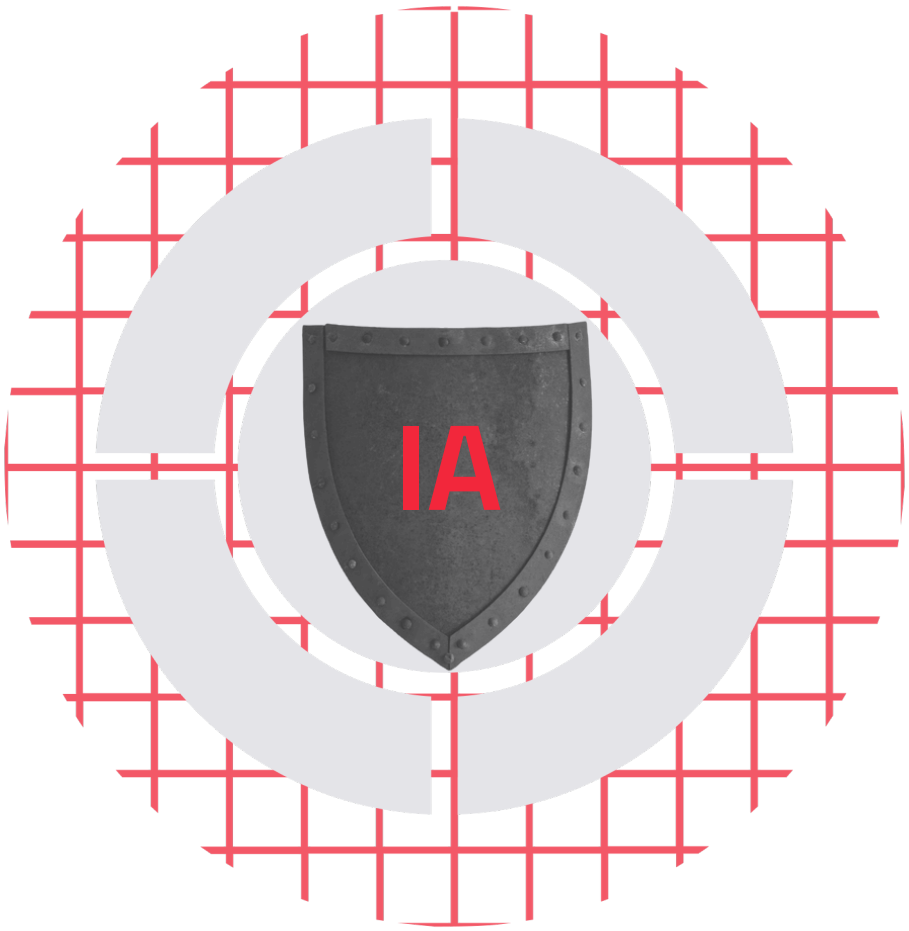
ENTHEC

WHITEPAPER

CYBER THREAT INTELLIGENCE

AI extends the reach of cybersecurity



INDEX

INTRODUCTION

Cybersecurity was born linked to the concepts of internal perimeter and risk management: organizations were in the first phase of their digital transformation, the complexity of their IT systems was small, cybercrime was just starting and attacks were unsophisticated. In that scenario, the strategic approach of protecting the internal perimeter of organizations through shielding and managing risk was the most effective, affordable and rational. There was no need to go further.
However, time has passed and the speed of technological innovation and its impact on markets have injected complexity into both corporate IT systems and relationships between organisations and have allowed for the sophistication of cybercrime attacks.
Cloud operations, the entry of third parties into internal systems, the connection between internal and third-party systems and the use of the latest technologies by cybercriminals today render the strategic focus limited to the internal perimeter and risk management ineffective, mainly due to two factors:

- The low effectiveness of its results, as demonstrated by the number of successful cyberattacks that grows unstoppably every year and the perfection of social engineering techniques.

- The cost in resources of protecting systems and managing increasingly complex and ever-expanding risks.

Despite this manifest ineffectiveness, the inside-out approach to cybersecurity remains the basis of most corporate cybersecurity strategies, causing corporate cyber protection policies to enter into a dynamic shaped by their cost, their poor results and the board's resistance to new investments in cybersecurity, which fully affects the work of the CISO. Despite the fact that cybersecurity is today a business risk problem, which directly affects the survival and sustainability of the business, CISOs still have to fight for the allocation of resources.

INTRODUCTION

Changing this approach, expanding the controlled perimeter, and using new technologies such as AI to reduce costs are the evolutions that cybersecurity strategies need to overcome this loop and reduce the success rates of cyberattacks.
Organizations are no longer small, isolated tribes that can defend themselves from unknown attacks by entrenching themselves behind a wall.

Today, organizations are complex entities with extended perimeters that are difficult to define. These require, in addition to defense and protection strategies, intelligence strategies that allow them to manage risk and exposure to threats. These strategies also require tools capable of infiltrating the territory where the enemy operates to obtain information about its tactics and resources.

Following a mantra that has been engraved in military strategies for thousands of years and executed through espionage: in complex environments, information is the basis of the protection strategy.

In this document we will study and compare perimeter cybersecurity and extended cybersecurity strategies, the traditional inside-out approach versus the emerging outside-in approach, and how AI is one of the determining factors for the success of the new paradigm in cybersecurity: cyber threat intelligence.

PERIMETER CYBERSECURITY: RISK MANAGEMENT

The perimeter cybersecurity strategy is based on an inside-out approach and risk management: the internal corporate perimeter is protected and shielded according to the data obtained from the hypotheses raised in the risk management process. Once the perimeter is shielded, different attack simulation tests are periodically carried out to check the effectiveness of the shielding and make the necessary corrections and updates.

> The perimeter cybersecurity strategy is the most basic, it works effectively in simple environments and is always the basis on which the rest of the strategies must be implemented.

In a simple environment, with simple IT systems, well-defined corporate perimeters and unsophisticated cyberattacks, a perimeter cybersecurity strategy may be sufficient and represent an affordable resource cost for the organization.

But that simple environment, if it ever existed, is gone today and will not return.

Organizations and their governing bodies must be aware that the digital environment in which their businesses operate today is complex and will continue to be so, and that is why cybersecurity strategies based on hypotheses that consider this to be the case will never again yield good results.

Shielding the internal perimeter of organizations remains essential and necessary, but in a complex environment such as the current one is insufficient.

PERIMETER CYBERSECURITY: RISK MANAGEMENT

- Cybercrime has reached a high level of sophistication and success thanks to the use of new technologies such as AI and the improvement of social engineering techniques.

In 2022, data breach notifications were 6.3% higher than in the previous year, with ransomware and unauthorized access being the main attacks carried out.
Data from the Spanish Data Protection Agency (AEDP).

- A large part of organizations' solutions, operations and information is hosted in third-party clouds and applications.

In 2022, the number of users who increased their budget for cloud solutions increased by 55%. Forecasts indicate that the cloud market will grow by more than 21% in 2023.
Cloud Market Report in Spain 2022. Quint 2023

- Third parties such as partners, suppliers and collaborators often have input in the internal systems of organizations.

Third-party vulnerability was the fourth attack vector in 2022 data breaches in the financial and banking sector.
Europa Press

LIMITATIONS OF PERIMETER CYBERSECURITY

Our tribe has grown, the wall that once served to keep it protected and secure is no longer enough to hold the resources and weapons stored in warehouses in other tribes, because ours can no longer hold them, or the keys to the wall held by inhabitants of other tribes who collaborate with ours, or the enemies disguised in our uniforms who deceitfully obtain the password to open our doors. Cybercriminals now have the ability to gain entry using the same means that an employee or third party can gain entry into the organization. How capable is perimeter cybersecurity of preventing this type of attack?

Despite being the basic strategy, perimeter cybersecurity in complex environments has limitations that destroy its effectiveness:

Risk management works on hypotheses

The risk calculation used to size and design the perimeter cybersecurity strategy is based on the quantification of all possible risks and threats, including those that have occurred and are known and those that are likely to occur. This is the first series of hypotheses that affects the result: probability. The second series includes all those attacks that are not even known, but that must be included in the calculation, to take into account the unforeseen.

Thus, perimeter cybersecurity strategies tend to handle weak data, sometimes distorted by analyst bias and with an upward trend in order to cover cyber protection against an unknown number of risks with an unknown degree of threat.

LIMITATIONS OF PERIMETER CYBERSECURITY

Third party risk

Perimeter cybersecurity is of little use against third-party risk. A failure in third-party security causes the cyberattack to be carried out undetected. In addition, third-party risk management is carried out by checking compliance with a series of requirements through questionnaires and the results of specific intrusion tests, as a snapshot. Checks and tests that cannot reach the fourth or nth (third parties of the third parties of the organization).

The complexity of organizations' IT systems

At a time when organizations have passed the stage of digitization and their natural environment is already digital, the complexity of IT systems grows permanently and continuously. In order to secure their shielding, the perimeter cybersecurity solutions that protect the corporate IT system must grow and be updated in the same way. This translates into a strategy of perimeter cybersecurity that is in permanent need of growth and that is outdated very quickly.

The sophistication of cyber attacks

The determining factor in any protection and defence strategy is the enemy's capacity. In cybersecurity, this factor translates into an adversary that uses constantly innovative techniques and has the human factor playing in its favour. Cybercrime quickly and effectively incorporates any technological innovation. New technologies such as AI or Machine Learning are already used to obtain the information that serves to open the way for a cyberattack. The ability to create deep fakes has a direct impact on the vulnerability of the human factor, the weakest link in any cybersecurity strategy. And the ability to track and analyse organisations in search of information improves this capacity, against which perimeter cybersecurity has very few defences.

LIMITATIONS OF PERIMETER CYBERSECURITY

The cost of perimeter shielding

The cost of resources to maintain the effective and updated shielding on which the perimeter cybersecurity strategy is based is unaffordable for any organization, since it is calculated on hypotheses that overestimate the risks and threat levels in order not to fail and, in addition, they have to reach a corporate IT system in permanent growth, which means that this cost tends to infinity. This causes cybersecurity to end up being conceived within management as an expense that slows down business growth and not as an investment in it.

Incorrect assessment of the business impact of risk

The consequence of risk management working on hypotheses is that the assessment of the business impact of risk also does so. Because of this, the assessment of the business impact of risk suffers from the same problems as the assessment of risk through hypotheses: working with weak data, sometimes distorted by the analyst's bias and with an upward trend in order to cover cyber protection against an indefinite number of impacts of an undetermined size. This, in addition to the natural overvaluation of the impacts to cover one's back, causes the rest of the departments and management to be very little involved in the assessment itself and the results of the assessment contain greater inaccuracy.

> Lack of data means we cannot validate a risk estimate or review the historical accuracy of previous risk estimates. Formalized risk assessment and quantification processes encode erroneous cybersecurity beliefs about threats, vulnerabilities, and links between infrastructure and business processes.
> Maverick Research: Risk Management Delivers Poor Cybersecurity. Gartner 2023

All these limits cause the perimeter cybersecurity strategy to end up falling into a dynamic that fully impacts the CISO's work:
High cost in resources + Low efficiency =
Resistance of the directive to invest in cybersecurity

EXTENDED CYBERSECURITY: MANAGING EXPOSURE TO THREATS

A complex environment requires a cybersecurity strategy that can be efficient and affordable regardless of that complexity and its variations. The perimeter cybersecurity strategy, or inside-out approach to cyber protection, is inefficient and costly when the environment becomes complex.

The need to broaden the scope and shift to an outside-in approach to gather information that serves as a basis for designing a cybersecurity strategy was detected thousands of years ago in military protection: military intelligence. Transferring this military paradigm to cybersecurity strategies is now essential to achieve advanced, evolved-level cybersecurity capable of providing the responses in terms of efficiency and costs that the current environment requires.

Extended cybersecurity, in addition to including risk management, focuses on managing exposure to threats. It goes beyond the internal perimeter of organizations to find vulnerabilities that threaten the organization and are within reach of any cybercriminal, to allow them to design a cyber protection strategy against that particular threat, detect the security breach that caused it and eliminate it, and control the time of exposure to said vulnerability.

Extended cybersecurity and the outside-in approach focus their effectiveness on the value of information in any security strategy, on extending cyber intelligence beyond the perimeter of organizations to work on real information and not on hypotheses.

EXTENDED CYBERSECURITY: MANAGING EXPOSURE TO THREATS

Going outside the organization's perimeter to find out what corporate information cybercriminals have, what security gaps they are exploiting, and what tactics associated with a vulnerability they can use, that is, managing exposure to threats through cyber intelligence, allows the organization's response to be prior to the attack, fast, accurate, effective and without implying a high cost of resources. Extended cyber intelligence strategy that covers the management of exposure to threats due to internal causes, and also, the exposure to threats caused by third parties.

> Maverick Strategic Planning Assumption: By 2030, boards will rely on AI-summarized threat exposure data to prioritize investments, rather than cybersecurity risk assessments, up from less than 1% in 2023.
> Maverick Research: Risk Management Delivers Poor Cybersecurity. Gartner 2023

CYBER THREAT INTELLIGENCE: LOCATION AND DEFINITION OF RISK

Extended cybersecurity aims to manage exposure to threats. The basis of their strategy is extended cyberintelligence, that, locates exposed vulnerabilities and corporate security breaches within the reach of any cybercriminal to eliminate them or take measures capable of counteracting them in the event that they are used to execute a cyberattack.

Locating a risk allows you to define it, know its scope and design the most effective strategy to eliminate it.

The mission of extended cyber intelligence is to monitor and track 24x7 the external perimeter of the organization where cybercriminals move to locate and define internal and third-party risks and transfer the information in real time to the corporate security department or the corresponding MSSP.

While in the early stages of cybersecurity this capability was beyond the reach of organisations, the emergence of new technologies such as AI and Machine Learning have enabled the emergence of automated solutions capable of scanning the Web, Deep Web and Dark Web in the same way that cybercriminals do. Extended cyber intelligence allows organisations to stay ahead of cybercriminals, as automated and continuous monitoring allows threats to be located and defined as they arise and thus neutralised before a cybercriminal has had time to plan how to use them.

CYBER THREAT INTELLIGENCE: LOCATION AND DEFINITION OF RISK

Exposure to a threat over time increases its dangerousness exponentially.

When an organization has the ability to locate the threat and define the associated risk at the very moment the vulnerability is created, it has the ability to get ahead of the cybercriminal who has also located that same threat and is preparing to use it to carry out an attack. AI allows organizations to have the ability to classify the threats located by category and know the most effective actions to nullify them, all without human intervention.

Continuing with the analogy of our tribe, extended cyber intelligence would be having an army of spies continuously gathering and transferring information from enemy territory.

If cybercrime has become more effective without increasing costs thanks to the use of new technologies, cybersecurity has no other option but to evolve in the same way in order to confront it.

CYBER THREAT INTELLIGENCE: BUSINESS IMPACT ASSESSMENT

Calculating business impact is essential for optimizing resources dedicated to cyber protection.

When an organization's cybersecurity strategy is limited to securing the perimeter, the business impact assessment of the risks is done based on the hypotheses used to calculate the risks. The involvement of the rest of the organization's departments and management in calculating the business impact is small, since it is difficult to work on the basis of these hypotheses outside the cybersecurity environment. In addition, as we have already pointed out, the hypotheses are always biased by the analyst and tend to overestimate both the risks and their impacts to ensure the protection of the organization, with the consequence that the resource figures required for the cybersecurity strategy are also overestimated.

When an organization opts for extended cyber intelligence strategy beyond the perimeter, the ability to identify and define risks allows organisations to accurately assess their business impact and to allocate the necessary resources to minimise it.

Threat exposure management through extended cyber intelligence facilitates the calculation of business impact, since it does not work on hypotheses, but on the information obtained through automated and continuous monitoring of threats, and allows the departments that may be affected and management to be involved in the calculation of the impact. The consequence is that more precise calculations of the business impact of each given risk are obtained and only the resources necessary to nullify it are dedicated.

THE ROLE OF AI IN CYBER THREAT INTELLIGENCE

The development of cyber threat intelligence has been one of the innovations brought to cybersecurity by the emergence of AI.

The dark web and deep web, which, together with the web, make up the external perimeter of organizations, are environments that host content not indexed by conventional search engines.

Cybercriminals use these network parts to carry out illegal activities, such as exchanging leaked information, selling stolen data, spreading malware, and other cybercrimes.

AI plays an essential role in the main activity of cyber threat intelligence: monitoring and detecting threats in the visible and hidden layers of the Internet.

Using machine learning algorithms and natural language processing techniques, AI analyzes large volumes of real-time data to identify leaked corporate information and detect patterns and signals of suspicious activities. This includes locating compromised passwords, detecting conversations related to the sale of corporate leaked information, or identifying the organization as a target for future cyberattacks.

In addition, AI can help in identifying sources of data breaches and evaluating their authenticity. By analyzing metadata, comparing information with reliable sources and tracking the chain of custody, AI can determine whether the leaked information is genuine and what steps should be taken to mitigate the associated risks. In this way, false positives and the expenditure on resources associated with them are
avoided.

THE ROLE OF AI IN CYBER THREAT INTELLIGENCE

Early detection of corporate information leaked beyond the internal perimeter, on the Web, Dark Web and Deep Web, allows organizations and law enforcement to take proactive measures to protect data, close security gaps and prevent the business impact of the cyberattack. This includes notifying affected departments, reinforcing necessary cybersecurity measures and implementing strategies to track and dismantle the cyberattack before it succeeds.

The evolutionary nature of AI means that its adaptation to the continuous changes arising from the sophistication of cybercrime is not complex, thus revealing itself as the best weapon to face the challenge of modern cyberattacks.

The use of AI has managed to break the limits that the perimeter of organizations established for cybersecurity strategies. Complemented by other technological innovations such as automation and machine learning, they have turned cyber threat intelligence into an evolved cybersecurity strategy that gains in effectiveness, reduces resource costs and is capable of hindering the latest generation of cyberattacks.

Cyber Threat Intelligence + AI

Localization of vulnerabilities in real time

Definition of risk

Business impact analysis

Definition and execution of actions

ADVANTAGES OF CYBER THREAT INTELLIGENCE AND THE OUTSIDE-IN APPROACH

- Works on accurate data and not on hypotheses or biases.
- Localization of vulnerabilities in real-time.
- Rationalizing the use of resources in cybersecurity.
- Involvement of management and other departments in the cybersecurity strategy.
- Using AI to locate and define risks.
- Using AI to analyze the business impact of threats.
- Location of vulnerabilities that can be used to develop social engineering techniques.
- Innovation and ease of updating and scaling cyber intelligence tools.
- Automation, monitoring, information localization and risk analysis without human intervention.
- Location and definition of third-party and n-party risk.
- The capacity of the extended cybersecurity strategy does not depend on the size or internal circumstances of the organization, but on the power of the solution and its development.
- Contribution of valuable data to the design of intrusion tests on internal shielding.

External attack surface management (EASM) provides valuable risk context and actionable insights through continuous analysis to assess and prioritize localized risks and vulnerabilities. External attack surface management is a priority for security teams and security risk managers.

Gartner, Peer Insights

ENTHEC

WHITEPAPER

kartos©

Kartos Corporate Threat Watchbots: Continuous Threat Exposure Management (CTEM)

Automated, continuous, real-time monitoring of the organization's threat exposure, focused on cybersecurity and business criteria.

EXTERNAL ATTACK SURFACE

Location of the Company's open and exposed information and vulnerabilities on the Internet, the Deep Web, Dark Web and Social Networks: Phishing, fraud and scam campaigns; CVEs; DNS health; leaked passwords and credentials; leaked and exposed documentation and databases.

DIGITAL RISK PROTECTION

Detection of contextual information about potential attackers, their tactics and processes for carrying out malicious activities. Elimination of malicious activities on behalf of the Company. Brand, domain and subdomain protection. Corporate email protection. Ransomware protection. Web security and threat removal.

THIRD PARTY RISK

Real-time monitoring of third-party risk. Objective data on ongoing threats related to the value chain. Comprehensive view of any organization's cybersecurity maturity using a non-intrusive, external approach. Extension and weighting of information provided by traditional third-party risk assessment methods.

COMPLIANCE

Monitoring of corporate and third-party legal compliance based on objective data taken in real time.
ISO 27001. PCI - DSS. ENS. RGPD.
Justification of compliance with legal and regulatory requirements for associations, mergers and acquisitions, audits, certifications and contracts with the administration

CYBERSECURITY SCORING

It allows security information to leave the CISO's office and be presented in a simple way to people who need to be involved in security management without having a technical background.
Own and third-party cybersecurity scoring for partnerships, audits, mergers, acquisitions and government contracts.

Analysis of 9 Threat Categories

- **DNS**
- **Health/Phishing**
- **Patch Management**
- **IP Reputation**
- **Web Security**
- **Email Security**
- **Document Leaks**
- **Credential Leaks**
- **Social Networks**

ENTHEC

WHITEPAPER

kartos©

- **AI layer** that enables 100% automated operation without human intervention anywhere in the process.
- **Strictly non-intrusive tool.** The research is carried out on the Internet, the Deep Web, and the DarkWeb, and the organizations' IT perimeter is not attacked, so its operation and the information obtained strictly comply with the imposed limits. by legislation.
- The only platform that analyzes **conversations on social networks from the threat and attack detection perspective,** beyond the relating to reputation and branding.
- **Continuous operation 365x24x7,** allowing detection of leaks of new information practically in real time. real time.
- **Maximum ease of use.** Does not require no complex configuration. Simply enter the domain into the platform and it works autonomously, without the need to configure search parameters or any other information location criteria.
- Automated, objective and continuous monitoring of the risks caused by **third parties belonging to the External Attack Surface of the organization.**

Learn more about our licenses
Try our tool for free
Start using Kartos

→ hello@enthec.com

Enthec Solutions is a Spanish technology company that develops cybersecurity software for the protection of organizations and people. Enthec Solutions has established itself as one of the Deep Tech companies with the most innovative and effective Cyber surveillance solutions thanks to the success of its **Kartos Corporate Threat Watchbots** platform, which provides organizations with Cyber Security, Cyber Intelligence, Cyberscoring, Compliance and Third-Party Risk Management Capabilities, and its innovative **Qondar Personal Threat Watchbots** platform for the individual online protection of the organization's relevant people.

www.enthec.com