ENTHEC

WHITEPAPER

THIRD-PARTY RISK:

How to gain accuracy in the assessment

TABLE OF CONTENTS

INTRODUCTION

The digitization of organizations has made the **interconnectivity of systems and the dependence on third parties common in the current business environment**, gaining agility and efficiency. However, this interconnection also leads to increased exposure to cyber risk, forcing organizations to become more aware of the importance of third-party risk management.

Providers, partners, and other third parties with access to an organization's sensitive systems and data **pose a significant risk to the organization's** Cybersecurity. Cybercriminals can use third-party weaknesses to circumvent an organization's Cybersecurity strategy to access sensitive information, steal data, and disrupt business operations. For this reason, organizations must **evaluate and manage the cyber risk of their third parties** effectively and accurately throughout their business relationship, to ensure the security and continuity of operations in an increasingly interconnected environment.

In this **Whitepaper**, we will analyze the importance of assessing the cyber risk of third parties within an organization, the standard methods of evaluating that risk, their deficits, and the benefits of introducing the **XTI approach** in third-party risk assessment as a complement and reinforcement. In addition, we will present some Use Cases to illustrate how organizations can improve their third-party risk management.

HIDDEN INFORMATION AND SCOPE

Organizations often focus on the security of their network and systems but neglect to protect the third-party systems and data they work with. As a result, suppliers, partners, and other third parties may have access to sensitive information, making them a potential risk to the organization's security.

As Gartner points out in its report on the third-party risk assessment model, the leaders of organizations recognize that the connection of their systems with third parties is a fundamental part of the operation of an organization and that the risks continue to grow due to the variability in the maturity of cyber protection of third parties, the increased involvement of those third parties with corporate assets and the increasing connections of those third parties with their third parties.

This essential connection with third parties entails two extreme difficulties when assessing risk: **hidden information and scope**.

HIDDEN INFORMATION

One of the main challenges in managing third-party cyber risks is the **lack of transparency**. Many suppliers and contractors are unwilling to provide complete information about their security practices, either because they do not have the resources to implement adequate security measures or because they do not want to disclose confidential details about their processes.

In addition, it is important to note that in many cases, third parties may also not be completely transparent about cybersecurity incidents not to jeopardize the continuity of agreements or their reputation. This can include concealing security breaches, lack of software updates, or failure to report these security incidents, further increasing the risk to the organization.

Also, organizations may not be aware that certain suppliers and contractors are outsourcing critical services to other third parties without due notice. This can lead to a lack of control over who has access to the organization's systems and data, increasing the risk of cyber attacks.

SCOPE: THE NTH-PARTY

Third-party risk management often overlooks an important aspect: the risk associated with third-party risks, also known as "**nth parties**."

The nth parties are third parties from third parties, those who have access to the systems and data of suppliers and contractors of the original organization. This complex dependency system adds to the difficulty of identifying and managing third-party risks. In addition, the umpteenth parties have their third parties and suppliers, further expanding the supply chain and complicating risk assessment. The original organization has no direct control over the nths, increasing the risk of security vulnerabilities in the supply chain. In addition, nths may be less transparent than direct third parties, which complicates the assessment of associated risks.

Within the risk assessment of third parties, the risk associated with the umpteenth parties begins to be considered by those responsible for cybersecurity as critical for organizations because of their apparent inability not to control it but simply to evaluate it.

THE ORGANIZATION AND THE THIRD PARTY RISKS

It is usually established in all organizations that the risks of third parties are the responsibility of the information security and legal departments. However, the scope of protection and the consequences of third-party risks extend beyond these two departments.

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.

For there to be a precise third-party risk assessment, all these departments of an organization must manage the risk protection responsibilities to third parties and be involved in the evaluation itself, within the parameters that affect their area, led by CISO and the information security department.

IMPORTANCE OF ACCURATELY ASSESSING THIRD PARTY RISKS

An **accurate risk assessment of third parties** is essential to protect the organization's security. Cyber-attacks targeting suppliers, partners, contractors, and other third parties can be very effective in gaining unauthorized access to the organization's systems and data. Therefore, any corporate cybersecurity strategy must provide for the practical assessment of third-party risks.

Third-party risk assessment involves assessing its ability to protect the organization's systems and data. It requires examining security policies and processes, security measures implemented and their effectiveness, regulatory compliance, and other critical factors that may affect the organization's security.

As a starting point, it is necessary to identify and classify the business risks associated with the interdependence of the organization with third parties since this interdependence implies that its vulnerabilities can significantly impact the organization's operations and reputation.

Assessing third-party risks as accurately as possible helps organizations **prioritize risk management and take appropriate preventive measures** in the face of a third-party cyber-attack.

The third-party vulnerability was the fourth attack vector in 2022 data breaches in the Spanish financial and banking sector

Europa Press

73% of organizations say their third parties have more access to data assets than three years ago

Gartner

Organizations recognize dedicating only 27% of resources to identify risks of third parties in the course of the relationship

Gartn

Accurate third-party risk assessment allows organizations to:

Information

- **Before starting a relationship with a third party, make more informed decisions about the selection of suppliers and contractors.** By carefully assessing suppliers and contractors in terms of their ability to protect the organization's security, organizations can make more informed decisions about their procurement and supply chain management. This can help reduce the risk of cyber-attacks and protect the organization's reputation.

Insight

- **Understand the full scope of cybersecurity risks associated with their supply chain** and take appropriate preventive measures to protect yourself. By carefully assessing suppliers and contractors, organizations can identify vulnerabilities and weaknesses in their supply chain and take steps to mitigate risks.

Compliance

- **Comply with safety regulations and standards.** Security regulations, such as different data protection laws, require organizations to implement appropriate security measures to protect their data, systems, and customers. Organizations can ensure that they comply with these regulations and standards by carefully evaluating suppliers and contractors.

Focus

- **Focus on suppliers and contractors who represent the most significant cybersecurity risk.** By prioritizing suppliers and contractors based on their cybersecurity risk, organizations can focus their resources on the most critical areas and reduce the costs and time associated with risk management.

THE COMPLEXITY OF THIRD-PARTY RISK ASSESSMENT

The risk assessment of a third-party begins before the contractual relationship is established and must continue until the collaboration ends and interdependence ends. Common valuation methods are:

Before

Due Diligence

It involves a thorough assessment of the security of suppliers and contractors who have access to the organization's systems and data, including an assessment of the maturity of the vendor's security program, identification of security vulnerabilities in systems, and assessment of the vendor's ability to respond to security incidents. It is usually done through questionnaires prepared by the organization itself.

During

Audits and Offensive Security

It involves the review of security audit reports and risk assessments carried out by the provider, as well as the performance and verification of the results of tests of Offensive Security (pent testing, Red Team...) carried out by the third-party.

DEFICITS

- Manual and objective methods based on questionnaires and tests.
- Mandatory authorization for intrusive testing.
- High testing costs (pen tests and the like).
- Failure to verify the accuracy of the information provided and the absence of hidden information.
- Risk assessment at a given time, without continuous risk monitoring throughout the relationship, including changes in the relationship.
- Outdated information in a few days.
- Inability to assess the risk of nths parts.

Added to these problems, one is paramount and poses a critical risk: limiting the risk assessment of third parties to the internal perimeter of your company. **Protecting the external attack surface** is a growing problem for businesses, as it has so far been impossible to control the level of risk of the extended IT perimeter that includes suppliers, customers, partners, and other third parties. Furthermore, it is proven that these are widely used attack vectors; therefore, any vulnerability in your cybersecurity system can automatically become a gateway for the companies to which it relates.

This complexity **makes the traditional assessment of third-party risk generally inaccurate and unreliable** and, therefore, does not help to design an effective protection strategy against third-party risks.

XTI CYBER SURVEILLANCE APPROACH: CONTROL BEYOND THE INTERNAL PERIMETER

One of the main reasons successful cyberattacks continue to occur in companies is that cybercriminals use leaked and exposed information on the Internet, Deep Web, and Dark Web to avoid defense systems in which companies invest vast resources. **Leaks are a key that unlocks any defense.**

This reality has led to a new approach within organizations' cybersecurity strategy: **XTI cyber surveillance beyond the corporate internal perimeter.**

XTI Cyber-surveillance is a cybersecurity strategy based on **monitoring and analyzing the Web, the Deep Web, and the Dark Web continuously to detect in real-time the leaked and exposed information of the organizations and the security breaches that have led to this 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.

A defense is effective only when all threats, own and third-party generated, are accurately known and when internal and external vulnerabilities are controlled.

XTI CYBER-SURVEILLANCE FOR THIRD-PARTY RISK ASSESSMENT

One of the main capabilities of XTI cyber-surveillance is to be used as a tool of **Security Rating Services (SRS)**: the independent assessment of own and third-party risks for a broad visualization of the maturity in cybersecurity of any organization using an external approach.

The SRS collects on the Web, Deep Web, and Dark Web data through non-intrusive means, analyzes them, and evaluates the security situation of the third-party using a specific scoring methodology. This information provided by XTI cyber-surveillance serves to **expand, complete, and weigh** the information obtained by traditional methods of risk assessment of third parties, such as Due Diligence or Offensive Security, allowing, in addition, the **real-time and continuous evaluation** of such risks for the duration of the collaboration between the organization and the third-party.

ADVANTAGES OF XTI CYBER-SURVEILLANCE IN ASSESSING THE RISK OF THIRD PARTIES

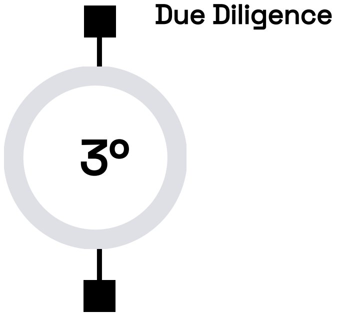
- Objective assessment method that does not require human intervention.
- Non-intrusive method that does not require authorization from the third-party.
- Precise data on the filtration and exposure of third-party information and the security breaches causing the filtration.
- Continuous and real-time monitoring and analysis of third-party risk during the business relationship.
- Control of hidden information.
- Ability to assess the risks of the nth parts.

APPLICATIONS

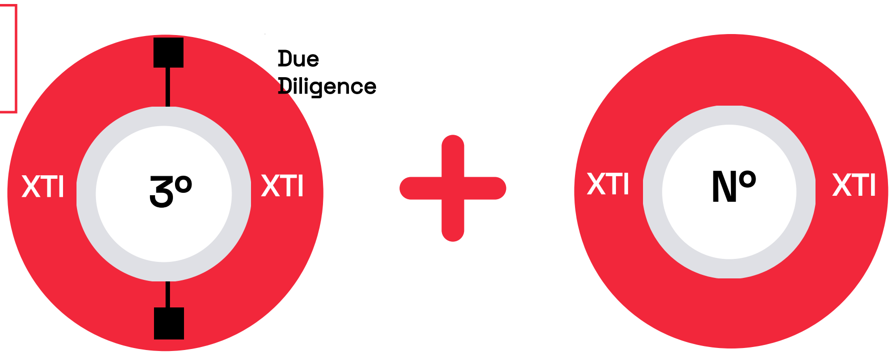
The **XTI approach** can be used for the **assessment of risks of third parties and nth parties** both in a one-off operation (acquisitions, mergers, cyberpolicies...) and in a lasting commercial relationship over time, providing the accuracy and reliability lacking in the most common valuation methods.

TIMELY THIRD-PARTY RISK ASSESSMENT

Without XTI approach



With XTI approach



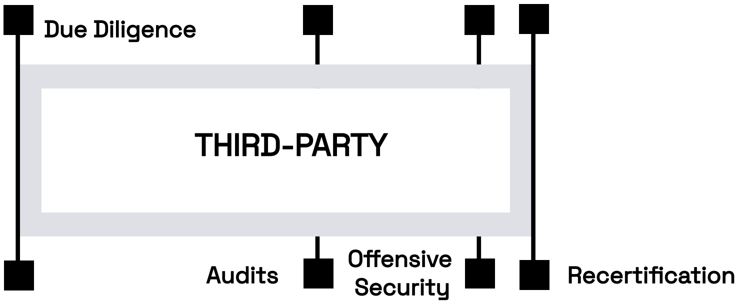
USE CASE

Covering the risk of a Cyberpolicy represents a critical decision for Insurance Companies. Thanks to the XTI approach in assessing the risk of third parties, an Insurance Company obtains a more precise and rigorous assessment of the risk of each Cyberpolicy and the maturity of the cybersecurity strategy of the potential client. At the same time, the Insurance Company can increase its overall offer to its policyholders with the Corporate Cyber Risk Analysis Service.

APPLICATIONS

CONTINUOUS THIRD-PARTY RISK ASSESSMENT

Without XTI approach



Due Diligence

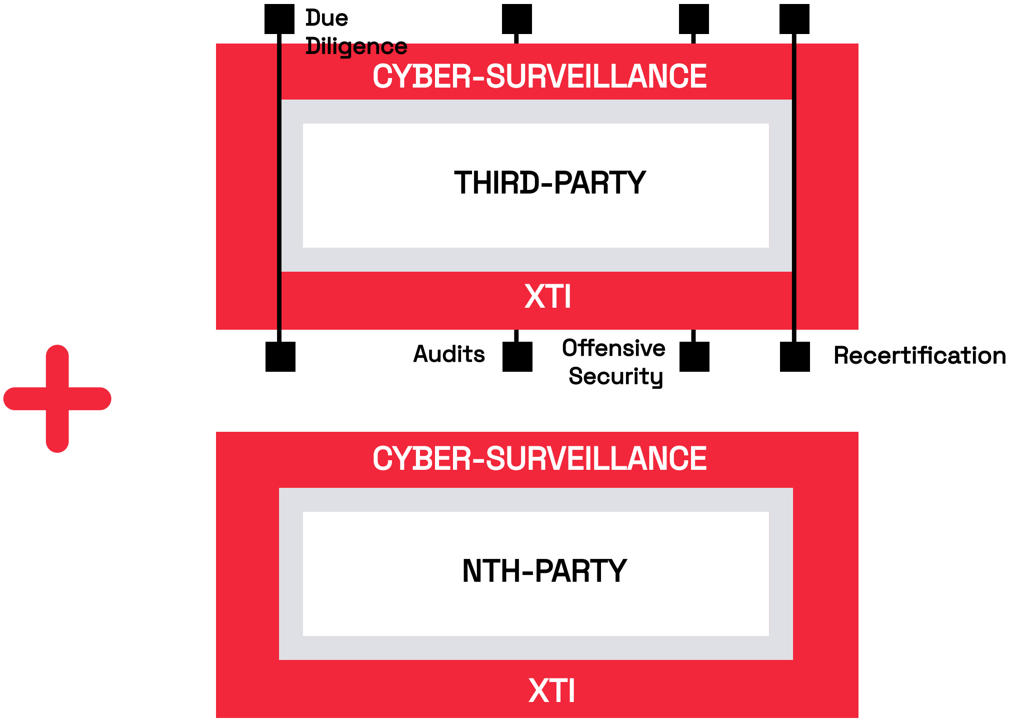
THIRD-PARTY

Audits

Offensive Security

Recertification

With XTI approach



Due Diligence

CYBER-SURVEILLANCE

THIRD-PARTY

XTI

Audits

Offensive Security

Recertification

CYBER-SURVEILLANCE

NTH-PARTY

XTI

USE CASE

Hospital data are regarded as sensitive information, and any leakage, besides posing a threat, carries strong economic sanctions. Thanks to the XTI approach to third-party risk assessment, a hospital monitors the risk of its third-parties and nth continuously and in real-time to control its protection against information leakage.

APPLICATIONS

RISK ASSESSMENT AND MANAGEMENT STRATEGIES FOR THIRD PARTIES WITH AN XTI APPROACH

Previous

Evaluation of potential third parties and nths

- Due Diligence.
- Automated XTI monitoring of the third potential domain during the evaluation time.
- Automated XTI monitoring of critical potential number domains during the evaluation time.
- Assessment of the information obtained:
- Ability to affect the organization.
- Estimated risk remediation time.

Continuous

Evaluation of third parties and nths

- Audits.
- Offensive Security.
- Automated XTI monitoring of the third potential domain during the evaluation time.
- Automated XTI monitoring of critical potential number domains during the evaluation time.
- Assessment of the information obtained:
- Ability to affect the organization.
- Estimated risk remediation time.
- Communication to the third party when the exposure of information detected through XTI Cyber Surveillance affects the organization.

APPLICATIONS

By adding an XTI Cyber-Surveillance strategy to the third-party risk assessment, the organization gains the ability to control, in an automated manner, the information of a third-party or potential third-party and the detection of its security breaches, as well as the critical nths associated with them, are continuously presented in real-time.

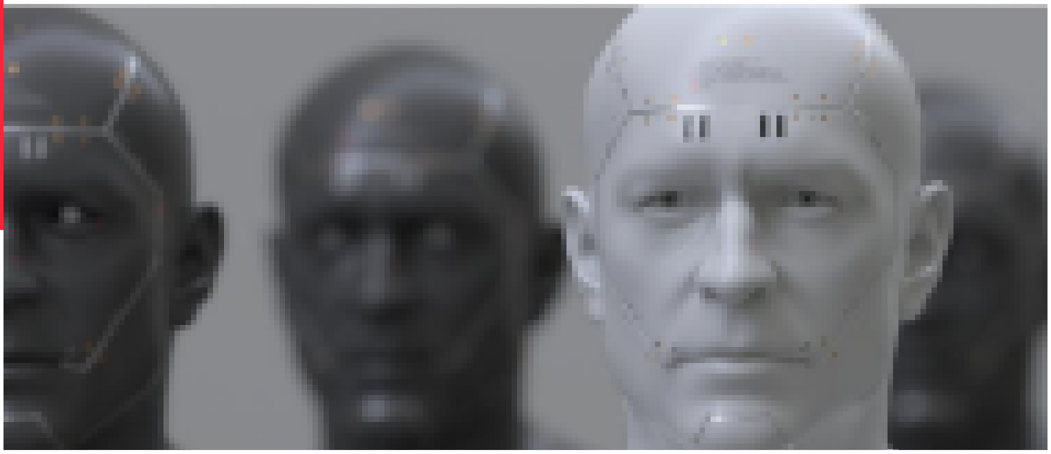
1 More accurate assessment of the risk of potential third parties and evaluation of the maturity of their cybersecurity strategy.

2 More effective risk management of third parties and nths throughout the contractual relationship and continuous evaluation of your cybersecurity strategy.

3 Automated, real-time detection of third-party and nth security breaches and assessment of the degree of risk threat to the organization.

4 Communication to third parties of their security breaches that affect the organization and monitoring of their remediation.

5 Communication to third parties of the risk of nth associated with their organizations and monitoring of their remediation.



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

kartos©

XTI watchbots

Kartos is the Cyber-Intelligence 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.

Analysis of 9 threat categories

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

THIRD-PARTY LICENSES

They take advantage of Kartos's non-intrusive operation to offer organizations the monitoring of the risk level of their value chain. They are designed to be purchased in license packages with different functions so that companies can build the surveillance system that best suits their needs.

Learn more about our Third-Party licenses
Try the Third-Party assessment for free → hello@enthec.com
Start using Kartos

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