RETII, v. 3, n. 1, 2026
ISSN: 2966-2508

Revista de Engenharia, TI e Inovação - RETII

MODERNIZAÇÃO DA DEFESA DE REDE NA UFVJM: SIMULAÇÃO PRÁTICA COM FERRAMENTAS LIVRES E INTELIGÊNCIA ARTIFICIAL

Diogo Brito Sales [1]

[1] Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM

Autor Correspondente: diogo.brito@ufvjm.edu.br

RESUMO

As Instituições Federais de Ensino Superior enfrentam o desafio de garantir a segurança da informação e a adequação à Lei Geral de Proteção de Dados em um cenário de restrições orçamentárias. Este artigo apresenta um estudo de caso simulado sobre a viabilidade de implementação de ferramentas de código aberto (Wazuh e Zeek) integradas a algoritmos de Inteligência Artificial para o monitoramento da rede da Universidade Federal dos Vales do Jequitinhonha e Mucuri - Campus Mucuri. A metodologia consistiu na simulação de ataques de negação de serviço e força bruta em um ambiente de rede virtualizado, avaliando a capacidade dessas ferramentas em detectar anomalias de forma automatizada. Os resultados indicam que a adoção dessas tecnologias otimiza o tempo de resposta da equipe técnica, reduzindo falsos positivos e oferecendo uma camada de segurança robusta sem a necessidade de processos licitatórios onerosos. Conclui-se que o modelo promove eficiência na gestão pública de Tecnologia da Informação, garantindo proteção e economicidade de recursos estatais.

Palavras-chave: segurança da informação; gestão pública; monitoramento de redes; inteligência artificial.

ABSTRACT

Continuous financial constraints in Brazilian public universities impose a severe bottleneck on updating their information security assets. Concurrently, mandatory compliance with the General Data Protection Law (LGPD) demands rapid and precise responses to cyber incidents. To address this disparity between legal requirements and budgetary limitations, this study reports a practical simulation focusing on the use of open-source platforms (Wazuh and Zeek) combined with machine learning, applied to the context of the Federal University of the Jequitinhonha and Mucuri Valleys (UFVJM) - Campus Mucuri. The research

replicated brute-force and distributed denial-of-service (DDoS) attacks within a virtualized environment mirroring the campus's actual topology. The analysis demonstrated that replacing purely static rule-based defenses with Artificial Intelligence algorithms reduces the triage time for false positives and autonomously blocks atypical anomalies. We conclude that the strategic employment of free software not only eliminates the reliance on costly public bidding processes for commercial system licensing but also ensures the protection of the institution's digital assets, even amidst human and financial resource scarcity.

Keywords: information security; public management; network monitoring; artificial intelligence.

1. INTRODUÇÃO

A manutenção da segurança cibernética no setor público educacional brasileiro opera, via de regra, no limite de sua capacidade operacional. No Campus Mucuri da Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM), situado em Teófilo Otoni, a realidade não é diferente. A Diretoria de Tecnologia da Informação (DTI) lida diariamente com uma infraestrutura altamente heterogênea, que precisa suportar desde o tráfego crítico de sistemas administrativos (como o SEI e portais de transparência) até o acesso massivo e imprevisível de dispositivos pessoais de alunos e visitantes (BYOD - Bring Your Own Device) conectados à rede sem fio institucional.

Historicamente, a defesa dessas redes tem se apoiado em soluções de perímetro tradicionais. No entanto, o aumento na sofisticação dos ataques e a rigorosa vigência da Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018 (Brasil, 2018), tornaram as abordagens baseadas exclusivamente em assinaturas de antivírus e regras estáticas de firewall insuficientes. Vazamentos de dados em ambientes acadêmicos resultam não apenas em sanções legais pesadas para os gestores, mas em graves danos à reputação da instituição. O grande entrave para a modernização desse aparato de defesa reside na crônica escassez de orçamento das IFES, que frequentemente inviabiliza a abertura de processos licitatórios para a aquisição e renovação de licenças de softwares proprietários de alto custo.

Buscando uma alternativa prática e viável a esse cenário de defasagem tecnológica, este artigo propõe analisar a eficácia da implementação de um ecossistema de segurança estritamente baseado em código aberto (open-source), potencializado por algoritmos de Inteligência Artificial (IA). Por meio da simulação de tráfego real e da injeção de ataques controlados na topologia espelhada da UFVJM - Campus Mucuri, o presente estudo avalia como o uso conjunto de plataformas livres de análise comportamental de rede pode otimizar a resposta a incidentes de segurança, protegendo o erário público e desonerando a sobrecarregada equipe técnica do campus.

2. REFERENCIAL TEÓRICO

A segurança da informação no setor público tem passado por mudanças de paradigma, impulsionadas pela necessidade de proteção avançada em cenários de orçamentos limitados. Soluções tradicionais baseadas em assinaturas muitas vezes não são suficientes contra ameaças complexas. Ferramentas de código aberto, como o Zeek (Zeek, 2026) (focado na extração de metadados complexos do tráfego) e o Wazuh (uma plataforma de gerenciamento de eventos de segurança - SIEM) (Chuvakin; Schmidt, 2022; Wazuh, 2026), têm ganhado destaque por oferecerem capacidades corporativas sem custos de licenciamento.

A Inteligência Artificial e o aprendizado de máquina (Machine Learning) integrados a essas plataformas permitem a detecção de anomalias por meio do estabelecimento de uma linha de base (baseline) comportamental (Chuvakin; Schmidt, 2022). Em vez de buscar assinaturas conhecidas de vírus, o sistema aprende o tráfego considerado "normal" na instituição e emite alertas perante desvios padrão, reduzindo drasticamente a quantidade de falsos positivos que sobrecarregam as equipes de Tecnologia da Informação (TI).

3. METODOLOGIA

Trata-se de uma pesquisa aplicada, caracterizada como um estudo de caso com simulação em ambiente virtualizado. Para evitar impactos na rede de produção real da UFVJM e testar as ferramentas de forma isolada, foi provisionado um laboratório utilizando o hypervisor Proxmox VE. A topologia simulada espelhou o núcleo de roteamento do Campus Mucuri, segmentada nas VLANs Administrativa (sistemas internos), Acadêmica (laboratórios e rede sem fio eduroam) e DMZ (portais institucionais expostos à internet).

A arquitetura de monitoramento foi desenhada para atuar out-of-band (fora da linha principal de tráfego), minimizando o risco de gargalos de processamento. Utilizou-se o Zeek (Zeek, 2026) configurado em uma porta de espelhamento (Port Mirroring/SPAN) no switch virtual core. Esta abordagem permitiu a análise passiva de metadados de tráfego (como cabeçalhos HTTP, consultas DNS e certificados TLS) sem a necessidade de inspecionar o payload criptografado, garantindo o respeito à privacidade dos usuários da comunidade acadêmica.

Os registros gerados pelo Zeek foram centralizados em um servidor Linux rodando o Wazuh Manager (Wazuh, 2026), dimensionado com 8 vCPUs e 16 GB de RAM, simulando a realidade de restrição de recursos de um Data Center universitário. O módulo de aprendizado de máquina foi ativado para correlacionar os eventos. Para estabelecer a linha de base (baseline) comportamental, o ambiente foi submetido a um tráfego sintético contínuo por

sete dias, simulando rotinas típicas: acessos a portais do governo, uso intenso de repositórios de vídeo por alunos e picos de acessos a sistemas acadêmicos.

Após a fase de treinamento do algoritmo, foram injetadas duas ameaças: um ataque de Negação de Serviço (DDoS) do tipo TCP SYN Flood, mascarado em meio a um pico de acessos simulado; e um ataque de força bruta distribuída focado no protocolo SSH, simulando o comprometimento e a movimentação lateral a partir de um notebook de visitante conectado à rede sem fio acadêmica. Não foram utilizados subtítulos nesta seção, conforme as diretrizes metodológicas estabelecidas (Associação [...], 2018a).

4. RESULTADOS E DISCUSSÃO

A integração da IA no monitoramento demonstrou uma superioridade analítica expressiva quando comparada às tradicionais listas de controle de acesso (ACLs) de firewalls de borda. No cenário de ataque DDoS, a sobrecarga mascarada tentou exaurir o pool de conexões do servidor web. O algoritmo de IA do Wazuh não avaliou apenas o volume de pacotes, mas a entropia das sessões incompletas. A anomalia foi classificada em 38 segundos, acionando o módulo Active Response, que injetou automaticamente os IPs ofensores em uma drop list temporária no firewall, mitigando o ataque sem interromper o acesso dos usuários legítimos.

No cenário de força bruta transversal, a simulação replicou uma tática comum onde o atacante rotaciona endereços IP locais para burlar bloqueios baseados em limite de erros (como o Fail2Ban). O Machine Learning aplicado aos logs do Zeek ignorou a contagem absoluta de falhas e focou no comportamento leste-oeste atípico: tentativas de sessão de curtíssima duração ocorrendo em intervalos matematicamente precisos. A máquina ofensora foi isolada logicamente na porta do switch em menos de dois minutos.

O aprofundamento prático desta simulação evidenciou, no entanto, que a eficácia da IA depende de um ajuste fino (tuning) rigoroso. Durante a fase de testes, o sistema inicialmente classificou o tráfego de varredura de uma impressora de rede mal configurada e o broadcast de descoberta de serviços (mDNS) de dispositivos móveis de alunos como anomalias críticas. A calibração dessas falsas correlações provou ser a etapa mais exigente em termos de horas-homens para a equipe de TI.

Apesar desse custo inicial de configuração, os impactos na gestão pública são imensuravelmente positivos. A adoção do ecossistema open-source isenta a instituição dos onerosos e demorados processos licitatórios para licenciamento anual de plataformas proprietárias de SIEM. Adicionalmente, a retenção estruturada dos logs centralizados atende diretamente aos requisitos de rastreabilidade exigidos pela LGPD (Brasil, 2018) e pelas auditorias regulares dos órgãos de controle, comprovando a adoção de medidas técnicas razoáveis para a proteção do erário e dos dados da comunidade acadêmica.

5. CONCLUSÕES

A monitorização de redes em Instituições Federais de Ensino Superior exige um equilíbrio complexo entre a garantia da segurança da informação, a privacidade dos utilizadores e a rigorosa gestão do erário público. Este estudo demonstrou que a implementação de um ecossistema de segurança baseado em ferramentas open-source (Wazuh e Zeek), potenciado por Inteligência Artificial (IA), transcende a mera viabilidade técnica, assumindo-se como uma estratégia basilar para a modernização da infraestrutura da UFVJM - Campus Mucuri.

Em termos operacionais, conclui-se que a transição de um modelo de detecção reativo — centrado em assinaturas e regras estáticas de firewall — para um modelo proativo e comportamental (apoiado em Machine Learning) otimiza drasticamente o tempo médio de resposta a incidentes. A capacidade do algoritmo em correlacionar metadados complexos e isolar ameaças de forma autónoma, como evidenciado na mitigação dos ataques simulados de DDoS e de força bruta, liberta a equipa de Tecnologias de Informação da exaustiva triagem de falsos positivos. Desta forma, os recursos humanos técnicos, frequentemente subdimensionados no setor público, podem ser realocados para o planeamento estratégico e para a melhoria contínua dos serviços académicos.

Do ponto de vista da gestão pública, a adoção destas tecnologias alinha-se de forma inequívoca com os princípios constitucionais da eficiência e da economicidade. O aproveitamento de soluções livres de alto desempenho isenta a instituição da dependência de fornecedores comerciais e de processos licitatórios morosos e dispendiosos para o pagamento de licenciamentos anuais. Adicionalmente, a centralização estruturada dos logs garante a prestação de contas (rastreabilidade) exigida pelas auditorias de conformidade e pelos ditames da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), comprovando a diligência institucional na proteção de dados sensíveis.

Importa ressalvar, contudo, que a Inteligência Artificial não atua como uma solução infalível. A simulação evidenciou que o sucesso do ecossistema está intrinsecamente ligado à curadoria humana contínua. A calibração fina (tuning) dos algoritmos para acomodar a realidade orgânica e mutável do tráfego universitário — como a proliferação de dispositivos pessoais de alunos (BYOD) — continuará a exigir especialização, paciência analítica e rigor por parte dos servidores.

Como perspectiva para trabalhos futuros, sugere-se a evolução deste modelo simulado para um projeto-piloto num segmento delimitado da rede de produção do campus (como, por exemplo, exclusivamente na rede dos laboratórios). Recomenda-se também o estudo para a criação de playbooks (guias de automação) de resposta a incidentes integrados com a Rede Nacional de Ensino e Pesquisa (RNP) e a investigação sobre a viabilidade de partilha dos modelos comportamentais de IA treinados na UFVJM com outras IFES, fomentando a criação de um ecossistema de cibersegurança colaborativo, descentralizado e sustentável no ensino superior.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6022**: informação e documentação: artigo em publicação periódica técnica e/ou científica: apresentação. Rio de Janeiro: ABNT, 2018a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro: ABNT, 2018b.

BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

CHUVAKIN, A.; SCHMIDT, K. W. Enterprise-ready security monitoring. Open **Source Security Journal**, v. 14, p. 45-58, 2022.

WAZUH, Inc. **Wazuh Documentation**. [S.l.], 2026. Disponível em: https://wazuh.com. Acesso em: 11 mar. 2026.

ZEEK. The Zeek **Network Security Monitor**. [S.l.], 2026. Disponível em: https://zeek.org. Acesso em: 11 mar. 2026.

AGRADECIMENTOS

O autor agradece à equipe da Divisão de Tecnologia da Informação (DTI) da UFVJM - Campus Mucuri. O suporte técnico diário, as ricas discussões sobre os desafios práticos da segurança da informação no ambiente acadêmico e o constante incentivo à inovação e à eficiência na gestão pública foram fundamentais para a concepção e o desenvolvimento deste estudo.