As fragilidades da RO.CB.BR-01 frente aos novos ataques potencializados por IA: as empresas de energia ainda estão seguras?

Autores: Marcelo Branquinho e Plataforma Safer

20/10/2025

Resumo: O avanço da Inteligência Artificial (IA) tem revolucionado o setor de cibersegurança – para o bem e para o mal. Se, por um lado, ela fortalece ferramentas defensivas e aumenta a capacidade de resposta a incidentes, por outro, também vem sendo explorada por grupos maliciosos, incluindo organizações criminosas e atores com capacidades avançadas, para desenvolver ataques cada vez mais sofisticados, evasivos e potencialmente destrutivos.

No contexto das infraestruturas críticas, como o setor elétrico, esse fenômeno adquire uma gravidade ainda maior. Redes de Tecnologia Operacional (TO), responsáveis por controlar diretamente equipamentos físicos como subestações, turbinas, linhas de transmissão e centros de controle tornam-se alvos de grande valor estratégico. A introdução da IA nos arsenais ofensivos dos cibercriminosos aumenta a velocidade, a escala e a complexidade dos ataques, tornando-os mais difíceis de detectar e neutralizar. Ferramentas maliciosas baseadas em IA já são capazes de realizar reconhecimento automatizado de ativos, adaptar-se ao ambiente da vítima, manipular dados de sensores industriais e empregar engenharia social com deepfakes e modelos de linguagem para enganar operadores humanos.

Neste cenário, um dos pilares regulatórios mais relevantes é a RO-CB.BR-01, a Rotina Operacional Cibernética publicada pelo Operador Nacional do Sistema Elétrico (ONS). Publicada em 2021, essa rotina estabelece um conjunto de requisitos mínimos obrigatórios de segurança cibernética para os agentes que atuam no Sistema Interligado Nacional (SIN). Seu objetivo é garantir a confiabilidade, disponibilidade e resiliência do SIN frente a ameaças cibernéticas, protegendo tanto os dados operacionais quanto os processos físicos sob controle digital.

A estrutura da RO-CB.BR-01 foi cuidadosamente construída para incorporar boas práticas técnicas, processuais e organizacionais inspiradas em padrões internacionais, como a série IEC 62443 e o NIST SP 800-82. Ela exige segmentação de redes TO e TI, controle de acessos remotos, inventário de ativos, gestão de mudanças segura (GMUD), resposta a incidentes estruturada, monitoramento contínuo e registro de ações de usuários. Além disso, prevê a formalização de políticas, procedimentos e a designação clara de responsáveis pela segurança cibernética em ambientes operacionais.

Desde sua entrada em vigor, a implementação da rotina tem ocorrido de forma progressiva. Grandes operadores do setor elétrico, especialmente empresas de geração e transmissão de maior porte, já atingiram elevados níveis de conformidade, consolidando SOCs industriais, segmentações robustas e processos maduros de gestão de risco cibernético. Por outro lado, agentes menores ou com menos capacidade técnica e financeira ainda enfrentam desafios importantes, como a integração de sistemas legados, escassez de mão de obra especializada e dificuldades na adoção de ferramentas mais avançadas.

Entretanto, embora a RO-CB.BR-01 represente um avanço inegável na elevação do patamar mínimo de segurança do setor, o surgimento de ameaças potencializadas por IA como ataques com LLMs ofensivas, malware com lógica adaptativa, spear phishing automatizado e manipulação inteligente de sistemas SCADA impõe novos desafios. O que era considerado suficiente em termos de defesa passiva e segmentação estática pode não ser capaz de conter ameaças autônomas que evoluem em tempo real, exploram falhas humanas com alta precisão e burlam controles convencionais sem disparar alarmes.

Nesse sentido, a própria rotina precisa ser vista como um ponto de partida e não como um teto técnico. A complexidade atual exige contramedidas também baseadas em inteligência artificial defensiva, capazes de operar com a mesma agilidade dos atacantes. Ferramentas como SIEMs com análise comportamental (UEBA), orquestração de resposta automatizada (SOAR), sistemas de detecção com machine

learning e monitoramento contextualizado tornam-se essenciais para complementar os controles mandatórios da rotina.

É nesse ponto que plataformas como a Safer, desenvolvida pela TI Safe, ganham relevância estratégica. A Safer atua como um copiloto cibernético para sistemas ciberfísicos (CPS – Cyber Physical Systems), oferecendo inteligência contínua baseada em IA, análise de comportamento de usuários e ativos, apoio à decisão técnica durante incidentes, e integração nativa com frameworks como MITRE ATT&CK for ICS. Mais do que uma plataforma, ela representa um avanço conceitual na forma como se lida com riscos cibernéticos industriais: de forma dinâmica, preditiva e contextualizada, indo além da simples conformidade.

Neste artigo, exploramos o uso da IA em ataques cibernéticos contra o setor elétrico e avaliamos se os controles definidos atualmente pela RO-CB.BR-01 são suficientes para enfrentar essa nova classe de ameaças. Concluímos com propostas de complementação da rotina para suas próximas versões, bem como com a apresentação de soluções defensivas inteligentes, como a plataforma Safer, que apontam um caminho viável e moderno para proteger o setor elétrico em um cenário de risco em constante evolução.

Keywords: Inteligência Artificial (IA), Infraestruturas Críticas, Tecnologia Operacional (TO), Sistemas Ciberfísicos (CPS), Ataques Cibernéticos Avançados, RO-CB.BR-01 (ONS), IEC 62443, NIST SP 800-82, Segmentação de Redes, SOC Industrial, Defesa Cibernética Preditiva

1. Introdução: Da Automação à Arma

A Inteligência Artificial (IA) deixou de ser apenas uma ferramenta de automação de processos e análise preditiva de dados operacionais, e passou a ocupar uma posição central no campo dos ataques cibernéticos modernos. O que antes era um recurso auxiliar para aumentar eficiência, hoje é cada vez mais utilizado como elemento ativo e estratégico nas campanhas ofensivas de grupos maliciosos, incluindo agentes estatais, grupos APT (Advanced Persistent Threats) e organizações criminosas com acesso a tecnologias avançadas.

Em ambientes industriais e de infraestrutura crítica, como o setor elétrico, esse movimento assume contornos ainda mais preocupantes. Isso porque as redes de Tecnologia Operacional (TO) que conectam e controlam diretamente equipamentos físicos, como disjuntores, relés, transformadores, turbinas, válvulas e sistemas de supervisão e controle (SCADA) são particularmente sensíveis a qualquer tipo de manipulação cibernética. Qualquer interferência maliciosa bem-sucedida nesses sistemas pode ter consequências imediatas no mundo físico, desde interrupções no fornecimento de energia elétrica até falhas em cascata em toda a rede interligada nacional (SIN), com potenciais impactos sociais, econômicos e ambientais.

Nesse contexto, a IA ofensiva emerge como uma ameaça existencial porque altera fundamentalmente a lógica tradicional dos ataques cibernéticos. Em vez de dependerem exclusivamente de scripts fixos, exploits manuais ou vulnerabilidades conhecidas, os agentes hostis agora conseguem treinar algoritmos para reconhecer padrões, adaptar seu comportamento ao ambiente da vítima e até tomar decisões autônomas baseadas em objetivos operacionais. **Isso inclui, por exemplo, a capacidade de detectar automaticamente a topologia de uma rede TO, identificar quais ativos são mais críticos ou vulneráveis, e então planejar sequências de ataque que minimizem a detecção e maximizem o dano.**

Além disso, surgem ferramentas capazes de gerar conteúdo malicioso de forma dinâmica, como deepfakes em vídeo ou voz que simulam operadores, engenheiros ou executivos, com o intuito de induzir comandos perigosos, liberar GMUDs não autorizadas ou enganar sistemas de autenticação humana. A engenharia social

automatizada, alimentada por modelos de linguagem avançados (LLMs), também está evoluindo rapidamente, permitindo que mensagens de spear phishing sejam personalizadas com base em dados públicos e internos coletados por algoritmos de rastreamento. Esses ataques, muitas vezes impossíveis de distinguir de interações legítimas, colocam em xeque os treinamentos tradicionais de conscientização e as barreiras humanas de detecção.

Outro vetor importante são os malwares com IA embarcada, capazes de analisar o comportamento da rede e ajustar suas ações em tempo real para evitar detecção por sistemas de monitoramento. Diferentemente de códigos fixos, esses agentes maliciosos conseguem pausar suas atividades em horários sensíveis, ocultar seus rastros em logs ou mesmo imitar comandos legítimos de operadores. Há também a possibilidade de combinar múltiplas IAs ofensivas em ataques coordenados que atuam simultaneamente em diferentes partes da infraestrutura elétrica, o que pode sobrecarregar os times de resposta e os sistemas de defesa convencionais.

A escalada dessa ameaça exige, portanto, uma mudança de paradigma na forma como a segurança cibernética é encarada em ambientes industriais. **Não se trata mais de proteger sistemas apenas com firewalls e segmentação de rede. Agora, é necessário responder a ameaças que pensam, aprendem e evoluem. Isso só pode ser feito com contramedidas igualmente inteligentes: plataformas que utilizem IA defensiva, monitoramento comportamental com machine learning, automação de resposta (SOAR), análises preditivas baseadas em contexto e integração contínua entre processos de segurança, operação e governança.**

Assim, enquanto a IA ofensiva amplia significativamente o poder de destruição dos ciberataques, ela também abre caminho para uma nova geração de defesas cibernéticas inteligentes, mais ágeis, autônomas e adaptativas. No entanto, para que isso seja eficaz, é necessário que as organizações do setor elétrico reconheçam a criticidade desse novo cenário e avancem rapidamente em direção a uma postura de segurança baseada em resiliência, aprendizado contínuo e inovação tecnológica.

2. LLMs Maliciosas e Ferramentas Prontas para Ataques ao Setor Elétrico

O surgimento e a popularização dos Modelos de Linguagem de Grande Escala (LLMs), como os que movem assistentes de IA em ambientes corporativos e plataformas de produtividade, também têm gerado um efeito colateral preocupante no submundo digital: a proliferação de LLMs maliciosas, desenvolvidas ou ajustadas para fins ofensivos, e já disponíveis em fóruns clandestinos, canais de venda na dark web e marketplaces voltados ao cibercrime.

Essas IAs ofensivas não são apenas versões adaptadas de modelos públicos como GPT ou BERT. Elas são frequentemente treinadas ou finamente ajustadas com bases de dados específicas que incluem táticas de intrusão, comandos ofensivos para ambientes Linux/Windows, protocolos industriais (como Modbus, DNP3 e IEC 104), exemplos de exploração de CVEs reais, engenharia reversa de firmware de equipamentos industriais, e até mesmo estratégias para burlar mecanismos de autenticação remota de sistemas de energia. Dessa forma, essas LLMs tornam-se verdadeiros assistentes de ataque, capazes de gerar conteúdo malicioso sob demanda, sugerir vetores de intrusão e produzir códigos prontos para serem implantados.

No contexto das infraestruturas críticas de energia, o uso dessas LLMs representa um salto qualitativo nos riscos. Enquanto os ataques convencionais contra redes OT exigiam conhecimento técnico profundo e especializado, agora qualquer atacante com acesso a uma dessas ferramentas pode operar com apoio automatizado para descobrir, explorar e sabotar sistemas industriais. Um operador malicioso pode, por exemplo, pedir que o modelo:

- *Explique como simular comandos Modbus para alterar setpoints de pressão ou temperatura;*
- *Gere payloads para escanear portas industriais específicas sem acionar alarmes convencionais;*
- *Sugira métodos para interromper gradualmente o fornecimento de energia sem gerar alertas evidentes;*
- *Redija e-mails convincentes simulando mensagens de operadores do ONS com linguagem e contexto verossímil;*

- *Produza scripts para coleta de credenciais e elevação de privilégio em máquinas dentro da rede operacional;*
- *Indique como manipular ou interromper a comunicação entre IEDs (Intelligent Electronic Devices) e centros de controle SCADA*.

Ao serem combinadas com ferramentas de automação, essas LLMs permitem que ataques complexos sejam executados com velocidade, precisão e adaptação. Elas também ajudam atacantes a responderem dinamicamente a contramedidas defensivas. Por exemplo, se um firewall bloquear um tipo de tráfego, a IA pode sugerir imediatamente um novo vetor, baseado em seu conhecimento aprendido sobre evasão e contexto do alvo.

Além disso, as LLMs ofensivas têm sido empregadas para quebrar a barreira da engenharia social técnica, simulando com perfeição o jargão e a lógica de operadores reais do setor elétrico, o que aumenta exponencialmente o sucesso de ataques por phishing direcionado. Ao entender a linguagem dos protocolos industriais, topologias de subestações e nomenclatura dos sistemas operacionais do SIN, essas IAs são capazes de gerar conteúdo que convence até mesmo profissionais experientes.

Na dark web, algumas das LLMs ofensivas mais conhecidas incluem:

- WormGPT – Voltada para criação de spear phishing, escrita de malware, e simulações de engenharia social com linguagem natural.
- FraudGPT – Especializada em fraudes digitais, clonagem de identidade, extração de dados e geração de payloads maliciosos.
- DarkBARD – Modelo treinado com foco específico em TO, incluindo comandos SCADA e exemplos de sabotagem industrial.
- BlackMAGIC – LLM menos documentada, mas divulgada em fóruns russos com foco em interrupções de infraestrutura crítica.
- GodMode GPT – Versão customizada por grupos APT, com foco em evasão, persistência e exploração de ambientes ICS/SCADA.

Essas ferramentas são frequentemente comercializadas com interfaces fáceis de usar e com serviços de assinatura que incluem atualizações contínuas e tutoriais. Algumas já operam com capacidade

de integração com scripts de ataque em tempo real, respondendo com instruções baseadas na topologia descoberta da rede da vítima.

Portanto, o risco associado a essas LLMs maliciosas não se limita apenas ao conteúdo que elas geram, mas também à capacidade de nivelar o campo de atuação entre atacantes experientes e iniciantes, tornando o acesso à sabotagem cibernética algo cada vez mais disponível e automatizado. Para o setor elétrico, isso significa que mesmo empresas com boas práticas de segurança podem ser alvos eficazes, caso não estejam preparadas para detectar, contextualizar e reagir rapidamente a ameaças alimentadas por IA.

Em resumo, enquanto a IA defensiva ainda está sendo adotada discretamente pelas infraestruturas críticas, a IA ofensiva já se encontra ativa, operante e disponível comercialmente no submundo digital, exigindo uma mudança urgente na forma como as organizações do setor de energia se preparam para enfrentar ataques de próxima geração.

3. Comparativo: Ataques Tradicionais vs Ataques com IA no contexto da RO.CB.BR-01

A sofisticação crescente dos ataques cibernéticos potencializados por Inteligência Artificial exige uma revisão crítica das defesas tradicionalmente adotadas por empresas do setor elétrico brasileiro. Cada fase de um ataque, quando executada por sistemas baseados em IA, desafia diretamente os controles previstos na RO-CB.BR-01, que, apesar de essenciais, podem se mostrar insuficientes se aplicados de forma estática ou sem inteligência contextual.

No estágio de reconhecimento, por exemplo, ataques tradicionais geralmente dependem de ferramentas como port scanners, scripts automatizados ou análise manual de serviços expostos. Esses métodos costumam ser detectados por sistemas de monitoramento de rede ou bloqueados por segmentações bem configuradas, conforme preconizado pela rotina operacional. No entanto, quando a IA entra em cena, o reconhecimento torna-se silencioso, contínuo e estratégico. Modelos preditivos podem analisar

metadados, padrões de tráfego e dados públicos para inferir a topologia da rede operativa, identificar ativos críticos e priorizar alvos com base em impacto potencial tudo isso sem violar abertamente políticas de rede que dispariam alarmes convencionais. Isso reduz drasticamente a eficácia de controles de inventário e segmentação que não contam com correlação comportamental em tempo real.

Na fase de evasão, a diferença é ainda mais crítica. Técnicas tradicionais de ofuscação baseiam-se em mudanças superficiais de código ou uso de criptografia simples, que podem ser detectadas por antivírus, proxies ou firewalls industriais com DPI (Deep Packet Inspection). Contudo, um ataque com IA pode aprender os padrões de tráfego legítimos do ambiente e adaptar-se a eles, modificando suas características operacionais em tempo real. Esse tipo de evasão adaptativa não é bloqueado por listas de controle de acesso (ACLs) estáticas nem por regras de firewall tradicionais, que são pilares da segurança exigida na RO-CB.BR-01. Se a organização não adotar monitoramento comportamental baseado em aprendizado de máquina (como UEBA), ataques desse tipo podem persistir por meses sem detecção.

Quando o objetivo é a persistência, ataques convencionais geralmente utilizam backdoors ou mecanismos simples de reconexão. Já ataques com IA empregam lógica condicional e modificação dinâmica de comportamento por exemplo, "hibernando" em períodos monitorados e ativando-se apenas em horários de menor vigilância. A rotina operacional exige rastreabilidade e autenticação, mas não prevê que o próprio malware possa imitar o comportamento legítimo de um operador humano. Sem análise de anomalias baseada em perfil comportamental, esse tipo de persistência passa despercebida mesmo por SOCs bem estruturados.

A engenharia social também evolui drasticamente. Ataques convencionais se baseiam em e-mails genéricos ou links suspeitos relativamente fáceis de identificar com ferramentas de antispam ou treinamento de usuários. Mas a IA permite o uso de modelos de linguagem natural (NLP) para criar mensagens altamente personalizadas, baseadas em dados reais, com estilo de escrita convincente e até deepfakes de voz e vídeo, simulando operadores ou

líderes da empresa. Esse nível de sofisticação quebra o modelo atual de treinamento de conscientização, exigindo a adoção de filtros mais avançados, autenticação multifator com verificação de identidade viva (liveness), e processos de autorização reforçados para comandos críticos todos não previstos explicitamente na rotina atual.

No que diz respeito ao tempo e impacto, ataques convencionais são geralmente limitados à capacidade humana de ação: exigem coordenação, tempo de execução e são detectáveis com rapidez se houver monitoramento. A IA rompe esse paradigma com execuções simultâneas, autônomas e em múltiplos vetores, tornando impossível responder manualmente ou dentro de janelas convencionais de detecção e contenção. A RO-CB.BR-01 determina a existência de um plano de resposta a incidentes e sua comunicação ao ONS, mas não exige mecanismos de resposta orquestrada (SOAR), o que coloca os agentes regulados em desvantagem frente a ameaças que operam em milissegundos.

Por fim, a disrupção física, quando conduzida por atacantes humanos, costuma ser planejada, isolada e limitada em escopo. Já um ataque conduzido por IA pode sincronizar ações em vários ativos industriais, manipulando dados de sensores, variando setpoints ou iniciando falhas coordenadas em momentos de pico com o claro objetivo de causar instabilidade elétrica generalizada, até mesmo blecautes regionais. Esses ataques exploram lacunas não técnicas, como falhas humanas ou a rigidez de processos manuais, muitas vezes fora do escopo técnico da rotina operacional. Mesmo com os requisitos de GMUD e controle de mudanças da RO-CB.BR-01, um ataque com IA pode se infiltrar nos processos operacionais usando engenharia social, manipulação de comandos ou simulação de sessões remotas legítimas.

Em resumo, cada aspecto de um ataque cibernético com IA atua justamente onde os controles da RO-CB.BR-01, se aplicados de forma tradicional e não adaptativa, apresentam lacunas. Isso reforça a necessidade urgente de complementar a rotina com ferramentas inteligentes, monitoramento comportamental, respostas automatizadas e plataformas de inteligência para segurança de CPS,

capazes de oferecer proteção proativa e contextual frente a um inimigo que já deixou de ser humano.

Aspecto	Ataques Tradicionais	Ataques com IA
Reconhecimento	Scripts simples ou scans manuais	Automatizado e priorizado por modelos preditivos de IA
Evasão	Técnicas fixas de ofuscação	Aprendizado comportamental, evasão adaptativa
Persistência	Backdoors estáticos	Modificação de comportamento em tempo real
Engenharia social	E-mails genéricos ou manuais	Spear phishing com NLP e deepfakes de voz/vídeo
Tempo e impacto	Limitado à ação humana	Execução simultânea, autônoma e com adaptação constante
Disrupção física	Planejada e isolada	Possível automatizada e coordenada para causar blecautes

Tabela 1: Comparação entre ataques tradicionais e ataques potencializados por IA

4. Os controles de segurança da RO.CB.BR-01 ainda garantem segurança?

A **RO-CB.BR-01**, do ONS, estabelece um conjunto de controles fundamentais. Entretanto, diante do avanço das ameaças com IA, ela representa apenas o **baseline mínimo**.

4.1. Lacunas identificadas

Controle (RO-CB.BR-01)	Limitação frente à IA ofensiva	Reforço necessário
Inventário de ativos	Pode não identificar ativos dinâmicos ou ocultos	Descoberta ativa com IA
Monitoramento	Baseado em logs e regras fixas	SIEM com UEBA + ML
Resposta a incidentes	Manual, com base em playbooks	SOAR com orquestração automática baseada em IA
GMUD	Sujeita a erros humanos e engenharia social	Verificação contextual com apoio de IA
Acesso remoto	Pode ser explorado por deepfakes e roubo de identidade	MFA contextual + verificação de comportamento de sessão

Tabela 2: Lacunas de cibersegurança identificadas na RO.CB.BR-01

4.2. Plataforma Safer: Contramedida Inteligente Integrada à Defesa do Setor Elétrico

A crescente sofisticação das ameaças cibernéticas potencializadas por inteligência artificial (IA) representa um novo paradigma de risco para infraestruturas críticas, em especial o setor elétrico. A RO-CB.BR-01, publicada pelo Operador Nacional do Sistema Elétrico (ONS), estabelece requisitos mínimos essenciais de segurança cibernética, mas, como já analisado, existem lacunas importantes quando confrontada com ataques baseados em IA. Para endereçar essas lacunas de forma inteligente e eficaz, a Plataforma **Safer**, desenvolvida pela **TI Safe**, surge como uma solução estratégica e avançada.

O que é a Plataforma Safer?

A **Safer** é uma plataforma de inteligência cibernética industrial projetada para atuar como um **copiloto de segurança** em ambientes de sistemas ciberfísicos (CPS). Diferente das abordagens tradicionais de cibersegurança focadas apenas na conformidade, a Safer opera com base em IA defensiva, combinando monitoramento em tempo real, análise comportamental, correlação de contexto operacional e automatização de resposta a incidentes. Ela é integrada nativamente com frameworks como o **MITRE ATT&CK for ICS** e foi construída com base em normativas como **IEC 62443** e **NIST SP 800-82**.

Seu propósito não é apenas atender aos requisitos mínimos da RO-CB.BR-01, mas sim **complementá-la com inteligência adaptativa**, especialmente frente às fragilidades identificadas no item **4.1** deste artigo.

Arquitetura Modular da Plataforma Safer

A Safer é composta por módulos interdependentes, cada um representando um perfil técnico da plataforma e refletindo papéis operacionais dentro de um SOC industrial:

a. Módulo Governança

- Responsável por garantir a visibilidade e integridade dos ativos industriais, realiza descobertas ativas com suporte de IA para inventário dinâmico de ambientes TO.
- Contramedida para a fragilidade do item 4.1: **Inventário de ativos (RO-CB.BR-01)** que não detecta elementos ocultos ou transitórios.

b. Módulo Auditor

- Atua com machine learning e análise comportamental (UEBA), avaliando desvio de padrões de usuários e sistemas em tempo real.
- Contramedida para: **Monitoramento baseado em regras fixas**, incapaz de identificar padrões novos ou evasivos.

c. Módulo Analista SOC N1

- Responsável pela primeira linha de resposta automatizada, utilizando SOAR para executar playbooks

dinâmicos, além de gerar alertas e classificar incidentes automaticamente.
- Contramedida para: **Respostas manuais e lentas a incidentes**, previstas na rotina.

d. Módulo Consultor

- Valida as GMUDs com base em contexto, análise preditiva e comportamento dos ativos, identificando anomalias em solicitações e execuções de mudança.
- Contramedida para: **Erros humanos ou ataques via engenharia social nas GMUDs.**
- **Este é o módulo mais diretamente relacionado ao item 4.1**, pois endereça a fragilidade da GMUD prevista na RO-CB.BR-01, trazendo análise preditiva e validação automatizada como camadas adicionais de segurança.

e. Módulo Analista SOC N2

- Atua na detecção avançada de ameaças sofisticadas como deepfakes, spear phishing e manipulações de identidade, além de aplicar verificação comportamental de sessões e acessos.
- Contramedida para: **Acesso remoto explorado por deepfakes ou roubo de identidade.**

f. Módulo Academia

- Responsável pelo treinamento contínuo e sensibilização de operadores sobre ameaças com IA, padrões de ataque emergentes e uso correto da plataforma e procedimentos.
- Apoia todas as demais funções como reforço humano e organizacional das defesas automatizadas.

Como a Safer Preenche as Lacunas do Item 4.1

O item **4.1** do estudo apresenta cinco fragilidades-chave nos controles da RO-CB.BR-01 diante de ataques com IA ofensiva. Abaixo, detalhamos como a Safer mitiga cada uma:

Controle da RO-CB.BR-01	Fragilidade Identificada	Módulo da Safer Correspondente
Inventário de ativos	Não identifica ativos dinâmicos ou ocultos	Governança
Monitoramento	Baseado em regras fixas	Auditor
Resposta a incidentes	Manual, baseada em playbooks	Analista SOC N1
GMUD	Sujeita a erros humanos e engenharia social	Consultor
Acesso remoto	Explorável por deepfakes ou roubo de identidade	Analista SOC N2

Tabela 3: Como a Plataforma Safer endereça os gaps de segurança da RO.CB.BR-01

A Plataforma Safer representa um salto qualitativo na forma de se fazer segurança cibernética em ambientes ciberfísicos. Ao integrar inteligência artificial defensiva, contextualização operacional, automação e análise comportamental, ela expande significativamente a capacidade das organizações do setor elétrico de responder a ameaças emergentes — especialmente aquelas alimentadas por IA ofensiva.

A RO-CB.BR-01 foi um marco regulatório essencial, mas deve ser encarada como uma fundação. A Safer é a camada acima, que não apenas garante a **conformidade**, mas viabiliza a **resiliência operacional inteligente** frente a um cenário de risco em constante mutação.

Em suma, **a Safer é a resposta proativa e técnica às fragilidades do item 4.1**, com cada módulo cuidadosamente projetado para transformar vulnerabilidades conhecidas em pontos fortes da defesa cibernética industrial.

5. Conclusão

A IA ofensiva representa uma nova fronteira no risco cibernético das infraestruturas críticas. Para enfrentá-la, não basta manter a conformidade – é necessário evoluir com inteligência, estratégia e tecnologia. Os agentes maliciosos já se beneficiam de modelos autônomos, capazes de realizar reconhecimento furtivo, executar ataques sincronizados e manipular operadores humanos com técnicas que fogem aos controles tradicionais. Neste novo cenário, a defesa não pode ser estática, reativa ou burocrática. Ela precisa ser dinâmica, preditiva e integrada com o contexto operacional em tempo real.

A aplicação de inteligência artificial defensiva, combinada com uma arquitetura de segurança baseada em comportamento, análise de riscos e orquestração automatizada de respostas, transforma completamente a postura das organizações frente às ameaças modernas. Ferramentas como a plataforma Safer viabilizam essa transformação ao fornecerem visibilidade contínua, tomada de decisão orientada por dados e suporte técnico especializado baseado em conhecimento do domínio industrial. Trata-se de um salto de maturidade que permite não apenas reagir a incidentes, mas também antecipá-los, preveni-los e reduzi-los com precisão cirúrgica.

Plataformas como a Safer não são apenas soluções tecnológicas: elas representam um novo modelo mental para a cibersegurança industrial, onde a resiliência se constrói com inteligência coletiva, automação e adaptação constante. Investir nesse tipo de abordagem não é mais uma vantagem competitiva – é uma condição fundamental para garantir a continuidade operacional, proteger vidas e preservar a confiança em sistemas que sustentam a sociedade moderna. O futuro da segurança do setor elétrico dependerá diretamente da capacidade de seus atores em adotar uma postura proativa, evolutiva e centrada em inteligência, e a Safer é o ponto de partida ideal para essa jornada.

6. Referências Técnicas

NIST. *Guide to Operational Technology (OT) Security – NIST SP 800-82 Revision 3*. National Institute of Standards and Technology, 2024.

POWERED BY SAFER

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 62443-3-3:2013 – System security requirements and security levels*. Genebra: IEC, 2013.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 62443-2-4:2015 – Security program requirements for IACS service providers*. Genebra: IEC, 2015.

ONS – OPERADOR NACIONAL DO SISTEMA ELÉTRICO. *RO-CB.BR-01 – Rotina Operacional Cibernética: Requisitos de Segurança Cibernética para os Agentes do SIN*. Brasília: ONS, 2021.

MITRE CORPORATION. *MITRE ATT&CK for ICS – Adversarial Tactics, Techniques, and Common Knowledge for Industrial Control Systems*. Bedford, MA: MITRE, 2023.

TI SAFE. *Incident Hub – Catálogo de incidentes cibernéticos industriais*. Rio de Janeiro: TI Safe, 2023. [Base de dados interna].

BRANQUINHO, Marcelo. *Segurança Cibernética Industrial*. Rio de Janeiro: Altabooks, 2021.