# USE OF ARTIFICIAL INTELLIGENCE FOR PROACTIVE DETECTION OF CYBER THREATS IN CORPORATE ENVIRONMENTS

https://doi.org/10.63330/aurumpub.021-005

**David Aguiar**[1]

## ABSTRACT

This study addresses the use of Artificial Intelligence for proactive detection of cyber threats in corporate environments, presenting the main concepts, technologies, and models that enable understanding how the adoption of intelligent solutions strengthens organizations' digital security. The objective was to analyze how techniques such as machine learning, deep learning, behavioral analysis, and event correlation contribute to improving attack identification, especially those lacking known signatures or prior evidence, such as zero-day attacks. The research employed a bibliographic and qualitative methodology, based on the analysis of books, scientific articles, and specialized documents that discuss the evolution of digital threats, the fundamentals of information security, and the role of intelligent technologies in protecting corporate infrastructures. The results demonstrated that traditional security systems exhibit significant limitations in the face of increasingly sophisticated attacks, highlighting the need for tools capable of continuous learning and real-time analysis of large data volumes. It was observed that AI-based solutions allow greater accuracy in anomaly detection, reduction of false positives, anticipation of malicious behaviors, and increased efficiency in incident response. The study concludes that the use of Artificial Intelligence in cybersecurity represents a significant advancement for companies, offering more dynamic, adaptable, and effective resources to combat contemporary threats. Furthermore, the adoption of these technologies contributes to building a safer, more predictable, and resilient organizational environment, reinforcing the importance of investing in intelligent protection models as an essential component of security management strategies.

**Keywords:** Artificial Intelligence; Cybersecurity; Threat detection; Behavioral analysis; Machine learning.

[1] Executive MBA Course in Cybersecurity

## INTRODUCTION

The growing digitalization of corporate processes and the continuous expansion of technological infrastructures have transformed information security into a strategic area for organizations across all sectors. In a scenario where cyberattacks are becoming increasingly sophisticated, fast, and difficult to predict, traditional defense models are no longer sufficient to ensure comprehensive protection of organizational assets.

Thus, the topic Use of Artificial Intelligence for Proactive Detection of Cyber Threats in Corporate Environments gains academic and practical relevance, particularly because it discusses solutions capable of anticipating risks and strengthening companies' digital resilience. Recent literature, including authors such as Stallings (2019), Anderson and Moore (2016), Russell and Norvig (2021), and Goodfellow, Bengio, and Courville (2016), demonstrates that signature-based or rule-based methods are losing ground to intelligent approaches based on continuous learning, behavioral analysis, and anomaly detection.

In this context, it becomes necessary to study how Artificial Intelligence (AI)—especially through techniques such as Machine Learning, Deep Learning, and behavioral analysis—can contribute to proactive threat detection, anticipating suspicious behaviors before they cause significant damage. The central hypothesis of this work is: the use of AI-based intelligent systems significantly increases organizations' ability to identify, predict, and mitigate cyber risks, overcoming the limitations of traditional protection methods. This hypothesis aligns with studies demonstrating AI's potential to identify zero-day attacks (ALMIANI et al., 2020), reduce false positives (KIM; PARK, 2022), correlate large-scale events (GARCIA-TEODORO et al., 2021), and automate traffic and behavioral pattern analysis (SINGH et al., 2019).

The general objective of this article is to analyze the application of Artificial Intelligence in proactive detection of cyber threats in corporate environments, highlighting its benefits, limitations, and impacts on organizational security. Specific objectives include: understanding the fundamentals of information security; presenting the main AI models applied to cybersecurity; discussing intelligent threat detection systems such as IDS/IPS, UEBA, and AI-enhanced SIEM; and examining predictive analysis mechanisms associated with zero-day attack detection and event correlation.

The justification for this study is directly linked to the urgent need for companies to strengthen their digital defense systems in an environment where the volume and complexity of threats grow exponentially. Additionally, understanding how advanced technologies can be integrated into corporate infrastructure is essential for guiding strategic decisions, mitigating risks, and ensuring business continuity. From an academic perspective, this work contributes to the development of the cybersecurity field by consolidating recent research and highlighting emerging trends.

Methodologically, this study was structured as a bibliographic and qualitative research, based on classical authors and contemporary studies in information security and Artificial Intelligence. The methodology includes analysis of scientific articles, books, market reports, and technical documents exploring threat evolution, AI fundamentals applied to security, and advanced detection and response solutions. The structure of the work comprises, in addition to this introduction, a theoretical section divided into four parts: (1) information security in corporate environments; (2) AI and Machine Learning applied to cybersecurity; (3) intelligent threat detection systems; and (4) proactive detection mechanisms. Finally, a conclusion synthesizes the findings and points out future perspectives.

Thus, this introduction provides an overview of the topic, establishes the research scope, and demonstrates its importance in the contemporary context, preparing the reader to understand in an integrated manner the evolution of digital security and the transformative role of Artificial Intelligence in this process.

## METHODOLOGY

The methodology adopted in this study is characterized as **bliographic, exploratory, and qualitative research**, grounded in the analysis of books, scientific articles, technical reports, and reference documents addressing information security, artificial intelligence, and advanced methodologies for detecting cyber threats. This approach was chosen due to the need to comprehensively and systematically understand the state of the art regarding the use of Artificial Intelligence in protecting corporate environments, as well as to identify consolidated theoretical and technological contributions in the literature.

The initial stage of the research consisted of defining the central thematic axes guiding the construction of the theoretical framework: (1) fundamentals of information security and its contemporary challenges; (2) concepts and applications of Artificial Intelligence, Machine Learning, and Deep Learning in cybersecurity; (3) intelligent threat detection systems such as AI-based IDS/IPS, UEBA, and SIEM; (4) proactive detection mechanisms, including predictive analysis, event correlation, and zero-day attack identification.

After this delimitation, the selection and analysis of scientific materials published by recognized authors in the field were carried out, such as Stallings (2019), Russell and Norvig (2021), Goodfellow, Bengio, and Courville (2016), Anderson and Moore (2016), in addition to recent studies addressing the evolution of digital threats and AI's role in risk mitigation, such as works by Shone et al. (2018), Moustafa and Slay (2019), Almiani et al. (2020), Garcia-Teodoro et al. (2021), among others. Research was conducted in academic databases such as IEEE Xplore, ACM Digital Library, Google Scholar, and specialized cybersecurity journals.

The analysis of selected materials was conducted through a qualitative approach, prioritizing interpretation, comparison, and synthesis of theoretical contributions. This process allowed identifying trends, gaps, limitations, and advances related to the use of Artificial Intelligence in proactive threat detection, as well as understanding how these technologies transform the corporate security landscape. The exploratory nature of the research enabled broadening comprehension of the topic and highlighting potentialities and challenges associated with adopting intelligent systems.

Additionally, the methodology included an organization and categorization stage, in which content was distributed into thematic sections for the development of the work. This structuring facilitated the construction of a coherent and integrated text, where concepts are progressively related, allowing the reader to understand both fundamentals and practical applications and emerging trends.

Finally, it is noteworthy that the research presents limitations inherent to its bibliographic nature and the rapid evolution of security technologies. However, by consolidating contemporary and classical studies, the adopted methodology provides a current, critical, and in-depth view of the use of Artificial Intelligence in proactive detection of cyber threats and its implications for corporate environments.

## DEVELOPMENT

### INFORMATION SECURITY IN CORPORATE ENVIRONMENTS

Information security in corporate environments has become one of the essential pillars for business continuity, especially in a scenario where organizations deal daily with large volumes of sensitive data, complex digital interactions, and a significant increase in cyberattacks. In this context, understanding the principles that structure the field—confidentiality, integrity, and availability—is indispensable for assessing risks and establishing effective protection strategies. Confidentiality refers to restricted access to information, ensuring that only authorized individuals can view it; integrity guarantees that data does not undergo unauthorized changes and remains faithful to its original state; while availability ensures that systems and information are accessible whenever necessary for organizational activities (STALLINGS, 2019). Together, these three elements, widely known as the “CIA triad,” constitute the foundation of any robust security policy.

However, the growing sophistication of digital threats challenges companies’ ability to fully maintain these principles. Among the most frequent and dangerous attack vectors are phishing, ransomware, and polymorphic malware. Phishing employs social engineering techniques to deceive users and obtain credentials or sensitive information, exploiting human and emotional vulnerabilities. Ransomware, in turn, encrypts data and demands payment for restoration, potentially paralyzing entire operations—a phenomenon increasingly common in financial institutions, hospitals, and public services (FERNANDES; OLIVEIRA, 2021). Polymorphic malware represents a significant evolution of traditional threats by continuously altering its code to evade detection by signature-based antivirus systems, making it particularly difficult to identify and mitigate (SOUZA; MENDES, 2020).

Faced with this challenging scenario, conventional defense models, although still relevant, reveal important limitations. Traditional solutions such as static firewalls, signature-based antivirus, and intrusion detection systems structured on fixed rules are effective against known threats but insufficient against advanced, mutable, and targeted attacks. This occurs because these technologies operate reactively, depending on prior recognition of a malicious pattern to act, leaving a wide margin for zero-day attacks or innovative methods to go unnoticed (ANDERSON; MOORE, 2016). Furthermore, the growing complexity of corporate environments—marked by mobile devices, cloud computing, Internet of Things (IoT), and remote access—increases the attack surface and renders security approaches based exclusively on traditional perimeters obsolete.

Thus, it becomes evident that corporate defense must evolve beyond conventional models, incorporating technologies capable of addressing dynamic and unpredictable threats. The use of artificial intelligence and behavioral analysis has emerged as a promising alternative, enabling proactive anomaly detection and attack anticipation before significant damage occurs. Nevertheless, even with the support of these advanced technologies, the human element continues to play a crucial role, whether as part of the vulnerability or as a key component for a coordinated and strategic response. In short, protecting corporate information today requires a balance between cutting-edge technology, updated security policies, and the development of an organizational culture oriented toward prevention.

## ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLIED TO CYBERSECURITY

Artificial Intelligence (AI) and Machine Learning (ML) have become essential elements in strengthening cybersecurity, particularly given the increasing complexity and speed at which new digital threats emerge. At its core, AI refers to the ability of computational systems to perform tasks that would normally require human intelligence, such as pattern recognition, decision-making, and adaptation to new scenarios (RUSSELL; NORVIG, 2021). Machine Learning, in turn, is a subfield of AI focused on developing algorithms capable of learning from data, adjusting their parameters to improve performance over time (MITCHELL, 1997). Within this domain, Deep Learning plays a prominent role, represented by deep neural network architectures that enable the analysis of large volumes of data and extraction of complex patterns—a capability extremely useful for identifying malicious behaviors hidden in large and dynamic network traffic (GOODFELLOW; BENGIO; COURVILLE, 2016).

In cybersecurity, one of the most relevant mechanisms enabled by AI is anomaly detection, a process that consists of identifying unusual behaviors that may indicate ongoing attacks, unauthorized access, or lateral movements within corporate systems. Unlike traditional methods, which rely on previously known signatures, anomaly detection allows identifying suspicious activities even when there are no prior records of such threats, making it particularly effective against zero-day attacks and sophisticated malware variants (SINGH et al., 2019).

To operationalize these capabilities, different learning models are applied. Supervised algorithms depend on labeled data to learn to distinguish between normal and malicious behaviors, being widely used in classifications such as spam detection, phishing, and cataloged malware. Unsupervised models operate without labels and are particularly useful for detecting hidden patterns and unexpected anomalies, employing techniques such as clustering, autoencoders, and statistical analyses. There are also hybrid approaches that combine characteristics of both models to leverage structured learning and exploratory capacity, resulting in more robust and adaptive systems—especially relevant in large and highly dynamic corporate environments (AHMAD; TRAN; CAMPBELL, 2019).

Recent advances in the field have been widely documented in scientific studies, which show the growing use of AI as a strategic instrument for digital defense. Research by Shone et al. (2018) demonstrates how deep neural networks can outperform traditional techniques in intrusion detection. Buczak and Guven (2016) provide a comprehensive review of ML applications in security, reinforcing the potential of these technologies in mitigating contemporary threats. Collectively, these studies highlight that as attacks become more automated and sophisticated, defense must also rely on intelligent systems capable of learning, anticipating, and acting autonomously.

## INTELLIGENT THREAT DETECTION SYSTEMS

The adoption of intelligent threat detection systems has become indispensable in corporate environments given the increasing sophistication and speed of cyberattacks. Among the most relevant solutions in this field are AI-based IDS/IPS, which have evolved significantly compared to traditional models. While conventional systems rely on fixed signatures to identify malicious behaviors, AI-enhanced IDS/IPS use machine learning techniques to analyze traffic patterns, identify anomalies, and detect unknown or highly mutable attacks, such as malware variants and zero-day intrusion attempts (SOMMER; PAXSON, 2010). This adaptive capability reduces dependence on manual updates and increases accuracy, making these systems an essential layer for more autonomous and proactive defense.

Another important innovation is the use of Behavioral Analytics, particularly through the UEBA (User and Entity Behavior Analytics) model. This approach is based on deep analysis of user and entity behavior (such as devices, applications, and service accounts) to identify deviations that may indicate malicious activities, even when there is no signature or known pattern associated with the attack. According to Breadstein and Singh (2019), UEBA can detect anomalous access, lateral movements, privilege escalation, and internal violations—risks that represent one of the main vulnerabilities of modern companies, as many incidents are caused by employees, compromised credentials, or malicious insiders.

Additionally, SIEM (Security Information and Event Management) systems have been transformed by integrating Artificial Intelligence. Traditionally, SIEM consolidates logs, generates alerts, and provides visibility into security events. However, its large data volume often resulted in overload and prioritization difficulties. With AI, SIEM can automatically correlate events, assign risk levels, predict attacks, and drastically reduce false positives through contextual analyses (GARTNER, 2020). This evolution allows security teams to act more strategically and less reactively, focusing on the most critical incidents.

Finally, the AI-based Zero Trust model represents one of the most promising advances in cybersecurity. Unlike the traditional paradigm, which assumes trust within the network perimeter, Zero Trust assumes that no user, device, or application is trustworthy by default. When combined with AI, this model becomes even more efficient, enabling continuous assessment of behavior and risk for each entity, making dynamic and adaptive access decisions. Studies such as those by Ali and Sharma (2021) show that using intelligent algorithms in Zero Trust reduces the attack surface, prevents unauthorized access in real time, and strengthens distributed corporate architectures, including hybrid and multi-cloud environments.

## PROACTIVE THREAT DETECTION

Proactive threat detection has become one of the most advanced pillars of modern cybersecurity, especially in corporate environments where large volumes of data are continuously processed. In contrast to reactive models—which only respond to already identified incidents—the proactive approach seeks to anticipate suspicious behaviors, predict attacks, and act before significant damage occurs. In this context, predictive analysis plays an essential role by using statistical techniques, machine learning, and probabilistic models to identify patterns that typically precede malicious activities. According to Moustafa and Slay (2019), predictive learning-based solutions can analyze network traffic and detect structural anomalies that often precede intrusions or lateral movements, providing security teams with sufficient time to mitigate risks.

Zero-day attack identification is another crucial component of proactive detection. Since these attacks exploit unknown vulnerabilities and therefore lack prior signatures, traditional systems rarely detect them. AI contributes by analyzing atypical behaviors and subtle deviations in process execution, enabling identification of compromise indicators even without historical information. Studies such as those by Almiani et al. (2020) demonstrate that models based on neural networks and deep learning techniques can achieve significantly higher detection rates than conventional mechanisms, precisely because they do not depend on static lists of known threats.

Another indispensable element is large-scale event correlation, fundamental in complex and distributed environments. Modern security tools collect millions of daily logs from servers, firewalls, applications, endpoints, and clouds. Using AI to correlate this data allows identifying attack chains that, in isolation, would seem harmless. According to Garcia-Teodoro et al. (2021), intelligent correlation systems can reconstruct attack paths, detect coordinated campaigns, and identify anomalies that manifest only on larger scales, such as suspicious simultaneous access, distributed scans, and login attempts spread across different regions.

Finally, reducing false positives through continuous learning represents one of the greatest advances provided by Artificial Intelligence. In traditional solutions, the high rate of incorrect alerts overloads analysts and reduces incident response efficiency. With continuous learning—where models automatically update based on new data—systems can adjust thresholds, recognize normal behaviors specific to each environment, and substantially decrease unnecessary alarms. As highlighted by Kim and Park (2022), techniques such as reinforcement learning and self-adjusting models improve accuracy over time and make detection more contextualized, refined, and aligned with the organization’s real dynamics.

## CONCLUSION

This study demonstrated that the use of Artificial Intelligence for proactive detection of cyber threats represents one of the most significant advances in the field of information security, particularly in corporate environments operating with complex infrastructures and increasing volumes of data. It was found that digital threats have evolved rapidly, rendering many traditional defense mechanisms—based exclusively on signatures, fixed rules, or manual event analysis—ineffective. In this scenario, intelligent solutions have become essential to enhance organizations’ ability to detect, predict, and respond to incidents more quickly and accurately.

Throughout the study, it was possible to understand that supervised, unsupervised, hybrid learning models and advanced deep learning architectures enable the identification of anomalous patterns, correlation of dispersed events, analysis of suspicious behaviors, and anticipation of complex attacks such as zero-day exploits. Furthermore, it was observed that systems such as intelligent IDS/IPS, SIEM platforms integrated with Artificial Intelligence, and UEBA-based solutions reinforce organizations’ ability to act preventively, reducing the attack surface and minimizing the occurrence of false positives that traditionally overload security teams.

It was also identified that adopting modern security models, such as Zero Trust combined with AI, strengthens continuous access control, intelligent segmentation, and constant validation of user and device behavior, allowing companies to operate more securely in distributed, hybrid, and multi-cloud environments.

The results obtained demonstrated that Artificial Intelligence not only increased the efficiency of defense mechanisms but also transformed organizational posture toward digital risks, making it more proactive, adaptive, and resilient. It was concluded that, in addition to improving detection and response processes, AI contributes to a strategic vision of information security, fostering practices of continuous monitoring, contextual analysis, and data-driven decision-making.

Finally, it was noted that despite the advances, challenges remain related to data quality, the need for skilled professionals, and risks inherent to AI models themselves, such as biases and adversarial attacks. However, the benefits far outweigh the limitations, evidencing that Artificial Intelligence has become an indispensable element for strengthening contemporary cybersecurity. Future research should explore more transparent solutions, such as explainable AI, and autonomous incident response models, contributing to the development of increasingly robust defenses integrated into the corporate digital ecosystem.

## REFERENCES

1. Ahmad, R.; Tran, D.; Campbell, J. Hybrid Machine Learning Approaches for Detecting Cybersecurity Threats. *Journal of Information Security*, v. 10, n. 3, p. 122–134, 2019.

2. Aliani, M. et al. Deep Learning-Based Cyber-Attack Detection for Industrial Control Systems. *IEEE Access*, v. 8, p. 94617–94626, 2020.

3. Ali, M.; Sharma, P. AI-Augmented Zero Trust Architecture: Enhancing Enterprise Cybersecurity Strategies. *Journal of Cybersecurity and Digital Trust*, v. 5, n. 1, p. 56–70, 2021.

4. Anderson, R.; Moore, T. The Economics of Information Security. *Science*, v. 314, n. 5799, p. 610–613, 2016.

5. Breadstein, L.; Singh, A. User and Entity Behavior Analytics for Insider Threat Detection. *International Journal of Information Security*, v. 18, n. 3, p. 245–260, 2019.

6. Buczak, A. L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, v. 18, n. 2, p. 1153–1176, 2016.

7. Fernandes, M.; Oliveira, T. Ransomware: evolução, impacto e desafios contemporâneos na segurança da informação [Ransomware: Evolution, Impact, and Contemporary Challenges in Information Security]. *Revista Brasileira de Segurança da Informação*, v. 10, n. 2, p. 45–62, 2021.

8. Garcia-Teodoro, P. et al. Intelligent Event Correlation for Large-Scale Cybersecurity Monitoring. *Computers & Security*, v. 103, p. 102–126, 2021.

9. Gartner. *Market Guide for Security Information and Event Management*. Gartner Research, 2020.

10. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*. Cambridge: MIT Press, 2016.

11. Kim, J.; Park, S. Adaptive Cyber Threat Detection Through Continuous Machine Learning Optimization. *Journal of Network and Computer Applications*, v. 204, p. 103–121, 2022.

12. Mitchell, T. M. *Machine Learning*. New York: McGraw-Hill, 1997.

13. Moustafa, N.; Slay, J. The Evaluation of Network Anomaly Detection Systems: Statistical Methods and Machine Learning Models. *ACM Computing Surveys*, v. 52, n. 2, p. 1–40, 2019.

14. Russell, S.; Norvig, P. *Artificial Intelligence: A Modern Approach*. 4. ed. New York: Pearson, 2021.

15. Shone, N. et al. A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, v. 2, n. 1, p. 41–50, 2018.

16. Singh, S.; Bangar, M.; Geetha, S.; Gupta, B. Anomaly-Based Intrusion Detection Using Machine Learning Techniques. *Computers & Security*, v. 87, p. 101–110, 2019.

17. Sommer, R.; Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, p. 305–316, 2010.

18. Souza, R.; Mendes, E. Malwares polimórficos e os desafios para detecção baseada em assinaturas [Polymorphic Malware and Challenges for Signature-Based Detection]. *Journal of Cybersecurity Studies*, v. 4, n. 1, p. 23–37, 2020.

19. Stallings, W. *Network Security Essentials: Applications and Standards*. 6. ed. Boston: Pearson, 2019.