Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

**Artificial intelligence applied to threat detection and cyber incident response.**
Artificial intelligence applied to threat detection and cyber incident response

**Gabriel Lima**

**Summary**

This study aims to evaluate the effectiveness and feasibility of implementing artificial intelligence and machine learning techniques in threat detection and cyber incident response, aiming to optimize operational security and protect critical infrastructure against cyberattacks. The methodology adopted includes the analysis of advanced network monitoring systems, behavioral traffic analysis, and predictive algorithms for identifying anomalies and vulnerabilities. The results demonstrate that AI-driven automation significantly reduces the average time to incident detection and response, although challenges persist such as the occurrence of false positives, the need for continuous model training, and high implementation costs. It concludes that the sustainable adoption of these technologies requires investments in technical training, data governance, and continuous research and development efforts.

**Keywords:** Artificial Intelligence. Cybersecurity. Threat detection. Incident response. Machine Learning.

**Abstract**

This study aims to evaluate the effectiveness and feasibility of implementing artificial intelligence and machine learning techniques for threat detection and cyber incident response, aiming to optimize operational security and protect critical infrastructures against cyberattacks. The adopted methodology includes the analysis of advanced network monitoring systems, behavioral traffic analysis, and predictive algorithms in identifying anomalies and vulnerabilities. The results show that AI-driven automation significantly reduces the mean time to detect and respond to incidents, although challenges such as false positives, the need for continuous model training, and high implementation costs persist. The findings suggest that sustainable adoption of these technologies requires investment in technical training, data governance, and ongoing research and development.

**Keywords:** Artificial Intelligence. Cybersecurity. Threat Detection. Incident Response.
Machine Learning.

**Summary**

This study aims to evaluate the effectiveness and feasibility of implementing artificial intelligence techniques and automatic learning in threat detection and response to cyber incidents, with the aim of optimizing operational security and protecting critical infrastructures against virtual attacks. The methodology adopted includes the analysis of advanced network monitoring systems, traffic behavior analysis and predictive algorithms for identifying anomalies and vulnerabilities. The results demonstrate that automation driven by artificial intelligence significantly reduces the average detection and response time to incidents, although challenges such as the occurrence of false positives, the need for continuous training of models and high implementation costs persist. It is concluded that the sustainable adoption of these technologies requires investments in technical capacity, data governance and continuous effort in research and development.

**Keywords:** Artificial Intelligence. Cybersecurity. Threat detection. Respond to incidents. Automatic Learning.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

## 1. Introduction

This study aims to analyze the application of advanced artificial intelligence methods.
(AI) and machine learning *in* threat detection and response to
cyber incidents, with the goal of optimizing operational security and mitigating risks of
cyberattacks and promote more efficient management of data and infrastructure protection.
technological.

The security management proposed in this study is based on the integration of analysis algorithms.
Behavioral and network monitoring sensors that operate continuously. In case
In case of anomalies or attempted intrusions, these intelligent systems signal in real time to
Security operations center (SOC), enabling rapid identification, containment and
mitigating threats.

Therefore, this study aims to answer the following question: what is the effectiveness and feasibility of
implementation of advanced methods based on artificial intelligence for the detection of
Cyber threats and incident response, aiming to increase the resilience of organizations.
To protect against cyberattacks?

The overall objective is to evaluate the effectiveness and feasibility of implementing techniques.
advanced artificial intelligence and machine learning in automation of
Network monitoring, early threat detection, and optimized response to
cybersecurity incidents.

## 2. Theoretical Framework

### 2.1 Intelligent Systems in the Context of Cybersecurity

Knowledge is fundamental to the development of society, which has evolved from
The agricultural economy is transitioning to an industrial one and is now in the information age, where information...
It has become the most valuable and strategic asset of organizations. This scenario plays a role.
a central role in the advancement of productive forces, with success and resilience
Corporate success depends on how entities create, manage, and protect their...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

knowledge and data against growing digital threats (Rezende, 2003).

The changes in modern society are numerous, with most driven by...

The advancement of information technologies has brought about real-time data processing.

reality, global interconnection, and the breaking down of geographical barriers. However, this

Hyperconnectivity has expanded the virtual attack surface, imposing on organizations the

The need for constant updating and monitoring to ensure the integrity of their

digital ecosystems (Chaves Junior, 2021).

In this ongoing transformation, the transition from purely physical to intellectual work.

It has established information as the driving force of the contemporary economy. In this environment, the

Preserving the confidentiality, availability, and authenticity of data has become...

an essential requirement for both the economic stability of companies and for

Operational sustainability of the market. Information and communication technology.

By breaking down borders between countries, it enabled new business models, but also

exposed systems to highly sophisticated transnational cyber threats (Rezende, 2003).

In the knowledge age, a company's adaptability and cybersecurity infrastructure define its

survival in the market. As the

The sophistication of cyberattacks is accelerating the obsolescence of traditional defenses.

In rigid rules, the need arises for mechanisms capable of analyzing large volumes.

autonomous network data transmission. In this scenario, advances in hardware and software

They enabled the application of Intelligent Systems (IS), which utilize techniques

advanced computational tools for manipulating specialized knowledge and identifying

malicious behavior.

As highlighted by Rezende (2003), the behavior and attributes of a System

Intelligent systems differ substantially from conventional computing systems.

While traditional tools operate in a reactive and static manner, the Systems

Intelligent systems applied to cybersecurity are capable of analyzing complex patterns.

to correlate network events and infer new risks. This ability to manipulate

Dynamic representations of the real world allow for the identification and mitigation of anomalies.

cyber incidents with technical superiority and less human intervention (Rezende,

2003).

### 2.2 Artificial Intelligence and Machine Learning in Cybersecurity

The term "machine learning" *emerged* in the late 20th century and can...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

to be defined as the ability of a system to improve its performance at a task by through experience and the identification of patterns in large volumes of data (Magalhães, 2015). In the field of information security, this technology employs tools such as artificial neural networks and support vector machines (SVMs), which have proven to be highly effective in processing and analyzing complex and noisy data, a characteristic distinctive of data packets and network traffic logs (Ventura, 2012).

Furthermore, the use of natural language processing (NLP) allows systems Analyze unstructured texts, such as threat *intelligence reports,* logs of Auditing and analyzing suspicious emails, identifying attack patterns and social engineering vectors, the which contributes to increasing the accuracy in vulnerability detection (Syam; Sharma, 2018). In this way, machine learning establishes itself as a tool indispensable for optimizing security operations in dynamic digital environments and subject to constant changes in threats (Magalhães, 2015).

Ferreira (2024) explains that a machine learning model acquires and uses knowledge when one is able to use historical information to infer new results and identify unprecedented behaviors. In the cyber context, this means Use historical traffic and past requests to identify new attack vectors. previously unpredictable. Thus, machine learning refers to the field in which... Algorithms, techniques, and tools that enable this capability were developed and analyzed. adaptive protection.

Methodologically, machine learning applied to cybersecurity is categorized into different approaches:

- **Unsupervised learning:** groups network data without prior labeling for identify anomalies, out-of-the-ordinary behaviors, and new variants of attacks *(zero-day);*
- **Supervised learning:** uses previously classified data (such as benign traffic versus malicious code) as training examples for the model It can categorize new threats with high precision;
- **Semi-supervised learning:** combines labeled and unlabeled data to Optimize system training, reducing the operational cost of data labeling. without compromising predictive capacity (Syam; Sharma, 2018).

In terms of risk mitigation, machine learning plays a decisive role in... to enable the early identification of anomalies in complex computing infrastructures, such as corporate networks and critical servers, minimizing exposure time to

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

explorations and reducing potential financial and operational losses (Arbex, 2009). By
In turn, artificial intelligence (AI) emerged in the 1950s with the goal of developing
systems capable of performing tasks that require human cognitive ability or that do not
They possessed a viable algorithmic solution through conventional programming (Skalfist,
Mikelsten, Teigens, 2020). Researchers in the field use theories about processing of
information as a basis for developing systems capable of emulating analytical reasoning in
data monitoring (Aguiar, 2025).

These approaches can be encoded into programs that allow machines to learn.
reasoning and making autonomous defensive decisions (Ventura, 2012). AI has been evolving
continuously influencing areas such as incident response automation,
Intelligence against threats and machine learning, becoming a strategic pillar of
modern cybersecurity (Magalhães, 2015).

Aguiar (2025) emphasizes that AI can be applied to optimize monitoring and protection.
Continuous monitoring of IT ecosystems, enabling real-time analysis of security events.
With the ability to predict intrusions and execute automatic access blocks, it cannot...
With authorized authorization, artificial intelligence substantially increases the resilience of digital defenses.
By directly detecting flaws and intrusions, AI analyzes anomalies in data.
operational issues identify behavioral deviations in users or systems, reducing
drastically reduce downtime caused by attacks such as *ransomware* or
Service unavailability in critical sectors (Borruso, 2019).

Borruso (2019) highlights that the application of AI in cybersecurity management offers
significant benefits, such as time savings in alert triage, and a decrease in...
Analyst fatigue and a reduction in human error. By automating complex processes of
In incident containment, the system optimizes the performance of security operations centers.
(SOC). However, it is crucial to recognize that AI also presents challenges, including
the risk of false positives, biases in the models, and the emergence of adversarial tactics
aimed at deceiving themselves. Such challenges must be managed continuously.
to ensure that automation brings operational reliability without introducing new
vulnerabilities (Córdova, 2025). Thus, the integration of intelligent algorithms in defense
Cybernetics radically transforms information governance, provided it is accompanied by
specialized human supervision and constant improvement.

## 2 Methodology

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

This study adopted a qualitative and exploratory methodological approach, based on an integrative literature review to analyze the application of advanced techniques of Artificial intelligence and machine learning in threat detection and response.
Cyber incidents.

The search for theoretical and empirical references was carried out in the academic databases of High-impact databases *such as IEEE Xplore, Scopus, Web of Science ,* and *Google Scholar* were used . combined descriptors in Portuguese and English, such as: "artificial intelligence in cybersecurity" *(artificial intelligence in cybersecurity),* " *threat* detection" *detection),* "cyber incident response" , "learning " *Machine learning intrusion detection"* and "automation in SOC" *(security operations center automation).* Additionally, articles were examined. relevant data identified through the snowball sampling technique , by analyzing the references of the selected works.

The defined inclusion criteria included:

• Full scientific articles and book chapters published in indexed journals;

• Studies that directly addressed the effectiveness, operational challenges, and feasibility of implementation of artificial intelligence and *machine learning* algorithms in security information;

• Work focused on detecting network anomalies, mitigating known threats and unknown *(zero-day)* threats and cyber incident response automation.

Studies with a purely theoretical focus and no practical applicability to safety were excluded. computational or industrial automation-related projects that did not interface with cybersecurity. After selecting the bibliographic corpus, a categorical analysis was performed to map the main technologies, algorithms, and computational architectures applied. To achieve the Given the specific objectives proposed, the following analytical procedures were adopted:

• **Mapping AI Technologies:** Identifying and categorizing the main technologies. artificial intelligence and machine learning architectures (supervised, unsupervised) Supervised and natural language processing applied to traffic monitoring. Network and real-time log analysis;

• **Evaluation of Effectiveness in Threat Detection:** Investigation of the performance of these tools for early intrusion detection, behavioral analysis of anomalies, prevention of complex attacks (such as *ransomware* and data breaches) and reduction of Mean time to detection (MTTD);

• **Response Analysis and Operational Integration:** Assessment of integration feasibility.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

These solutions contribute to security automation ecosystems, such as *Security* tools.
*Orchestration, Automation and Response* (SOAR) and Security Operations Centers
(SOC), aiming to optimize incident mitigation and reduce average response time.
(MTTR).

## 3. Results and Discussion

The studies analyzed focus on the application of artificial intelligence (AI) and machine learning.
*Machine learning* in cybersecurity shows significant progress in identifying
threats, in mitigating risks and in optimizing the operational performance of security centers.
Information *(Security Operations Centers* — SOC). The correlated literature demonstrates that the
The transition from traditional reactive methods to AI-based predictive ecosystems alters...
fundamentally the dynamics of cyber defense.

Studies focused on continuous network traffic monitoring reveal that the implementation
The use of unsupervised learning algorithms allows the creation of behavioral profiles.
Dynamic for devices and users. This approach has proven highly effective in detection.
of subtle anomalies and *zero-day* intrusions (threats without a known signature),
overcoming the limitations of strictly rule-based detection systems.
Results indicate that real-time predictive analytics dramatically reduces the average time of
detection *(Mean Time to Detect* — MTTD), identifying data leaks and
malicious lateral movements in the initial stages of the attack.
In the context of automating cyber incident response, research highlights the impact
the integration between artificial intelligence models and orchestration and response platforms
Security *Orchestration, Automation and Response* (SOAR). The application of
Intelligent algorithms in the initial screening of alerts enable the autonomous execution of workflows.
containment measures — such as the immediate isolation of compromised machines, the lockdown
Automatic detection of suspicious IP addresses and proactive revocation of access credentials.
It is evident that automating simple responses significantly reduces the average response time.
*Mean Time to Respond* ( MTTR), in addition to relieving the strain on analysts' response time.
safety and reduce fatigue caused by excessive alerts.
Additionally, the literature findings address operational feasibility and challenges.
economic advantages inherent in the adoption of these smart technologies:

• Predictive Effectiveness: The use of natural language processing (NLP) combined with
Predictive models for *threat* intelligence analysis enable...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

anticipation of complex attack vectors, such as sophisticated *phishing* campaigns and ransomware infections ;

• Impact Cost Reduction: Although the initial investment in infrastructure While computational, software licensing, and specialized training may be high, the analysis of Economic viability demonstrates a positive return as it prevents stockouts. Systemic solutions prevent astronomical financial losses resulting from data breaches and fines. regulatory;

• Operational Challenges: The literature points to persistent limitations that require governance. rigorous, with emphasis on the false positive rate, the risk of data poisoning of training *(data poisoning)* and evasion tactics employed by cybercriminals against own artificial intelligence models.

The synthesis of the results confirms that the integration of advanced AI and machine learning methods... The use of machines in cyber incident response not only increases resilience and... reliability of IT ecosystems, but it also presents itself as a strategy. Sustainable and economically viable for the long-term protection of critical digital assets.

**Final Considerations**

The overall objective of this study was to evaluate the effectiveness and feasibility of implementing Artificial intelligence (AI) and machine learning techniques in threat detection and in Cyber incident response, with a focus on optimizing operational security and mitigating To mitigate the risks of cyberattacks and promote efficient data protection management. With this goal in mind, the specific objectives guided the literature review and supported the... conclusions presented.

Research into the technologies available for real-time monitoring has demonstrated The application of AI and *machine learning* is widely recognized for its impact. positive in early intrusion detection and network defense automation. However, the The study also indicated that the effectiveness of these tools depends directly on their quality. of the training data and governance over the computational models, which is crucial Precise *log* and event management is essential to optimize algorithm learning and prevent errors. operational biases.

In assessing the early detection of threats and prevention of complex incidents (such as (Regarding *ransomware* and data breaches), it has become evident that predictive behavioral analysis It overcomes the limitations of traditional approaches based solely on static signatures.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. São Paulo-SP.

**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

However, it was observed that the occurrence of false positives and the sophistication of techniques of The evasive tactics employed by cybercriminals still present technical challenges that require... maintaining specialized human supervision at security operations centers. (SOC).

Regarding economic and operational viability, the study assessed the balance between Investments and benefits of automation in cybersecurity. Although acquisition and integration and maintenance of smart tools present high initial costs, the analysis This demonstrates that this investment is largely offset by the reduction in average time. response time to treatment (MTTR) and the prevention of devastating financial losses resulting from Data leaks, system outages, and regulatory sanctions.

Thus, this study reaffirms the crucial importance of artificial intelligence in strengthening of modern cybersecurity. However, it highlights the need to overcome challenges such as Reducing false positives, mitigating the risks of data poisoning, and the need continuous technical training. To maximize the observed benefits, it is essential to maintain Constant efforts in research and development, ensuring that the solutions of Artificial intelligence evolves at the same pace as cyber threats.

**References**

AGUIAR, David. Use of artificial intelligence for proactive detection of cyber threats in corporate environments. Aurum, p. 57-67, 2025.

CHAVES JUNIOR, Wankes Solony de Carvalho. Materials Engineering within the scope of Industry 4.0. RCMOS-Multidisciplinary Scientific Journal The Knowledge, v. 1, n. 6, p. 1–9, 2021.

CÓRDOVA, Paulo Roberto. Artificial intelligence: between fascination and fear. Contexto, 2025.

FERREIRA, Poliana N. Machine Learning. Senac São Paulo, 2024.

MAGALHÃES, Renato Vasconcelos. Artificial intelligence and law: a brief introduction. Historical. Law and Liberty Review, ESMARN, Mossoró, v. 1, n. 1, p. 355–370, Jul./Dec. 2015. ISSN Print 1809-3280 | ISSN Electronic 2177-1758.

REZENDE et al. Intelligent systems: fundamentals and applications. Barueri, SP: Manole. 2003.

SYAM, Niladri; SHARMA, Arun. Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. Industrial Marketing Management, vol. 69, p. 135-146, 2018.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google


**Year VII, v.2 2026 | Submission: July 1, 2026 | Accepted: July 20, 2026 | Publication: August 16, 2026**

SKALFIST, P., MIKELSTEN, D., TEIGENS, V. Artificial Intelligence: The Fourth Industrial Revolution. Cambridge Stanford Books. 2020.

VENTURA, RV et al. Use of artificial neural networks in predicting genetic values for Weight at 205 days in Tabapuã breed cattle. Arq. Bras. Med. Vet. Zootec., v.64, n.2, p.411–418, 2012.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.