Telefónica Tech

Transforming security operations:
Cyber intelligence and the new CTEM approach

FROST & SULLIVAN

Index

01

The growing attack surface: Risk expansion due to IT complexity and third-party vulnerabilities

Digital transformation initiatives such as cloud migration, remote working, and the adoption of the Internet of Things (IoT) have significantly expanded organizations' attack surfaces. Organizations struggle to keep their security operations in line with their digital footprint since IT environments become more complex.

Top Cyber Security challenges for organizations worldwide

Figure 1. Source: *Voice of the Enterprise Security Customer from Frost & Sullivan*

The main Cyber Security challenge for organizations worldwide is precisely the lack of visibility, according to Frost & Sullivan's Voice of the Enterprise Security Customer survey. **The growing volume of digital assets leads to more attack vectors, potential vulnerabilities,** and, in turn, the deployment of more security tools. This flood of information overwhelms organizations, leading to alert overload, false positives, and difficulties in prioritizing vulnerabilities. When security analysts lack the critical context needed to accurately assess risks, the effectiveness and speed of response to security incidents decline.

As a result, t**he frequency of successful attacks continues to rise.** According to data from Frost & Sullivan's global Voice of the Enterprise Security Customer survey, organizations suffer an average of 26 successful cyber attacks (i.e., attacks that result in negative consequences of various kinds) each year.

The rise of artificial intelligence further exacerbates this situation, **enabling cybercriminals to launch increasingly sophisticated and damaging attacks,** which translates into **constant pressure to reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to threats.** While data breaches are becoming more serious, the average cost of a breach is €4.49 million in 2024 (IBM Cost of a Data Breach Report 2024). In addition, the National Cyber Security Institute (INCIBE) also reports that in 2023, more than 83,000 Cyber Security incidents were handled in Spain, an increase of 24% over the previous year. However, hope is not lost. There is a way to transform security operations with intelligence and continue helping organizations effectively improve their security posture.

The starting point is to admit that attackers have evolved to exploit weaknesses in digital assets outside traditional networks, such as shadow IT (unmonitored domains or APIs), cloud configuration errors, and supply chain vulnerabilities.

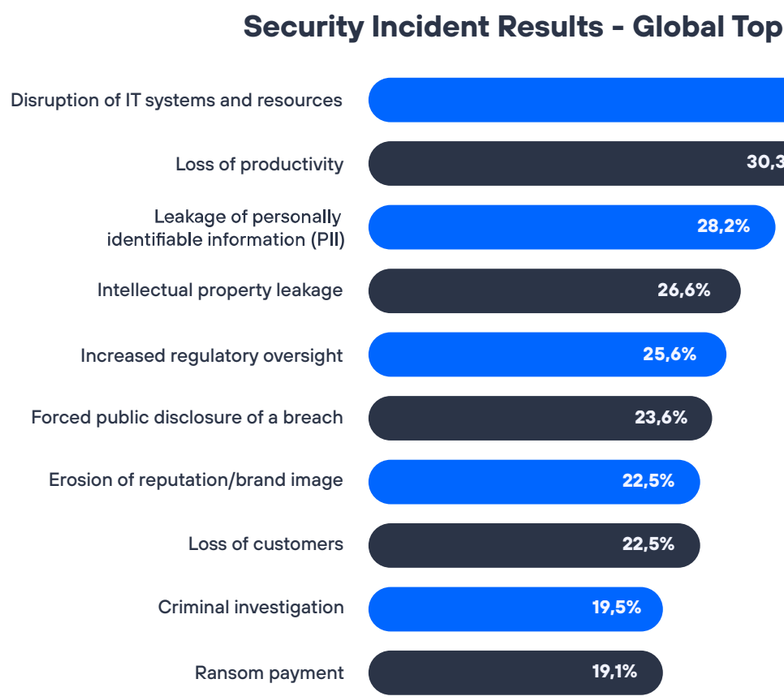


Figure 2. Source: *Voice of the Enterprise Security Customer from Frost & Sullivan survey*

Traditional, reactive security measures are becoming less effective as attacks become more frequent and complex. Organizations that fail to protect their external digital footprint face serious consequences, including operational disruptions, revenue loss, customer churn, and lasting damage to their reputation and brand image (Figure 2).

The State of Security Report 2024 H1 published by Telefónica Tech identifies the main security breaches that occurred in the first half of 2024, including those **affecting companies in important sectors such as energy, banking, insurance, and retail,** among many others, highlighting the serious consequences of data breaches and phishing attacks, especially their impact on customer trust and digital reputation.

In one of the cases analyzed, a financial institution, victim of a large-scale phishing campaign, attackers managed to deceive recipients through fraudulent emails, which led to the disclosure of sensitive credentials. **These credentials gave the attackers unauthorized access to a third-party database containing personally identifiable and confidential information,** such as names, addresses, bank accounts, and social security numbers of approximately 30 million customers and employees in Spain, Chile, and Uruguay. Once stolen, the data was published on the dark web for a sale price of $2 million.

The repercussions were not limited to financial losses, as the breach significantly increased the risk of identity theft and fraud for those affected.

Despite the financial institution's response efforts, the incident raised serious questions about the adequacy of existing security measures and third-party management practices. **This led to an erosion of customer trust and significant damage to the organization's reputation.**

These types of attacks highlight the urgent need to implement proactive security strategies based on cyber intelligence that include the following goals:

- Reduce risks related to shadow IT, incorrect cloud configurations, and exposure of sensitive data.
- Protect brand reputation.
- Minimizing the impact of incidents such as data leaks, identity theft, or exploitable vulnerabilities.

€4.49 million

million is the average cost of a breach in 2024.

Source: IBM Cost of a Data Breach Report 2024

+24% more incidents

to manage compared to 2023.

Source: Instituto Nacional de Ciberseguridad (INCIBE)

02

The Cyber Security paradigm shift: Continuous threat exposure management (CTEM)

The term **Continuous Threat Exposure Management** (CTEM) reflects an evolution in traditional Cyber Security practices, moving from reactive approaches to proactive and dynamic models. CTEM enables organizations to continuously **identify, assess, and mitigate evolving cyber threats, strengthening their resilience** and response capabilities against attacks**.** This approach combines advanced technologies, such as artificial intelligence and automation, with iterative processes that prioritize the most critical risks in real time, enabling organizations to maintain constant monitoring and adapt quickly to new threats. It is particularly relevant for sectors such as finance, healthcare, telecommunications, and energy, where disruptions or security breaches can have serious consequences.

CTEM seeks to provide a clear and up-to-date view of security vulnerabilities, considering both internal and external digital assets, with the aim of maintaining a robust and adaptable Cyber Security posture against constantly evolving threats. In this sense, CTEM is based on a cyclical process consisting of several interrelated phases, which feed back into each other as the program progresses, as can be seen in the chart.

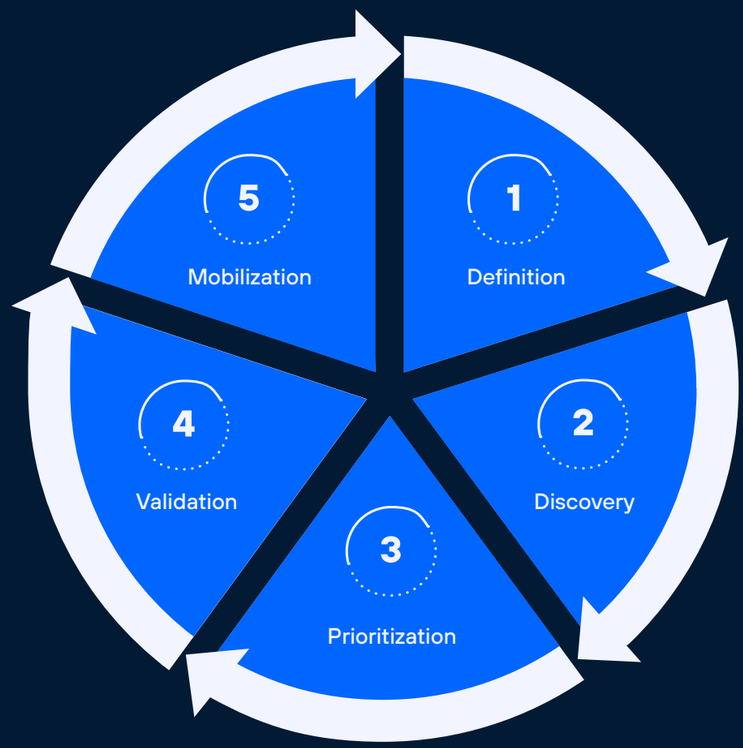
CTEM Program

CTEM is not a tool. It is a process

A five-step program:

- Simultaneous repetitive cycles
- Patchable and non-patchable exposures
- Priority validation
- Mobilize first, remediate later

A cyclical and adaptable process to reduce exposure to threats in this ever-changing world



1 **DEFINITION:** As a first step, organizations must **define their attack surfaces and evaluate the importance of each asset.** This process, which should be ongoing, establishes a framework for exposure assessments, prioritizing business impact over threat severity. It also ensures alignment with organizational goals by clarifying what, why, and how assets will be assessed, fostering collaboration across departments.

2 **DISCOVERY:** After defining the scope, the next step is to identify the assets, vulnerabilities, and threats present in the organization. This is done using tools and methods such as attack surface discovery, vulnerability assessments, and penetration testing. These activities allow you to map and understand the most relevant attack vectors. Threat modeling also plays a key role by providing a structured representation of possible attack scenarios and their consequences. **This approach ensures a detailed understanding of the digital environment and its associated risks.**

3 **PRIORITIZATION:** Once the asset and threat landscape has been identified, it is essential to classify vulnerabilities based on their impact and likelihood of exploitation. Prioritization helps focus Cyber Security analysts' efforts on the most critical issues, thereby maximizing operational efficiency. This approach optimizes incident management and reduces the risks associated with high-impact vulnerabilities. Proper prioritization **ensures that resources are allocated strategically, contributing to more effective protection of the organization's key assets.**

4 **VALIDATION:** This phase involves conducting controlled tests to discover and validate security gaps before they can be exploited by attackers. **Validation confirms whether risks are real, assesses the effectiveness of mitigation techniques,** and ensures that the response is quick and effective. Both manual and automatic methods are used, such as red teaming exercises, penetration testing, and attack simulations, ensuring that the Cyber Security measures are effective and allow for continuous improvements to strengthen security. According to interviews by Frost & Sullivan, a security manager stated that the manual process for testing a web application took approximately two weeks in their organization. Thanks to the implementation of automated vulnerability assessments and penetration testing, in conjunction with active application scanning, web application analysis time was significantly reduced, freeing up the manager to work on other projects.

5 **MOBILIZATION:** In this phase, the necessary resources are deployed to mitigate the identified threats and vulnerabilities. This includes implementing new security controls, improving existing ones, or adapting business processes to reduce exposure. Mobilization is an ongoing effort, as new threats and changes in the digital landscape require constant updates to the CTEM process. **This ensures that the organization remains proactive in risk** management. This increase in efficiency results in a more efficient use of the security budget: according to interviews conducted by Frost & Sullivan, organizations that implement a CTEM program reduce their pentesting costs by an average of 30% thanks to active scanning and automation.

03

CTEM: The key to detecting and protecting critical assets

The definition and discovery phases of a CTEM program are critical, as they clearly establish the program's goals and scope, as well as identify critical assets that require protection.

However, these phases often represent a significant challenge for organizations. Many find it difficult to effectively identify digital assets in hybrid and multicloud environments, especially when these include IoT devices, OT, and third-party systems. This difficulty is further compounded when organizations rely on outdated methods, such as Excel spreadsheets. Manual asset management, which involves tracking web-exposed systems, tagging assets, conducting audits, and collaborating with IT teams, is a labor-intensive, error-prone process that is unsustainable in today's dynamic environments.

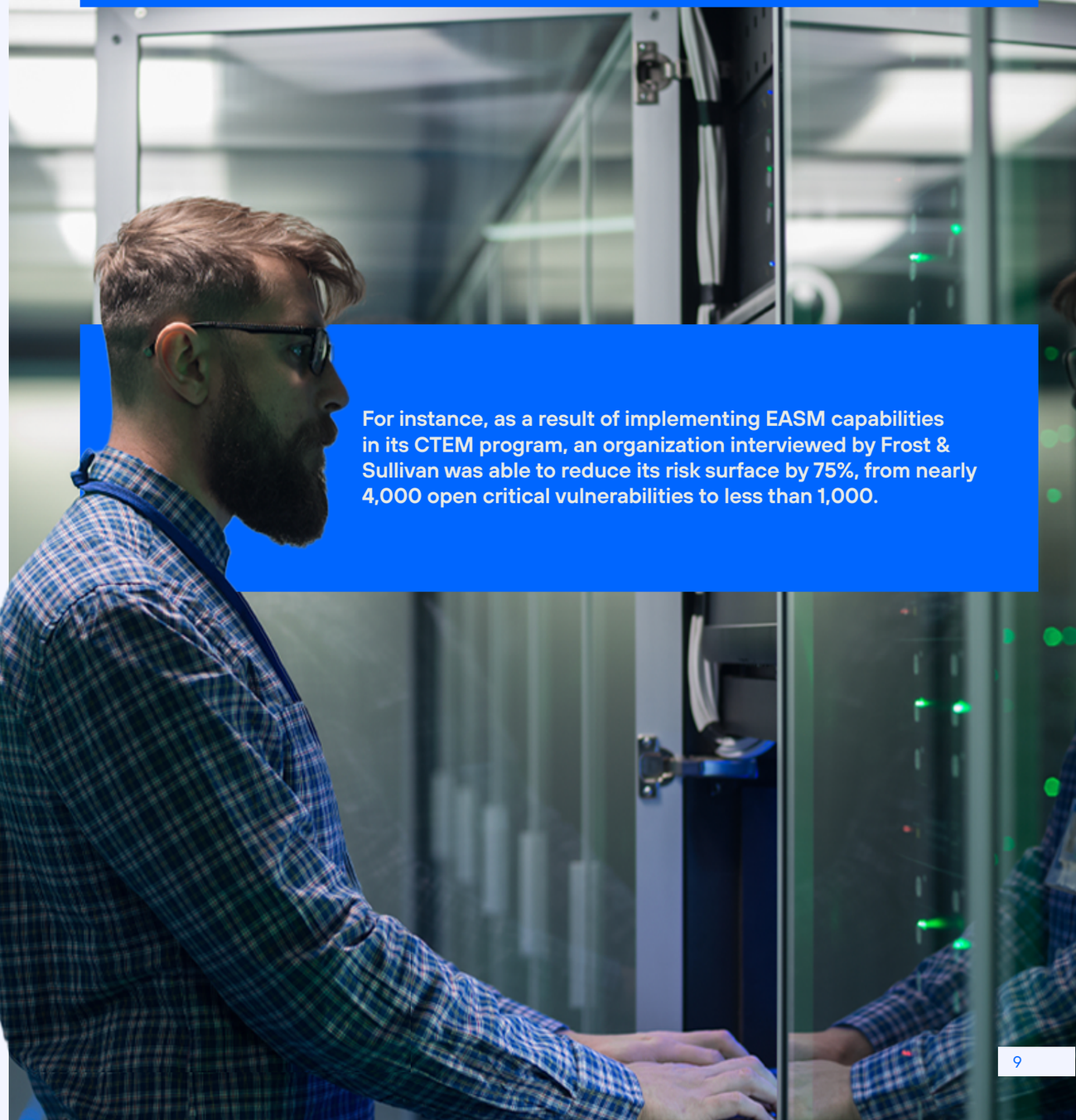
This problem is intensified by the workload resulting from a widespread shortage of specialized security personnel.

It is no surprise that the most significant challenge for organizations is the lack of visibility into their digital environment (Figure 1). Without continuous monitoring from internal and external perspectives, organizations lack the context necessary to identify all their critical assets and, consequently, understand their attack surface and associated risks. On the other hand, intangible assets such as intellectual property, customer data, business strategies, and brand reputation are critical to an organization's successand competitiveness.

These assets not only represent significant value in economic terms but are also essential for differentiation in the market. This makes them particularly attractive targets for cyber attackers seeking to steal sensitive and valuable information such as trade secrets, patented formulas, or customer databases. **The loss or compromise of these intangible assets can cause irreparable damage to a company's reputation, loss of customer trust, and ultimately, a significant financial impact.**

In this context, it is vital that a CTEM program covers both intangible and traditional assets. **Elements such as brands, social media profiles, key executives (VIPs), and intellectual property must be managed holistically alongside other traditional assets to ensure comprehensive protection against cyber threats.**

Leveraging capabilities such as External Attack Surface Management (EASM/ASM), Digital Risk Protection (DRP), and Cyber Threat Intelligence (CTI), organizations can gain greater visibility and more easily identify, prioritize, and mitigate risks, thereby protecting their critical assets and preserving customer trust in an increasingly sophisticated threat landscape.



For instance, as a result of implementing EASM capabilities in its CTEM program, an organization interviewed by Frost & Sullivan was able to reduce its risk surface by 75%, from nearly 4,000 open critical vulnerabilities to less than 1,000.

04

Intelligent prioritization in the age of information overload

Organizations are facing serious challenges in prioritizing alerts, threats, and vulnerabilities due to information overload.

Excessive noise, frequent false positives, and overwhelming volumes of data make it difficult for security teams to identify which threats are real (see Figure 1). **Many security leaders turn to numerous open sources to investigate breaches and ransomware threats. However, the lack of context and opportunities to integrate this information complicates the process, leading to delays in decision-making.**

In addition, limited access to dark web forums often prevents a comprehensive assessment of threats and data breaches, forcing teams to invest weeks of work and multiple analysts to complete investigations. The situation is further complicated when security leaders must prioritize vulnerabilities across a wide variety of assets but lack adequate validation. This can lead to inefficient resource allocation and delayed responses.

This is where a CTEM program, particularly in the discovery and prioritization phases, becomes relevant. **Including digital risk protection (DRP) services is essential in the discovery and prioritization phase of a CTEM program.** These services provide visibility into the digital threats facing organizations. The DRP team identifies potential threats and risks that could be exploited by malicious actors through constant monitoring of tangible and intangible assets, such as social networks, domains, and other exposed assets.

DRP enables organizations to prioritize their mitigation efforts, focusing attention on the most critical risks that could impact their operations by analyzing data on emerging threats and trends.

This translates into a more agile response to incidents and ensures that security measures are aligned with the most relevant threats.

A DRP service therefore optimizes the effectiveness of the CTEM program in two key areas: visibility and threat prioritization.

05

Cyber intelligence: the catalyst for continuous threat exposure management

In today's constantly evolving cyber threat landscape, organizations need to adopt a proactive approach to managing their exposure. Implementing a CTEM program is emerging as a key strategy, with cyber intelligence proving to be its main catalyst. The growing sophistication of attacks requires next-generation cyber intelligence that provides critical, actionable context. Such as the exploitability of assets; cybercriminal activity both at a general level and focused on specific industries; and knowledge of the tools, tactics, and technology used by malicious actors. This information allows organizations to prioritize their assets, vulnerabilities, and security efforts based on actual risk.

By using CTI within a CTEM program, for example, a security manager can identify and analyze:

- **A 0-day vulnerability** that is being actively exploited by ransomware groups
- That this group is **focused on attacking your organization's sector**
- **The specific tactics and techniques** that the ransomware group is using
- Details of **how other similar companies solved this or other similar situations**

Thanks to CTI, security managers can mitigate these risks by applying patches and resolving configuration issues and receiving recommendations for specific security solutions. What's more, the information provided by CTI provides a central framework for integrating and automating security through security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms.

According to studies conducted by Frost & Sullivan, 51% of organizations worldwide already have a designated CTI provider. **The use of CTI within a CTEM program refines all phases of the process, especially discovery, prioritization, and mobilization.** According to Frost & Sullivan interviews with users of CTI and DRP services, security managers can reduce threat enrichment and analysis time by up to 50% compared to organizations that do not use this technology.

51% of organizations

already have a designated CTI provider

Source: Voice of the Enterprise Security Customer from Frost & Sullivan

Up to 50%

reduction in threat enrichment and analysis time in organizations using CTI and DRP technologies

06

Enhancing effective security with cyber intelligence applied to CTEM programs

As we have seen, a cyber intelligence-driven CTEM program that integrates ASM, CTI, DRP, Vulnerability Management (VM), offensive security, and managed security services offers unique benefits that strengthen an organization's security posture.

- **Comprehensive visibility of the attack surface:** CTEM helps improve visibility into business exposure, thereby increasing threat detection efficiency. According to interviews conducted by Frost & Sullivan with CISOs and security managers from various organizations, after implementing a CTEM program, two out of four of these organizations increased their phishing site detection rates by 60% to 90% with the help of CTI and DRP services, helping to eliminate malicious content and protect their brand integrity. One of the organizations interviewed also reported an 80% increase in asset discovery after deploying an ASM solution, enabling them to effectively onboard new assets and proactively mitigate vulnerabilities.

- **Improved anticipation and response through cyber intelligence:** CTEM significantly increases organizational productivity by optimizing security processes. Real-time intelligence and proactive risk detection reduce the time needed to identify and respond to threats: according to interviews conducted by Frost & Sullivan with CISOs who have implemented CTI in the last year, more than 90% experienced an improvement in mean time to respond to threats (MTTR), with increases ranging from 30% to 165% depending on the organization.

- **Minimized financial impact:** The application of a CTEM approach leads to better prioritization of Cyber Security investments. This allows organizations to focus on areas that really need attention, avoiding unnecessary spending on solutions that do not address their most critical risks. One of the organizations interviewed by Frost & Sullivan saved nearly €300,000 in one year by using a combination of CTI and DRP to prevent fraud through the use of compromised credit card information. Companies can optimize their resources, reduce incident response times, and ultimately minimize the financial impact of potential incidents by having a clear view of the threats they face.

In short, a cyber intelligence-driven CTEM program that integrates ASM, CTI, DRP, VM, offensive security, and managed security services not only optimizes cyber defense capabilities, but also enables greater resilience to threats, reducing risks and improving response to security events.

Up to a 165% improvement in mean time to respond to threats (MTTR) after 12 months of implementing CTI

Source: Acording to Frost & Sullivan interviews

07

Comprehensive protection with **Telefónica Tech's** CTEM approach

In short, Cyber Security managers are currently facing multiple challenges (alert fatigue, increased frequency of attacks, and greater sophistication, among others). This means that Cyber Security managers must rely on technology partners such as managed security service providers (MSSPs) to overcome these problems. According to data from Frost & Sullivan's Voice of the Enterprise Security Customer survey, nearly 70% of organizations have partially or completely outsourced their Cyber Security operations to external providers, demonstrating the importance of MSSPs in improving Cyber Security Resilience.

Telefónica Tech is the ideal partner for implementing an effective Continuous Threat Exposure Management (CTEM) program because it combines leading technologies with the proven expertise of its team of security analysts. Its comprehensive offer ranges from attack surface management to threat intelligence, attack simulations, and controlled offensive strategies, all based on the CTEM framework.

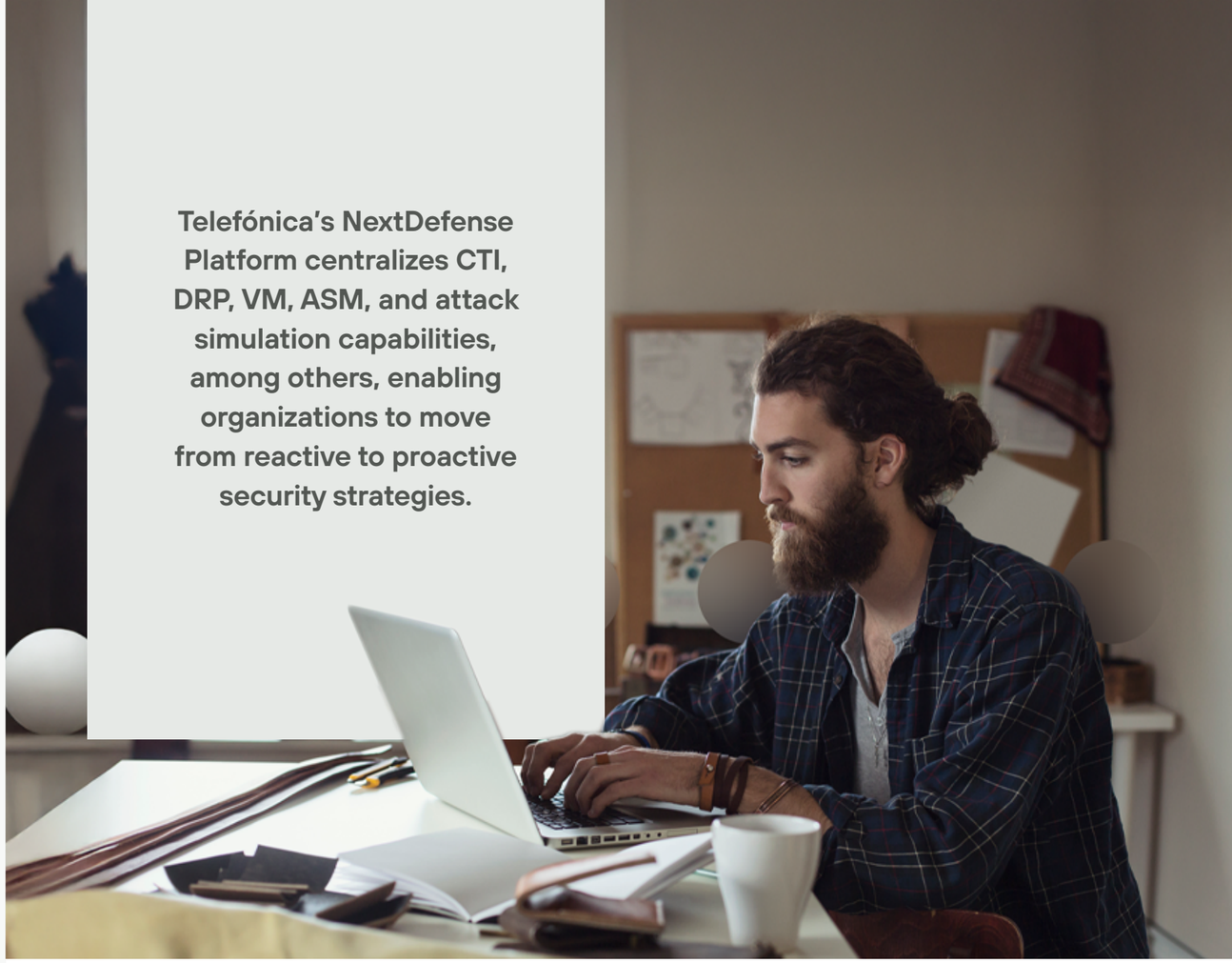
70%

of organizations have outsourced their Cyber Security operations to external providers.

Source: datos de la encuesta Voice of the Enterprise Security Customer de Frost & Sullivan

Telefónica's service portfolio covers all phases of the process, from risk identification and prioritization to automated remediation, ensuring a more robust security posture and effective reduction of critical exposures.

Telefónica's NextDefense Platform centralizes CTI, DRP, VM, ASM, and attack simulation capabilities, among others, enabling organizations to move from reactive to proactive security strategies.



Incidents such as those discussed in this paper highlight how these solutions can play a critical role in both prevention and mitigation. Cyber Security leaders should leverage CTI and DRP capabilities to identify phishing campaigns in their early stages, detecting malicious domains and suspicious activity on the dark web before they result in significant damage. Likewise, security tools such as ASM and VM offer continuous monitoring of digital assets and vulnerabilities, helping to secure third-party systems. Even after a data breach, DRP solutions serve to further mitigate risks by tracking, investigating, and addressing credentials leaked on the dark web.

Overall, these solutions optimize attack surface visibility and improve threat anticipation and response. This not only minimizes the financial impact on businesses, but more importantly, ensures customer trust.

About Telefónica Tech

Telefónica Tech is a global technology integrator and leader in digital transformation. The company offers a wide range of integrated technology services and solutions in Cyber Security, cloud, IoT, big data, and artificial intelligence. In all these verticals, we rely on our own technologies as well as the best ecosystems of strategic partners, and this is recognized by both industry analysts and our customers. All of this is also possible thanks to our hubs in Spain, the UK, Germany, Brazil, and Hispam, which allow us to reach more than 5.5 million customers in over 175 countries.

About Frost & Sullivan

Frost & Sullivan, the growth pipeline company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation, and leadership. The company's Growth Pipeline as a Service provides the CEO and the CEO's Growth Team with transformational strategies and best-practice models to drive the generation, evaluation, and implementation of powerful growth initiatives. Frost & Sullivan leverages over 60 years of experience in partnering with 1000 Global companies, emerging businesses, and the investment community from more than 40 offices on six continents.

Should you have any questions, please

→ **CONTACT US**

Telefónica Tech

FROST & SULLIVAN