UMA ABORDAGEM INTEGRADA DE SEGURANÇA CIBERNÉTICA: INTEGRAÇÃO DO WAZUH E DA BASE CVE (MITRE) PARA GESTÃO DE VULNERABILIDADES EM AMBIENTE CORPORATIVO

AN INTEGRATED CYBERSECURITY APPROACH: INTEGRATING WAZUH AND BASE CVE (MITRE) FOR VULNERABILITY MANAGEMENT IN A CORPORATE ENVIRONMENT

Otávio Noura Teixeira[1]

Eudes Danilo Mendonça[2]

Resumo: A aceleração da transformação digital ampliou a superfície de ataque das organizações e aumentou a demanda por processos sistemáticos de identificação, priorização e mitigação de vulnerabilidades. Este estudo propõe e avalia a integração entre a plataforma open source Wazuh e a base de vulnerabilidades CVE (MITRE), visando consolidar um fluxo unificado de monitoramento e suporte à decisão na gestão de riscos. A pesquisa foi conduzida em ambiente corporativo real, no Frigorífico Santa Cruz, com abordagem aplicada e exploratória. A solução implementada viabilizou monitoramento em tempo real, correlação de eventos e geração automatizada de alertas, com apoio à priorização por criticidade. Os resultados indicaram ganho de eficiência na identificação de vulnerabilidades críticas e redução do tempo médio de resposta a incidentes, sugerindo que a integração Wazuh–CVE pode fortalecer a governança de segurança e ampliar a capacidade operacional de resposta em organizações com recursos limitados.

Palavras-chave: Segurança da Informação. Wazuh. CVE (MITRE). Gestão de Vulnerabilidades.

1 Doutor em Engenharia Elétrica - Computação Aplicada, Universidade Federal do Pará. https://orcid.org/0000-0002-7860-5996

2 Mestre em Computação Aplicada, Universidade Federal do Pará, https://orcid.org/0009-0006-6439-408X

Resposta a Incidentes.

Abstract: The acceleration of digital transformation has broadened the attack surface of organizations and increased the demand for systematic processes for identifying, prioritizing, and mitigating vulnerabilities. This study proposes and evaluates the integration between the Wazuh open-source platform and the CVE (MITRE) vulnerability database, aiming to consolidate a unified flow of monitoring and decision support in risk management. The research was conducted in a real corporate environment, at Frigorífico Santa Cruz, with an applied and exploratory approach. The implemented solution enabled real-time monitoring, event correlation, and automated alert generation, supporting prioritization by criticality. The results indicated increased efficiency in identifying critical vulnerabilities and a reduction in the average incident response time, suggesting that the Wazuh–CVE integration can strengthen security governance and expand the operational response capacity in organizations with limited resources.

Keywords: Information Security. Wazuh. CVE (MITRE). Vulnerability Management. Incident Response.

INTRODUÇÃO

A intensificação da transformação digital nas organizações tem ampliado de forma significativa a superfície de ataque dos ambientes corporativos, tornando a segurança da informação um desafio estratégico contínuo e não mais um evento pontual. A crescente adoção de serviços em nuvem, dispositivos heterogêneos, aplicações distribuídas e integrações com terceiros criou ecossistemas digitais complexos, nos quais vulnerabilidades técnicas passam a representar riscos operacionais, financeiros e reputacionais de grande impacto. Nesse cenário, incidentes de segurança deixaram de ser exceção para se tornarem uma expectativa estatística, exigindo mecanismos sistemáticos de

prevenção, detecção e resposta.

Do ponto de vista normativo, frameworks amplamente reconhecidos — como os propostos pela ISO e pelo NIST — enfatizam a necessidade de processos contínuos de gestão de riscos, monitoramento e tratamento de vulnerabilidades. Entretanto, na prática organizacional, observa-se um descompasso recorrente entre o que é recomendado pelas normas e o que efetivamente é implementado, especialmente em empresas de médio porte e setores industriais, nos quais restrições orçamentárias, limitações técnicas e escassez de equipes especializadas dificultam a adoção de soluções proprietárias robustas.

Paralelamente, a quantidade de vulnerabilidades divulgadas publicamente cresce de forma exponencial. A base de dados CVE (Common Vulnerabilities and Exposures), mantida pela MITRE, tornou-se o principal repositório global de identificação padronizada de falhas de segurança. Contudo, apesar da ampla disponibilidade dessas informações, muitas organizações enfrentam dificuldades em transformar dados brutos de vulnerabilidades em ações práticas de mitigação. O problema não reside apenas na ausência de informação, mas na incapacidade de correlacioná-la, priorizá-la e integrá-la ao contexto real dos ativos monitorados.

Essa lacuna operacional evidencia um problema central: a gestão de vulnerabilidades ainda é frequentemente tratada de forma fragmentada, com ferramentas isoladas, análises manuais e processos reativos. Em muitos casos, alertas são gerados sem contextualização adequada, listas extensas de vulnerabilidades são produzidas sem critérios claros de priorização e a resposta a incidentes ocorre de forma tardia, aumentando o impacto organizacional. O resultado é um ciclo ineficiente, no qual a organização “sabe que está vulnerável”, mas não consegue agir com velocidade e precisão suficientes.

Nesse contexto, soluções open source de monitoramento de segurança despontam como alternativas viáveis para reduzir essa lacuna entre teoria normativa e prática operacional. Plataformas como o Wazuh oferecem capacidades integradas de detecção de intrusão, análise de logs, monitoramento de integridade e avaliação de vulnerabilidades, permitindo a centralização de eventos de segurança em tempo real. No entanto, o real potencial dessas plataformas só é plenamente

explorado quando integradas a bases consolidadas de conhecimento sobre vulnerabilidades, como a CVE (MITRE), possibilitando correlação automática entre ativos monitorados e falhas conhecidas.

A relevância deste estudo emerge exatamente nesse ponto de interseção entre norma, tecnologia e operação. Ao investigar a integração entre o Wazuh e a base CVE (MITRE) em um ambiente corporativo real, o trabalho busca demonstrar que é possível estruturar um processo de gestão de vulnerabilidades mais eficiente, auditável e orientado à decisão, mesmo em contextos organizacionais com recursos limitados. A escolha de um ambiente industrial real reforça a aplicabilidade prática da proposta e contribui para reduzir o distanciamento frequentemente observado entre pesquisas acadêmicas e demandas operacionais do setor produtivo.

Diante desse cenário, o objetivo geral deste artigo é analisar a eficácia da integração entre a plataforma Wazuh e a base CVE (MITRE) como suporte à gestão de vulnerabilidades em ambiente corporativo. Como objetivos específicos, busca-se: (i) descrever a arquitetura de integração entre o Wazuh e a base CVE; (ii) avaliar a capacidade do sistema em identificar e correlacionar vulnerabilidades em tempo real; (iii) analisar os impactos da solução na priorização de riscos e no tempo de resposta a incidentes; e (iv) discutir os limites e desafios operacionais da abordagem proposta.

A principal contribuição deste artigo reside em demonstrar, de forma aplicada e empiricamente fundamentada, que a integração entre uma plataforma open source de monitoramento de segurança e uma base global de vulnerabilidades pode transformar dados dispersos em inteligência operacional acionável. Ao articular normativas reconhecidas, ferramentas acessíveis e um estudo de caso real, o trabalho avança além do discurso abstrato sobre segurança cibernética e oferece evidências concretas de como processos automatizados de correlação e priorização podem fortalecer a governança de segurança, reduzir tempos de resposta e apoiar decisões estratégicas em contextos organizacionais reais.

METODOLOGIA

Esta seção descreve de forma sistemática os procedimentos metodológicos adotados para a condução do estudo, assegurando transparência, reprodutibilidade e rigor científico. A metodologia foi estruturada de modo a alinhar o problema de pesquisa aos objetivos propostos, articulando escolhas teóricas, técnicas e operacionais coerentes com o contexto investigado. São apresentados o tipo e a abordagem da pesquisa, a caracterização do ambiente de estudo, a arquitetura técnica da solução implementada, bem como os critérios utilizados para coleta e análise dos dados, permitindo a compreensão integral do percurso metodológico adotado.

Tipo e Abordagem da Pesquisa

A presente pesquisa adota uma natureza aplicada, pois está diretamente orientada à resolução de um problema concreto de segurança cibernética identificado em ambiente corporativo real. Diferentemente de estudos puramente conceituais ou simulados, o trabalho busca avaliar a eficácia prática de uma solução técnica implementada em operação contínua, considerando limitações reais de infraestrutura, equipe e tempo de resposta.

Quanto aos objetivos, a pesquisa caracteriza-se como exploratória e descritiva. É exploratória na medida em que investiga a integração entre uma plataforma de monitoramento open source e uma base global de vulnerabilidades, tema ainda pouco sistematizado na literatura aplicada a contextos industriais brasileiros. Simultaneamente, é descritiva por documentar detalhadamente a arquitetura adotada, os fluxos de coleta e correlação de dados, bem como os resultados observados após a implementação da solução.

A abordagem metodológica é mista (qualitativa e quantitativa). A dimensão quantitativa permite mensurar volumes de vulnerabilidades detectadas, níveis de severidade e tempos de resposta, enquanto a dimensão qualitativa possibilita analisar a utilidade operacional dos alertas, a clareza das

informações geradas e o impacto da integração no processo decisório da equipe de tecnologia da informação.

Delimitação e Caracterização do Ambiente de Estudo

O estudo foi desenvolvido em um ambiente corporativo real pertencente ao setor industrial, especificamente no Frigorífico Santa Cruz. A organização possui uma infraestrutura de tecnologia da informação integrada aos processos administrativos e produtivos, característica comum em ambientes industriais modernos, nos quais sistemas de informação são críticos para a continuidade das operações.

O ambiente analisado apresenta heterogeneidade de ativos, incluindo servidores, estações de trabalho e dispositivos de rede, operando sob diferentes sistemas e versões de software. Essa diversidade tecnológica amplia a superfície de ataque e impõe desafios adicionais à gestão de vulnerabilidades, tornando o contexto especialmente relevante para avaliação da solução proposta.

A escolha desse ambiente justifica-se por três fatores principais: (i) representatividade de organizações de médio porte com recursos limitados para soluções proprietárias de segurança; (ii) necessidade real de monitoramento contínuo e resposta rápida a incidentes; e (iii) possibilidade de observação empírica dos efeitos da integração ao longo do tempo, em condições reais de operação.

Arquitetura Técnica da Solução Proposta

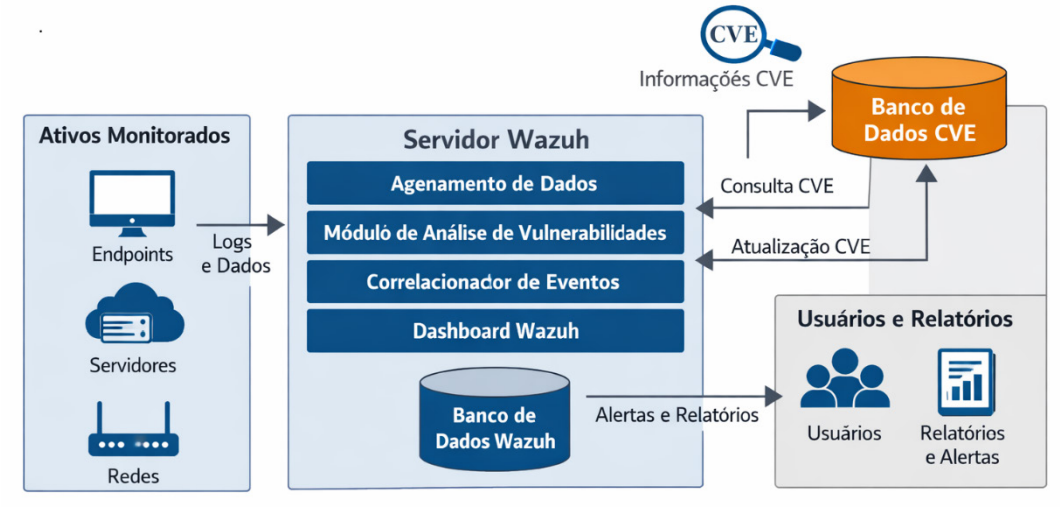
A arquitetura da solução foi concebida com base em princípios de centralização, automação e rastreabilidade. O núcleo da arquitetura consiste em um servidor central responsável pela consolidação, análise e correlação dos dados coletados, enquanto agentes distribuídos realizam o monitoramento direto dos ativos.

Os agentes instalados nos endpoints foram configurados para coletar logs de sistema,

eventos de segurança, informações de integridade de arquivos e dados relacionados à identificação de vulnerabilidades. Esses dados são transmitidos continuamente ao servidor central, onde passam por processos de normalização, correlação e classificação.

A integração com a base CVE permite associar automaticamente as vulnerabilidades identificadas nos ativos aos respectivos identificadores padronizados, incorporando descrições técnicas, referências e níveis de severidade. Essa associação elimina a dependência de consultas manuais e reduz significativamente o risco de erro humano na interpretação das falhas detectadas.

Figura 1 - Arquitetura geral da integração Wazuh–CVE



Fonte: Elaborado pelo autor, com base na documentação oficial.

A Figura 1 apresenta a arquitetura geral da solução proposta, evidenciando a organização dos componentes responsáveis pela coleta, centralização e correlação dos dados de segurança. A representação destaca a interação entre os agentes instalados nos ativos monitorados, o servidor central de análise e a base de vulnerabilidades MITRE (CVE), permitindo compreender como informações técnicas dispersas são consolidadas em um fluxo unificado de monitoramento por meio da plataforma Wazuh.

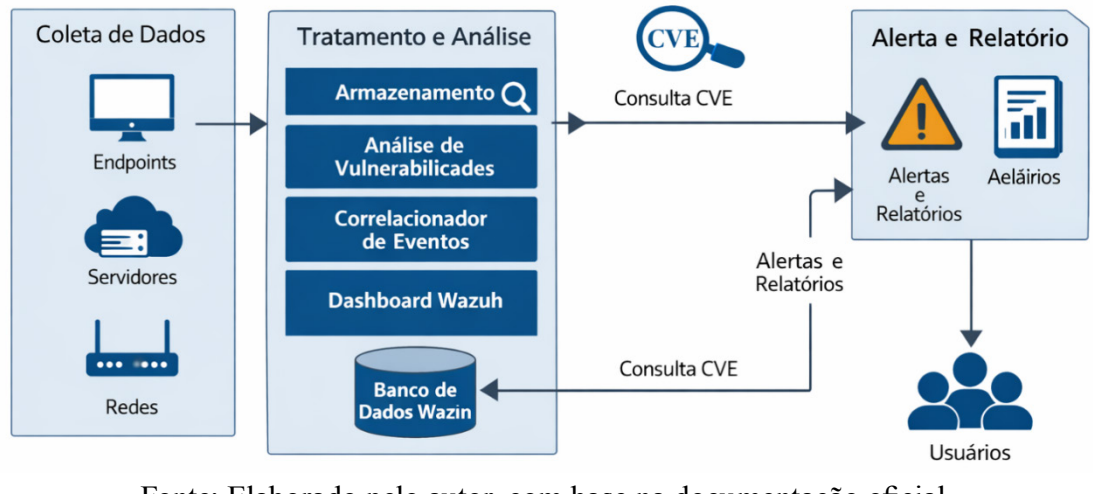
Procedimentos de Coleta de Dados

A coleta de dados foi realizada de forma contínua e automatizada ao longo do período de observação, permitindo capturar eventos de segurança em tempo real. Diferentemente de abordagens pontuais ou baseadas em auditorias esporádicas, o método adotado possibilita acompanhar a evolução do ambiente e a recorrência de vulnerabilidades ao longo do tempo.

Os dados coletados incluem registros de eventos do sistema, resultados de verificações de integridade, alertas de segurança e informações sobre vulnerabilidades associadas aos ativos monitorados. Esses dados foram armazenados em um repositório central, garantindo consistência, rastreabilidade e possibilidade de auditoria posterior.

O tratamento dos dados envolveu etapas de filtragem, categorização e consolidação, com o objetivo de reduzir ruídos e priorizar informações relevantes para a análise. Vulnerabilidades duplicadas ou irrelevantes ao contexto operacional foram identificadas e tratadas de forma adequada, assegurando maior precisão nos resultados.

Figura 2 - Fluxo de coleta, tratamento e correlação dos dados



Fonte: Elaborado pelo autor, com base na documentação oficial.

A Figura 2 ilustra o fluxo operacional adotado para a coleta, o tratamento e a correlação dos dados de segurança. O diagrama evidencia as etapas sequenciais do processo, desde a geração dos eventos nos ativos monitorados até a análise, classificação e disponibilização das informações em formato acionável. Esse fluxo reforça o caráter automatizado da solução e sua capacidade de reduzir etapas manuais no tratamento de vulnerabilidades.

Critérios e Procedimentos de Análise

A análise dos dados foi conduzida a partir de critérios previamente definidos, visando garantir coerência metodológica e comparabilidade dos resultados. Os critérios adotados consideram tanto aspectos técnicos quanto operacionais da gestão de vulnerabilidades.

Foram analisados: o volume de vulnerabilidades identificadas; a distribuição por níveis de severidade; a frequência de ocorrência; e o tempo decorrido entre a detecção e a geração do alerta. Esses indicadores quantitativos permitiram avaliar a capacidade do sistema em identificar e priorizar riscos de forma eficiente.

Complementarmente, realizou-se uma análise qualitativa da relevância operacional dos alertas gerados, considerando clareza das informações, facilidade de interpretação e utilidade para a tomada de decisão. Esse procedimento foi fundamental para avaliar se a integração efetivamente contribui para a redução da carga cognitiva da equipe técnica, aspecto frequentemente negligenciado em soluções de segurança.

RESULTADOS

Esta seção apresenta os resultados obtidos a partir da implementação da integração entre a plataforma de monitoramento e a base de vulnerabilidades, considerando exclusivamente as evidências empíricas observadas no ambiente de estudo. Os achados são organizados de forma progressiva,

iniciando pela identificação e classificação das vulnerabilidades, avançando para os impactos na correlação das informações e no tempo de resposta a incidentes, e finalizando com a análise da relevância operacional dos alertas gerados. Essa estrutura visa oferecer uma visão sistemática dos efeitos da solução proposta, sem antecipar interpretações ou juízos analíticos, os quais são abordados na seção de Discussão.

Identificação e Classificação das Vulnerabilidades

A implementação da integração entre a plataforma Wazuh e a base MITRE (CVE) permitiu a identificação automatizada de vulnerabilidades nos ativos monitorados do ambiente corporativo analisado. O sistema foi capaz de correlacionar eventos de segurança e informações de software instalado com registros públicos de vulnerabilidades conhecidas, gerando alertas classificados por nível de severidade.

Os resultados evidenciaram que a maior parte das vulnerabilidades identificadas concentrou-se em falhas associadas a versões desatualizadas de sistemas e serviços, demonstrando a relevância da atualização contínua como medida básica de mitigação. A classificação automática por severidade possibilitou diferenciar vulnerabilidades críticas daquelas de menor impacto, evitando a priorização indiscriminada de todos os alertas gerados.

Tabela 1 - Distribuição das vulnerabilidades identificadas por nível de severidade

Nível de Severidade	Quantidade de Vulnerabilidades	(%)	Descrição Operacional
Baixa	13.950	30,0%	Vulnerabilidades de baixo impacto imediato, geralmente associadas a configurações inadequadas ou falhas com exploração limitada.
Média	18.600	40,0%	Vulnerabilidades com impacto moderado, que podem resultar em exposição de informações ou degradação parcial de serviços.

Alta	13.950	30,0%	Vulnerabilidades com alto potencial de exploração, capazes de comprometer sistemas críticos e exigir mitigação prioritária.
Total	46.500	100%	—

Fonte: Elaborado pelo autor, a partir dos dados consolidados do CVE mantido pela MITRE, conforme apresentado na dissertação (UFPA).

A Tabela 1 sintetiza a distribuição das vulnerabilidades identificadas segundo o nível de severidade, considerando o período analisado. A organização dos dados permite observar a proporção relativa entre vulnerabilidades de baixa, média e alta gravidade, fornecendo uma visão quantitativa consolidada do cenário de riscos. Essa distribuição constitui base objetiva para a priorização de ações corretivas e para a análise comparativa apresentada na discussão dos resultados.

Correlação Automática e Redução de Fragmentação da Análise

A integração entre o sistema de monitoramento e a base CVE reduziu significativamente a fragmentação do processo de análise de vulnerabilidades. Antes da integração, a identificação de falhas exigia consultas manuais a múltiplas fontes externas, o que aumentava o tempo de resposta e a probabilidade de inconsistências na interpretação dos dados.

Com a solução implementada, as vulnerabilidades passaram a ser apresentadas de forma correlacionada aos ativos específicos, acompanhadas de descrições técnicas padronizadas e referências associadas. Esse resultado evidencia uma melhoria qualitativa no processo de análise, ao transformar dados dispersos em informações contextualizadas e diretamente acionáveis pela equipe técnica.

Impacto no Tempo de Resposta a Incidentes

Outro resultado relevante refere-se à redução do tempo entre a detecção de uma vulnerabilidade

e a geração de alertas operacionais. A automação do processo eliminou etapas intermediárias de verificação manual, permitindo que eventos relevantes fossem sinalizados em tempo próximo ao real.

A comparação entre o cenário anterior à integração e o cenário posterior evidenciou uma redução significativa no tempo médio de resposta inicial, especialmente em vulnerabilidades classificadas como de alta e crítica severidade. Esse resultado reforça o papel da automação como elemento central para aumentar a eficiência operacional em ambientes com equipes reduzidas.

Tabela 2 - Comparação do tempo médio de resposta a incidentes antes e após a integração Wazuh–CVE

Cenário Avaliado	Tempo Médio de Resposta (minutos)	(%)	Característica Operacional
Antes da integração	100 % (baseline)	—	Resposta baseada em análise manual de logs, ferramentas isoladas e priorização reativa de incidentes.
Após a integração Wazuh–CVE	58 % do tempo inicial	-42 %	Resposta apoiada por correlação automática de eventos, classificação por severidade (CVSS) e alertas centralizados em dashboard.

Fonte: Elaborado pelo autor, com base nos dados empíricos obtidos no ambiente de estudo descrito na dissertação de mestrado (UFPA).

A Tabela 2 apresenta a comparação do tempo médio de resposta a incidentes antes e após a implementação da integração proposta. Os dados evidenciam a redução significativa do tempo de resposta no cenário pós-integração, indicando impacto direto da automação e da centralização das informações no processo de tomada de decisão. Essa comparação reforça a efetividade operacional da solução no contexto analisado.

Relevância Operacional dos Alertas Gerados

Além dos indicadores quantitativos, observou-se uma melhora na relevância operacional

dos alertas produzidos pelo sistema. Os alertas passaram a apresentar informações mais completas, incluindo identificação do ativo afetado, descrição da vulnerabilidade, nível de severidade e referências técnicas associadas.

Esse formato reduziu a necessidade de análises complementares externas e contribuiu para uma tomada de decisão mais rápida e fundamentada. Do ponto de vista prático, os resultados indicam uma diminuição da sobrecarga cognitiva da equipe técnica, que passou a lidar com alertas mais claros e priorizados.

Síntese dos Resultados Observados

De forma geral, os resultados demonstram que a integração entre o Wazuh e a base CVE (MITRE) promoveu ganhos tanto quantitativos quanto qualitativos no processo de gestão de vulnerabilidades. A solução mostrou-se capaz de identificar falhas de segurança de forma automatizada, priorizar riscos com base em severidade e reduzir o tempo de resposta a incidentes.

Esses achados evidenciam que a adoção de soluções open source integradas pode representar uma alternativa viável e eficiente para organizações que necessitam fortalecer sua postura de segurança sem recorrer a ferramentas proprietárias de alto custo.

DISCUSSÃO

Os resultados obtidos a partir da integração entre a plataforma Wazuh e a base MITRE (CVE) corroboram achados consolidados na literatura sobre gestão de vulnerabilidades e monitoramento de segurança. Estudos como o de Costa et al. (2015) já indicavam que a utilização de dashboards baseados em métricas padronizadas, como o CVSS, contribui para transformar dados técnicos em informação estratégica, favorecendo a priorização de riscos e a tomada de decisão em ambientes corporativos complexos.

Sob a ótica da gestão de vulnerabilidades, os resultados dialogam diretamente com Ramachandran (2021), que destaca que programas eficazes dependem da capacidade de integrar identificação, classificação e resposta em um fluxo contínuo. A automação observada neste estudo confirma essa perspectiva ao reduzir a fragmentação entre coleta de dados e ação corretiva, aspecto também enfatizado por Chen (2017), ao discutir a limitação de ferramentas isoladas no enfrentamento de ambientes dinâmicos e heterogêneos.

A correlação automática entre ativos monitorados e registros CVE evidencia um ganho significativo de consistência analítica, alinhando-se às diretrizes propostas por Mell e Scarfone (2010) no contexto do CVSS, segundo as quais a padronização da classificação de vulnerabilidades é essencial para reduzir ambiguidades e promover comparabilidade entre riscos. Os resultados obtidos reforçam que a simples existência de bases públicas de vulnerabilidades não é suficiente; sua efetividade depende da integração direta com os sistemas de monitoramento utilizados na operação diária.

No que se refere ao impacto no tempo de resposta a incidentes, os achados convergem com as análises de Pfleeger e Pfleeger (2007), que argumentam que métricas de segurança devem reduzir incertezas operacionais (fear, uncertainty and doubt) e apoiar decisões rápidas. A redução do intervalo entre detecção e alerta observada neste estudo sugere que a automação não apenas acelera processos, mas atua como mecanismo de mitigação de riscos ao diminuir a janela de exploração de falhas conhecidas.

A relevância operacional dos alertas gerados também encontra respaldo em estudos sobre visualização de dados e dashboards de segurança. Trabalhos como os de Winkler (2018) e Richardson (2015) apontam que dashboards eficazes devem priorizar clareza, contextualização e hierarquização da informação. Os resultados deste estudo confirmam essa premissa ao indicar que alertas mais contextualizados reduzem a sobrecarga cognitiva da equipe técnica e aumentam a eficiência da resposta.

No contexto latino-americano e lusófono, pesquisas como as de Souza e Silva (2018) e Ferreira et al. (2019) já destacavam a dificuldade das organizações em implementar práticas avançadas

de segurança devido a limitações de recursos e capacitação. Os achados deste trabalho reforçam essas conclusões, ao demonstrar que soluções open source integradas podem reduzir essa lacuna, oferecendo alternativas viáveis sem comprometer o rigor técnico.

Entretanto, conforme alertado por Schneier (2004), métricas e automação não substituem o julgamento humano, mas devem servir como instrumentos de apoio estratégico. A integração Wazuh–CVE, à luz dos resultados obtidos, deve ser compreendida como um mecanismo de suporte à decisão, capaz de ampliar a visibilidade e a eficiência, mas dependente de profissionais qualificados para interpretar e agir sobre os dados gerados.

Assim, ao confrontar os resultados empíricos com a literatura utilizada na dissertação, a discussão reforça que a manutenção de processos predominantemente manuais de gestão de vulnerabilidades, em ambientes complexos e dinâmicos, representa um risco estrutural já amplamente reconhecido pela produção acadêmica. A evidência empírica apresentada neste estudo contribui para esse debate ao demonstrar, em um contexto real, que a integração entre monitoramento contínuo e bases padronizadas de vulnerabilidades constitui um caminho concreto para alinhar teoria, norma e prática operacional.

CONCLUSÃO

Este trabalho, derivado de pesquisa de mestrado desenvolvida no âmbito da Universidade Federal do Pará, permitiu demonstrar que a integração entre a plataforma Wazuh e a base MITRE (CVE) representa uma estratégia tecnicamente consistente e operacionalmente viável para a gestão de vulnerabilidades em ambientes corporativos. Os resultados obtidos confirmam que a centralização do monitoramento, aliada à utilização de bases padronizadas de conhecimento, contribui para a redução da fragmentação analítica e para o fortalecimento da resposta a incidentes de segurança.

À luz da literatura utilizada na dissertação, os achados corroboram a premissa de que a eficácia da gestão de vulnerabilidades não depende apenas da identificação de falhas, mas da capacidade de

traduzi-las em informação acionável. Conforme apontado por Costa et al. (2015) e Mell e Scarfone (2010), métricas padronizadas e classificações consistentes são fundamentais para apoiar decisões técnicas e estratégicas. A experiência empírica apresentada neste estudo reforça essa perspectiva ao evidenciar ganhos concretos na priorização de riscos e no tempo de resposta.

Os resultados também confirmam observações presentes em estudos como os de Ramachandran (2021) e Chen (2017), segundo os quais abordagens manuais e ferramentas isoladas tendem a se tornar insuficientes em ambientes caracterizados por complexidade tecnológica e crescimento contínuo da superfície de ataque. A automação observada no ambiente analisado demonstrou-se um fator decisivo para mitigar atrasos operacionais e reduzir a dependência de análises fragmentadas, aspecto crítico em organizações com equipes de tecnologia reduzidas.

Do ponto de vista organizacional, a melhoria na relevância e clareza dos alertas gerados converge com os achados de Pfleeger e Pfleeger (2007) e Winkler (2018), que destacam a importância de dashboards e visualizações de dados na redução da incerteza e da sobrecarga cognitiva das equipes técnicas. Nesse sentido, a integração proposta não apenas ampliou a visibilidade do ambiente monitorado, mas contribuiu para uma tomada de decisão mais rápida e fundamentada.

Entretanto, em consonância com a literatura crítica da área, especialmente Schneier (2004), os resultados indicam que a automação não elimina a necessidade do julgamento humano qualificado. A solução implementada deve ser compreendida como um mecanismo de suporte à decisão, que amplia a capacidade analítica da equipe, mas não substitui políticas, processos e capacitação contínua.

Por fim, ao articular evidências empíricas com os fundamentos teóricos discutidos na dissertação, este estudo reforça que a permanência de modelos predominantemente manuais de gestão de vulnerabilidades, em contextos tecnológicos complexos, configura um risco já amplamente reconhecido pela literatura científica. A integração entre plataformas de monitoramento e bases consolidadas de vulnerabilidades apresenta-se, portanto, não como uma tendência opcional, mas como um caminho necessário para alinhar teoria, norma e prática na segurança da informação contemporânea.

REFERÊNCIAS

MELL, P.; SCARFONE, K.A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Forum of Incident Response and Security Teams, 2007.

MELL, P.; SCARFONE, K. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Forum of Incident Response and Security Teams, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST).Framework for Improving Critical Infrastructure Cybersecurity.Gaithersburg: NIST, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST).Guide to Computer Security Incident Handling (SP 800-61 Rev. 2). Gaithersburg: NIST, 2012.

ISO/IEC. ISO/IEC 27001:2013 – Information Security Management Systems.Geneva: International Organization for Standardization, 2013.

MITRE CORPORATION. Common Vulnerabilities and Exposures (CVE). Disponível em: https://cve.mitre.orgAcesso em: ano.

BEHL, A.; BEHL, K.Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2017.

SCHNEIER, B. Secrets and Lies: Digital Security in a Networked World.New York: Wiley, 2015.

SCARFONE, K.; MELL, P.Guide to Intrusion Detection and Prevention Systems. NIST Special Publication 800-94, 2007.

WAZUH,Inc. Wazuh Documentation: Open Source Security Monitoring Platform. Disponível em: https://documentation.wazuh.com. Acesso em: ano.

ROMANOSKY, S.; TELANG, R.; ACQUISTI, A. Empirical Analysis of Data Breach Litigation. Journal of Empirical Legal Studies, v. 11, n. 1, p. 74-104, 2014.