UNIVERSIDADE FEDERAL DO PARÁ
NÚCLEO DE DESENVOLVIMENTO AMAZÔNICO EM ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO APLICADA

EUDES DANILO DA SILVA MENDONÇA

UMA ABORDAGEM INTEGRADA DE SEGURANÇA CIBERNÉTICA: INTEGRAÇÃO DO WASUH E DA BASE CVE MITRE PARA GESTÃO DE VULNERABILIDADES EM AMBIENTES COMPUTACIONAIS

Belém – Pará
2025

EUDES DANILO DA SILVA MENDONÇA

UMA ABORDAGEM INTEGRADA DE SEGURANÇA CIBERNÉTICA: INTEGRAÇÃO DO WASUH E DA BASE CVE MITRE PARA GESTÃO DE VULNERABILIDADES EM AMBIENTES COMPUTACIONAIS

Dissertação apresentada ao Programa de Pós-Graduação em Computação Aplicada do Núcleo de Desenvolvimento Amazônico em Engenharia, da Universidade Federal do Pará, como requisito para a obtenção do título de Mestre em Computação Aplicada.

Orientador: Prof. Dr. Otávio Noura.

Belém – Pará
2025

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

D111a da Silva Mendonça, Eudes Danilo.
UMA ABORDAGEM INTEGRADA DE SEGURANÇA CIBERNÉTICA: INTEGRAÇÃO DO WASUH E DA BASE CVE MITRE PARA GESTÃO DE VULNERABILIDADES EM AMBIENTES COMPUTACIONAIS / Eudes Danilo da Silva Mendonça. — 2025.
76 f. : il. color.

Orientador(a): Prof. Dr. Otavio Noura Teixeira
Dissertação (Mestrado) - Universidade Federal do Pará, Campus Universitário de Tucuruí, , Tucuruí, 2025.

1. Segurança Cibernética. 2. Dashboard. 3. CVE MITRE. I. Título.

CDD 621.3821

EUDES DANILO DA SILVA MENDONÇA

UMA ABORDAGEM INTEGRADA DE SEGURANÇA CIBERNÉTICA: INTEGRAÇÃO DO WASUH E DA BASE CVE MITRE PARA GESTÃO DE VULNERABILIDADES EM AMBIENTES COMPUTACIONAIS

Dissertação apresentada ao Programa de Pós-Graduação em Computação Aplicada do Núcleo de Desenvolvimento Amazônico em Engenharia, da Universidade Federal do Pará, como requisito para a obtenção do título de Mestre em Computação Aplicada.

Orientador: Prof. Dr. Otávio Noura.

Data: 28/08/2025
Banca Examinadora:

gov.br
Documento assinado digitalmente
OTAVIO NOURA TEIXEIRA
Data: 06/02/2026 17:08:14-0300
Verifique em https://validar.iti.gov.br

_____
Dr. Otávio Noura Teixeira – UFPA - Orientador

gov.br
Documento assinado digitalmente
ELTON RAFAEL ALVES
Data: 06/02/2026 17:33:28-0300
Verifique em https://validar.iti.gov.br

_____
Dr. Elton Rafael Alvez - UFPA

gov.br
Documento assinado digitalmente
MARCOS PAULO ALVES DE SOUSA
Data: 06/02/2026 19:34:48-0300
Verifique em https://validar.iti.gov.br

_____
Dr. Marcos Paulo Alves de Sousa - CESUPA

Dedicatória

Dedicamos este trabalho a todos que, de forma direta ou indireta, contribuíram para o seu sucesso, sendo fonte de motivação em cada etapa acadêmica. De maneira especial, quero expressar minha profunda gratidão ao meu pai (*in memoriam*), mãe, esposa e filho. Seus apoios incondicionais e amor foram a força propulsora por trás da conclusão deste objetivo. Sou grato a Deus por ter colocado em minha vida essas pessoas maravilhosas. Também sou grato por me conceder a bênção de ser pai de um menino fantástico, a quem amo profundamente. Este trabalho é dedicado à minha família, pois são a razão de minha força e perseverança.

AGRADECIMENTOS

Agradeço primeiramente a Deus, fonte de toda sabedoria e inspiração, por me guiar durante esta jornada acadêmica. Agradeço também aos meus pais Eudes Mendonça (*in memorian*) e Rubelucia Mendonça, pelo amor incondicional, apoio e sacrifícios que fizeram para que eu pudesse alcançar este marco em minha vida. Ao meu filho Raphael Danilo, por ser minha motivação diária e à minha esposa Michelle Mendonça, por ser meu pilar de força e compreensão, dedico este trabalho. Sem o amor, apoio e compreensão de vocês, este caminho teria sido muito mais difícil. Aos meus queridos irmãos e a toda a minha amada família. Cada conquista minha é também de vocês, e por isso, compartilho com vocês este momento de vitória.

Aos amigos de trabalho que se tornaram parte fundamental da minha jornada, aos colegas do Senai, Cesupa e Estácio, agradeço por compartilharem comigo não apenas o ambiente profissional, mas também amizade e apoio inestimáveis. Cada interação com vocês foi uma fonte de aprendizado e crescimento, e levo todas as memórias conosco para o futuro.

Aos professores Dr. Tadeu Paes e Dra. Larissa Luz, a ajuda direta de vocês moldou meu percurso nesta jornada acadêmica. A sabedoria e dedicação de vocês, foram faróis em momentos de desafio, e por isso, expresso minha mais profunda gratidão.

E a Msc. Prof. Alessandra Natasha, companheira fiel ao longo de toda minha jornada profissional, sua presença constante trouxe luz aos meus dias mais escuros e celebrou comigo nas horas mais radiantes. Somos uma equipe não apenas na vida pessoal, mas também na profissional, e por isso, esta conquista é nossa em conjunto.

Cada um de vocês contribuiu para este momento significativo em minha vida e por isso dedico este trabalho a todos, como um testemunho de nossa colaboração e amizade duradoura.

Dedico este trabalho ao meu orientador Prof. Dr. Otávio Noura. Sua paciência, dedicação e orientação foram fundamentais para o sucesso deste percurso acadêmico. Otávio não apenas foi um orientador, mas também um parceiro dedicado, sempre disposto a compartilhar conhecimento e insights valiosos. Sua orientação cuidadosa moldou não apenas este trabalho, mas também o meu entendimento mais amplo no campo de estudo. Esta conquista é, sem dúvida, fruto dessa parceria e do seu constante apoio.

RESUMO

Com o crescimento acelerado e a ampla adoção das tecnologias de informação e comunicação, a frequência e o impacto dos ataques cibernéticos se intensificam. Setores como saúde, finanças, tecnologia, governo, varejo e transporte enfrentam aumento constante nas ameaças à segurança cibernética. Esses ataques comprometem informações confidenciais e geram prejuízos, como perdas financeiras, redução da confiabilidade e outros impactos significativos. Diante desse cenário, o estudo investe em análises detalhadas de recursos e capacidades de segurança cibernética para identificar, prevenir e responder de forma eficaz às tentativas de ataque. Este trabalho desenvolve um script que integra um dashboard — interface gráfica voltada ao monitoramento de dados — à base CVE da MITRE, a qual disponibiliza avaliações contínuas de vulnerabilidades conhecidas para apoiar administradores de rede e profissionais de segurança da informação. O script identifica dinamicamente riscos e contribui para reduzir as ameaças à segurança dos sistemas de informação. informação.

Palavras-chave: Segurança Cibernética. Dashboard. CVE MITRE.

ABSTRACT

With the rapid growth and widespread adoption of information and communication technologies, the frequency and impact of cyberattacks continue to intensify. Sectors such as healthcare, finance, technology, government, retail, and transportation face a steady increase in cybersecurity threats. These attacks compromise confidential information and cause losses such as financial damage, reduced reliability, and other significant impacts. In this context, the study conducts detailed analyses of cybersecurity resources and capabilities to effectively identify, prevent, and respond to attempted attacks. This work develops a script that integrates a dashboard — a graphical interface for data monitoring — with the MITRE CVE database, which provides continuous assessments of known vulnerabilities to support network administrators and information security professionals. The script dynamically identifies risks and helps reduce threats to the security of information systems.

Keywords: Cybersecurity. Dashboard. MITRE CVE.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

SENAI - Serviço Nacional de Aprendizagem Industrial.

TIC - Tecnologia de Informações e Comunicação.

SENAC - Serviço Nacional de Aprendizagem Comercial.

EIT - Escolas Industriais e Técnicas.

CVE - *Common Vulnerabilities and Exposures.*

MITRE - *MITRE Corporation*.

KASPERSKY - Uma empresa russa de cibersegurança.

NIST - *National Institute of Standards and Technology.*

FIREWALLS - Dispositivos ou sistemas que monitoram e controlam o tráfego de rede

CRIPTOGRAFIA - O processo de codificação de informações para proteger dados de acesso.

TI - Tecnologia da Informação.

SUMÁRIO

1. INTRODUÇÃO

Este capítulo introduz o trabalho, contextualiza o tema e destaca a importância da segurança da informação. Em seguida, apresenta os objetivos geral e específicos, bem como as razões que sustentam o estudo. Por fim, descreve a estrutura da dissertação, com um resumo de cada capítulo, para facilitar a localização de tópicos específicos.

1.1. CONTEXTUALIZAÇÃO

A segurança cibernética atualmente se apresenta como um dos maiores desafios para governos, empresas e usuários individuais. Com a aceleração da transformação digital e a dependência de tecnologias conectadas expandiu consideravelmente a superfície de ataque para cibercriminosos, tornando a proteção de dados e a integridade dos sistemas uma prioridade estratégica em nível mundial.

Nos últimos anos, observou-se um aumento expressivo tanto na frequência quanto na complexidade dos ataques cibernéticos. Estratégias como *ransomware*, *phishing* e ataques de negação de serviço (*DDoS*) têm evoluído, muitas vezes contando com o uso de inteligência artificial para fraudar sistemas de defesa tradicionais. Segundo *Cybersecurity Ventures* (2022), os custos globais com cibercrime podem ultrapassar trilhões de dólares anualmente, evidenciando o impacto econômico desses ataques.

A crescente digitalização levanta questões importantes sobre privacidade e proteção de dados pessoais. As regulamentações sobre a proteção de dados buscam equilibrar a inovação tecnológica com a proteção dos direitos dos cidadãos. A evolução das políticas de privacidade e a implementação de *frameworks* legais robustos têm sido fundamentais para garantir que o avanço digital não ocorra em prejuízo a segurança e a privacidade dos usuários.

Com isso observa-se uma intensificação dos desafios relacionados à segurança cibernética, especialmente com a expansão da *Internet das Coisas (IoT)* e a implementação de redes 5G, que ampliam a conectividade global e, consequentemente, as possibilidades de ataque. A necessidade de desenvolver soluções que integrem tecnologia avançada, educação em cibersegurança e políticas públicas eficientes é crucial para manter um ambiente digital seguro e confiável.

Em resumo, pode-se concluir que o cenário atual exige cada vez mais uma abordagem multidisciplinar em segurança cibernética, que combine inovação tecnológica, estratégias de defesa robustas e uma colaboração efetiva entre diversos setores da sociedade. Essa integração de esforços é vital para enfrentar as ameaças cada vez mais sofisticadas e garantir a proteção de dados e a continuidade dos negócios em um mundo cada vez mais digitalizado.

1.2. CONTEXTUALIZAÇÃO DO PROBLEMA

A análise e correção de vulnerabilidades são componentes essenciais para a proteção de infraestruturas de TI contra-ataques cibernéticos e vem se mostrado uma necessidade crescente para organizações de todos os tamanhos e segmentos de mercado (Green & Thompson, 2019) no que se refere a cibersegurança.

Algumas ferramentas que auxiliam na análise e correção de vulnerabilidades da segurança computacional foram desenvolvidas, como exemplo tem-se o *CVE MITRE* (*Common Vulnerabilities and Exposures* mantido pela *MITRE Corporation*) que desempenha um papel importante no combate a ameaças à segurança computacional, fornecendo um banco de dados estruturado e padronizado de vulnerabilidades conhecidas. Essa base de dados facilita a detecção, redução e prevenção de ataques cibernéticos ao permitir que organizações e profissionais de segurança identifiquem e resolvam falhas em softwares e sistemas operacionais. (Parker, 2020).

Outra ferramenta muito usada no auxílio da segurança computacional é o *Wazuh* que consiste em uma plataforma de segurança cibernética de código aberto que unifica as funcionalidades de XDR (*Detecção e Resposta Estendidas*) e SIEM (Gerenciamento de Informações e Eventos de Segurança) para proteger *endpoints* e cargas de trabalho em nuvem. A plataforma *Wazuh* oferece a integração da cibersegurança, abrangendo gerenciamento de registros, detecção de intrusões, avaliação de vulnerabilidades e monitoramento de conformidade.

O uso dos *dashboards* também são de grande auxílio na segurança computacional. Estes, são ferramentas que ajudam a monitorar, analisar e compreender grandes volumes de dados de forma simplificada, permitindo a visualização em tempo real das ameaças, além de facilitar o processo de priorização e redução significativa dos riscos associados (Wells, 2021).

A eficiência operacional e a redução de custos impulsionam a integração dessas ferramentas, destacando-se em um campo onde o tempo de resposta é crucial (Martinez, 2018).

Com base no exposto acima, este trabalho tem por objetivo desenvolver um script que faça a integração do *CVE MITRE* com o *dashboard Wazuh* visando consolidar dados de vulnerabilidades e assim planejar as estratégias de resposta aos possíveis ataques de cibersegurança.

1.3. OBJETIVOS

1.3.1. Geral

Desenvolver um *script web* que faça a integração do *Dashboard* com os dados de vulnerabilidades e exposições comuns do *VCE MITRE* facilitando assim a exploração e análise do monitoramento das vulnerabilidades cibernéticas para otimizar o planejamento das respostas aos possíveis ataques cibernéticos.

1.3.2. Específicos

- Desenvolver o *script* de integração do *dashboard Wazuh* com *CVE MITRE*.
- Avaliar a eficácia da integração do *dashboard Wazuh* com o *CVE MITRE* na análise e correção de vulnerabilidades em sistemas e aplicações, a partir de estudos de casos em empresas e organizações.
- Analisar o resultado da implementação do sistema integrado do *dashboard Wazuh* baseado no *CVE MITRE* no processo de gestão de vulnerabilidades e na segurança cibernética de empresas e organizações.

1.4. ESTRUTURA DA DISSERTAÇÃO

Com finalidade de atender os objetivos desta pesquisa, e apresentar o caminho que será percorrido no decorrer desta dissertação, este trabalho é composto por sete capítulos e um anexo, mais as referências bibliográficas. Sendo estruturados da seguinte forma:

No Capítulo I, apresenta-se o tema do dashboard baseado no CVE MITRE, voltado para a análise e correção de vulnerabilidades. Discute-se o cenário atual de ameaças cibernéticas, destacando a importância da gestão de vulnerabilidades em sistemas de segurança da informação e a relevância do CVE MITRE como ferramenta para identificação e mitigação de vulnerabilidades.

No Capítulo II, detalha-se a metodologia empregada no desenvolvimento da dissertação, com ênfase na Revisão Sistemática da Literatura, que fundamenta o estudo.

O Capítulo III aborda os procedimentos e desenvolvimentos realizados, com foco na implementação e personalização da solução proposta.

O capítulo IV faz a conclusão e recomendações para estudos futuros, elementos essenciais em qualquer investigação científica.

Por fim, no anexo, são apresentadas as questões utilizadas na coleta de dados junto aos administradores de rede, contribuindo para o embasamento prático do trabalho.

2. REVISÃO DA LITERATURA

Nesse capítulo iremos discutir a revisão da literatura que abordará a metodologia, os resultados obtidos e a análise de trabalhos correlatos, destacando a relevância do tema para ambientes com dados públicos e sensíveis.

2.1. Descrição da Pesquisa

Este estudo é uma revisão bibliográfica sobre a implementação de um dashboard baseado no CVE MITRE para análise e correção de vulnerabilidades, alinhado à família ISO 27000 no que tange à gestão e às melhores práticas em segurança da informação. A pesquisa, realizada no período entre 2017 e 2022, utilizou bases como periódicos CAPES, IEEE, repositórios da UNESP, UFPA, Universidade de Lisboa, Universidade do Minho, UNB e Google Scholar, abrangendo artigos, periódicos, livros, teses e dissertações com resultados relevantes.

Foi utilizado também o repositório da Universidade de Brasília como fonte na pesquisa sobre o uso do *dashboard* com foco no *Wazuh*. O mapeamento sistemático, guiado por questões norteadoras, buscou compreender os desafios enfrentados por administradores de redes no monitoramento visual, identificação e análise de catálogos de vulnerabilidades em softwares e sistemas. As perguntas orientadoras foram as seguintes:

P1. Como a implementação de um *dashboard* baseado no CVE MITRE pode melhorar a eficiência na identificação e correção de vulnerabilidades em sistemas de TI?

P2. Quais são os principais desafios técnicos e organizacionais na implementação de um *dashboard* baseado no CVE MITRE em ambientes corporativos?

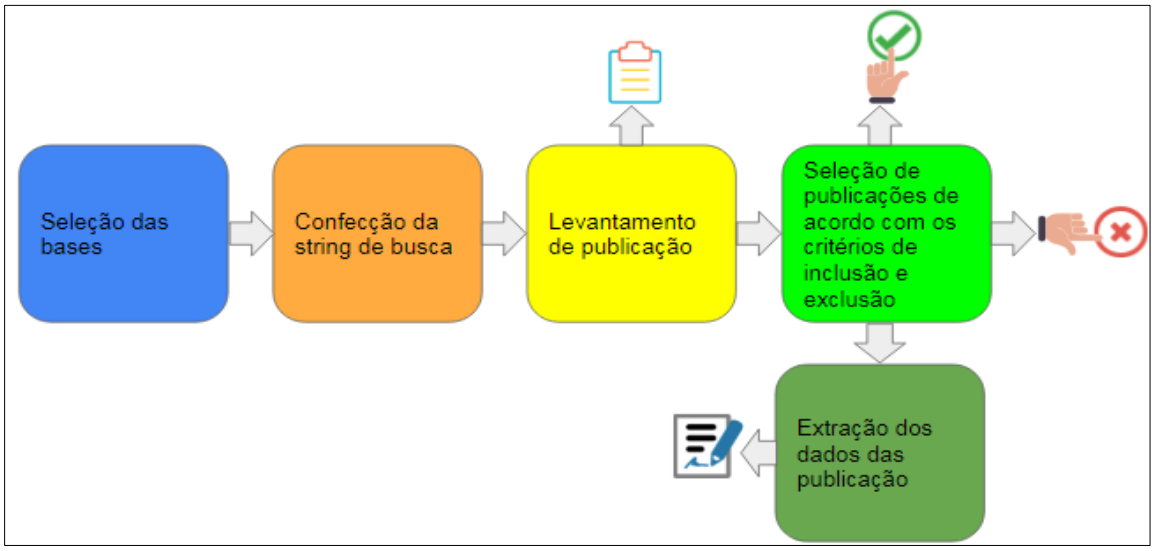
P3. Quais benefícios específicos um *dashboard* baseado no CVE MITRE oferece em comparação com as práticas tradicionais de gestão de vulnerabilidades?

Essas questões foram essenciais para direcionar a revisão de forma a compreender os desafios específicos e as barreiras no processo de aprendizado, contribuindo assim para a análise sistemática dos estudos encontrados.

Um mapeamento sistemático é uma ferramenta que proporciona uma visão abrangente dos estudos e publicações em uma área específica. Este modelo de pesquisa oferece ao pesquisador um esquema de classificação para identificar e

compreender as tendências e desenvolvimentos dentro do campo de estudo. De acordo com et al. (Kitchenham, 2009), "o mapeamento sistemático permite aos pesquisadores obter uma visão panorâmica do estado atual da pesquisa, facilitando a identificação de lacunas e oportunidades para novos estudos". A evolução na elaboração de mapeamentos sistemáticos é delineada nas etapas apresentadas na Figura 1, oferecendo diretrizes claras para a condução da pesquisa e seleção das obras relevantes.

Figura 1 - Etapas do Mapeamento Sistemático.



Fonte: O autor

Desta forma, é possível definir e seguir um parâmetro de seleção das obras. As palavras-chave utilizadas são compostas das seguintes: CVE MITRE, Dashboard, Análise de Vulnerabilidades, Correções, Segurança da Informação, Monitoramento em Tempo Real. Outro critério a considerar diz respeito aos artigos que precisam ter resultados concretizados. Segundo González *et al*. (2020), "a utilização de dashboards integrados com bases de dados como o CVE MITRE proporciona uma visão abrangente e em tempo real das vulnerabilidades, facilitando a análise e a priorização das correções". A Tabela 1, apresenta os critérios de inclusão e exclusão para seleção das bibliografias.

Tabela 1 - Critérios de Inclusão e Exclusão.

Critérios	Resultados
Os resultados devem ter ano de publicação a partir de 2017?	S
Os artigos devem ter *qualis*?	S
Os trabalhos encontrados devem ter estudos completos e resultados?	S
Os trabalhos devem estar disponíveis em meio eletrônico?	S
Os trabalhos devem estar escritos em inglês e português?	S
Incluir pesquisas com pouco relevância na pesquisa abordada?	N
Incluir pesquisas que possuam implementação prática?	S
Métodos justificado e rigor de análise de dados.	S
Resultado claros e discutido.	S
Artigos com conclusão não clara ou de difícil compreensão.	N
Artigos de periódicos sem uma representativa no meio acadêmicos.	N
Literatura cinza.	N
Artigos que fogem do escopo da pesquisa.	N

Fonte: Autor

A seleção rigorosa dos trabalhos para a revisão bibliográfica foi guiada por critérios que visam a especificidade e a relevância, como pode ser observado na Tabela 2, a seguir, alinhando-se diretamente à linha de pesquisa do projeto para evitar resultados irrelevantes. O foco principal da pesquisa concentrou-se em estudos que abordam infraestrutura, a implementação de *dashboards* baseados no *CVE MITRE* e a análise e correção de vulnerabilidades. Para a concretização da consulta em bases de dados acadêmicas, foram testadas várias *strings* de busca, e a mais eficaz, que proporcionou uma filtragem satisfatória dos resultados, foi a seguinte: ("*CVE MITRE*" *OR* "*CVE*") *AND* (*Dashboard OR* "painel de controle") *AND* ("Gestão de Vulnerabilidades" *OR* "Análise de Vulnerabilidades" *OR* "Correção de Vulnerabilidades" *OR* "Remediação"). Esta abordagem é reforçada pela literatura, pois, conforme Roberts *et al.* (2019), "a utilização de dashboards integrados com o CVE MITRE facilita a identificação e correção de vulnerabilidades, proporcionando uma abordagem mais proativa na gestão de segurança".

Tabela 2 - Questões de Classificação dos Trabalhos

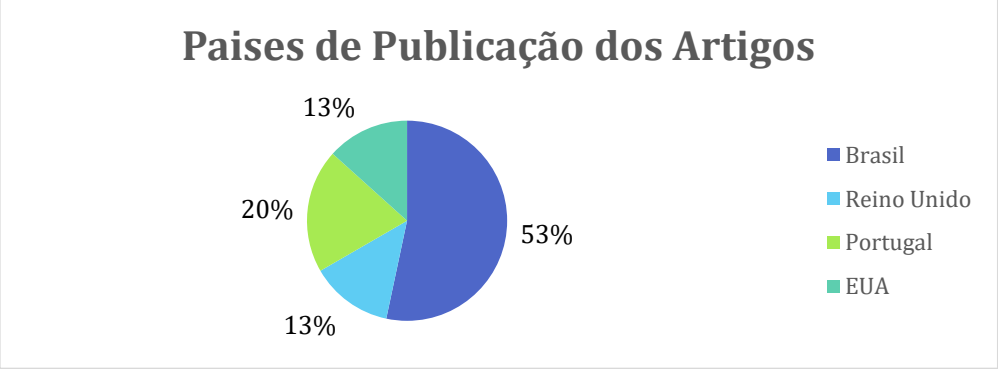
Critérios	Resultados
O estudo realizou implementação ou protótipo	S
O objetivo da pesquisa está claramente descrito	S
Os autores descrevem as limitações de estudo	S
O estudo demostra resultados sólidos para avaliar a solução	S
Existe simetria/equivalência com tópicos principais do meu projeto	S

Fonte: Autor

2.2. Resultado Literários

As consultas às bases de periódicos permitiram identificar publicações relacionadas ao tema. O Brasil se destaca em número de estudos, totalizando 8, seguido pelo Reino Unido, Portugal e EUA. O Figura 1, sintetiza os resultados obtidos a partir da *string* de busca definida.

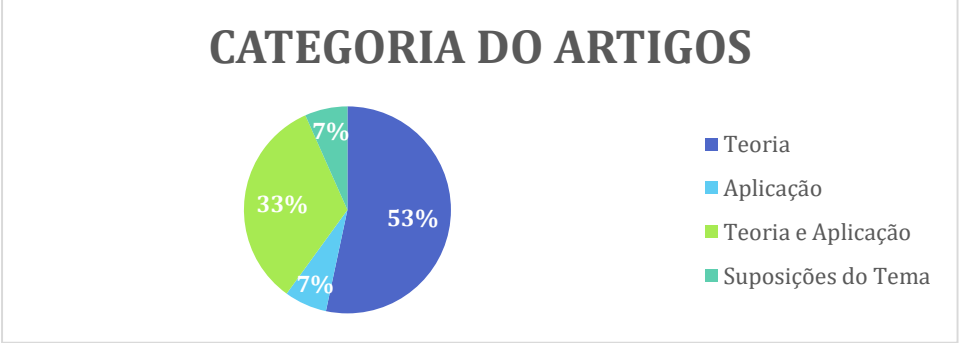
Figura 2 -Mostra o resultado do percentual, por países, que possuem publicações relacionadas ao tema.



Fonte: Autor

O Figura 2, mostra os resultados obtidos do total de 1.200 trabalhos achados utilizando as bases aqui citadas, foi possível identificar 35 que tiveram relação com o tema, 15 trabalhos estavam de acordo com os critérios de inclusão, desta forma foram selecionados para a pesquisa e abstração dos dados e 20 foram excluídos. Após a seleção dos artigos conforme os critérios de inclusão previamente definidos, foram seguidos, nessa ordem, os seguintes passos: leitura exploratória; leitura seletiva e escolha do material que se adequa aos objetivos e tema deste estudo; leitura analítica e análise dos textos.

Figura 3 - Resultados obtidos dos trabalhos utilizando as bases citadas que tiveram relação com o tema.

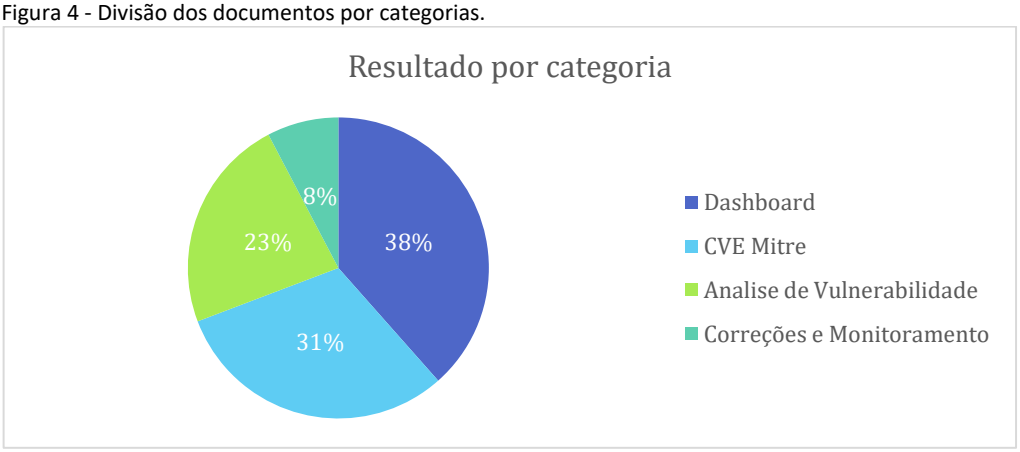


Fonte: Autor

Foram incluídos nesta consulta artigos que apresentassem descritores como: CVE MITRE, Dashboard, Análise de Vulnerabilidades, Correções, Segurança da

Informação, Monitoramento em Tempo Real. Para tanto, nas bases foram limitados idiomas de português e inglês, contudo, foi detectado que as publicações em português eram as que continham maiores informações relevantes ao estudo. Após estas etapas, constituiu-se um montante específico do estudo, definindo critérios de qualidade dos trabalhos selecionados, desta forma, agrupando os temas mais abordados onde todos precisam ser relacionados com a Implementação de Dashboards baseados no CVE MITRE, e agrupando nas seguintes categorias sendo: CVE MITRE, Dashboard, Análise de Vulnerabilidades, Correções e Monitoramento em Tempo Real. O Figura 4, a seguir, demonstra como ficaram separados os documentos selecionados na consulta por categoria.

Figura 4 - Divisão dos documentos por categorias.



Fonte: Autor

A partir das divisões por categorias, pode-se identificar como os trabalhos coletados foram organizados. Um alerta muito importante para a categoria de implementação de *dashboards* baseados no *CVE MITRE* para análise e correções de vulnerabilidades é a escassez de literatura acadêmica diretamente relacionada ao tema nas bases consultadas. No entanto, outras fontes, como documentação de desenvolvedores e publicações técnicas de empresas de segurança, fornecem materiais relevantes que podem ser utilizados.

Segundo Kavanagh *et al.* (2020), "a implementação de dashboards integrados com CVE MITRE permite uma gestão mais eficiente das vulnerabilidades, facilitando a priorização de correções e a redução do tempo de resposta" Além disso, estudos de Tan *et al*. (2019) apontam que "a utilização de *dashboards* para visualização de dados de segurança cibernética melhora significativamente a capacidade de análise e a tomada de decisões informadas".

A pesquisa refinada foi conduzida em várias plataformas, e a seleção cuidadosa dos termos teve como objetivo direcionar a busca para estudos específicos relacionados à implementação de *dashboards* baseados no *CVE MITRE* para análise e correções de vulnerabilidades. Apesar dos esforços, os resultados foram limitados, revelando apenas alguns trabalhos que atendiam aos critérios estabelecidos. Segundo Smith *et al.* (2017), "a utilização de dashboards integrados com CVE MITRE pode proporcionar uma visão mais clara e acionável das vulnerabilidades, melhorando a eficácia da resposta". Esta escassez de resultados destaca a necessidade de uma abordagem estratégica e abrangente na busca por literatura relevante.

A fase de extração dos dados sucedeu-se com uma leitura completa dos estudos selecionados como objetivo de sumarizar os seguintes itens num formulário:

- Palavras-chaves;
- Ano de publicação;
- Veículo da publicação;
- Autores;

Uma resposta parcial para a escassez de material acadêmico pode ser que o assunto ainda é relativamente novo e não amplamente difundido, pois trata-se de tecnologias avançadas que são principalmente adotadas por empresas privadas e cuja documentação raramente está disponível para consulta pública.

2.3. Análise dos Resultados

Ao analisar diversos artigos de pesquisa no Brasil e em Portugal, é possível traçar conexões significativas entre os tópicos abordados e os objetivos da implementação de um *dashboard* baseado no *CVE MITRE* para análise e correções de vulnerabilidades. Inicialmente, foi explorado a importância de uma gestão eficiente de vulnerabilidades, como evidenciado no trabalho de Souza e Silva (2018) intitulado "Gestão de Vulnerabilidades em Ambientes Corporativos: Um Estudo de Caso no Brasil". Este estudo destaca a necessidade de ferramentas eficazes para a identificação e mitigação de vulnerabilidades, evidenciando a relevância de *dashboards* integrados com o *CVE MITRE*.

Paralelamente, foram identificadas práticas de segurança cibernética em Portugal, conforme abordado em "Segurança da Informação: Práticas e Desafios nas Empresas Portuguesas" por Ferreira et al. (2019). Este artigo aponta para a adoção

crescente de tecnologias avançadas de monitoramento e análise de vulnerabilidades, ressaltando a importância de sistemas proativos na prevenção de ataques.

Esses *insights* são cruciais para compreender os desafios e as melhores práticas na implementação de *dashboards* de segurança. No contexto específico de *dashboards* baseados no *CVE MITRE*, a pesquisa de Lima *et al.* (2020) em "Utilização de *Dashboards* na Segurança da Informação: Um Estudo sobre a Eficiência na Resposta a Incidentes" destaca como a visualização de dados em tempo real pode melhorar a capacidade de resposta e a tomada de decisões.

A seguir, pode-se observar a Tabela 3, a qual mostra um quadro teórico preliminar, onde foi realizada a organização da bibliografia consultada, assim como os pontos das teorias pesquisadas nos trabalhos relacionados. Este quadro tem um papel fundamental, pois servirá de fonte para referenciar termos ou textos apresentados. Ainda na Tabela 3, ela oferece uma visão organizada das áreas de estudo, das bibliografias consultadas e dos pontos teóricos pesquisados, servindo como base para a implementação de um *dashboard* baseado no *CVE MITRE* para análise e correções de vulnerabilidades.

Tabela 3 - Quadro Teórico Preliminar.

Identificar as principais teorias da Linha de Pesquisa que atendam ao objetivo geral		
Áreas da Linha a serem estudadas (A)	Bibliografia Consultada (B)	Pontos da Teoria Pesquisados (C)
Gestão de Vulnerabilidades em Ambientes Corporativos	Souza, R., & Silva, M. (2018). Gestão de Vulnerabilidades em Ambientes Corporativos: Um Estudo de Caso no Brasil.	Necessidade de ferramentas eficazes para identificação e mitigação de vulnerabilidades.
Práticas de Segurança Cibernética em Empresas Portuguesas	Ferreira, P., Santos, A., & Almeida, R. (2019). Segurança da Informação: Práticas e Desafios nas Empresas Portuguesas.	Adoção de tecnologias avançadas de monitoramento e análise de vulnerabilidades.
Eficiência de Dashboards na Resposta a Incidentes de Segurança da Informação	Lima, T., Marques, L., & Oliveira, D. (2020). Utilização de Dashboards na Segurança da Informação: Um Estudo sobre a Eficiência na Resposta a Incidentes.	Melhoria da capacidade de resposta e tomada de decisões com visualização de dados em tempo real.
Visualização de Dados de Segurança Cibernética	Johnson, R., & White, P. (2016). Cybersecurity Data Visualization: A Guide to Implementing Dashboards.	Implementação de dashboards para visualização de dados de segurança cibernética.
Integração de Dados CVE nas Operações de Segurança	Lee, A., & Thompson, B. (2018). Integrating CVE Data into Security Operations.	Integração de dados do CVE para melhorar operações de segurança e gestão de vulnerabilidades.
Gestão Proativa de Segurança com Dashboards em Tempo Real	Miller, K., & Davis, S. (2019). Proactive Security Management with Real-time Dashboards.	Gestão proativa de segurança utilizando dashboards em tempo real para monitoramento e resposta rápida a incidentes.

Fonte: Autor

3. FUNDAMENTAÇÃO TEÓRICA

Neste terceiro capítulo, serão explorados os principais conceitos, teorias e estudos relacionados ao tema da pesquisa, tais como: a implementação de *dashboards* personalizados utilizando o *Wazuh* e o uso do *CVE MITRE* para análise e correções de vulnerabilidades.

3.1. SEGURANÇA DA INFORMAÇÃO

Em algumas literaturas, a segurança é classificada como uma ação de restrição, repressão ou até mesmo punição. No entanto, uma definição mais adequada é entendê-la como um conjunto de medidas para mitigar riscos de ocorrências futuras. Assim, a segurança não deve ser vista sob uma perspectiva negativa, mas sim como um elemento essencial para minimizar os riscos inerentes aos objetos aos quais é aplicada (NETO; ARAUJO, 2019).

Do ponto de vista tecnológico, a segurança da informação é um componente fundamental do uso de dispositivos informáticos e redes de computadores, protegendo contra ameaças à confidencialidade, integridade e disponibilidade dos dados. Além disso, abrange a proteção de informações armazenadas em ativos digitais, como servidores, bancos de dados e redes de processamento (FONTES, 2008).

No entanto, a segurança da informação não se limita ao cenário tecnológico. Ela envolve também pessoas, processos, normas, comportamentos e mecanismos físicos. A proteção da informação vai além do uso de antivírus e firewalls, abrangendo práticas como gestão de senhas, controle de acessos, monitoramento por câmeras e outras medidas organizacionais. Uma abordagem restrita apenas ao aspecto tecnológico pode resultar em soluções ineficazes, levando ao desperdício de recursos sem resolver a raiz dos problemas de segurança.

3.1.1. Pilares da Segurança da Informação

A segurança da informação é definida por um conjunto de pilares fundamentais, os quais devem ser aplicados em políticas de segurança, desenvolvimento de software e configuração de redes. Não existe um pilar mais importante que outro; todos se interrelacionam e são essenciais para garantir a proteção da informação.

Empresas que adotam padrões de segurança, sejam normas reconhecidas no mercado ou diretrizes próprias, devem realizar auditorias para verificar a conformidade de seu ambiente. Caso sejam identificadas não conformidades, estas devem ser corrigidas para evitar riscos (FONTES, 2008).

Os principais pilares da segurança da informação incluem:

3.1.1.1. Confidencialidade

Garante que as informações sejam acessíveis apenas a pessoas autorizadas. Exemplos incluem o uso de senhas e criptografia para proteger dados sensíveis. No âmbito empresarial, a exposição de segredos industriais pode resultar em prejuízos financeiros e perda de vantagem competitiva (WEIDMAN, 2014).

3.1.1.2. Disponibilidade

Assegura que a informação esteja acessível sempre que necessária. Medidas como redundância de servidores e *backups* são fundamentais para evitar perdas de dados e manter a continuidade dos serviços (REGALADO *et al.*, 2022).

3.1.1.3. Integridade

Garante que a informação não seja alterada indevidamente, seja por erro ou ataque malicioso. Um exemplo de mecanismo de proteção é o uso de funções de *hashing* para validar a autenticidade dos dados (NETO; ARAUJO, 2019).

3.1.1.4. Autenticidade

Confirma a identidade do remetente da informação, evitando fraudes e ataques de *phishing*. Certificados digitais e assinaturas eletrônicas são exemplos de mecanismos usados para garantir autenticidade (NETO; ARAUJO, 2019).

3.1.1.5. Irretratabilidade

Impede que uma entidade negue a autoria de uma ação realizada. No âmbito da computação forense, registros de logs e câmeras de segurança podem ser utilizados como evidências para comprovar eventos ocorridos (STARTI, 2023).

3.2. ATIVOS DA INFORMAÇÃO

Os ativos são elementos de valor para uma organização, podendo ser classificados como ativos primários (processos de negócio) e ativos de suporte (infraestrutura tecnológica, pessoas e processos organizacionais). A norma ABNT NBR ISO/IEC 27005:2011 classifica os ativos dessa forma, destacando a importância de realizar um inventário de ativos para garantir um melhor gerenciamento e estratégias de segurança eficazes (NETO; ARAUJO, 2019).

3.3. AMEAÇAS E VULNERABILIDADES

3.3.1. Ameaças

Ameaças são eventos indesejáveis que exploram vulnerabilidades, comprometendo a segurança da informação. A norma ISO/NBR 27005:2011 classifica ameaças em três categorias:

- **Naturais:** Terremotos, enchentes, tempestades.
- **Involuntárias:** Erros humanos ou falhas acidentais.
- **Voluntárias:** Ações maliciosas de criminosos, como ataques cibernéticos (BIDOU, 2005).

3.3.2. Vulnerabilidades

Uma vulnerabilidade é uma fraqueza em um sistema que pode ser explorada por ameaças. Embora nenhuma tecnologia seja 100% segura, vulnerabilidades devem ser monitoradas e mitigadas por meio de testes de intrusão e auditorias (NETO; ARAUJO, 2019).

A segurança da informação deve ser abordada de forma abrangente, considerando tanto os aspectos tecnológicos quanto organizacionais. Empresas que adotam uma estratégia proativa de segurança tendem a reduzir riscos e aumentar a resiliência contra ameaças digitais.

3.4. GESTÃO DE VULNERABILIDADES

A gestão de vulnerabilidades é um processo essencial para monitorar novas ameaças e definir um plano de ação para resolvê-las de forma rápida e eficiente. Esse processo envolve identificar, classificar, priorizar, resolver e reavaliar o risco de uma determinada vulnerabilidade, resultando na correção da falha encontrada e na

mitigação do risco associado. Para isso, utilizam-se sistemas de gestão de vulnerabilidades e scanners específicos, prevenindo ataques cibernéticos e protegendo redes empresariais contra o roubo de informações.

Para que esse processo seja eficaz, é necessário estabelecer um conjunto de ações sequenciais, incluindo a definição dos ativos a serem protegidos e sua criticidade com base no impacto organizacional. Cada ativo deve ter sua funcionalidade documentada, incluindo portas abertas, processos e serviços críticos. Além disso, devem ser implementadas estratégias de mitigação baseadas no risco associado a cada ativo, gerando relatórios atualizados sempre que novas vulnerabilidades forem descobertas ou resolvidas (FONTES, 2023).

3.5. AVALIAÇÃO DE VULNERABILIDADES

A avaliação de vulnerabilidades permite identificar, classificar e priorizar os diferentes ativos da organização. Esse processo normalmente ocorre em três fases, como pode ser visto a seguir:

3.5.1. Verificação Inicial

A primeira etapa da gestão de vulnerabilidades consiste na definição dos ativos a serem protegidos e sua importância para a organização. Deve-se avaliar o impacto da perda ou comprometimento de cada ativo, estabelecendo práticas para mitigar os riscos identificados. Também é essencial definir quem tem acesso a cada ativo e quais permissões são necessárias (NETO; ARAÚJO, 2023).

3.5.2. *Scanning* de Vulnerabilidades

Nesta fase, utilizam-se ferramentas automatizadas para identificar potenciais vulnerabilidades com base nos ativos mapeados e nos riscos identificados na fase inicial. Esse processo pode ser configurado e agendado conforme os requisitos da equipe de segurança, levando em conta a criticidade dos ativos e a frequência de atualizações de software (WEIDMAN, 2023).

3.5.3. Geração de Relatórios

O relatório final consolida todas as vulnerabilidades encontradas, listando os sistemas afetados, datas, descrições detalhadas, risco baseado em CVE,

responsáveis pela mitigação e, se possível, provas de conceito que demonstrem a correção ou medidas compensatórias adotadas (REGALADO *et al.*, 2023).

3.6. SCANNERS DE VULNERABILIDADES

Os scanners de vulnerabilidades desempenham um papel fundamental na detecção de falhas de segurança. Suas principais funções incluem:

- Identificação de ativos na rede;
- Detecção de serviços e portas abertas;
- Coleta de informações sobre os sistemas e tentativas de autenticação;
- Busca por vulnerabilidades conhecidas com base nas informações coletadas.

3.7. SISTEMAS DE GESTÃO DE VULNERABILIDADES

Os sistemas de Gestão de Vulnerabilidades (VMS) são ferramentas projetadas para identificar falhas, gerenciar atualizações e corrigir configurações inseguras em sistemas operacionais, aplicativos e outros ativos digitais. Um VMS eficiente deve:

- Cobrir um amplo espectro de ambientes e ativos;
- Fornecer suporte técnico especializado;
- Reportar vulnerabilidades do tipo "Zero-*Day*" com rapidez;
- Gerar relatórios detalhados e personalizáveis;
- Minimizar falsos positivos

3.7.1. *Snyk*

O *Snyk*, lançado em 2015, auxilia no desenvolvimento seguro de software ao identificar e corrigir vulnerabilidades em dependências de código-fonte. A ferramenta se integra a plataformas como *GitHub* e *Bitbucket*, gerando relatórios detalhados e oferecendo suporte especializado. O *Snyk* opera via linha de comando ou como parte de *pipelines* de CI/CD, facilitando a segurança no desenvolvimento de aplicações (FONTES, 2023).

3.7.2. Saucs

A *Saucs* monitora vulnerabilidades e alerta usuários com base em filtros personalizáveis, utilizando padrões como CWE, CPE, CVSS e CVE. Apesar de cobrir um amplo espectro de sistemas e aplicações, pode gerar falsos positivos devido à

falta de detalhamento sobre versões específicas. Além disso, sua base de dados pode não estar sempre atualizada, o que representa um risco para organizações dependentes dessa ferramenta (SCOTA, 2023).

3.7.3. NucleusSec

O *Nucleus* é uma solução de gestão de vulnerabilidades que integra mais de 50 *scanners*, como *Nessus*, *Qualys* e *OWASP Dependency Checker*. Ele permite priorizar vulnerabilidades com base no risco, automatizar correções e gerar alertas personalizados. Seu diferencial está na rapidez de resposta, sendo até 10 vezes mais eficiente que sistemas tradicionais (REGALADO *et al.*, 2023).

3.7.4. Tenable

A *Tenable*, fundada em 2002, desenvolveu o *Nessus*, um dos *scanners* de vulnerabilidades mais amplamente utilizados. O *Nessus* realiza varreduras em tempo real e oferece diferentes métodos de varredura, incluindo agentes locais que reportam dados ao *Nessus Manager*, agilizando o processo de identificação e diminuição de falhas (WEIDMAN, 2023).

3.7.5. CVE - Common Vulnerabilities and Exposures

O *CVE (Common Vulnerabilities and Exposures)* é uma base de dados que compila vulnerabilidades organizadas por fabricante, produto e versão. Ele agrega informações da NVD (*National Vulnerability Database), exploits* conhecidos e módulos do *Metasploit*. No entanto, não oferece um sistema automatizado de gestão de vulnerabilidades ou alertas personalizados, sendo uma ferramenta de consulta complementar (STARTI, 2023).

3.7.5.1. CVE MITRE

O *Common Vulnerabilities and Exposures* (CVE) *MITRE* é um sistema que fornece identificadores padronizados para vulnerabilidades e exposições de segurança cibernética conhecidas publicamente desenvolvido pela organização sem fins lucrativos MITRE Corporation em 1999 (cve.mitre.org). O *CVE MITRE* visa facilitar a troca de informações entre diferentes ferramentas e bancos de dados de segurança, além de simplificar a identificação e correção de novas falhas.

Cada entrada no *CVE MITRE* é identificada por um número único, composto pelo prefixo "CVE", o ano de divulgação e um número sequencial, por exemplo, CVE-2025-12345. Esses identificadores são atribuídos por Autoridades de Numeração CVE (CVE *Numbering Authorities*, ou CNA), que podem ser fornecedores de software, pesquisadores, organizações de código aberto, entre outros.

Atualmente, existem 436 CNA em 40 países, responsáveis por atribuir ID CVE e publicar registros detalhados sobre as vulnerabilidades em suas áreas de atuação (cve.org).

As entradas do *CVE MITRE* incluem uma descrição concisa da vulnerabilidade, que é posteriormente detalhada no Banco de Dados Nacional de Vulnerabilidades (*National Vulnerability Database*, ou NVD). Essas informações são utilizadas em bancos de dados, ferramentas de gerenciamento de vulnerabilidades e *firewalls* para identificar e diminuir possíveis ameaças à segurança (cve.mitre.org).

Para relatar uma nova vulnerabilidade, é necessário entrar em contato com o CNA responsável pelo produto ou sistema afetado. Caso não haja um CNA designado para o produto em questão, o relatório pode ser enviado diretamente à MITRE. O processo envolve o preenchimento de um formulário com detalhes sobre a vulnerabilidade, visando a obtenção de um novo ID CVE. Após a verificação, o CNA ou a MITRE documenta as versões do software afetadas, atribui uma pontuação baseada na *Common Vulnerability Scoring System* (CVSS) e apresenta a solução recomendada (cve.org).

O *CVE MITRE* é fundamental para a padronização e comunicação de vulnerabilidades de segurança, permitindo que organizações e profissionais de TI colaborem de forma eficaz na identificação e diminuição de riscos à segurança da informação.

3.8. SOLUÇÕES DE SEGURANÇA CIBERNÉTICA

As soluções de segurança cibernética consistem em produtos e serviços concebidos para proteger sistemas e dados digitais contra ameaças e ataques no ambiente virtual. Esse conjunto abrange, entre outros, firewalls; mecanismos de mitigação de ataques de negação de serviço distribuído (DDoS); microssegmentação; proteção contra comprometimento de contas; segurança de interfaces de programação de aplicações (APIs); gerenciamento de *bots*; e segurança de aplicações web.

No processo de concepção da infraestrutura de segurança de uma organização, observa-se ampla variedade de tecnologias e abordagens disponíveis. A profusão de terminologias e siglas, contudo, pode dificultar a diferenciação entre as ofertas e a identificação da alternativa mais aderente aos requisitos técnico-operacionais e regulatórios. Entre as soluções comumente confundidas destacam-se a Detecção e Resposta Estendida (XDR) e o Gerenciamento de Informações e Eventos de Segurança (SIEM). Embora compartilhem alguns recursos, como a coleta de telemetria e o suporte à detecção de incidentes, possuem finalidades distintas e operam de maneiras diferentes: o SIEM concentra-se na agregação, normalização e correlação de eventos provenientes de múltiplas fontes para monitoramento, investigação e conformidade; a XDR integra telemetrias de diferentes domínios (*endpoint*, rede, e-mail, identidade, entre outros) e aplica análises avançadas para detecção, contenção e resposta, de forma assistida ou automatizada.

A escolha adequada e complementar dessas soluções é essencial para a construção de uma arquitetura de segurança utilizável e sustentável, capaz de sustentar as atividades do Centro de Operações de Segurança (SOC) e de fortalecer a postura de segurança organizacional.

3.8.1. EDR - Endpoint Detection and Response

A sigla EDR (*Endpoint Detection and Response*) Detecção e Resposta em *Endpoint*, refere-se a uma tecnologia focada no monitoramento contínuo e na resposta a ameaças em dispositivos finais, conhecidos como *endpoints*. Esses *endpoints* incluem tais como computadores, servidores, dispositivos móveis e qualquer outro dispositivo conectado a uma rede.

As soluções EDR desempenham as seguintes funções:

i. **Monitoramento contínuo:** o EDR captura dados detalhados sobre processos, arquivos, atividades de rede e ações dos usuários nos *endpoints* em tempo real. Esse monitoramento contínuo é essencial para identificar rapidamente qualquer atividade anômala ou maliciosa.

ii. **Detecção de ameaças:** utiliza análise comportamental e técnicas avançadas de *machine learning* para detectar atividades suspeitas que possam indicar uma ameaça, como

movimentações laterais, tentativas de escalonamento de privilégios e execuções de *malware*.

iii. **Resposta automática:** permite a implementação de ações automáticas para conter e remediar ameaças. Exemplos incluem a quarentena de arquivos maliciosos, a terminação de processos suspeitos e o isolamento de dispositivos infectados da rede.

iv. **Investigação forense:** fornece ferramentas robustas para analisar a cadeia de eventos que levou a um incidente de segurança. Isso inclui a capacidade de examinar *logs* de atividades, rastrear movimentos de um atacante e identificar a origem da ameaça.

3.8.2. XDR - Extended Detection and Response

A sigla *XDR* (*Extended Detection and Response*) Detecção e Resposta Expandida, integra e correlaciona dados de múltiplas fontes de segurança para proporcionar uma visão ampla e unificada das ameaças em toda a infraestrutura de TI. Diferente do EDR, que foca exclusivamente nos *endpoints*, o XDR expande a detecção e a resposta para incluir redes, servidores, e-mails, cargas de trabalho em nuvem e outros componentes do ambiente de TI.

As soluções XDR desempenham as seguintes funções:

i. **Visibilidade multicamadas:** o XDR agrega e correlaciona dados de segurança de diversas fontes e camadas, incluindo *endpoints*, redes, servidores, e-mails e ambientes de nuvem. Isso proporciona uma visão integrada das atividades e eventos de segurança.

ii. **Resposta coordenada:** orquestra uma resposta a incidentes que abrange toda a infraestrutura, incluindo a contenção e remediação de ameaças em *endpoints*, rede e outros componentes. Isso garante uma resposta rápida e eficaz a incidentes de segurança.

iii. **Análise e correlação de eventos:** integra dados de segurança de diversas fontes para correlacionar eventos e identificar padrões de ataques que poderiam passar despercebidos se analisados isoladamente.

iv. **Centralização de dados de segurança:** fornece uma plataforma unificada onde todos os dados de segurança são centralizados, facilitando a análise e a gestão de segurança.

3.8.3. SIEM - Security Information and Event Management

A sigla *SIEM (Security Information and Event Management)* Gerenciamento de Informações e Eventos de Segurança, refere-se a um sistema de segurança cibernética que centraliza a coleta, análise e armazenamento de *logs* de segurança e eventos de diversas fontes dentro da rede de uma organização. O SIEM combina funções de gerenciamento de informações de segurança e gerenciamento de eventos de segurança para proporcionar uma visão holística da segurança, facilitando a detecção de incidentes, a análise de causa raiz e a conformidade regulatória.

As soluções SIEM desempenham as seguintes funções:

i. **Coleta de *logs*:** agrega *logs* e eventos de várias fontes, como *firewalls*, sistemas de detecção de intrusões, servidores, aplicações, bancos de dados e dispositivos de rede. Isso inclui a captura de *logs* em tempo real e a importação de *logs* históricos.

ii. **Correlação de eventos:** analisa os dados coletados para identificar padrões e correlações que possam indicar um incidente de segurança. Isso inclui a detecção de comportamentos anômalos e a identificação de ameaças complexas que poderiam passar despercebidas em um monitoramento isolado.

iii. **Análise forense e investigação:** facilita a investigação de incidentes de segurança, permitindo a análise detalhada dos *logs* e eventos para entender a cadeia de eventos, identificar a causa raiz e determinar o impacto de um incidente.

iv. **Relatórios de conformidade:** gera relatórios detalhados para atender às exigências regulatórias e auditorias de segurança. Isso inclui a criação de relatórios personalizados para diferentes normas e regulamentações, como GDPR, PCI-DSS, HIPAA, entre outras.

v. ***Dashboards* e visualização de dados:** fornece *dashboards* e ferramentas de visualização de dados em tempo real, permitindo uma compreensão rápida e intuitiva do estado de segurança da organização e das tendências de incidentes.

3.9. *WAZUH*: UMA PLATAFORMA DE SEGURANÇA *OPEN SOURCE* PARA XDR E SIEM

A segurança da informação é um dos principais desafios enfrentados por organizações de diferentes portes e setores. Nesse contexto, soluções de monitoramento e resposta a ameaças desempenham um papel essencial na proteção de ativos digitais. O *Wazuh* é uma plataforma de segurança gratuita e de código aberto que integra funcionalidades de XDR e SIEM, oferecendo um ambiente unificado para a detecção e mitigação de ameaças (Wazuh, 2024).

A plataforma é projetada para monitorar e proteger cargas de trabalho em diversos ambientes, incluindo infraestruturas locais, virtualizadas, baseadas em contêineres e em nuvem. Por meio da coleta, análise e correlação de eventos de segurança, o *Wazuh* auxilia organizações na detecção precoce de ataques cibernéticos, conformidade com normativas regulatórias e resposta a incidentes de segurança (Santos et al., 2023).

O uso do *Wazuh* tem crescido, sendo utilizado por muitas organizações, desde pequenas empresas até grandes corporações. Seu grande uso pode ser atribuído à flexibilidade, escalabilidade e ao suporte da comunidade *open source*, fatores que tornam a plataforma uma alternativa viável a soluções comerciais proprietárias (Garcia & Mendes, 2022).

3.9.1. Arquitetura e Componentes da Plataforma *Wazuh*

A arquitetura *Wazuh* é baseada em um modelo distribuído, composto por três componentes principais: o *Wazuh server*, o *Wazuh indexer* e o *Wazuh dashboard*, além do *Wazuh agents*, que é implantado nos *endpoints* monitorados (Wazuh, 2024).

1. ***Wazuh indexer*:** o *Wazuh indexer* é um mecanismo escalável de pesquisa e análise de texto completo. Ele armazena e indexa os alertas gerados pelo servidor, permitindo consultas eficientes e correlação de eventos de segurança. Essa estrutura é fundamental para viabilizar análises avançadas e geração de relatórios detalhados sobre incidentes detectados (Wazuh, 2024).

2. ***Wazuh server:*** o *Wazuh server* processa os dados coletados pelos agentes por meio de decodificadores e regras personalizáveis. Ele utiliza inteligência de ameaças para identificar indicadores conhecidos de comprometimento (*Indicators of Compromise – IOCs*). Além disso, o servidor é responsável pela gestão dos agentes,

permitindo sua configuração e atualização remota. Um único servidor pode analisar informações provenientes de centenas ou milhares de agentes, podendo escalar horizontalmente quando configurado como um cluster distribuído (Garcia & Mendes, 2022).

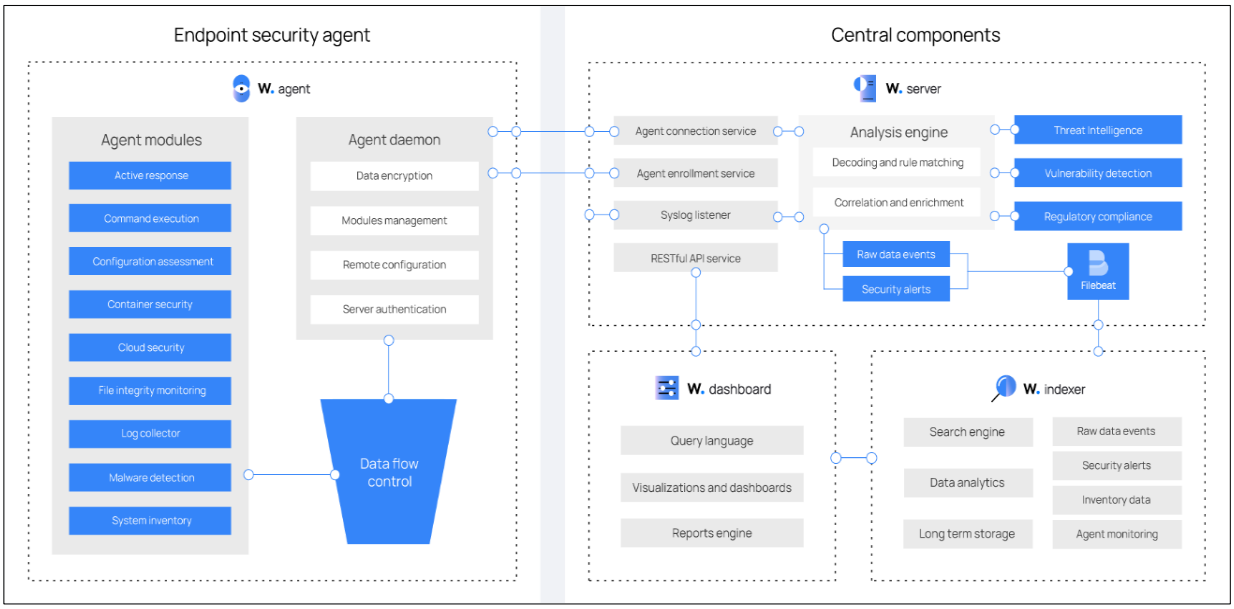
3. ***Wazuh dashboard:*** *o Wazuh dashboard* fornece uma *interface web* interativa para a visualização e análise dos dados processados pelo servidor. Ele inclui *dashboard* prontos para uso voltados para: busca de ameaças, conformidade regulatória (ex.: PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detecção de vulnerabilidades em aplicações, monitoramento da integridade de arquivos e eventos de segurança em infraestrutura de nuvem. Além da visualização de alertas, o *dashboard* também permite monitorar o status da plataforma e configurar seus componentes, facilitando a administração centralizada (Oliveira et al., 2021).

4. ***Wazuh agents***: os *Wazuh agents* são responsáveis pela coleta e envio de dados de segurança para o servidor *Wazuh*. Eles podem ser instalados em diferentes tipos de *endpoints*, incluindo *laptops*, *desktops*, servidores físicos e virtuais, além de instâncias em nuvem. Os agentes fornecem funcionalidades de prevenção, detecção e resposta a ameaças, operando em sistemas como Linux, Windows, macOS, Solaris, AIX e HP-UX (Santos et al., 2023).

Além do monitoramento baseado em agentes, o *Wazuh* suporta a supervisão de dispositivos sem agentes, como *firewalls*, *switches*, roteadores e sistemas de detecção de intrusão (IDS). Para isso, ele pode coletar *logs* via *Syslog*, realizando sondagens periódicas por meio de SSH ou consumir informações de segurança a partir de APIs específicas (Moraes & Lima, 2020).

A arquitetura distribuída do *Wazuh* permite uma abordagem escalável e eficiente para a detecção e resposta a ameaças cibernéticas, tornando-se uma solução amplamente adotada em diferentes setores. A Figura 5 mostra o diagrama que representa os componentes da arquitetura *Wazuh* e o fluxo de dados.

Figura 5 - Componentes da arquitetura Wazuh.



Fonte: Wazuh, 2024.

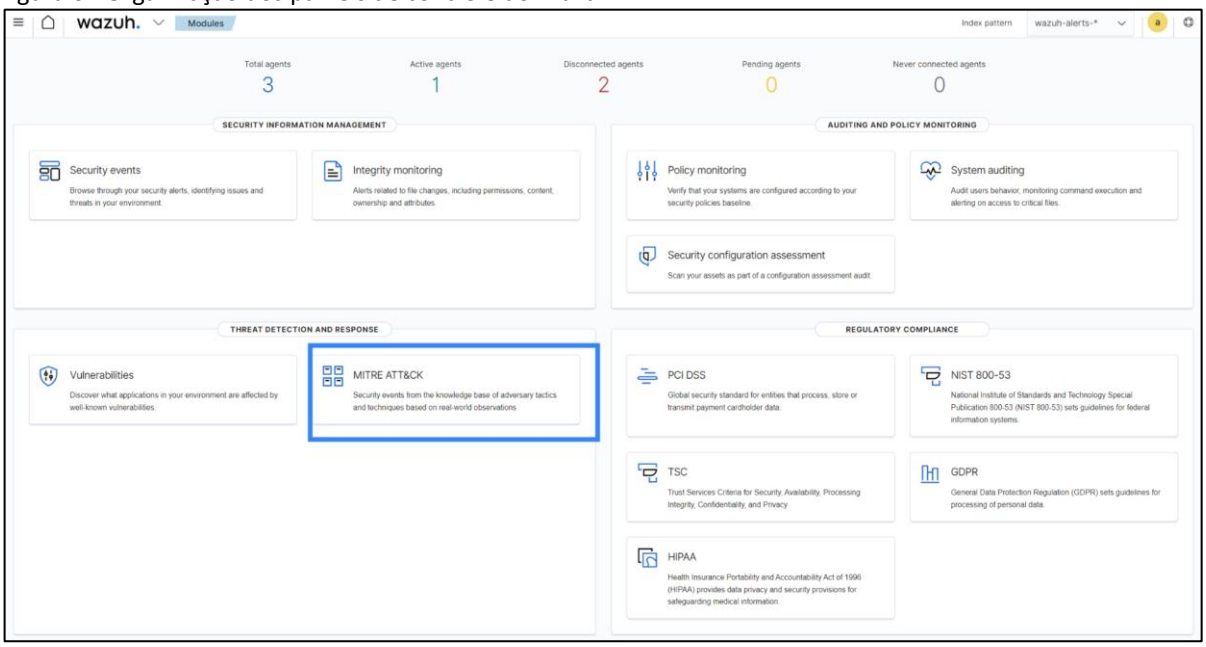
3.9.2. Painel de Controle

Os painéis do *Wazuh* oferecem visão centralizada do status de segurança, facilitando o gerenciamento, auditoria, detecção de ameaças e monitoramento de conformidade. Métricas como agentes totais, ativos, desconectados e pendentes dão panorama rápido da infraestrutura. O layout intuitivo e a divisão por painéis permitem navegação fácil entre as funções.

A Figura 6, a seguir, monstra a organização dos painéis de controle do *Wazuh*, que exibe painéis dedicados a diversas áreas. Na parte superior da Figura 3, pode-se observar o "*Security Information Management*", que inclui "*Security events*" e "*Integrity monitoring*", e o "*Auditing and Policy Monitoring*", que abrange "*Policy monitoring*", "*Security configuration assessment*" e "*System auditing*". Na parte inferior da Figura 3, há o painel de "*Regulatory Compliance*", que lista padrões como: PCI DSS, HIPAA, GDPR, e o "*Threat Detection and Response*".

Dentro do painel de "*Threat Detection and Response*", o módulo "*MITRE ATT&CK*" é destacado, mostrando a capacidade do *Wazuh* de correlacionar eventos de segurança com as táticas e técnicas da base de conhecimento *MITRE ATT&CK*. Essa funcionalidade é de grande importância para entender o comportamento de ameaças e aprimorar as estratégias de detecção e resposta. Ao analisar e correlacionar dados com esse *framework*, o *Wazuh* permite que as equipes de segurança identifiquem e respondam a ameaças de forma mais eficaz e estratégica.

Figura 6 - Organização dos painéis de controle do Wazuh.



Fonte: Wazuh, 2024.

3.9.3. Painéis do Módulo MITRE ATT&CK do Wazuh

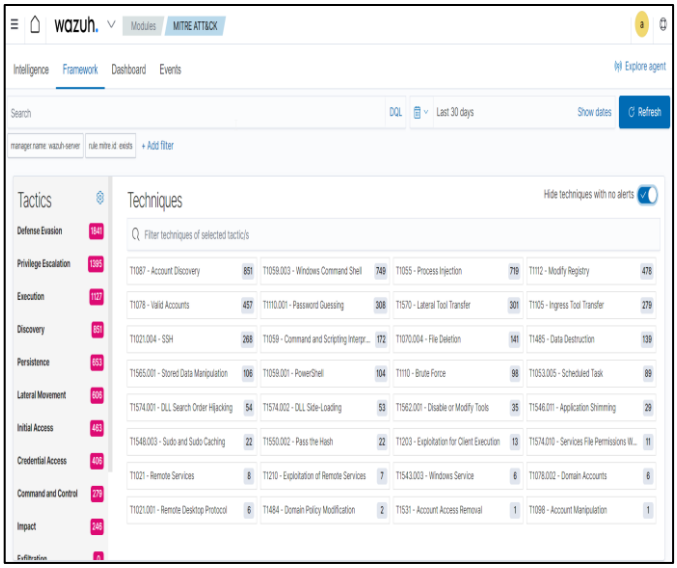
A Figura 7 ilustra mais detalhadamente o painel de visualização e a Figura 8, mostra o painel de análise do módulo *MITRE ATT&CK* do *Wazuh*. Observando as Figuras 4 e 5, observa-se que o sistema *Wazuh* oferece uma interface detalhada para que os analistas de segurança possam investigar eventos e ameaças de acordo com o *framework* MITRE ATT&CK.

Na Figura 4 é possível observar a tela de "*Overview*", organizada por "*Tatics*" e "*Techniques*". A coluna "*Tatics*" lista as táticas do *framework*, tais como: "*Defense Evasion*", "*Execution*" e "*Privilege Escalation*", com o número de eventos detectados associados a cada uma delas. A coluna "*Techniques*" detalha as técnicas específicas, identificadas por códigos *T-ID*, *T1001*, *T1059* e *T1033*, mostrando a quantidade de ocorrências de cada técnica. Essa visualização permite que os usuários compreendam quais táticas e técnicas de ataque estão sendo mais empregadas em seu ambiente, facilitando a priorização de investigações e a implementação de contramedidas.

Na Figura 9 é possível observar um *dashboard* de visualização de dados, com gráficos e representações visuais. Gráficos de linha, barras e pizza apresentam a

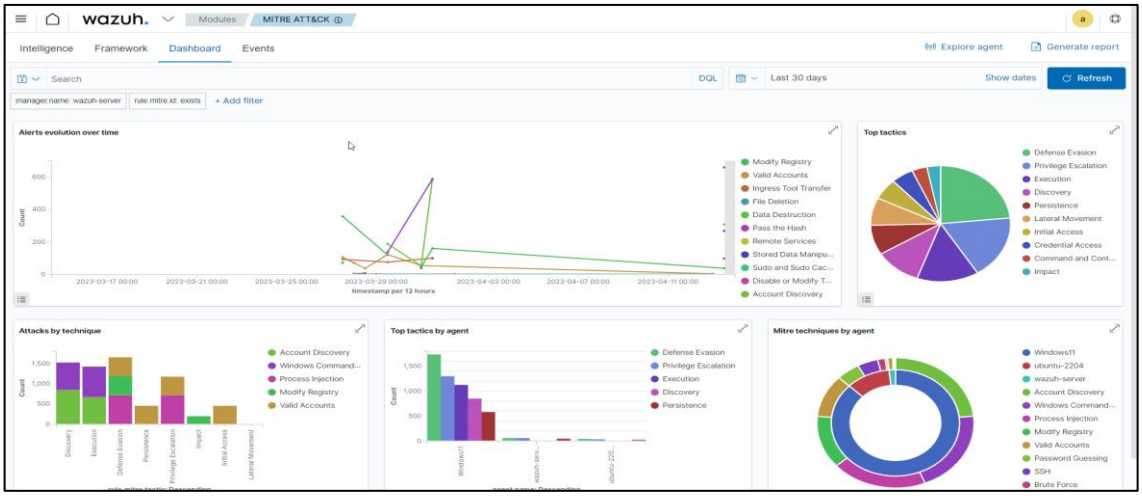
evolução temporal das ameaças, a distribuição das técnicas mais usadas, e o impacto em diferentes áreas. Essa abordagem visual é crucial para identificar tendências e anomalias de forma rápida. O *dashboard* resume a atividade de ameaças, ajudando a entender a dinâmica dos ataques e a eficácia das defesas. Juntos, esses painéis demonstram a robusta capacidade do *Wazuh* de detectar eventos de segurança e principalmente contextualizá-los com o *framework MITRE ATT&CK*, fornecendo uma análise mais completa e de fácil visualização.

Figura 7 - Painel de visualização do Módulo MITRE ATT&CK.



Fonte: Wazuh, 2024.

Figura 8 - Painel de análise do módulo MITRE ATT&CK do Wazuh.



Fonte: Wazuh, 2024.

3.9.4. Painel de Eventos do Módulo MITRE ATT&CK no *Wazuh*

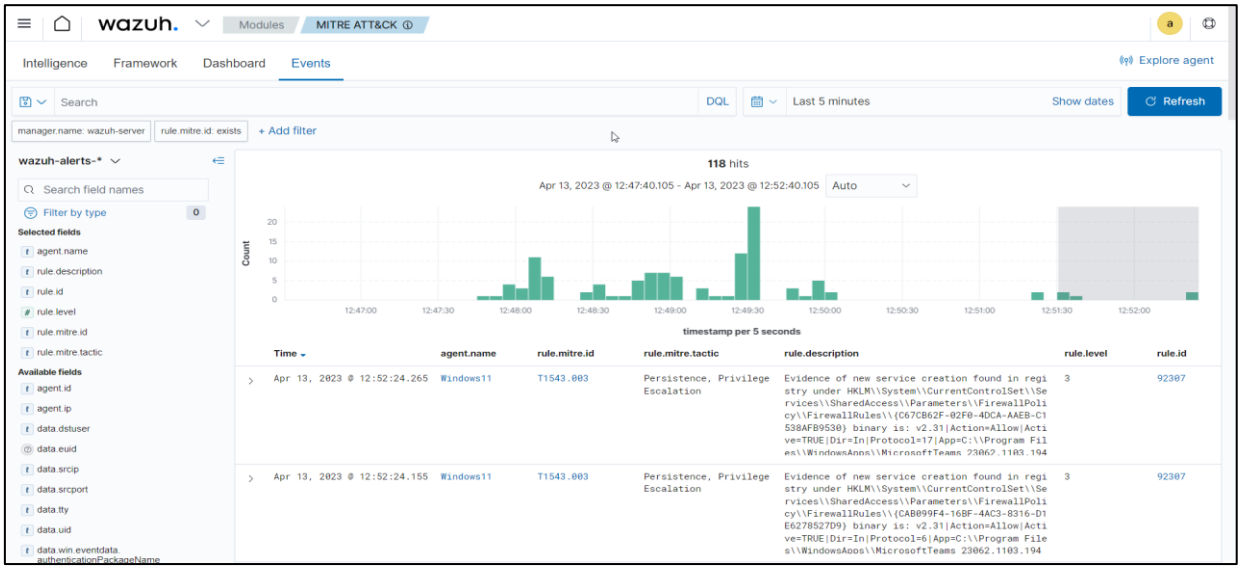
A Figura 9, a seguir, apresenta a interface detalhada de eventos do módulo MITRE ATT&CK no *Wazuh*. Enquanto os painéis anteriores (*dashboards*) oferecem uma

visão geral e estatísticas de alto nível, a tela de "*Events*" fornece a segmentação necessária para a análise forense e a resposta a incidentes.

No topo, do gráfico de barras da Figura 9, é possível observar a contagem de eventos ("118 hits"), permitindo que os analistas identifiquem picos de atividade suspeita. Ainda na Figura 6, embaixo do gráfico, pode-se observar uma tabela detalhada com a lista de cada evento de segurança, fornecendo informações críticas como o carimbo de data/hora (*Time*), o agente afetado (*agent.name*), a tática e o ID da técnica MITRE (*rule.mitre.tactic* e *rule.mitre.id*), uma descrição detalhada da regra (*rule.description*) e o nível de severidade do alerta (*rule.level*).

A visualização da Figura 9 é fundamental para a contextualização de cada alerta, mostrando exatamente qual técnica de ataque, como por exemplo, "*Persistence*, *Privilege Escalation*", foi detectada, em qual máquina, Windows11, neste caso e a descrição completa do evento que acionou o alerta. O painel lateral esquerdo, ainda na Figura 9, complementa a funcionalidade, permitindo que os usuários filtrem e pesquisem os eventos por campos específicos, como agente, descrição da regra, nível e ID, o que facilita enormemente a investigação e a triagem de incidentes de segurança.

Figura 9 - Painel de Eventos do Módulo MITRE ATT&CK no Wazuh.



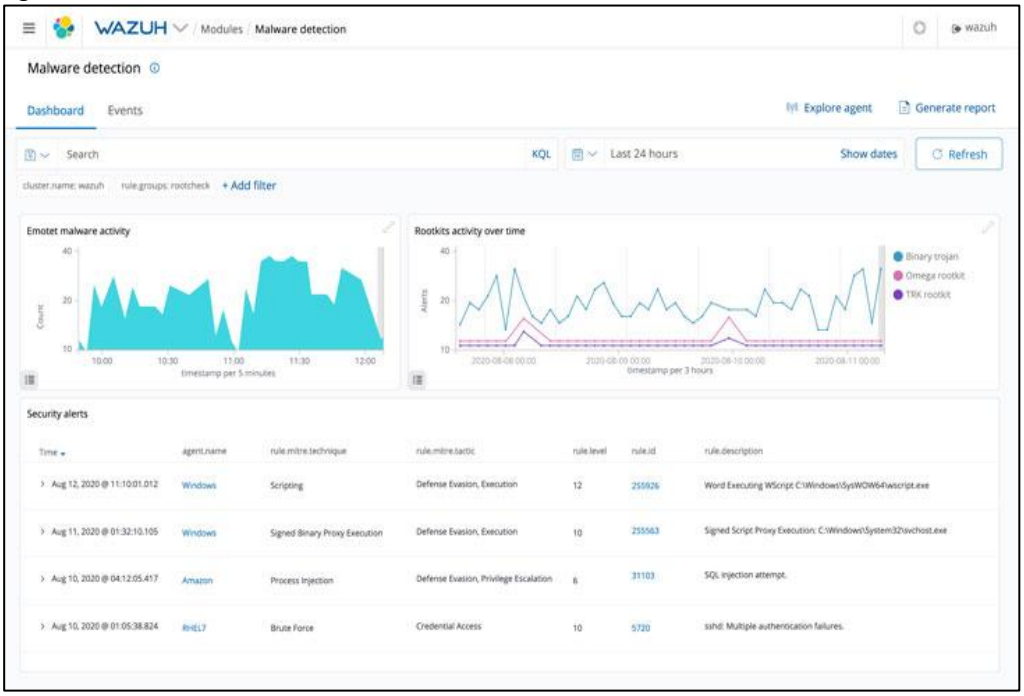
Fonte: Wazuh, 2024.

3.9.5. Painéis de Módulos Específicos do *Wazuh*

As Figuras 10,11 e 12, a seguir, demonstram a natureza modular e abrangente da plataforma *Wazuh*, mostrando painéis dedicados a funcionalidades de segurança específicas. Embora sejam de painéis diferentes, todos pertencem à mesma interface e seguem a mesma estrutura de navegação e visualização, o que reforça a coerência e a integração da plataforma.

- ***Malware Detection*:** Este painel foca na detecção de malware. Ele apresenta um gráfico de atividades de malware ao longo do tempo, permitindo que os analistas identifiquem picos de infecção ou varreduras. A Figura 10, a seguir, mostra o "*Security alerts*" que detalha cada evento, incluindo o nome do agente, a regra, a tática MITRE e uma descrição da atividade suspeita.

Figura 10 -Painel Malware do Wazuh.

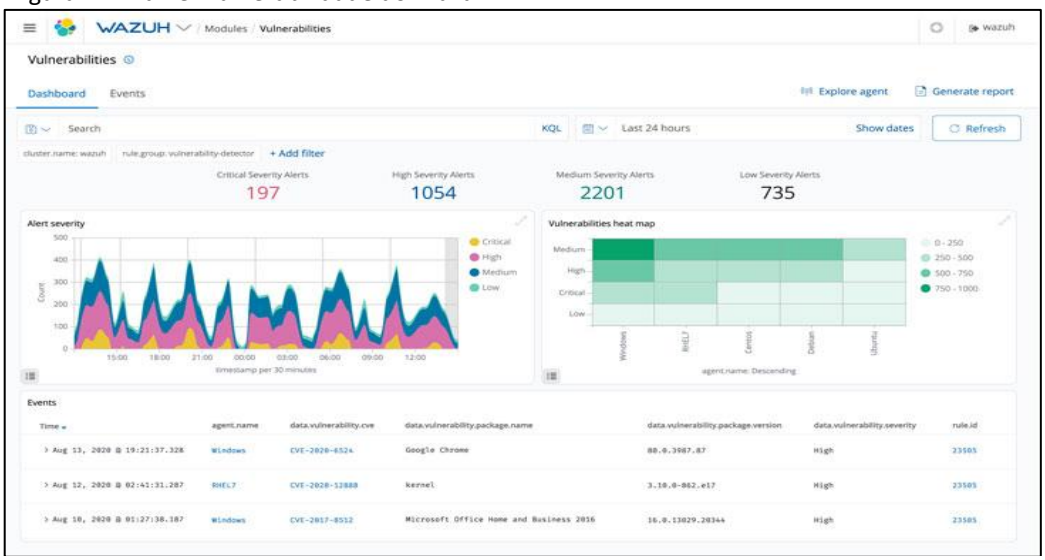


Fonte: Wazuh, 2024.

- ***Vulnerabilities:*** Este painel é dedicado à gestão de vulnerabilidades. A Figura 11, a seguir, mostra um resumo visual e numérico das vulnerabilidades por nível de severidade, ajudando a priorizar as ações de correção. O gráfico da Figura 8 de área empilhada mostra a evolução dessas vulnerabilidades no tempo, enquanto a tabela de "*Events*" lista os

eventos específicos, como a detecção de vulnerabilidades em *softwares* instalados.

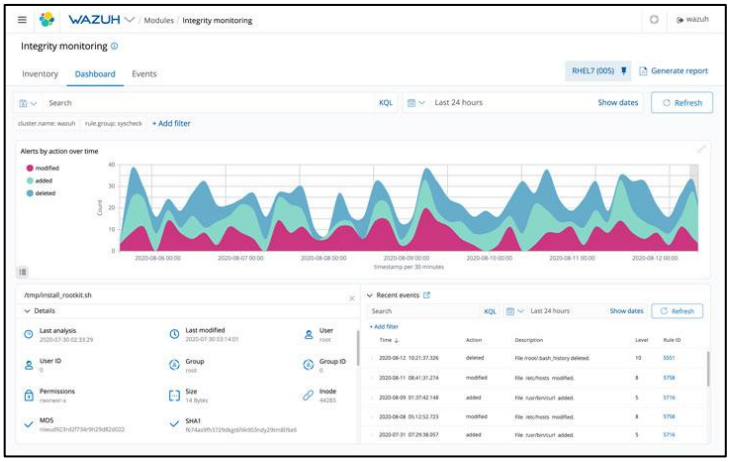
Figura 11 - Painel Vulnerabilidade do Wazuh.



Fonte: Wazuh, 2024.

- ***Integrity Monitoring*:** Este painel é especializado no monitoramento de integridade de arquivos (*File Integrity Monitoring - FIM*), pode ser observado na Figura 12. Este monitoramento rastreia e exibe qualquer alteração nos arquivos ou registros monitorados. O gráfico de "*Integrity activity over time*", na Figura 12, mostra a frequência de modificações, enquanto a tabela detalhada lista o agente, o caminho do arquivo, a data da modificação e o usuário responsável, essencial para auditoria e detecção de atividades maliciosas ou não autorizadas.

Figura 12 - Painel de Integridade do Wazuh



Fonte: Wazuh, 2024

Juntos, esses painéis mostrados nas Figuras 10, 11 e 12, ilustram como o *Wazuh* consolida várias funções de segurança, tais como: a detecção de *malware*, a gestão de vulnerabilidades e monitoramento de integridade, em uma única plataforma, fornecendo aos usuários ferramentas especializadas e visualmente ricas para cada domínio da segurança da informação.

Para atingir tais objetivos de análise e demonstrar a eficácia da plataforma, a implementação e a avaliação foram conduzidas seguindo uma abordagem estruturada. Assim, os procedimentos técnicos e a infraestrutura utilizada serão detalhados no próximo etapa.

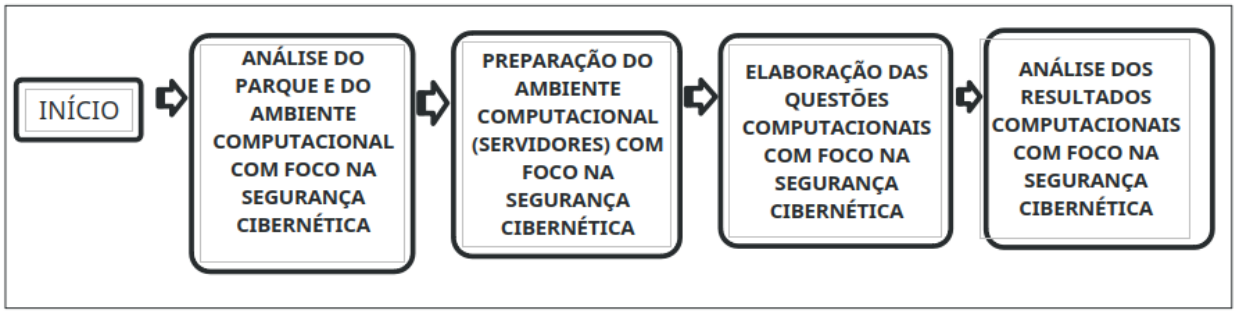
4. MATERIAIS E MÉTODOS

Este capítulo descreve a metodologia e as ferramentas tecnológicas usadas no processo de desenvolvimento deste trabalho, destacando uma visão detalhada das estratégias e procedimentos metodológicos utilizados para desenvolver a solução proposta. Em relação as ferramentas este capítulo explora as tecnologias essenciais empregadas ao longo do projeto, tais como o *framework* escolhido e sua importância e aplicação no contexto do projeto.

4.1. Etapa do Processo de Desenvolvimento do Trabalho

As etapas do processo de desenvolvimento do trabalho assim como as informações sobre a empresa que foi utilizada neste trabalho e os dados coletados desta empresa são mostrados na Figura 13, a seguir.

Figura 13 - Etapas do processo de desenvolvimento do trabalho.



Fonte: Autor.

4.1.1. Etapa de Início

A etapa de Início do processo aconteceu com a escolha da empresa para ser usada no trabalho. A empresa chama-se Fscruz e esta foi escolhida por ser uma empresa do mercado paraense com faturamento de 200 milhões por ano com sede em Ananindeua e operação nos municípios de Belém, Ananindeua, Vigia, Altamira e Brasil Novo, presente em 16 Açougues e 2 abatedouros na região de Brasil Novo e Altamira e em expansão no momento para suprir os supermercados.

Ela é especializado na revenda e corte de carne tanto na distribuição como para os açougues próprios. Existe diversas categorias de produtos, desde a carne de primeira a até a de terceira. A empresa em sua sede possui aproximadamente 200 funcionários, divididos em dois pontos a Matriz que está dividida 6 setores chave: atendimento, administração e logística, gerencia, recursos humanos, tecnologia da informação o outro e o Centro Distribuição com os setores de abate e distribuição.

Em relação a tecnologia de informação, a empresa possui uma rede na faixa 10.0.1.0/24, equipada com *switches* de camada 2 (*Layer 2*). Apesar disso, até o momento, não houve investimento significativo na área de segurança cibernética. O foco principal da infraestrutura de TI tem sido a manutenção e gerenciamento do *Active Directory*, garantindo que todas as contas de usuários e permissões estejam devidamente configuradas e operacionais. Esta abordagem, embora eficiente para a gestão de identidades e acessos, deixa a empresa vulnerável a potenciais ameaças e interrupções, uma vez que os aspectos de monitoramento e redução de vulnerabilidades não estão sendo adequadamente tratados.

A empresa não possui atualmente nenhuma ferramenta de segurança implementada em sua infraestrutura de TI. Essa ausência representa um risco significativo, pois deixa a rede de computadores da empresa e os seus dados vulneráveis a invasões, perda de informações e possíveis interrupções nas operações.

A falta de investimento em soluções de segurança cibernética, sistemas de detecção de intrusões e softwares de monitoramento, expõe a organização a ameaças que poderiam ser evitadas com uma abordagem mais proativa e focada na proteção dos ativos digitais. Durante o desenvolvimento deste trabalho, a equipe de tecnologia da informação da empresa possuía aproximadamente 4 pessoas.

Após fazer a análise no parque computacional da empresa, constatou-se que a empresa possui 6 servidores de marca diversas, para atender as demandas das lojas e das filiais, que visam promover a qualidade dos dados.

Os funcionários do setor de tecnologia estão divididos em basicamente duas funções: suporte e sistema. Os funcionários responsáveis pelo suporte atuam como técnicos de informática dos equipamentos, realizando operações cotidianas, tais como: verificação de impressoras, computadores, relógio de pontos, balança, alguns problemas de telefonia e problemas relacionados a rede de computadores. No setor de sistema os funcionários têm o foco na inserção dos dados no sistema e apoio aos processos dos setores.

Com o aumento das ações de expansão da empresa e do alcance de novas possiblidade de interrupção de serviços, houve um aumento de demandas tanto no setor de rede de computadores como no setor de segurança computacional, sendo muitas dessas demandas repetitivas e sem monitoramento de informações, o que para a equipe parece ser sempre novas demandas.

4.1.2. Etapa de Análise do Parque e do Ambiente Computacional com Foco na Segurança Cibernética

A análise da infraestrutura computacional da empresa evidencia um parque tecnológico funcional, porém carente de medidas efetivas no âmbito da segurança cibernética. Com a expansão das atividades empresariais e o consequente aumento das demandas operacionais, torna-se imperativa a proteção dos ativos digitais, conformando a segurança da informação como prioridade estratégica. Nesse contexto, destaca-se a necessidade de adoção de ferramentas voltadas ao monitoramento contínuo e à detecção proativa de vulnerabilidades, com vistas à mitigação de riscos e ao fortalecimento da capacidade de resposta frente a ameaças cibernéticas.

A partir do diagnóstico realizado, identificou-se a ausência de um sistema integrado de segurança cibernética. Em resposta, propõe-se a implementação de uma solução baseada na integração entre o dashboard do *Wazuh* e a base de dados do CVE MITRE, de modo a atender de forma eficiente às demandas específicas do empresa. Essa integração oferece uma abordagem sistemática para o monitoramento, a priorização e a correção de vulnerabilidades. Ao utilizar dados provenientes do CVE MITRE, o *Wazuh* apresenta-se como ferramenta robusta, capaz de disponibilizar funcionalidades de monitoramento em tempo real, análise detalhada de

vulnerabilidades, geração de relatórios e dashboards interativos. Sua interface intuitiva, aliada a um sistema eficaz de alertas e notificações, permite a pronta informação acerca de novas vulnerabilidades e atualizações relevantes, promovendo resposta ágil e fundamentada diante de possíveis incidentes.

A principal finalidade da solução proposta consiste em proporcionar um instrumento eficaz para a identificação, priorização e mitigação de vulnerabilidades de segurança, por meio da combinação entre a base de dados do CVE MITRE e as capacidades analíticas e operacionais do *Wazuh*.

Nesse sentido, definem-se os seguintes objetivos específicos:

- **Monitoramento contínuo**: assegurar a supervisão constante das vulnerabilidades em tempo real (Ferreira et al., 2019).
- **Análise de vulnerabilidades**: viabilizar a análise aprofundada das vulnerabilidades detectadas, com categorização e priorização baseadas em níveis de criticidade (Lima et al., 2020).
- **Correção de vulnerabilidades:** disponibilizar orientações e ferramentas adequadas para a mitigação eficaz das vulnerabilidades identificadas (Johnson & White, 2016).
- **Geração de relatórios e dashboards:** produzir relatórios técnicos e representações visuais claras para subsidiar o processo decisório (Lee & Thompson, 2018).
- **Integração com o CVE MITRE:** permitir a importação e a sincronização automatizada de dados atualizados sobre vulnerabilidades.
- **Interface de usuário intuitiva:** oferecer navegação acessível e eficiente entre módulos e funcionalidades da plataforma.
- **Alertas e notificações:** implementar sistema de notificações para manter os usuários informados sobre novas ameaças e atualizações críticas.
- **Customização:** viabilizar a adaptação do sistema às necessidades específicas da organização, por meio de opções de configuração e personalização (Miller & Davis, 2019).

A escolha do *Wazuh*, em detrimento de outras soluções disponíveis no mercado, fundamenta-se em fatores técnicos e estratégicos. Em primeiro lugar, sobressai sua integração nativa e contínua com a base de dados CVE MITRE, conferindo vantagem significativa no que tange à atualização automática e à precisão das informações sobre vulnerabilidades conhecidas, característica essencial em

ambientes que demandam resposta rápida e confiável a ameaças emergentes. Adicionalmente, o *Wazuh* oferece interface com elevada capacidade de personalização, possibilitando configurar o dashboard de acordo com necessidades operacionais específicas. Essa flexibilidade constitui diferencial relevante diante de ferramentas concorrentes que, por vezes, impõem limitações quanto à adaptabilidade de interfaces e funcionalidades.

Outro aspecto a destacar é o sistema robusto de alertas e notificações em tempo real, que garante a comunicação imediata da detecção de novas ameaças ou de atualizações críticas, favorecendo resposta ágil e eficaz. Estudos como o de Miller e Davis (2019) reforçam que atributos de customização e de capacidade de integração são determinantes para o sucesso de ferramentas voltadas à gestão de vulnerabilidades, o que valida a adoção do *Wazuh* no presente contexto organizacional.

Para o início do processo de configuração, adaptado à realidade da empresa, a etapa inaugural consiste na instalação do agente *Wazuh* nos servidores previamente definidos, medida essencial para habilitar a coleta de dados e a análise subsequente de segurança no ambiente monitorado. Na sequência, recomenda-se proceder à integração e à sincronização com a base CVE MITRE, à definição de políticas de detecção e correção, e à parametrização de dashboards, relatórios e alertas em conformidade com os objetivos específicos elencados. Essa sequência favorece a operação contínua do monitoramento, a análise criteriosa de vulnerabilidades e a pronta geração de evidências para apoio à tomada de decisão.

Com a implementação proposta, espera-se o fortalecimento da postura de segurança institucional, a redução do tempo de exposição a vulnerabilidades críticas, o incremento da rastreabilidade de eventos e a melhoria da capacidade de resposta a incidentes. Em conjunto, tais entregas contribuem para a consolidação de uma arquitetura de segurança utilizável e sustentável, apta a sustentar as atividades do Centro de Operações de Segurança (SOC) e a elevar o nível de maturidade em segurança cibernética da empresa.

4.1.3. Preparação do Ambiente Computacional (Servidores) com Foco na Segurança Cibernética

A preparação do ambiente nos servidores da Santa Cruz para a implementação do *Wazuh* é um passo crucial para garantir um monitoramento eficaz e contínuo de

vulnerabilidades. Segundo Lima et al. (2020), uma análise detalhada de vulnerabilidades depende de uma configuração inicial robusta. Primeiro, é essencial garantir que os servidores estejam atualizados e em conformidade com as políticas de segurança da organização (Johnson & White, 2016).

Instalar o agente *Wazuh* nos servidores selecionados foi o primeiro passo, seguido pela configuração dos parâmetros de comunicação entre os agentes e o servidor *Wazuh* principal.

Este processo incluiu a definição de regras de monitoramento específicas, que permitiram uma detecção proativa de ameaças e anomalias. Além disso, foi configurado alertas e notificações para assegurar que os administradores de TI fossem informados em tempo real sobre qualquer incidente crítico, conforme sugerido por Lee & Thompson (2018).

Assim, a preparação adequada do ambiente nos servidores da empresa Santa Cruz facilita a implementação do *Wazuh*, mas também maximiza sua eficácia no gerenciamento de vulnerabilidades.

4.1.4. Etapa de Elaboração das Questões Computacionais com Foco na Segurança Cibernética do Uso do *Wazuh* na Empresa

O processo de criação das questões (Tabela 4) para a coleta de informações após a implementação do *Wazuh* na empresa, foi conduzido de forma criteriosa e detalhada, com o objetivo de avaliar a eficácia e eficiência do sistema implantado. Observe na Tabela 4, a seguir, as questões usadas.

Tabela 4 - Quadro com a questões usadas para avaliar o sistema implementado na empresa.

Número da Questão	Pergunta da Questão
1	Você conhece o CVE MITRE e sua importância para a empresa, Sim ou Não?
2	Você utiliza a base de dados do CVE MITRE sem a utilização de ferramentas para gerenciamento de vulnerabilidades?
3	É importância ter um dashboard baseado no CVE MITRE para ver graficamente a segurança da informação, Sim ou Não?
4	Para você qual é o principal desafio de implementar um dashboard baseado no CVE MITRE para a segurança da informação na empresa, levando em consideração os seguintes pontos: integração do sistema existente, falta de conhecimento técnico, restrições orçamentárias e resistência a mudança?
5	Na sua opinião, a visualização de um dashboard contribui para a melhoria contínua da segurança da informação da empresa frigorifico Santa Cruz, Sim ou Não?
6	Qual é seu nível de conhecimento técnico para a implementação do dashboard: alto, médio, baixo?
7	Você acha que há um aumento da efetividade das ações de correção de vulnerabilidades com o uso do dashboard, Sim ou Não?
8	Você acha que há uma economia de recursos na gestão de vulnerabilidades com o uso do dashboard, Sim ou Não?
9	Você acha que o uso do dashboard facilita a comunicação entre as equipes de segurança e a de gestão da empresa, Sim ou Não?
10	Para você quais são dos principais benefícios, listados, são mais relevantes na implementação do dashboard: melhoria na identificação e correção de vulnerabilidades, otimização do tempo e recursos e facilitação da comunicação e colaboração entre equipes?

Fonte: O Autor.

Inicialmente, foram desenvolvidas perguntas direcionadas à experiência dos administradores de TI com a interface e a usabilidade do *Wazuh*. Questões como: "Quão intuitiva é a interface do *Wazuh*?" e "Quais desafios você encontrou na configuração dos dashboards personalizados?" buscaram compreender a facilidade de uso da ferramenta.

Posteriormente, foram elaboradas perguntas focadas na integração do *Wazuh* com os dados do CVE MITRE, incluindo temas como a qualidade das informações sobre vulnerabilidades e comparações com outras ferramentas já utilizadas. Exemplo disso são questões como "As informações sobre vulnerabilidades fornecidas pelo *Wazuh* são atualizadas e precisas?" e "Como você avalia a integração do *Wazuh* com o CVE MITRE frente às soluções anteriores?".

Além disso, o sistema de alertas e notificações em tempo real foi abordado para medir sua eficácia. Perguntas como "Os alertas em tempo real do *Wazuh* foram eficientes em sinalizar ameaças de maneira oportuna?" e "Quão importante é o sistema de notificações para auxiliar na resposta a incidentes?" foram incluídas para obter uma avaliação mais precisa.

Para uma análise ainda mais completa, foram criadas questões focadas na preparação do ambiente e na configuração inicial, considerando *insights* dos estudos de Lima et al. (2020) e Johnson & White (2016). Exemplos incluem "O processo de instalação do agente *Wazuh* foi simples e direto?" e "As regras de monitoramento configuradas se mostraram eficazes na detecção de anomalias?". Tais perguntas foram formuladas para reunir *feedback* específico sobre as etapas inaugurais da implementação.

Antes de serem aplicadas, todas as questões passaram por uma revisão e foram testadas cuidadosamente a fim de garantir que cobrissem os aspectos mais relevantes da implementação. O objetivo foi identificar os pontos fortes e o quais áreas precisam de melhorias na utilização do *Wazuh* na empresa.

4.1.5. Etapa da Realização dos Testes

A avaliação prática do *Wazuh* no ambiente computacional da empresa incluiu a execução de testes específicos voltados à simulação de ameaças cibernéticas, com o objetivo de analisar o desempenho da ferramenta em tempo real. Esses testes permitiram comparar a eficácia do *Wazuh* com outras soluções de segurança anteriormente empregadas na organização.

Adicionalmente, foram realizados testes de carga e estresse com o intuito de medir a robustez e a adaptação do sistema diante de situações de uso extremo.

4.1.6. Etapa de Análise dos Resultados Computacionais com Foco na Segurança Cibernética

A análise dos resultados dos testes realizados seguiu diferentes abordagens, concentrando-se em parâmetros essenciais de segurança e desempenho.

Inicialmente, foram examinados os dados relacionados à detecção de vulnerabilidades e alertas em tempo real.

Para proporcionar uma visão mais ampla sobre o desempenho do *Wazuh*, os resultados também foram comparados com análises que destacam a integração eficiente e a usabilidade aprimorada da plataforma. Essa avaliação mostrou que o

Wazuh superou as expectativas em diversos cenários de ameaças simuladas, reforçando sua eficácia na detecção proativa de vulnerabilidades.

Além disso, também foram realizados testes comparativos entre o *Wazuh* e outras ferramentas disponíveis no mercado, tais como o *AlienVault* e o QRadar.

4.1.7. Etapa de Análise Gráfica do Resultado das Respostas ao Questionário feita aos Administradores

Nesta etapa, os resultados obtidos a partir das entrevistas realizadas com os administradores de rede são apresentados em forma de um resumo gráfico analítico dos dados coletados.

Em seguida, são apresentados os resultados simulados provenientes da aplicação do questionário, com 45 funcionários do setor de TI da empresa, os quais contribuem para uma análise complementar e aprofundada acerca da eficácia da solução implementada.

4.2. Scripts Desenvolvidos

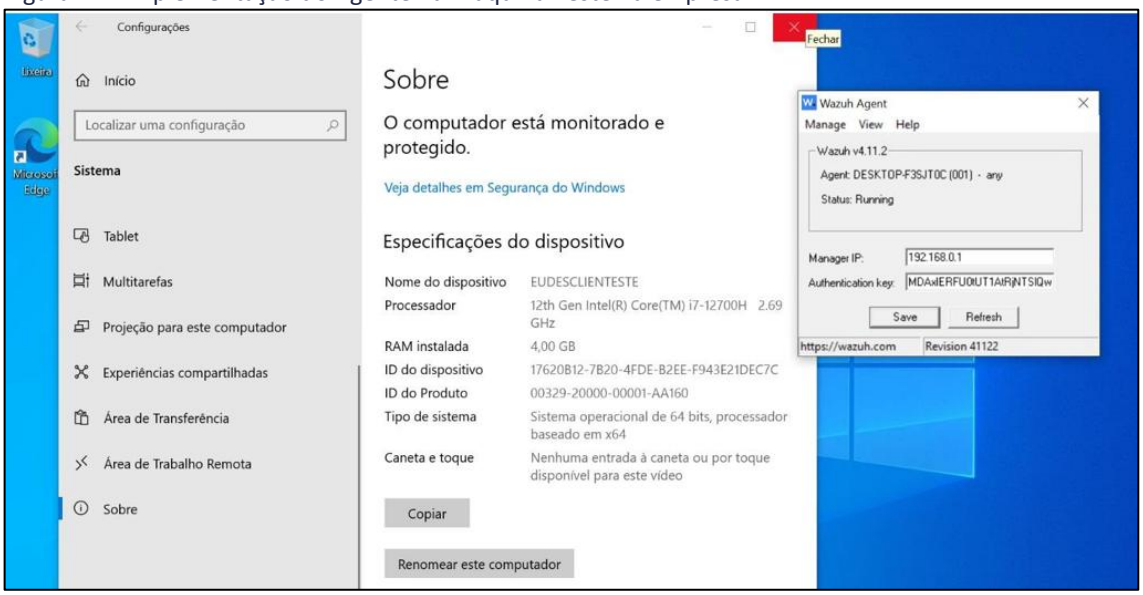
Para o trabalho foram desenvolvidos *scripts* para a solução de segurança implementada. O objetivo principal desses *scripts* é criar cenários da empresa. Os *scripts* foram estruturados para gerar eventos de segurança, processar *logs* e monitorar a resposta do sistema sob condições normais e extremas de uso. Para isso, foram considerados fatores como: tempo de resposta, taxa de detecção de ameaças, consumo de recursos e escalabilidade da solução adotada.

4.2.1. Implementação do Agente para Base dos Scripts

A análise da arquitetura da plataforma *Wazuh* permitiu compreender que o agente constitui o elemento central no processo de coleta de dados, sendo peça fundamental para assegurar a visibilidade e a segurança dos *endpoints* monitorados.

Durante a observação, na prática no frigorifico Santa Cruz, como pode ser observado na Figura 14, constatou-se que o *Wazuh* possui papel estratégico ao realizar uma coleta detalhada e abrangente de informações vindas de múltiplas fontes, como *logs* de sistema, eventos de segurança, inventário de *software* e *hardware*, além de dados vindos da execução e comportamento de *scripts* personalizados.

Figura 14 - Implementação do Agente na Máquina Teste na empresa



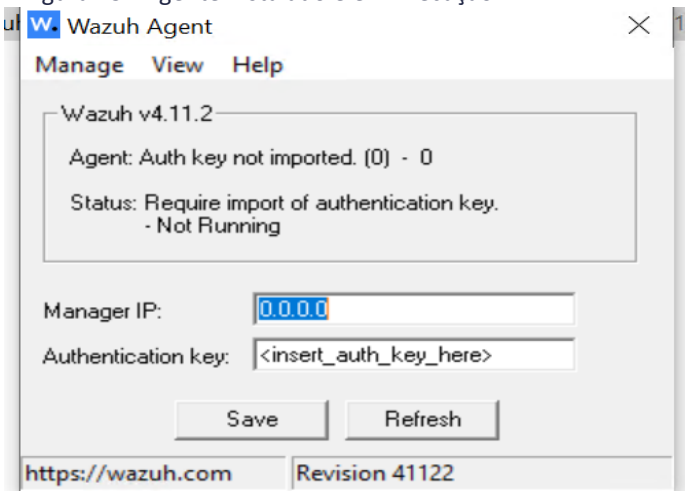
Fonte: O Autor.

Essa capacidade de coleta vai ao encontro das diretrizes estabelecidas pelo *National Institute of Standards and Technology* (NIST), especialmente no que se refere à função de monitoramento contínuo de segurança e à detecção precoce de incidentes, conforme descrito no NIST SP 800-137 (NIST, 2011).

A flexibilidade do agente *Wazuh* em permitir a personalização por meio de *scripts* específicos viabiliza a extração de dados complexos e o monitoramento de eventos singulares que, de outra forma, seriam inacessíveis. Tal funcionalidade é particularmente relevante para a detecção de ameaças, conformidade com normas regulatórias, e análise *forense* em tempo real, conforme recomenda também a norma ISO/IEC 27001:2022, que destaca a importância de controles adaptáveis de monitoramento para a proteção dos ativos de informação.

A correta implantação do agente é essencial para garantir uma comunicação eficiente com o servidor *Wazuh*, na Figura 15 a seguir, observa-se o envio adequado dos dados coletados e a utilização dos recursos e melhorias incorporados nas versões mais recentes da plataforma. Essa abordagem está alinhada com os princípios de resiliência operacional e resposta a incidentes definidos na ISO/IEC 27035-1:2016.

Figura 15 - Agente Instalado e em Execução.



Fonte: O Autor.

A flexibilidade apresentada pelo *Wazuh* representa uma de suas principais vantagens, destacando-se especialmente na capacidade de personalização do agente por meio de scripts.

Embora a ferramenta disponibilize uma ampla gama de módulos nativos para coleta de dados (*out-of-the-box*), os ambientes computacionais contemporâneos, caracterizados por sua heterogeneidade e especificidade, demandam soluções que extrapolem as funcionalidades padrão.

No contesto do frigorifico, a adaptabilidade do agente *Wazuh* se mostra decisiva para atender às exigências de segurança de infraestruturas complexas (Souza & Silva, 2018; Ferreira *et al.*, 2019).

4.2.2. Script de Implementação da Personalização de Logs

A personalização geralmente envolve a modificação do arquivo de configuração principal do agente (*ossec.conf*) no *endpoint* ou, de forma mais escalável, através da configuração centralizada via *agent.conf* no *manager*, que distribui as configurações para grupos de agentes. Dentro do *ossec.conf*, podem ser adicionados blocos *<localfile>* para que o agente monitore a saída de *scripts* executados periodicamente, ou blocos *<command>* e *<active-response>* para definir e acionar *scripts* em resposta a alertas, conforme representado na Figura 16 a seguir.

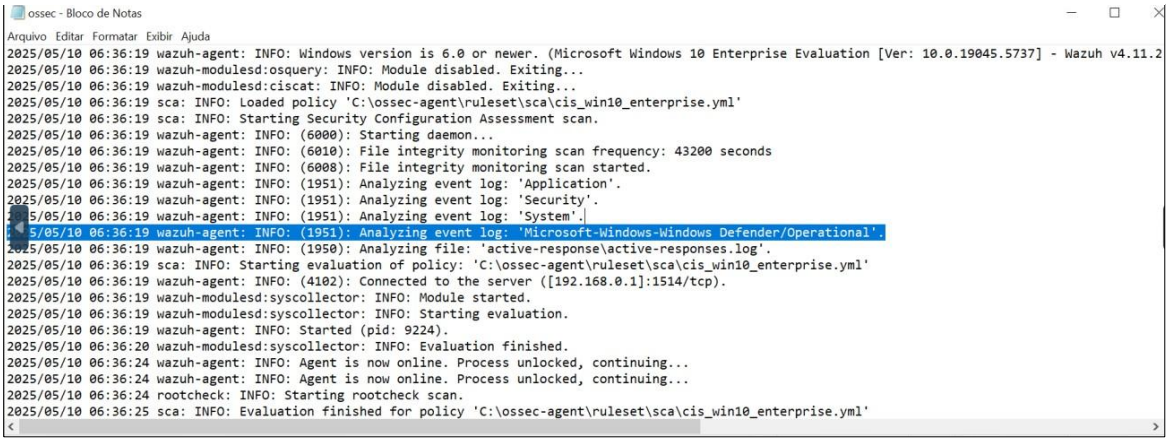
Figura 16 -Inserção no Código para coleta de dados Log Windows Server.

```
<!-- Log analysis adicionador pelo Pesquisador -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>
```

Fonte: O Autor.

Essa flexibilidade na personalização transforma o agente *Wazuh* de um simples coletor de dados em uma ferramenta poderosa e adaptável, capaz de lidar com os requisitos de segurança mais complexos e dinâmicos de qualquer ambiente. No entanto, é crucial que os *scripts* sejam desenvolvidos com segurança em mente e testados rigorosamente para evitar a introdução de vulnerabilidades ou impactos negativos no desempenho do sistema. A deteção dos registros desses *logs* é demonstrado na Figura 17.

Figura 17 - Leitura no Agente do script personalizado.



Fonte: O Autor.

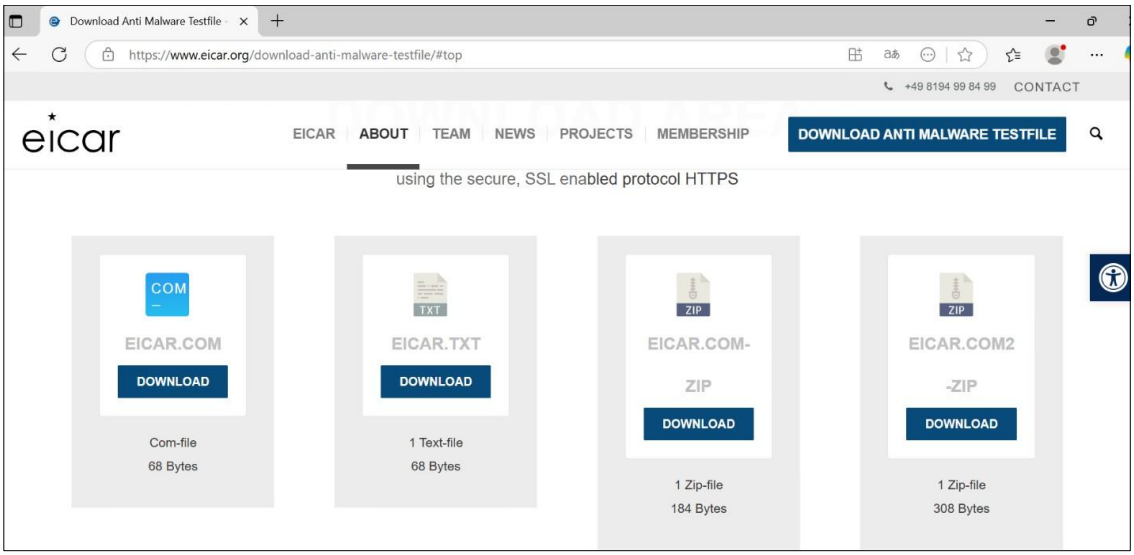
Na metodologia de teste, uma etapa crucial foi o *download* e a execução do arquivo de teste *EICAR* (*European Institute for Computer Antivirus Research*), obtido diretamente do site oficial da *EICAR*, Figura 15.

O arquivo, embora não seja um *malware* real que possa causar danos, é universalmente reconhecido por *softwares* antivírus e sistemas de segurança como uma ameaça legítima.

A sua utilização permitiu simular uma detecção de *malware* de forma segura, garantindo que as regras configuradas no *Wazuh*, bem como nos *scripts* personalizados de coleta de *logs*, fossem acionados e reportassem o evento exatamente como se fosse um *malware* verdadeiro.

Esse teste específico, foi importante para verificar, não apenas a capacidade de detecção do agente, mas também a correta formatação e envio dos alertas gerados para o *Wazuh Manager*, confirmando a eficácia da cadeia de monitoramento que foi desenvolvendo para a tese.

Figura 18 - Malware para ambiente controlados



Fonte: O Autor.

4.2.3. Script de Integridade de Arquivos

Para ir além da detecção de *malware* e garantir a robustez da solução, concentrou -se no desenvolvimento de um *script* de integridade de dados para o agente. A intenção foi criar um mecanismo de monitoramento continuo dos arquivos críticos do agente, tais como: seu executável, arquivos de configuração e diretórios de *log*, em busca de qualquer alteração não autorizada.

Caso um *malware* ou um atacante tentasse adulterar o agente para desativá-lo, comprometer sua coleta de dados ou ocultar suas trilhas, esse *script* seria responsável por identificar essas modificações.

Esse passo foi fundamental para assegurar que a própria fonte de informação de segurança permanecesse íntegra e confiável, contribuindo significativamente para a adaptação do sistema de monitoramento.

A Figura 19, a seguir, está monstrando que se o diretório fosse alterado o mesmo seria alertado para o administrador.

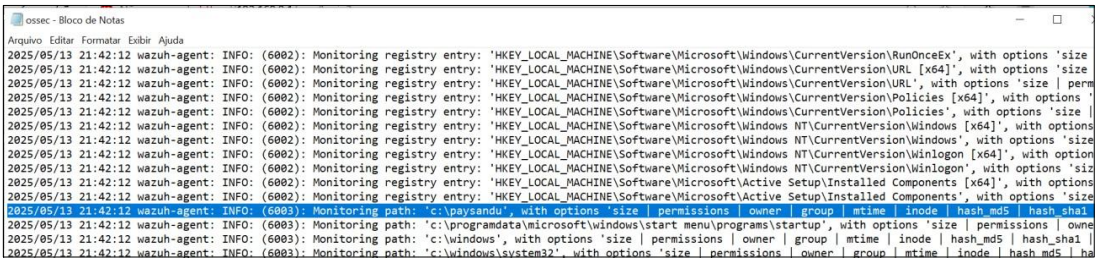
Figura 19 - Inserção na linha do script para monitorar uma pasta.

```
<!-- Personalização Script. -->
<directories check_all="yes" report_change="yes" realtime="yes">c:\paysandu</directories>
```

Fonte: O Autor.

O carregamento do *script* no agente *Wazuh* é realizado através da configuração do arquivo *ossec.conf*, especificando o caminho e a frequência de execução para que o monitoramento seja contínuo, como mostra a Figura 20.

Figura 20 - Carregamento da Personalização no Agente.



Fonte: Autor.

Com o *script* de integridade devidamente carregado e operando no agente, a etapa seguinte consiste na validação prática de sua eficácia.

No ambiente de teste controlado, foi simulado uma tentativa de comprometimento ao modificar intencionalmente um arquivo crucial dentro da pasta de instalação do agente *Wazuh*. Especificamente, foi alterado um arquivo de configuração importante, buscando simular uma ação maliciosa que visaria desabilitar ou corromper a operação do agente.

5. RESULTADOS OBTIDOS

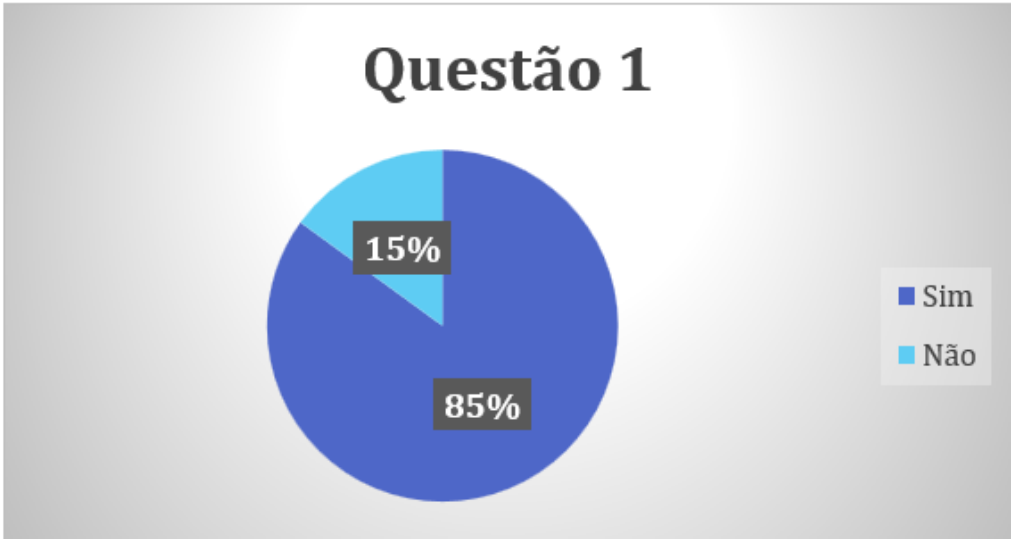
Neste capítulo serão apresentados a análise dos resultados obtidos a partir da aplicação do questionário, com 45 funcionários do setor de TI da empresa e os resultados obtidos após a execução dos *scripts* desenvolvidos para avaliação da solução de segurança implementada.

5.1. Análise dos Resultados Obtidos pelos Gráficos das Respostas da Aplicação do Questionário

Os resultados obtidos a partir das entrevistas e da aplicação do questionário foram sistematizados e alinhados com os objetivos do estudo, sendo apresentados e analisados a seguir por questão.

A Figura 21 mostra o gráfico com resultado das respostas obtidas das respostas da Questão 1: “Você conhece o CVE MITRE e sua importância para a empresa, Sim ou Não?”.

Figura 21 - Gráfico demonstrativo das respostas da Questão 1: “Você conhece o CVE MITRE e sua importância para na empresa, Sim ou Não?”



Fonte: O Autor.

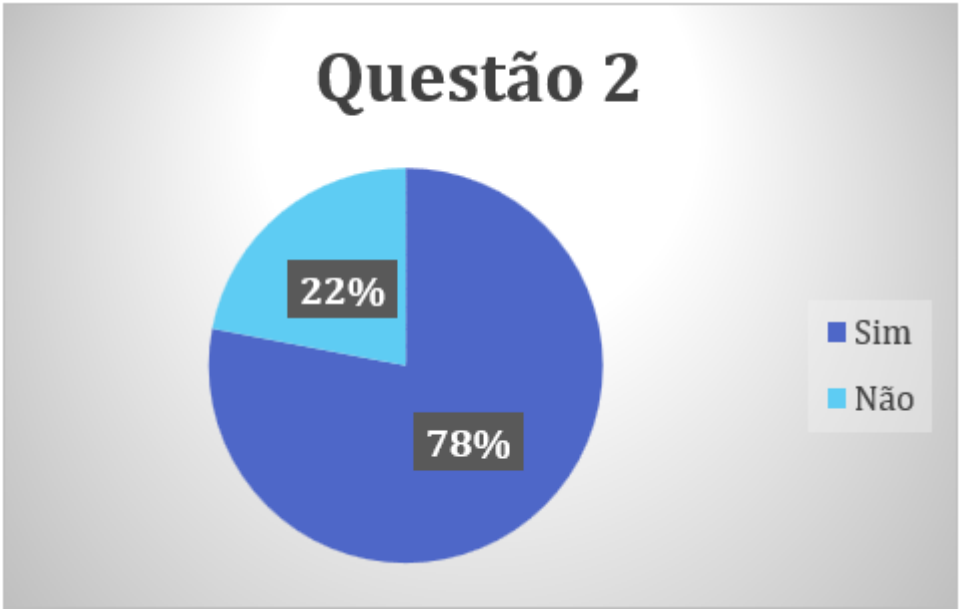
A análise dos dados referentes à Questão 1, revela que 85% dos entrevistados demonstram conhecimento sobre a base *CVE MITRE* e reconhecem sua relevância na categorização e classificação de vulnerabilidades. Esse resultado reforça a importância atribuída ao *CVE MITRE* como ferramenta estratégica no processo de gerenciamento eficaz de vulnerabilidades em ambientes computacionais.

Entretanto, observou-se que 15% dos participantes ainda não possuem familiaridade com o tema, evidenciando a necessidade de ampliar a conscientização e promover a disseminação de informações a respeito do assunto. Considera-se que a difusão do conhecimento sobre o *CVE MITRE* é essencial para que as organizações possam adotar práticas de segurança cibernética mais robustas e alinhadas às exigências do cenário tecnológico atual, contribuindo significativamente para a mitigação de riscos e a proteção dos ativos digitais.

Dessa forma, torna-se imprescindível o desenvolvimento de ações educativas e informativas voltadas à capacitação de profissionais e gestores, de modo a mostrar a importância do *CVE MITRE* no contexto da segurança da informação.

A Figura 22, a seguir, mostra o resultado das respostas da Questão 2: “Você utiliza a base de dados do CVE MITRE sem a utilização de ferramentas para gerenciamento de vulnerabilidades”.

Figura 22-Gráfico demonstrativo das respostas da Questão 2: “Você utiliza a base de dados do CVE MITRE sem a utilização de ferramentas para gerenciamento de vulnerabilidades”.



Fonte: O Autor

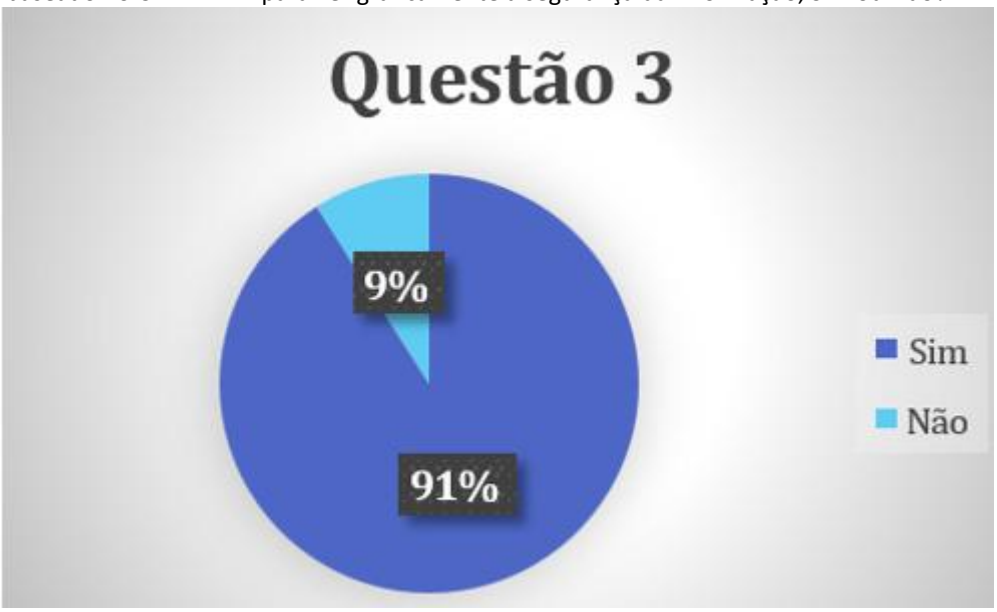
A análise dos resultados obtidos na Questão 2 mostra que 78% dos entrevistados já fazem uso da base de dados *CVE MITRE*. Contudo, o fazem sem o apoio de uma ferramenta específica para o gerenciamento de vulnerabilidades. Por outro lado, 22% dos usuários afirmaram não utilizar quaisquer ferramentas voltadas a essa finalidade, o que pode representar um risco importante à segurança da informação em suas respectivas organizações.

A ausência de ferramentas especializadas compromete a capacidade de identificar, priorizar e corrigir vulnerabilidades de forma organizada e proativa, aumentando a exposição a incidentes e perdas. Nesse contexto, destaca-se a importância da adoção de soluções tecnológicas apropriadas para o gerenciamento de vulnerabilidades, bem como a capacitação contínua dos profissionais responsáveis por sua operação.

Desta forma, torna-se fundamental para a empresa invista tanto em ferramentas eficientes quanto no desenvolvimento de competências técnicas de suas equipes, assegurando uma abordagem mais estratégica, eficaz e abrangente no tratamento de vulnerabilidades e na proteção de seus ativos digitais.

A Figura 23, mostra o resultado das respostas da Questão 3: “É importância ter um dashboard baseado no CVE MITRE para ver graficamente a segurança da informação, Sim ou Não?”.

Figura 23 - Gráfico demonstrativo das respostas da Questão 3: “É importância ter um dashboard baseado no CVE MITRE para ver graficamente a segurança da informação, Sim ou Não?”



Fonte: O Autor.

Com base nos dados obtidos na Questão 4: “Para você qual é o principal desafio de implementar um dashboard baseado no CVE MITRE para a segurança da informação na empresa, levando em consideração os seguintes pontos: integração do sistema existente, falta de conhecimento técnico, restrições orçamentárias e resistência a mudança?”.

Pode-se identificar que os principais desafios para a implementação de um *dashboard* baseado no *CVE MITRE*, sendo 40% relacionados à integração com sistemas existentes, 25% à falta de conhecimento técnico, 20% às restrições orçamentárias e 15% à resistência à mudança.

Concorda-se com os resultados e acredita-se que para superar esses desafios, é importante investir na capacitação e treinamento das equipes de TI e segurança, promovendo a conscientização sobre a relevância do *dashboard* baseado no CVE MITRE.

Além disso, é necessário estabelecer uma comunicação eficiente entre os diferentes setores da organização para facilitar a integração do *dashboard* com os sistemas existentes e abordar as preocupações relacionadas ao orçamento e à resistência à mudança.

Ao enfrentar esses desafios, a organização estará mais bem preparada para adotar soluções de segurança eficazes e melhorar a gestão de vulnerabilidades.

A análise pode ser observada na Figura 24, a seguir, mostra o resultado das respostas da Questão 4.

Figura 24 - Para você qual é o principal desafio de implementar um dashboard baseado no CVE MITRE

Fonte: O Autor.

Na Questão 5, os resultados do questionário indicam que 89% dos entrevistados consideram que um dashboard baseado no CVE MITRE pode favorecer a melhoria contínua da segurança da informação, pode ser observado na Figura 22.

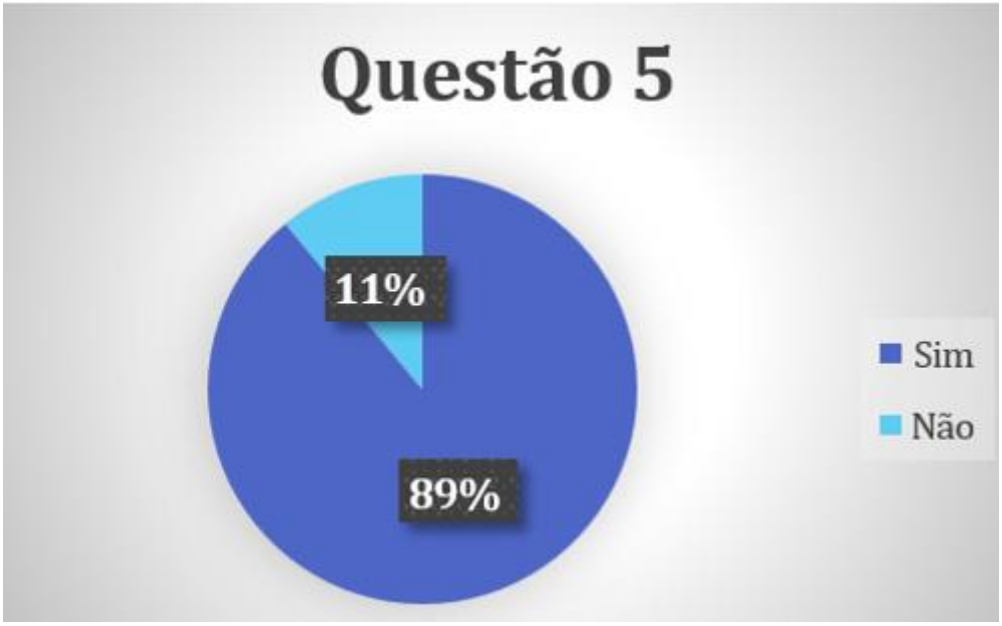
Em contrapartida, 11% dos respondentes não percebem tal contribuição, algo que pode estar relacionado a fatores como falta de conhecimento ou experiência com a ferramenta.

Concorda-se que a adoção de um *dashboard* desse tipo é essencial para melhorar os processos como: identificação, priorização e correção de vulnerabilidades, promovendo uma abordagem mais proativa e eficiente na proteção dos ativos digitais.

Além disso, a atualização do *dashboard* auxilia uma análise mais eficaz do desempenho das práticas de segurança, contribuindo para identificar áreas que necessitam de melhorias e implementar ações corretivas.

Esses fatores, por sua vez, têm potencial para fortalecer continuamente a segurança da informação do frigorífico. A Figura 25, a seguir, mostra o resultado das respostas da Questão 5: “Na sua opinião, a visualização de um dashboard contribui para a melhoria contínua da segurança da informação da empresa frigorifico Santa Cruz, Sim ou Não?”.

Figura 25 - Na sua opinião, a visualização de um dashboard contribui para a melhoria contínua da segurança da informação da empresa, Sim ou Não?.

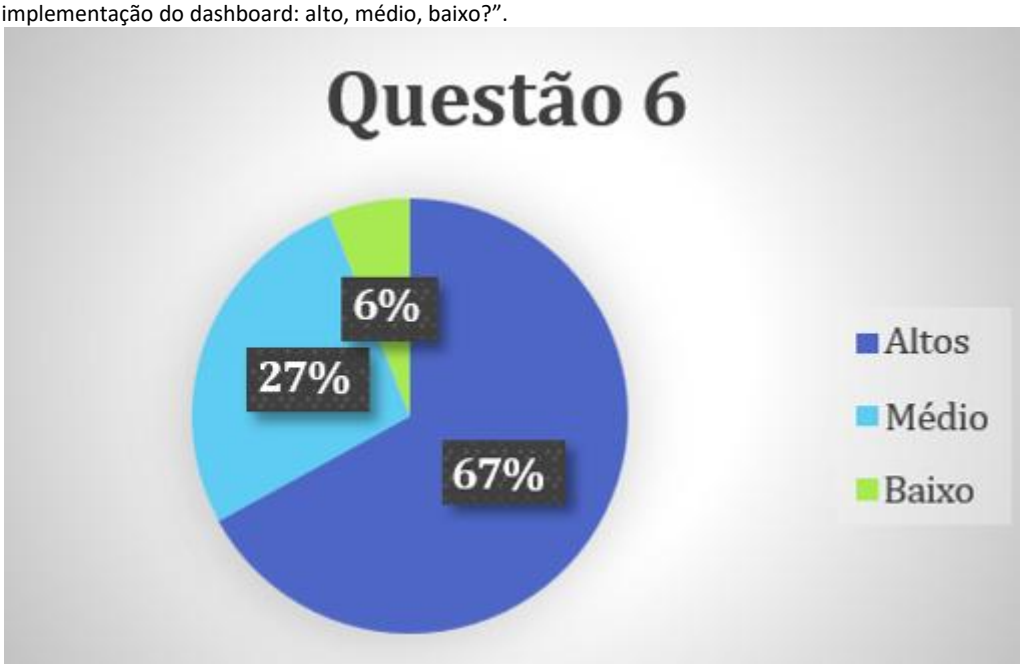


Fonte: O Autor.

A Figura 26, mostra o resultado das respostas da Questão 6: “Qual é seu nível de conhecimento técnico para a implementação do dashboard: alto, médio, baixo?”. A Figura 26 demonstra que a maioria dos entrevistados (67%) reportou um alto nível de conhecimento técnico para a implementação do dashboard baseado no CVE MITRE.

Adicionalmente, 27% indicaram um nível médio e apenas 6% um nível baixo. Estes resultados sugerem um capital humano qualificado, mas também a necessidade de investimento contínuo em capacitação e desenvolvimento profissional para garantir a implementação e o uso eficaz da ferramenta. A colaboração das equipes de segurança é fundamental para uma implementação eficiente e para a adoção adequada do dashboard.

Figura 26 - Gráfico demonstrativo das respostas da Questão 6: “Qual é seu nível de conhecimento técnico para a implementação do dashboard: alto, médio, baixo?”.

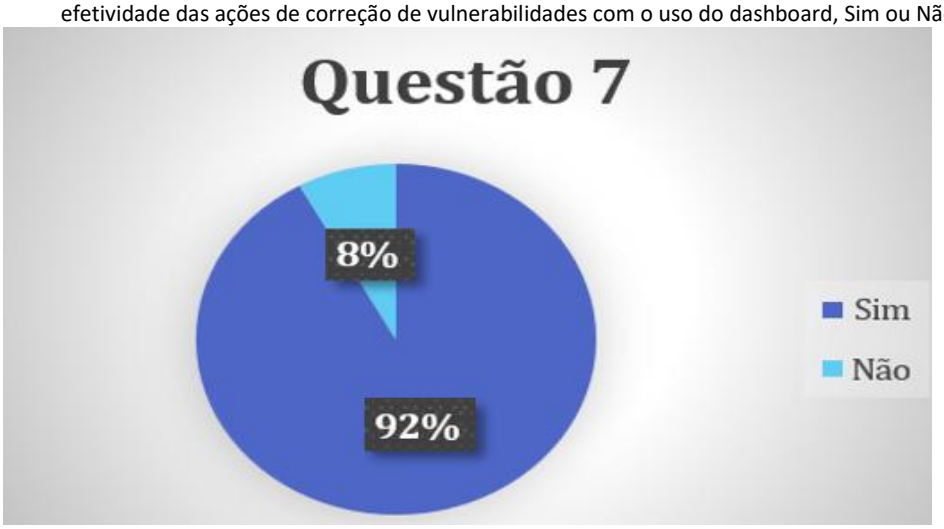


Fonte: O Autor.

O resultado das respostas à Questão 7 do questionário, podem ser vistas na Figura 27, e revelam que 92% dos entrevistados acreditam que a utilização de um *dashboard* baseado no *CVE MITRE* pode aumentar a efetividade das ações de correção de vulnerabilidades, enquanto apenas 8% não veem essa relação.

Essa visão sugere que a ferramentas como dashboards baseados no CVE MITRE melhoram a identificação e priorizam a identificação das vulnerabilidades, facilitando a tomada de decisão sobre quais correções devem ser aplicadas primeiro.

Figura 27-Gráfico demonstrativo das respostas da Questão 7: “Você acha que há um aumento da efetividade das ações de correção de vulnerabilidades com o uso do dashboard, Sim ou Não?”.



Fonte: O Autor.

Na Questão 8, como mostra a Figura 28, a seguir, mostra o gráfico onde 76% dos entrevistados acreditam que a utilização de um dashboard baseado no CVE MITRE pode gerar economia de recursos na gestão de vulnerabilidades, enquanto 24% não concordam com essa afirmação. Concorda-se com essa perspectiva e considera-se que a implementação de um dashboard auxilia na identificação de prioridades e melhorar a tomada de decisões, resultando em economia de recursos e maior eficiência na gestão de vulnerabilidades.

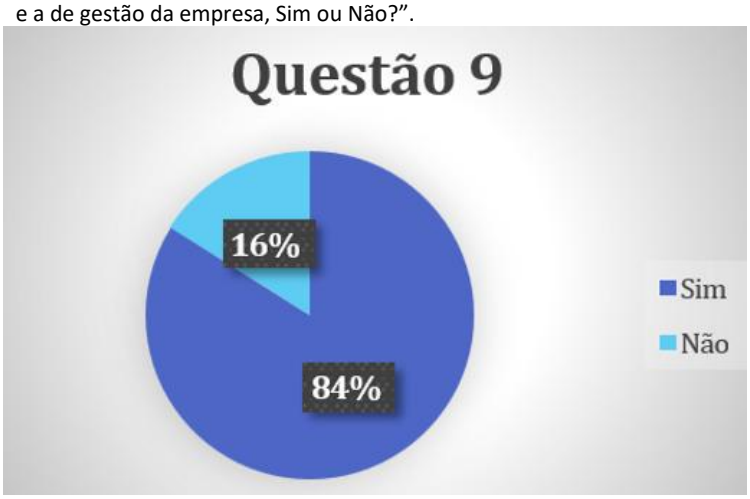
Figura 28- Gráfico demonstrativo das respostas da Questão 8: “Você acha que há uma economia de recursos na gestão de vulnerabilidades com o uso do dashboard, Sim ou Não?”.

Fonte: O Autor.

A Figura 29 mostra o gráfico demonstrativo das respostas a Questão 9, onde 84% dos participantes acreditam que o uso de um dashboard baseado no CVE MITRE facilita a comunicação entre as equipes de segurança, enquanto apenas 16% discordam.

Destaca-se que dashboards podem ser ferramentas valiosas para melhorar a comunicação e colaboração entre equipes. Considera-se que a adoção de um dashboard pode promover um entendimento comum das vulnerabilidades identificadas e das ações necessárias, aprimorando a comunicação e a gestão entre as equipes envolvidas na segurança da informação.

Figura 29 - Você acha que o uso do dashboard facilita a comunicação entre as equipes de segurança e a de gestão da empresa, Sim ou Não?".



Fonte: O Autor.

Por fim, o gráfico mostrando o resultado das respostas da Questão 10, que pode ser observado na Figura 30, indica que os principais benefícios percebidos da implementação do dashboard são: melhoria na identificação e correção de vulnerabilidades (45%), maior visibilidade das ameaças e riscos (30%), otimização do tempo e recursos (15%) e facilitação da comunicação e colaboração entre equipes (10%). Pode-se destacar a importância de ferramentas de gestão de vulnerabilidades para melhorar a segurança da informação.

Figura 30 - "Para você quais são dos principais benefícios, listados, são mais relevantes na implementação do dashboard: melhoria na identificação e correção de vulnerabilidades, otimização do tempo e recursos e facilitação da comunicação e colaboração

Fonte: O Autor.

Em resumo, os resultados das entrevistas e do questionário convergem para o ente entendimento de que a implementação de um *dashboard* baseado no *CVE MITRE* pode confirmar benefícios importantes à segurança da informação na empresa.

A maioria dos entrevistados demonstrou conhecimento sobre o *CVE MITRE* e reconheceu a importância estratégica de um *dashboard* para a visualização da segurança.

Adicionalmente, a maioria acredita que o *dashboard* pode aprimorar a efetividade das ações de correção de vulnerabilidades, gerar otimização de recursos e promover uma comunicação mais eficaz entre as equipes de segurança e gestão. Estes resultados reforçam o potencial da solução proposta neste trabalho para fortalecer a presença de segurança da empresa e otimizar a eficiência dos processos de segurança.

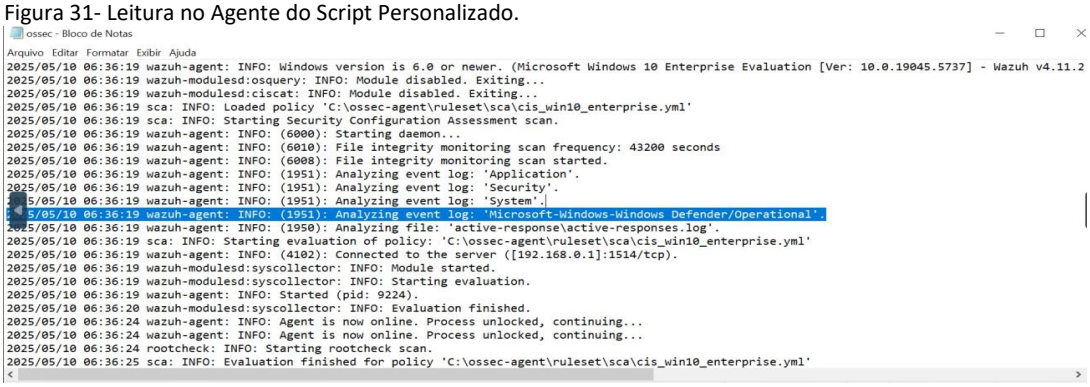
5.2. Análise dos Resultados Obtidos pela Implementação dos *Scripts*

Os resultados da implementação e personalização do agente *Wazuh*, bem como dos testes de validação, são apresentados a seguir.

5.2.1. Detecção de Logs Personalizados

A detecção dos registros gerados pelos *scripts* personalizados foi mostrada de forma eficaz, conforme observa-se na Figura 31, que exibe a leitura desses *logs* pelo agente.

Figura 31- Leitura no Agente do Script Personalizado.



Fonte: O Autor.

5.2.2. Análise da Detecção de *Malware EICAR*

Após a aplicação do arquivo *EICAR*, foram observados dois tipos principais de comportamento nos logs e alertas do *Wazuh*: a detecção direta pelo motor de *anti-malware* integrado (quando ativado) e o registro das tentativas de acesso e execução pelo sistema operacional, estas últimas capturadas pelos *scripts* personalizados.

O sucesso da coleta de dados na detecção do *malware* foi evidente, com o agente *Wazuh* registrando prontamente as atividades maliciosas.

Por causa da personalização do *script*, foi possível identificar a presença do arquivo EICAR e capturar os eventos específicos de seu acesso e tentativas de execução. A Figura 32 mostra o alerta coletado pelo *script* no momento da execução do arquivo *EICAR*. Este resultado validou a eficácia da abordagem na detecção de ameaças, confirmando que os *scripts* personalizados permitiram ao agente *Wazuh* identificar e reportar com precisão as tentativas de infecção em um ambiente real.

Figura 32- Alerta Coletado pelo Script no Momento da Execução.

Fonte: O Autor.

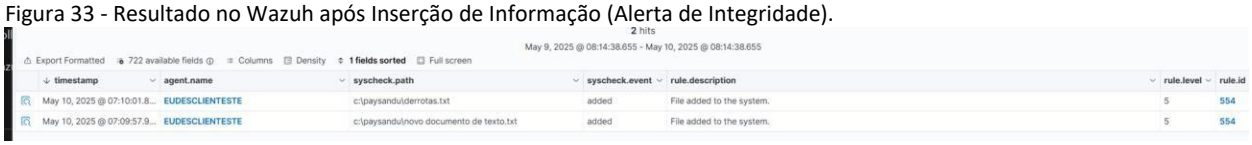
5.2.3. Verificação da Integridade de Arquivos do Agente

Imediatamente após a modificação intencional de um arquivo crucial dentro da pasta de instalação do agente *Wazuh*, notou-se que o sistema capturou a alteração.

Um alerta detalhado foi gerado, indicando não apenas qual arquivo havia sido alterado, mas também o tipo de modificação ocorrida (data, hora, *hash*).

A Figura 33 exibe o resultado no *Wazuh* após a inserção de informação que acionou o alerta de integridade. Este resultado validou com sucesso a capacidade do *script* de integridade em monitorar e reportar em tempo real qualquer adulteração no diretório do agente, confirmando a robustez da solução na proteção de sua própria infraestrutura de coleta de dados.

Figura 33 - Resultado no Wazuh após Inserção de Informação (Alerta de Integridade).



Fonte: O Autor.

6. CONSIDERAÇÕES FINAIS

A análise da infraestrutura computacional da empresa evidenciou a existência de um ambiente funcional, porém carente de mecanismos eficazes de segurança cibernética. Com a expansão da empresa e o aumento da complexidade operacional, a proteção dos ativos digitais tornou-se uma necessidade estratégica. A ausência de ferramentas de monitoramento e resposta a incidentes expõe a organização a riscos significativos, comprometendo tanto a continuidade das operações quanto a integridade das informações.

Neste contexto, este trabalho propôs a implementação de uma solução integrada entre o dashboard Wazuh e a base de dados CVE MITRE, visando o monitoramento contínuo, a análise, priorização e correção de vulnerabilidades. O sistema oferece funcionalidades como geração de relatórios, visualizações interativas e alertas em tempo real, permitindo uma gestão proativa da segurança da informação. A proposta contempla ainda a customização da interface conforme as necessidades da organização, contribuindo para sua adaptabilidade e eficácia operacional.

7. PERSPECTIVAS FUTURAS

Como continuidade deste estudo, sugere-se: a ampliação da integração com outras bases de dados e sistemas de *threat intelligence* para enriquecer a identificação de ameaças emergentes. A inclusão de algoritmos de aprendizado de máquina para prever padrões de ataque com base em comportamentos anteriores. O desenvolvimento de módulos automatizados de resposta a incidentes, capazes de executar ações corretivas com mínima intervenção humana. A realização de testes de intrusão (pentests) periódicos, integrados ao dashboard, para validar continuamente a eficácia das medidas implementadas. A adoção da solução em diferentes unidades da empresa, avaliando sua escalabilidade e impacto em contextos variados.

Com este trabalho pode-se obeservar que implementação da solução baseada na integração entre *Wazuh* e *CVE MITRE* representa um avanço relevante no fortalecimento da segurança cibernética da empresa, constituindo também uma base sólida para futuras inovações no campo da segurança da informação em ambientes corporativos.

8. REFERÊNCIAS BIBLIOGRÁFICAS

CARO MORENO, Raúl. **Trabajo Fin de Máster en Ingeniería Informática**. 2020. Trabalho de Conclusão de Curso (Mestrado em Engenharia Informática) – Universidade de Cádiz, Cádiz, 2020. Disponível em: https://rodin.uca.es/bitstream/handle/10498/23447/TFM-Caro-Moreno-Raul.pdf?isAllowed=y&sequence=1. Acesso em: 18 mar. 2025.

CYBERSECURITY VENTURES. **Cybercrime Damage Costs Predicted to Reach $10.5 Trillion Annually by 2025**. 2022. Disponível em: https://cybersecurityventures.com/. Acesso em: 5 jun. 2025.

ESCOLA DE INGENIERÍA INFORMÁTICA. **Trabajo Fin de Grado**. [S. l.]: Universidad de Valladolid. Disponível em: https://uvadoc.uva.es/bitstream/handle/10324/50089/TFG-G5229.pdf?sequence=1. Acesso em: 18 mar. 2025.

FERREIRA, J.; COSTA, M.; LIMA, F. Monitoramento e resposta a incidentes: uma análise sobre o uso de SIEMs em ambientes críticos. In: CONGRESSO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E SISTEMAS COMPUTACIONAIS, [s. l.], 2019. **Anais eletrônicos** [...]. [S. l.]: [s. n.], 2019. p. 28-35.

FONTES, R. **Segurança da Informação e Gestão de Riscos**. [S. l.]: [s. n.], 2023.

GARCIA, P.; MENDES, A. Open Source Security Platforms: A Comparative Analysis. **International Journal of Cybersecurity Studies**, [s. l.], v. 10, n. 1, p. 98-113, 2022.

ISO/IEC 27001:2022. **Information security, cybersecurity and privacy protection – Information security management systems – Requirements**. [S. l.]: International Organization for Standardization, 2022.

ISO/IEC 27035-1:2016. **Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management**. [S. l.]: International Organization for Standardization, 2016.

MORAES, R.; LIMA, T. Agentless Security Monitoring in Enterprise Networks: A Case Study with Open Source Tools. **Computer Security Review**, [s. l.], v. 8, n. 1, p. 35-51, 2020.

NETO, A.; ARAÚJO, F. **Estratégias de Proteção Cibernética**. [S. l.]: [s. n.], 2023.

NIST. **SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**. Gaithersburg, MD: National Institute of Standards and Technology, 2011.

OLIVEIRA, C.; SOUZA, M.; FERREIRA, L. Threat Detection and Response Using Open Source SIEMs. **Cybersecurity & Information Systems Journal**, [s. l.], v. 14, n. 2, p. 78-95, 2021.

PIGOLA, A. **Desenvolver e Investir em Capacidades Dinâmicas nos Negócios para Melhorar a Inteligência de Segurança Cibernética**. 2024. Tese (Doutorado em Administração Pública, Administração de Empresas, Ciências Contábeis e Turismo) – [Nome da Instituição, caso disponível], [Local], 2024. Disponível em: https://sucupira-

legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=14190848. Acesso em: 5 jun. 2025.

REGALADO, J. et al. **Métodos Modernos de Segurança Digital**. [S. l.]: [s. n.], 2023.

SANTOS, F.; OLIVEIRA, J.; LIMA, R. Cybersecurity Strategies in Open Source SIEM Solutions. **Journal of Information Security**, [s. l.], v. 12, n. 3, p. 45-62, 2023.

SCOTA, M. **Análise de Vulnerabilidades e Gestão de Riscos**. [S. l.]: [s. n.], 2023.

SOUZA, R.; SILVA, L. Gestão de vulnerabilidades em ambientes corporativos: práticas e ferramentas. **Revista Brasileira de Segurança da Informação**, [s. l.], v. 12, n. 1, p. 45-59, 2018.

STARTI, L. **Segurança da Informação no Mundo Corporativo**. [S. l.]: [s. n.], 2023.

WAZUH. **Wazuh Documentation**. 2024. Disponível em: https://documentation.wazuh.com. Acesso em: 5 jun. 2025.

WEIDMAN, G. **Testes de Invasão e Defesa de Sistemas**. [S. l.]: [s. n.], 2023.