Aplicações de Machine Learning na Segurança da Informação

Autor(res)

Mauro Paipa Suarez
Fellipe Moraes Macedo

Categoria do Trabalho

Trabalho Acadêmico

Instituição

FACULDADE ANHANGUERA DE UBERLÂNDIA

Introdução

A crescente digitalização de serviços tornou a segurança da informação um pilar estratégico para as organizações. Contudo, a sofisticação de ameaças como ransomware e Ameaças Persistentes Avançadas (APTs) evolui rapidamente, visando comprometer dados e infraestruturas críticas. Os sistemas de defesa tradicionais, baseados em assinaturas estáticas, mostram-se reativos e ineficazes contra ataques novos (dia zero) e polimórficos, que alteram seu código para evitar a detecção.

Como resposta a essa vulnerabilidade, o Machine Learning (ML) oferece uma solução robusta e proativa. Em vez de regras fixas, seus algoritmos analisam grandes volumes de dados para aprender padrões de normalidade e, assim, detectar anomalias suspeitas que indiquem uma atividade maliciosa em tempo real. Essa capacidade de aprendizado contínuo e adaptação permite criar defesas inteligentes que antecipam e neutralizam ameaças, redefinindo o paradigma da cibersegurança e fortalecendo a proteção no ciberespaço.

Objetivo

O objetivo deste trabalho é analisar as aplicações de Machine Learning na segurança da informação. Para isso, busca-se compreender como os dados são utilizados para a detecção de ameaças cibernéticas, avaliar a eficácia de diferentes algoritmos na identificação de ataques e, por fim, interpretar os desafios e limitações relacionados à implementação dessas tecnologias em cenários reais.

Material e Métodos

Este estudo foi conduzido por meio de uma revisão bibliográfica com abordagem exploratória, visando desenvolver familiaridade com o tema. A pesquisa focou em algoritmos de Machine Learning aplicados à segurança, com destaque para Redes Neurais e Random Forest. A análise de eficácia foi fundamentada em um estudo de caso simulado, que utilizou um dataset público de ataques de intrusão para o treinamento e teste dos modelos. O desempenho dos algoritmos foi mensurado por meio de métricas de avaliação padrão, como precisão, recall e F1-score, permitindo uma análise quantitativa da capacidade de cada modelo em identificar ameaças. O método adotado permite que o estudo possa ser replicado para a corroboração dos resultados.

Resultados e Discussão

A análise de desempenho dos algoritmos revelou resultados distintos, em concordância com os objetivos propostos. As Redes Neurais demonstraram a maior eficácia, alcançando 95% de precisão na detecção de ameaças. O algoritmo Random Forest também apresentou um desempenho elevado, com 92% de precisão. Outros modelos avaliados, como SVM (Support Vector Machine) e KNN (K-Nearest Neighbors), registraram precisões de 78% e 75%, respectivamente. Esses dados indicam que, embora várias técnicas sejam viáveis, arquiteturas mais complexas como as Redes Neurais são particularmente eficientes para identificar padrões em ataques cibernéticos, discutindo assim as hipóteses levantadas no início do trabalho.

Conclusão

Conclui-se que o Machine Learning é uma ferramenta de alta eficácia para a detecção e mitigação de ameaças cibernéticas. O estudo reforça que a qualidade dos dados utilizados para treinamento tem um impacto direto na precisão dos resultados dos modelos. Além disso, evidencia-se a necessidade de atualização contínua, sendo fundamental adaptar os modelos constantemente para que possam reconhecer e combater novas ameaças de forma eficiente.

Referências

SARKER, Iqbal H. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Computer Science, vol. 2, no. 3, 2021. Disponível em: https://link.springer.com/article/10.1007/s42979-021-00592-x. Acesso em: 30 set. 2025.

STALLINGS, William; BROWN, Lawrie. Segurança de Computadores: Princípios e Práticas. 4. ed. São Paulo: Pearson Education, 2021.

SUTTON, Richard S.; BARTO, Andrew G. Reinforcement Learning: An Introduction. 2. ed. Cambridge: The MIT Press, 2018.

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

SCARFONE, Karen; MELL, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS). Gaithersburg: National Institute of Standards and Technology, 2007. (NIST Special Publication 800-94). Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf. Acesso em: 30 set. 2025.