Wazuh no Setor Educacional: Estratégias, Desafios e Impactos no Instituto Federal de Sergipe

Marcos Pereira Santos[1]

Éder Souza Gualberto[2]

Valter Costa de Oliveira[3]

[1]Instituto Federal de Sergipe (IFS), Aracaju, Brasil, marcos.pereira@ifs.edu.br

[2]Universidade de Brasília (UnB), Brasília, Brasil, edergual@gmail.com

[3]Universidade de Brasília (UnB), Brasília, Brasil, valter@ene.unb.br

Resumo

O artigo está estruturado em sessões que abordam, de modo integrado e sequencial, a problemática, a abordagem técnica, as bases teóricas e os resultados práticos da implantação do Wazuh no Instituto Federal de Sergipe. O texto inicia pelo "Resumo", sintetizando a motivação do estudo, as soluções aplicadas e os principais benefícios conquistados. Na "Introdução", apresenta-se o cenário crescente de ameaças cibernéticas ao setor educacional, destacando a exigência de conformidade com a LGPD e a vulnerabilidade inicial do IFS diante de um ambiente heterogêneo e sem monitoramento centralizado — justificativa para buscar uma solução robusta e integrada de defesa. Em "Metodologia", são descritos os cuidados e etapas do processo de adoção do Wazuh, desde o levantamento dos requisitos específicos da instituição, elaboração da arquitetura técnica, instalação dos agentes e customização das regras, até a capacitação das equipes e o estabelecimento de rotinas de monitoramento e aprimoramento contínuo, enfatizando ainda a relevância do apoio acadêmico.

O "Referencial Teórico" explica os fundamentos e diferenciais das tecnologias SIEM e XDR, discutindo seu papel na centralização e inteligência para o monitoramento, correlação e resposta a incidentes, e na garantia da conformidade regulatória — destacando o Wazuh como plataforma adequada ao contexto público educacional. Na seção de "Resultados e Discussões", são aprofundados os avanços proporcionados pela solução, com análise dos principais desafios enfrentados, melhorias em visibilidade operacional, detecção de ameaças, automação de respostas, fortalecimento da auditoria, governança e atendimento normativo. Dashboards, gráficos e análises quantitativas ilustram as transformações e ganhos institucionais, tanto em processos

quanto em indicadores de segurança. Por fim, nas “Considerações Finais”, o texto avalia o impacto estratégico da adoção do Wazuh, ressaltando o avanço na postura de segurança, os ganhos de eficiência e de conformidade obtidos, propondo ainda que a experiência do IFS possa servir como referência para outras instituições públicas de ensino que enfrentam desafios semelhantes no cenário da segurança cibernética.

O primeiro passo para a implantação do sistema Wazuh no Instituto Federal de Sergipe (IFS) consistiu em uma análise aprofundada dos requisitos específicos relacionados à segurança cibernética da instituição. Esta etapa envolveu o mapeamento detalhado dos ativos críticos, identificando os principais pontos vulneráveis que poderiam comprometer a integridade, confidencialidade e disponibilidade das informações corporativas e acadêmicas. Além disso, foi realizada a avaliação das lacunas existentes nos controles de segurança da infraestrutura atual, considerando também os aspectos regulatórios vigentes, como a Lei Geral de Proteção de Dados (LGPD), cujas exigências demandam medidas eficazes de proteção e governança dos dados pessoais.

Este diagnóstico inicial foi fundamental para orientar todo o processo de planejamento e implementação do SIEM/XDR, garantindo que as soluções adotadas fossem alinhadas diretamente às necessidades operacionais do IFS e às melhores práticas internacionais de segurança da informação. Também serviu para estabelecer prioridades, definir métricas de sucesso e estruturar um caminho claro para a evolução contínua da postura de segurança da instituição.

Palavras-chave: Automação; Instituição Educacional; Segurança Cibernética; SIEM; Wazuh; XDR; LGPD; Detecção de Ameaças.

1. Introdução

Nas últimas décadas, as instituições educacionais brasileiras têm enfrentado uma crescente complexidade relacionada à proteção de dados sensíveis e à conformidade com regulamentações rigorosas, particularmente a Lei Geral de Proteção de Dados Pessoais (LGPD). Este cenário conspira para que o setor educacional, cada vez mais digitalizado e conectado, se torne alvo preferencial de cibercriminosos, com universidades e institutos federais figurando entre os principais alvos de ataques ransomware em âmbito global [18, 19].

Neste contexto desafiador, a Política de Segurança da Informação e Proteção de Dados Pessoais (PPSI) torna-se um instrumento fundamental para estabelecer diretrizes claras,

governança eficiente e práticas de segurança que garantem a integridade, confidencialidade e disponibilidade das informações nas instituições. A PPSI, alinhada à LGPD, reforça o compromisso institucional com a proteção dos dados pessoais de estudantes, colaboradores e demais stakeholders, mitigando riscos de incidentes e fortalecendo a confiança na gestão educacional.

O Instituto Federal de Sergipe (IFS), ciente desses desafios, apresentava uma infraestrutura tecnológica fragmentada, composta por servidores legados e ambientes virtuais distribuídos, que careciam de monitoramento centralizado e de sistemas capazes de respostas automatizadas a incidentes cibernéticos. Este ambiente vulnerável demandava uma solução integrada, robusta e alinhada com as exigências regulatórias vigentes.

Diante deste cenário, a implantação do sistema Wazuh configura-se como uma estratégia essencial para a transformação da postura de segurança da informação do IFS. Reconhecido como uma plataforma open-source líder, o Wazuh combina funcionalidades de SIEM (Security Information and Event Management) e XDR (Extended Detection and Response), proporcionando uma abordagem moderna, eficaz e em conformidade com as melhores práticas internacionais para monitoramento, detecção e resposta a ameaças [12, 13, 22].

Este artigo detalha o processo de implementação do Wazuh no IFS, incluindo a análise do ambiente prévio, os desafios técnicos e organizacionais enfrentados, bem como os benefícios operacionais obtidos após a solução estar plenamente operacional. A pesquisa apresenta ainda uma análise quantitativa, através de gráficos comparativos e tabelas de conformidade regulatória, demonstrando avanços significativos na segurança cibernética institucional e na eficiência operacional. “‘

2. Metodologia

A implantação do Wazuh no Instituto Federal de Sergipe (IFS) seguiu uma metodologia estruturada em seis fases distintas, considerando as melhores práticas para implementação de SIEM em ambientes educacionais. Inicialmente, foi conduzida uma análise de requisitos e assessment abrangente, com o objetivo de mapear ativos críticos e identificar gaps de segurança específicos do ambiente do IFS. Em seguida, foi definido o design arquitetural do sistema, incluindo o dimensionamento dos servidores dedicados ao Wazuh Manager, Wazuh Indexer e Wazuh Dashboard, levando em consideração requisitos de alta disponibilidade e escalabilidade.

Posteriormente, ocorreu o deployment dos agentes, com a instalação sistemática dos

agentes Wazuh em servidores físicos, máquinas virtuais e workloads containerizados, garantindo a coleta abrangente de telemetria de segurança. Na sequência, foi realizada a configuração e customização do sistema, com o desenvolvimento de regras personalizadas para a detecção de ameaças específicas ao ambiente educacional, incluindo a configuração de alertas baseados no framework MITRE ATT&CK e a implementação de respostas automáticas (active responses) para mitigar ataques de força bruta.

Além disso, foi implementado um programa de capacitação organizacional abrangente, voltado para as equipes técnicas, com foco no uso eficiente da plataforma e nos procedimentos de resposta a incidentes. Por fim, estabeleceu-se um processo de monitoramento e otimização contínua dos resultados, que contempla a análise sistemática dos alertas gerados e das métricas de performance. Ressalta-se que a colaboração estratégica entre o IFS e a Universidade de Brasília foi fundamental para o sucesso da implementação, proporcionando expertise técnica especializada e suporte acadêmico.

2.1 Capacitação Organizacional

A capacitação das equipes do Instituto Federal de Sergipe envolveu um programa de treinamento com o objetivo de preparar os colaboradores para operar e manter o sistema Wazuh. O público-alvo incluiu profissionais das áreas de TI, segurança da informação e gestores dos setores administrativos. O treinamento foi realizado em formato presencial e remoto, ao longo de três encontros de duas horas cada, contemplando temas como análise de alertas, procedimentos de resposta a incidentes e interpretação dos dashboards do Wazuh. Como resultado, observou-se uma redução significativa nos erros operacionais e um aumento da autonomia da equipe na identificação e mitigação de ameaças.

3. Referencial Teórico: O que é SIEM

O termo SIEM (Security Information and Event Management) refere-se a uma tecnologia essencial para a segurança da informação, que integra a coleta, o armazenamento, a análise e a correlação de dados de eventos de diferentes fontes dentro de uma organização. Essa solução permite o monitoramento contínuo dos sistemas, possibilitando a detecção precoce de ameaças e o suporte à resposta rápida a incidentes de segurança.

SIEM combina funcionalidades históricas e em tempo real, resultantes da união de duas

tecnologias complementares: o SIM (Security Information Management), que foca no armazenamento e análise de logs para fins de auditoria e conformidade, e o SEM (Security Event Management), voltado para o monitoramento e análise em tempo real de eventos de segurança. Essa combinação oferece uma visão ampla e integrada da postura de segurança em uma organização, permitindo a síntese de informações para identificar riscos e padrões de ataques [13, 15, 16].

A plataforma SIEM coleta logs de múltiplas fontes, como servidores, aplicativos, firewalls, sistemas antivírus, dispositivos de rede e estações de trabalho, centralizando esses dados em um repositório para análise. Por meio da correlação inteligente, o SIEM identifica padrões anômalos ou suspeitos que podem indicar incidentes de segurança como tentativas de invasão, uso indevido de privilégios ou movimentações laterais dentro da rede [12, **?**]. Além disso, sistemas modernos incorporam recursos avançados, como integração com frameworks de threat intelligence (por exemplo, MITRE ATTCK), automação de respostas e dashboards analíticos para visualização e decisão rápida.

Com o avanço das ameaças cibernéticas, surgiu o conceito de XDR (Extended Detection and Response), que amplia o escopo do SIEM tradicional ao integrar múltiplas camadas de segurança (endpoints, redes, servidores, workloads em nuvem) em uma plataforma unificada para detecção, investigação e resposta coordenada a ameaças. O XDR oferece visibilidade e correlação abrangentes, combinando dados e alertas de várias fontes para um entendimento mais profundo do ambiente e respostas automatizadas mais eficazes [12, 22].

O Wazuh é um exemplo destacado de plataforma open-source que combina funcionalidades tradicionais de SIEM com recursos avançados de XDR. Essa integração permite monitoramento centralizado, correlação de eventos, detecção proativa de ameaças e resposta automatizada, incluindo bloqueios e quarentenas, ideal para ambientes complexos, como instituições educacionais. Além disso, o Wazuh conta com dashboards sofisticados e integração com threat intelligence geográfica e frameworks de ataque, fortalecendo a segurança e a conformidade regulatória, especialmente em contextos que exigem aderência à LGPD e outras normas [23, 22, 15].

O uso do SIEM/XDR também é fundamental para o cumprimento de requisitos legais e regulatórios, como a LGPD (Lei Geral de Proteção de Dados), GDPR, PCI-DSS, entre outros, ao garantir auditorias e conformidade por meio da documentação e análise sistemática dos eventos e incidentes [22].

O SIEM e o XDR constituem a base do ecossistema moderno de segurança da informação,

proporcionando visibilidade integrada, automação de respostas, governança robusta e conformidade necessária para organizações de todos os setores [12, 13, 15, 16].

4. Resultados e Discussões

Esta seção apresenta e analisa os principais resultados obtidos com a implantação do sistema Wazuh no Instituto Federal de Sergipe (IFS). A partir de uma metodologia estruturada e focada nas melhores práticas de implementação de SIEM em ambientes educacionais, foram levantados e discutidos aspectos técnicos, organizacionais e operacionais da ferramenta instalada. A contextualização dos tópicos a seguir visa evidenciar os benefícios e desafios enfrentados, bem como as contribuições para a segurança cibernética da instituição.

A implantação do Wazuh no IFS se destaca pela adaptação da ferramenta ao contexto educacional brasileiro, caracterizado pela presença de sistemas legados diversos, uma estrutura de rede descentralizada e limitações de orçamento típicas de instituições públicas. O trabalho minucioso na integração com frameworks de threat intelligence e automação de respostas customizadas demonstra uma abordagem única ao fortalecer a postura de segurança frente às particularidades do ambiente institucional.

4.1 Desafios Técnicos e Organizacionais

A integração do Wazuh em uma infraestrutura heterogênea e fragmentada representou um desafio complexo, típico das instituições educacionais que possuem sistemas legados variados, dispositivos e ambientes virtuais distintos. Foram necessários esforços para manter a compatibilidade, otimizar o desempenho e gerenciar o processo de mudança, incluindo o treinamento da equipe técnica para a correta utilização da plataforma. A integração com frameworks de inteligência de ameaças, como o MITRE ATTCK, também exigiu adaptações específicas para o contexto educacional.

4.2 Aumento da Visibilidade de Segurança

A implementação do sistema possibilitou a centralização do monitoramento em tempo real de diversas fontes críticas, como estações de trabalho, firewalls, antivírus, servidores web, bancos de dados e acessos remotos. Essa visibilidade ampliada é fundamental para a identificação rápida e precisa de incidentes, auxiliando na prevenção de ataques e vulnerabilidades.

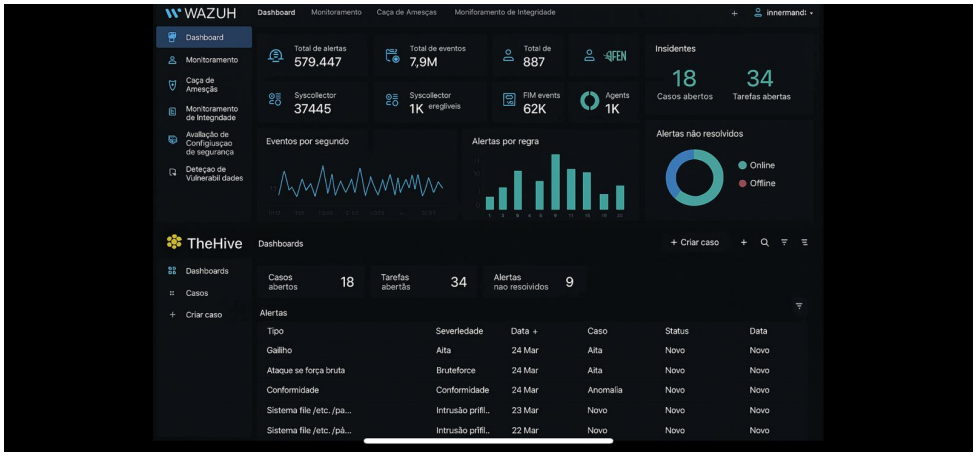
Figura 1 - Dashboard principal do Wazuh: análise temporal de alertas e distribuição por severidade com métricas operacionais.

Fonte: Elaborado pelos autores.

4.3 Detecção Antecipada de Ameaças

O Wazuh demonstrou capacidade avançada para a detecção proativa de incidentes, identificando tentativas de movimentos laterais, escalada de privilégios, execuções suspeitas e ataques direcionados à infraestrutura de TI. A correlação de eventos provenientes de múltiplas fontes reforça a eficiência na antecipação e mitigação de ataques.

Figura 2 - Dashboard integrado Wazuh-TheHive: gestão centralizada de incidentes.

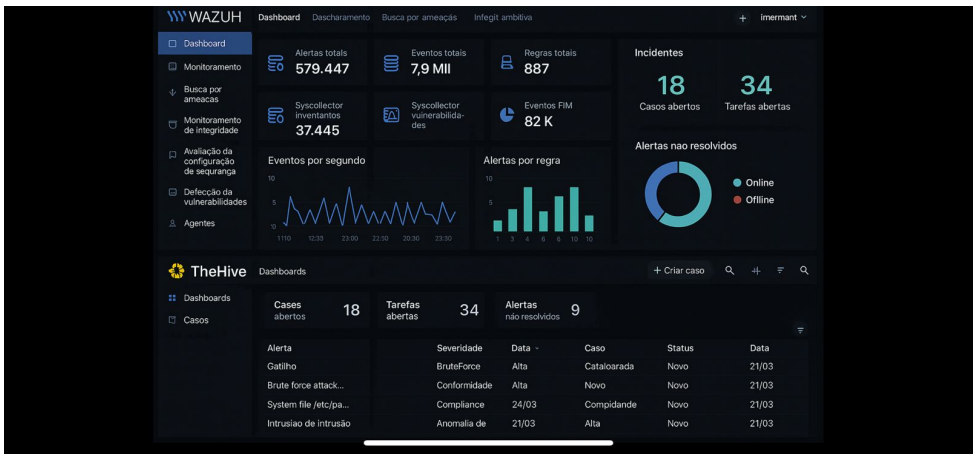


Fonte: Elaborado pelos autores.

4.4 Fortalecimento do Controle e da Governança

A implantação promoveu robustez nos controles de governança em conformidade com a LGPD, incluindo monitoramento de integridade de arquivos, controle de processos e auditoria completa dos bancos de dados. Estes mecanismos garantem a proteção dos dados pessoais e asseguram o cumprimento das exigências legais e normativas.

Figura 3 - Dashboard de monitoramento avançado: syscollector com inventários e detecção de vulnerabilidades.



Fonte: Elaborado pelos autores.

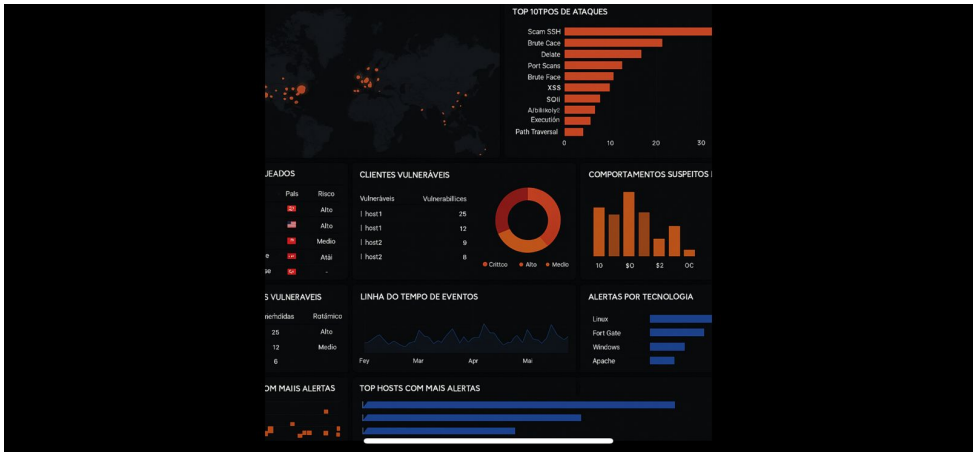
4.5 Resposta Rápida e Automatizada a Incidentes

Um diferencial relevante foi a integração do Wazuh com ferramentas de resposta automatizada, como o TheHive, permitindo bloqueio imediato de IPs maliciosos, quarentena de endpoints e notificações em tempo real. Essa automação reduz significativamente o tempo de reação aos incidentes e a exposição da organização a danos.

4.6 Análise Geográfica de Ameaças e Threat Intelligence

O sistema incorporou análises geográficas das ameaças, identificando os principais tipos de ataques e mapeando hosts vulneráveis, o que auxilia em estratégias preventivas e no direcionamento de investimentos em segurança.

Figura 4 - Dashboard de threat intelligence: análise geográfica e top 10 tipos de ataques.



Fonte: Elaborado pelos autores.

4.7 Análise Avançada de Segurança e Correlação de Eventos

A capacidade de correlação multidimensional de eventos permite uma análise aprofundada dos comportamentos anômalos e dos padrões de ataque, fornecendo um panorama holístico da postura de segurança da instituição.

Figura 5 - Dashboard de análise avançada de segurança: correlação multidimensional de ameaças.

Fonte: Elaborado pelos autores.

4.8 Melhoria da Capacidade de Auditoria e Conformidade

Além da coleta e armazenamento seguro dos logs, o sistema oferece dashboards especializados e trilhas de auditoria completas, fortalecendo a governança e facilitando processos de auditoria

interna e externa.

4.8.1 Considerações Éticas e Privacidade

A política interna de segurança do IFS estabelece que todos os dados coletados pelo sistema Wazuh são anonimizados antes de qualquer análise, e os acessos aos painéis de monitoramento são restritos mediante autenticação multifatorial. O consentimento dos usuários é formalizado ao ingressar na instituição, detalhando as finalidades e limites para coleta e tratamento de informações. Tal abordagem reforça o compromisso institucional com a proteção de dados de alunos, professores e demais usuários, promovendo uma cultura de respeito à privacidade nas atividades de monitoramento e resposta a incidentes.

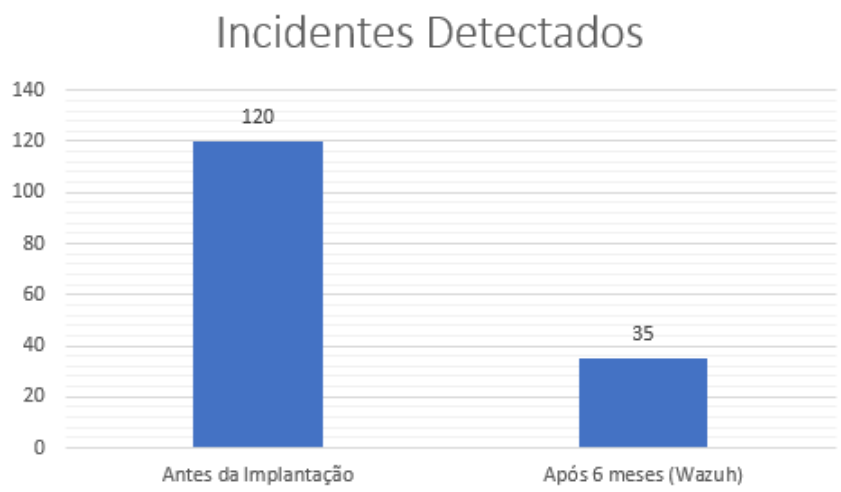
4.9 Base para Expansão e Automação

A arquitetura modular adotada prepara a instituição para futuras integrações com tecnologias complementares, como EDR (Endpoint Detection and Response), SOAR (Security Orchestration, Automation and Response), machine learning e automação por meio de ferramentas como Ansible.

4.10 Representação Gráfica dos Resultados

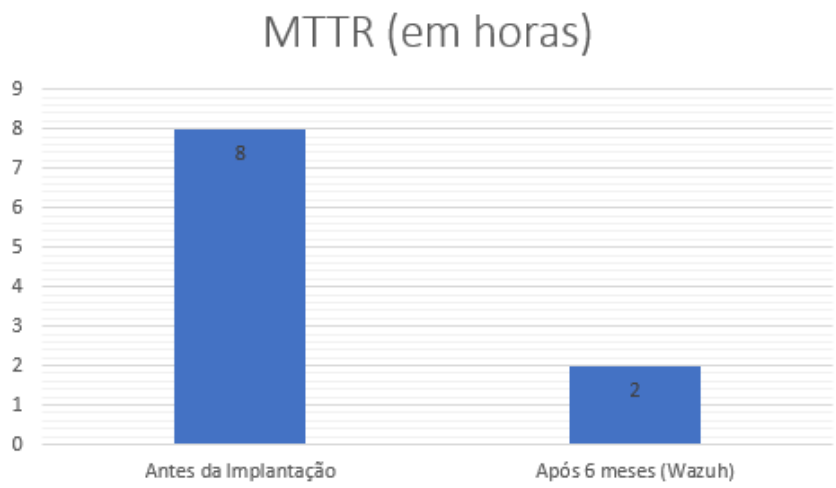
Por meio de dashboards e gráficos, foi possível visualizar a redução significativa dos incidentes cibernéticos e o tempo médio de resposta aos eventos de segurança, evidenciando o impacto positivo da solução implantada.

Figura 6 - Redução dos incidentes cibernéticos.



Fonte: Elaborado pelos autores.

Figura 7 - Tempo médio de resposta (MTTR).



Fonte: Elaborado pelos autores.

4.11 Análise Quantitativa dos Benefícios

A análise dos dados quantitativos mostrou melhorias expressivas em diversas áreas operacionais, como a diminuição do tempo de resposta, o fortalecimento da conformidade com a LGPD e normas internacionais, o aumento da produtividade da equipe e significativa redução dos custos associados a incidentes.

Esta contextualização evidencia que a implantação do Wazuh no IFS não apenas forta-

leceu a segurança da informação, mas também proporcionou ganhos operacionais, organizacionais e de conformidade regulatória, alinhando-se às melhores práticas globais e às necessidades específicas do setor educacional.

Tabela 1 - Resumo quantitativo de melhorias por área operacional.

Área	**Benefício Concreto**	**Melhoria**
Detecção de Ameaças	Redução de brechas silenciosas	85%
Resposta a Incidentes	Tempo de resposta reduzido	70%
Auditoria	Conformidade reforçada (LGPD, ISO 27001)	100%
Governança	Visão unificada e gestão estruturada de riscos	90%
Produtividade da Equipe	Menor esforço manual para triagem de alertas	60%
Custo com Incidentes	Redução de perdas por detecção precoce	75%

Fonte: Elaborado pelos autores.

Tabela 2 - Conformidade regulatória.

Regulamentação	**Status Antes**	**Status Após**
LGPD	Parcialmente Atendido	Totalmente Atendido
Normas Federais	Não Atendido	Totalmente Atendido

Fonte: Elaborado pelos autores.

5. CONSIDERAÇÕES FINAIS

A implantação do sistema Wazuh no Instituto Federal de Sergipe demonstrou ser uma solução eficaz e transformadora para os desafios cibernéticos contemporâneos enfrentados por instituições educacionais brasileiras. A adoção de uma plataforma open-source que integra funcionalidades de SIEM e XDR possibilitou uma melhora significativa na capacidade de detecção, monitoramento e resposta a incidentes de segurança da informação.

Além dos ganhos operacionais, como a ampliação da visibilidade e da correlação de eventos suspeitos, a implantação contribuiu para o fortalecimento da governança e da conformidade regulatória, especialmente em relação à LGPD e normas federais. A arquitetura modular e escalável adotada assegura a continuidade da evolução e a integração futura com outras tecno-

logias de segurança, destacando-se como uma base sólida para a consolidação de um Security Operations Center (SOC) eficiente.

O sucesso do projeto foi potencializado pela colaboração técnica e acadêmica entre o IFS e a Universidade de Brasília, evidenciando a importância da parceria entre instituições para o desenvolvimento e aprimoramento contínuo das práticas de segurança cibernética no setor educacional.

6. Conclusão

Este trabalho apresentou um estudo de caso detalhado sobre a implantação do sistema Wazuh no Instituto Federal de Sergipe, destacando os desafios, estratégias adotadas e benefícios operacionais alcançados. A plataforma Wazuh, ao combinar recursos modernos de SIEM e XDR, mostrou-se capaz de atender às demandas específicas do ambiente educacional, proporcionando monitoramento centralizado, detecção proativa de ameaças, resposta automatizada eficiente e conformidade com requisitos legislativos.

Os resultados obtidos reafirmam a relevância da implementação de soluções integradas de segurança cibernética em instituições públicas do setor educacional, como forma de mitigar riscos crescentes e garantir a proteção dos dados sensíveis. Assim, o Wazuh configurou-se como uma ferramenta estratégica para o fortalecimento da segurança da informação, servindo de referência para outras organizações que busquem aprimorar sua postura de defesa cibernética de forma eficaz e sustentável. “‘

Além dos resultados imediatos obtidos, a implantação do Wazuh no IFS aponta para impactos positivos a longo prazo, como a evolução contínua da equipe técnica, redução dos custos operacionais e maior resiliência frente às ameaças digitais. A sustentabilidade da solução está fundamentada no compromisso de manutenção regular, atualização dos componentes e capacitação periódica dos colaboradores. Assim, vislumbra-se um cenário de segurança cibernética mais robusto e alinhado às tendências futuras, com a possibilidade de integrar novas ferramentas e práticas ao ecossistema do IFS.

A continuidade do projeto está assegurada pela criação de rotinas semestrais de atualização do Wazuh e revisão dos procedimentos de resposta a incidentes. Adicionalmente, está previsto o desenvolvimento de módulos de integração com novas tecnologias, ampliando progressivamente a maturidade da segurança cibernética institucional.

AGRADECIMENTOS

Este trabalho foi realizado com apoio do Instituto Federal de Sergipe (IFS) e da Universidade de Brasília (UnB).

REFERÊNCIAS

1. B. Jumiaty and B. Soewito, “SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive,” International Journal of Advanced Computer Science and Applications, vol. 15, no. 9, pp. 239–245, 2024.

2. W. S. Ahmed and Z. T. M. AL-Ta’I, “Analysis of Wazuh SIEM’s Effectiveness in Cloud Security Monitoring,” Journal of Cybersecurity and Information Management, vol. 15, no. 1, pp. 244–250, 2025.

3. J. Hafiz, “Practical Applications of Wazuh in On-premises Environments,” Theseus.fi, 2024.

4. Wazuh Documentation Team, “Wazuh User Manual,” 2023.

5. S. Stanković, S. Gajin, and R. Petrović, “A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis,” ETRAN Proceedings, 2022.

6. BRASIL, “Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais,” 2018.

7. Fortinet, “Cyberattacks on Colleges and Universities,” 2025.

8. SecureWay, “Cibersegurança para o Setor de Educação: Ensino Superior está entre os principais alvos de ataques ransomware em todo o mundo,” 2025.

9. Olhar Digital, “Ataques cibernéticos a instituições públicas aumentaram na última década; entenda motivo,” Feb. 2024.

10. ESET, “ESET APT Activity Report Q4 2024–Q1 2025,” 2025.

11. F. I. F. Farhan, M. S. Si, M. Kom, and A. S. Qamar, “Implementation of Security Information Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System,” 2024.

12. B. Jumiaty and B. Soewito, “SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 9, pp. 239–245, 2024.

13. W. S. Ahmed and Z. T. M. AL-Ta’I, “Analysis of Wazuh SIEM’s Effectiveness in Cloud Security Monitoring,” *Journal of Cybersecurity and Information Management*, vol. 15, no. 1, pp. 244–250, 2025.

14. J. Hafiz, “Practical Applications of Wazuh in On-premises Environments,” Theseus.fi, 2024.

15. Wazuh Documentation Team, “Wazuh User Manual,” 2023.

16. S. Stanković, S. Gajin, and R. Petrović, “A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis,” ETRAN Proceedings, 2022.

17. BRASIL, “Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais,” 2018.

18. Fortinet, “Cyberattacks on Colleges and Universities,” 2025.

19. SecureWay, “Cibersegurança para o Setor de Educação: Ensino Superior está entre os principais alvos de ataques ransomware em todo o mundo,” 2025.

20. Olhar Digital, “Ataques cibernéticos a instituições públicas aumentaram na última década; entenda motivo,” Feb. 2024.

21. ESET, “ESET APT Activity Report Q4 2024–Q1 2025,” 2025.

22. F. I. F. Farhan, M. S. Si, M. Kom, and A. S. Qamar, “Implementation of Security Information Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System,” 2024.

23. J. Hafiz, “Practical Applications of Wazuh in On-premises Environments,” Theseus.fi, 2024.