ENTHEC®

WHITEPAPER

EXTENDED CYBERSECURITY:

When strategy builds the concept

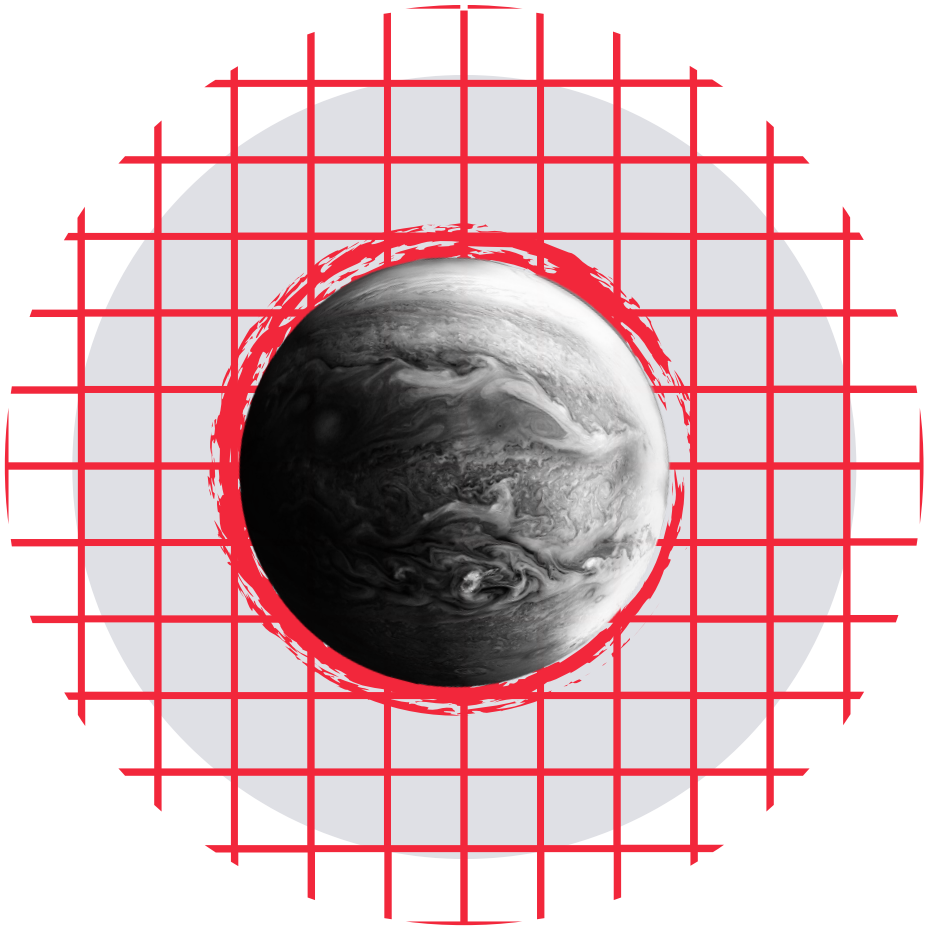


TABLE OF CONTENTS

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 mitigating risks related to cybersecurity.

Theoretically, this leadership does not imply that corporate cybersecurity is only CISO´s responsibility. In practice, however, CISO faces several challenges that hinder its ability to protect the organization effectively and relate to factors complementary to its activity, such as the scope of the strategy, zero involvement of the rest of the organization, and corporate resources for designing an effective cybersecurity strategy. Challenges that are the result of a misconception of corporate cybersecurity that causes it to be perceived within the organization as an activity restricted to the internal system, which is the sole responsibility of the CISO and which represents an expense for the organization detached from its core business, rather than being considered an investment, despite being crucial for the sustainability of the company in the short, medium and long term.

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

FACTORS THAT DETERMINE THE CORPORATE CYBERSECURITY

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

Often, organizations perceive cybersecurity as the activity of shielding the internal system, a responsibility that is only the competence and commitment of the CISO and an expense that can be under constant review because it is not attached to the main business activity and because until a successful attack, potential threats are confused with alarmism.

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

SCOPE

Width field vision

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 corporate vulnerabilities are exposed to be used by cybercriminals, and third parties in the organization, whose vulnerabilities pose a complicated control risk.

INVOLVEMENT

To lead does not mean to be solely responsible.

CISO has the responsibility to lead, design, implement and direct the corporate cybersecurity strategy, but the responsibility to adopt and follow it is the responsibility of every organization member, starting with the rest of the CXO with areas that may be affected by the risks.

RESOURCES

Smart protection is an investment

Dedicating the necessary resources to cybersecurity is to invest in the viability of the business, but this investment must be smooth in its growth. Therefore, the cybersecurity strategy and the solutions must be intelligent and innovative to protect with the most excellent efficiency without compromising corporate, professional, and economic resources.

SCOPE FACTOR

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

In the past, CISOs were mainly focused on protecting the internal perimeter of the organization, that is, the network and computer systems, and this is the concept of cybersecurity that has been fixed in most organizations.

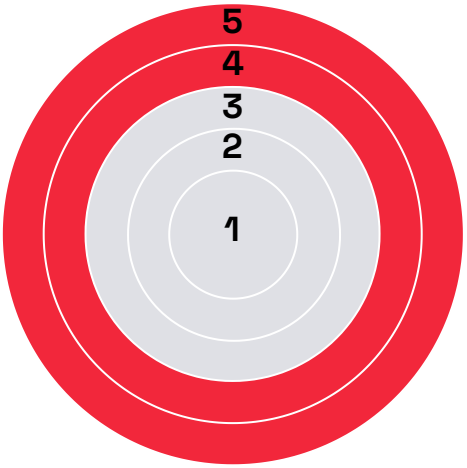
However, with the proliferation of mobile devices, the adoption of the cloud, the necessary collaboration with third parties, and the existence of a market where cybercriminals filter and expose organizations' information, the boundaries of the corporate security perimeter have expanded and become more diffuse. As a result, organizations should now consider the risks associated with managing third parties and suppliers, the risks associated with employees using personal devices and cloud applications to perform their tasks, and vulnerabilities represented by security breaches and corporate information filtered and exposed.

Attack Surface

1. Internal perimeter
2. Remote devices
3. Cloud
4. Third-Parties
5. Web, Deep Web and Dark Web

Internal

External



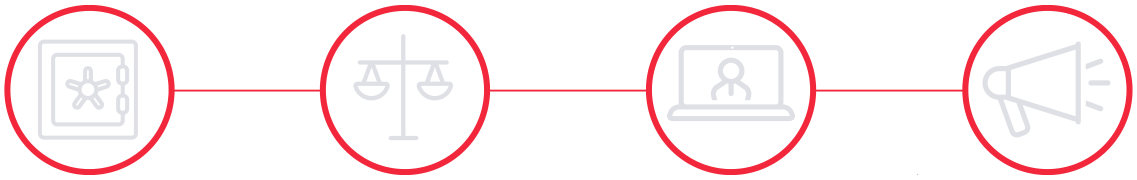
EASM provides valuable risk context and actionable information through: Monitoring continuously for exposed assets and asset discovery for external-facing assets and systems Analysis to assess and prioritize the risks and vulnerabilities discovered External attack surface management is a top priority for security teams and security risk managers.

Gartner, Peer Insights

INVOLVEMENT FACTOR

Another challenge facing the CISOs is the need for more involvement of the rest of the organization in the information security strategy. As a result, information security is often considered the sole responsibility of the TI department or the CISO.

However, information security is also the direct responsibility of the other members of the management in particular. Therefore, CISOs must ensure that the rest of the board members participate, assume and take responsibility for the development of the cybersecurity strategy and foster a cybersecurity culture in the professionals in charge, and include it in decision-making and goal-setting.



Information security: Corporate cybersecurity strategy and protection of the organization's information.

Legal: Legal compliance and effective protection of third party data and the intellectual or industrial property of the organization.

TI: Correct operation, updates and renovations of the technological infrastructure of the organization.

Marketing and Communications: Brand reputation and customer relationship.

Operations: Continuity of the operational functioning of the organization.

.Financial: Assessing the third parties risks and third party relationship.

CEO: Ultimately responsible for the business.

The study also found that when board members are more educated and engaged in the cybersecurity function, they ask tougher questions, dig deeper into issues, and are more likely to make the leap from technical to business issues.

Cybersecurity in the C-suite and Boardroom, ESG 2020

RESOURCES FACTOR

The resources available for the information security strategy are limited and constitute a departure from the business offering. Faced with this, traditional cybersecurity solutions are costly in terms of deployment, maintenance, and upgrade. This leads to a tendency to limit the resources dedicated to cybersecurity and the CISO having to fight at every moment for each item dedicated to a cybersecurity strategy. The result is too often minimal and ineffective protection against significant threats.

Therefore, the current obligations of the CISO are to design strategies and find the most effective cybersecurity solutions and less compromise corporate human and material resources. A part of this objective is usually covered by transferring corporate security management to a third party through a Managed Security Service. But whether you opt for in-house cybersecurity or managed by a third party, the key is to use solutions that serve to eliminate threats before they materialize and whose implementation, maintenance, and upgrades do not represent an unaffordable expense in the short and medium term, thanks to the introduction of new technologies, such as automation or AI.

Through 2026, more than 60% of threat detection, investigation and response (TDIR) capabilities will leverage exposure management data to validate and prioritize detected threats, up from less than 5% today. As organizational attack surfaces expand due to increased connectivity, use of SaaS and cloud applications, companies require a broader range of visibility and a central place to constantly monitor for threats and exposure.

Gartner Security & Risk Management Summit, Sydney 2023

EXTENDED CYBERSECURITY: THE XTI STRATEGY

XTI Cyber-surveillance is a cybersecurity strategy based on continuous monitoring and analyzing the Web, Deep Web, and Dark Web to detect in real-time the leaked and exposed information of the organizations and the security breaches that have led to such a leak. In this way, an organization can know in real time what corporate information is available to any cybercriminal to control and neutralize their ability to attack.

Scope

- Cybersurveillance XTI allows the organization and CISO to reach the corporate external perimeter and to know and control security vulnerabilities beyond the internal perimeter and the level of third-party cybersecurity related to the organization.

Involvement

- Continuous monitoring in real-time allows the issuance of alarms for vulnerabilities and assigns them to the different managers and professionals of the departments potentially affected by this threat. In this way, they have risk information simultaneously as the CISO.

Resources

- Knowing continuously and in real-time the corporate vulnerabilities that are within reach of anyone considerably reduces the costs of protection, minimization, and remediation resources.

A strategy with an outside-inside approach of Cybersurveillance XTI for own and third-party risks, through solutions with capabilities to issue customized alerts for vulnerabilities to different members of the organization and reports adapted to varying levels of knowledge in cybersecurity, allows the CISO to implement the concept of extended cybersecurity in the organization through the strategy.

ADVANTAGES OF THE XTI STRATEGY FOR CISO

1. **Proactive protection against external and internal threats:** XTI Cyber-surveillance provides the CISO with a broader view of the cyber risks threatening the organization, inside and outside the corporate perimeter.

2. **Digital risk identification and management:** The DRPS capability enables CISOs to identify digital risks associated with the organization's brand, reputation, intellectual property, and other critical digital assets.

3. **Improving Corporate Cyber-Resilience:** XTI Cyber-surveillance with EASM, DRPS, and SRS capabilities enables CISO to detect, respond to, and minimize any threat, improving corporate cyber-resilience in the short, medium, and long term.

4. **Compliance:** XTI Cyber-surveillance with EASM, DRPS, and SRS capabilities helps the organization comply with information security and data protection regulations.

5. **Data-driven decision-making:** The SRS capability allows the CISO to gain a clear view of the organization's security position as well as related third parties, including suppliers, partners, and competitors.

CYBER-SURVEILLANCE XTI: EXTEND THE CORPORATE CYBERSECURITY

- Cyber-surveillance that reaches beyond the corporate perimeter, including third parties, with the ability to pose a risk to corporate cybersecurity.
- Cyber-surveillance that issues alerts on configurable and customizable vulnerabilities so that they reach, in addition to the CISO, the affected managers and departments that must take measures to correct them or neutralize their effects.
- Cyber-surveillance that optimizes and rationalizes the allocation of resources dedicated to the remediation and minimization of damages in corporate cybersecurity.
- 24X7 automated 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 degree of technical knowledge of each receiver of the same.
- Cyber-surveillance that allows having under control the vulnerabilities associated with the filtered and exposed information of the organization on the Web, Dark Web, and Deep Web.

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 Management

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.

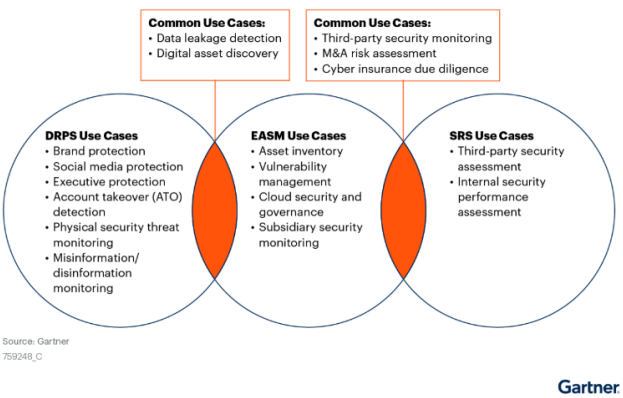
Security Rating Services

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