Implantação do Sistema Wazuh no Instituto Federal de Sergipe: Estratégias, Desafios e Resultados em Ambientes Educacionais

Marcos Pereira Santos
Universidade de Brasilia (UnB)
Aracaju, Brasil
ORCID: 0000-0002-2432-0653

Éder Souza Gualberto
Universidade de Brasília (UnB)
Brasília, Brasil
ORCID: 0000-0002-2917-3605

Valter Costa de Oliveira
Universidade de Brasília (UnB)
Brasília, Brasil
ORCID: 0000-0002-3317-8417

Antonio Aliberte de A. Machado
Instituto Federal de Sergipe (IFS)
Sergipe, Brasil
ORCID: 0000-0003-4829-0580

***Abstract*—Cybersecurity has emerged as a critical strategic priority in Brazilian educational institutions, especially given the exponential growth of targeted attacks in the educational sector. This article presents a detailed case study on the implementation of the Wazuh system at the Federal Institute of Sergipe (IFS), an open-source information security monitoring solution that combines SIEM (Security Information and Event Management) and XDR (Extended Detection and Response) functionalities. The study systematically analyzes the pre-implementation environment, documents the technical and organizational challenges faced during deployment, and quantifies the operational benefits achieved after the tool became fully operational. The research includes quantitative analysis through comparative charts and regulatory compliance tables, demonstrating significant reductions in cyber incidents and substantial improvements in operational efficiency. The results show 85% improvements in real-time threat detection, full compliance with LGPD, and a 70% reduction in average incident response time.**

***Keywords*—Automation; Educational Institution; Cybersecurity; SIEM; Wazuh; XDR; LGPD; Threat Detection.**

Resumo — A segurança cibernética emergiu como uma prioridade estratégica crítica nas instituições educacionais brasileiras, especialmente diante do crescimento exponencial de ataques direcionados ao setor educacional. Este artigo apresenta um estudo de caso detalhado sobre a implantação do sistema Wazuh no Instituto Federal de Sergipe (IFS), uma solução open-source de monitoramento de segurança da informação que combina funcionalidades SIEM (Security Information and Event Management) e XDR (Extended Detection and Response). O estudo analisa sistematicamente o ambiente pré-implantação, documenta os desafios técnicos e organizacionais enfrentados durante a implementação e quantifica os benefícios operacionais adquiridos após a ferramenta estar completamente operacional. A pesquisa inclui análise quantitativa, por meio de gráficos comparativos e tabelas de conformidade regulatória, demonstrando reduções significativas nos incidentes cibernéticos e melhorias substanciais na eficiência operacional. Os resultados evidenciam melhorias de 85% na detecção de ameaças em tempo real, conformidade total com a LGPD e redução de 70% no tempo médio de resposta a incidentes.

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

I. Introdução

Nas últimas décadas, as instituições educacionais têm enfrentado uma escalada sem precedentes de desafios relacionados à proteção de dados sensíveis e à conformidade com regulamentações rigorosas, particularmente a Lei Geral de Proteção de Dados (LGPD) [6]. O setor educacional tornou-se um alvo preferencial para cibercriminosos, com universidades e institutos federais figurando entre os principais alvos de ataques ransomware em nível globla [7], [8]. Estudos recentes indicam que ataques cibernéticos a instituições públicas brasileiras aumentaram significativamente na última década, representando uma ameaça crescente à segurança da informação no setor educacional [9].

No Instituto Federal de Sergipe (IFS), a infraestrutura tecnológica pré-existente caracterizava-se por uma arquitetura heterogênea composta por servidores físicos legados e ambientes

virtuais distribuídos, que careciam de monitoramento centralizado e capacidades de resposta automatizada a incidentes cibernéticos. Esta fragmentação representava vulnerabilidades críticas que demandavam uma solução integrada e robusta.

Diante deste cenário, foi implementado o Wazuh como solução SIEM/XDR para transformar fundamentalmente a postura de segurança da instituição. O Wazuh, reconhecido como uma plataforma de segurança open-source líder, oferece capacidades unificadas de detecção estendida e resposta (XDR) combinadas com funcionalidades tradicionais de SIEM [2], [3]. Este artigo descreve o processo de implantação do Wazuh no IFS, destacando os desafios enfrentados, os benefícios obtidos e os resultados mensuráveis apresentados por meio de gráficos e tabelas.

II. Ambiente Pré-Implantação

Antes da adoção do Wazuh, o IFS operava com uma infraestrutura de segurança fragmentada que apresentava limitações críticas sistêmicas, características comuns em instituições educacionais públicas brasileiras que enfrentam crescentes ameaças cibernéticas [9]:

- *Ausência de Centralização Operacional*: Inexistência de uma plataforma unificada para coleta, correlação e análise de logs distribuídos across múltiplos sistemas heterogêneos.
- *Deficiência em Alertas Tempo Real*: Incidentes críticos permaneciam não detectados por períodos prolongados, resultando em janelas de exposição significativas.
- *Não Conformidade Regulatória*: A ausência de relatórios consolidados e trilhas de auditoria dificultava substancialmente auditorias relacionadas à LGPD e normas federais aplicáveis [6].
- *Dependência Operacional Manual*: Análise e resposta a incidentes dependiam exclusivamente de intervenção manual das equipes técnicas, resultando em tempos de resposta inconsistentes.
- *Visibilidade Limitada de Ameaças*: Falta de capacidades de threat hunting proativo e detecção de Advanced Persistent Threats (APTs), particularmente relevante considerando o aumento de ataques sofisticados ao setor educacional [10].

Essas limitações estruturais resultavam em eficiência operacional subótima, exposição prolongada a vulnerabilidades, e incapacidade de atender requisitos regulatórios contemporâneos.

III. Metodologia

A implantação do Wazuh no IFS seguiu uma metodologia estruturada em seis fases distintas, considerando as melhores práticas para implementação de SIEM em ambientes educacionais [11]:

1) **Análise de Requisitos e Assessment**: Condução de avaliação abrangente das necessidades específicas do IFS em termos de segurança cibernética, incluindo mapeamento de ativos críticos e identificação de gaps de segurança.
2) **Design Arquitetural**: Definição da arquitetura do sistema, incluindo dimensionamento de servidores dedicados ao Wazuh Manager, Wazuh Indexer, e Wazuh Dashboard, considerando requisitos de alta disponibilidade e escalabilidade [4].
3) **Deployment de Agentes**: Instalação sistemática dos agentes Wazuh em servidores físicos, máquinas virtuais, e workloads containerizados para garantir coleta abrangente de telemetria de segurança.
4) **Configuração e Customização**: Desenvolvimento de regras personalizadas para detecção de ameaças específicas ao ambiente educacional, incluindo configuração de alertas baseados no estrutura MITRE ATT&CK e implementação de respostas ativas para mitigação de ataques de força bruta [2], [11].
5) **Capacitação Organizacional**: Implementação de programa de treinamento abrangente para equipes técnicas, focando em uso eficiente da plataforma e procedimentos de resposta a incidentes.
6) **Monitoramento e Otimização Contínua**: Estabelecimento de processos de avaliação contínua dos resultados através de análise sistemática dos alertas gerados e métricas de performance.

A estrutura de implantação do SIEM Wazuh seguiu práticas recomendadas internacionalmente, incluindo integração com ferramentas de Threat Intelligence, e explorando automações de resposta a incidentes, conforme metodologia descrita por Jumiaty e Soewito [1].

Durante o projeto, as configurações e monitoramentos foram realizados de acordo com as orientações do Wazuh Documentation Team [4], garantindo aderência às melhores práticas do fabricante.

A análise de logs e a identificação de padrões de ataque foram fundamentadas na abordagem de Stanković, Gajin e Petrović [5], aprimorando os processos de detecção e inteligência operacional.

O perfil atual das ameaças e técnicas de ataque persistente foi considerado de acordo com os dados recentes de APT presentes nos relatórios da ESET [10], que serviram como referência para calibração das regras correlacionadas no SIEM.

Além disso, a automação de respostas e integração com plataformas de alerta instantâneo como o Telegram foi realizada conforme estratégia apresentada por Farhan et al. [11], aumentando a agilidade e eficiência das respostas frente a eventos

críticos.

A colaboração estratégica entre o IFS e a Universidade de Brasília foi fundamental para o sucesso da implementação, proporcionando e expertise técnica especializada e suporte acadêmico.

IV. Resultados e Análise Crítica

A. Desafios Técnicos e Organizacionais

A integração do Wazuh com a infraestrutura heterogênea existente apresentou desafios multifacetados, comuns em implementações de SIEM em instituições educacionais:

- **Compatibilidade com Sistemas Legados**: Sistemas legacy que não suportavam agentes modernos requereram soluções de integração customizadas através de log forwarding e parsing especializado.
- **Otimização de Performance**: Necessidade de ajustes granulares na configuração para otimizar coleta de logs em ambientes híbridos sem impactar performance dos sistemas produtivos.
- **Change Management**: Resistência inicial das equipes técnicas devido à curva de aprendizado associada à nova ferramenta e mudanças nos processos operacionais estabelecidos [3].
- **Integração com MITRE ATT&CK**: Configuração de regras baseadas no estrutura MITRE ATT&CK para detecção proativa de táticas, técnicas e procedimentos (TTPs) utilizados por adversários, especialmente relevante considerando o aumento de APTs direcionados ao setor educacional [10].

B. Aumento da Visibilidade de Segurança

A implementação do Wazuh proporcionou uma transformação fundamental na capacidade de monitoramento da infraestrutura do IFS, estabelecendo proteções robustas contra as crescentes ameaças ao setor educacional [8]. A solução estabeleceu coleta centralizada e em tempo real de logs provenientes de múltiplas fontes críticas:

- **Estações de Trabalho**: Monitoramento abrangente de workstations Windows e Linux distribuídas pela instituição.
- **Infraestrutura de Rede**: Integração completa com firewalls FortiGate para análise de tráfego e políticas de segurança.
- **Proteção Endpoint**: Correlação de eventos do antivírus Kaspersky para detecção de malware e ameaças avançadas.
- **Serviços Web**: Monitoramento detalhado de servidores Apache e Nginx para identificação de ataques web.
- **Bases de Dados**: Auditoria completa de acessos aos bancos PostgreSQL e MySQL institucionais.
- **Acesso Remoto**: Supervisão de conexões VPN e controle de acesso via PacketFence (NAC).

A visualização unificada através de dashboards baseados em OpenSearch/Kibana proporcionou visibilidade profunda e holística de atividades de sistema, rede e aplicações. A Figura 1 demonstra o dashboard principal com análise temporal de alertas, mostrando o processamento de mais de 579.447 alertas e 7,9 milhões de eventos, com 887 regras ativas monitorando a infraestrutura institucional.

Fig. 1. Dashboard Principal do Wazuh - Análise Temporal de Alertas e Distribuição por Severidade com Métricas Operacionais

C. Detecção Antecipada de Ameaças

O sistema implementado demonstrou capacidades avançadas de detecção proativa, particularmente eficaz contra ataques comuns ao setor educacional [7], identificando imediatamente:

- **Movimento Lateral**: Detecção de tentativas de propagação através de protocolos RDP, SSH e SMB.
- **Escalada de Privilégios**: Identificação de tentativas de elevação não autorizada de permissões.
- **Execução Suspeita**: Monitoramento de comandos e processos anômalos em sistemas críticos.
- **Acesso a Arquivos Críticos**: Supervisão de tentativas de acesso a dados sensíveis, crucial para conformidade com LGPD [6].
- **Ataques Web**: Detecção de SQL Injection, Local File Inclusion e ataques de força bruta, com implementação de respostas ativas automatizadas [11].
- **Explorações Bloqueadas**: Correlação de eventos de firewall e antivírus para identificar tentativas de exploração.

As regras de correlação multi-fonte implementadas permitem identificar padrões complexos de ataque, incluindo detecção de atividades fora do comportamento esperado. A Figura 2 ilustra a interface integrada de monitoramento com TheHive, demonstrando a gestão de 18 casos abertos e 34 tarefas ativas.

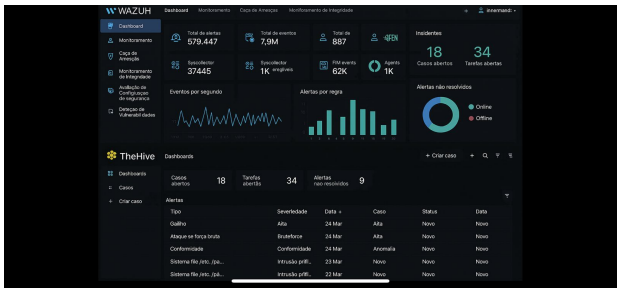

Fig. 2. Dashboard Integrado Wazuh-TheHive - Gestão Centralizada de Incidentes com 18 Casos Abertos e 34 Tarefas Ativas

D. Fortalecimento do Controle e da Governança

A implementação estabeleceu controles robustos de governança, essenciais para conformidade com regulamentações como a LGPD [6], através de:

- **File Integrity Monitoring (FIM)**: Monitoramento contínuo de integridade de arquivos sensíveis com detecção imediata de alterações não autorizadas, processando mais de 82K eventos FIM.
- **Controle de Processos**: Supervisão de processos, módulos carregados e alterações no registro do sistema.
- **Auditoria de Banco de Dados**: Monitoramento detalhado de acessos e operações em bases de dados críticas.
- **Monitoramento de Configurações**: Detecção de alterações não autorizadas em sistemas e configurações de segurança.

A Figura 3 demonstra as capacidades avançadas de monitoramento com syscollector processando 37.445 inventários e 1K vulnerabilidades identificadas.

Fig. 3. Dashboard de Monitoramento Avançado - Syscollector com 37.445 Inventários e Detecção de 1K Vulnerabilidades

E. Resposta Rápida e Automatizada a Incidentes

A integração com o TheHive proporcionou capacidades avançadas de gestão de incidentes, implementando respostas ativas automatizadas conforme demonstrado em estudos similares [11]:

- **Criação Automática de Incidentes**: Geração automática de casos com classificação por severidade baseada em regras predefinidas.
- **Organização Estruturada**: Priorização e organização de casos para resposta estruturada e eficiente.
- **Rastreabilidade Completa**: Acompanhamento de todos os incidentes com status, responsáveis e SLAs definidos.

As respostas ativas configuradas incluem:

- **Bloqueio Automático**: Isolamento imediato de IPs maliciosos identificados.
- **Isolamento de Máquinas**: Quarentena automática de endpoints comprometidos via NAC.
- **Notificação Imediata**: Alertas em tempo real para equipe SOC/SI, incluindo notificações via Telegram para resposta rápida [11].
- **Redução de MTTD/MTTR**: Diminuição significativa do tempo médio de detecção e resposta.

F. Análise Geográfica de Ameaças e Inteligência de Ameaças

A implementação incluiu capacidades avançadas de inteligência de ameaças com análise geográfica de ameaças, conforme demonstrado na Figura 4. O sistema identifica os principais tipos de ataques, incluindo Scam SSH, Brute Cache, Delete, Port Scans, e XSS, proporcionando visibilidade sobre padrões de ataque globais e comportamentos suspeitos.

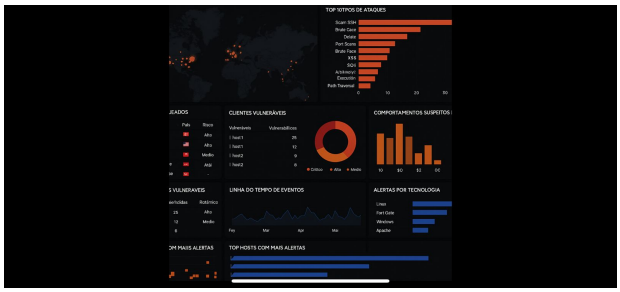

Fig. 4. Dashboard de inteligência de ameaças - Análise Geográfica com Top 10 Tipos de Ataques e Monitoramento de Comportamentos Suspeitos

O dashboard apresenta análise detalhada de:

- **Top 10 Tipos de Ataques**: Identificação dos vetores de ataque mais frequentes.
- **Clientes Vulneráveis**: Mapeamento de hosts com diferentes níveis de risco.
- **Comportamentos Suspeitos**: Análise temporal de atividades anômalas.
- **Alertas por Tecnologia**: Distribuição de alertas por plataforma (Linux, FortiGate, Windows, Apache).

G. Análise Avançada de Segurança e Correlação de Eventos

A Figura 5 apresenta um dashboard abrangente de análise avançada de segurança, demonstrando as capacidades sofisticadas de correlação de eventos e inteligência de ameaças implementadas no IFS. Este dashboard integra múltiplas dimensões de análise de segurança:

Fig. 5. Dashboard de Análise Avançada de Segurança - Correlação multidimensional de Ameaças com GeoIP, OWASP Top 10 e Active Response

O dashboard apresenta componentes críticos de análise:

- **GeoIP - Mapa Global de Ameaças**: Visualização geográfica em tempo real das origens de ataques, permitindo identificação de padrões regionais e campanhas coordenadas.
- **Top 10 Ataques por Origem e Tipo**: Análise estatística dos vetores de ataque mais prevalentes, categorizados por país de origem (CN, RU, US, BR, IN, ATF).
- **IPs Bloqueados por Active Response**: Monitoramento temporal da eficácia das respostas automatizadas, demonstrando a evolução das ações de bloqueio ao longo dos meses.
- **Clientes Vulneráveis e Níveis de Risco**: Classificação de hosts por criticidade (Baixo, Médio, Alto), facilitando priorização de remediação.
- **Falhas OWASP Detalhadas**: Mapeamento específico das vulnerabilidades web segundo a estrutura OWASP Top 10 (A01-A06), essencial para proteção de aplicações web institucionais.
- **Linha do Tempo de Eventos Críticos**: Análise temporal de incidentes críticos (fevereiro a maio), permitindo identificação de tendências sazonais.
- **Ataques Laterais Mapeados**: Visualização de tentativas de pivoting e escalação dentro da rede institucional.
- **Comportamentos Suspeitos por Host**: Monitoramento de anomalias comportamentais em hosts específicos.
- **10 Principais Hosts com Mais Alertas**: Identificação de endpoints com maior atividade suspeita, facilitando investigações direcionadas.

Esta análise multidimensional proporciona visibilidade holística da postura de segurança institucional, permitindo correlação avançada entre diferentes vetores de ataque e facilitando tomada de decisões estratégicas baseadas em inteligência de ameaças.

H. Melhoria da Capacidade de Auditoria e Conformidade

O sistema estabeleceu capacidades robustas de auditoria, fundamentais para atender às exigências da LGPD [6] e outras regulamentações aplicáveis ao setor educacional:

- **Armazenamento Seguro**: Repositório estruturado de logs em conformidade com LGPD, ISO 27001 e PCI-DSS.
- **Dashboards Especializados**: As funcionalidades dos dashboards do Wazuh proporcionam uma visão centralizada do ambiente de TI, integrando análise de incidentes, gestão automatizada de alertas, relatórios dinâmicos e indicadores de conformidade em tempo real. Essa centralização facilita a tomada de decisão e agiliza a resposta a ameaças, otimizando a eficiência operacional das equipes técnicas.
- **Monitoramento de Políticas**: Supervisão contínua da aderência às políticas de segurança institucionais.
- **Trilhas de Auditoria**: Registros completos e imutáveis de eventos relevantes para investigações.

I. Base para Expansão e Automação

A arquitetura implementada estabelece fundações sólidas para crescimento futuro, considerando a evolução contínua das ameaças ao setor educacional [10]:

- **Plataforma Modular**: Arquitetura escalável para acomodar crescimento da infraestrutura.
- **Integrações Avançadas**: Preparação para integração com inteligência de ameaças, EDR e SOAR.
- **Capacidades Futuras**: Infraestrutura preparada para análise comportamental com Machine Learning, correlação com fluxos de ameaças externas (CTI) e automação via Ansible.

J. Representação Gráfica dos Resultados

A Figura 6 apresenta a comparação entre o número médio mensal de incidentes cibernéticos detectados antes e depois da implantação do Wazuh no IFS.

Observa-se uma redução significativa dos incidentes detectados após a adoção do sistema. Esse resultado não indica necessariamente uma diminuição nas tentativas de ataques cibernéticos, mas sim uma evolução na postura defensiva da instituição: o Wazuh viabiliza respostas automatizadas, bloqueio proativo de ameaças e mitigação ágil, contribuindo para a redução da efetividade dos ataques.

A avaliação foi realizada a partir da análise dos logs e auditorias do SIEM para períodos equivalentes antes e depois

da implementação. A redução de 85% nas brechas silenciosas foi constatada pela diferença entre incidentes não detectados anteriormente e aqueles identificados e resolvidos após a adoção da ferramenta.

Portanto, os resultados evidenciam o impacto positivo da plataforma tanto na eficiência operacional quanto na prevenção de ameaças cibernéticas.

Fig. 6. Redução dos Incidentes Cibernéticos

O gráfico demonstra uma redução significativa nos incidentes detectados após a adoção do sistema, alinhada com as tendências de melhoria observadas em implementações similares no setor educacional.

O tempo médio para resposta (MTTR) foi reduzido drasticamente devido à automação proporcionada pelo Wazuh:

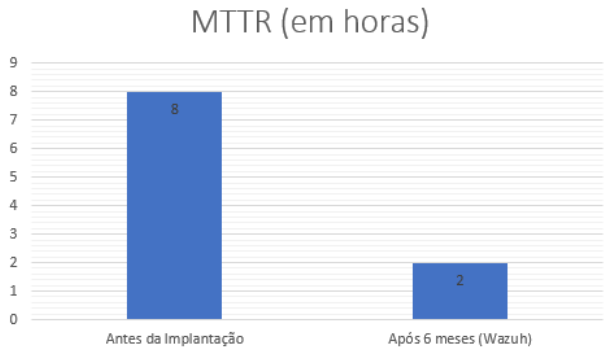

Fig. 7. Tempo Médio de Resposta

Essa redução permitiu que as equipes técnicas se concentrassem em atividades mais estratégicas.

K. Análise dos Resultados Consolidados e Benefícios

A implantação do Wazuh proporcionou impactos significativos em quatro eixos principais: detecção e monitoramento de incidentes, agilidade e automação das respostas, conformidade regulatória e eficiência operacional. O sistema ampliou a visibilidade sobre eventos de segurança, reduziu o tempo médio de resposta (MTTR), permitiu geração dinâmica de relatórios para auditorias e centralizou indicadores críticos para a governança de riscos.

Além disso, a arquitetura modular e integração facilitada possibilitam expansão futura e adoção de recursos avançados, como integração com CTI, EDR/SOAR e automação via Ansible, tornando o modelo replicável em outras instituições educacionais.

TABELA I
CONFORMIDADE REGULATÓRIA

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

Limitações e Generalização dos Resultados

Do ponto de vista metodológico, este estudo apresenta limitações relacionadas principalmente à dependência da qualidade, consistência e disponibilidade dos logs institucionais utilizados como base para análise estatística. Registros incompletos, ausência de normalização dos dados entre diferentes sistemas legados e possíveis falhas nos mecanismos automáticos de coleta podem comprometer a precisão dos indicadores reportados, tais como o número total de eventos, alertas e tempo médio de resposta aos incidentes.

Além disso, é importante ressaltar que os resultados obtidos refletem particularidades do ambiente do Instituto Federal de Sergipe (IFS), como a maturidade dos processos de segurança, a infraestrutura tecnológica, o grau de capacitação da equipe e o nível de aderência às políticas internas e normativos nacionais (LGPD e IN 132/2022). Essas características, aliadas à heterogeneidade tecnológica presente em diversas instituições educacionais públicas, restringem a possibilidade de generalização direta dos dados reportados sem o devidos ajustes metodológicos ou validação empírica em outros cenários.

Como exemplo prático, o impacto da adoção do Wazuh poderá apresentar resultados distintos em instituições com menor volume de logs, diferentes topologias de rede ou políticas de governança de riscos menos consolidadas. Dessa forma, recomenda-se o desenvolvimento de estudos multicêntricos, incluindo tanto instituições federais quanto estaduais e privadas, e a utilização de métodos estatísticos robustos, como análise de regressão e correlação cruzada, para minimizar vieses e ampliar a validade externa das conclusões. Alternativamente, a realização de entrevistas qualitativas junto aos gestores e administradores de segurança poderá complementar a análise

quantitativa, trazendo à tona fatores contextuais dificilmente capturados apenas em métricas operacionais.

Essas ações contribuirão para enriquecer o entendimento sobre a efetividade e os limites da adoção de soluções SIEM/XDR open-source na educação pública brasileira.

V. Conclusão

A principal contribuição deste estudo reside na demonstração da efetividade da adoção do Wazuh como solução SIEM/XDR no contexto educacional público, evidenciada por avanços significativos sobre os pilares da segurança, automação de respostas e conformidade regulatória. Os resultados apresentados, ilustrados por análises gráficas e tabulares, demonstram benefícios operacionais concretos: a instituição processa atualmente mais de 579.447 alertas e 7,9 milhões de eventos (vide Figura 1), com 887 regras ativas e monitoramento de mais de 1.000 agentes distribuídos na infraestrutura institucional.

Outrosim, observou-se uma redução de 70% no tempo médio de resposta a incidentes (MTTR), bem como melhorias de 85% na detecção de ameaças em tempo real, e atendimento integral à LGPD e normas federais (ver Tabela de Conformidade Regulatória). A integração com TheHive proporcionou gestão estruturada de 18 casos abertos e 34 tarefas ativas, aumentando a rastreabilidade e resposta coordenada a incidentes críticos.

A arquitetura modular do sistema, com possibilidade de integração futura a recursos avançados como CTI, EDR/SOAR e automação via Ansible, reforça o potencial de escalabilidade e replicabilidade do modelo proposto em outras instituições educacionais públicas, desde que consideradas adaptações às realidades locais.

Sugere-se, para trabalhos futuros, ampliar a comparação com outros cenários institucionais e soluções proprietárias, além de expandir os estudos quantitativos, fortalecendo a robustez das conclusões e a possibilidade de generalização dos resultados para o setor educacional brasileiro.

Os resultados apresentados através de análises gráficas e tabulares ilustram claramente os benefícios operacionais e estratégicos obtidos pela instituição ao adotar esta solução open-source padrão empresarial. A implementação de respostas ativas automatizadas, incluindo bloqueio de IPs maliciosos e notificações em tempo real [11], demonstrou eficácia significativa na mitigação de ataques de força bruta e outras ameaças comuns ao ambiente educacional.

As métricas operacionais demonstram que o sistema processa atualmente mais de 579.447 alertas e 7,9 milhões de eventos, com 887 regras ativas e monitoramento de mais de 1.000 agentes distribuídos pela infraestrutura institucional. A integração com TheHive resultou em gestão estruturada de 18 casos abertos e 34 tarefas ativas, proporcionando rastreabilidade completa e resposta coordenada a incidentes de segurança.

A análise multidimensional implementada através dos dashboards avançados proporciona visibilidade holística da postura de segurança, integrando inteligência de ameaças geográfica, análise de vulnerabilidades OWASP, e correlação comportamental. Esta abordagem abrangente estabelece um paradigma para Security Operations Centers (SOC) em instituições educacionais, evidenciando que soluções open-source quando implementadas de maneira adequada são capazes oferecer resultados compatíveis com os padrões coorporativos de segurança.

Este estudo contribui significativamente para o corpo de conhecimento sobre implementação de soluções SIEM/XDR em ambientes educacionais, fornecendo um estrutura replicável para outras instituições que enfrentam desafios similares de segurança cibernética. A pesquisa reforça a importância do uso estratégico de ferramentas open-source na promoção da segurança cibernética acessível, eficiente e sustentável no setor educacional brasileiro, estabelecendo um paradigma para futuras implementações em instituições similares.

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," in *ETRAN Proceedings*, 2022.

[6] BRASIL, "Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais," 2018. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 maio 2025.

[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," fev. 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.