ENTHEC

WHITEPAPER

CYBER THREAT INTELLIGENCE

AI extends the reach of Cybersecurity

TABLE OF CONTENT

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 beginning and the attacks were unsophisticated. In that scenario, the strategic approach of protecting the internal perimeter of organizations through their shielding and managing risk was the most effective, affordable and rational. There was no need to go any further.

However, time has passed and the speed of technological innovation and its impact on markets have injected complexity both in corporate IT systems and in relations between organizations and have allowed the sophistication of the attacks of the cybercrime.

Cloud operation, third-party entry into internal systems, the connection between own systems and third parties and the use of the latest technologies by cybercriminals today render ineffective the strategic approach limited to the internal perimeter and risk management, mainly by two factors:

- The low efficiency of its results, as evidenced by the number of successful cyber attacks that grows unstoppable every year and the improvement of social engineering techniques.

- The resource cost of shielding systems and managing increasingly complex and expanding risks

Despite this manifest inefficiency, the inside-out approach to cybersecurity remains the basis of most corporate cybersecurity strategies, causing corporate cybersecurity policies to enter into a cost-driven dynamic, its poor performance and the board's resistance to new investments in cybersecurity, which squarely affects the work of CISO. Although cybersecurity is now a business risk issue, directly affecting the survival and sustainability of the business*, CISOS still has to fight for resource allocation.

INTRODUCTION

Changing this approach, expanding the controlled perimeter and using new technologies such as AI to lower costs is the evolution that cybersecurity strategies need to overcome this loop and reduce the success figures of cyberattacks.

The organizations are no longer isolated small tribes that can defend themselves from attacks they do not know by entrenching themselves behind a wall. Today, organizations are complex entities with extended perimeters that are difficult to delineate, which need, in addition to defense and protection strategies, intelligence strategies that allow them to manage, along with risk, exposure to threats, tools capable of infiltrating the territory where the enemy operates to obtain information about their tactics and resources. Following a mantra recorded 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 the strategies of perimeter cybersecurity and extended cybersecurity, the traditional inside-out approach to the emerging outside-approachin and how AI is one of the determinants of the success of the new paradigm in cybersecurity: cyber threat intelligence.

PERIMETER CYBERSECURITY: RISK MANAGEMENT

The strategy of perimeter cybersecurity 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 performed periodically to check the effectiveness of the shield 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, the perimeter cybersecurity strategy can be sufficient and cost the organization affordable resources.

But, if it ever existed, that simple environment has disappeared today and will not return.
Organizations and their management bodies must be aware that the digital environment in which their businesses today operate is complex and will not cease to be so, and that's why cybersecurity strategies based on hypotheses that consider it will never work again.

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

CIBERSEGURIDAD PERIMETRAL: LA GESTIÓN DEL RIESGO

- Cybercrime has achieved a high level of sophistication and success through 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 constituting the main attacks executed.
Data from the Spanish Data Protection Agency (AEDP).

- Much of the solutions, operations and information of organizations are hosted in clouds and third-party applications.

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

- Third parties such as partners, suppliers and collaborators often have input into 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 armored and secure does not even reach the resources and weapons that are kept in stores of other tribes, because in ours no longer fit, neither to the keys of the wall with which they count inhabitants of other tribes that collaborate with ours nor to the enemies disguised with our uniforms that they get under cover the password to open our doors.

Cybercriminals now have the ability to enter with the same means that an employee or third party enters the organization. What capacity does perimeter cybersecurity have to prevent this type of offensive?

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

Risk management works on hypotheses.

The calculation of the risks that serve to size and design the strategy of perimeter cybersecurity is based on the quantification of all possible risks and threats, including those that occurred and known and those that are imagined to be likely to occur. This is the first series of hypotheses that affect the result: that of probability. The second involves all those attacks that are not even known, but that have to enter the calculation, to count on the unforeseen.

In this way, perimeter cybersecurity strategies tend to handle weak data, sometimes deformed by analyst bias and upward trend to cover cyberprotection against an unknown number of risks with an unknown degree of threat.

LIMITATIONS OF PERIMETER CYBERSECURITY

Third-Party Risk

Perimeter cybersecurity has little effectiveness against third-party risk. A failure in the security of the third party causes the cyberattack offensive to take place undetected. In addition, third-party risk management is carried out by checking compliance with a number of requirements through questionnaires and the results of spot intrusion tests, as a fixed photo. Some checks and tests that cannot reach the fourth or nth (third parties of the third parties of the organization).

The current 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 of any strategy of protection and defense is the capacity of the enemy. In cybersecurity this factor translates into an adversary who uses techniques in permanent innovation and who has the human factor playing in his favor. Cybercrime quickly and effectively incorporates any technological innovation. New technologies such as AI and Machine Learning are already used to obtain the information that serves to open the way for a cyberattack. The ability to create deep fakes directly impacts the vulnerability of the human factor, the weakest link in any cybersecurity strategy. And the ability of organizations to track and analyze information improves this capacity, against which perimeter cybersecurity has very few defenses.

LIMITATIONS OF PERIMETER CYBERSECURITY

The cost of perimeter shielding.

The cost of resources to maintain the effective and up-to-date shielding on which the perimeter cybersecurity strategy is based is unaffordable for any organization, as it is calculated on assumptions that overestimate risks and threat levels so as not to fail and, In addition, they have to reach a corporate IT system in permanent growth, which implies that that cost store to infinity. This causes cybersecurity to end up being conceived within the management as an expense that slows the growth of the business and not as an investment in it.

Incorrect assessment of the business impact of the risk.

The consequence of risk management working on assumptions is that the business impact assessment of risk also does. For them, the assessment of the business impact of risk suffers from the same problems as the evaluation of the same through hypotheses: work with weak data, sometimes deformed by the analyst's bias and trending upwards to cover cyber protection against an indefinite number of impacts of an undetermined size. This, in addition to the natural overestimation of impacts to cover their backs, causes the rest of the departments and management to be very little involved in the evaluation itself and the results of the assessment contain greater inaccuracy.

> The lack of data means that we cannot validate a risk estimate or review the historical accuracy of previous risk estimates. Formalized risk assessment and quantification processes encode misconceptions about threats, vulnerabilities and links between infrastructure and business processes.
> Maverick Research: Risk management produces bad cybersecurity. Gartner 2023

All these limits make the strategy of perimeter cybersecurity end up creating a dynamic that impacts fully in the work of the CISO:

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 capable of being efficient and affordable regardless of such complexity and variations. The strategy of perimeter cybersecurity, or inside-out approach to cyberprotection, 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 as a basis for designing the 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 cybersecurity of an evolved level capable of providing the answers in efficiency and costs that the current environment needs.

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

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

EXTENDED CYBERSECURITY: MANAGING EXPOSURE TO THREATS

Go outside the organization's perimeter to learn about the corporate information cybercriminals have, what security breaches they are exploiting and what tactics are associated with a vulnerability they can use, That is, managing exposure to threats through cyberintelligence, allows the organization's response to be prior to the attack, fast, accurate, effective and without involving a high cost of resources. An extended cyberintelligence strategy that manages exposure to threats from internal causes, as well as exposure to threats from third parties.

> Maverick's strategic planning assumption: By 2030, boards will rely on threat exposure data summarized by AI to prioritize investments, rather than cybersecurity risk assessments, compared to less than 1% by 2023.
> Maverick Research: Risk management produces bad 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 cyberintelligence is to monitor and track 24x7 the outside perimeter of the organization where cybercriminals move to locate and define internal and third-party risks and transfer information in real time to the security department or the corresponding MSSP.

Although in the early stages of cybersecurity, this capacity was beyond the reach of organizations, the emergence of new technologies such as AI and Machine Learning have allowed the emergence of automated solutions capable of tracking the Web, the Deep Web and the Dark Web in the same way as cybercriminals do. Extended cyberintelligence allows organizations to stay ahead of cybercriminals, since automated and continuous surveillance allows threats to be located and defined at the time of emergence and thus neutralized before a cybercriminal has had time to plan how to use them.

CYBER THREAT INTELLIGENCE: LOCATION AND DEFINITION OF RISK

Exposure over time to a threat increases its dangerousness exponentially.

When an organization has the ability to locate the threat and define the associated risk just at the time the vulnerability is created, has the ability to anticipate the cybercriminal who has also located the same threat and is ready to use it to execute an attack. AI allows organizations to have the capacity to classify threats by categories and to know the most effective actions to eliminate them, all if human intervention.

Following the simile of our tribe, the extended cyberintelligence would be to have an army of spies collecting and continuously transferring information from the enemy's terrain.

If cybercrime has become more effective without increasing costs through the use of new technologies, cybersecurity has no choice but to evolve equally to deal with it.

CYBER THREAT INTELLIGENCE: BUSINESS IMPACT ASSESSMENT

The calculation of the business impact is essential for the optimization of the resources dedicated to cyberprotection.

When an organization's cybersecurity strategy is limited to shielding the perimeter, the assessment of the business impact of risks is made based on the assumptions used to calculate the risks. The involvement of the other departments of the organization and management in the calculation of the business impact is small, since it is difficult to work on the basis of those assumptions outside the cybersecurity environment. In addition, as we have already pointed out, the hypotheses always have the analyst's bias 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.

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.

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

These parts of the network are used by cybercriminals to carry out illegal activities, such as the exchange of leaked information, the sale of stolen data, the spread of malware and other cybercrimes.

AI plays an essential role in the main activity of cyber threat intelligence: monitoring and detecting threats in the visible layer 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, 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 competent authorities to take proactive measures to protect data, to close security breaches and prevent the corporate impact of cyberattack. This includes notifying affected departments, strengthening 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 derived 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 limit that the perimeter of organizations set to cybersecurity strategies. Complemented by other technological innovations such as automation and machine learning, have turned cyber threat intelligence into an evolved cybersecurity strategy that gains in effectiveness reduces resource costs and is capable of hindering next-generation cyber attacks.

CYBER THREAT INTELLIGENCE + AI

Location of vulnerabilities in real-time

Definition of risk

Business impact analysis

Definition and proposal of actions

ADVANTAGES OF CYBER THREAT INTELLIGENCE AND THE OUTSIDE-IN APPROACH

- Work on specific data and not on hypotheses or biases.
- Location of vulnerabilities in real-time.
- Rationalization of the use of resources in cybersecurity.
- Involvement of management and other departments in the cybersecurity strategy.
- Use of AI to locate and define risks.
- Use of 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 of cyber intelligence tools.
- Automation, monitoring, location of information and risk analysis without human intervention.
- Location and definition of risk of third parties and nths.
- 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.
- It provides valuable data to design intrusion tests on the internal shielding and make them more effective.

External Attack Surface Management (EASM) provides valuable risk context and actionable information 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©

XTI watchbots

Kartos XTI Watchbots: EASM + DRPS + SRS on a single platform

Kartos XTI Watchbots is the Cyber-surveillance platform developed by Enthec Solutions to extend the security perimeter controlled by organizations and institutions. Conceived from a hacker strategy approach, Kartos is in an ongoing R&D process to incorporate categories and capabilities ahead of the evolution of cyberattacks.

External Attack Surface Manageme

Detection of corporate assets and information about systems, cloud services, and applications that are available and visible in the public domain to any cybercriminal.

Digital Risk Protection Services

Detection of contextual information about possible attack agents, their tactics and processes to carry out malicious activities, and removal of malicious activities on behalf of the organization.

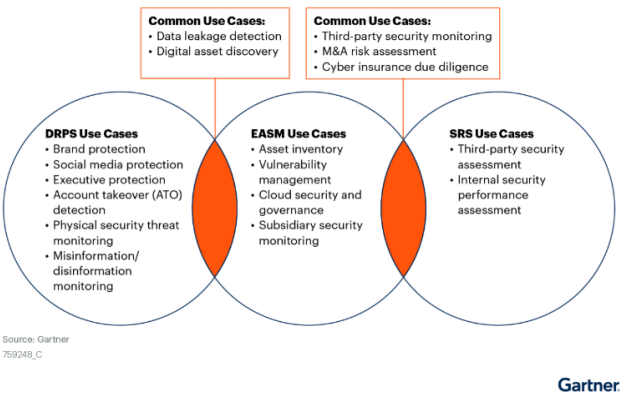
Security Rating Services

Independent risk assessment of own and third parties for a broad visualization of the maturity in cybersecurity of any organization using an external approach. Extension and weighting of information provided by third-party risk assessment traditional methods.

Analysis of 9 threat categories

- Network
- DNS Health / Phishing
- Patch Management
- IP Reputation
- Web Security
- Email Security
- Document Filtering
- Credential Filtering
- Social Networking

The Common Use Cases Supported by DRPS, EASM and SRS



WHITEPAPER

kartos©

XTI watchbots

- **AI layer** that allows operation 100% automated without intervention in any part of the process.
- **Continuous operation 365x24x7**, allowing you to detect new information leaks practically in real time.
- **Strictly non-intrusive tool.** The research is conducted on the Internet, the Deep Web and DarkWeb, and does not attack the IT perimeter of companies, so their operation and the information obtained strictly comply with the limits imposed by the legislation.
- **Maximum ease of use.** No complex configuration is required. Simply enter the domain in the platform and it works autonomously without configuring search parameters or other criteria for locating information.
- The only platform that analyzes **conversations on social networks from the perspective of detecting threats and attacks** beyond that relating to reputation and branding.
- **Automated, objective, and continuous monitoring** of risks caused by third-parties belonging to the Company´s External Attack Surface.

Learn more about our licenses
Try the XTI Cyber-surveillance for free
Start using Kartos

→ hello@enthec.com

Enthec is a Deep Tech that develops and manufactures cybersecurity software with a hacker approach to extend the reach of cyber-protection strategies of organizations.

Founded as a startup in 2019 by María Rojo, Enthec has grown through funding rounds and the success of its Kartos platform to consolidate itself as one of the Deep Tech with more innovative and effective solutions in the field of Cybersecurity.

To learn more about us, you can visit our website:

www.enthec.com