 pessoas treinadas pela Academia

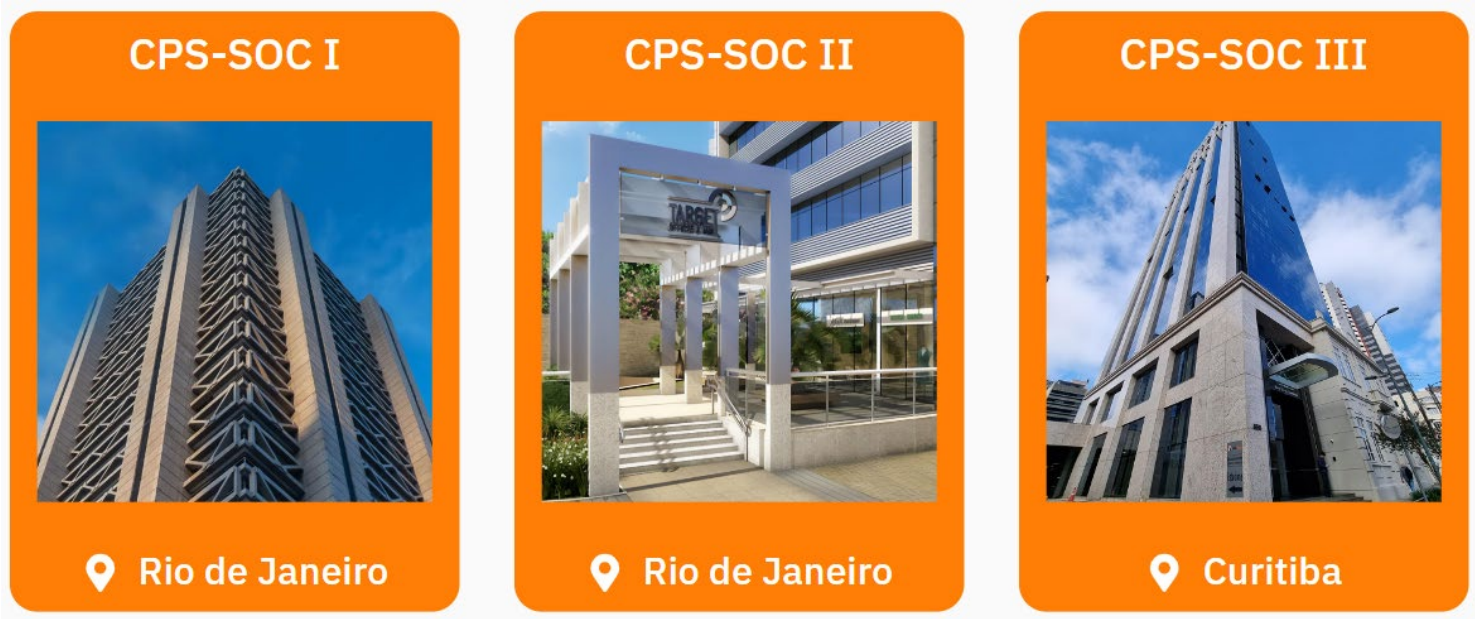
2024
- Safer – 1ª plataforma de IA para segurança de CPS

2025
- 3º livro

2026
- 4º livro
- Plataforma Safer para o mercado

Capacidade Operacional da TI Safe

- Operação 24x7 especializada em CPS
- Equipes multidisciplinares com experiência industrial
- Atuação global e multilíngue
- Plataforma Safer como cérebro cognitivo
- Certificação IEC 62443 e operações auditadas internacionalmente



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

DAkkS Deutsche Akkreditierungsstelle D-ZE-11321-01-00

TÜV SÜD Product Service

CERTIFICATE

No. IITS1 116504 0001 Rev. 00

Holder of Certificate: TI Safe
Segurança Cibernética Industrial LTDA.
Estrada do Pau Ferro 480
Bloco 1, Loja R, Pechincha, Jacarepaguá
22743-051 Rio de Janeiro RJ
BRAZIL

Site(s): TI Safe Segurança Cibernética Industrial LTDA.
Estrada do Pau Ferro 480,
Bloco 1, Loja R, Pechincha, Jacarepaguá,
22743-051 Rio de Janeiro RJ,
BRAZIL

Certification Mark:

Type: Industrial IT Security

Scope of Certificate: **TI Safe ICS.SecurityFramework**

Applied Standard(s): IEC 62443-2-4:2015/AMD1:2017
PPP 15010B:2021 (IEC 62443-2-4 ML2 Process Profile for a Generic Service Provider)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

Report No.: 22CR11S016

Valid until: 2025-03-31

Date, 2022-05-31 (Enrico Seidel)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

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

A superfície de ataque dos CPS mudou. O modelo tradicional de SOC não acompanha mais.

Ransomware em operação industrial | Interrupção operacional | Multas

Impacto financeiro | Risco físico/Safety | IA sendo usada pelos atacantes

Os desafios dos SOCs que operam sem IA

Processos manuais, excesso de dados e falta de contexto impedem decisões rápidas e eficazes

Excesso de alertas e ruído operacional	Milhares de alertas diários geram sobrecarga, dificultam priorização e aumentam o risco de falsos positivos.
Tempo alto para detecção e resposta	A análise manual e a falta de contexto atrasam a identificação de ameaças e a resposta, permitindo que incidentes se agravem.
Dependência de especialistas escassos	Profissionais experientes são difíceis de encontrar e caros. A dependência de pessoas limita a escalabilidade da operação.
Ferramentas isoladas e falta de integração	Dados desconectados entre ferramentas impedem correlação eficiente e visão única do ambiente, reduzindo a efetividade da análise.
Baixa eficiência operacional	Tarefas repetitivas e manuais consumem tempo dos analistas e tiram o foco do que realmente importa: o risco ao negócio.
Falta de contexto de negócio e de OT	A ausência de contextualização com o ambiente operacional e o impacto no processo gera decisões reativas e pouco assertivas.
Dificuldade de governança e compliance	Processos manuais dificultam evidências, relatórios e auditorias, aumentando o risco de não conformidade.

O IMPACTO DISSO NO NEGÓCIO

- Maior risco de incidentes e interrupções operacionais
- Aumento de custos com operações, horas extras e retrabalho
- Impacto direto na produtividade e eficiência das equipes
- Maior exposição a ameaças e perdas financeiras
- Risco de multas, sanções e perda de confiança de clientes e parceiros

A grande mudança – Quebra de paradigma
Do SOC tradicional para o Next Generation SOC com IA

ANTES: SOC TRADICIONAL

Ferramentas isoladas
Silos de dados e baixa integração entre tecnologias.

Segurança reativa
Resposta após a ocorrência do incidente, com foco em contenção.

Baseado em alerta
Alto volume de alertas e falsos positivos geram ruído e consumo de tempo.

Humano sobrecarregado
Análises manuais, processos repetitivos e alta pressão operacional.

Baixa eficiência e escalabilidade
Dificuldade para acompanhar o crescimento de dados, ativos e ameaças.

QUEBRA DE PARADIGMA

Tecnologia + IA potencializam os analistas e transformam resultados.

DEPOIS: NEXT GENERATION SOC

Plataforma integrada
Visão unificada de dados, contexto e inteligência em tempo real.

Segurança inteligente
Detecção precoce, priorização de riscos e previsão de ameaças com IA.

Baseado em contexto
Correlação automática, redução de falsos positivos e foco no que realmente importa.

IA + humano
Automação de tarefas repetitivas e análises avançadas para decisões assertivas.

Alta eficiência e escala
Operação ágil, processos automatizados e capacidade de evoluir com o negócio.

O futuro da cibersegurança é colaborativo:
IA para potencializar pessoas, não para substituí-las.

Respostas mais rápidas

Menos risco, mais proteção

Menor custo, mais valor

Bem vindos a Nova Era: CPS-SOC Inteligente

O Next Generation SOC da TI Safe

Quem precisa de um CPS-SOC Inteligente?

Para organizações que precisam proteger operações críticas com inteligência, automação e contexto industrial.

01

Organizações acelerando a convergência TI/TO

Empresas que precisam ganhar visibilidade, contexto e capacidade operacional de defesa em ambientes híbridos.

02

Operações sobrecarregadas por alertas e escassez de especialistas

Organizações que precisam escalar detecção e resposta com IA, automação e especialistas CPS.

03

Ambientes críticos que exigem contexto operacional

Operações industriais onde segurança, disponibilidade e continuidade precisam coexistir.

CPS-SOC Inteligente: o Next Generation SOC da TI Safe
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

Como a Segurança Cibernética Inteligente gera retorno financeiro mensurável

ONDE GERAMOS VALOR

Redução estrutural de custos
- Eliminação da necessidade de construir e operar um SOC próprio (incluindo operação 24x7)
- Redução da dependência de especialistas e otimização dos investimentos existentes

Aumento de eficiência operacional
- Maior produtividade com menor dependência de atividades manuais
- Operação mais ágil, com melhor aproveitamento das equipes internas

Redução de riscos e impactos financeiros
- Decisões mais rápidas com melhor priorização de riscos
- Redução de indisponibilidade, perdas operacionais e exposição a multas

Previsibilidade e escala
- Maior previsibilidade orçamentária com modelo estruturado
- Crescimento da segurança sem aumento proporcional de custos

CPS-SOC INTELIGENTE

IA + ESPECIALISTAS + CONTEXTO INDUSTRIAL

OPERAÇÃO 24x7 ESPECIALIZADA
Em TI e OT/CPS

RETORNO FINANCEIRO MENSURÁVEL

Menos custo fixo
OPEX previsível e otimizado sem necessidade de alto CAPEX e equipe 24x7 própria.

↑ REDUÇÃO DE CUSTOS ESTRUTURAIS

Mais eficiência e produtividade
Automação e IA reduzem o esforço manual e aumentam a capacidade da equipe interna.

↑ MAIOR PRODUTIVIDADE OPERACIONAL

Menos perdas, menos risco
Detecção e resposta rápidas evitam incidentes, paradas não planejadas e penalidades regulatórias.

↑ MENOR IMPACTO FINANCEIRO DE INCIDENTES

Crescimento seguro e escalável
Modelo escalável que acompanha o negócio com previsibilidade e controle de custos.

↑ ESCALA COM CONTROLE DE CUSTOS

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

REDUÇÃO DE CUSTOS ESTRUTURAIS
Eliminação de CAPEX e OPEX de um SOC próprio 24x7

ATÉ 60–80% MENOS ATIVIDADES MANUAIS
Automação e IA aumentam a eficiência da operação

ATÉ 70% MENOS TEMPO PARA DETECÇÃO E RESPOSTA
Incidentes contidos rapidamente, reduzindo impactos financeiros

REDUÇÃO DE PERDAS OPERACIONAIS E MULTAS
Menos indisponibilidade, riscos e penalidades

ROI CONTÍNUO E SUSTENTÁVEL
Mais segurança, mais valor para o negócio

Ti Safe

Com o CPS-SOC Inteligente, a segurança cibernética deixa de ser apenas defesa e passa a gerar continuidade operacional, eficiência e retorno financeiro mensurável.

Estamos prontos para apoiar sua organização nessa transformação.

Contem conosco!

TI Safe

Obrigado!

Marcelo Branquinho, CEO

Vamos avaliar como o CPS-SOC Inteligente pode ser aplicado ao seu ambiente?