# [CYBERSECURITY: TRENDS_REPORT]

## 2025

SOFISTIC CYBERSECURITY 480

# Results of SOC Audits and Monitoring Conducted by Sofistic in 2024 and Cybersecurity Recommendations for 2025

March 2025

# INDEX

# [1] WHAT INSIGHTS DOES THIS CYBERSECURITY REPORT OFFER YOU?

**Manuel Ginés**
Head of R&D

**Juan Carlos García**
Chief Operations Officer & SOC Director y Ph.D. in Computer Science

Organizations are facing an increasingly complex wave of cyber threats, driven by more sophisticated attacks, expanded attack surfaces, and the rise of generative AI systems. At Sofistic, Cuatroochenta's cybersecurity division, we understand this fast-evolving and highly challenging landscape that demands swift and effective responses. That's why staying up to date on the state of cybersecurity—analyzing vulnerabilities and identifying the most effective strategies—is more critical than ever.

This is exactly what we have done in the third edition of the **Cybersecurity Trends Report 2025**. As in previous years since 2022, we have analyzed anonymized results from SOC (Security Operations Center) audits and monitoring conducted by Sofistic throughout 2024 for companies in Latin America and Spain. Our goal is to provide a comprehensive perspective that helps organizations strengthen their defenses, optimize resources, and respond effectively to cyber threats.

Beyond being an exercise in transparency and disclosure, this report shares our knowledge and experience in prevention, detection, and active response. Understanding the origin, scope, and impact of threats is essential for navigating an ever-evolving cybersecurity landscape.

The most effective cybersecurity is the kind that operates seamlessly in the background, ensuring protection without disruption. At Sofistic, we believe this is best achieved through a comprehensive security approach, backed by a highly prepared team capable of identifying risks, strengthening defenses, and responding effectively to security incidents.

# [2] SAMPLE

This report is based on a large and representative sample of the work carried out by Sofistic's team of professionals in 2024. It includes the results of security audits and SOC monitoring. Below, we provide a detailed breakdown of both samples, along with their geographic and sectoral scope:

## Vulnerabilities Identified in Security Audits

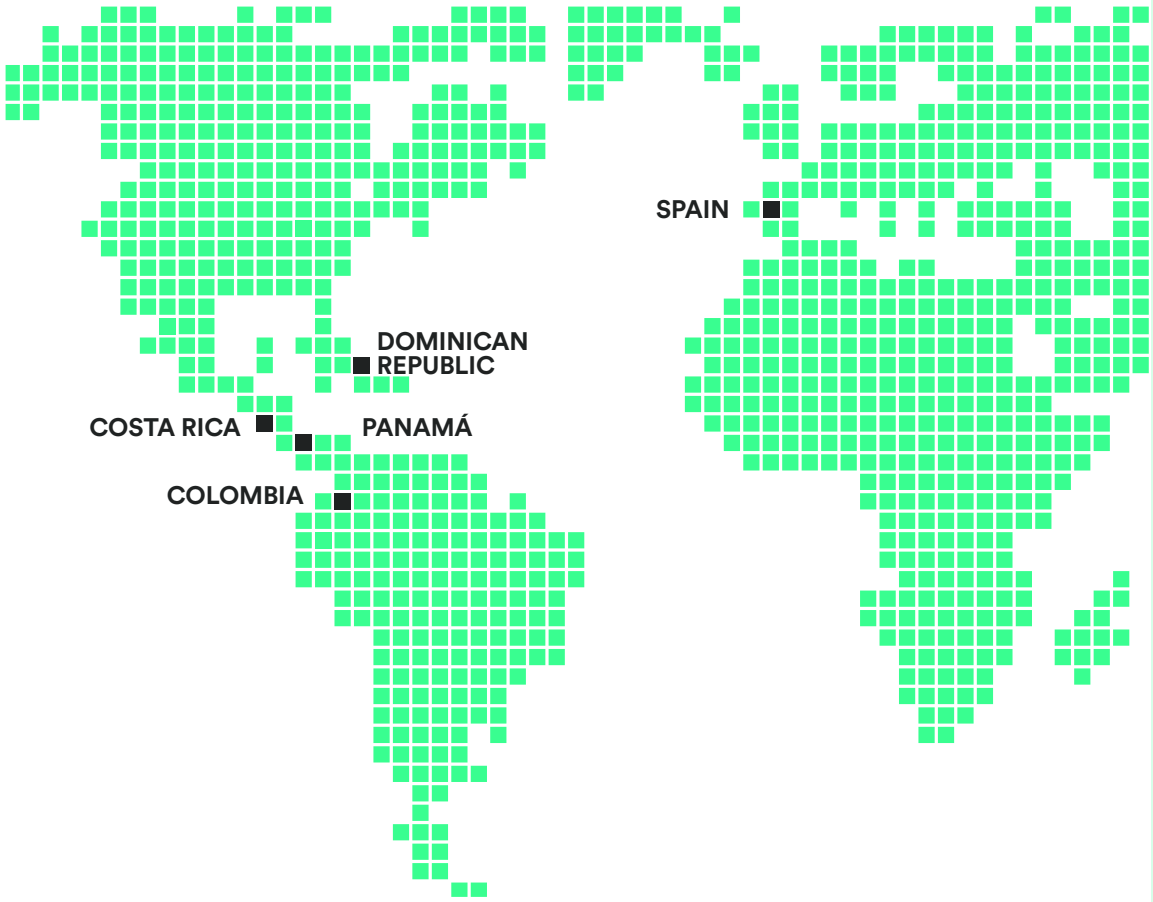
We analyzed a sample of 140 audits conducted for 40 clients, identifying a total of 1,350 vulnerabilities. The audits covered applications (both web and mobile), infrastructures (external and internal), source code, and social engineering.

## Security Cases Detected in the SOC

We analyzed a representative sample of 100,000 alerts and 1,500 cases from those managed by Sofistic's SOC team in Spain, Colombia, and Panama during 2024. This sample size is substantial enough to identify the key threats and incidents detected over the past year. Notably, in 2024, we revised our nomenclature to enhance precision. In previous reports, the term incident was used to categorize all managed events. Now, these are classified as cases, further divided into Requests for Information and Investigations (RFI), Cyber Threat Intelligence (CTI), Incidents (INC), and Configuration Cases (CONF).

## Geographic Scope

Sofistic's clients are primarily located in Spain and Latin America, with a strong presence in countries such as Colombia, Panama, Costa Rica, and the Dominican Republic.




## Sectors

**Critical infrastructures** (energy companies, water distribution, airports and hospitals)

**Banking and finance**

**Industry and services**

# [3] RESULTS

## [3.1] Security Audits

### Enhanced Protection Against Less Critical Attacks

We begin this report by examining the security flaws identified across various systems through conducted audits. Based on this detailed sample, we can analyze the evolution of vulnerabilities in 2024 compared to 2023.

| | |
|---|---|
| Audits | -8% |
| Vulnerabilities | +2% |
| Criticality | -8% |

Variation 2023/24

In 2024, we observed an 8% decrease in the number of audits conducted, as well as an 8% decline in reports generated from these analyses—marking a shift after two years of significant growth. However, this reduction is not due to a lower demand for these services, but rather to organizations reaching a more advanced level of cybersecurity. After assessing their critical environments and systems, many no longer require the same level of audits. Despite this decrease, the number of identified vulnerabilities has risen slightly (+2%) compared to 2023, while their severity has dropped significantly (-8%). This trend, which we first started noticing in 2023, reflects the growing cybersecurity maturity of companies and institutions.

**3 audits per client**

We have observed that after auditing their most critical environments, identifying vulnerabilities, and assisting in implementing improvements and corrections, these companies extend and replicate these analyses across other solutions and systems..

### Increase in Web Audits Amid Decline in Other Audits

| By type of audit | Variation 2021/22 | Variation 2022/23 | Variation 2023/24 |
|---|---|---|---|
| Web | +3% | +45% | +8% |
| Infrastructure | +112% | +24% | -14% |
| Cloud | +400% | -40% | -33% |
| Mobile | -10% | +44% | -23% |
| Phishing | +18% | -8% | -25% |
| Code review | +92% | -19% | -72% |

Analysis of the audit and vulnerability sample reveals an 8% increase in web security scans, while other types of audits declined compared to 2023. This trend may be due to the dynamic and ever-evolving nature of company websites and services, which require regular assessments to maintain security. Additionally, as publicly exposed entry points, websites are frequent targets for cyberattacks, making audits a crucial tool for mitigating potential risks.

Despite this trend, infrastructure audits remain the most frequently conducted. This is expected, as infrastructure—comprising networks, servers, and devices—serves as the backbone of technological systems. Its vulnerabilities could compromise security and disrupt an organization's operations, making it a primary focus for assessments.

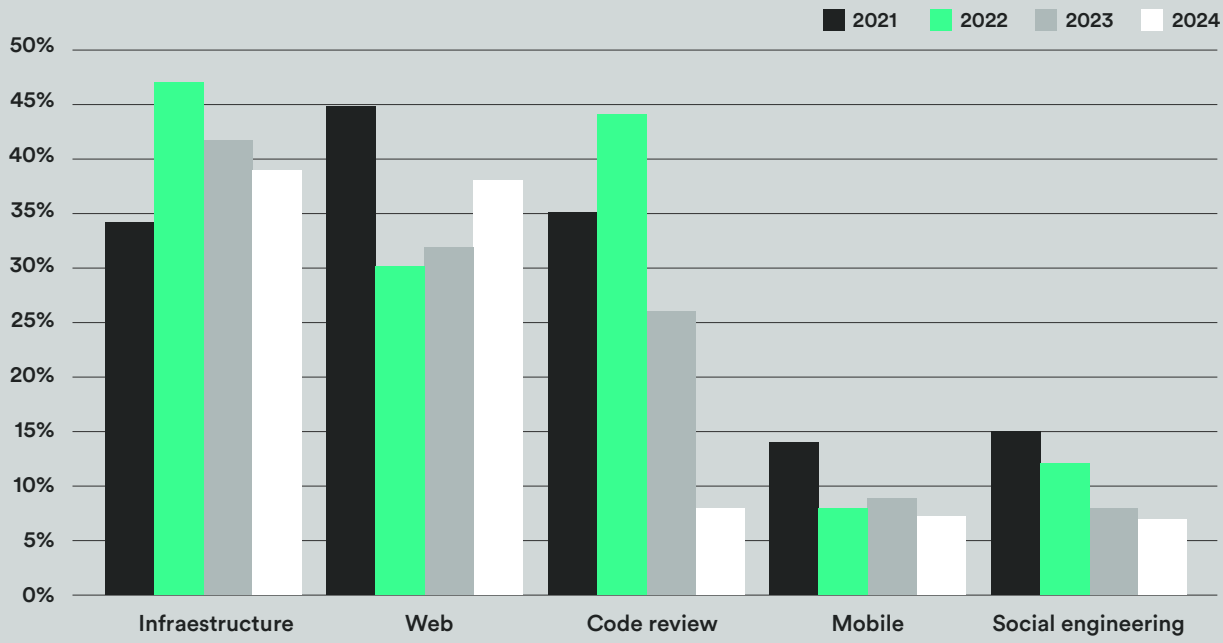
The sample also reveals that code review audits saw the sharpest decline (-72%) compared to the previous year. This trend suggests that, as a sign of growing cybersecurity maturity, organizations have increasingly integrated code analysis tools into their development workflows, reducing the need for standalone audits. Additionally, it is important to note that code reviews are often included as part of web and mobile application audits.

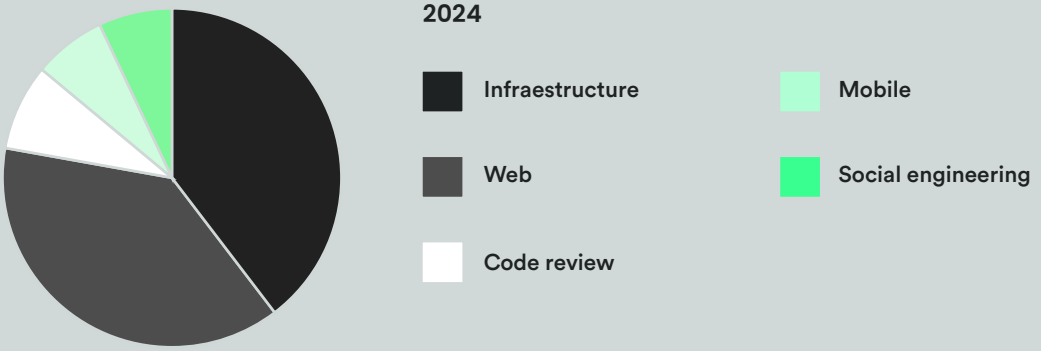
## Infrastructure Audits: The Most Frequent Due to Their Critical Importance

| Top type of audits by volume | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Infrastructure | 34% | 47% | 42% | 39% |
| Web | 45% | 30% | 32% | 38% |
| Code review | 35% | 44% | 26% | 8% |
| Mobile | 14% | 8% | 9% | 7% |
| Social engineering | 15% | 12% | 8% | 7% |

**39%** **infrastructure audits**

## Types of audits

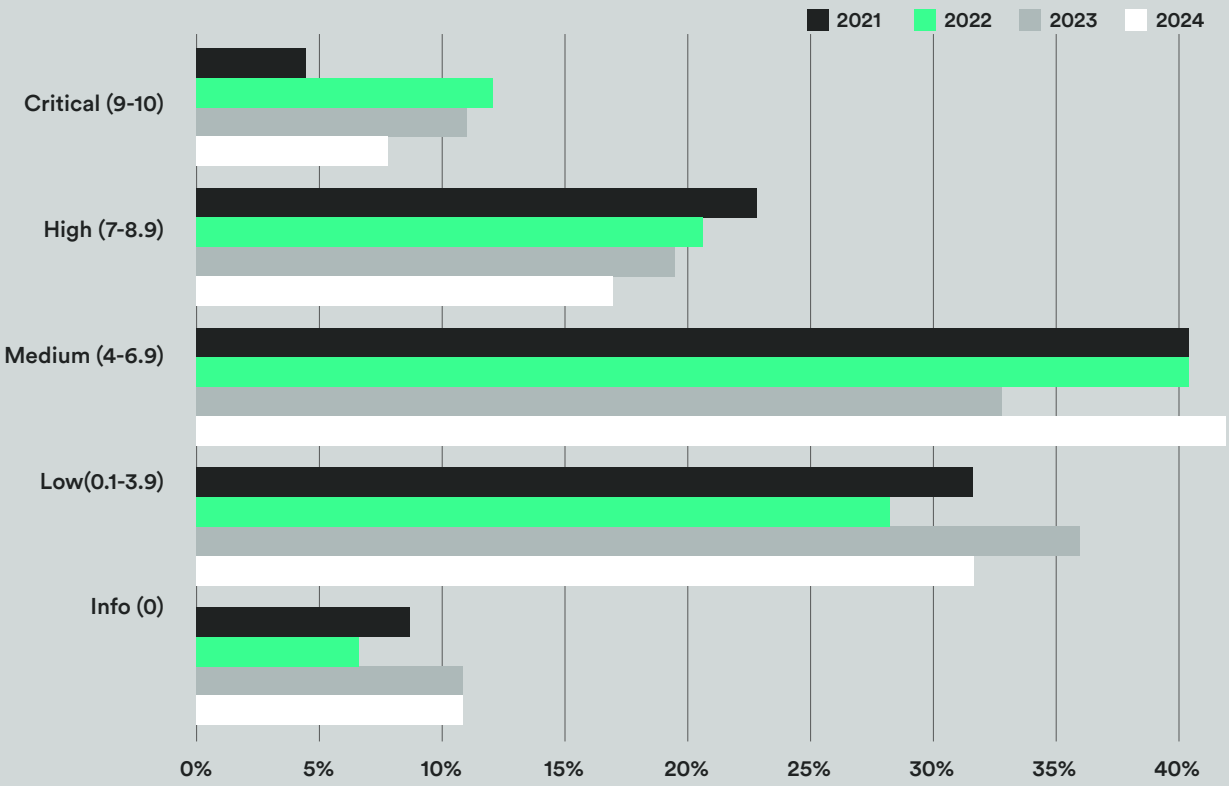



## Critical and High-Risk Vulnerabilities Decrease, While Medium-Risk Cases Rise

| Severity (% of total) | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Critical (9-10) | 4% | 11% | 10% | 7% |
| High (7-8.9) | 21% | 19% | 18% | 15% |
| Medium (4-6.9) | 37% | 37% | 30% | 37% |
| Low (0.1-3.9) | 29% | 26% | 33% | 28% |
| Info (0) | 8% | 6% | 10% | 10% |

## Severity of Vulnerabilities




In 2024, the severity of detected vulnerabilities continued to decline, a trend first observed in 2023. According to the audit sample, critical vulnerabilities decreased by 3 percentage points, now representing 7% of the total, while high-risk vulnerabilities also dropped by 3 points to 15%.

This is a positive development, indicating that flaws capable of compromising systems, networks, or data—and potentially paralyzing services—have been effectively mitigated or corrected. However, medium-risk vulnerabilities increased by 7 points, making up the largest share at 37%. While these issues, such as outdated software exposure or insecure password storage, may not immediately compromise a system, they can be exploited in combination with other weaknesses, leading to larger-scale attacks that threaten a company's security.

Critical and high-risk vulnerabilities account for **22% of detected cases**, a decrease of 6 percentage points compared to the previous year.

## Types of failures

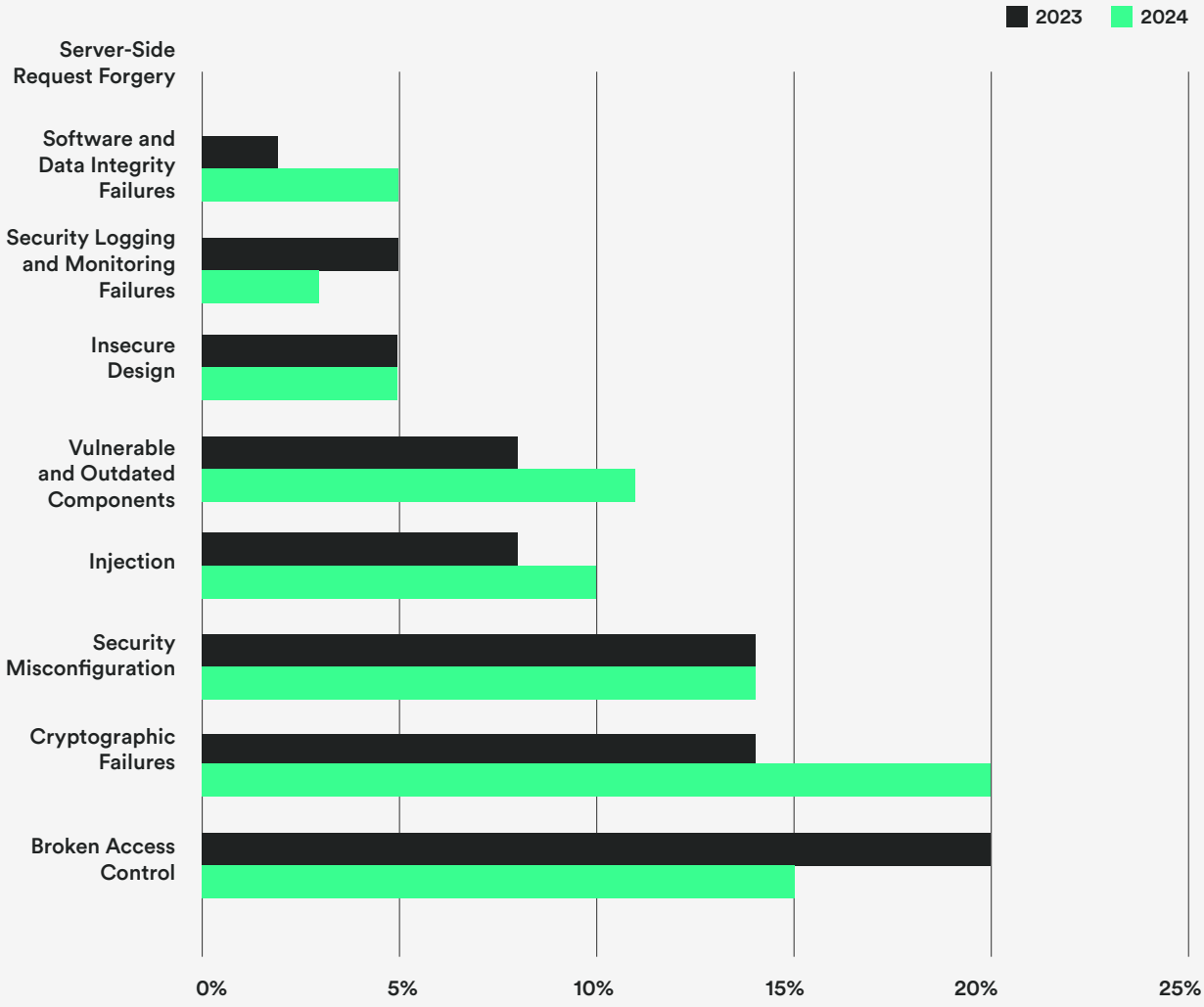
When analyzing vulnerabilities by category, we observe a slight shift in the ranking compared to 2023. Access control flaws—caused by incorrect authorizations and poorly implemented access restrictions—now top the list, moving up from second place in 2022. They are followed by cryptographic vulnerabilities, which have dropped one position compared to the previous year. These weaknesses often arise from misconfigured or outdated encryption and data protection mechanisms, making them exploitable by cybercriminals. Such vulnerabilities are particularly common in web applications, which, according to the analyzed sample, are the environments where security audit demand has grown the most. In third place are system configuration flaws, which occur when a system, application, or service is improperly configured, potentially exposing sensitive data, allowing unauthorized access, or enabling other types of attacks. The rest of the ranking remains largely unchanged from the previous year, with two exceptions: injection vulnerabilities, which have moved up to fourth place, and security logging and monitoring flaws, which have climbed to seventh place.

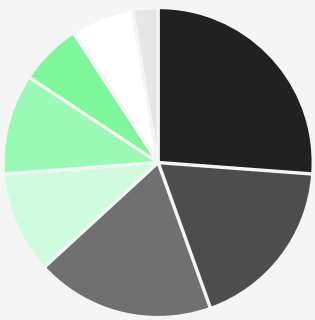
Analyzing the evolution of vulnerabilities by volume relative to the total, we observe an increase in logging and monitoring failures, access control failures, and insecure design flaws. Conversely, software and data integrity failures, identification and authentication flaws, cryptographic vulnerabilities, and outdated component weaknesses have decreased.

The following table summarizes the relative weight of each impact category and its evolution since 2021, including the current top 10 ranking:

| **Category** | **Volume** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Stockholder | 2021 | 2022 | 2023 | 2024 | Variation 2022-2023 | 2023 | 2024 | |
| Broken Access Control | 21% | 18% | 18% | 26% | +49% | 2 | 1 | +1 |
| Cryptographic Failures | 17% | 25% | 24% | 18% | -23% | 1 | 2 | -1 |
| Security Misconfiguration | 18% | 16% | 16% | 11% | +11% | 3 | 3 | = |
| Injection | 14% | 13% | 12% | 7% | -9% | 5 | 4 | +1 |
| Vulnerable and Outdated Components | 10% | 13% | 13% | 18% | -22% | 4 | 5 | -1 |
| Insecure Design | 10% | 7% | 6% | 10% | +16% | 6 | 6 | = |
| Security Logging and Monitoring Failures | 2% | 3% | 4% | 2% | +57% | 8 | 7 | +1 |
| Identification and Authentication Failures | 7% | 5% | 6% | 0% | -55% | 7 | 8 | -1 |
| Software and Data Integrity Failures | 1% | 0% | 1% | 6% | -100% | 9 | 9 | = |
| Server-Side Request Forgery | 0,00% | 0,00% | 0,00% | 0% | 0% | 10 | 10 | = |

## Vulnerability categories



Broken Acces Control
Cryptographic Failures
Security Misconfiguration
Injection
Vulnerable and Outdated Components
Insecure Design
Security Logging and Monitoring Failures
Identification and Authentication Failures
Software and data Integrity Failures
Server-Side Request Forgery

## Phishing: Half of Users Open Fraudulent Emails, but Fewer Fall for the Scam

| Phishing | 2021 | 2022 | 2023 | 2024 | 2021 - 2022 | 2022 - 2023 | 2023 - 2024 |
|---|---|---|---|---|---|---|---|
| Open Email | 50% | 36% | 33% | 50% | -28% | -8% | +53% |
| Access link | 29% | 18% | 40% | 24% | -40% | +128% | -39% |
| Credentials | 11% | 10% | 20% | 17% | -5% | +95% | -31% |

An analysis of social engineering audits conducted in 2024 reveals a significant increase (+53%) in the number of users interacting with phishing emails. However, the percentage of users clicking on fraudulent links (-39%) and entering credentials (-31%) has decreased notably. These findings indicate that, thanks to training and awareness efforts, users are more vigilant and better equipped to recognize and verify deceptive emails. Even if they open them, they are less likely to click on malicious links or provide sensitive information. Despite this positive trend, a significant number of users still fall victim to phishing scams, creating potential security vulnerabilities. The key takeaways from the data are:

**1 out of 2**

**users who receive a phishing e-mail open it**

**24%**

**of users open links**

**17%**

**provide data**

These findings are partly the result of phishing simulation campaigns conducted within organizations as part of their awareness and training strategies. These initiatives help employees recognize and report suspicious emails, strengthening the overall cybersecurity culture. As noted in last year's report, this progress has allowed phishing awareness efforts to shift from broad, company-wide campaigns to more targeted training for specific groups with key roles or responsibilities. Despite these improvements, the growing use of generative AI (Gen AI) in phishing attacks cannot be overlooked. Tools based on large language models (LLMs) like ChatGPT, Copilot, and the disruptive DeepSeek enable cybercriminals to automate, personalize, and enhance their attacks—not just through text, but also via audio and video. This makes phishing attempts significantly more realistic, credible, and ultimately more effective. To counter these evolving threats, companies must adopt proactive measures and strengthen defenses against deepfakes and voice cloning, which are increasingly being used for fraud and misinformation.

# [3.2] Incidents Detected in the SOC

## Cybersecurity Monitoring Services

The second part of our report focuses on the results obtained from 24/7 monitoring conducted by Sofistic's Security Operations Centers (SOCs) in Colombia, Spain, and Panama. These centers play a crucial role in identifying attacks that impact organizations. In analyzing the study sample for 2024, we observed a growing interest among companies in centralizing and monitoring their security through an advanced detection and response center, such as those operated by Sofistic across two continents. This increasing demand reflects the urgent need for businesses to enhance their security posture with high-speed threat detection and response, supported by a highly specialized and skilled team.

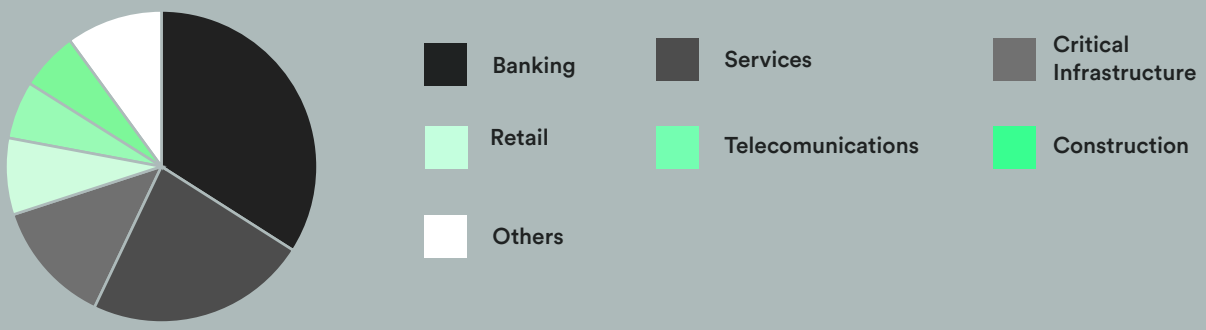
Based on the analyzed sample, there has been a 17% decrease in the number of detected alerts. However, this trend does not indicate a reduction in cybercrime activity or threats but rather reflects improvements in detection systems. These technologies are becoming increasingly precise in identifying risks and anomalies, reducing the number of false alerts. Additionally, this decline is complemented by the higher level of security maturity that organizations have developed over time. What has continued to rise, according to the data, is the number of cases handled (+27%). As mentioned in the sample description, in 2024, we refined our nomenclature to enhance precision and improve the service provided to our clients. In previous reports, the term incident was used to group all managed events. Now, they are categorized as cases and further classified into Requests for Information and Investigations (RFI), Cyber Threat Intelligence (CTI), Incidents (INC), and Configuration Cases (CONF).

**-17%** Managed alerts

**+27%** Incidents investigated

## Banking and Services: The Most Vigilant Sectors

| Sector | Banking | Services | Critical Infrastructure | Retail | Telecomunicacions | Construction | Others |
|---|---|---|---|---|---|---|---|
| % | 34% | 23% | 13% | 8% | 6% | 6% | 10% |

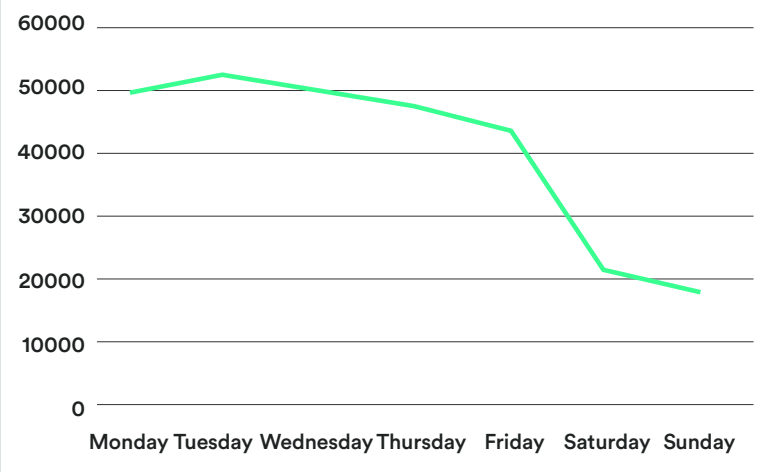


The banking sector accounts for the largest volume of alerts managed through Sofistic's SOCs across different countries. It is followed by the services sector, which has dropped one position compared to the previous year, and critical infrastructure, now in third place. This ranking is influenced by the prominence of clients from these sectors in the analyzed sample. While the proportion of alerts generated by banking and critical infrastructure has decreased, they remain the most active sectors. Currently, 6 out of 10 managed alerts come from these two industries, compared to eight out of ten in the previous year.

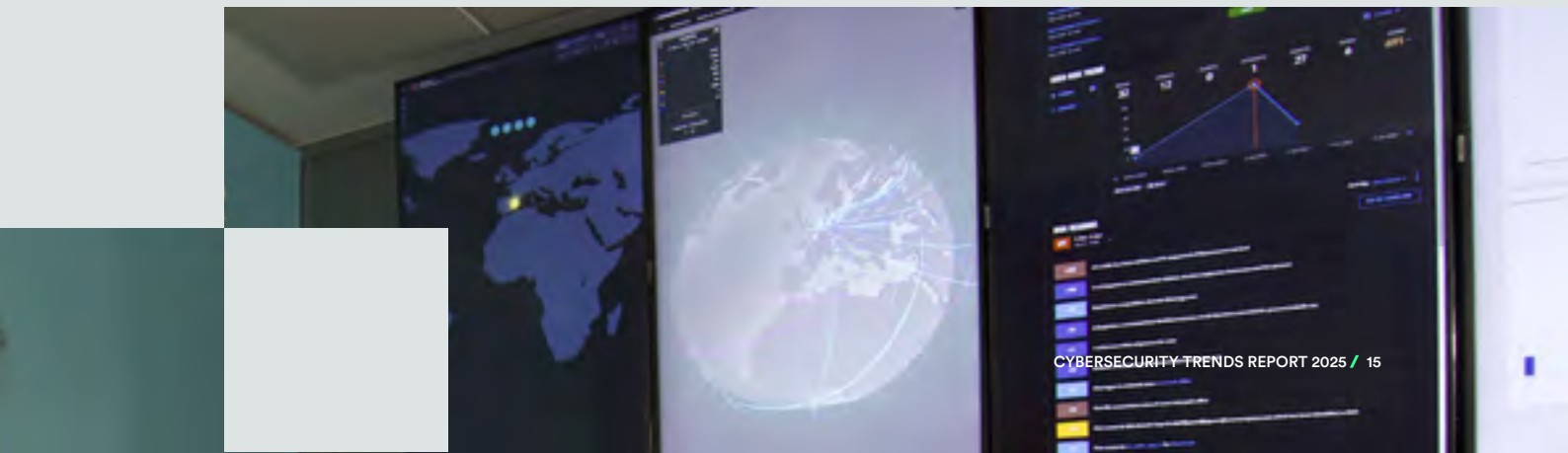
This ranking reflects the varying levels of cybersecurity maturity and investment across different economic sectors. Both banking and critical infrastructure have been highly proactive in cybersecurity, each for distinct reasons. These sectors provide essential services—such as transportation, healthcare, and basic utilities—and are also subject to strict regulatory requirements. As a result, they have long invested in cybersecurity measures and advanced detection and response technologies. Meanwhile, the services sector has shown increasing awareness in recent years. However, there is still room for improvement in adopting more robust protection measures.

## Massive Automated Attacks Targeting Vulnerabilities on Weekends

SOC monitoring reveals that more cases and alerts are registered on weekdays. This data suggests that the attack surface is larger during the workweek, with more employees active and more devices connected.




Cybercriminals, using automated and large-scale tactics such as mass login attempts or unauthorized access scans, actively seek vulnerabilities throughout the week. They then exploit these weaknesses on weekends when organizations are at their most vulnerable—staffing is reduced, attention levels are lower, and less-protected devices, such as mobile phones, are more frequently used. This trend reinforces the reality that cybercrime never rests and continues to evolve with increasing sophistication and professionalism.



## 10% of Managed Cases Are Classified as Critical or High Severity

| | Critical | High | Medium | Low | Info |
|---|---|---|---|---|---|
| **Severity (% total)** | 1% | 9% | 70% | 12% | 8% |

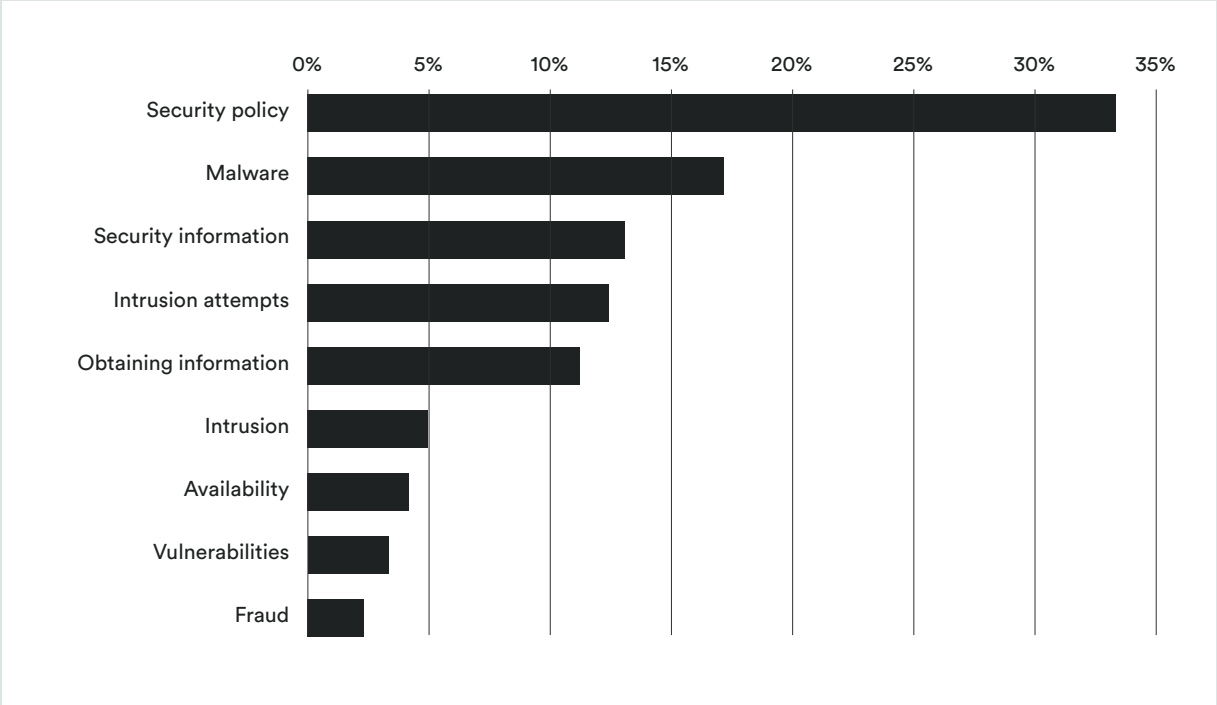
Consistent with the trend observed in audits, SOC monitoring shows a 7-point increase in medium-severity cases, which now account for 70% of the total. Meanwhile, there is a slight decline in critical and high-severity cases—the most urgent threats, as they have the potential to compromise an organization's operations. As previously mentioned, this trend reflects growing cybersecurity maturity among companies. Many organizations have been investing in security for years, and after addressing their most critical vulnerabilities, they are now shifting their focus to lower-risk weaknesses. While these may not pose an immediate threat, they still require attention, as they can serve as entry points for more complex attacks.

## Access to unauthorized services, the main reason

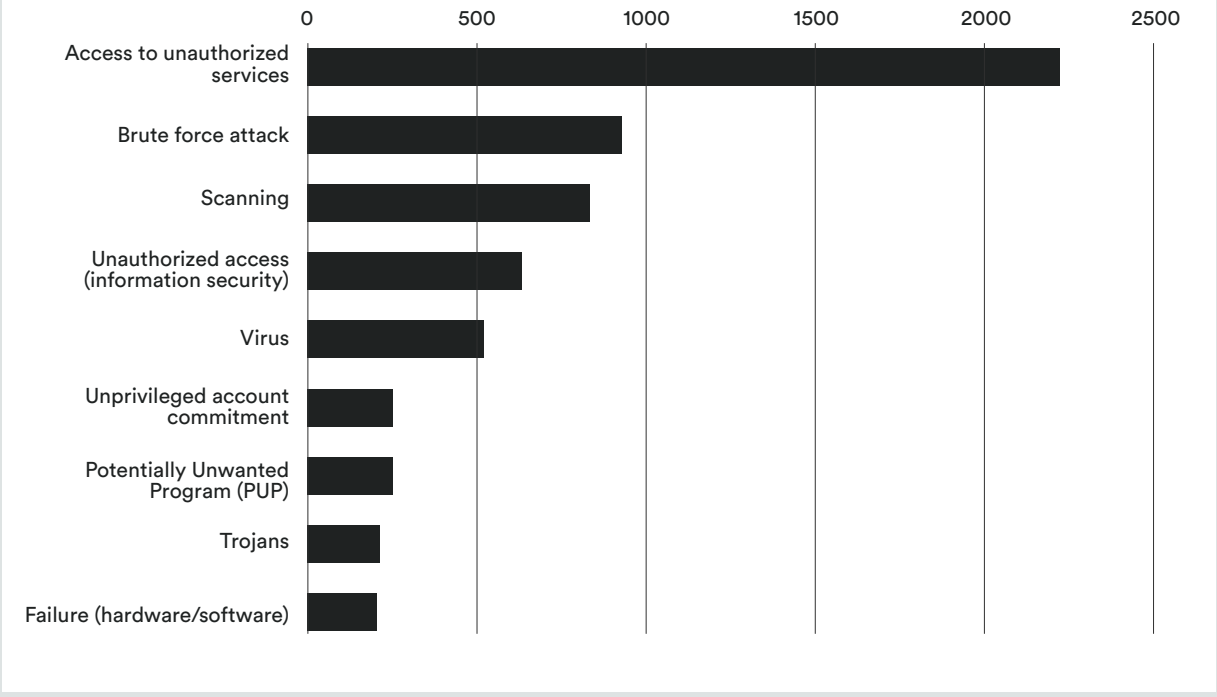
| Type of cases by main category | % |
|---|---|
| Security policy | 33% |
| Malware | 17% |
| Information security | 13% |
| Intrusion attempts | 12% |
| Obtaining information | 11% |
| Intrusion | 5% |
| Availability | 4% |
| Vulnerabilities | 3% |
| Fraud | 2% |

| Type of cases by subcategory | % |
|---|---|
| Access to unauthorized services | 29% |
| Brute force attack | 12% |
| Scanning | 10% |
| Unauthorized access (information security) | 8% |
| Virus | 7% |
| Unprivileged account commitment | 3% |
| Potentially Unwanted Program (PUP) | 3% |
| Trojans | 3% |
| Failure (hardware/software) | 3% |

## Cases by main category



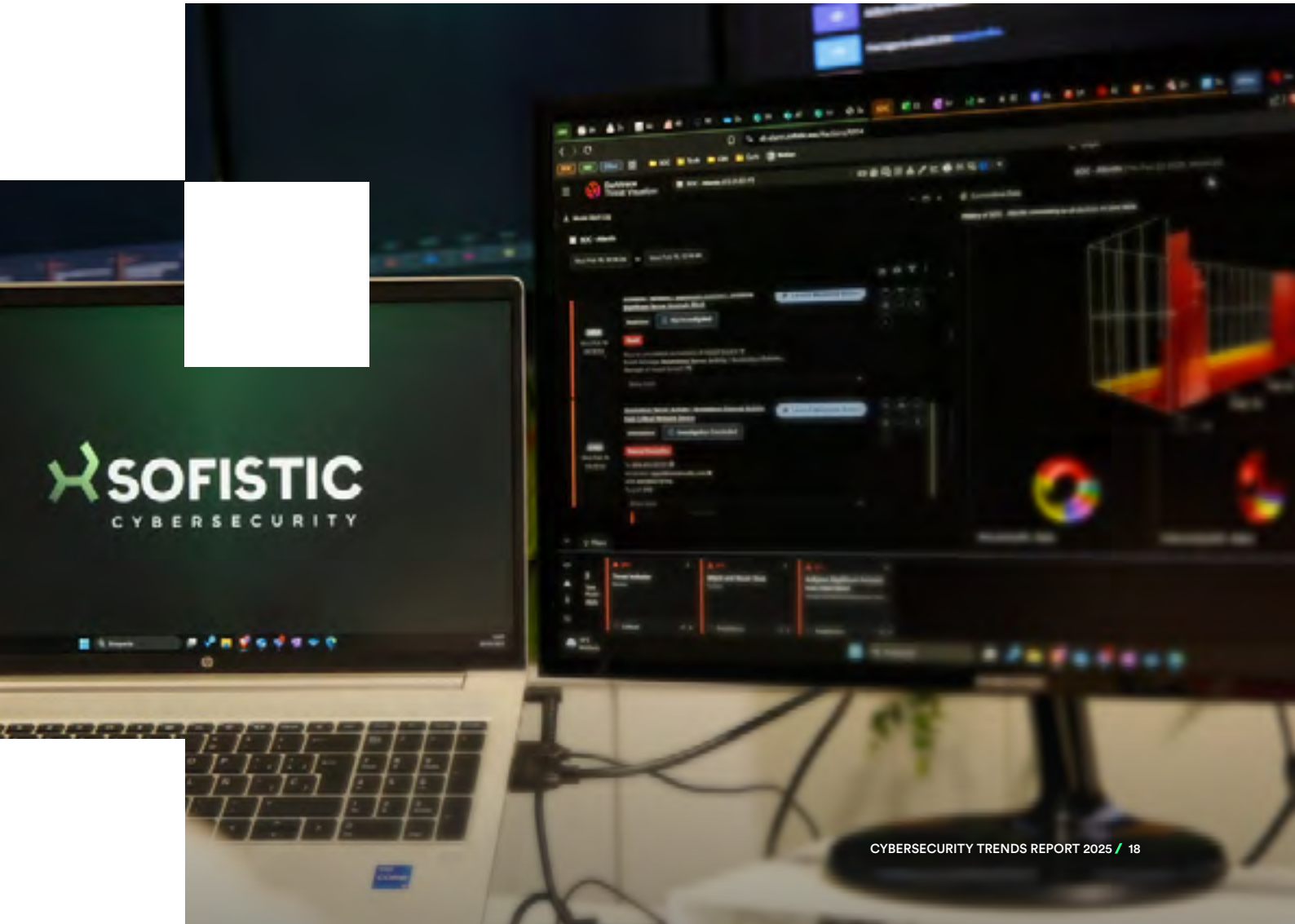

## Cases by subcategory



Once again, SOC monitoring confirms that security policy violations account for the majority of managed cases (33%). The vast majority of these cases (29% of the total) involve attempts to access unauthorized services. Other common triggers, though to a lesser extent, include privilege abuse, the use of remote access tools, infrastructure changes, and outdated systems.

It is increasingly common for companies with advanced cybersecurity maturity to establish their own highly detailed security standards and policies. As a result, alert systems are tailored to these specific rules, use cases and detection models, triggering warnings when policies are breached. This factor partially explains the high percentage of cases linked to security policy violations.

Malware cases ranked second in volume (17%), primarily involving viruses, potentially unwanted programs (PUPs), and Trojans. Information security cases moved up two places in the ranking to take third place. These include incidents such as unauthorized access to information, unauthorized modification or deletion of data, and data exfiltration—the theft or unauthorized transfer of sensitive information. Additionally, intrusion attempts remain a significant concern. These typically involve brute-force attacks or the exploitation of known vulnerabilities to gain unauthorized access to systems.



# [4] CONCLUSIONS

The findings from our analysis of Sofistic's security audit and SOC monitoring sample align with other benchmark reports from leading cybersecurity agencies. Cybercriminals are increasingly exploiting geopolitical tensions, trade conflicts, and economic rivalries. Combined with emerging technologies, supply chain dependencies, and the growing sophistication of AI-driven attacks, these factors are making the cybersecurity landscape more complex than ever—a concern recently highlighted by the World Economic Forum. Understanding this evolving context is essential for improving security investments and enhancing response capabilities. The data in our report suggests that companies are recognizing this priority, strengthening their resilience to meet these challenges. With this in mind, we have outlined the key takeaways that can help guide your future cybersecurity decisions:

---

**Enhanced Monitoring for Lower-Risk Attacks.** Despite the increasing complexity of the cybersecurity landscape and the rise in threats and vulnerabilities, organizations' growing maturity in cybersecurity has led to the correction of critical and high-risk vulnerabilities that could compromise operations. Additionally, threat monitoring has significantly improved. However, companies must continue implementing measures to mitigate medium-risk vulnerabilities, as these weaknesses could still serve as entry points for more severe attacks.

---

**The main vulnerabilities detected,** in order, are:

1. **Access control failures** caused by incorrect authorizations or poorly implemented access restrictions, allowing unauthorized users or systems to access restricted data, applications, or resources.

2. **Cryptographic failures** resulting from improperly configured or outdated encryption and data protection mechanisms, potentially exposing sensitive data and compromising its confidentiality or integrity.

3. **Configuration faults** that expose weaknesses in security settings, potentially providing entry points for cybercriminals. These vulnerabilities highlight the complexity of cybersecurity management, emphasizing the need for highly specialized and skilled IT professionals.

4. **Injection failures** that enable attackers to take control of a system or environment by inserting malicious code, altering its operation through unauthorized commands.

**More Users Engage with Phishing Emails, but Fewer Fall Victim.** Training has significantly improved cybersecurity awareness, equipping users with the skills to recognize the signs of deceptive emails. However, despite increased awareness, 24% still click on fraudulent links, and 17% provide credentials—actions that can grant cybercriminals access to systems and compromise an organization, leading to severe financial, legal, or reputational consequences.

---

**The main cases managed by the SOC are driven by:**

1. **Access to Unauthorized Services:** A user or system gains access to an application, network, or resource without proper authorization, often due to configuration errors or compromised credentials.

2. **Brute Force Attacks:** Cybercriminals attempt multiple password combinations in a repetitive and automated manner to gain unauthorized access to an environment, system, or network.

3. **Scanning:** Through network scanning, exposed devices or services are identified, potentially making them targets for cyberattackers.

4. **Unauthorized Access to Sensitive Information:** Occurs when a user or system accesses or modifies data without proper authorization, often due to misconfigurations or stolen credentials.

**Massive Automated Attacks Exploiting Vulnerabilities on Weekends.**

SOC monitoring reveals a higher incidence of cases during the workweek, likely due to a larger attack surface as organizational activity increases.

Cybercriminals use automated, large-scale systems to identify breaches and vulnerabilities throughout the week, strategically exploiting them on weekends when companies are at their most vulnerable—operating with reduced activity and fewer personnel on duty.

# [5] CYBERSECURITY RECOMMENDATIONS FOR 2025

The analysis of cybersecurity trends observed in 2024 has led us to outline a series of practical recommendations to minimize risks in 2025. With increasing regulatory requirements—such as the NIS2 directive on network and information security and the DORA regulation governing cybersecurity in the financial sector—many of these measures are becoming mandatory to enhance security management and ensure business continuity in the face of digital threats. Additionally, global spending on cybersecurity products and services is projected to grow by 13%, according to McKinsey estimates. In this evolving landscape, it is crucial to understand where future investments should be prioritized:

**Develop Comprehensive Cybersecurity Strategies for Maximum Efficiency and Effectiveness.**

The growing complexity of cyber threats calls for an interconnected approach that identifies vulnerabilities through audits, strengthens security with targeted technologies, and ensures continuous monitoring. The goal is to accelerate incident detection and response while minimizing potential impact.


**Prioritize Artificial Intelligence Models.**

Artificial intelligence presents both a risk and an opportunity in cybersecurity management. Cybercriminals are using AI to customize social engineering attacks, significantly increasing their success rate. At the same time, companies must integrate AI-driven solutions to predict potential cyberattacks and enhance their investigation and incident response capabilities. However, regardless of the industry, organizations must exercise extreme caution to mitigate new attack vectors related to LLM systems, such as data exfiltration, model compromise, and the reliability and consistency of AI-generated responses. Recognizing the potential of this technology, Sofistic is collaborating with INCIBE to develop a pioneering cloud-based alert management solution, powered by AI, to accelerate cyberattack response times. This initiative exemplifies the strength of public-private collaboration in reinforcing the cybersecurity ecosystem.

**Evaluate Supplier Risks and Integrate Cybersecurity Across the Entire Supply Chain.**

Cybercriminals exploit all possible attack vectors, including vulnerabilities in suppliers and partners. In this context, it is essential to enforce the same level of cybersecurity across the entire external environment and supplier network. This prevents incidents from spreading or being used as an entry point to compromise your infrastructure.

**Strengthen the Security Culture.**

The growing sophistication of phishing attacks, driven by generative AI, necessitates more than just robust technological controls and administrative processes. Companies must also implement continuous training and awareness programs to equip all employees with the skills needed to recognize and mitigate risks.

# [6] WHO WE ARE


At **Sofistic**, Cuatroochenta's cybersecurity unit, we specialize in the banking sector and critical infrastructures. We serve key clients in these industries across Colombia, Panama, Costa Rica, the Dominican Republic, and Spain.

We provide both preventive and proactive protection, along with an effective incident response, powered by cutting-edge software. Our highly skilled professionals specialize in identifying and mitigating attacks, simplifying security, and minimizing risk. With 18 years of experience, we have a proven track record of enhancing protection and response capabilities—ensuring maximum security without compromising business efficiency.

Both our employees and the company hold numerous security certifications, including ISO 27001, ISO 9001, ENS, and SOC 2 Type II. These certifications reaffirm our compliance with strict standards for security, availability, integrity, confidentiality, and data privacy, in accordance with the GDPR and various local Personal Data Protection regulations. Additionally, we collaborate with leading international (FIRST) and national (CSIRT.es and Red Nacional de SOC) organizations to exchange information that enhances cybersecurity for other companies. We are also part of strategic alliances like ioXt, working to build trust in IT products. All these efforts reflect our commitment to upholding the highest standards of quality and cybersecurity.

At Sofistic, we integrate advanced technology with artificial intelligence in cybersecurity to deliver a proactive and effective approach to protecting organizations:

**Security Audits.** We evaluate an organization's true security position, identifying vulnerabilities before cybercriminals can exploit them. Through advanced penetration testing and real-world attack simulations, we help strengthen our clients' cybersecurity defenses..

**MSSP Services (*Managed Security Services Provider*):** Beyond simply implementing tools, we manage and optimize organizational security, ensuring continuous adaptation to emerging threats. Our team of professionals provides expert assistance and preventive maintenance, guaranteeing maximum performance and strong resilience against cyberattacks.

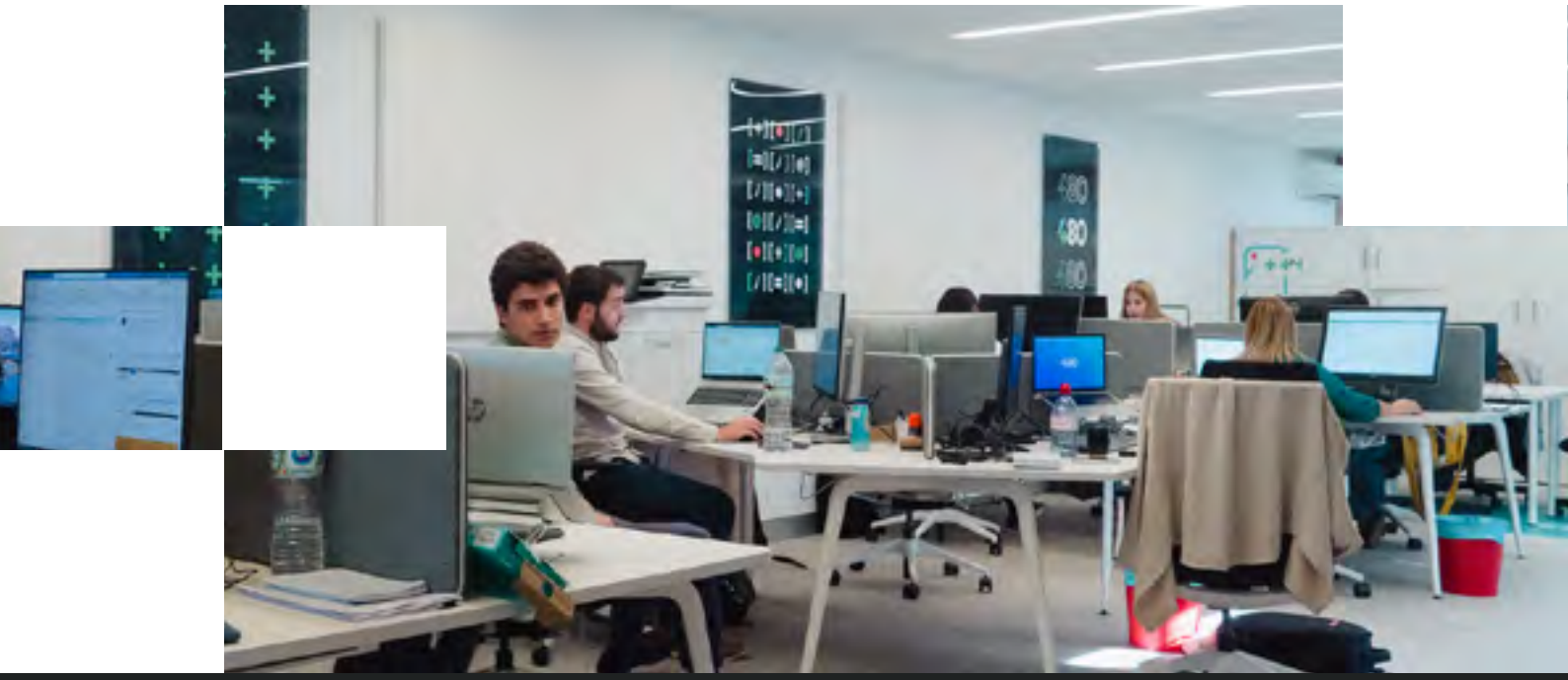
***Managed Detection & Response (MDR)*:** From our SOCs in Europe and Latin America, we provide 24/7 real-time threat detection and response. By combining industry-leading security technologies with advanced AI algorithms, we analyze and detect anomalous behavior before it becomes a risk to businesses.

480

**Cuatroochenta** is a technology company specializing in cloud-based digital solutions and cybersecurity to enhance organizational performance.

In addition to securing critical infrastructure and financial institutions through Sofistic, Cuatroochenta operates as an **Independent Software Vendor (ISV)** with its Facility Management & Services applications, FAMA and CheckingPlan, as well as the Escena Online ticketing platform. The company also serves as a **Value-Added Reseller (VAR)** for Microsoft and Zoho business management solutions and a **Value-Added Services (VAS)** provider through its custom development division, 480:DEV.

Cuatroochenta's solutions serve over 20 million users across 32 countries. Headquartered in the Espaitec technology park at Universitat Jaume I in Castelló de la Plana (Spain), the company operates offices in Madrid, Barcelona, Valencia, Burgos, Lugo, Málaga, Bogotá, Panama, Mexico City, Santo Domingo, and San José, employing more than 270 professionals. Since October 2020, Cuatroochenta has been listed on BME Growth under the ticker 480S.



The following contributors participated in the preparation of this report:

**Manuel Ginés,** Head of R&D de Sofistic
**Juan Carlos García,** CCO & SOC Director de Sofistic
**Arturo Beltran,** CISO de Cuatroochenta
**Patrick Campillo,** MD/MDR Team Leader de Sofistic
**Bárbara Villuendas,** Branded Content Manager de Cuatroochenta

480

SOFISTIC
CYBERSECURITY

cuatroochenta.com