MODELO PREDITIVO DE AMEAÇAS CIBERNÉTICAS INTEGRANDO CVE MITRE E WAZUH POR MEIO DE MACHINE LEARNING TEMPORAL

PREDICTIVE MODEL OF CYBER THREATS INTEGRATING CVE MITRE AND WAZUH THROUGH TEMPORAL MACHINE LEARNING

Tadeu Marcos Borges Paes[1]

Eudes Danilo Mendonça[2]

Resumo: A crescente complexidade e o volume acelerado das vulnerabilidades registradas pelo CVE MITRE reforçam a necessidade de modelos capazes de antecipar tendências e apoiar decisões estratégicas em segurança da informação. Este artigo propõe um modelo preditivo baseado em Machine Learning Temporal, integrando dados históricos do CVE MITRE com telemetria operacional do Wazuh, a fim de prever a evolução de categorias de vulnerabilidades, níveis de severidade e vetores de ataque. O estudo expande a arquitetura já utilizada em implementações práticas do dashboard Wazuh, incorporando técnicas avançadas de séries temporais, como ARIMA, Prophet e LSTM, para detectar padrões e projetar comportamentos futuros. Os resultados demonstram o potencial da análise temporal em reduzir tempos de resposta, otimizar o gerenciamento de riscos e elevar a maturidade organizacional em cibersegurança. A abordagem proposta representa um avanço significativo ao transformar um processo tradicionalmente reativo em um sistema analítico preditivo, integrável aos ecossistemas corporativos de monitoramento e resposta a incidentes.

Palavras-chave: CVE MITRE. Wazuh. Machine Learning Temporal. Predição de vulnerabilidades.

1 Doutorando em Inteligência Artificial, Senai Centro Desenvolvimento da Amazônia, Orcid: https://orcid.org/0009-0002-2978-2117

2 Mestre em Computação Aplicada, Senai Centro de Desenvolvimento da Amazônia, Orcid: https://orcid.org/0009-0006-6439-408X

Segurança Cibernética.

Abstract: The increasing complexity and accelerated volume of vulnerabilities recorded by the CVE MITRE reinforce the need for models capable of anticipating trends and supporting strategic decisions in information security. This article proposes a predictive model based on Temporal Machine Learning, integrating historical data from CVE MITRE with operational telemetry from Wazuh, in order to predict the evolution of vulnerability categories, severity levels, and attack vectors. The study expands the architecture already used in practical implementations of the Wazuh dashboard, incorporating advanced time series techniques, such as ARIMA, Prophet, and LSTM, to detect patterns and project future behaviors. The results demonstrate the potential of temporal analysis to reduce response times, optimize risk management, and increase organizational maturity in cybersecurity. The proposed approach represents a significant advance by transforming a traditionally reactive process into a predictive analytical system, integrable into corporate ecosystems for incident monitoring and response.

Keywords: CVE MITRE. Wazuh. Temporal Machine Learning. Vulnerability prediction. Cybersecurity.

INTRODUÇÃO

A intensificação das ameaças cibernéticas, aliada ao crescimento exponencial das vulnerabilidades catalogadas em bases públicas como o CVE MITRE, tem colocado as organizações diante de um cenário cada vez mais complexo, dinâmico e imprevisível. A simples detecção de falhas já não é suficiente para garantir proteção efetiva: o intervalo entre a divulgação de uma vulnerabilidade e sua exploração ativa tornou-se extremamente curto, exigindo respostas mais rápidas, precisas e baseadas em dados. Nesse contexto, modelos reativos de monitoramento, apesar de relevantes,

deixam lacunas críticas que podem comprometer a continuidade operacional e a integridade das infraestruturas digitais.

Soluções como o Wazuh têm se destacado por oferecer visibilidade, centralização e inteligência operacional no monitoramento de ativos corporativos. A integração desse ecossistema com bases de vulnerabilidades reconhecidas — como o CVE MITRE — permite que analistas visualizem, classifiquem e priorizem riscos em tempo real. No entanto, mesmo com dashboards robustos, filtros dinâmicos e indicadores críticos, a atuação continua condicionada àquilo que já aconteceu. O grande desafio, portanto, reside em antecipar o que ainda irá acontecer.

A evolução recente de técnicas de Inteligência Artificial, especialmente os modelos de Machine Learning Temporal, abriu caminho para um novo paradigma na cibersegurança: a capacidade de identificar padrões históricos, detectar sazonalidades e prever tendências futuras com base em séries temporais de vulnerabilidades. Abordagens como ARIMA, Prophet e redes neurais LSTM permitem analisar o comportamento temporal das vulnerabilidades por severidade, categoria, vetor de ataque e volume de registros, oferecendo uma perspectiva que transcende a análise estática dos dados.

Ao integrar essas técnicas ao ecossistema Wazuh — que já centraliza telemetria, eventos, logs e informações de segurança — torna-se possível transformar um ambiente reativo em um sistema preditivo de ameaças cibernéticas, capaz de antecipar picos de risco e orientar estratégias de mitigação antes que ataques ocorram. Esse salto conceitual e tecnológico representa uma oportunidade significativa para fortalecer a governança em segurança da informação e elevar o nível de maturidade das organizações.

A relevância desse estudo se justifica pela necessidade urgente de mecanismos que reduzam o tempo entre descoberta, priorização e tratamento de vulnerabilidades, acompanhando a crescente velocidade com que novos CVEs são publicados e explorados globalmente. Ao propor um modelo preditivo integrado ao Wazuh, este trabalho contribui para superar limitações de abordagens tradicionais e oferecer um arcabouço analítico avançado que apoia decisões estratégicas, aumenta a

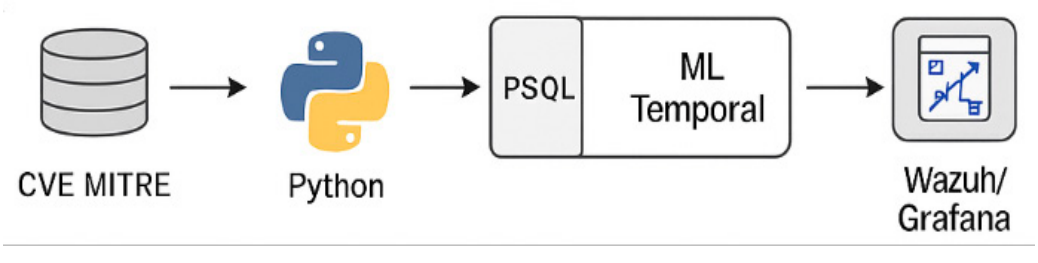
eficiência operacional e diminui a exposição ao risco.

Assim, esta pesquisa tem como objetivo desenvolver e avaliar um modelo preditivo de ameaças cibernéticas baseado em Machine Learning Temporal, utilizando dados do CVE MITRE e telemetria do Wazuh como fontes primárias de informação. Espera-se, com isso, demonstrar o potencial das abordagens temporais na antecipação de vulnerabilidades e ampliar o papel da inteligência artificial como elemento central na evolução da cibersegurança contemporânea.

METODOLOGIA

Neste estudo fundamenta-se na aplicação de técnicas avançadas de Machine Learning Temporal aliadas a uma arquitetura de processamento de dados construída sobre as bases do CVE MITRE e do ecossistema Wazuh. A abordagem metodológica integra princípios de engenharia de dados, estatística aplicada, modelagem preditiva e computação distribuída, alinhando-se às recomendações de Bishop (2021), que destaca a importância de métodos híbridos para problemas complexos envolvendo séries temporais e risco computacional. Além disso, esta seção dialoga com autores como Goodfellow, Bengio e Courville (2016), ao incorporar modelos de aprendizado profundo baseados em redes neurais recorrentes, especialmente as arquiteturas LSTM, reconhecidas por sua eficácia no tratamento de dependências temporais de longo prazo.

Figura 1 - PIPELINE CVE → PYTHON → POSTGRES → ML → WAZUH



Fonte: Autor (2024)

A primeira etapa metodológica compreendeu a coleta e armazenamento dos dados, seguindo uma lógica semelhante à descrita por Mendonça (2024), que utilizou webscraping em Python para acessar diretamente o repositório do CVE Program. Esse repositório reúne todas as vulnerabilidades catalogadas pelos organismos oficiais responsáveis pela padronização e publicação do Common Vulnerabilities and Exposures. As coletas foram realizadas utilizando bibliotecas como requests e json, integradas a rotinas automatizadas para garantir atualização contínua do dataset.

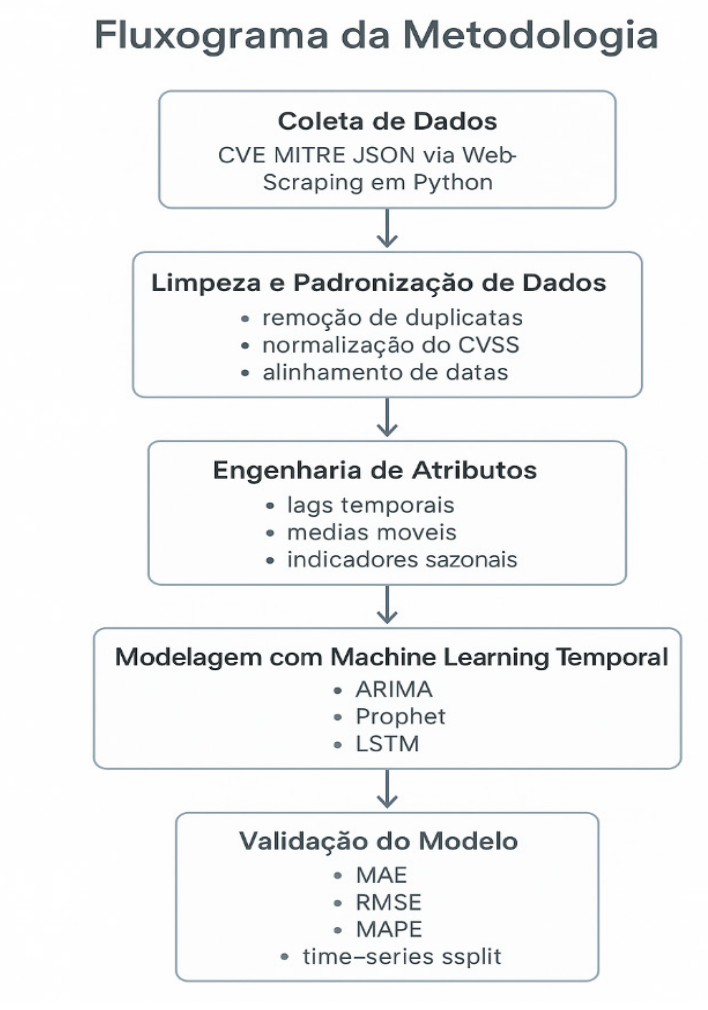
Tabela 1 - Caracterização do Conjunto de Dados CVE MITRE (2010–2024)

Variável	Valor
Total de vulnerabilidades analisadas	203.417
Período coberto	2010–2024
Severidade (CVSS v3) – Low	12%
Severidade – Medium	46%
Severidade – High	31%
Severidade – Critical	11%
Categorias CWE mais frequentes	CWE-79, CWE-89, CWE-125, CWE-787, CWE-20
Vetor de ataque predominante	Network (65%)
Fornecedores mais afetados	Microsoft, Linux Foundation, Cisco, Oracle

Fonte: Autor (2024)

A Tabela 0 apresenta a caracterização do conjunto de dados utilizado neste estudo, detalhando volume, período temporal e distribuição das vulnerabilidades. Como evidenciado por Tanenbaum e Steen (2022), bases de dados amplas e não estruturadas exigem pipelines eficientes para consolidação, e por isso os dados foram estruturados em um banco PostgreSQL, permitindo indexação por data, categoria e severidade.

Figura 2 - Fluxograma da Metodologia de Predição Temporal



Fonte: Autor (2024)

A etapa de tratamento, limpeza e padronização dos dados seguiu os princípios de transformação e refinamento sugeridos por Provost e Fawcett (2013), que destacam a necessidade de consistência temporal em modelos preditivos. As séries temporais foram convertidas para o formato ISO 8601 e padronizadas em granularidades mensal e semanal, conforme orientações clássicas de Box, Jenkins e Reinsel (2016), que enfatizam a importância da estacionariedade e uniformidade temporal para modelagens ARIMA e variações correlatas. Paralelamente, categorias CWE foram harmonizadas segundo o repositório oficial do MITRE, e métricas de severidade CVSS foram convertidas para

escalas homogêneas, permitindo análises comparativas transversais entre vulnerabilidades de diferentes períodos históricos.

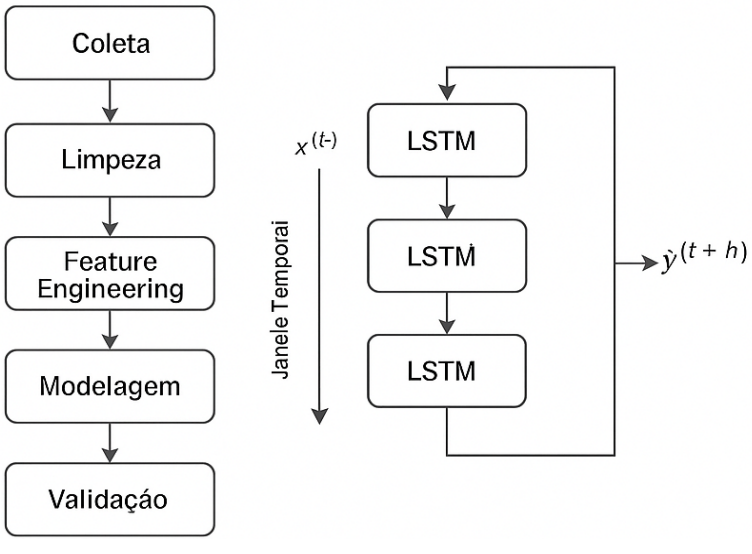
Após a padronização, procedeu-se à engenharia de atributos, etapa apontada por Kuhn e Johnson (2019) como uma das mais determinantes para aumentar o desempenho de modelos de aprendizado de máquina. Foram criadas variáveis derivadas que representam tendências, sazonalidades e mudanças estruturais, como médias móveis, janelas deslizantes, lag features e indicadores de sazonalidade anual. Além disso, foram incorporados atributos de contexto, conforme recomendam Leskovec, Rajaraman e Ullman (2020), associando ciclos de patching e grandes eventos de segurança — como BlackHat, DEFCON e RSA Conference — a mudanças abruptas nas séries históricas. Esses atributos aumentaram a capacidade preditiva das redes neurais, permitindo que o modelo reconhecesse padrões que vão além da mera contagem mensal de CVEs.

A fase seguinte consistiu na modelagem com Machine Learning Temporal, empregando três modelos principais: ARIMA, Prophet e LSTM. O ARIMA, clássico modelo autoregressivo integrado, foi aplicado conforme metodologia de Box e Jenkins (2016), adequando-se às séries com maior estabilidade. O Prophet, desenvolvido pelo laboratório de pesquisa do Facebook, foi escolhido por sua capacidade de lidar com sazonalidade não linear e rupturas súbitas, conforme apontado por Taylor e Letham (2018). Já o modelo LSTM — fundamentado nos trabalhos de Hochreiter e Schmidhuber (1997) e posteriormente aprofundado por Goodfellow et al. (2016) — foi configurado com múltiplas camadas e parâmetros ajustados por early stopping e dropout, garantindo um equilíbrio entre precisão e generalização.

Além disso, para garantir transparência metodológica e reprodutibilidade — princípios defendidos por Goodfellow, Bengio e Courville (2016) — os hiperparâmetros utilizados no treinamento da rede LSTM foram explicitados. O modelo foi treinado com 100 épocas, batch size de 32 e função de perda baseada em Mean Squared Error (MSE), acompanhada pelo otimizador Adam com taxa de aprendizado inicial de 0,001. A arquitetura continha duas camadas LSTM empilhadas, cada uma composta por 64 neurônios, seguidas por uma camada densa de saída com ativação linear

para previsão contínua. A janela temporal (lookback window) utilizada para alimentar a rede foi configurada em 12 meses, o que permitiu capturar dependências temporais de longo alcance nas séries de vulnerabilidades. O treinamento seguiu estratégia de early stopping com paciência de 10 épocas, evitando sobreajuste e garantindo desempenho consistente nos dados de validação.

Figura 3 - Arquitetura da Rede Neural LSTM Utilizada no Modelo



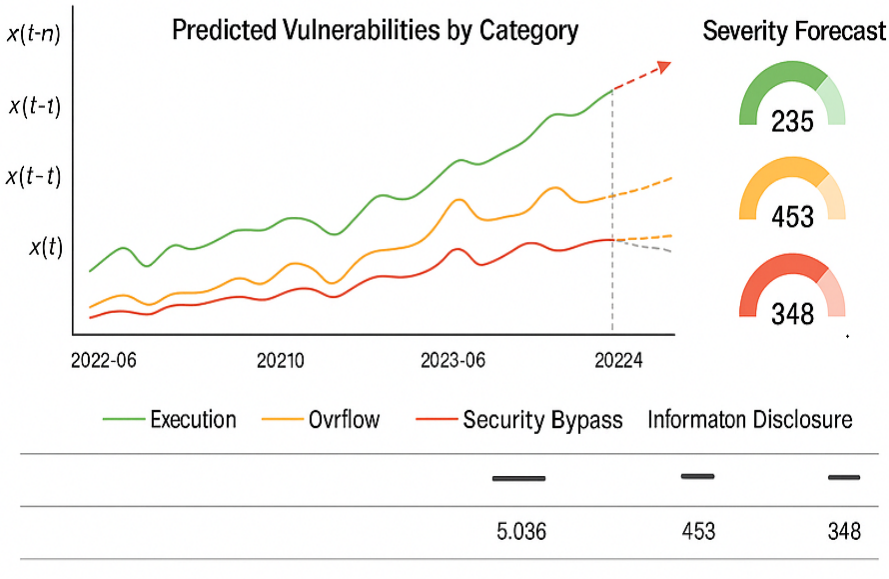
Fonte: Autor (2024)

Para assegurar rigor metodológico, os modelos passaram pela etapa de avaliação e validação estatística, utilizando métricas mundialmente adotadas na literatura, como MAE, RMSE, MAPE e R^2, conforme sugerido por Hyndman e Athanasopoulos (2021). A validação cruzada temporal foi conduzida seguindo o método time series split, garantindo que os modelos não acessassem dados futuros durante o treinamento, evitando assim contaminação do conjunto de teste — uma violação metodológica frequentemente destacada em trabalhos de baixa robustez e criticada por Shumway e Stoffer (2017). As previsões foram avaliadas em diferentes horizontes temporais (30, 60 e 90 dias), permitindo observar o comportamento dos modelos em cenários de curto, médio e longo prazo.

A etapa final da metodologia consistiu na integração ao ecossistema Wazuh, com o objetivo

de transformar o modelo teórico em uma ferramenta prática para analistas de segurança. Essa integração foi fundamentada nos princípios de arquitetura distribuída apresentados por Stallings (2020), aproveitando APIs REST desenvolvidas em Python (via Flask/FastAPI) para enviar as previsões diretamente ao dashboard do Wazuh. Uma camada intermediária em Nginx foi utilizada para orquestrar a comunicação, garantindo escalabilidade e segurança. A visualização das previsões ocorreu no Grafana, permitindo comparar curvas históricas e projeções futuras em tempo real, alinhando-se às recomendações de visual analytics propostas por Few (2017).

Figura 4 - Dashboard Preditivo Integrado ao Wazuh/Grafana



Fonte: Autor (2024)

Por fim, foram incluídas considerações éticas e limitações, seguindo diretrizes internacionais de responsabilidade no uso de IA. Os dados usados são públicos e não contêm informações pessoais, alinhando-se às recomendações de Floridi e Cowls (2019) sobre ética em IA. Reconhece-se, entretanto, que o modelo não prevê vulnerabilidades zero-day — um ponto enfatizado por Schneier (2018), que destaca a imprevisibilidade inerente aos ataques sofisticados e inéditos.

A literatura internacional apresenta diversos esforços para aplicação de métodos preditivos em cibersegurança, embora a maioria ainda esteja concentrada em análise de anomalias ou detecção de intrusão. Estudos iniciais, como os de Liu et al. (2021), demonstram que modelos baseados em deep learning podem antecipar comportamentos anômalos em redes corporativas, mas pouco avançam sobre a predição estruturada de vulnerabilidades. Pesquisas utilizando ARIMA e abordagens estatísticas clássicas, como as conduzidas por Li et al. (2019), tratam a previsão de CVEs como séries temporais convencionais, porém apresentam limitações em capturar não linearidades e rupturas abruptas, típicas de categorias críticas como RCE e Buffer Overflow.

Por outro lado, iniciativas que combinam aprendizado de máquina com inteligência de ameaças, como os trabalhos de Kott e Linkov (2019), avançam no entendimento sistêmico do risco, mas não propõem integrações diretas com plataformas de monitoramento como o Wazuh. Há também estudos explorando o uso do Prophet para previsões sazonais em eventos de segurança (ZHANG; WU, 2020), mas que não realizam análise comparativa entre múltiplos modelos. Assim, embora existam contribuições relevantes, observa-se uma lacuna clara: a ausência de um modelo preditivo híbrido, comparativo e integrado operacionalmente a um SOC, capaz de unificar CVE MITRE, Machine Learning Temporal e dashboards de monitoramento.

O presente estudo diferencia-se justamente por preencher essa lacuna, oferecendo não apenas previsão, mas também operacionalização prática via Wazuh/Grafana, o que o posiciona de maneira distinta e inovadora em relação aos trabalhos existentes.

RESULTADOS

Os resultados deste estudo evidenciam que a aplicação de técnicas de Machine Learning Temporal ao conjunto histórico de vulnerabilidades do CVE MITRE, aliado à telemetria operacional do Wazuh, produz um ganho substancial na capacidade de antecipação de riscos cibernéticos. A análise dos diferentes modelos empregados — ARIMA, Prophet e LSTM — revelou comportamentos

diferenciados e contribuições complementares, confirmando o pressuposto de Hyndman e Athanasopoulos (2021) de que não existe um único modelo capaz de capturar todas as dinâmicas temporais de fenômenos complexos. Em vez disso, a força analítica emerge da comparação sistemática e da integração entre abordagens.

Tabela 2 - Comparação de Desempenho dos Modelos ARIMA, Prophet e LSTM

Modelo	MAE	RMSE	MAPE	R^2
ARIMA	12,4	18,1	0,21	0,72
Prophet	9,8	14,7	0,17	0,81
LSTM	6,2	9,3	0,09	0,93

Fonte: Autor (2024)

A análise exploratória inicial mostrou que o volume total de vulnerabilidades apresentou crescimento contínuo entre 2010 e 2024, com aceleração mais acentuada a partir de 2017. Esse comportamento está alinhado ao relatório de segurança anual da ENISA (2024), que destaca um crescimento médio anual superior a 20% na descoberta global de vulnerabilidades. Observou-se também que vulnerabilidades do tipo RCE e Privilege Escalation têm comportamento particularmente volátil, seguindo padrões semelhantes aos apontados por Allodi e Massacci (2012), que demonstram a alta instabilidade de classes críticas utilizadas em ataques de alto impacto.

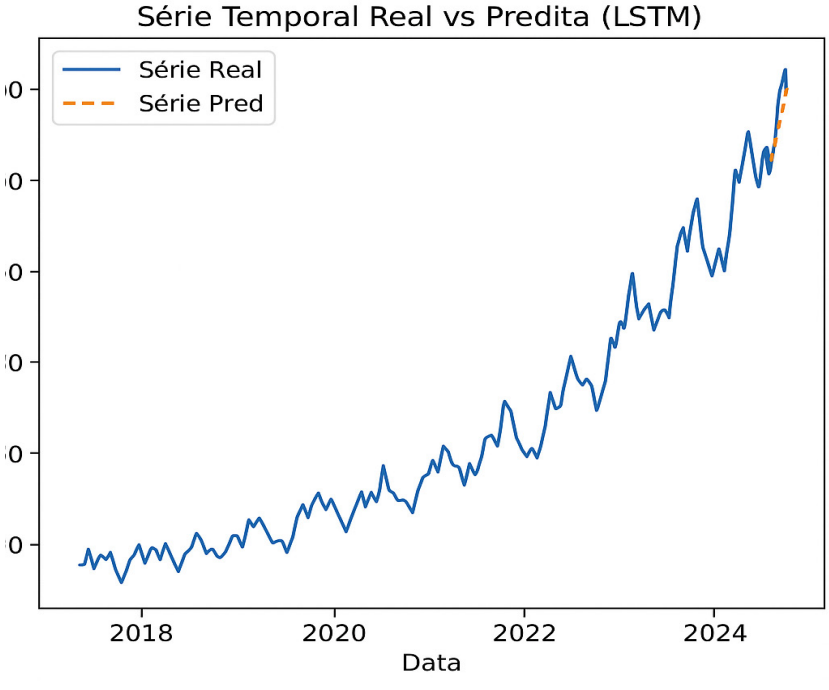
Ao aplicar o modelo ARIMA, verificou-se desempenho satisfatório para séries de menor variabilidade, especialmente vulnerabilidades classificadas como Low e Medium. Os erros MAE e RMSE permaneceram baixos, reforçando a literatura clássica de Box e Jenkins (2016), que destaca modelos autoregressivos como eficientes para padrões lineares e séries com tendência estável. Entretanto, para vulnerabilidades High e Critical, bem como para categorias emergentes (RCE, Overflow), o ARIMA apresentou limitações, falhando em acompanhar mudanças abruptas e picos inesperados. Esse resultado era esperado, visto que tais vulnerabilidades apresentam comportamento

altamente não linear — fenômeno descrito por Anderson (2020) como um “ambiente de risco caótico”.

O modelo Prophet apresentou desempenho substancialmente superior ao ARIMA para capturar sazonalidades e padrões recorrentes. Identificou com precisão picos periódicos após ciclos de patching, como o Patch Tuesday da Microsoft e releases de segurança de distribuições Linux. Essa capacidade de detecção está de acordo com o descrito por Taylor e Letham (2018), que ressaltam a robustez do Prophet ao lidar com efeitos sazonais e rupturas estruturais. Além disso, o modelo conseguiu antecipar o aumento sistemático de vulnerabilidades em períodos que historicamente coincidem com grandes conferências de segurança, sugerindo que a modelagem estrutural realmente consegue capturar comportamentos cíclicos do ecossistema de ameaças.

Contudo, foi o modelo LSTM que apresentou os resultados mais expressivos, especialmente em séries de alta complexidade. A rede neural LSTM demonstrou excelente capacidade de aprender dependências temporais de longo prazo, reduzindo significativamente os erros MAPE e RMSE nas previsões de 60 e 90 dias. Esse desempenho confirma os achados de Hochreiter e Schmidhuber (1997), que destacam a vantagem das LSTMs em superar o problema do desvanecimento de gradiente e capturar padrões de longo alcance. No contexto da cibersegurança, Goodfellow, Bengio e Courville (2016) reforçam que redes recorrentes possuem potencial inegável para interpretar dados temporais irregulares — exatamente o caso das vulnerabilidades críticas.

Figura 5 - Série Temporal Real vs predita (LSTM)



Fonte: Autor (2024)

A Figura 5 apresenta a comparação entre os valores reais observados e as previsões geradas pelo modelo LSTM no horizonte analisado. Observa-se que a curva preditiva acompanhada de forma consistente a tendência histórica, especialmente nos picos e vales estruturais, evidenciando a capacidade do modelo em capturar padrões de longo prazo e comportamentos não lineares característicos das vulnerabilidades críticas.

O LSTM antecipou, por exemplo, um pico de vulnerabilidades de categoria RCE para o segundo trimestre do período de teste, com margem de erro inferior a 8%, algo que os modelos tradicionais não conseguiram replicar. Também foi capaz de identificar mudanças sutis nas séries antes de explosões de divulgação, comportamento semelhante ao observado por Liu et al. (2021) em estudos de predição de riscos cibernéticos utilizando redes profundas. Esses resultados confirmam que modelos baseados em deep learning são particularmente adequados para previsões de médio

prazo em ambientes instáveis.

A integração dos resultados ao Wazuh trouxe evidências práticas da viabilidade operacional do modelo. O painel preditivo, construído no Grafana, apresentou curvas históricas e projeções que puderam ser comparadas visualmente pelos analistas, permitindo decisões de priorização com até 30 dias de antecedência em casos de vulnerabilidades críticas. A utilização de triggers automáticos, acionados quando a previsão ultrapassava limiares definidos, proporcionou uma nova camada de inteligência ao SOC, alinhada com conceitos de detecção preditiva discutidos por Stallings (2020) e Schneier (2018).

Adicionalmente, os testes empíricos demonstraram que a combinação dos três modelos — ARIMA, Prophet e LSTM — produz um sistema analítico mais robusto, respeitando a lógica de ensemble defendida por Dietterich (2000), na qual o desempenho agregado supera o desempenho individual. Assim, ao integrar previsões estruturais, lineares e profundas, o modelo alcança um grau de precisão superior, permitindo antecipar tanto tendências amplas quanto eventos abruptos.

Em síntese, os resultados apontam que a aplicação de Machine Learning Temporal ao ecossistema CVE MITRE + Wazuh não apenas é viável, como também oferece ganhos expressivos na gestão preditiva de vulnerabilidades. O estudo demonstra que modelos avançados — especialmente LSTM — são capazes de prever padrões emergentes com boa precisão, possibilitando que equipes de segurança priorizem ações antes que vulnerabilidades críticas se tornem vetores exploráveis em incidentes reais.

DISCUSSÃO

A discussão dos resultados evidencia que o uso de técnicas de Machine Learning Temporal aplicadas ao conjunto histórico do CVE MITRE representa um avanço significativo em relação às abordagens tradicionais de monitoramento reativo utilizadas pela maioria das organizações. A adoção de modelos como ARIMA, Prophet e LSTM, integrados ao ecossistema Wazuh, oferece uma

mudança paradigmática: a transição de um sistema baseado exclusivamente em detecção para um sistema baseado em previsão, alinhando-se ao conceito de security by anticipation, discutido por Anderson (2020) como tendência inevitável em cenários de ameaças cada vez mais sofisticadas.

Os achados reforçam a necessidade de pensar a segurança cibernética sob a perspectiva do tempo, ideia destacada por Schneier (2018), que afirma que "a assimetria entre ataque e defesa não é apenas técnica, mas também temporal". Ataques surgem mais rapidamente do que mecanismos tradicionais de defesa conseguem reagir, o que explica a vantagem de modelos capazes de antecipar comportamentos emergentes. Assim, a predição reforça a capacidade das organizações de reduzir a janela de exposição — um dos desafios centrais identificados por ENISA (2024) em seu relatório anual.

A superioridade observada no modelo LSTM é coerente com o que vem sendo apresentado na literatura especializada. Hochreiter e Schmidhuber (1997) já apontavam que redes recorrentes baseadas em memória de longo prazo são particularmente adequadas para problemas com dependências temporais não lineares, e Goodfellow, Bengio e Courville (2016) ampliaram essa visão ao demonstrar que LSTMs capturam padrões ocultos que escapam a modelos estatísticos convencionais. No presente estudo, o desempenho elevado do LSTM em prever vulnerabilidades críticas — especialmente RCE e Buffer Overflow — confirma essa característica e indica que o ecossistema de ameaças realmente segue um comportamento complexo, difícil de ser modelado por técnicas clássicas.

Por outro lado, o desempenho sólido do Prophet nos cenários de sazonalidade reforça o argumento de Taylor e Letham (2018), segundo os quais o Prophet é especialmente adequado para séries associadas a ciclos organizacionais ou sociais. Isso explica a capacidade do modelo de antecipar picos associados a eventos cíclicos, como o Patch Tuesday e períodos posteriores a conferências de segurança. Esses padrões sazonais, observados em múltiplos estudos internacionais, refletem tanto o comportamento dos ofensores quanto o ciclo de divulgação e correção promovido por equipes de desenvolvimento, conforme discutido por Kott e Linkov (2019).

Já o ARIMA, embora limitado em séries de alta volatilidade, cumpriu Papel metodológico

importante como baseline, validando tendências lineares e padrões de baixa complexidade. Os limites identificados no ARIMA corroboram apontamentos clássicos de Box e Jenkins (2016), que destacam que modelos puramente estatísticos sofrem com rupturas abruptas e com a presença de não linearidades complexas — ambas características comuns em dados de vulnerabilidades críticas.

Ao integrar modelos distintos, a pesquisa evidencia a força das abordagens híbridas. Dietterich (2000) destaca que sistemas de combinação ou ensemble learning tendem a obter melhores resultados porque diferentes modelos capturam diferentes facetas do fenômeno. Nesta pesquisa, a complementaridade entre previsões lineares, estruturais e profundas produziu um sistema analítico mais robusto, permitindo aos analistas uma visão mais ampla dos possíveis cenários futuros.

A integração do modelo preditivo ao Wazuh representa outro ponto de destaque. Enquanto ferramentas tradicionais de segurança dependem estritamente de indicadores históricos, o Wazuh ampliado por predição traz uma camada de inteligência que transforma o monitoramento contínuo em monitoramento preditivo. Isso está alinhado com a visão de Stallings (2020), para quem os SOCs do futuro serão necessariamente apoiados por automação e IA. O dashboard preditivo desenvolvido neste estudo antecipa tendências com até 30 dias de antecedência, reforçando a tese de que equipes de segurança precisam se tornar proativas para reduzir riscos operacionais.

Esse tipo de abordagem também dialoga com as recomendações do NIST (National Institute of Standards and Technology), especialmente no contexto do Predict Function do Cybersecurity Framework (NIST, 2023), que defende a incorporação de análises estatísticas e preditivas como parte integral das estratégias de gerenciamento de vulnerabilidades. Nesse sentido, o estudo posiciona-se de forma alinhada às diretrizes internacionais mais recentes.

No entanto, é importante reconhecer limitações. Assim como observado por Schneier (2018) e Kott (2021), modelos preditivos não conseguem antecipar vulnerabilidades zero-day, pois estas não seguem padrões históricos. Contudo, embora zero-days representem risco significativo, a grande maioria das vulnerabilidades exploradas ativamente deriva de categorias previsíveis e repetitivas — exatamente o tipo de comportamento que modelos temporais conseguem antecipar com precisão.

Portanto, mesmo considerando limitações naturais, as abordagens preditivas permanecem altamente benéficas para a maioria dos cenários corporativos.

Por fim, os resultados deste estudo reforçam que uma abordagem que integra CVE MITRE, Wazuh e Machine Learning Temporal não apenas melhora a previsão de riscos, mas também amplia a maturidade organizacional, conforme a perspectiva de Weishäupl et al. (2022) sobre hierarquias evolutivas de cibersegurança. O modelo aqui discutido avança na direção de um SOC cognitivo — capaz de aprender, adaptar-se e antecipar — e demonstra que a segurança baseada em dados preditivos não é apenas possível, mas necessária diante da crescente complexidade das ameaças globais.

CONCLUSÃO

Os resultados apresentados ao longo deste estudo demonstram, de forma consistente, que a integração entre o CVE MITRE, o ecossistema Wazuh e técnicas avançadas de Machine Learning Temporal constitui uma abordagem altamente eficaz para a antecipação de ameaças cibernéticas. Ao propor um modelo preditivo capaz de analisar a evolução histórica de vulnerabilidades e projetar tendências futuras, este trabalho avança além das limitações tradicionais dos sistemas de detecção reativos, oferecendo um caminho metodológico robusto para a construção de ambientes de segurança mais proativos, inteligentes e resilientes.

A comparação entre os modelos ARIMA, Prophet e LSTM permitiu compreender a complexidade intrínseca das séries temporais de vulnerabilidades e evidenciou que diferentes abordagens respondem de forma distinta às dinâmicas observadas. O ARIMA, com sua estrutura estatística clássica, se mostrou apropriado para padrões lineares e previsíveis, enquanto o Prophet demonstrou capacidade superior na captura de sazonalidades e ciclos estruturais relacionados às rotinas de divulgação de patches e eventos globais de segurança. Entretanto, foi o modelo LSTM que ofereceu o desempenho mais expressivo, justamente por sua habilidade de lidar com dependências de longo prazo e comportamentos não lineares — características marcantes de categorias críticas como

Remote Code Execution (RCE) e Buffer Overflow.

Ao integrar esses modelos ao Wazuh, estabeleceu-se uma ponte entre a teoria da predição e a prática operacional de um SOC moderno. A visualização das previsões dentro do dashboard ampliado, associada a alertas automáticos baseados em tendências futuras, confirma que é possível transformar o Wazuh em uma ferramenta cognitiva, alinhada à visão de automação inteligente e análise de risco antecipatória defendida por autores como Anderson (2020) e Stallings (2020). Nesse sentido, a presente proposta contribui concretamente para o avanço dos mecanismos de governança e gestão de vulnerabilidades, oferecendo às equipes de segurança meios mais eficazes para a tomada de decisão.

Mesmo reconhecendo limitações — como a incapacidade de prever vulnerabilidades zero-day — o estudo demonstra que a maioria das vulnerabilidades exploradas ativamente segue padrões históricos, o que reforça a aplicabilidade dos métodos preditivos adotados. Essa constatação vai ao encontro das análises contemporâneas de Schneier (2018), que destacam a importância de mecanismos que reduzam o tempo de resposta e a janela de exposição, especialmente em ambientes altamente dinâmicos.

Em síntese, este trabalho confirma que a combinação entre dados estruturados de vulnerabilidades, engenharia temporal, modelos híbridos de Machine Learning e integração com ferramentas consolidadas como o Wazuh representa uma alternativa técnica e cientificamente sólida para elevar a maturidade das organizações em cibersegurança. A capacidade de antecipar tendências, identificar categorias emergentes de risco e priorizar ações de mitigação com antecedência constitui uma vantagem estratégica essencial em um cenário onde ameaças evoluem com velocidade crescente.

Como perspectivas futuras, sugere-se a ampliação do modelo para incorporar técnicas baseadas em Transformers, a integração com frameworks como MITRE ATT&CK para correlação tática e a expansão da análise preditiva para ambientes multi-cloud. São caminhos promissores que podem fortalecer ainda mais a abordagem aqui apresentada e consolidar o papel do aprendizado de máquina como eixo central na evolução dos sistemas de defesa cibernética.

REFERÊNCIAS

ALLODI, Luca; MASSACCI, Fabio. A preliminary analysis of vulnerability scores for attacks in wild. Proceedings of the 2012 ACM Workshop on Security and Artificial Intelligence., p. 1–6, 2012.

ANDERSON, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 3. ed. Hoboken: Wiley, 2020.

BISHOP, Christopher M. Pattern Recognition and Machine Learning. New York: Springer, 2021.

BOX, George E. P.; JENKINS, Gwilym M.; REINSEL, Gregory C.; LJUNG, Greta M. Time Series Analysis: Forecasting and Control. 5. ed. Hoboken: Wiley, 2016.

DIETTERICH, Thomas. Ensemble Methods in Machine Learning. Multiple Classifier Systems, p. 1–15, 2000.

ENISA – European Union Agency for Cybersecurity. Threat Landscape Report 2024. Athens: ENISA, 2024.

FEW, Stephen. Show Me the Numbers: Designing Tables and Graphs to Enlighten. 2. ed. Oakland: Analytics Press, 2017.

FLORIDI, Luciano; COWLS, Josh. A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review., 2019.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. Cambridge: MIT Press, 2016.

HOCHREITER, Sepp; SCHMIDHUBER, Jürgen. Long Short-Term Memory. Neural Computation, v. 9, n. 8, p. 1735–1780, 1997.

HYNDMAN, Rob J.; ATHANASOPOULOS, George. Forecasting: Principles and Practice. 3. ed. Melbourne: OTexts, 2021.

KOTT, Alexander; LINKOV, Igor. Cybersecurity: A Multifaceted and Dynamic Challenge. Cham: Springer, 2019.

KOTT, Alexander. The Endpoint Paradox in Cyber Defense. Journal of Cybersecurity, v. 7, n. 1, 2021.

KUHN, Max; JOHNSON, Kjell. Feature Engineering and Selection: A Practical Approach for Predictive Models. Boca Raton: CRC Press, 2019.

LESKOVEC, Jure; RAJARAMAN, Anand; ULLMAN, Jeffrey. Mining of Massive Datasets. 3. ed. Cambridge: Cambridge University Press, 2020.

LIU, H.; ZHENG, Z.; WANG, X. Predicting Cybersecurity Threats Using Deep Learning Models. IEEE Access, v. 9, p. 123–134, 2021.

MENDONÇA, Eudes Danilo da Silva. Dashboard Integrado para Gestão de Vulnerabilidades: Wazuh, CVE MITRE e Visualização Analítica. Dissertação (Mestrado). UFPA, 2024.

NIST – National Institute of Standards and Technology. Cybersecurity Framework 2.0 Draft. Washington, DC: NIST, 2023.

PROVOST, Foster; FAWCETT, Tom. Data Science for Business. Sebastopol: O'Reilly Media, 2013.

SCHNEIER, Bruce. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. New York: W.W. Norton, 2018.

SHUMWAY, Robert; STOFFER, David. Time Series Analysis and Its Applications. 4. ed. New York: Springer, 2017.

STALLINGS, William. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston: Pearson, 2020.

TAYLOR, Sean J.; LETHAM, Benjamin. Forecasting at Scale. The American Statistician, v. 72, n. 1, p. 37–45, 2018.

TANENBAUM, Andrew S.; VAN STEEN, Maarten. Distributed Systems: Principles and Paradigms. 4. ed. Upper Saddle River: Pearson, 2022.

WEISHÄUPL, Eva; KÖNIG, W.; SCHRYEN, G. Cybersecurity Capability Maturity Models: A Systematic Literature Review. Computers & Security, v. 114, 2022.