IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Data da publicação xxxx 00, 0000, data da versão atual xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Estratégias de Mitigação de Ataques de Autenticação usando Wazuh e Inteligência Artificial: Uma Revisão com Base no PPSI

VOLPI, CARLOS A[1]
[1]Secretaria de Governo Digital- SGD. Ministério da Gestão e Inovação em Serviços Públicos (MGI) (e-mail: carlos.volpi@gestao.gov.br)
Corresponding author: Volpi. Carlos A (e-mail: cvolpi@ifes.edu).

ABSTRACT Este artigo apresenta uma revisão sistemática da literatura com o objetivo de analisar como a integração da plataforma Wazuh, um SIEM/XDR de código aberto, com técnicas de Inteligência Artificial (IA) pode aprimorar a detecção e mitigação de ataques a serviços de autenticação, mapeando essa abordagem aos controles do Programa de Privacidade e Segurança da Informação (PPSI). Foram consultadas bases de dados acadêmicas e literatura técnica especializada, selecionando estudos recentes que abordam vetores de ataque, capacidades do Wazuh, uso de *machine learning* para detecção de anomalias e aplicações de User and Entity Behavior Analytics (UEBA). A análise mostrou que abordagens híbridas, combinando correlação de eventos e modelos de aprendizado de máquina, aumentam a acurácia da detecção e reduzem falsos positivos, especialmente em cenários complexos de autenticação. No contexto do setor público, a solução proposta alinha-se às diretrizes do PPSI, fortalecendo a postura de segurança cibernética e promovendo conformidade regulatória. Como contribuição, o estudo apresenta um modelo teórico integrado Wazuh+IA, acompanhado do mapeamento de suas funcionalidades aos controles do PPSI, e propõe a implementação futura de uma prova de conceito para validação empírica.

INDEX TERMS Wazuh, SIEM, XDR, Inteligência Artificial, UEBA, PPSI, Autenticação, Detecção de Anomalias.

I. INTRODUCTION

OS ataques cibernéticos têm se tornado uma ameaça crescente para organizações públicas e privadas, afetando setores como governo, educação, saúde e indústria. No Brasil, a transformação digital acelerada, impulsionada pela pandemia de COVID-19, intensificou a dependência de serviços online e ampliou a superfície de ataque das infraestruturas de Tecnologia da Informação (TI) [1]. Esse cenário expôs sistemas críticos — que armazenam dados sensíveis e sustentam operações essenciais — a riscos como vazamento de informações, interrupção de serviços e danos à reputação institucional.

Entre os serviços mais visados por cibercriminosos estão os mecanismos de autenticação, utilizados para controlar o acesso a recursos protegidos. Plataformas como o Active Directory (AD) e outros sistemas de autenticação centralizada desempenham papel fundamental na verificação de identidade e na concessão de permissões. No entanto, a complexidade desses ambientes e a dependência de credenciais de usuário tornam-nos alvos atrativos para ataques como password spraying, credential stuffing e exploração de vulnerabilidades em protocolos de autenticação [2].

A detecção de atividades maliciosas nesses serviços em tempo real é desafiadora, especialmente em ambientes heterogêneos e distribuídos, onde múltiplas fontes de logs e eventos precisam ser correlacionadas. Ferramentas tradicionais de segurança, como firewalls e antivírus, tendem a se basear em regras estáticas e assinaturas conhecidas, mostrando-se insuficientes contra ameaças sofisticadas, como ataques de dia zero e malware polimórfico. A necessidade de visibilidade completa sobre o tráfego e comportamento dos usuários, aliada ao crescente volume de dados gerados, exige soluções capazes de identificar padrões anômalos e responder de forma rápida e precisa.

Nesse contexto, plataformas de gestão de eventos e informações de segurança (Security Information and Event Man-

agement — SIEM), como o Wazuh, destacam-se por permitir a coleta, correlação e análise centralizada de logs de autenticação e outros eventos de segurança. Quando integradas a técnicas de Inteligência Artificial (IA) e Aprendizado de Máquina (Machine Learning — ML), essas soluções podem evoluir para análises comportamentais avançadas (User and Entity Behavior Analytics — UEBA), capazes de identificar desvios sutis e antecipar ameaças que passariam despercebidas por métodos convencionais [3].

A aplicação de IA sobre dados coletados por um SIEM open source como o Wazuh possibilita criar modelos que detectam tentativas de login fora de padrões habituais, acessos de "viagem impossível", horários de atividade atípicos e comportamentos que indicam ataques de força bruta ou exploração interna. Essa abordagem não apenas aumenta a acurácia na detecção, mas também reduz falsos positivos e melhora a eficiência operacional dos centros de operações de segurança (Security Operations Center — SOC).

Considerando o cenário brasileiro, a necessidade de soluções como essa é ainda mais relevante diante da obrigatoriedade de conformidade com políticas nacionais, como o Programa de Privacidade e Segurança da Informação (PPSI), que estabelece controles técnicos e organizacionais para proteção de dados e mitigação de riscos. O PPSI exige que órgãos e entidades públicas adotem medidas de prevenção, detecção e resposta a incidentes cibernéticos, alinhadas a padrões reconhecidos de segurança da informação. No entanto, muitas organizações ainda enfrentam lacunas significativas, seja por limitações orçamentárias, seja pela ausência de equipes especializadas ou pela dependência de ferramentas tradicionais com capacidade limitada de detecção proativa.

Assim, este estudo parte da constatação de que a proteção eficaz dos serviços de autenticação requer uma abordagem integrada, combinando capacidades de monitoramento e correlação de eventos providas pelo Wazuh com técnicas avançadas de IA para detecção de anomalias. Ao realizar uma revisão de literatura abrangente, busca-se mapear como essa integração pode contribuir para mitigar ataques a serviços de autenticação e como suas funcionalidades se alinham aos controles definidos pelo PPSI, oferecendo um modelo teórico de solução aplicável a diversos contextos institucionais.

II. REFERENCIAL TEÓRICO

1) Ataques a Serviços de Autenticação

Os serviços de autenticação estão sujeitos a diversos vetores de ataque que exploram vulnerabilidades técnicas e humanas. Entre os mais relevantes destacam-se:

- **Brute force e dictionary attacks**: tentativas automatizadas de adivinhação de credenciais por meio de combinações exaustivas ou listas pré-definidas de senhas comuns [14].
- **Password spraying**: estratégia que distribui tentativas de acesso com senhas populares entre múltiplas contas, evitando o bloqueio por tentativas repetidas em um mesmo usuário [14].
- **Credential stuffing**: utilização de credenciais comprometidas em serviços anteriores para acessar outros sistemas; devido ao hábito de reutilização de senhas, ataques em larga escala se tornam eficazes [15].
- **Replay attack**: reenvio de transmissões válidas interceptadas para simular uma autenticação legítima e obter acesso não autorizado [18].
- **Man-in-the-middle (MITM)** e **man-in-the-browser (MITB)**: interceptação ou alteração de comunicação entre cliente e servidor, podendo comprometer credenciais mesmo em canais com criptografia [17].
- **Thermal e shoulder-surfing attacks**: métodos físicos ou observacionais para captar informações de autenticação — o primeiro detecta padrões térmicos deixados em teclados ou telas, enquanto o segundo envolve observação direta ou gravação visual das entradas do usuário [17], [20].
- **Ataques baseados em Kerberos (Silver/Golden Ticket)**: criação de tíquetes falsificados no protocolo Kerberos (Silver Ticket para serviços e Golden Ticket para domínio), permitindo acesso e movimentação privilegiada em ambientes com AD [21], [22].
- **Impersonation-as-a-Service (ImpaaS)**: infraestrutura criminosa emergente que possibilita ataques de personificação em escala com uso de perfis e credenciais automatizados, contornando controles como MFA e sistemas de risco adaptativo [23].

A. SIEM/XDR OPEN SOURCE

As soluções de *Security Information and Event Management* (SIEM) e *Extended Detection and Response* (XDR) são fundamentais para a detecção, análise e resposta a incidentes de segurança cibernética. Um SIEM centraliza e correlaciona eventos de segurança provenientes de múltiplas fontes, enquanto o XDR amplia essa abordagem integrando diferentes camadas de segurança — endpoints, redes, aplicações e nuvem — em uma plataforma unificada [34], [35].

Tradicionalmente, SIEMs e XDRs eram produtos proprietários com licenças comerciais, como Splunk, IBM QRadar e Microsoft Sentinel. Entretanto, nos últimos anos, soluções *open source* ganharam popularidade por oferecerem flexibilidade, auditabilidade do código e ausência de custos de licenciamento, sendo particularmente atrativas para organizações públicas e de menor porte [36].

Entre as vantagens das soluções *open source* destacam-se:

- **Customização**: possibilidade de adaptar a plataforma para atender a requisitos específicos de conformidade e segurança;
- **Integração**: suporte nativo ou facilitado para APIs, ferramentas de IA e outras plataformas de segurança;
- **Comunidade ativa**: colaboração de usuários e desenvolvedores para melhoria contínua, correção de vulnerabilidades e desenvolvimento de novos módulos;
- **Transparência**: acesso ao código-fonte, permitindo auditorias independentes e maior confiança na integridade do sistema [36], [37].

No ecossistema *open source*, destacam-se projetos como OSSEC, TheHive, MISP, Security Onion e Wazuh — este último, um SIEM/XDR que combina recursos avançados de coleta, análise e resposta, além de integração facilitada com modelos de IA e técnicas de *User and Entity Behavior Analytics* (UEBA) [24].

B. A PLATAFORMA WAZUH COMO SIEM/XDR

O Wazuh é uma plataforma de segurança de código aberto que atua como *Security Information and Event Management* (SIEM) e *Extended Detection and Response* (XDR), oferecendo capacidades de monitoramento, detecção e resposta a incidentes em múltiplos ambientes, incluindo servidores, estações de trabalho, contêineres e serviços em nuvem [24]. Sua arquitetura modular é composta por três elementos principais: **agentes**, que coletam dados de endpoints e servidores; o **servidor Wazuh** (ou *manager*), responsável por processar, correlacionar e armazenar eventos; e o **Wazuh indexer e dashboard**, que fornecem indexação, busca e visualização em tempo real, com base no OpenSearch [25].

Como SIEM, o Wazuh executa:

- Coleta e centralização de logs de diversas fontes (sistemas operacionais, aplicações, dispositivos de rede);
- Correlação de eventos com base em regras pré-configuradas;
- Geração de alertas automáticos a partir de padrões suspeitos detectados [24].

No contexto da autenticação, a plataforma é capaz de monitorar e analisar:

- **Windows Event Logs:** eventos como o ID4624 (logon bem-sucedido) e ID4625 (falha de logon), provenientes do *Security Event Channel*;
- **Linux/Unix:** registros em `/var/log/auth.log` e `/var/log/secure`, incluindo tentativas de login, uso de `sudo` e conexões SSH;
- **Serviços e Aplicações Web:** logs de autenticação de servidores Apache, Nginx e sistemas corporativos.

Suas regras pré-definidas permitem detectar comportamentos suspeitos, como múltiplas falhas de login em curto intervalo, logins de contas privilegiadas fora do horário comercial ou a partir de endereços IP não reconhecidos. Esses eventos podem ser correlacionados e enriquecidos com metadados para aumentar a precisão da análise.

Como XDR, o Wazuh expande suas funcionalidades para incluir:

- Detecção baseada em análise comportamental (*behavioral analysis*);
- Resposta ativa a incidentes, via execução automatizada de scripts;
- Integração com inteligência de ameaças e módulos externos de análise.

Um diferencial estratégico é sua API RESTful, que viabiliza integração com soluções de Inteligência Artificial, possibilitando exportar eventos para análise por modelos de *machine learning* ou *User and Entity Behavior Analytics* (UEBA) e reimportar alertas qualificados para acionar a *Active Response* da própria plataforma. Essa capacidade de automação e integração é apontada por Al-Harthy [8] como um fator que torna o Wazuh competitivo frente a SIEMs proprietários, especialmente para organizações que buscam alinhamento com normas e controles nacionais, como o PPSI.

Estudos recentes reforçam que, quando integrada a mecanismos de IA, a plataforma Wazuh pode reduzir significativamente falsos positivos e ampliar a detecção de ameaças complexas, incluindo ataques de autenticação que não seriam identificados apenas por regras estáticas [8], [28].

Essa flexibilidade torna o Wazuh não apenas uma ferramenta robusta para centralizar e correlacionar eventos de segurança, mas também uma base estratégica para implementar soluções avançadas de detecção baseadas em Inteligência Artificial. Ao fornecer dados estruturados e contextualizados, a plataforma permite que modelos de *machine learning* identifiquem padrões sutis e comportamentos anômalos que métodos baseados apenas em regras dificilmente captariam. Essa sinergia entre a capacidade de coleta e correlação do Wazuh e o poder analítico da IA é essencial para evoluir de uma postura reativa para uma abordagem preditiva, conforme explorado na próxima subseção sobre detecção de anomalias e *User and Entity Behavior Analytics* (UEBA).

C. IA E MACHINE LEARNING PARA DETECÇÃO DE ANOMALIAS E UEBA

A aplicação de Inteligência Artificial (IA) e *Machine Learning* (ML) na detecção de anomalias tornou-se um dos pilares da cibersegurança moderna, especialmente para análise de eventos de autenticação. Essas técnicas permitem identificar padrões incomuns de comportamento que podem indicar atividades maliciosas, mesmo quando não correspondem a assinaturas conhecidas ou regras pré-definidas [29], [30].

O conceito de *User and Entity Behavior Analytics* (UEBA) utiliza algoritmos de aprendizado para criar um perfil de comportamento "normal" para cada usuário ou entidade. A partir desse *baseline*, desvios significativos — como logins a partir de localizações geográficas incompatíveis, acessos fora do horário habitual, movimentações laterais não previstas ou alterações abruptas no volume de operações — são sinalizados como potenciais incidentes [32], [33].

A literatura aponta diferentes abordagens algorítmicas para detecção de anomalias:

- **Modelos não supervisionados** — como *Isolation Forest*, *One-Class SVM* e *Random Cut Forest*, eficazes na identificação de padrões atípicos sem a necessidade de dados rotulados [5];
- **Modelos supervisionados** — como *Random Forest* e redes neurais, treinados com dados previamente classificados para distinguir eventos legítimos de maliciosos;
- **Modelos baseados em séries temporais** — como ARIMA e LSTM, capazes de capturar padrões sazonais e tendências de comportamento ao longo do tempo [29], [31];

- **Modelos de aprendizado profundo explicável** — como *Deep Autoencoders* combinados a *Doc2Vec*, que modelam a dinâmica temporal de atividades e oferecem interpretabilidade, requisito essencial em ambientes regulados [7].

Diversos estudos demonstram a aplicação prática dessas técnicas em conjunto com o Wazuh. Chamkar [4] propôs um método híbrido integrando *Random Forest* e *DBSCAN* ao pipeline nativo da plataforma, alcançando acurácia de 97,2% e redução expressiva de falsos positivos. Noman [5] explorou o módulo de *Anomaly Detection* do OpenSearch acoplado ao Wazuh, utilizando *Random Cut Forest* para identificar falhas de login repetitivas e acessos em horários incomuns. Musa [6] apresentou o uso de *Large Language Models* (LLMs), como o Llama 3, para *threat hunting*, permitindo correlação contextual entre eventos e aumento na precisão da triagem de alertas.

Segundo o Artioli [33], UEBA representa o estado da arte na detecção de ameaças baseadas em comportamento, especialmente quando integrado a SIEMs/XDR. No caso do Wazuh, sua arquitetura aberta e API RESTful permitem a ingestão e exportação de eventos para análise externa, bem como o retorno de alertas qualificados para acionar respostas ativas. Essa combinação entre coleta estruturada de dados, análise comportamental avançada e capacidades de resposta reduz falsos positivos, amplia a detecção de ameaças sofisticadas — como ataques distribuídos de autenticação e técnicas de evasão — e eleva o nível de maturidade em segurança das organizações.

No contexto brasileiro, essa abordagem também favorece o atendimento a requisitos normativos e diretrizes estratégicas, sendo particularmente relevante para a conformidade com o Programa de Privacidade e Segurança da Informação (PPSI), que estabelece controles e boas práticas voltados à proteção de dados, prevenção de incidentes e resposta eficaz a ameaças cibernéticas. A seguir, será apresentado o PPSI, destacando seus objetivos, estrutura de controles e relação direta com a abordagem proposta neste estudo.

D. O PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

O *Programa de Privacidade e Segurança da Informação* (PPSI) é uma iniciativa do Governo Federal, coordenada pela Secretaria de Governo Digital, que visa estruturar ações integradas para elevar a maturidade e a resiliência em privacidade e segurança da informação nos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Instituído pela *Portaria SGD/MGI nº 852, de 28 de março de 2023*, o PPSI estabelece diretrizes, metodologias e mecanismos de governança para a gestão desses temas [9].

O PPSI está alinhado a padrões e normas de referência como a *ISO/IEC 27002:2022*, que define boas práticas de segurança da informação, cibersegurança e proteção da privacidade, ao *Center for Internet Security Controls v8* e ao *NIST Cybersecurity Framework*, utilizando-os como base para estruturar seus controles [12]. Essa integração garante que os órgãos públicos adotem uma postura de segurança comparável às melhores práticas internacionais, reforçando a proteção de ativos e dados sensíveis.

O programa está estruturado em cinco áreas temáticas principais:

1) **Governança**: avalia, direciona e monitora as ações do programa, garantindo alinhamento estratégico e engajamento das partes interessadas [9];
2) **Maturidade**: diagnostica o grau de implementação dos controles de privacidade e segurança e acompanha a execução dos planos de trabalho [9];
3) **Metodologia**: define e mantém a estrutura de controles, promovendo boas práticas por meio de guias, processos e modelos [9];
4) **Pessoas**: promove a cultura de privacidade e segurança e coordena o Centro de Excelência em Privacidade e Segurança da Informação [9];
5) **Tecnologia**: coordena o Centro Integrado de Segurança Cibernética (CISC Gov.br), identifica vulnerabilidades e apoia a resposta a incidentes cibernéticos [9].

O PPSI é sustentado por um *Framework de Privacidade e Segurança da Informação*, que deve ser adotado por todos os órgãos do SISP. Esse framework abrange controles, metodologias e ferramentas para identificação e mitigação de lacunas institucionais, estruturando um ciclo contínuo de autoavaliação, análise de lacunas, planejamento e implementação [10], [11]. A primeira autoavaliação, realizada em 2023, estabeleceu a linha de base para os indicadores de maturidade: *iSeg* (segurança da informação) e *iPriv* (privacidade) [11].

Além de orientar a implantação de práticas e tecnologias, o PPSI destaca-se por fomentar a adoção de soluções abertas e integráveis que apoiem diretamente seus controles, como ferramentas SIEM, sistemas de Gestão de Identidade e Acesso (IAM) e mecanismos de autenticação forte. Experiências relatadas na literatura mostram que ferramentas como o Wazuh, quando devidamente configuradas, permitem monitorar eventos de autenticação, detectar padrões anômalos e apoiar a resposta a incidentes, alinhando-se a controles de detecção, análise e mitigação previstos no PPSI [13].

O PPSI está em conformidade com a Lei Geral de Proteção de Dados (LGPD), a Política Nacional de Segurança da Informação (PNSI), e diretrizes da AGU, ANPD, GSI/PR, além de se inspirar em padrões internacionais como ISO, NIST e CIS [10].

III. ANÁLISE DA SOLUÇÃO À LUZ DA LITERATURA

A. CAPACIDADES DO WAZUH PARA MONITORAMENTO DE AUTENTICAÇÃO

A literatura e a documentação oficial do Wazuh descrevem um conjunto robusto de funcionalidades voltadas ao monitoramento de eventos de autenticação. A plataforma coleta e processa logs de diferentes sistemas operacionais e serviços, permitindo a detecção centralizada de atividades suspeitas [24], [25].

Entre as principais fontes de dados para autenticação, destacam-se:

- **Windows**: Eventos de autenticação registrados no *Security Event Log*, incluindo `Event ID 4624` (logon bem-sucedido) e `Event ID 4625` (falha de logon);
- **Linux/Unix**: Registros no arquivo `/var/log/auth.log`, contendo tentativas de login locais e via SSH;
- **Serviços de diretório**: Integração com Active Directory e LDAP para monitoramento de autenticações centralizadas [25], [27].

O Wazuh disponibiliza regras pré-configuradas para identificação de múltiplas falhas de login em um intervalo curto de tempo, detecção de uso de contas desativadas, e tentativas de acesso provenientes de endereços IP suspeitos. Essas regras podem ser adaptadas e enriquecidas por meio de correlação personalizada e integração com feeds de inteligência de ameaças (*threat intelligence*) [26].

Além do processamento interno, a plataforma expõe uma **API RESTful** que permite a exportação de dados e a integração com mecanismos externos de análise, incluindo módulos de Inteligência Artificial para detecção comportamental (*UEBA*) e sistemas de resposta automática. Isso viabiliza arquiteturas híbridas nas quais o Wazuh atua como camada de coleta e pré-processamento, enquanto algoritmos externos realizam análises mais avançadas [8], [28].

Estudos demonstram que, ao combinar o monitoramento nativo do Wazuh com algoritmos de IA, é possível reduzir significativamente o número de falsos positivos e aumentar a detecção de anomalias de autenticação, incluindo padrões de *password spraying*, logins geograficamente incompatíveis (*impossible travel*) e acessos fora do horário de expediente [8].

B. MODELOS DE IA PARA ANÁLISE DE LOGS DE ACESSO

A aplicação de Inteligência Artificial (IA) para análise de logs de autenticação permite identificar comportamentos anômalos que, muitas vezes, não seriam detectados por regras estáticas de correlação. A literatura indica que, para este fim, modelos de aprendizado de máquina — especialmente os de aprendizado não supervisionado — são eficazes na detecção de padrões fora do normal [29], [31].

Entre os algoritmos mais utilizados para detecção de anomalias em dados de autenticação, destacam-se:

- **Isolation Forest**: modelo baseado em árvores de decisão que isola pontos de dados atípicos de forma eficiente, mesmo em grandes volumes de informação;
- **One-Class SVM**: algoritmo que aprende a delimitar a região de alta densidade dos dados normais, identificando como anomalias os pontos fora dessa região;
- **Modelos baseados em séries temporais**: como LSTM (*Long Short-Term Memory*), capazes de aprender sequências de eventos e detectar mudanças abruptas de padrão;
- **Modelos supervisionados**: como *Random Forest* e redes neurais profundas, utilizados quando há disponibilidade de dados rotulados para treinar classificadores de eventos legítimos e maliciosos.

O conceito de *User and Entity Behavior Analytics* (UEBA) é central nesse contexto, pois envolve a criação de um perfil de comportamento normal para cada usuário ou entidade e a detecção de desvios significativos. Exemplos de anomalias detectáveis por UEBA incluem:

- *Impossible travel*: tentativas de login a partir de localizações geográficas incompatíveis no intervalo de tempo observado;
- Acessos fora do horário habitual de trabalho;
- Ataques distribuídos de *password spraying*;
- Uso anômalo de contas com privilégios administrativos [32], [33].

Estudos recentes demonstram que a integração de modelos de IA com plataformas SIEM/XDR, como o Wazuh, pode reduzir falsos positivos e aumentar a detecção de ataques sofisticados [8], [28]. Essa abordagem também favorece a detecção de ameaças desconhecidas (*zero-day*), já que o modelo não depende de assinaturas pré-definidas, mas sim da análise comportamental dos eventos [31].

C. ARQUITETURA TEÓRICA DA INTEGRAÇÃO WAZUH + IA

Com base na literatura revisada, propõe-se uma arquitetura conceitual que integra a plataforma Wazuh a um módulo de Inteligência Artificial (IA) para análise comportamental e detecção de anomalias em serviços de autenticação. Essa arquitetura visa potencializar a detecção precoce de ameaças, reduzir falsos positivos e alinhar as ações de resposta aos controles estabelecidos pelo PPSI.

O fluxo proposto é composto pelas seguintes etapas:

1) **Coleta de Logs:** agentes do Wazuh instalados em endpoints e servidores capturam eventos de autenticação de múltiplas origens (Windows, Linux, aplicações web).
2) **Análise Inicial no Wazuh Manager:** aplicação das regras pré-configuradas do Wazuh para filtragem e classificação básica de eventos.
3) **Exportação via API RESTful:** eventos relevantes são enviados, em tempo quase real, para o módulo de IA externo.
4) **Análise Comportamental/UEBA:** modelos de ML (ex.: Isolation Forest, Deep Autoencoders) processam os dados, detectando anomalias como "viagem impossível" ou acessos fora do padrão horário/geográfico.
5) **Retorno ao Wazuh:** alertas qualificados são reimportados no Wazuh para registro, visualização no dashboard e possível acionamento da *Active Response*.
6) **Resposta Ativa:** bloqueio automático de IPs, encerramento de sessões e notificações aos analistas de SOC.

A Figura 1 ilustra esse fluxo.

Estudos como os de Chamkar [4] e Noman [5] comprovam a viabilidade técnica dessa integração, enquanto Musa [6]

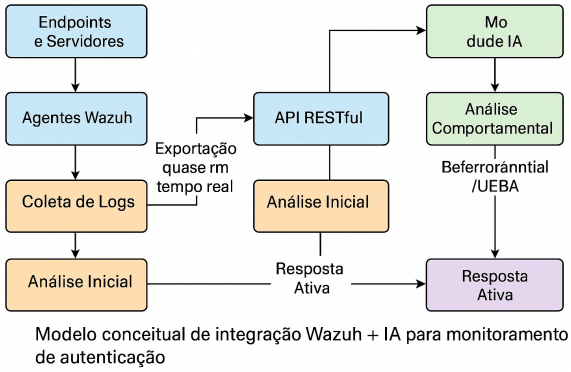

FIGURE 1. Modelo conceitual de integração Wazuh + IA para monitoramento de autenticação.

destaca os ganhos de contexto e precisão trazidos por modelos de IA avançados. Essa arquitetura também é compatível com recomendações de segurança do PPSI, permitindo mapeamento direto a controles de detecção, resposta e mitigação.

IV. MAPEAMENTO COM OS CONTROLES DO PPSI

O mapeamento a seguir relaciona as funcionalidades do modelo conceitual de integração Wazuh + IA com os controles específicos do *Programa de Privacidade e Segurança da Informação* (PPSI). Esse alinhamento visa demonstrar a aderência teórica da solução aos requisitos estabelecidos no framework, reforçando sua viabilidade no contexto do setor público.

A. DESCRIÇÃO DO ATENDIMENTO AOS CONTROLES

1.5 / 1.6 — Endereçar e tratar ativos não autorizados O Wazuh utiliza agentes para inventariar hardware e software, detectando dispositivos não cadastrados. A integração com IA pode analisar padrões de conexão e identificar comportamentos atípicos, como dispositivos legítimos operando em locais ou horários incomuns, permitindo resposta mais rápida.

2.2 — Software atualmente suportado Monitora integridade e versão de softwares, identificando aplicações obsoletas. Modelos de Machine Learning podem prever riscos associados a determinados softwares com base em vulnerabilidades conhecidas e histórico de incidentes.

2.3 — Lista de permissões de software autorizado Controla a execução de processos cruzando com listas de softwares autorizados. Algoritmos de IA podem classificar automaticamente novos softwares detectados, reduzindo o esforço manual.

2.5 — Lista de permissões de scripts autorizados Valida scripts executados contra listas permitidas. A análise comportamental pode identificar scripts que, mesmo autorizados, passam a apresentar padrões de uso suspeitos.

2.7 — Endereçar software não autorizado Gera alertas para execuções não autorizadas. Modelos de detecção de anomalias podem diferenciar entre um falso positivo e uma instalação maliciosa disfarçada.

3.14 — Registrar acesso a dados sensíveis O Wazuh coleta logs de acesso a arquivos e bases de dados sensíveis. Com UEBA, é possível detectar acessos fora do perfil habitual de cada usuário, como tentativas de leitura em massa de arquivos ou consultas em horários incomuns.

4.6 — Gerenciar com segurança os ativos e software Inventário contínuo aliado à coleta segura. A IA auxilia na priorização de ativos com base no risco e criticidade para a organização.

5.1 — Inventário de contas Gera inventário de contas a partir de logs de autenticação. Modelos de análise comportamental podem indicar contas que, embora ativas, apresentam padrões de uso incompatíveis com a função atribuída.

5.3 — Desabilitar contas inativas Identifica contas sem uso por períodos configuráveis. A IA pode prever a probabilidade de abuso de contas inativas com base em padrões históricos.

5.5 — Inventário de contas de serviço Monitora contas de serviço a partir de eventos de sistema. UEBA pode detectar quando uma conta de serviço passa a realizar operações atípicas.

7.1 — Processo de gestão de vulnerabilidade Integra com scanners (OpenVAS, Nessus) e correlaciona no SIEM. A IA

TABLE 1. Mapeamento das Capacidades do Wazuh aos Controles do PPSI

Controle PPSI	Capacidades do Wazuh que Atendem ao Controle
1.5 / 1.6	Descoberta e inventário de ativos via agentes; alertas para dispositivos não autorizados na rede.
2.2	Monitoramento de integridade e detecção de software desatualizado ou sem suporte.
2.3	Listagem de software autorizado com geração de alertas para execuções fora da lista.
2.5	Controle e monitoramento de execução de scripts conforme lista autorizada.
2.7	Detecção e alerta para softwares não autorizados.
3.14	Coleta e análise de logs de acesso a dados sensíveis; integração com UEBA para anomalias.
4.6	Inventário contínuo de ativos e software com segurança na coleta e armazenamento.
5.1	Relatórios de inventário de contas de usuários a partir de logs de autenticação.
5.3	Identificação de contas inativas com base em registros de login.
5.5	Inventário de contas de serviço monitoradas em logs de sistema.
7.1	Integração com scanners de vulnerabilidade e correlação no SIEM.
8.1	Gestão centralizada de logs de auditoria com retenção segura.
8.5	Coleta de logs detalhados de múltiplas fontes (SO, aplicações, dispositivos de rede).
10.7	Detecção de comportamento suspeito indicativo de malware por regras de comportamento.
13.3	Prevenção de intrusão baseada em host por monitoramento e resposta ativa.
13.7	Centralização e correlação de alertas de segurança no servidor Wazuh.
13.8	Detecção de intrusão baseada em host via regras e análise de logs.
13.11	Ajuste dinâmico de limites e thresholds de alertas conforme baseline.

pode ajudar a priorizar correções de acordo com o contexto de exploração em tempo real.

8.1 — Processo de gestão de log de auditoria Centraliza e armazena logs de forma segura. Algoritmos de detecção de anomalias ajudam a identificar inconsistências ou manipulações em registros.

8.5 — Coleta de logs detalhados Capta dados de múltiplas fontes. A IA pode correlacionar eventos dispersos e identificar ameaças que passariam despercebidas na análise isolada.

10.7 — Anti-malware baseado em comportamento Detecta padrões suspeitos de execução que indicam malware, mesmo sem assinatura conhecida. Modelos como Isolation Forest ou Autoencoders permitem detectar ataques zero-day.

13.3 — Prevenção de intrusão baseada em host Monitora tentativas de intrusão e pode acionar respostas ativas. Com IA, a precisão de detecção é aumentada pela análise contínua de comportamento.

13.7 — Centralização de alertas de segurança Todos os eventos são correlacionados no servidor central. O uso de IA reduz sobrecarga ao agrupar alertas relacionados e priorizar incidentes mais críticos.

13.8 — Detecção de intrusão baseada em host Analisa logs e eventos para detectar anomalias. UEBA aprimora essa detecção ao criar perfis de comportamento e alertar apenas para desvios significativos.

13.11 — Ajuste de limites de alertas de segurança Permite ajustes dinâmicos nos thresholds com base em comportamento histórico. A IA automatiza esse ajuste, reduzindo falsos positivos e adaptando a detecção a mudanças legítimas no ambiente.

V. DISCUSSÃO

A literatura analisada aponta que a integração de plataformas SIEM/XDR, como o Wazuh, com técnicas de Inteligência Artificial (IA) e Análise Comportamental (UEBA) pode elevar significativamente a capacidade de detecção de ameaças, especialmente em cenários de autenticação. Estudos recentes [7], [33], [36] evidenciam ganhos substanciais na acurácia dos alertas e na redução de falsos positivos quando modelos de aprendizado supervisionado e não supervisionado são aplicados a dados de logs, em comparação a regras estáticas tradicionais. Esses resultados indicam que abordagens híbridas — combinando regras pré-configuradas e modelos adaptativos — oferecem melhor equilíbrio entre sensibilidade e precisão.

Entretanto, os mesmos trabalhos ressaltam desafios técnicos relevantes. A complexidade na implementação de modelos de *machine learning* em ambientes de produção envolve desde a escolha do algoritmo até o processo contínuo de ajuste fino (*tuning*), passando pela definição de métricas de desempenho adequadas. Outro ponto crítico é a construção de uma linha de base comportamental confiável: uma calibragem inadequada pode levar tanto à subdetecção de ataques quanto à emissão excessiva de falsos positivos [29], [31].

Como estratégias de mitigação, a literatura sugere práticas como: (i) uso de dados sintéticos e históricos para treinamento e validação incremental dos modelos; (ii) integração de *feedback* humano no ciclo de revisão dos alertas, aproveitando a expertise do time de segurança; e (iii) adoção de *pipelines* de MLOps para automatizar atualização de modelos e versionamento de *datasets* [34].

No contexto do setor público, as vantagens identificadas tornam-se ainda mais relevantes. Órgãos governamentais lidam com dados sensíveis, operam sob forte pressão por conformidade normativa e são alvos frequentes de ataques direcionados. A integração de IA ao Wazuh, mapeada aos controles do PPSI, não apenas aprimora a detecção de ameaças, mas também reforça a governança e a rastreabilidade das ações de segurança, alinhando-se às diretrizes de modernização e eficiência do Governo Digital.

Por fim, tendências emergentes apontadas em estudos recentes incluem o uso de modelos de linguagem de grande porte (LLMs) para contextualizar alertas e gerar relatórios interpretáveis para equipes não técnicas, além da integração de UEBA com arquiteturas *Zero Trust* e plataformas XDR abertas. Essas perspectivas sugerem que soluções como a proposta neste trabalho têm potencial para evoluir de forma contínua, incorporando novas camadas de inteligência e automação.

VI. CONCLUSÃO

Com base na revisão sistemática e técnica realizada, foi possível estabelecer um modelo teórico robusto para a integração da plataforma Wazuh com técnicas de Inteligência Artificial voltadas à análise comportamental (UEBA), demonstrando de forma consistente sua aderência aos controles do Programa de Privacidade e Segurança da Informação (PPSI). O estudo atendeu aos objetivos propostos, identificando os principais vetores de ataque a serviços de autenticação, descrevendo as capacidades nativas do Wazuh, investigando técnicas de detecção de anomalias por IA e construindo um mapeamento entre as funcionalidades da solução proposta e os controles do PPSI.

A análise evidenciou que a adoção de abordagens híbridas — combinando regras de correlação pré-configuradas do Wazuh com modelos de aprendizado de máquina — oferece ganhos significativos em acurácia e redução de falsos positivos, ao mesmo tempo em que amplia a detecção de ameaças desconhecidas (*zero-day*). Além disso, a integração com frameworks comportamentais como UEBA se mostrou alinhada às práticas mais modernas de segurança, conforme apontado na literatura [7], [36].

Do ponto de vista estratégico, a implementação de uma arquitetura integrada Wazuh+IA apresenta alto potencial de impacto no setor público, pois não apenas reforça a postura de segurança cibernética, mas também contribui para o cumprimento de normativas nacionais e padrões internacionais de segurança da informação. Esse alinhamento com o PPSI garante que a solução proposta seja tecnicamente sólida e regulatoriamente aderente.

Como trabalho futuro, propõe-se a implementação de uma prova de conceito (PoC) para validar empiricamente os achados teóricos aqui discutidos, medindo o desempenho do modelo integrado em cenários reais e avaliando métricas como tempo médio de detecção (MTTD), tempo médio de resposta (MTTR) e taxa de falsos positivos. Essa etapa permitirá refinar o modelo, adaptá-lo às particularidades operacionais do setor público e explorar a aplicação de novas tecnologias emergentes, como modelos de linguagem de grande porte (LLMs) para análise contextual de eventos de segurança. Dessa forma, a pesquisa aqui apresentada não se encerra, mas estabelece uma base sólida para um ciclo contínuo de evolução tecnológica e aderência regulatória, alinhado às diretrizes de modernização do Governo Digital.

REFERENCES

[1] E. J. Ribeiro, J. P. de Camargo, V. J. R. Barbosa, R. R. de Lima, and F. C. de Souza, "TECNOLOGIA EDUCACIONAL E CIBERSEGURANÇA: UMA ALIANÇA NECESSÁRIA," *Lumen et Virtus*, vol. 16, no. 49, pp. 7556–7567, Jun. 2025, doi:10.56238/levv16n49-094.

[2] G. Nebbione and M. C. Calzarossa, "A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments," *IEEE Access*, vol. 11, pp. 15119–15130, 2023, doi:10.1109/ACCESS.2023.3244490.

[3] T. Hase, "The Path to Choosing a SIEM System – A Systematic Literature Review," *FH Wedel University of Applied Sciences*, 2024. [Online]. Available: https://www.fh-wedel.de/fileadmin/Mitarbeiter/Records/Hase_2024_-_The_Path_to_Choosing_a_SIEM_System_-_A_Systematic_Literature_Review.pdf

[4] S. A. Chamkar et al., "Improving Threat Detection in Wazuh Using Machine Learning Techniques," *J. Cybersecur. Priv.*, vol. 5, no. 2, p. 34, Jun. 2025, doi:10.3390/jcp5020034.

[5] A. Al Noman, "Enhancing IT security with anomaly detection in Wazuh," *Wazuh Blog*, Oct. 12, 2023. [Online]. Available: https://wazuh.com/blog/enhancing-it-security-with-anomaly-detection/

[6] F. Musa, "Leveraging artificial intelligence for threat hunting in Wazuh," *Wazuh Blog*, Jun. 13, 2025. [Online]. Available: https://wazuh.com/blog/leveraging-artificial-intelligence-for-threat-hunting-in-wazuh/

[7] J. Fuentes, I. Ortega-Fernández, N. M. Villanueva, and M. Sestelo, "Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders," *arXiv preprint*, arXiv:2505.11542, May 2025. [Online]. Available: https://arxiv.org/abs/2505.11542

[8] A. R. Al-Harthy, "Augmenting Wazuh SIEM with machine learning for advanced cyber threat analytics," EJE-CIP (European Journal of Emerging Computation and Information Processing), 2024. [Online]. Available: https://parthenonfrontiers.com/index.php/ejecip/article/view/84.

[9] Brasil, Secretaria de Governo Digital, "Programa de Privacidade e Segurança da Informação (PPSI)," Portal Governo Digital, atualizado em 20 Mar. 2024. [Online]. Available: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-atual. Accessed: 10 Aug. 2025.

[10] Brasil, Secretaria de Governo Digital, "Framework de Privacidade e Segurança da Informação — Guias e Modelos," Portal Governo Digital, 2023. [Online]. Available: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos. Accessed: 10 Aug. 2025.

[11] Instituto Federal de Minas Gerais (IFMG), "PPSI – Programa de Privacidade e Segurança da Informação," Portal IFMG, publicado 27 Jun. 2025, última modificação 10 Jul. 2025. [Online]. Available: https://www.ifmg.edu.br/portal/seguranca-da-informacao/ppsi-programa-de-privacidade-e-seguranca-da-informacao. Accessed: 10 Aug. 2025.

[12] L. B. P. Tomaz, P. A. Oliveira, and É. S. Gualberto, "Investigação da ferramenta Keycloak na Mitigação de Incidentes Cibernéticos: Uma Abordagem Integrada com o Programa de Privacidade e Segurança da Informação (PPSI)," in *Anais Estendidos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, 2024, pp. 1–4.

[13] W. S. Aguiar, "Configuração e aplicação de um SOC (Security Operation Center) gratuito: um estudo prático para aplicação do SIEM Wazuh," in *Proceedings of the 19th CONTECSI – International Conference on Information Systems and Technology Management*, São Paulo, Brazil, Dec. 2022, pp. 1–15.

[14] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *Journal of Network and Computer Applications*, vol. 188, Art. 103080, 2021, doi:10.1016/j.jnca.2021.103080.

[15] H. R. El-Taj, D. Hamedah, and R. Saeed, "Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry," *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 1, pp. 935–948, 2025, doi:10.22399/ijcesen.754.

[16] A. M. Alnajim, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Defense Mechanisms," *Technologies*, vol. 11, no. 6, p. 161, 2023, doi:10.3390/technologies11060161.

[17] H. Fereidouni, "IoT and Man-in-the-Middle Attacks," *Internet Technology Letters*, vol. 8, no. 1, e70016, 2025, doi:10.1002/spy2.70016.

[18] A. M. Alnajim, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Defense Mechanisms," *Technologies*, vol. 11, no. 6, p. 161, 2023, doi:10.3390/technologies11060161.

[19] T. Vasilas, I. Mavridis, and D. Kavallieros, "Beat the Heat: Syscall Attack Detection via Thermal Side-Channel Analysis," *Future Internet*, vol. 16, no. 8, p. 301, 2024, doi:10.3390/fi16080301.

[20] H. Gao, Z. Liu, X. Chang, X. Liu, and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing," *arXiv preprint*, arXiv:1306.2882, Jun. 2013. [Online]. Available: https://arxiv.org/abs/1306.2882

[21] D. Pöhn and W. Hommel, "TaxIdMA: Towards a Taxonomy for Attacks related to Identities," *arXiv preprint*, arXiv:2301.00443, Jan. 2023. [Online]. Available: https://arxiv.org/abs/2301.00443

[22] D. Pöhn and W. Hommel, "Towards an Improved Taxonomy of Attacks related to Digital Identities and Identity Management Systems," *arXiv preprint*, arXiv:2407.16718, Jul. 2024. [Online]. Available: https://arxiv.org/abs/2407.16718

[23] M. Campobasso and L. Allodi, "Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)*, 2020, pp. 1665–1680, doi:10.1145/3372297.3417892.

[24] Wazuh, "Wazuh: The Open Source Security Platform," 2025. [Online]. Available: https://wazuh.com. Accessed: 10 Aug. 2025.

[25] Wazuh, "Wazuh Documentation," 2025. [Online]. Available: https://documentation.wazuh.com. Accessed: 10 Aug. 2025.

[26] Wazuh, "Use cases and examples," 2025. [Online]. Available: https://wazuh.com/resources/use-cases/. Accessed: 10 Aug. 2025.

[27] Wazuh, "Monitoring Active Directory logons with Wazuh" (seção de proof-of-concepts), Wazuh Documentation, 2024. [Online]. Available: https://documentation.wazuh.com — via conteúdo realocado. Accessed: 10 Aug. 2025.

[28] F. Ismail, "Wazuh Security Event Response with Retrieval-Augmented Generation," *Sensors*, vol. 25, no. 3, Art. 870, 2025, doi:10.3390/s25030870.

[29] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Generation Computer Systems*, vol. 55, pp. 278–288, 2016.

[30] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, Article 15, Jul. 2009, doi:10.1145/1541880.1541882.

[31] H. Huang, P. Wang, J. Pei, J. Wang, S. Alexanian, and D. Niyato, "Deep Learning Advancements in Anomaly Detection: A Comprehensive Survey," arXiv preprint arXiv:2503.13195, Mar. 2025. [Online]. Available: https://arxiv.org/abs/2503.13195. Accessed: 10 Aug. 2025.

[32] J. Fuentes, I. Ortega-Fernández, N. M. Villanueva, and M. Sestelo, "Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders," *arXiv preprint*, arXiv:2505.11542, May 2025. [Online]. Available: https://arxiv.org/abs/2505.11542. Accessed: 10 Aug. 2025.

[33] P. Artioli, et al., "A comprehensive investigation of clustering algorithms for UEBA," *Frontiers in Big Data*, 2024. doi:10.3389/fdata.2024.1375818.

[34] D. L. Pissanidis and K. Demertzis, "Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and its Application in Intrusion Detection and System Log Management," preprint, Dec. 2023, doi:10.20944/preprints202312.0205.v1.

[35] M. Sheeraz, M. A. Paracha, M. Ul Haque, M. H. Durad, S. M. Mohsin, S. S. Band, and A. Mosavi, "Effective Security Monitoring Using Ef-

ficient SIEM Architecture," *Human-centric Computing and Information Sciences*, vol. 13, no. 17, 2023, doi:10.22967/HCIS.2023.13.017.

[36] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLoS ONE*, vol. 19, no. 3, p. e0301183, 2024, doi:10.1371/journal.pone.0301183.

[37] A. Asswad, "Analysis of attacks and prevention methods in cybersecurity," M.Sc. thesis, Università degli Studi di Brescia, 2022. [Online]. Available: https://ans.unibs.it/assets/documents/thesis/Thesis_Annas_Asswad.pdf. Accessed: 10 Aug. 2025.