A Inteligência Artificial na Segurança Cibernética de Sistemas de Informação: Respostas Inteligentes a Ameaças em Tempo Real

João Melro
Instituto Superior Miguel Torga (ISMT)
Coimbra, Portugal
12987@ismt.pt

Joaquim Limeira
Instituto Superior Miguel Torga (ISMT)
Coimbra, Portugal
13112@ismt.pt

Sara Rodrigues
Instituto Superior Miguel Torga (ISMT)
Coimbra, Portugal
12697@ismt.pt

***Abstract*—A deteção e mitigação de ameaças cibernéticas em tempo real é um dos desafios mais relevantes na proteção dos Sistemas de Informação (SI). A Inteligência Artificial (IA), através de técnicas como aprendizagem automática (machine learning), análise comportamental, deep learning e processamento de linguagem natural (PLN), tem-se revelado uma ferramenta promissora para enfrentar ataques cada vez mais sofisticados. Este artigo apresenta uma revisão fundamentada de abordagens baseadas em IA aplicadas à segurança cibernética, com ênfase na deteção de anomalias, intrusões em redes e resposta a incidentes. São discutidos os principais benefícios da IA, as limitações práticas da sua adoção e exemplos reais de aplicação, como o caso da plataforma Darktrace. A análise integra também abordagens complementares emergentes, como o raciocínio baseado em casos aplicado a contextos colaborativos.**

***Index Terms*—Inteligência Artificial, Sistemas de Informação, Segurança Cibernética, Deteção de Ameaças, Machine Learning, Deteção de Anomalias**

I. Introdução

A transformação digital tem promovido uma dependência crescente das infraestruturas tecnológicas e dos Sistemas de Informação (SI), fundamentais para o funcionamento de organizações em todos os setores. Com essa dependência, aumentam também os riscos e a complexidade das ameaças cibernéticas, que se tornaram mais frequentes, persistentes e difíceis de detetar. Paralelamente, os modelos de defesa convencionais, como os baseados em regras fixas ou assinaturas, revelam-se insuficientes face a ataques novos ou modificados (zero-day).

Neste cenário, a Inteligência Artificial (IA) surge como uma solução com elevado potencial transformador, ao permitir a automatização de processos de deteção, resposta e análise de ameaças. A IA pode aprender padrões de comportamento normal, identificar desvios em tempo real e sugerir ou executar respostas autónomas, reduzindo a dependência da intervenção humana e o tempo de reação. Este artigo analisa, de forma aprofundada, o papel da IA na segurança cibernética dos SI, integrando contributos teóricos, técnicos e exemplos práticos.

II. Enquadramento Teórico

Os Sistemas de Informação são compostos por hardware, software, pessoas e procedimentos organizados para recolher, processar, armazenar e disseminar informação, suportando a tomada de decisão [6]. A segurança dos SI — ou segurança cibernética — consiste num conjunto de práticas e tecnologias voltadas para a proteção desses sistemas contra acessos não autorizados, roubo de dados, interrupções e ataques.

A Inteligência Artificial, neste contexto, engloba um conjunto de técnicas computacionais que simulam processos cognitivos humanos, como aprendizagem, raciocínio e autoajuste. Dentre estas técnicas, destacam-se:

- **Aprendizagem automática (Machine Learning):** utiliza dados históricos para treinar modelos que distinguem comportamentos normais de anómalos [1];
- **Deep Learning:** redes neurais profundas que detetam padrões complexos em grandes volumes de dados;
- **Processamento de Linguagem Natural (PLN):** útil na análise de comunicações suspeitas, e-mails de phishing e logs de sistema;
- **Raciocínio Baseado em Casos (CBR):** sistemas que resolvem problemas com base em experiências passadas, adaptando soluções anteriores a novos cenários [4].

A deteção de anomalias, por exemplo, pode assumir diferentes formas, como deteção estatística, baseada em clusters ou em redes neurais. Chandola et al. [2] classificam essas técnicas com base nas suas abordagens e pressupostos, identificando os pontos fortes e limitações conforme o domínio de aplicação.

III. Análise Crítica

A. Benefícios

- **Deteção precoce de ameaças:** permite identificar padrões de comportamento malicioso antes que causem danos [7];
- **Resposta automatizada:** reduz o tempo de contenção e minimiza o impacto de ataques;
- **Redução de falsos positivos:** adaptabilidade ao contexto permite distinguir entre atividades anómalas reais e variações inofensivas;
- **Análise preditiva:** modelos alimentados com históricos de ataques podem prever novas ameaças ou vulnerabilidades [5].

B. Limitações

- **Dependência de dados de qualidade:** sem dados adequados, o modelo pode falhar ou generalizar incorretamente;
- **Vulnerabilidade a ataques adversariais:** inputs maliciosos podem ser manipulados para enganar modelos de IA;
- **Complexidade de implementação:** exige recursos tecnológicos e humanos especializados;
- **Problemas de explicabilidade:** muitos modelos funcionam como "caixa negra", dificultando auditorias e conformidade.

Sommer e Paxson [8] chamam atenção para as dificuldades de aplicar IA a deteção de intrusões em redes reais, onde o tráfego é ruidoso, heterogéneo e em constante mudança.

IV. Estudo de Caso: Darktrace

A Darktrace [3] é uma empresa de cibersegurança que desenvolveu uma plataforma baseada em IA autoaprendente, conhecida como "Enterprise Immune System". Esta tecnologia utiliza aprendizagem não supervisionada para estabelecer uma linha base de comportamento normal na rede de uma organização. Quando ocorre uma anomalia — como acesso a um ficheiro confidencial em horário invulgar — o sistema gera alertas e pode agir autonomamente para neutralizar a ameaça.

Além disso, o sistema evolui continuamente, incorporando novos padrões e ajustando-se a alterações nos hábitos dos utilizadores. Esta abordagem tem sido adotada por organizações em setores como saúde, energia, defesa e finanças, devido à sua capacidade de deteção precoce e adaptabilidade a infraestruturas complexas.

V. Outras Abordagens Inteligentes

Em contextos colaborativos e distribuídos, como habitações inteligentes interligadas, a IA tem sido aplicada para gestão energética eficiente. Giret [4] propõe um sistema baseado em raciocínio baseado em casos, onde as casas partilham soluções para problemas energéticos semelhantes. Este paradigma, baseado em aprendizagem social e difusão de conhecimento, pode ser adaptado à segurança cibernética, permitindo que sistemas partilhem informações sobre ameaças e estratégias de resposta, aumentando a resiliência global.

VI. Ferramentas e Técnicas Utilizadas

A aplicação da Inteligência Artificial na segurança cibernética é suportada por um conjunto de ferramentas específicas que viabilizam as soluções descritas. Algumas das ferramentas mais relevantes incluem:

- **Snort + ML Pipelines:** Snort é um IDS de código aberto amplamente utilizado, que pode ser integrado com pipelines de aprendizagem automática para deteção de intrusões baseada em padrões.
- **Splunk e IBM QRadar:** plataformas SIEM que utilizam IA para correlação de eventos, deteção de anomalias e resposta automatizada a incidentes.
- **Elastic Stack com X-Pack ML:** ferramenta poderosa para análise de logs e deteção de anomalias com integração de algoritmos de machine learning.
- **Darktrace Enterprise Immune System:** sistema baseado em IA não supervisionada para deteção de ameaças e resposta autónoma em tempo real.
- **Cortex XDR (Palo Alto Networks):** plataforma de deteção e resposta estendida com capacidades de IA para proteger endpoints, redes e servidores.
- **Microsoft Defender for Endpoint:** solução de proteção avançada com integração de IA para deteção comportamental e remediação automática.
- **MISP (Malware Information Sharing Platform):** ferramenta para partilha de inteligência sobre ameaças, integrada com IA para correlação preditiva de ataques.

Estas ferramentas representam a fusão entre engenharia de software, cibersegurança e ciência de dados, sendo pilares fundamentais na construção de ambientes digitais mais seguros e autónomos.

VII. Conclusão e Perspetivas Futuras

A IA representa um avanço disruptivo na forma como se abordam os desafios da segurança cibernética nos SI. A sua capacidade de aprendizagem contínua, adaptação a novos cenários e execução de respostas automáticas torna-a indispensável para ambientes dinâmicos e de risco elevado.

No entanto, a eficácia destas soluções depende da disponibilidade de dados de treino representativos, da transparência nos modelos e da integração com políticas organizacionais. Torna-se essencial investir em modelos explicáveis, infraestruturas seguras e formação especializada.

As perspetivas futuras passam pelo desenvolvimento de arquiteturas híbridas — combinando IA com supervisão humana — e pelo reforço da colaboração interorganizacional na partilha de ameaças e boas práticas. Esta convergência entre inteligência computacional e consciência situacional poderá definir o próximo estágio da cibersegurança em SI.

References

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016. https://doi.org/10.1109/COMST.2015.2494502

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[3] Darktrace, "Enterprise Immune System: Cyber AI for Threat Detection", 2023. [Online]. Available: https://www.darktrace.com

[4] A. Giret, "Smart Heating in Reasoning-Enabled Collaborative Residential Units," *ScienceDirect*, 2021.

[5] S. Kumar, S. Singh, and A. Sharma, "Artificial intelligence techniques in cybersecurity: Recent advancements and future directions," *Journal of Information Security and Applications*, vol. 65, 103143, 2022. https://doi.org/10.1016/j.jisa.2022.103143

[6] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*, 16th ed., Pearson, 2020.

[7] I. H. Sarker, A. S. M. Kayes, and P. A. Watters, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 8, no. 1, pp. 1–29, 2021. https://doi.org/10.1186/s40537-021-00436-x

[8] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *IEEE Symposium on Security and Privacy*, 2010.