ESCOLA SUPERIOR DE GUERRA

CAIO CÉSAR MORI CARÉLO

A AMEAÇA CIBERNÉTICA ÀS INFRAESTRUTURAS CRÍTICAS NACIONAIS:

Gestão contínua de exposição a ameaças cibernéticas na Petrobras

Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Rafael Carduz Rocha

Rio de Janeiro

2024

C2024ESG

Documento assinado digitalmente
gov.br
CAIO CESAR MORI CARELO
Data: 22/10/2024 10:04:11-0300
Verifique em https://validar.iti.gov.br

_____

CAIO CÉSAR MORI CARÉLO

RESUMO

Este ensaio analisa a Gestão Contínua de Exposição a Ameaças Cibernéticas (CTEM, do inglês *Continuous Threat Exposure Management*) na Petrobras, uma empresa que detém uma das principais infraestruturas críticas nacionais. O estudo explora a aplicação do CTEM na companhia e suas implicações para a segurança cibernética, com foco em práticas de integração com governança, riscos e conformidade, bem como na detecção e respostas a ameaças cibernéticas. Observa-se que a Petrobras tem avançado em sua maturidade cibernética, mas desafios permanecem, particularmente na priorização e validação de ameaças. A pesquisa também destaca a importância de aprimorar a postura de segurança da empresa, promovendo uma abordagem proativa e integrada que possa responder eficazmente às ameaças emergentes.

Palavras-chave: infraestruturas críticas; gestão contínua de exposição a ameaças; segurança cibernética; Petrobras.

ABSTRACT

This essay analyzes Continuous Threat Exposure Management (CTEM) at Petrobras, a company that holds one of the nation's most critical infrastructures. The study explores the application of CTEM within the company and its implications for cybersecurity, focusing on practices for integration with governance, risk, and compliance, as well as on threat detection and response. It is observed that Petrobras has made progress in its cybersecurity maturity; however, challenges remain, particularly in the prioritization and validation of threats. The research also highlights the importance of enhancing the company's security posture, promoting a proactive and integrated approach that can effectively respond to emerging threats.

Keywords: *critical infrastructures; continuous threat exposure management; cybersecurity; Petrobras.*

1 INTRODUÇÃO

Sistemas e ativos críticos são essenciais para o funcionamento de uma sociedade contemporânea. A interrupção ou eliminação desses recursos pode resultar em significativos efeitos econômicos, sociais e na segurança do país (Araujo, 2020). Dentre as entidades que dispõem dessas infraestruturas essenciais, são notáveis aquelas dos segmentos de energia, telecomunicações, saneamento, transportes, saúde e segurança pública (Nonato; Pinho, 2021). Em sua grande parte, esses sistemas são altamente interligados e suscetíveis a ataques físicos e cibernéticos (Brasil, 2024). Portanto, assegurar a proteção dessas estruturas é crucial para a estabilidade e a qualidade de vida da sociedade (Moraes, 2019).

Uma das maiores dificuldades nas estratégias convencionais de segurança cibernética em infraestruturas críticas é o enfoque reativo, que procura mitigar vulnerabilidades através de correções e atualizações esporádicas. Esta estratégia se torna inviável em contextos em que qualquer interrupção pode resultar em consequências devastadoras (D'Hoinne; Shoard; Schneider, 2023).

Dentro deste contexto, a Gestão Contínua de Exposição a Ameaças (CTEM, do inglês *Continuous Threat Exposure Management*) se apresenta como uma estratégia alternativa, possibilitando que as organizações avaliem os riscos e vulnerabilidades de seus ativos digitais e físicos de forma mais ampla. O propósito central do CTEM é aprimorar continuamente as prioridades de segurança cibernética, desenvolvendo um plano de remediação compreensível para os executivos e viável para as equipes de cibersegurança.

Desta forma, o propósito deste ensaio é investigar como a Petrobras implementa o processo de gerenciamento contínuo de exposição a ameaças cibernéticas, com o intuito de salvaguardar suas infraestruturas críticas.

1.1 Petróleo Brasileiro S.A. (Petrobras)

A Petrobras é uma empresa estatal de economia mista, fundada em 1953. A União, representada pelo Governo Federal, é a acionista majoritária, sendo responsável por nomear o presidente da companhia — um fator relevante ao longo

dos seus 68 anos de operação, durante os quais a empresa foi presidida por diversas lideranças militares (Petrobras, 2024).

Com sede no Rio de Janeiro, a Petrobras atua em dez países e emprega aproximadamente quarenta mil funcionários. A empresa é uma das maiores produtoras de petróleo e gás do mundo, com foco na exploração, produção, refino, geração e comercialização de energia. Entre seus ativos, destacam-se sessenta e sete plataformas que extraem 2,84 milhões de barris de óleo equivalente por dia, treze refinarias com uma produção diária de 1,8 milhão de barris de derivados, uma frota de mais de cento e trinta navios, cinco unidades de biocombustíveis e vinte usinas termelétricas (Petrobras, 2023).

Nos últimos anos, a Petrobras tem fortalecido suas estratégias de segurança cibernética. Desde 2020, após enfrentar um ataque direcionado ao ambiente de aplicações expostas na Internet, a empresa adotou uma postura mais resiliente, assegurando a integridade de suas operações.

Como parte dessa evolução, foi criada uma Gerência Executiva de Segurança da Informação, que opera de forma independente, mas em paridade hierárquica com o departamento de Tecnologia da Informação e Telecomunicações, ambos subordinados à mesma diretoria corporativa. Essa estrutura organizacional promove uma divisão clara de papéis e responsabilidades, reforçando a segurança cibernética da empresa.

Outro exemplo dos avanços na maturidade cibernética da Petrobras foi a elaboração de um Plano Diretor de Segurança da Informação em 2024, no qual a empresa definiu dois objetivos estratégicos complementares para fortalecer sua atuação, ambos diretamente relacionados ao presente ensaio acadêmico:

- Proteger as Informações e os ativos críticos para habilitar os negócios da Petrobras, atuando com excelência operacional baseada nas melhores práticas de mercado; e
- Ser reconhecida como uma área estratégica e agregadora de valor, disseminando uma cultura de Segurança da Informação que antecipe riscos por meio de soluções inovadoras, simples e eficientes para a companhia e seus usuários.

1.2 Organização do trabalho

Além desse capítulo introdutório, o ensaio é composto por mais dois capítulos:

- **Capítulo 2:** apresenta a fundamentação teórica do ensaio, abordando a definição e os objetivos do CTEM, as cinco etapas fundamentais de um ciclo CTEM, bem como os desafios associados a essa abordagem; e
- **Capítulo 3:** conclui a pesquisa, fornecendo as considerações finais e um resumo da posição da Petrobras em relação ao CTEM.

2 FUNDAMENTAÇÃO TEÓRICA

A constante evolução das ameaças cibernéticas apresenta novos desafios para as empresas, especialmente para aquelas que possuem infraestruturas críticas, como é o caso da Petrobras. Neste contexto, o CTEM emerge como uma estratégia para administrar, priorizar e minimizar riscos cibernéticos (D'Hoinne; Shoard, 2023).

Neste sentido, este capítulo explora em detalhes a aplicação do CTEM na Petrobras. Inicialmente, a Seção 2.1 aborda a definição e objetivos do programa. Em seguida, a Seção 2.2 detalha as cinco etapas fundamentais de um ciclo CTEM. O capítulo é finalizado com a Seção 2.3, listando os desafios do CTEM.

2.1 Definição e objetivos do CTEM

O CTEM é um programa integrado, iterativo e contínuo que prioriza tratamentos e aprimora a postura de segurança da organização. Seu ciclo inclui cinco etapas fundamentais: Escopo, Descoberta, Priorização, Validação e Mobilização. Essa abordagem se diferencia por não apenas focar em vulnerabilidades tradicionais, mas também por considerar superfícies de ataque mais amplas, incluindo ambientes de nuvem e infraestruturas expostas à internet.

Dentre os principais objetivos da adoção de um programa integrado de CTEM, destacam-se:

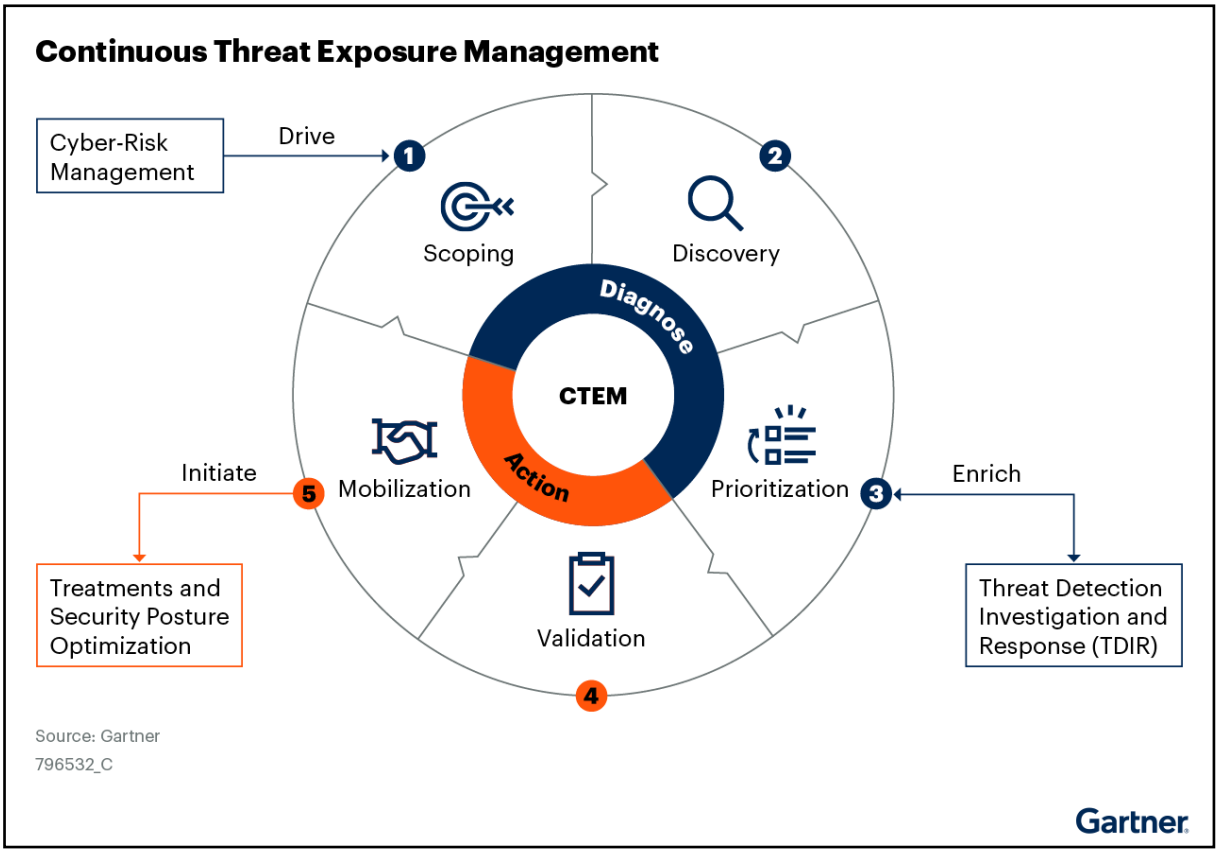
- **Avaliar e gerenciar continuamente a exposição a ameaças**: visa identificar, monitorar e reduzir a exposição a ameaças, considerando tanto vulnerabilidades quanto outras formas de exposição, como falhas de configurações em dispositivos de usuários e elementos de rede;
- **Priorizar vulnerabilidades com base no impacto nos negócios:** o programa busca alinhar a priorização das ameaças e vulnerabilidades de acordo com os ativos mais críticos e o impacto potencial para o negócio, levando em conta o ponto de vista do atacante;
- **Melhorar a remediação de segurança de forma consistente:** tem como objetivo fornecer um plano de ação contínuo e acionável para remediação de exposições, que seja compreendido pelos executivos e executado pelas equipes técnicas;

- **Facilitar a mobilização e colaboração entre equipes:** incentiva a colaboração entre diferentes áreas, como segurança da informação, operações de infraestrutura e arquitetos de sistemas, para garantir uma resposta coordenada às ameaças; e
- **Expandir a gestão de exposição para superfícies de ataque:** busca incluir novas áreas de exposição dentro do processo de remediação, considerando, por exemplo, ambientes de nuvem, cadeia de suprimentos e outros ativos externos ao controle direto da organização.

2.2 As cinco etapas fundamentais de um ciclo CTEM

Cada etapa de um ciclo CTEM tem um papel específico no processo contínuo de identificação, avaliação e tratamento de vulnerabilidades. A Figura 1 ilustra essas etapas, dividindo-as em duas fases: diagnóstico e ação.

Figura 1 - As cinco etapas fundamentais de um ciclo CTEM.



Fonte: D'Hoinne e Shoard (2023).

2.2.1 Escopo

A etapa de escopo é o ponto inicial de um ciclo CTEM e tem como objetivo definir a extensão da superfície de ataque a ser avaliada. Nessa fase, é crucial identificar os ativos e sistemas que apresentam maior risco para a organização, garantindo que os esforços de segurança se concentrem nas áreas mais críticas. Um escopo bem delineado permite alinhar o CTEM com as prioridades do negócio, otimizando o uso de recursos e assegurando que as vulnerabilidades mais relevantes sejam abordadas primeiro.

Atualmente, na Petrobras, o escopo é estabelecido com ênfase na camada de infraestrutura, levando em conta critérios de risco como aplicações que são auditadas pela Lei Sarbanes-Oxley (SOX) e ativos situados em áreas desmilitarizadas (DMZ). Contudo, para progredir, é necessário expandir essa perspectiva, incorporando o cenário de ameaças de maneira mais ampla, intensificando a integração com a Governança, Riscos e Conformidade (GRC) e expandindo o alcance para abranger todas as infraestruturas críticas e subsidiárias do sistema Petrobras. Ademais, é imprescindível considerar campos como desenvolvimento seguro e computação em nuvem para uma gestão de vulnerabilidades mais completa e unificada.

2.2.2 Descoberta

Após definir o escopo, a etapa de descoberta envolve a identificação e catalogação de vulnerabilidades, configurações incorretas e outras exposições presentes nos ativos definidos. Nesta fase, a organização utiliza ferramentas e técnicas para mapear completamente a superfície de ataque, identificando potenciais pontos de entrada que possam ser explorados por adversários.

No momento, a fase de descoberta na Petrobras é feita principalmente através de ferramentas como *ServiceNow ITOM* e *Tenable IO*, concentrando-se em aspectos como portas abertas na DMZ. Contudo, a meta futura é ampliar essa detecção, integrando dados de várias fontes para aprimorar a precisão e oferecer uma visão mais abrangente da exposição externa. Este passo é crucial para obter uma visão mais abrangente das possíveis ameaças.

2.2.3 Priorização

A etapa de priorização no CTEM é crucial para determinar quais vulnerabilidades e exposições identificadas devem ser tratadas primeiro. Dado que a maioria das organizações, incluindo a Petrobras, não consegue corrigir todas as vulnerabilidades ao mesmo tempo, é necessário priorizar as ameaças com base em diversos critérios. Esses critérios incluem: criticidade da vulnerabilidade, impacto no negócio, probabilidade de exploração e eventuais medidas de segurança compensatórias.

Atualmente, a priorização na Petrobras é fundamentada em indicadores de ameaças amplamente conhecidos, como o *Exploit Prediction Scoring System* (EPSS) e o *Vulnerability Priority Rating* (VPR), que são utilizados para avaliar a probabilidade de uma vulnerabilidade ser explorada e qual o impacto potencial para as organizações, respectivamente.

Para alcançar o estado almejado, é crucial conectar de forma mais aprofundada as informações sobre ameaças aos processos de gestão de vulnerabilidades e relacioná-las aos riscos empresariais. Esta estratégia possibilitará que a priorização de vulnerabilidades seja feita de forma mais estratégica, em consonância com as metas e demandas da organização. Por exemplo, imagine que a Petrobras identifica duas vulnerabilidades:

1. Vulnerabilidade A: Baixa probabilidade de exploração, mas alto impacto nas operações industriais.
2. Vulnerabilidade B: Alta probabilidade de exploração, mas impacto moderado no sistema de e-mail.

Se a prioridade de tratamento fosse dada apenas pelos indicadores EPSS e VPR, a Vulnerabilidade B seria corrigida primeiro. No entanto, ao considerar o impacto no negócio proposto pelo CTEM, a Petrobras deve priorizar a Vulnerabilidade A devido às possíveis interrupções operacionais.

2.2.4 Validação

Na etapa de validação, as medidas de segurança propostas são testadas para garantir sua eficácia e viabilidade operacional. O objetivo é assegurar que as ações de remediação planejadas realmente mitiguem os riscos identificados e possam ser

implementadas sem prejudicar as operações da empresa. Essa fase pode envolver a execução de testes de penetração, simulações de ataques ou o uso de ferramentas especializadas de simulação de ameaças, avaliando a capacidade da organização de se defender contra cenários de ataque reais e validando a adequação dos controles de segurança adotados.

No modelo atual, a fase de validação na Petrobras inclui verificações básicas e a execução de testes de penetração ocasionais. A intenção da companhia é estabelecer um programa de testes mais organizado, alinhado com as prioridades da gestão de vulnerabilidades, além de implantar soluções automatizadas para validar a exploração das vulnerabilidades no ambiente da Petrobras. Estas melhorias possibilitarão uma fase validação mais sólida e um controle mais eficaz sobre a exposição.

2.2.5 Mobilização

A etapa final do ciclo CTEM é a mobilização, que consiste no momento em que as descobertas e priorizações do ciclo do CTEM são transformadas em ações práticas, garantindo que a segurança cibernética seja continuamente aprimorada e alinhada com as necessidades estratégicas da organização.

Na mobilização, é essencial superar barreiras de comunicação e possíveis conflitos de prioridade entre equipes, garantindo que os esforços de segurança não ocorram isoladamente, mas de maneira integrada com os objetivos do negócio. Na Petrobras, esse ponto é particularmente desafiador, pois na maioria das vezes a mobilização envolve a coordenação entre diferentes departamentos para garantir que todas as partes estejam cientes das ações a serem tomadas.

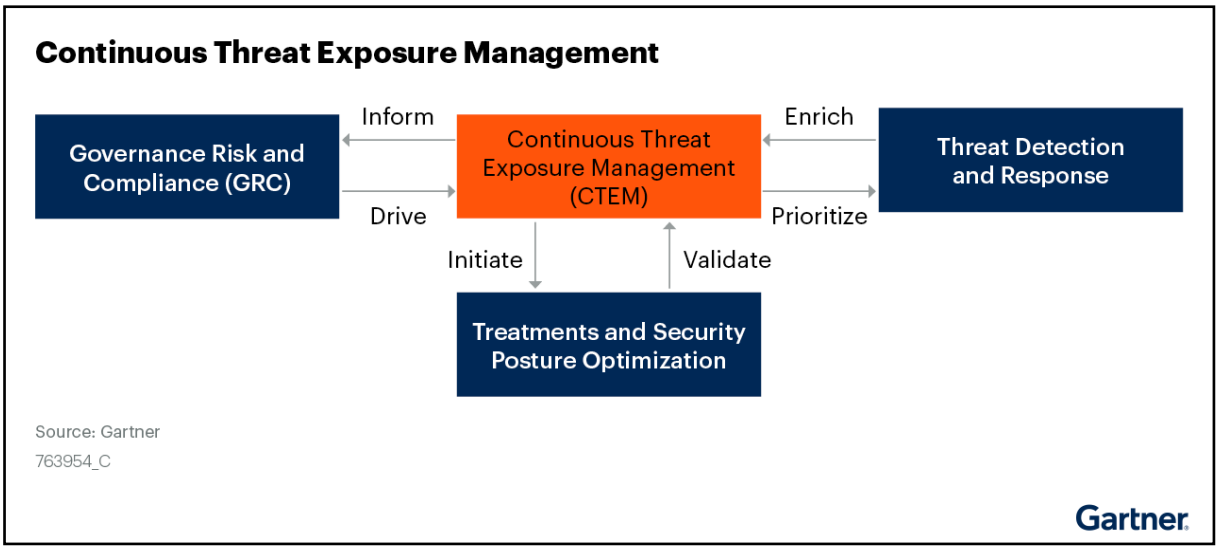
Atualmente, a fase de mobilização na Petrobras utiliza indicadores caseiros para validar sua eficácia, que não permitem comparação com outras empresas. Para alcançar o estado futuro pretendido, a empresa pretende adotar indicadores de mercado, além de intensificar a colaboração entre o grupo Grupo de Resposta a Incidentes de Segurança (CSIRT, do inglês *Computer Security Incident Response Team*) e os times de infraestrutura, assegurando que essas unidades estejam totalmente engajadas.

2.3 Desafios do CTEM

Embora os benefícios sejam evidentes, a aplicação do CTEM apresenta desafios consideráveis. Muitas organizações falham em suas estratégias de CTEM devido a abordagens centradas em ferramentas e processos fragmentados, que resultam em longas listas de remediação pouco acionáveis. Outro desafio é a validação das medidas de segurança implementadas e a mobilização das equipes para ações colaborativas. A dependência excessiva de ferramentas de automação pode levar a um falso senso de segurança, e a falta de integração entre diferentes equipes pode comprometer a eficácia das ações.

A Figura 2 apresenta os três principais processos que interagem com o CTEM, e na sequência cada uma dessas interações serão detalhadas e debatidas.

Figura 2 – Integrações do CTEM com outros processos.



Fonte: D'Hoinne, Shoard e Schneider (2023).

2.3.1 Integração do CTEM com Governança, Riscos e Conformidade

A integração do CTEM com o GRC é essencial para alinhar as práticas de segurança com os riscos e requisitos corporativos. O GRC desempenha um papel central, fornecendo orientação estratégica para o CTEM e ajudando a priorizar ameaças com base no impacto potencial nos ativos críticos, conhecidos como as "joias da coroa".

Essa integração auxilia na criação de planos de ação efetivos para mitigar riscos e otimizar a postura de segurança. Além disso, a colaboração entre GRC e CTEM garante que as medidas de mitigação sejam continuamente aprimoradas, promovendo uma abordagem proativa para a segurança cibernética.

Na prática, a Petrobras enfrenta desafios na integração plena entre o GRC e o CTEM. Há necessidade de maior visibilidade e análise crítica conjunta do processo de remediação de riscos corporativos, assim como de um alinhamento mais próximo com o negócio. A Petrobras reconhece a necessidade de aprimorar a relação entre descobertas, mitigações e riscos corporativos para fortalecer a postura de segurança de forma dinâmica e responsiva.

2.3.2 Integração com Detecção e Resposta a Ameaças

Outro aspecto crítico do CTEM é sua integração com a Detecção e Resposta a Ameaças. Esse processo fornece dados valiosos sobre atividades suspeitas e incidentes em andamento, enriquecendo o CTEM com informações que ajudam a priorizar vulnerabilidades mais suscetíveis de serem exploradas por adversários. Essa integração contínua é vital para garantir que as medidas de segurança permaneçam eficazes e sejam ajustadas conforme novas ameaças surjam.

A Petrobras tem implementado esse ciclo de feedback em suas métricas, considerando informações de ameaças nas avaliações de vulnerabilidades. Contudo, há espaço para aprimoramento, especialmente em relação à integração de informações associadas a vulnerabilidades existentes em seus ambientes e à adoção de uma solução de gerenciamento da superfície de ataque.

2.3.3 Tratamentos e Otimização da Postura de Segurança no CTEM

Um CTEM eficaz vai além de remediações automatizadas. A otimização da postura de segurança envolve a integração de diferentes tratamentos, considerando também situações em que as remediações não são simples ou automatizáveis. O CTEM permite que as organizações definam prioridades baseadas não apenas na criticidade das ameaças, mas também na viabilidade de implementação das medidas, considerando as possíveis implicações para o negócio.

O CTEM na Petrobras não se limita apenas a remediações técnicas, como aplicação de correções de segurança, mas também abrange uma abordagem mais ampla, incluindo a validação constante das medidas implementadas. Por outro lado, a companhia precisa avançar na integração com atividades de como testes de penetração, simulações de ataques e avaliação contínua da eficácia das ações tomadas.

3 CONSIDERANÇÕES FINAIS

O presente estudo investigou a Gestão Contínua de Exposição a Ameaças (CTEM, do inglês *Continuous Threat Exposure Management*) no contexto da Petrobras, uma das principais organizações uma das principais organizações que compõem a infraestrutura crítica nacional. A pesquisa explorou como o CTEM é vital para proteger os ativos estratégicos da empresa, detalhando o estado atual de cada uma de suas etapas.

Recomenda-se que a Petrobras (i) amplie o escopo de avaliação, incluindo, por exemplo, infraestruturas críticas de suas subsidiárias; (ii) aperfeiçoe as etapas de descoberta e priorização, visando criar uma visão mais abrangente das vulnerabilidades e exposições existentes; (iii) fortaleça a etapa de validação com a incorporação de ferramentas automatizadas; e (iv) adote indicadores de mercado que permitam uma comparação de desempenho mais robusta com outras empresas.

Assim, com base nas informações levantadas, conclui-se que a Petrobras demonstra um nível significativo de maturidade cibernética, embora ainda enfrente desafios importantes, especialmente na integração plena entre o CTEM e a disciplina de governança, riscos e conformidade, de modo a garantir que a gestão de vulnerabilidades esteja em sintonia com as prioridades estratégicas da empresa.

Em conclusão, o CTEM representa uma abordagem essencial para mitigar riscos cibernéticos em infraestruturas críticas. A experiência da Petrobras ilustra a necessidade de adaptação contínua e investimentos constantes para enfrentar a complexidade crescente das ameaças cibernéticas às infraestruturas críticas nacionais.

REFERÊNCIAS

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. 2020. Monografia (Especialização) – Escola Superior de Guerra, Brasília, DF, 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Segurança de Infraestruturas Críticas (SIC)**. Brasília, DF: GSI, 2022. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic. Acesso em: 20 set. 2024.

D'HOINNE, J.; SHOARD, P.; SCHNEIDER, M. **Implement a Continuous Threat Exposure Management (CTEM) Program**. Stamford, CT: Gartner, Inc., 2023. Disponível em: https://www.gartner.com/document-reader/document/4016760. Acesso em: 11 set. 2024.

D'HOINNE, J.; SHOARD, P. **Top Strategic Technology Trends for 2024:** continuous threat exposure management. Stamford, CT: Gartner, Inc., 2023. Disponível em: https://www.gartner.com/document-reader/document/4840631. Acesso em: 11 set. 2024.

MORAES, Maria Helena dos Reis. **Infraestruturas críticas e o papel do Estado:** um estudo sobre a governança no Brasil. São Paulo: Editora USP, 2019.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. **A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional**. 2021. Monografia (Especialização) – Escola Superior de Guerra, Brasília, DF, 2021.

PETROBRAS. **Perfil: conheça mais sobre a nossa empresa**. Rio de Janeiro: Petrobras, 2023. Disponível em: https://petrobras.com.br/quem-somos/perfil. Acesso em: 20 set. 2024.

PETROBRAS. In: WIKIPÉDIA: a enciclopédia livre, [2024]. Disponível em: https://pt.wikipedia.org/wiki/Petrobras. Acesso em: 20 set. 2024.