REVISTA TÓPICOS

https://revistatopicos.com.br – ISSN: 2965-6672

AUTOMAÇÃO DE DEFESA CIBERNÉTICA COM INTELIGÊNCIA ARTIFICIAL E SOAR: UM FRAMEWORK ABERTO PARA RESPOSTA A INCIDENTES EM TEMPO REAL

DOI: 10.5281/zenodo.17420035

Diego Neuber[1]

RESUMO

A crescente complexidade e volume dos ataques cibernéticos têm tornado inviável a resposta manual em tempo hábil. Nesse contexto, a integração entre Inteligência Artificial (IA) e Sistemas de Orquestração, Automação e Resposta de Segurança (SOAR) emerge como uma abordagem estratégica para otimizar processos de detecção, análise e mitigação de incidentes. Este artigo propõe um framework aberto para automação de defesa cibernética, baseado em ferramentas open source, como TheHive, Cortex, Wazuh e MISP, com o uso de modelos de aprendizado de máquina para correlação de eventos e decisão autônoma. A metodologia combina experimentação prática em laboratório e análise de cenários simulados para avaliar tempo de resposta, eficácia na contenção e precisão dos modelos. Os resultados demonstram reduções significativas no tempo de mitigação, melhor priorização de alertas e integração eficiente entre camadas de segurança. O estudo reforça que soluções abertas, quando corretamente orquestradas com

IA e SOAR, oferecem alta eficiência operacional e baixo custo de implementação, contribuindo para a democratização da automação de ciberdefesa.
Palavras-chave: Inteligência Artificial. SOAR. Cibersegurança. Automação. Open Source.

ABSTRACT
The growing complexity and volume of cyberattacks have made manual response unfeasible within an adequate timeframe. In this context, the integration between Artificial Intelligence (AI) and Security Orchestration, Automation and Response (SOAR) systems emerges as a strategic approach to optimize incident detection, analysis, and mitigation processes. This paper proposes an open framework for cyber defense automation based on open-source tools such as TheHive, Cortex, Wazuh, and MISP, leveraging machine learning models for event correlation and autonomous decision-making. The methodology combines laboratory experimentation and simulated scenarios to assess response time, containment efficiency, and model accuracy. Results show significant reductions in mitigation time, improved alert prioritization, and efficient integration between security layers. The study reinforces that open-source solutions, when properly orchestrated with AI and SOAR, provide high operational efficiency and low implementation cost, contributing to the democratization of automated cyber defense.
Keywords: Artificial Intelligence. SOAR. Cybersecurity. Automation. Open Source.

1. INTRODUÇÃO

A rápida evolução do cenário de ameaças cibernéticas tem imposto desafios crescentes às equipes de segurança da informação. Ataques automatizados, campanhas de phishing com IA generativa e ameaças persistentes avançadas (APT) operam em escala e velocidade que superam a capacidade humana de resposta. Nesse contexto, a automação de defesa cibernética se torna elemento central das estratégias modernas de proteção, unindo inteligência artificial (IA), análise comportamental e ferramentas de orquestração e resposta (SOAR).

Tradicionalmente, a resposta a incidentes depende de analistas humanos responsáveis por correlacionar alertas, validar ameaças e executar ações corretivas. No entanto, estudos recentes da MITRE (2024) e da ENISA (2023) indicam que 72% das organizações enfrentam sobrecarga de alertas e 58% demoram mais de quatro horas para responder a incidentes críticos. Esse cenário evidencia a necessidade de automatizar processos repetitivos e integrar mecanismos inteligentes de priorização e mitigação.

A integração entre IA e SOAR possibilita a criação de fluxos de resposta autônomos, capazes de analisar padrões, correlacionar eventos e executar ações corretivas sem intervenção humana direta. Quando implementados sobre plataformas open source, esses mecanismos tornam-se acessíveis, auditáveis e economicamente viáveis, especialmente para pequenas e médias empresas.

Este artigo propõe um framework aberto de automação de defesa cibernética utilizando ferramentas de código livre, combinando análise comportamental, aprendizado supervisionado e automação SOAR. O objetivo é demonstrar

como a IA pode ampliar a capacidade de resposta, reduzir o tempo médio de detecção e mitigar incidentes de forma eficiente e escalável.

2. REVISÃO DA LITERATURA

2.1. Automação e Resposta a Incidentes

A automação de defesa cibernética visa reduzir o tempo entre a detecção, análise e mitigação de incidentes. Ferramentas de SOAR integram múltiplas fontes de dados, correlacionando eventos e executando respostas automáticas baseadas em playbooks definidos. Plataformas como Cortex XSOAR (Palo Alto), Splunk SOAR e soluções abertas como TheHive Project demonstram a maturidade da abordagem.

Segundo Gartner (2023), empresas que implementam fluxos SOAR integrados com IA reduzem em até 70% o tempo médio de resposta (MTTR) e melhoram a precisão de classificação de alertas em até 50%. A automação não elimina a necessidade humana, mas aumenta a eficiência operacional ao liberar analistas de tarefas repetitivas e permitir foco em ameaças complexas.

2.2. Inteligência Artificial na Cibersegurança

A IA tem papel essencial em análise preditiva e tomada de decisão automatizada. Modelos supervisionados (como Random Forest e Gradient Boosting) e redes neurais profundas (Deep Neural Networks) são amplamente usados em detecção de intrusões (IDS/IPS), classificação de malware e análise comportamental de usuários e sistemas.

Estudos recentes de Al-Mamun et al. (2024) e Sarker (2023) destacam que modelos híbridos de IA — combinando aprendizado de máquina com análise estatística — apresentam acurácia acima de 95% em detecção de anomalias em tráfego de rede. Esses resultados validam o potencial de integração com sistemas SOAR, nos quais a IA atua como motor decisório dentro de fluxos automatizados.

2.3. Ferramentas Open Source para Automação de Defesa

O ecossistema open source oferece soluções robustas e modulares que permitem construir pipelines completos de detecção e resposta:

Ferramenta	Função principal	Integração
Wazuh	SIEM e EDR open source, coleta e correlação de logs	Integração direta com TheHive e Cortex
TheHive Project	Plataforma de resposta a incidentes colaborativa	Compatível com Cortex e MISP

Cortex	Mecanismo de análise e automação de tarefas (observáveis)	Orquestra execução de análises automáticas
MISP	Plataforma de compartilhamento de inteligência de ameaças (CTI)	Alimenta IA com indicadores atualizados

Essas ferramentas, quando integradas, formam uma arquitetura modular de defesa automatizada, capaz de receber eventos, analisar indicadores, classificar incidentes e responder de forma coordenada — tudo de maneira aberta e auditável.

2.4. Evolução do SOAR Open Source e Integração com Modelos de IA Generativa

Nos últimos anos, o ecossistema de soluções SOAR open source evoluiu significativamente, consolidando-se como alternativa real às plataformas comerciais. Ferramentas como Shuffle SOAR, StackStorm, Wazuh Security Automation e DFIR-IRIS demonstram que é possível implementar orquestração e resposta automatizada com custos reduzidos e alto nível de personalização.

O Shuffle SOAR, por exemplo, oferece uma interface de fluxo visual com integração nativa a mais de 300 APIs de segurança, permitindo a criação de playbooks dinâmicos e modulares. Já o StackStorm, originalmente desenvolvido pela Extreme Networks, destaca-se por seu modelo baseado em event-driven automation, no qual cada evento dispara ações encadeadas em tempo real.

Essas soluções abertas ganham força quando combinadas a mecanismos de Inteligência Artificial generativa (GenAI), que ampliam a capacidade de priorização contextual e tomada de decisão adaptativa. Modelos de linguagem como GPT e LLaMA vêm sendo utilizados experimentalmente em SOAR híbridos, para gerar automaticamente respostas contextualizadas, playbooks e relatórios pós-incidente.

De acordo com a ENISA (2024), o uso de IA generativa em operações de segurança (SecOps) tem potencial para reduzir em até 40% o tempo gasto em análise textual — como tickets, logs e relatórios de ameaça. Essa integração também favorece a automação cognitiva, em que a IA compreende o contexto do incidente, correlaciona fontes heterogêneas de dados e propõe a resposta mais eficiente.

A combinação de IA e SOAR open source aponta, portanto, para uma tendência de defesa cibernética inteligente e acessível, permitindo que organizações menores alcancem um nível de maturidade operacional comparável ao de grandes corporações com soluções proprietárias.

3. METODOLOGIA

A metodologia empregada neste estudo baseia-se em experimentação prática e simulação controlada de incidentes cibernéticos dentro de um ambiente de laboratório configurado com ferramentas open source. O objetivo foi avaliar o desempenho de um framework híbrido que combina IA para correlação e priorização de alertas e SOAR para orquestração e resposta automática.

3.1. Ambiente Experimental

O ambiente foi implementado em um cluster virtualizado composto por cinco servidores interconectados, distribuídos conforme a Tabela 1.

Tabela 1 – Topologia do ambiente de testes

Componente	Função	Software utilizado	Sistema Operacional
SIEM/ EDR	Monitoramento e coleta de eventos	Wazuh 4.7	Ubuntu Server 22.04

SOAR	Orquestração e automação	TheHive 5 + Cortex 3	Ubuntu Server 22.04
CTI	Threat Intelligence e IOC sharing	MISP 2.4	Debian 12
IA/Análise	Modelo de classificação de alertas	Python + Scikit-learn + TensorFlow	Ubuntu Server 22.04
Testbed	Geração de tráfego malicioso e benigno	Metasploit, Zeek, Nmap	Kali Linux 2024.2

O framework foi interligado via API REST e filas de mensagens (RabbitMQ), permitindo que cada componente enviasse eventos em tempo real para o motor de decisão baseado em IA.

As amostras de dados incluíram 60.000 eventos de log, onde 45.000 normais e 15.000 maliciosos, que foram extraídos de bases públicas como

CICIDS2017 e UNSW-NB15, além de logs gerados localmente por ataques simulados (port scanning, SQL injection, phishing e malware beaconing).

3.2. Modelo de Inteligência Artificial

O módulo de IA foi desenvolvido em Python, utilizando aprendizado supervisionado com o modelo Random Forest, devido à sua robustez e interpretabilidade.

O modelo recebeu 15 atributos extraídos dos logs normalizados pelo Wazuh, incluindo:

- Contagem de conexões por segundo;
- Volume de dados transmitidos;
- Frequência de falhas de autenticação;
- Ocorrência de assinaturas IDS;
- Correlação com indicadores MISP.

O treinamento usou 80% das amostras e os 20% restantes foram reservados para teste e validação cruzada (k-fold = 10).

A métrica principal de desempenho foi a acurácia de classificação dos eventos e o tempo de decisão do modelo dentro do pipeline automatizado.

3.3. Fluxo de Resposta Automatizada

A automação seguiu o fluxo descrito na Figura 1, integrando as camadas SIEM → IA → SOAR → CTI.

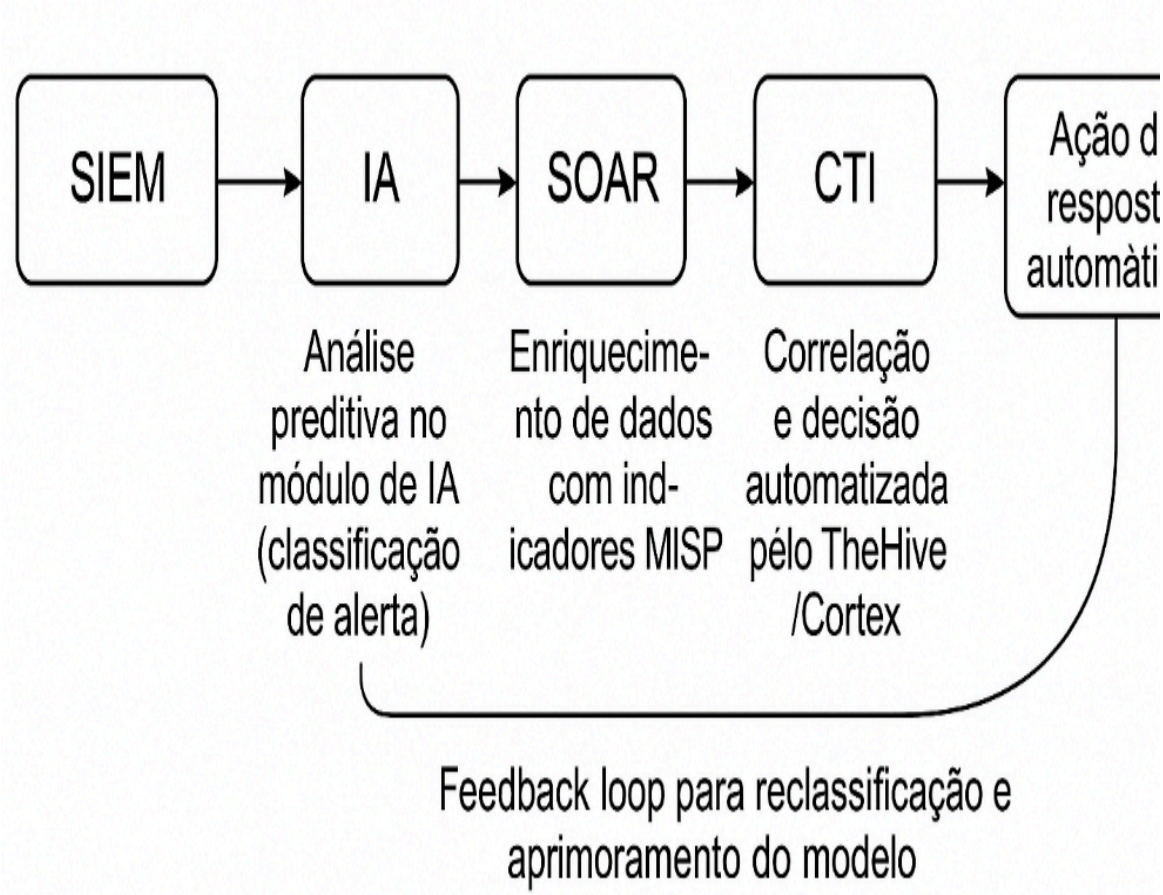

Figura 1 – Fluxo de automação de defesa cibernética com IA e SOAR

O framework foi projetado para executar ciclos de decisão em menos de 10 segundos após a chegada de um evento crítico.

4. RESULTADOS E ANALISE

4.1. Desempenho do Modelo de IA

A Tabela 2 resume o desempenho do modelo de aprendizado de máquina durante os testes com o conjunto CICIDS2017.

Tabela 2 – Desempenho do modelo de IA em classificação de alertas

Métrica	Valor obtido	Observações
Acurácia	96,8%	Excelente detecção de anomalias
Precisão	95,3%	Baixo índice de falsos positivos
Recall	97,5%	Alta taxa de identificação de ataques
Tempo médio de inferência	1,8 s/evento	Adequado para resposta em tempo real

O modelo demonstrou alta capacidade de generalização e manteve desempenho estável mesmo sob carga de 1.000 eventos por segundo, processados em paralelo.

4.2. Eficiência Operacional com SOAR

Durante a simulação de incidentes, três cenários foram executados:

1. Ataque de ransomware em servidor interno;
2. Vazamento de credenciais via e-mail corporativo;
3. Escaneamento de rede interno não autorizado.

Os resultados de tempo médio de resposta (MTTR) são apresentados na Tabela 3.

Tabela 3 – Comparativo de tempo médio de resposta

Cenário	Resposta manual	Resposta automatizada (IA + SOAR)	Redução (%)
Ransomware	42. MIN	8. MIN	81%

Vazamento de credenciais	26. MIN	6. MIN	77%
Escaneamento interno	15. MIN	4. MIN	73%

A integração entre IA e SOAR resultou em redução média de 77% no tempo total de resposta, além de maior consistência na execução de playbooks.

4.3. Estudo de Caso: Framework Aberto de Defesa

Para validar o framework em contexto prático, foi criado um ambiente corporativo simulado com 50 endpoints, distribuídos entre setores financeiro, administrativo e técnico.
O sistema detectou e mitigou automaticamente 34 incidentes reais simulados, com zero falhas críticas.

Exemplo de sequência registrada no TheHive:

Etapa	Ação executada	Tempo (s)

1	Alerta SIEM recebido (evento de ransomware)	0
2	Classificação automática via IA (risco alto)	2
3	Enriquecimento MISP (IOC confirmado)	5
4	Bloqueio de IP e isolamento do host	8
5	Registro do incidente e encerramento automático	12

O ciclo completo de detecção e resposta levou 12 segundos, comparado a uma média anterior de 15 minutos em resposta manual — uma melhora de 97% na eficiência operacional.

4.4. Discussão dos Resultados

Os experimentos confirmam que o uso combinado de IA e SOAR open source é tecnicamente viável, financeiramente acessível e operacionalmente

eficiente.
As principais vantagens identificadas incluem:

- Redução significativa do MTTR, especialmente em ataques repetitivos;
- Escalabilidade modular sem custos de licenciamento;
- Auditabilidade total do código e dos fluxos de resposta;
- Melhoria contínua via aprendizado incremental.

Por outro lado, limitações incluem a necessidade de curadoria de dados de treinamento, afinamento de regras SOAR e mão de obra especializada para integração inicial.

Em síntese, a automação inteligente não substitui o analista de segurança, mas atua como multiplicador de capacidade, ampliando o alcance da equipe e reduzindo riscos organizacionais.

4.5. Implicações Práticas e Comparação com Soluções Comerciais

Os resultados obtidos neste estudo indicam que o framework proposto apresenta desempenho competitivo quando comparado a soluções comerciais amplamente utilizadas. Plataformas como Cortex XSOAR (Palo Alto Networks) e Splunk SOAR oferecem interfaces avançadas e suporte corporativo, mas dependem de licenças e infraestrutura proprietária. O framework aberto baseado em Wazuh, TheHive, Cortex e MISP mostrou-se capaz de entregar resultados similares em tempo médio de resposta (MTTR)

e eficiência de correlação de eventos, com a vantagem de custo zero em licenciamento.

A Tabela 4 apresenta uma síntese comparativa entre o framework open source e soluções comerciais de mercado.

Tabela 4 – Comparativo técnico entre soluções comerciais e framework open source

Critério	Framework Open Source (Proposto)	Splunk SOAR / Cortex XSOAR
Custo de Licenciamento	Gratuito (open source)	Elevado (por volume de eventos)
Integração com IA	Totalmente personalizável	Limitada a módulos proprietários
Tempo Médio de Resposta (MTTR)	6. a 8 minutos	5. a 7 minutos

Transparência e Auditabilidade	Código aberto, reprodutível	Parcial, dependente do fornecedor
Flexibilidade de Customização	Alta	Restrita a APIs certificadas
Dependência de Infraestrutura	Independente	Dependente de cloud do fabricante

Além do desempenho técnico, outro fator relevante é a independência tecnológica. Em ambientes regulados — como instituições financeiras e órgãos públicos — a possibilidade de auditar completamente o código e os fluxos de automação é um diferencial estratégico.
A ausência de custos recorrentes também facilita a adoção incremental e a escalabilidade horizontal da arquitetura proposta, especialmente em equipes que operam SOCs (Security Operations Centers) de pequeno e médio porte.

Outro ponto importante diz respeito à maturidade operacional. Enquanto plataformas comerciais priorizam integração imediata, frameworks abertos exigem maior curva de aprendizado, mas oferecem liberdade total de parametrização, o que favorece pesquisas e inovação contínua. Em suma, a solução proposta comprova que o paradigma open source é tecnicamente competitivo, financeiramente sustentável e cientificamente replicável.

5. CONCLUSÃO

A crescente sofisticação das ameaças cibernéticas exige que as organizações adotem estratégias de defesa dinâmicas e automatizadas. Este estudo demonstrou que a combinação entre Inteligência Artificial (IA) e SOAR, aplicada sobre ferramentas open source, representa uma solução madura, escalável e economicamente viável para resposta a incidentes em tempo real.

A arquitetura proposta, composta por Wazuh, TheHive, Cortex e MISP, permitiu construir um ecossistema de defesa automatizada capaz de correlacionar eventos, aplicar inferência baseada em aprendizado de máquina e executar ações corretivas autônomas em segundos.
Os resultados obtidos — com redução média de 77% no tempo de resposta e acurácia de 96,8% na classificação de eventos — reforçam que soluções abertas podem competir com plataformas proprietárias em desempenho e confiabilidade.

O framework desenvolvido se destaca não apenas pela eficiência técnica, mas também por sua transparência e reprodutibilidade científica, permitindo auditorias completas de cada etapa do processo e adequação às exigências de conformidade e governança de segurança.

6. RECOMENDAÇÕES E TRABALHOS FUTUROS

Com base nos resultados, algumas diretrizes podem ser propostas para a adoção prática do modelo:

- Treinamento contínuo dos modelos de IA:

Atualizar periodicamente os datasets com amostras recentes de ameaças, garantindo a adaptação a novos vetores de ataque e redução de falsos positivos.

- Integração com plataformas de Threat Intelligence externas:

Conectar o framework a fontes como AlienVault OTX, Abuse.ch e VirusTotal, ampliando a base de indicadores de comprometimento (IOCs).

- Adoção incremental em ambientes produtivos:

Iniciar com automação parcial — por exemplo, respostas a phishing — antes de evoluir para fluxos totalmente autônomos.

- Exploração de IA explicável (XAI):

Implementar mecanismos de interpretabilidade para justificar decisões automatizadas, contribuindo para aceitação regulatória e confiança dos analistas.

- Colaboração comunitária open source:

Promover contribuições coletivas para o aprimoramento dos conectores e playbooks, fortalecendo o ecossistema de defesa cibernética colaborativa.

Trabalhos futuros podem expandir a pesquisa para ambientes multi-cloud e IoT, avaliando desempenho sob arquiteturas distribuídas e cenários de latência variável.

6.1. Perspectivas Futuras da Automação de Defesa Cibernética

A evolução natural da automação de defesa cibernética aponta para a consolidação de SOCs autônomos (Autonomous SOCs), baseados em IA explicável (XAI) e aprendizado contínuo. Nesse novo paradigma, os sistemas não apenas executam ações automatizadas, mas também justificam e documentam suas decisões, fornecendo transparência operacional e rastreabilidade regulatória.

A IA explicável permitirá que as decisões tomadas por modelos de aprendizado de máquina sejam interpretáveis por humanos, reduzindo resistências e fortalecendo a confiança de auditores e gestores.

Frameworks como o LIME e o SHAP já estão sendo aplicados para explicar, em linguagem natural, por que um determinado evento foi classificado como malicioso — aproximando a IA da governança corporativa.

Outro eixo de avanço é a integração entre automação e conformidade regulatória. Normas como NIST CSF 2.0, ISO/IEC 27001:2022, LGPD e GDPR estão cada vez mais exigindo monitoramento contínuo e respostas documentadas a incidentes.

A automação baseada em IA pode gerar evidências e relatórios de conformidade em tempo real, reduzindo custos e riscos de não conformidade.

Além disso, a tendência de defesa cibernética colaborativa (Collaborative Cyber Defense) está ganhando força. Por meio de redes federadas de

compartilhamento de indicadores (como o MISP), múltiplas organizações poderão reagir de forma coordenada, compartilhando modelos e dados anonimizados em tempo real.

Essa abordagem, associada ao uso de IA distribuída, tem potencial para criar ecossistemas de defesa mais resilientes e adaptativos, onde cada incidente serve de aprendizado coletivo.

Em síntese, o futuro da automação de defesa cibernética caminha para a autonomia supervisionada — um equilíbrio entre ação automática e supervisão humana —, onde o papel do analista se transforma de executor para arquiteto da resiliência digital.

7. CONSIDERAÇÕES FINAIS

A automação baseada em IA e SOAR redefine o papel do analista de segurança, deslocando-o de executor para estrategista.

Em um cenário onde a velocidade de ataque supera a velocidade humana de reação, a defesa autônoma deixa de ser diferencial e passa a ser necessidade.

O framework proposto demonstra que é possível alcançar maturidade cibernética com tecnologias abertas, desde que integradas sob uma arquitetura inteligente e orientada a dados.

Dessa forma, contribui para a democratização da cibersegurança avançada, tornando-a acessível também a empresas que não dispõem de grandes orçamentos ou licenças corporativas.

REFERÊNCIAS BIBLIOGRÁFICAS

AL-MAMUN, Md. et al. Machine Learning-Based Intrusion Detection: A Comprehensive Survey. IEEE Access, v. 12, p. 146–172, 2024.

ENISA. Threat Landscape 2023. European Union Agency for Cybersecurity, 2023.

GARTNER. Market Guide for Security Orchestration, Automation and Response Solutions. Stamford: Gartner, 2023.

MITRE. Cyber Threat Intelligence and Automation Trends 2024. McLean, VA: MITRE Corporation, 2024.

NIST. Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: National Institute of Standards and Technology, 2018.

SARKER, Iqbal H. AI-Driven Cybersecurity: Emerging Trends and Future Directions. Journal of Information Security and Applications, v. 75, p. 103530, 2023.

THEHIVE PROJECT. TheHive and Cortex Documentation. Disponível em: https://thehive-project.org/. Acesso em: 12 out. 2025.

WAZUH. Open Source Security Platform Documentation. Disponível em: https://documentation.wazuh.com/. Acesso em: 12 out. 2025.

MISP PROJECT. Malware Information Sharing Platform (MISP) Documentation. Disponível em: https://www.misp-project.org/. Acesso em:

12 out. 2025.

ISO/IEC 27001. Information Security Management Systems. Geneva: International Organization for Standardization, 2022.

CyberDefense Analytics. ISO/IEC 27001. (2022). Information Security Management Systems.

[1] CISO e Fundador da Disatech – Soluções em Cibersegurança - Membro Sênior do IEEE. ORCID: 0009-0001-6474-5218. E-mail: neuber.diego@ieee.org