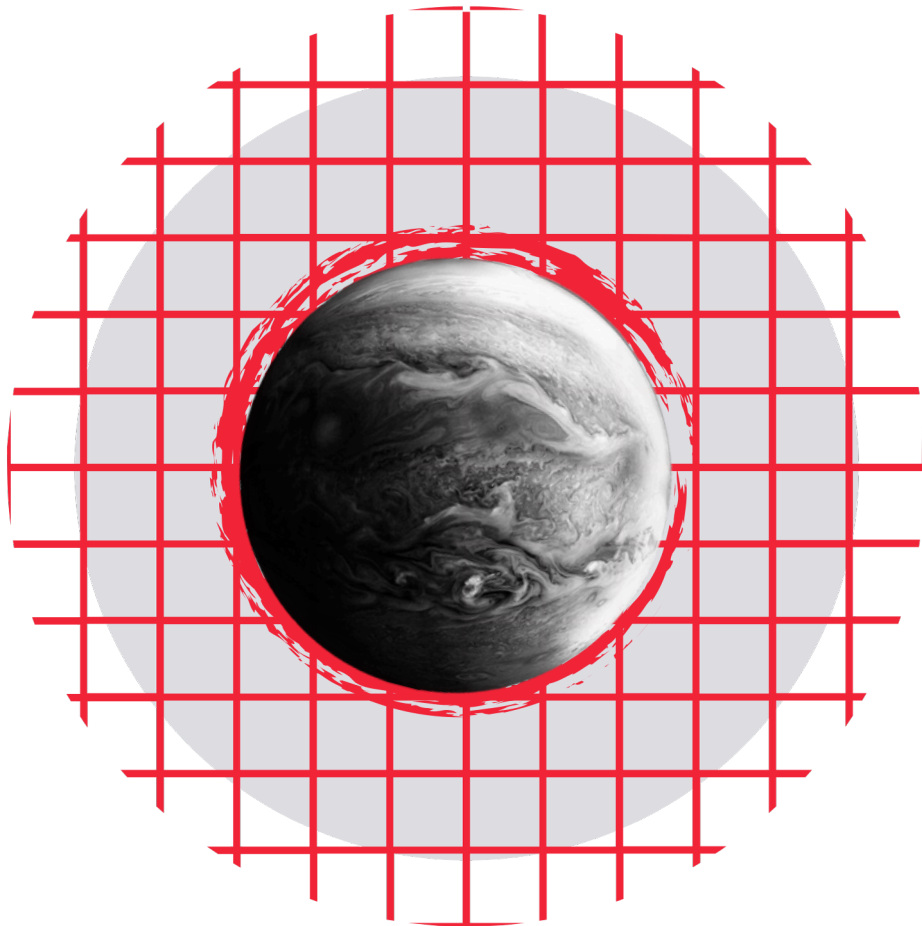


# **EXTENDED CYBERSECURITY:**

**When strategy builds the  
concept**



# INDEX

Introduction	02
Factors that influence corporate cybersecurity	03
Scope factor	04
Involvement factor	05
Resource factor	06
Extended Cybersecurity: Managing Threat Exposure	07
Advantages of the CTEM strategy for the CISO	08
CTEM Cybervigilance: Extended Cybersecurity	09

## INTRODUCTION



The CISO, Chief Information Security Officer, is responsible for leading the information security strategy in an organization, ensuring the protection of its critical assets and the mitigation of risks related to cybersecurity.

In theory, this leadership does not imply that corporate cybersecurity is solely their responsibility. However, in practice, the CISO faces a series of challenges that hinder their ability to effectively protect the organization and that have to do with factors complementary to their activity, such as the scope of the strategy, the lack of involvement of the rest of the organization and the corporate resources allocated to the design of an effective cybersecurity strategy. Challenges that are the result of a mistaken concept of corporate cybersecurity that causes it to be perceived within the organization as an activity restricted to the internal system, that is the exclusive responsibility of the CISO and that represents an expense for the organization that is separate from its main activity, instead of being considered an investment, despite being crucial for the sustainability of the business in the short, medium and long term.

In this document we will analyze the consequences of this misconception and how to change it using our own corporate cybersecurity strategy based on innovative cybersecurity solutions.

# FACTORS THAT CONDITION CORPORATE CYBERSECURITY

A correct concept of what corporate cybersecurity is, what it means and what it entails is essential not only to design an effective strategy, but also for the CISO to be able to effectively exercise leadership within the organization.

Organizations often perceive cybersecurity as the activity of protecting the internal system, a responsibility that is only the responsibility of the CISO and an expense that is subject to constant review because it is not part of the core business activity and because until a successful attack is suffered, potential threats are confused with scaremongering.

**Scope, involvement and resources are factors whose perception must be adequate in order to accurately design the cybersecurity strategy that the organization needs:**

## RANGE

### Field of view amplitude

Cybersecurity not only affects the internal perimeter of an organization, but extends to the external perimeter, including the web, deep web and dark web, where information is exposed. corporate vulnerabilities to be used by cybercriminals, and the organization's third parties, whose vulnerabilities pose a risk of complicated control.

## IMPLICATION

### Being the one who leads does not mean being the only one responsible

The CISO is responsible for leading, designing, implementing and directing the corporate cybersecurity strategy, but the responsibility for adopting and following it is the responsibility of each and every member of the organization, starting with the rest of the CXOs with areas that may be affected by the risks.

## RESOURCES

### Protecting yourself intelligently is an investment

Dedicating the necessary resources to cybersecurity is an investment in the viability of the business, but it is essential that this investment does not become a burden on their growth. Therefore, both the cybersecurity strategy and the solutions to execute it must be intelligent and innovative to protect as effectively as possible without compromising corporate, professional and economic resources.

# SCOPE FACTOR

WHITEPAPER

One of the main challenges facing CISOs is the scope of their security strategy.

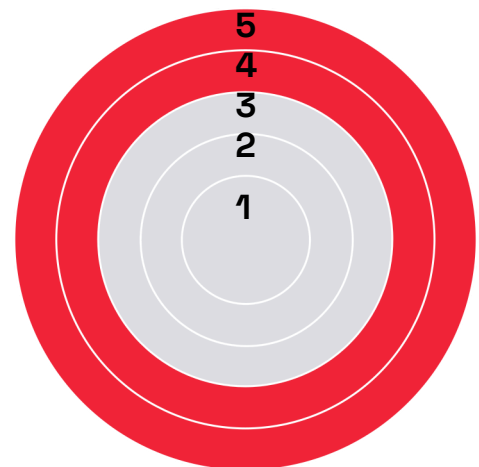
In the past, CISOs focused primarily on protecting the internal perimeter of the organization, i.e. the network and IT systems, and this is the concept of cybersecurity that has become fixed in most organizations.

However, with the proliferation of mobile devices, the adoption of the cloud, the need for collaboration with third parties, and the existence of a market where cybercriminals leak and expose organizations' information, the boundaries of the corporate security perimeter have expanded and become more blurred. Organizations must now consider the risks associated with managing third parties and vendors, the risks associated with employees using personal devices and cloud applications to perform their tasks, and the vulnerabilities posed by security breaches and leaked and exposed corporate information.

## Attack surface

1. Corporate internal perimeter
2. Remote devices
3. Cloud
4. Third parties
5. Web, Deep Web y Dark Web

- Internal to the organization
- External to the organization



*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.*

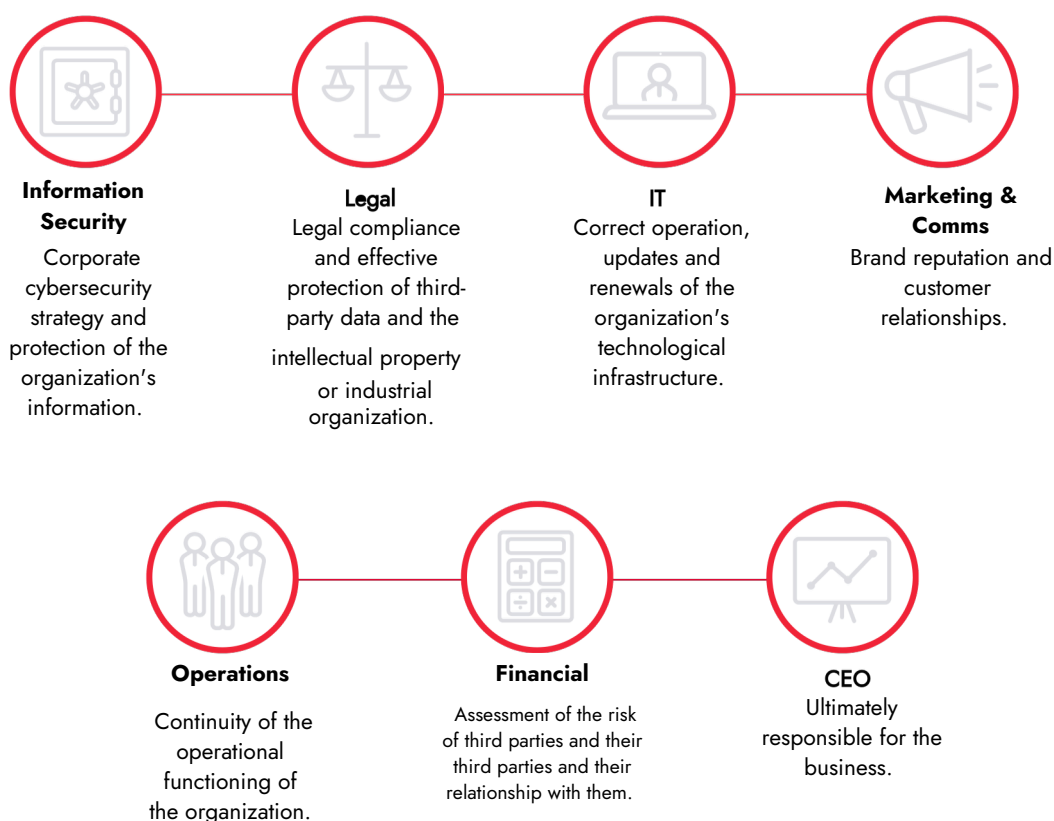
Gartner, Peer Insights

# FACTOR INVOLVEMENT

WHITEPAPER

Another challenge CISOs face is the lack of involvement from the rest of the organization in the information security strategy. Information security is often considered the sole responsibility of the IT department or the CISO.

However, information security is also the direct responsibility of all board members. CISOs must ensure that the rest of the board members participate, assume and take responsibility for the development of the cybersecurity strategy and for promoting a cybersecurity culture among the professionals under their charge, in addition to including it in decision-making and the establishment of objectives.



*The perception of Spanish CISOs of a lack of alignment with their boards of directors has increased, as only 17% of Spanish CISOs say they strongly agree with the statement that their board of directors agrees with them on cybersecurity issues.*

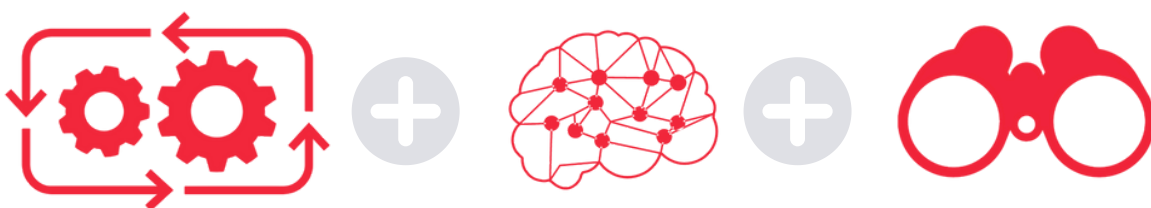
Informe Voice of the CISO 2022

## RESOURCES FACTOR

WHITEPAPER

The resources available for the information security strategy are limited and are an item outside the business offering. In contrast, traditional cybersecurity solutions are expensive in terms of implementation and, just as importantly, maintenance and updating. This leads to a tendency to limit the resources dedicated to cybersecurity and to the CISO having to fight at every moment for each item dedicated to the cybersecurity strategy. The consequence is too often minimal protection and therefore ineffective against major threats.

Therefore, the current obligations of the CISO include designing strategies and finding the most effective cybersecurity solutions that least compromise corporate resources, both human and material. Part of this objective is usually met by choosing to transfer the management of corporate security to a third party, through a Managed Security Service. But whether you choose in-house cybersecurity or one managed by a third party, the key is to use solutions that serve to eliminate threats before they materialize and whose implementation, maintenance and updates do not entail an unaffordable expense in the short and medium term thanks to the introduction of new technologies, such as automation or AI.



*By 2026, more than 60% of threat detection and incident response capabilities will leverage exposure management data to validate and prioritize detected risks, up from 5% today. As organizational attack surfaces expand through increased connectivity, the use of software as a service (SaaS), and cloud applications, enterprises require a broad range of visibility and a central location to constantly monitor threats and exposure.*

Gartner, Security and Risk Management Summit 2023

# EXTENDED CYBERSECURITY: MANAGING THREAT EXPOSURE

Continuous Threat Exposure Management (CTEM) is a cybersecurity strategy based on continuous monitoring and analysis of the Web, Deep Web and Dark Web to detect in real time leaked and exposed information from organizations and the security breaches that have led to said leak. In this way, an organization can know in real time what corporate information is available to any cybercriminal in order to control and neutralize their attack capacity.

## Scope

CTEM Cyber Surveillance allows the organization and the CISO to reach the corporate external perimeter and know and control security vulnerabilities beyond the internal perimeter and the cybersecurity level of third parties related to the organization.



## Involvement

Continuous real-time monitoring allows vulnerability alarms to be issued and assigned to the different managers and professionals in the departments potentially affected by the threat. In this way, they gain information about the risk at the same time as the CISO.



## Resources

Continuously and in real time, knowing the corporate vulnerabilities that are accessible to anyone considerably reduces the costs of protection, minimization and remediation resources.

Management of Exposure to Threats from the organization itself and from related third parties, through solutions with the capacity to issue personalized alerts for vulnerabilities to different members of the organization and reports adapted to different levels of knowledge in cybersecurity, allows the CISO to implement the concept of Extended Cybersecurity in the organization through the strategy.



# ADVANTAGES OF CTEM STRATEGY FOR THE CISO

WHITEPAPER

1

## Proactive protection against internal and external threats

Continuous monitoring provides the CISO with a broader view of cyber risks that threaten the organization, both inside and outside the corporate perimeter.

2

## Identification and management of digital risks

The DRPS capability enables CISOs to identify digital risks associated with the organization's brand, reputation, intellectual property, and other important digital assets.

3

## Improving corporate cyber resilience

Threat Exposure Management with EASM, DRPS and SRS capabilities enables the CISO to detect, respond to and minimise any threat, improving corporate cyber resilience in the short, medium and long term.

4

## Regulatory compliance

Continuous Threat Exposure Management enables an organization to comply with information security rules and regulations and to prove compliance.







5

## Data-driven decision making

The Continuous Threat Exposure Management capability enables the CISO to gain a clear view of the security posture of the organization as well as any third parties connected to it.

# CYBERSURVEILLANCE CTEM: EXTENDED CYBERSECURITY



-  Cyber surveillance that reaches beyond the corporate perimeter, including third parties capable of posing a risk to corporate cybersecurity.
-  Cyber surveillance that issues alerts about configurable and customizable vulnerabilities so that they reach, in addition to the CISO, the affected managers and departments who must take measures to correct them or neutralize their effects.
-  Cyber surveillance that optimizes and rationalizes the resources dedicated to remediation and damage minimization in corporate cybersecurity.
-  Automated 24X7 cyber surveillance with real-time alerts on vulnerabilities associated with the monitored domain.
-  Cyber surveillance that provides information on the state of corporate cybersecurity adapted to the level of technical knowledge of each recipient.
-  Cyber surveillance that allows you to keep under control the vulnerabilities associated with the organization's leaked and exposed information on the Web, Dark Web and Deep Web.



## 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

Enables security information to leave the CISO's office and be easily presented to people who need to be involved in security management without technical training. Own and third-party cybersecurity scoring for partnerships, audits, mergers, acquisitions, and government contracts.

### Analysis of 9 threat categories

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



# kartos<sup>®</sup>



**AI layer** that enables 100% automated operation without human intervention anywhere of the process.



**Continuous operation 365x24x7**, allowing detection of leaks of new information practically in real time.



**Strictly non-intrusive tool.**

The research is carried out on the Internet, the Deep Web and the DarkWeb and the IT perimeter of the organizations is not attacked, so its operation and the information obtained strictly comply with the imposed limits by legislation.



**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.



The only platform that **analyzes conversations on social networks from the threat and attack detection perspective**, beyond the relating to reputation and branding.



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 and extend your corporate cybersecurity strategy.



[hello@enthec.com](mailto: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 **Gondar Personal Threat Watchbots** platform for the individual online protection of the organization's relevant people.

[www.enthec.com](http://www.enthec.com)