

LANDSCAPE

2025 → 2026

THREAT

MAXUR

# Summary

Message from Axur	3
Executive Summary	4
Cybersecurity Landscape	9
2025 in Numbers	15
Cyber Threat Intelligence	33
Geopolitical Landscape	38
Trends	45
Cybersecurity Actions for 2026	54
About Axur	61

# Message from Axur

In 2025, cybersecurity experienced a clear paradox. We have more data, more visibility, and more tools than ever before, and yet we've never been so overwhelmed with alerts. The challenge is no longer knowing what's happening, but transforming information into action.

The landscape has changed. Supply chain attacks have become frequent, targeting the foundation: repositories, libraries, and solutions that support entire ecosystems. And increasingly, threat groups have exploited insiders, the internal vector used by malicious actors to compromise environments with precision and discretion.

It's in this context that Axur has been strengthening its mission to deliver structured, enriched, and prioritized data. The launch of Axur Command represents a step beyond, taking automation to the next level and allowing validation policies to be executed autonomously.

For 2026, our vision is clear. Data consolidation and the ability to act in an integrated manner will be the major differentiators. Axur wants to be, for the attack surface, what observability platforms are for engineering: a central nervous system. A single point where everything connects, prioritizes, and resolves.

This report presents our reading of the 2025 threat landscape, with trends, data, and practical perspectives for the coming year. We hope it helps security teams prioritize better, act faster, and, above all, anticipate risks before they become incidents.

Technology continues to advance, and with it come new possibilities. Our role is to ensure that this advancement happens with security, confidence, and responsibility.

**Count on us in  
this journey.**



Fábio Ramos  
CEO, Axur.

# Executive Summary

## Key Numbers

-  +6 billion new and unique credentials detected
-  Phishing cases total 71,399 pages detected
-  Fraudulent brand use cases grow, with 454,000 incidents
-  We removed over 343,000 fraudulent content through automated takedown flows
-  395 million credit and debit cards detected
-  Phishing grows 65% for the financial sector
-  Similar domain threats grows +1000%
-  Fake profiles and information exposure continue to be used to attack executives and VIPs, with over 19,000 incidents.

## Featured Bulletins

### Critical

Bybit Heist: \$1.5 Billion Lazarus Group Safe {Wallet} Exploit Revealed

[Learn more ↗](#)

### Critical

SAP NetWeaver Zero-Day Exploited, Exposing Critical Remote Code Execution Risk

[Learn more ↗](#)

### Critical

UNC6395 Exploits OAuth Tokens in Sophisticated Salesforce Data Breach

[Learn more ↗](#)

### High

Red Hat GitHub Breach Poses High-Risk Threat to the Supply Chain

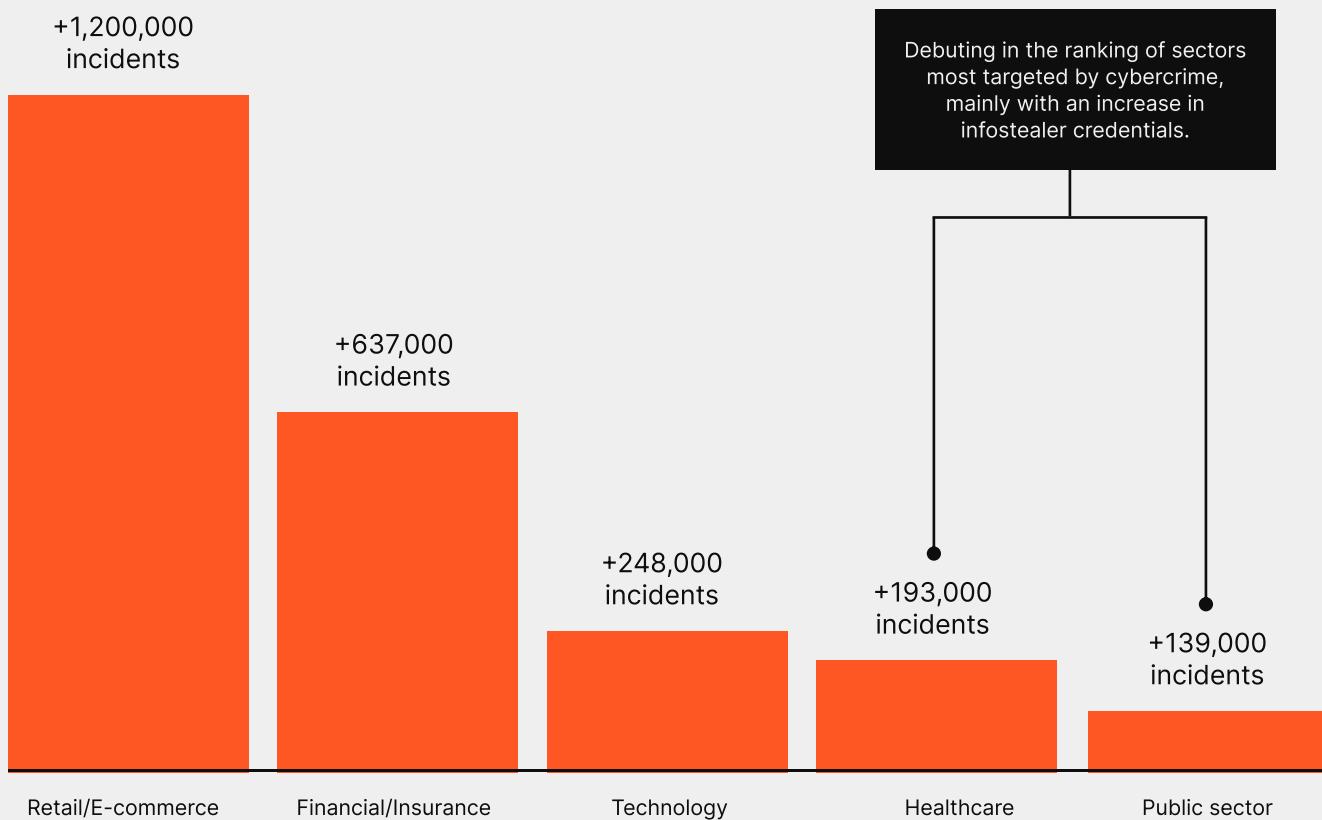
[Learn more ↗](#)

### High

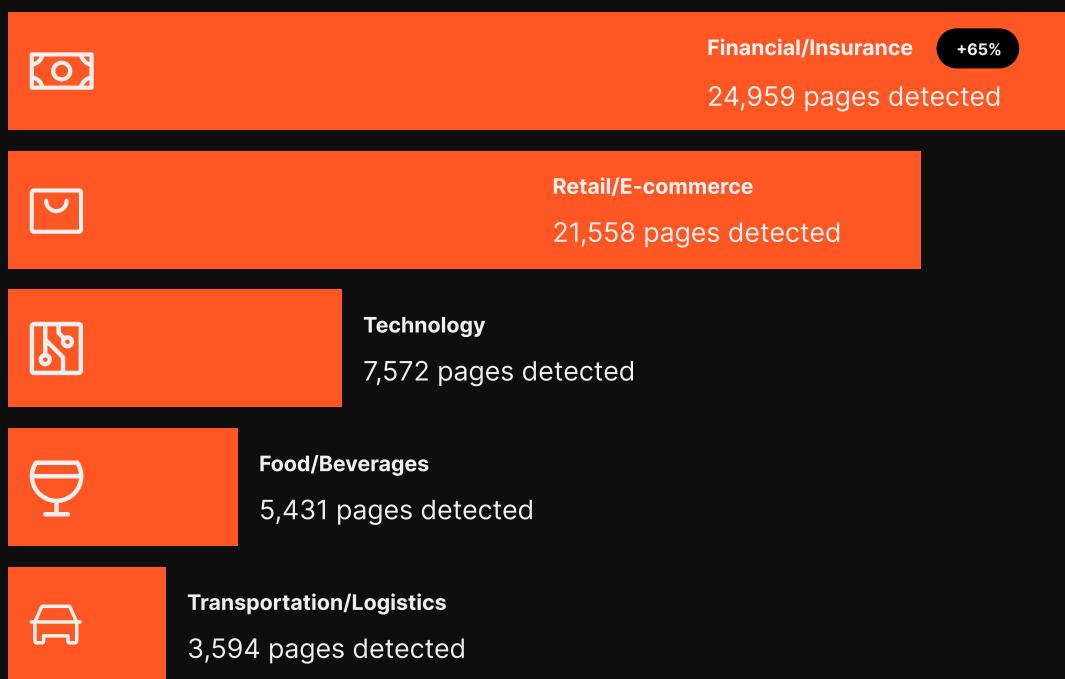
Cloudflare Thwarts Record-Breaking 22.2 Tbps DDoS Attack

[Learn more ↗](#)

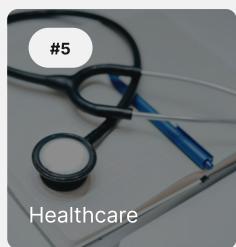
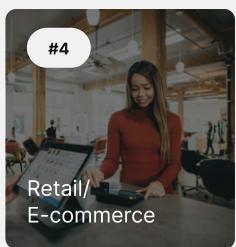
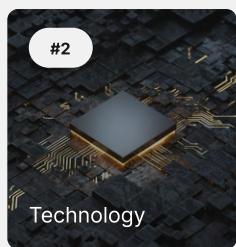
## Sector Ranking by Incidents



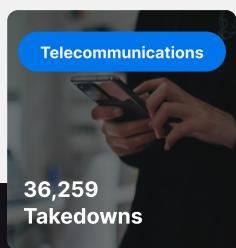
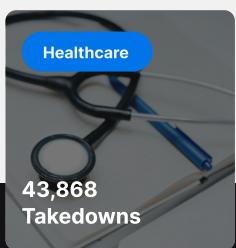
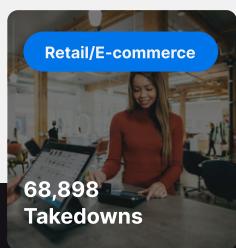
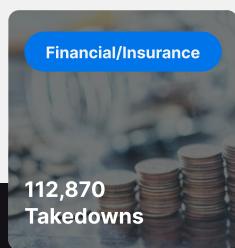
## Sectors Most Targeted by Phishing



## Sectors Most Targeted on the Deep & Dark Web



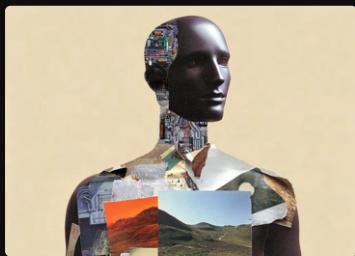
## Takedown Rankings



## Most Impacted Locations



## Trends for 2026



### AI agents gain autonomy

Tools that today act as assistants will begin making operational decisions, escalating responses, prioritizing investigations, and triggering automated remediations. This accelerates defense but also creates decision points that require strict governance: who authorizes what AI can execute?



### Criminals consolidate AI use

The same capacity to orchestrate and learn in real-time has been incorporated into attacks, with automatic generation of hyper-personalized phishing campaigns, model-guided fuzzing, and massive payload variation to evade detection.



### The race for digital sovereignty

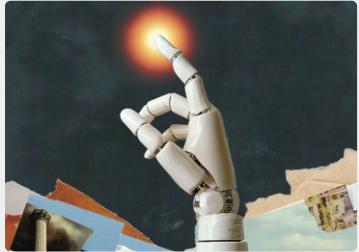
Regulations and national policies will fragment data flows and require local or hybrid architectures, which redesigns trust chains, increases compliance complexity, and creates new operational vectors for those who don't adapt.



### Forgotten threats return to action

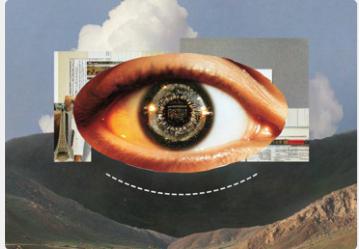
Legacy hardware in IoT/OT, poorly maintained or exposed, is being reactivated as a resource in botnets and persistent campaigns.

## Recommendations for Upcoming Challenges



### Prepare for the age of agents

Autonomous agents are taking on critical response and investigation tasks. Before delegating actions, establish autonomy policies, operational limits, and audit mechanisms. Define who authorizes automated executions and how to revoke instructions in case of anomalous behavior.



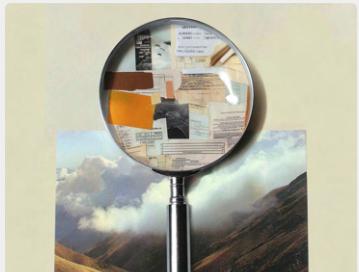
### Look beyond the perimeter

Most exposures begin outside internal assets. Monitoring leaked credentials, build artifacts, and brand mentions in external sources is essential to anticipate incidents. Early detection in external environments significantly reduces mean time to detection (MTTD).



### Protect critical internal assets

Developers and support teams remain among the primary targets of phishing and credential stuffing. Implement MFA resistant to push bombing, segregation of duties, and monitoring of remote access tool usage. Successful attacks on these profiles have a multiplier effect across the entire infrastructure.



### Map the third-party surface

CISA's alert about large-scale compromise of the npm ecosystem highlighted the growing risk in software supply chains. Dependencies, APIs, and partner pipelines expand the attack surface and require continuous validation of integrity and permissions, as a single compromised supplier can propagate malicious code throughout the entire environment.

# Cybersecurity Landscape

It's difficult to summarize the cybersecurity landscape in just a few threats or challenges. In a way, the challenge lies precisely in the diversity of threats and the volume of issues requiring attention.

In recent years, cybersecurity has become more sensitive to each business's needs, which contributes to risk management and project prioritization. In this sense, we cannot fail to mention that the business environment is also challenging, with regulatory and commercial uncertainties on a global scale that reverberate even to small and medium enterprises.

The technological environment has also changed. Some companies have been reducing the proportion of employees working remotely, but not even the end of remote work would end "remote data" stored in the cloud, with partners and third parties. But since this isn't always so evident, there's a risk that remote access security may be neglected. At the same time, there's growing demand for interactive and intelligent services, whether in e-commerce or service provision. New engagement modalities also open opportunities for criminals.

All of this is happening without any truce in vulnerability exploitation or ransomware incidents.

On the contrary: vulnerabilities in network devices are increasingly concerning, and are now cited in ransomware attacks and data breaches. Meanwhile, social engineering scams are partially shifting from end users to IT professionals, reaching a new audience in unexpected ways.

## Edge Devices Become Priority Target

Attacks on edge devices (mainly VPNs and firewalls) stood out in 2024 and consolidated in 2025.

The exploitation of vulnerabilities was a concerning point in these attacks, but not the only one. Hackers also managed to carry out invasions using stolen credentials and even brute force attacks. Some of these attacks drew attention for bypassing two-factor authentication, either through the use of vulnerabilities or perhaps thanks to a leak of the one-time code generation keys.

The Vulnerability Catalog of the United States Cybersecurity Agency (CISA) indicates that devices and software from various manufacturers had their vulnerabilities exploited throughout the year. Broadcom, Cisco, Fortinet, Ivanti, Juniper, Palo Alto Networks, and SonicWall are some of the brands on the 2025 list.

The objective of exploiting these devices was quite varied.

Part of the attacks aimed to invade corporate networks to **install ransomware** and carry out the already well-known extortion fraud in which hackers demand a ransom to recover encrypted files or to not disclose information exfiltrated from compromised systems.

Another set of attacks was attributed to **state-sponsored actors**. In these attacks, targets were typically critical infrastructure operators, such as telecommunications companies, energy companies, or government entities.

In the case of attacks against home routers, invaders typically install malware to connect the compromised equipment to a **botnet**.

The devices can then be used in DDoS attacks or to act as proxies for criminals, hiding the origin of other activities. At least some of the codes used are based on Mirai, an IoT malware first detected in 2016.

## Social Engineering Attacks Target Support and Recruitment Teams

It's been a few years since the Scattered Spider group's activities have been demonstrating the effectiveness of innovative approaches in cyberattacks, mainly using social engineering. This happened again in 2025, with invasions

that began from illegitimate phone calls asking for help to reset passwords.

This contact strategy with IT support teams differs from what is most common in social engineering, which are direct attacks against users. In these new cases, fraudsters pose as users asking for help with their credentials and thereby manage to obtain a valid credential to access the company's network or some platform.



The most notorious attacks with this approach happened in the UK, where retail chains were impacted and announced significant losses resulting from the invasions.

Social engineering tactics associated with employment and recruitment also deserve attention. This scam can be carried out against both companies and candidates.

In the case of fraud against recruiters, it occurs especially in stages where the candidate has the opportunity to send some material to the company. When the recruiter opens the received file, they may end up compromising their system and possibly the company's network.

Frauds against candidates happen in a similar manner. Scammers send fake job offers, suggesting that the professional participate in the selection process. The support material for participating in the process will be contaminated with malware, and the consequences can even reach the corporate network if the professional is currently employed.

Interestingly, these frauds frequently involve IT jobs and professionals. It's quite likely that targets are handpicked to reach specific companies or projects. Projects associated with the cryptocurrency market, for example, tend to be heavily targeted by criminals.



### Scattered Spider

Financially motivated cybercriminal collective active since 2022 (USA and UK).

#### Main Tactics

Social engineering (spear phishing, smishing, vishing), SIM swapping, MFA fatigue, and use of legitimate remote access tools (SupremoControl, AnyDesk, ConnectWise, Splashtop).

#### Malware Used

BlackCat, Qilin, Akira, DragonForce; stealers like Racoon and Meduza.

#### Notable Targets

MGM Resorts, Caesars Entertainment, Snowflake, and major financial institutions.

#### Objective

Data theft and extortion for financial gains.

## Expert Commentary



Pedro Moura

Researcher at  
Axur Research Team

Although Scattered Spider became notable as an affiliate of groups like BlackCat/ALPHV and, later, DragonForce, the collective evolved in 2025 to develop its own ransomware, abandoning the intermediary role. CISA confirmed this transition in a recent alert, highlighting the increase in the group's operational sophistication.

The supposed "shutdown of operations" and the seizure banner displayed on their onion domains are widely interpreted as PsyOps actions, designed to confuse the security community and mask a possible restructuring.

## Triple Extortion Makes Ransomware More Difficult to Contain

Ransomware attacks continue to represent a significant threat to businesses, and nearly all recorded malicious activities end up having some involvement with these attacks.

The RaaS (ransomware as a service) model establishes a structure in which various "affiliates" are responsible for finding ways to install the malware within corporate networks.

This way, the same ransomware can be associated with multiple attack strategies. Phishing, supply chain attacks, credential abuse, recruitment of internal collaborators, vulnerabilities – all these tactics are used to invade IT infrastructure and initiate the ransomware scam.

A point of attention in the ransomware context concerns the **extortion modalities** at the incident's outcome. Traditionally, ransomware encrypts system files to paralyze business activities and then charges for the key capable of restoring data and recovering systems.

Given the frequency of these attacks, many companies have adopted robust recovery processes to restore systems from protected backups, which reduced the criminals' coercive power.

Scammers then responded with **double and triple extortion** tactics, in which the company is also threatened with the **exposure of corporate data and DDoS attacks** – situations for which the company may not be prepared or cannot even prevent.

More recently, criminals have also been resorting to extortion attempts based solely on the threat of exposing corporate data.

Even though criminals dispense with blocking systems and files through encryption, all other characteristics of the scam follow the ransomware pattern.

### Expert Commentary

Double extortion is already consolidated and appears almost as mandatory in the current scenario. Additionally, there are growing extortions exclusively related to data leaks without necessarily having encryption.



Alisson Moretto

Head of Threat Hunting at Axur

Dispensing with data encryption, criminals can attempt extortion even when it wasn't feasible to obtain write access to certain systems, or when they know files can be easily recovered (as in the case of cloud storage).

The arguments during "negotiation" with companies have also been evolving in the same direction. Gangs exploit the fear of legal repercussions and reputation damage resulting from data leaks to convince the victim to make the payment, including the use of supposed "lawyers" who would be offering legal advice.

## Supply Chain Attacks Become Recurrent

Attacks against the supply chain have consolidated as a robust vector for cyberattacks. The best-known historical incidents are possibly that of retailer Target, which suffered a data breach from the access of an HVAC service provider in 2013, and that of SolarWinds, which had its software tampered with by an invader to implant backdoors in several clients.

In recent years, the notion of supply chain risks has been expanded in certain aspects. The use of standardized platforms and software as a service (SaaS) solutions has enabled a new category of mass attacks, with or without the use of specific vulnerabilities. The cases of MOVEit Transfer (2023) and Cleo (2024) are examples of mass incidents involving some vulnerability in software.

Meanwhile, the data theft attacks that exploited Snowflake (2024) and Salesforce (2025) services used stolen credentials and social engineering, respectively. These recurring campaigns show that the strategy of attacking suppliers and third parties has consolidated among attackers.

Attacks against third parties have always been possible, of course, but now they are intentional and strategic, including to obtain privileged information (such as credentials) or to have access to an easier path to invade the final target's network.

## Software Supply Chain Becomes Contamination Vector

A subgroup of supply chain attacks are attacks on software development infrastructure, which typically boils down to "software supply chain." This definition can include cases like SolarWinds and other situations where software is directly tampered with, but there is an even more specific portion of attacks located exclusively in software development processes.

In these attacks, criminals create or modify packages in repositories like npm and PyPI, which are used by engineers in other software. With this, malicious behavior spreads to other projects, affecting corporate solutions that use these codes.

It's quite common for small improvised applications for IT administrative activities to use these repositories, so the existence of direct risk cannot be ruled out just because the company doesn't formally engage in software development.

In addition, there is considerable indirect risk if the company uses other software that depends on packages in these libraries or in software development support services that may be compromised.

Throughout 2025, several malicious packages were observed in npm and PyPI. Hackers created various fake packages and tampered with legitimate packages, which was possible after stealing the maintainers' credentials.

## Salesloft Incident Shows How Supply Chain Amplifies Breach Reach

An incident that hit Salesloft and its clients in August 2025 exemplifies several of the attack strategies that compose the year's landscape. It was a supply chain attack that began with social engineering against IT staff to steal credentials.

The hackers attacked a company engineer, possibly with social engineering, to obtain a GitHub credential. This credential was used to access the cloud infrastructure, from where criminals extracted OAuth tokens associated with Drift, a Salesloft chatbot.

Drift needed these OAuth authorizations to link to clients' Salesforce CRM instances and access the data that would support the personalized experience provided by the chatbot. Since these OAuth tokens gave access to Salesloft clients' corporate data, several companies were compromised.

[Learn more ↗](#)



# 2025 in Numbers



## Credentials

The Axur platform detected **6 billion new unique credentials in 2025**. It's important to note that, until last year, our report brought the total number of credentials detected. The change came through processes implemented to bring accurate verification of collected data, in line with what we commented about less noise and more relevant alerts.

With the increase of large data recompilations being disclosed as if they were a new leak, it's more important than ever to offer security teams curated alerts that avoid the rework of checking credentials frequently reshared in cybercriminal groups and forums. Therefore, a unique credential counts as a login and password set shared only once.

This number shows that there are still many malicious activities aimed at stealing credentials. These compromised credentials circulate in the criminal underworld spaces, fueling various threats and scams.

A point of attention is that the majority of new credentials (52.2%) are tied to corporate systems.

It's possible that these credentials grant access to systems that store commercial or personal information whose exposure would harm the company's activities or reputation. In several countries, the leak of personal data also generates legal consequences.

A recurring example in 2025 was attacks that used credentials from VPNs and other network edge devices.

Although MFA adoption reduces risks from leaked credentials, criminals have managed to combine these credentials with phishing scams, convincing a support analyst to disable or reconfigure MFA. Since the password is already in the criminals' hands, this is sufficient to compromise the account.

Credential leakage also increases the risk associated with vulnerabilities that allow bypassing MFA.

For these reasons, monitoring leaked credentials is an important mechanism to increase the resilience of authentication processes across all corporate systems, even if an MFA solution is in use.



## Phishing

Axur detected 71,399 phishing pages in 2025.

Phishing is one of the best-known and most constant cyber frauds. At Axur, we count the web pages where phishing occurs, regardless of the channel used to deliver these pages to victims. Thus, in addition to links to fake sites disclosed in emails, Smishing pages (phishing by SMS) and sites promoted by paid ads are also counted.

After a significant increase in phishing page detection in the previous year, the total volume of pages remained stable in 2025.

Phishing detection can be combined with the takedown process to remove the fraud from the air, decreasing the impact on the brand and consumers. With the use of [Clair \(Cyber Lens for Anomaly and Impersonation Recognition\)](#), our artificial intelligence model, it's possible to identify phishing pages reliably and automatically.

Additionally, the attributes identified by Clair become filters that allow detection beyond keywords.



70% of phishing scams don't use a keyword in the domain



18% don't bring the keyword in the page's HTML code

Phishing cases that use brand colors, for example, are found by automated monitoring and subject to automatic takedown. Additionally, it's possible to use Threat Hunting to search for URLs with varied attributes.

### Possible Searches:

→ **Brand imitation by visual elements:** identifies sites that imitate well-known brands or display specific logos. For example, detect varying levels of "BrandName" imitation or find sites displaying the "BrandLogo".

→ **Content type and sensitive data requests:** phishing sites by content type, such as login pages, error pages, or e-commerce sites. It's also possible to identify those requesting sensitive information, such as passwords or payment data.

→ **Domain analysis and lifecycle:** domains based on creation or expiration dates, or filter results by recent detection dates to find new threats.

→ **References and URL attributes:** examines specific URLs or references and filters by domain, subdomain, or top-level domain (TLD) attributes to refine searches.

→ **HTML content:** searches for specific terms present in detected pages' code, such as emails, phone numbers, and more.

→ **Language and region-specific threats:** investigations in certain languages or regions identify more localized phishing campaigns.



## Division by Sector

Analyzing the volume of phishing pages by sector of the brand used in the scam, we observed an increase in the proportion of attacks aimed at banks and financial institutions. In the previous year, retail had a comfortable margin at the top of the list, but this was not the case in 2025.

It's worth remembering that scams using retail brands can easily adopt narratives to steal credit cards and other financial data. Therefore, a difference in the type of brand used doesn't in itself characterize a change in criminals' interests.

The 2025 data indicates a relevant shift in the focus of phishing campaigns. The **Financial/Insurance** sector recorded a 65% increase in detections, surpassing **Retail/E-Commerce**. This movement suggests that threat actors are redirecting efforts toward financial institutions, attracted by the potential for direct gain.

The Transportation sector also showed growth. These frauds exploit the delivery tracking ecosystem and the use of fake carrier pages, expanding the attack surface against consumers and companies in the sector.

**Evolution of Sectors Most Targeted by Phishing Between 2024 and 2025**

	2024	2025
Retail/E-Commerce	27.305	21.558
Banks/Financial	18.915	24.959
Technology	9.502	7.752
Food/Beverages	3.462	5.431
Transportation	3.330	3.359

↓ -21%

↑ +65%

↓ -18%

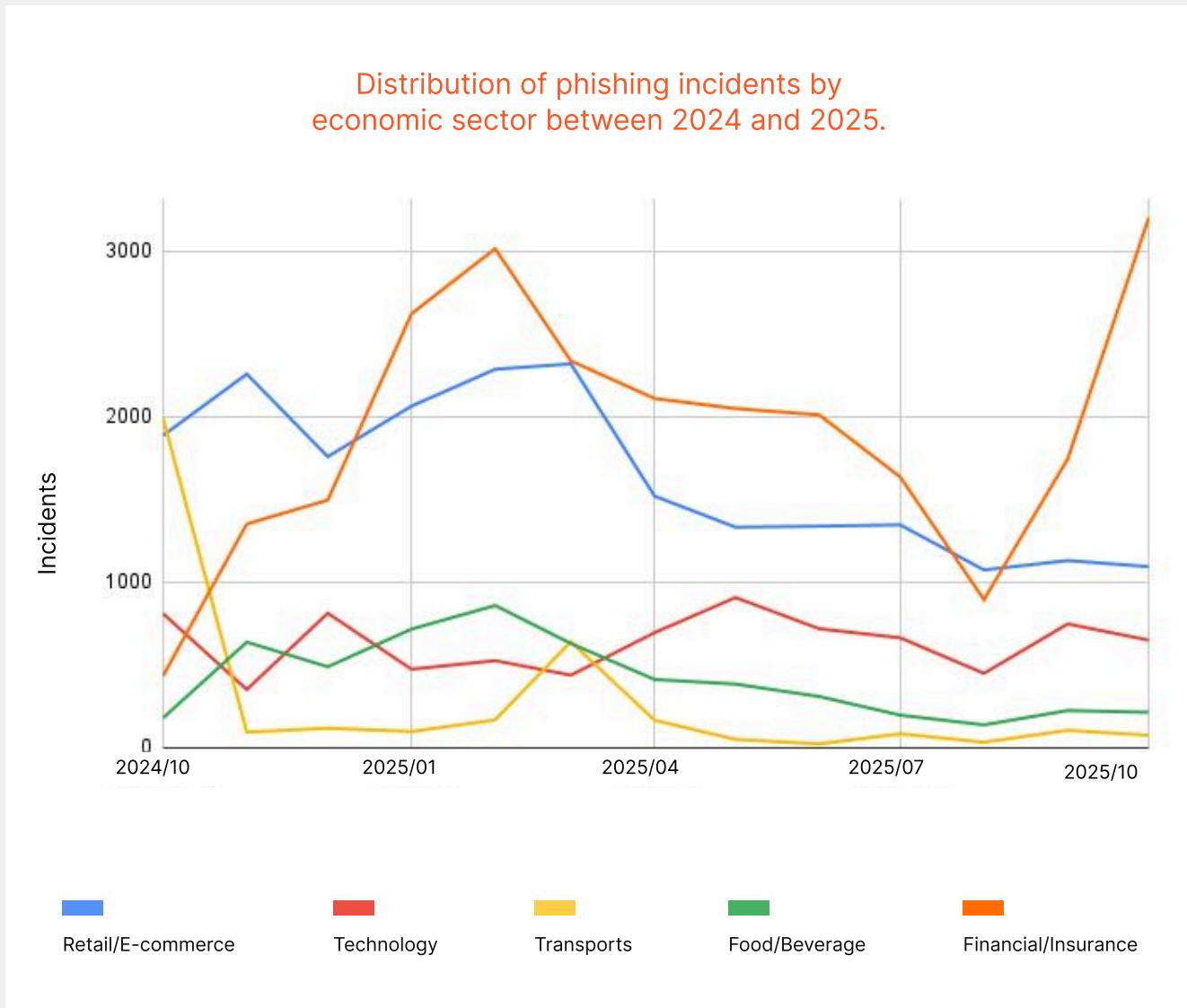
↑ +56%

↑ +0,87%

## Phishing Trends: Evolution by Sector

In the sector breakdown, a relevant change is observed in the distribution of phishing incidents. The financial/insurance segment took the lead in attack volume, surpassing retail and e-commerce, which had occupied the first position in the previous year. This reversal may be related to the increase in exploitation of corporate credentials and the use of SaaS integrations as an initial access vector. The transport and logistics sectors showed occasional fluctuations, while food and beverages maintained relative stability, with smaller volumes.

Distribution of phishing incidents by economic sector between 2024 and 2025.



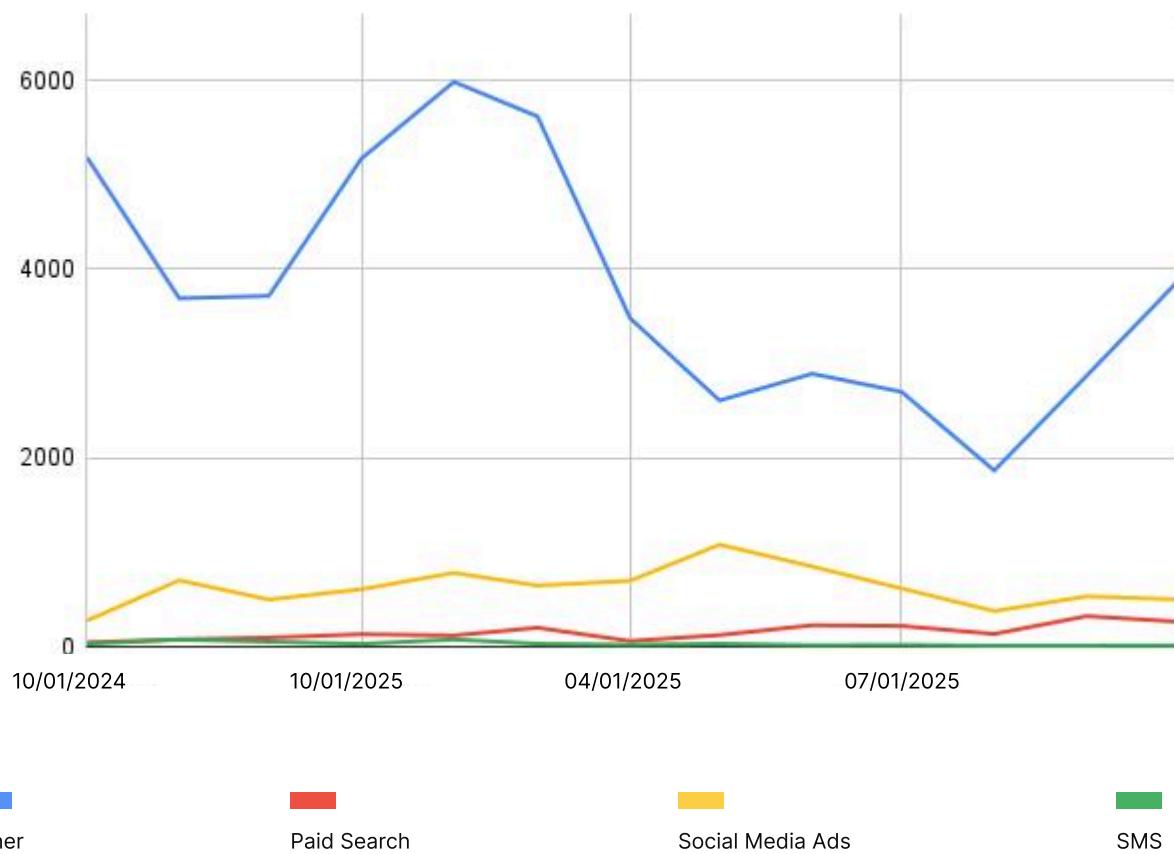
## Phishing Trends: Evolution by Attack Vector

Attack vectors showed considerable variation throughout the year. The more traditional campaigns, grouped under the "other" category, which includes fake pages and cloned sites, remained predominant but exhibited irregular behavior with peaks concentrated in the first quarter. Among specific channels, **social media ads** maintained a consistent presence, while **paid search** showed gradual growth. **SMS-based attacks** remained at low levels, though they continue to be employed in short-range campaigns targeting specific audiences.

The diversification of targets and expansion of fraud channels suggest that attackers are distributing their efforts across sectors and platforms to maximize campaign impact.

This landscape reinforces the need for broader monitoring and threat correlation approaches capable of encompassing the digital exposure ecosystem as a whole.

Monthly evolution of the main attack vectors observed between late 2024 and 2025.



## AI Accelerates Phishing: Fake Pages Created in Minutes with Tools like Lovable

Digital fraud groups have incorporated AI-assisted generation tools like Lovable to automate the creation of phishing pages with high visual fidelity. These builders allow them to replicate legitimate interfaces, banks, e-commerce providers, authentication services, in a matter of minutes, without requiring advanced technical knowledge.

The use of generative models to clone login flows, adjust persuasive text, and adapt language to the target accelerates the production and customization of campaigns, reducing the time between conception and execution. This trend consolidates phishing as a highly scalable and difficult-to-detect attack vector, especially when combined with kits hosted on legitimate infrastructure and newly registered domains.

The screenshot shows a dark-themed user interface for threat hunting. At the top, there is a search bar with the query "impersonatedBrandsHigh='Netflix' and domain=lovable.app". Below the search bar, a message states "For compliance reasons, searches are stored and may be monitored by Axur." On the left, there are buttons for "Edit columns", "Export", and "Share". On the right, there are navigation controls for "1 - 3 of 3 results". The main area displays a table with the following data:

Detection date	Reference	Domain creation date	Screenshot	Content type	Impersonated brand
07/23/2025 at 02:33 AM	<a href="https://preview--netflix-auth-guardian.lovable.app/">https://preview--netflix-auth-guardian.lovable.app/</a>	05/06/2023 at 11:03 AM		Login page	Netflix - High Impersonation Google - Low Impersonation
05/19/2025 at 03:52 AM	<a href="http://flixreviewer.lovable.app">http://flixreviewer.lovable.app</a>	05/06/2023 at 11:03 AM		Other	Netflix - High Impersonation
05/19/2025 at 02:16 AM	<a href="https://flixreviewer.lovable.app/">https://flixreviewer.lovable.app/</a>	05/06/2023 at 11:03 AM		Other	Netflix - High Impersonation

Screenshot from Axur's Threat Hunting shows phishing cases created with the Lovable tool.

## Top-Level Domain Usage

The list of top-level domains (TLDs) most used by criminals remained very similar to the previous year. The rising share of .app clearly shows how AI-powered website builders have become a go-to resource for criminals creating fraudulent pages. **Netlify, Vercel, and Lovable account for 75% of phishing cases using the .app TLD.**

Top TLDs most used between late 2024 and 2025

	2024	2025	
.com	26,612	20,921	↓ -21.4%
.online	9,147	4,861	↓ -46.9%
.site	5,062	6,392	↑ +26.3%
.shop	5,196	6,358	↑ +22.4%
.com.br	3,644	4,275	↑ +17.3%
.store	1,721	1,607	↓ -6.6%
.net	1,489	922	↓ -38.1%
.org	1,254	861	↓ -31.3%
.ru	1,017	552	↓ -45.7%
.de	928	895	↓ -3.6%
.xyz	997	494	↓ -50.5%
.app	-	1619	New
.top	-	952	New

TLDs are the suffixes of web addresses, such as ".com" (which can be used by any person or organization), ".gov" (exclusive to United States government sites), and ".uk" (country suffix).

TLD granting was quite restricted in the past, as only a few institutions were authorized to operate them, typically to represent regions or countries (such as ".br", ".de", ".jp", ".ar", among others).

Since 2012, there has been a procedure to apply for a generic top-level domain (gTLD) concession, making the creation of new suffixes more flexible. Each TLD is operated by a registry, which can choose to sell subdomains to recover the infrastructure and application costs.

Since the procedure to apply for a gTLD is expensive and quite bureaucratic, cybercriminals need to choose from existing TLDs to register a domain that serves to expand the reach of a fraud or make it more convincing.

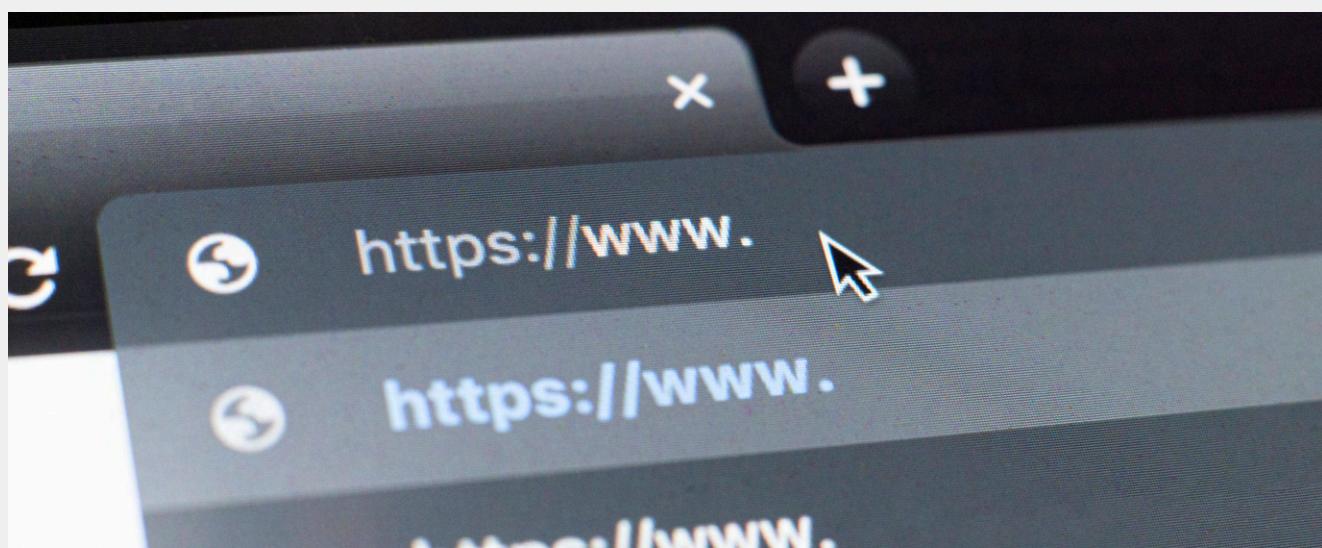
This choice is especially important for phishing sites, as the page address will likely be checked by victims. To make this choice, the scammer typically considers several elements:

→ **Domain availability:** Since short addresses, simple words, and trademarks are no longer available in traditional TLDs, criminals may try to find these addresses in newer generic TLDs or similar alternatives.

→ **Link to the fraud:** Many gTLD suffixes are thematic. A criminal may understand that some of them will make the fraud more convincing. This is one of the factors that may explain the increase in the use of the ".app" TLD, for example.

→ **Cost:** Some TLDs are more expensive than others. In cases like ".edu" and ".gov", which cannot be registered, the cybercriminal's only option is to compromise a site with these suffixes to host the fraud.

→ **Registrar policies and fraud prevention:** There are rules that all domain registrars must follow. However, there may be differences in handling specific cases that motivate a preference on the part of criminals, as this affects how long the fraud can remain active.





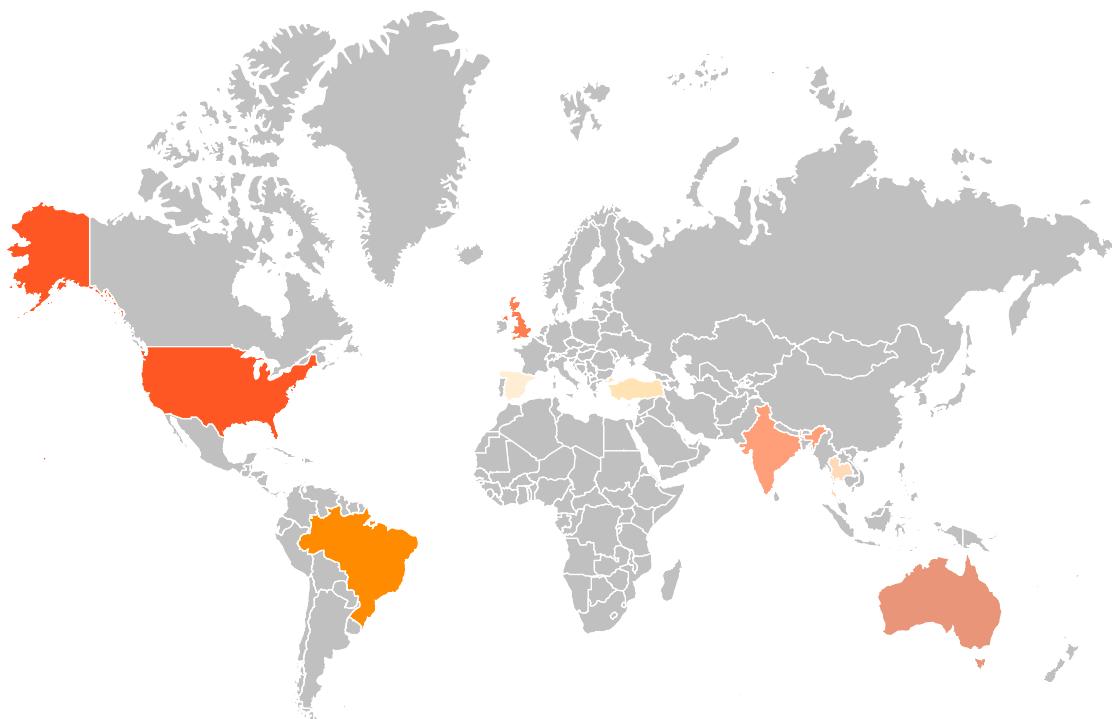
## Cards

The Axur Platform detected the breach of data from 395 million credit and debit cards.

The number of detected leaked cards in 2025 remained stable compared to the previous report period. Unfortunately, the number of leaked cards is still significant and concerning.

Thanks to the BIN (Bank Identification Number), it's possible to identify the origin of each card.

Top 10 Countries with Most Valid Cards Exposed



United States: **56.16%** | Brazil: **5.36%** | UK: **2.24%** | Australia: **1.73%** | India: **1.67%**  
Thailand: **1.32%** | Turkey: **0.74%** | Spain: **0.71%** | Israel: **0.68%** | Others: **6.49%**

In 2025, the United States continues to lead globally in leaked cards, followed by Brazil and UK.

Card theft represents a significant risk for financial institutions and e-commerce. After a card is used fraudulently, the consumer typically initiates a chargeback process, forcing the store to refund the charged amount. Since the merchandise cannot always be recovered, the store will suffer a loss from this transaction.

With Axur's data, retailers can detect the use of leaked cards and block the purchase or perform the necessary validations to ensure its legitimacy.

Verification is also especially important for payment institutions. Card exposures directly impact **financial institutions and processors** that need to validate transactions quickly and accurately to reduce losses and maintain trust with card networks.

### Real Use Case

150%  
less time in card  
validation

In 2025, fintech company **Zoop**, which provides technological infrastructure for the financial sector, integrated Axur's exposed cards database into its validation process.

The verification occurs in milliseconds and preventively blocks about 30% of transaction attempts with compromised cards, reducing operational response time by 150% and strengthening payment operations security.

### CASE STUDY

///AXUR

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

**How Zoop Reduced Fraud and Reinforced Trust with Credit Card Networks Using Axur**

**The Challenge**  
Zoop, a leading fintech in embedded financial services, needed to validate card information to prevent fraud and ensure secure transactions for their clients.

**The Solution**  
With the solution implemented with Axur and Zoop's new architecture, validation times were reduced by 150%, preventing 30% of transaction attempts with compromised cards.

**The Differentiators**  
A faster validation process with Axur and partner Axur's data integration for card validation, which takes less than 100ms to validate each card.

**The Impact**  
150% less time to validate cards.  
30% of transactions blocked at the edge.

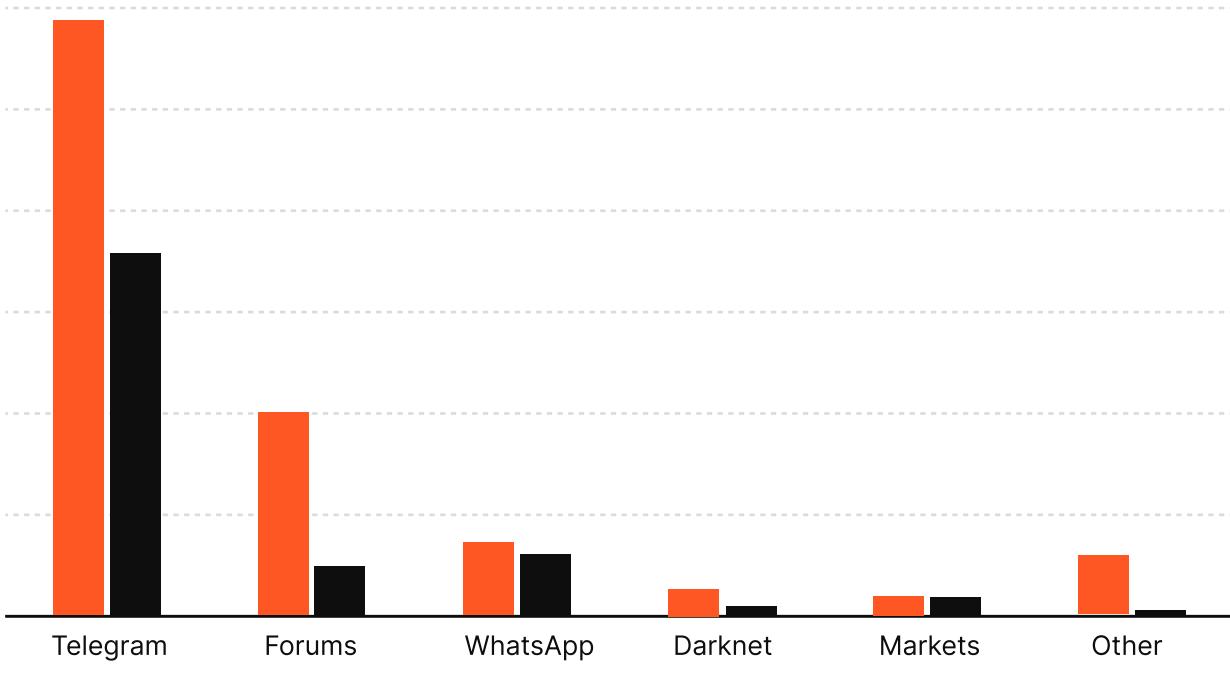


## Deep & Dark Web

In 2025, we found 496,403 suspicious communications on the Deep & Dark Web that were converted into incidents for investigation and intelligence gathering.

The cybercrime ecosystem has a series of channels that typically remain outside the visible web for most people, as they don't appear in simple search engine queries, and entry to these channels, groups, or forums is often restricted.

However, these Deep & Dark Web spaces used by criminals can be monitored to generate intelligence about the cyber threats being discussed in these locations.



Sources of incidents on the deep and dark web in 2025.

## Most Affected Sectors on the Deep & Dark Web

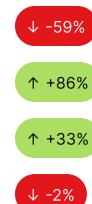
The financial sector took the lead, rising from 26.1% to 48.6% of occurrences, while retail dropped from 45% to 18.1%. This reversal reflects the growth of fraud targeting the banking and payment methods ecosystem.

The increase also suggests greater sophistication in criminal group strategies, which are exploiting more structural vulnerabilities with greater force, such as system integrations and access credentials at financial institutions.

The advance of the technology sector, from 16.8% to 22.5%, also reinforces this movement: infrastructure providers, fintechs, and SaaS platforms have come to occupy a central role in the risk chain. Meanwhile, telecommunications maintained stability with a slight reduction, which may indicate greater maturity of controls and more agile incident response.

Together, the data confirm a trend of fraud campaign migration toward targets with greater systemic impact, where the exploitation of credentials, APIs, and integrations can generate cascading effects across multiple financial services.

	2024	2025
Retail/E-commerce	45%	18.1%
Financial/Insurance	26.1%	48.6%
Technology	16.8%	22.5%
Telecommunications	4.8%	4.7%



Axur has visibility into several of these channels and conducts monitoring that transforms collected signals into incidents that can be investigated. In some situations, these signals even allow blocking an action before it actually occurs.

# Insider Detection from Dark Web Evidence

In 2025, Grupo Casas Bahia used Axur's deep & dark web monitoring to investigate evidence of corporate information leakage identified in restricted forums. Based on these signals, the cybersecurity team conducted an in-depth analysis that revealed the operation of insiders involved in extracting and commercializing internal data.

The investigation made it possible to map the leak's origin, contain the responsible group, and implement preventive controls to avoid recurrences and mitigate any reputational impact.

## CASE STUDY

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedown requests in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedowns in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedown requests in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedowns in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedown requests in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration

**AXUR**

**CASASBAHIA**

Grupo Casas Bahia strengthens business security with Axur's advanced solutions

**The Challenge**  
As digital sales and customer interactions expanded, the brand began closely monitoring its presence on social media to ensure consumers only engaged with official channels and trustworthy information. This focus helps safeguard customer experience and strengthens brand credibility in online environments.

**The Solution**  
Axur became a strategic ally in identifying and removing threats at record speed. The platform enables the Grupo Casas Bahia team to monitor, validate, and request takedowns of unauthorized content with a single click. It also offers smart automation and continuous support — including coverage across the deep and dark web.

**The Impact**  
Without Axur, responding to digital threats would demand intense manual work and long turnaround times. Taking down fake profiles or malicious ads would require an entire team dedicated solely to this task — increasing headcount, costs, and operational load. The company also wanted to go further in protecting its customers, extending its ability to respond proactively.

Tackling high-scale threats in a business with massive volume and visibility  
223 takedowns in 30 days  
100% success rate  
Median time to first notification: 3 minutes  
Over 100 fake profiles taken down every month, plus 77 cases of brand misuse  
170,000 exposed credentials handled in just 3 months, with automated resets via Axur's API integration



## Fake Profiles, Illegitimate Apps, and Fraudulent Brand Usage

No fraud reaches victims by identifying itself as fraud. Instead, they use known brands and people, preferably in plausible scenarios, so that victims believe the scam narrative.

Axur's monitoring scans the web to detect situations where a brand is used improperly to promote illegitimate content and offers, malicious apps, fraudulent profiles, and unauthorized brand use in sponsored search links.

In 2025, incidents of improper brand use registered an increase, with indications that practices related to typosquatting, cybersquatting, or similar domain registration (+1000%), and brand use in paid ads contributed to this movement.

Fraudulent brand use remains the most common incident, followed by fake social media profiles and fake apps.

Fake social media profiles can be used to deceive consumers with offers or services that don't exist.

The consumer may believe they're talking to a genuine company representative and purchase products or services that will never be delivered, creating an undesirable situation for the company, which lost a customer, and the consumer themselves, who lost their money.

Brand use in paid search also increased, from 1,282 to 5,499 records, which corroborates the trend observed by Axur researchers that scammers have increasingly sought to use online advertising to give an appearance of legitimacy to frauds.

Fake apps for mobile devices are a serious threat especially for financial sector companies, as these apps can use the brand of banks and financial institutions to request victims' data and credentials.

In 2025, fake mobile apps appear to show a significant decline. However, as we showed in the TLD analysis, this movement may be related to a tactical migration by threat actors, who began to exploit URLs hosted on .app domains more intensively.

	2024	2025	
Fraudulent brand use	204,060	262,302	↑ +28.5%
Fake social media profile	126,432	132,349	↑ +4.7%
Fake mobile app	17,621	11,561	↓ -34.4%
Similar domain name	248	2,954	↑ +1,091.1%
Brand use in paid search	1,282	5,499	↑ +328.9%



## Executives and VIPs

We detected over 19 thousand incidents involving the image and information of Executives & VIPs.

Criminals can take advantage of the image and information of executives and other well-known personalities in various scenarios.

Executive data can fuel Business Email Compromise (BEC) scams, in which the scammer sends fake emails to other company employees or business partners. If the recipients believe the message, they may follow dangerous instructions and even conduct improper financial transactions.

This personal information can also be used to craft frauds against the executives themselves, creating a risk for the organization and its internal systems.

We detected about 2000 incidents involving the exposure of credentials from executives or senior management at companies.

Meanwhile, executives' images in fake profiles and social media content can be used to increase the credibility of some product or service. On this issue, we have observed a regionalization of frauds involving the endorsement of investment opportunities, using the image of well-known executives in the country, such as Elon Musk.

The improvement of artificial intelligence tools has facilitated the creation of convincing deepfakes, whether in static images or videos. As a result, many people may have difficulty identifying that the content is fake. In certain incidents, the fake content may only be in the photo caption, distorting the image's context to mislead the victim.

Threats to Executives	Quantity
Fake social media profile	8,759
Personal information exposure	8,572
Credential exposure	2,460
Card exposure	27
Total	19,818



## Agentic Takedown: A New Stage in Response Automation

By October 2025, 343 thousand cases of fraudulent content had already been removed thanks to Axur's automated notifications.

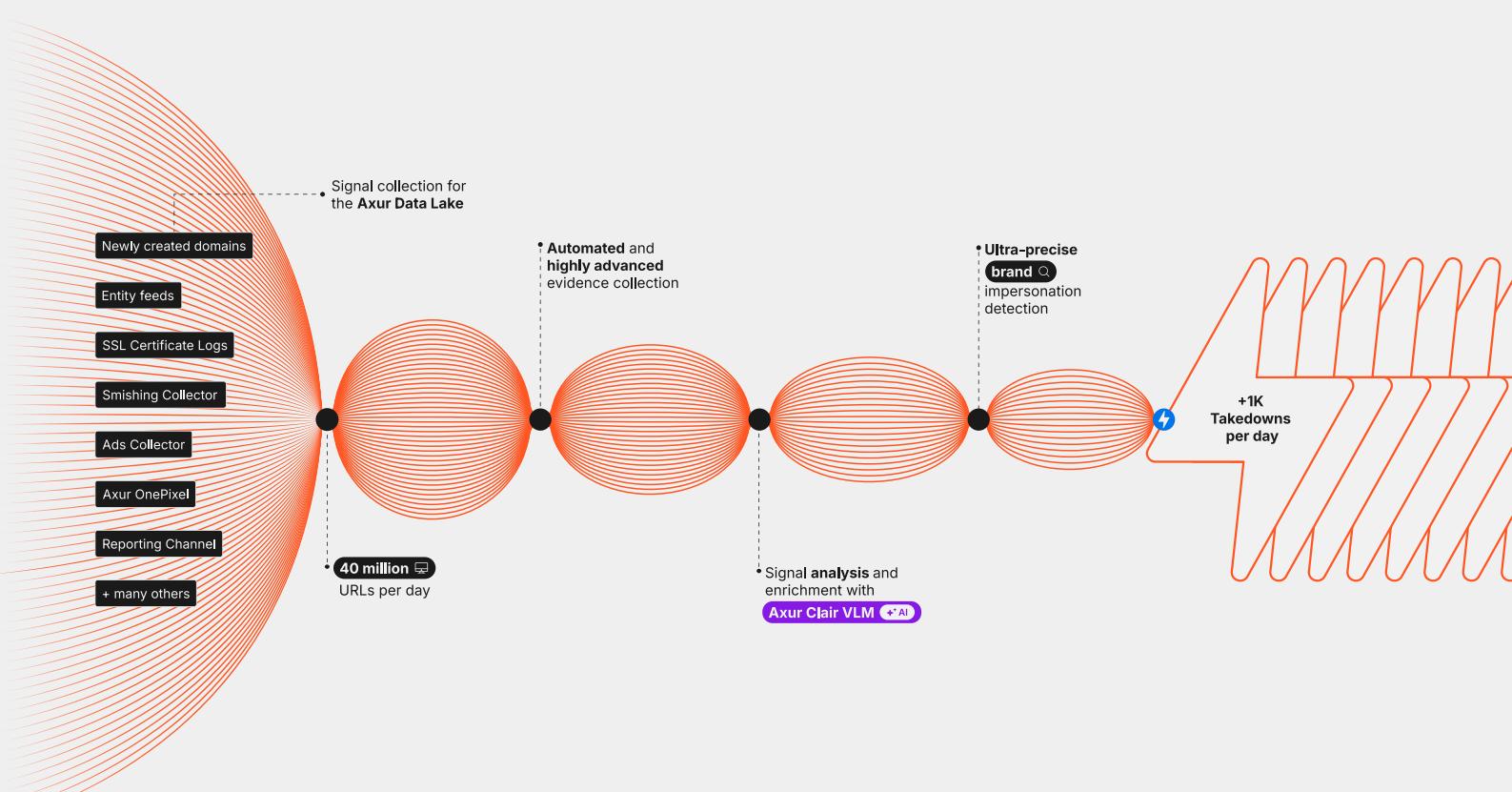
The volume, sustained by AI-based flows and evidence validation, consolidated the maturity of a process that today evolves toward a new paradigm: **agentic takedown**.

Unlike traditional automation, which executes pre-programmed tasks based on fixed rules, agentic takedown introduces autonomous decision-making capability. The Clair model, **Cyber Lens for Anomaly and Impersonation Recognition**, based on Vision Language Model (VLM) architecture, interprets both textual content and visual elements of each page, identifying fraud patterns, impersonation indicators, and phishing signals even when the brand is not explicitly mentioned.

From this contextual analysis, the system is capable of defining the appropriate action, notifying the responsible provider, and tracking responses, operating continuously and with minimal human intervention. This is an **agentic** model, in which AI not only detects and reports but decides and executes.

The differentiator lies in the integration between multimodal analysis and automated decision-making, allowing Clair to conduct the complete response cycle, from threat identification to takedown execution, with traceability and consistency.

It's an evolution that brings digital security closer to a truly risk mitigation model, making processes faster, more accurate, and sustainable over time.

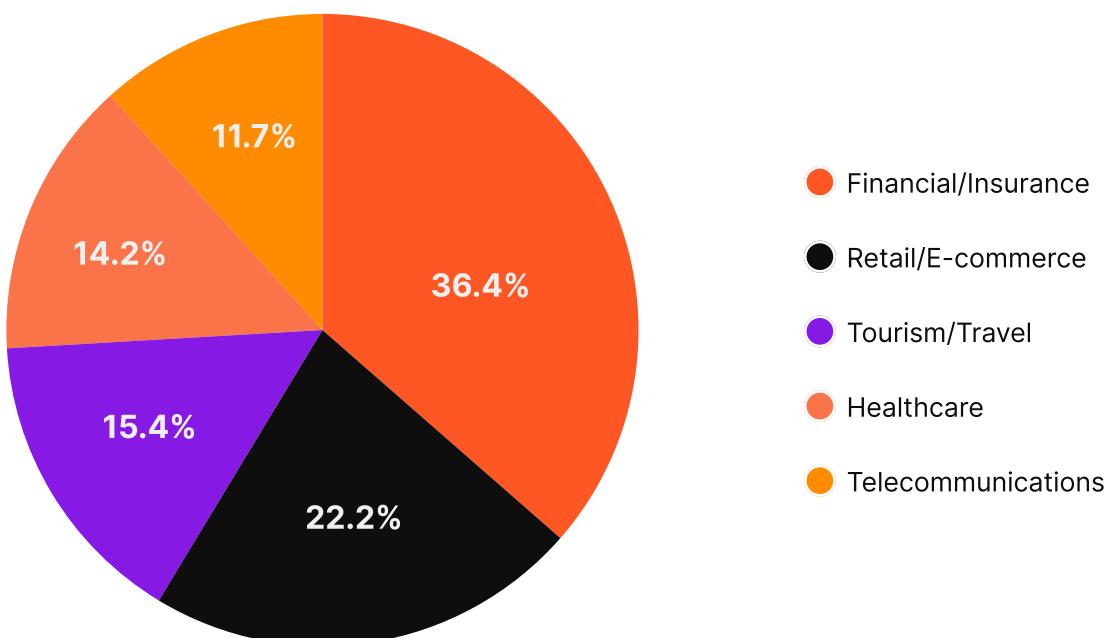


## Takedowns by Sector

The distribution of takedowns by sector shows that the financial sector accounts for 36.4% of removals, remaining the primary target, a result consistent with the increase in fraud observed in the segment throughout the period. Next come retail and e-commerce (22.2%), travel and tourism (15.4%), healthcare (14.2%), and telecommunications (11.7%).

The predominance of the financial sector reflects both the high economic attractiveness of banking fraud and the greater detection and response capability of institutions, which translates into more takedown actions conducted during the period.

Distribution of takedowns by sector  
between late 2024 and 2025.



## Most Notified Platforms

In 2025, we removed over 70 thousand fake profiles through notifications to Meta, responsible for Facebook, Instagram, WhatsApp, and Threads networks.

## Time to First Notification

Time to first notification is one of the most critical indicators in the incident response cycle, as it determines how quickly an identified threat reaches the mitigation stage.

Data from the Axur platform shows that the first notification is issued between three and five minutes (median time) after the takedown request. The shortest time was observed in cases of similar domain name (3.05 minutes) and unauthorized distribution (3.02 minutes).

Reducing the interval between detection and first notification means decreasing the exposure window, the period during which the threat remains active and potentially accessible to victims.

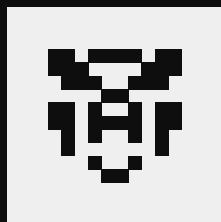
At scale, this difference of a few minutes can represent thousands of avoided accesses to fake pages or fraudulent profiles, reinforcing the importance of automated monitoring and intelligent alert prioritization.

Type	1st notification
Phishing	5.07 minutes
Fake social profile	3.22 minutes
Similar domain name	3.05 minutes
Unauthorized distribution	3.02 minutes
Unauthorized sale	3.78 minutes

# Cyber Threat Intelligence

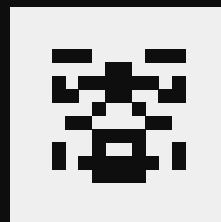
Through Axur's Cyber Threat Intelligence module, it's possible to track the most relevant threats and understand the threat landscape for a specific period, such as the 2025 timeframe.

## Malicious Actors



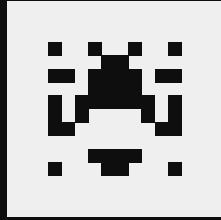
Scattered  
Spider

Scattered Spider is a Western group that gained significant attention in 2025 after several successful attacks against companies in the United Kingdom. The group is known for using exposed credentials and phishing attacks (primarily voice-based) to obtain these credentials or weaken multifactor authentication. After forming an alleged alliance with ShinyHunters and LAPSUS\$, the group also conducted a successful campaign of attacks on Salesforce environments, combining phishing and exploitation of third-party integrations.



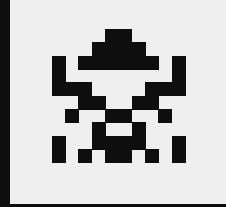
Qilin

Qilin is a gang that operates in the ransomware-as-a-service (RaaS) model. Each affiliate can choose their own method to gain initial access to targets, which means there is considerable diversity in the techniques used. The group apparently consolidated activities that previously belonged to other groups, making it possibly the most active name in the ransomware category at the end of 2025.



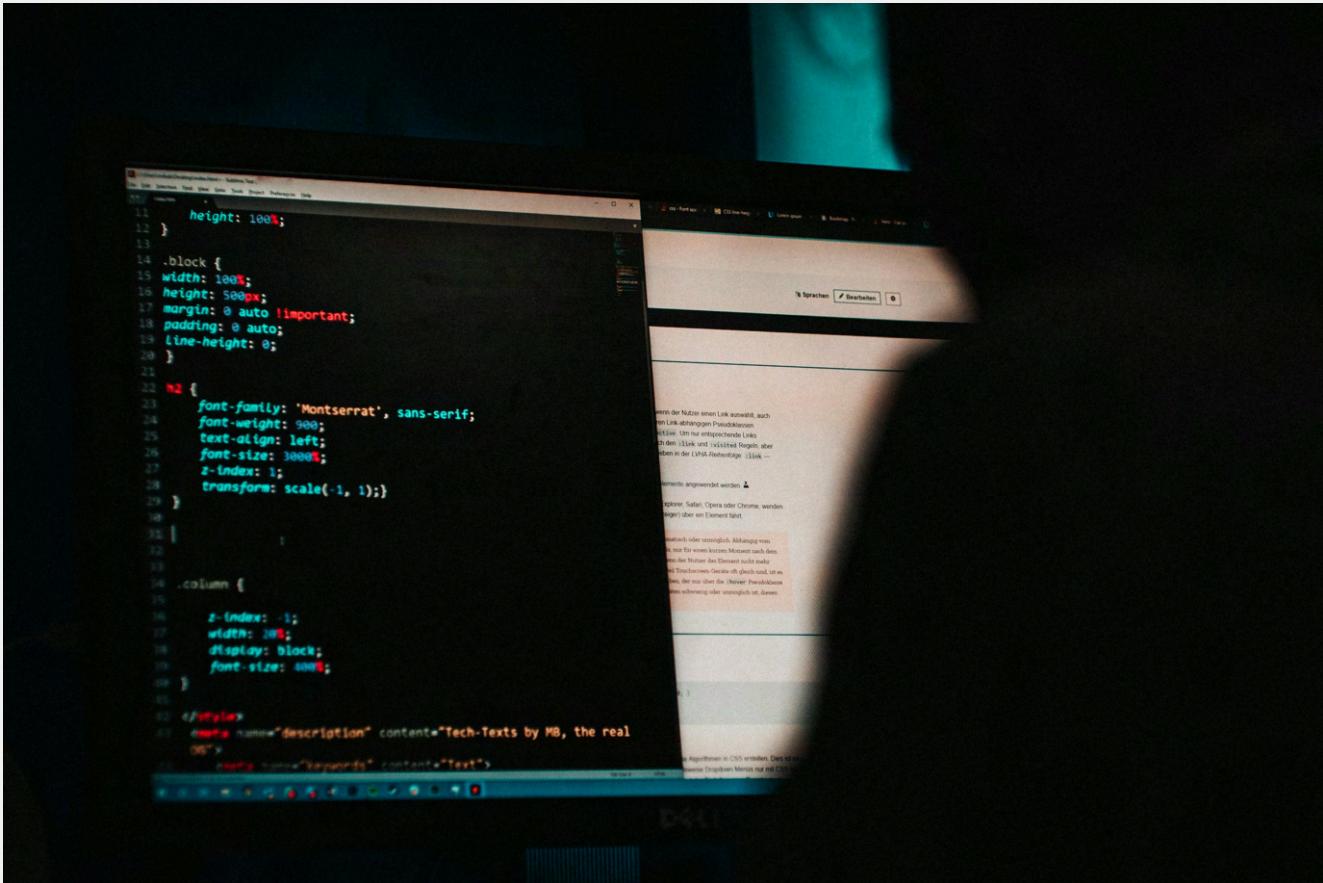
## RansomHub

Considered a reincarnation of the Knight ransomware. It quickly became one of the most prominent groups, especially after police actions against LockBit3 resulted in a significant drop in its activity. The group claimed over 210 new victims, according to the FBI, including companies such as Kawasaki Motors and American communications provider Frontier Communications, in addition to leaking Change HealthCare data following the BlackCat/ALPHV attack, but reduced its activities in April.



## Salt Typhoon

Many experts believe that Salt Typhoon is associated with the Chinese government. It stood out in 2025 due to a series of attacks that began in 2024, when the press reported that several telecommunications companies in the United States had been compromised by Salt Typhoon. This group is notorious for attacking critical infrastructure targets (such as telecommunications and energy) and government agencies, typically with the purpose of obtaining information about third parties.



## Featured CVEs

The main vulnerabilities of 2025 practically tell a story: they are flaws that begin in network edge devices and migrate to endpoints, where the attacker then obtains administrative access to consolidate their presence in the corporate network.

### CVE-2024-21762



9.8

This CVE refers to one of several vulnerabilities exploited in edge devices throughout 2025. This flaw was present in some versions of FortiOS and allows command execution from specific requests.

### CVE-2024-55591



9.8

This CVE refers to another vulnerability in FortiOS. When successfully executed, the attack bypasses the authentication process and grants administrative permissions to the attacker.

### CVE-2025-53770



9.8

Technical information about a SharePoint vulnerability was leaked to some attackers who exploited the gap in zero-day mode, that is, before the patch was distributed by Microsoft. Several companies were attacked by hacker groups associated with China.

### CVE-2025-29824



7.8

This CVE addresses a Windows vulnerability with privilege escalation impact. It can be used by attackers to facilitate lateral movement within a corporate network after the breach and to install malicious software that is harder to detect and remove.

### CVE-2023-46805



8.2

Another vulnerability that bypasses the authentication process in edge devices. The affected system is Ivanti Connect Secure (ICS), a remote access solution (VPN). This vulnerability can grant initial access to the corporate network.

### CVE-2024-21887

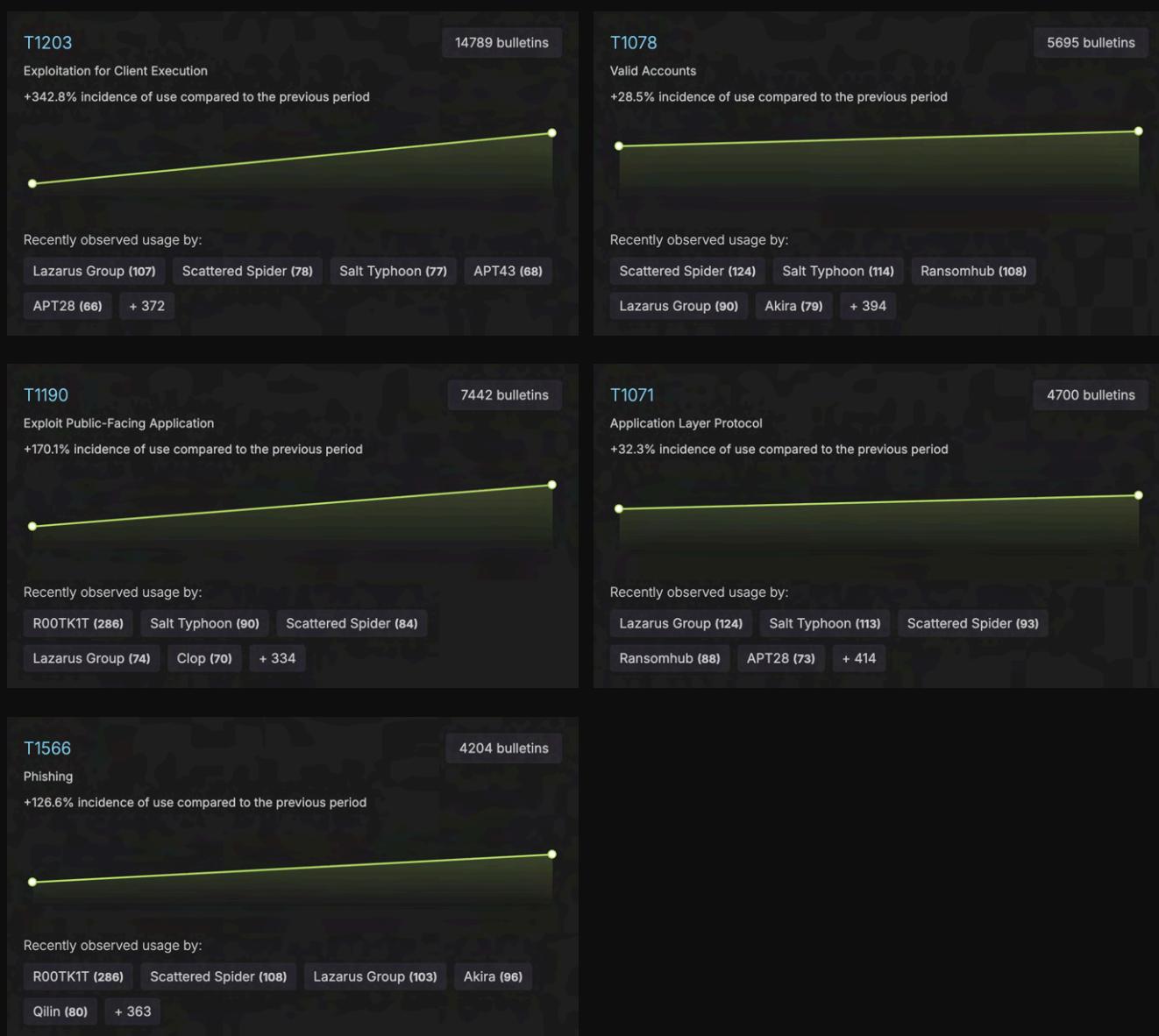


9.1

Yet another vulnerability in Ivanti Connect Secure. In this case, the flaw is in the processing of specific requests, allowing the attacker to execute arbitrary code on the system.

## Featured TTPs

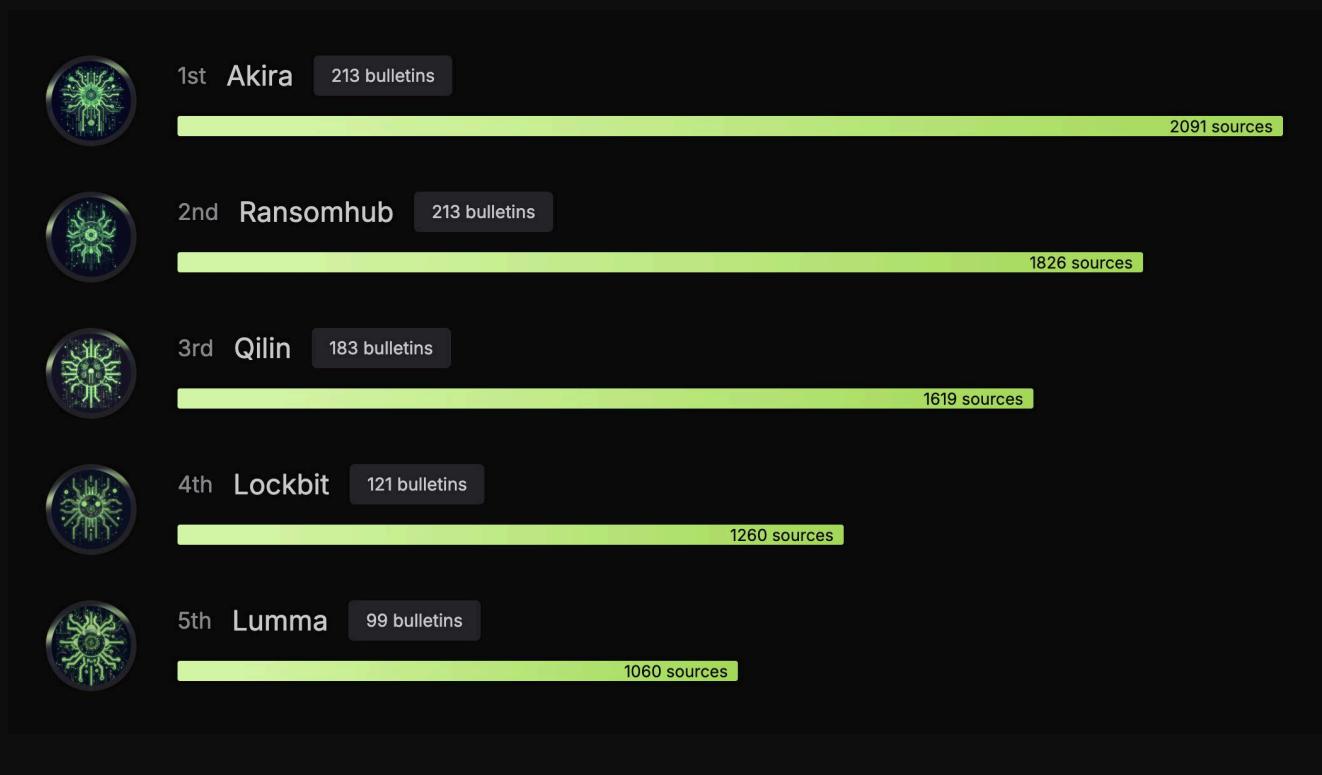
The most recurrent techniques in 2025 reflect the increasing sophistication of attacks: they exploit vulnerabilities in exposed or client applications to achieve code execution and initial access (T1190, T1203), advance through the use of valid credentials (T1078) to maintain persistence and escalate privileges, and consolidate with disguised communications (T1071) and targeted phishing campaigns (T1566) that ensure control and lateral movement within the corporate network.



## Featured Malware

The most active ransomware groups in 2025 reinforce the consolidation of the “as a service” model. Akira and LockBit maintain a high volume of double extortion attacks, exploiting valid credentials for initial access, while Ransomhub emerges as the successor of previous operations, expanding its focus on leaking high-value data.

Qilin stands out for the sophistication and customization of its code, which hinders defensive analysis, while Lumma Stealer, operating under the MaaS model, focuses on stealing and reselling credentials, fueling the initial access ecosystem.



Axur Platform Insight

## Cyber Threat Intelligence

The current complexity of cybersecurity requires teams to filter, correlate, and prioritize information amid massive volumes of data. Axur's CTI was developed precisely to solve this challenge, combining AI algorithms and a language model trained in cyber threats to transform fragmented data into curated and contextual alerts.

Daily, the system analyzes hundreds of sources, such as reports, feeds, specialized groups, and news, and identifies what is truly relevant for each environment, mapping threats and vulnerabilities according to each client's attack surface.

# Geopolitical Landscape

## Geopolitical Landscape Overview

International agreements and partnerships were weakened in 2025 by a combination of challenges.

On one side, we have regulatory barriers: trade tariffs, export restrictions, financial sanctions, realignment of priorities, and new legislation that came into effect.

On the other, we have the concrete challenges that motivated these measures: cyberattacks against critical infrastructure, concerns about China's dominance as a supplier of parts, equipment, and products in strategic sectors, the dispute over technological leadership in artificial intelligence, the war between Russia and Ukraine, and the escalation of conflicts and uncertainties in the Middle East.

These factors contributed to the view that protecting specific companies or sectors is not enough, since they depend on an entire supply chain. Diversity and redundancy would not be viable solutions, since everyone sees themselves interconnected by a limited number of software developers and IT platforms.

This perspective sparked debate about digital sovereignty, shaping a new wave of ideas and investments in IT infrastructure.

Politics and global tensions have always impacted business, especially for companies whose operations are not limited to the borders of a single country. With the internet and digital services, we have a scenario where almost everyone depends on software, equipment, and technology services enabled by a complex web of global suppliers.

Under these circumstances, the relationship between geopolitical tensions and challenges in cybersecurity tends to expand.

Evidence of this appeared in a World Economic Forum survey published in early 2025 in which 60% of companies said they believed geopolitical tensions impacted their cybersecurity strategy.

The relevance of these tensions varies for each company. Therefore, it's worth listing the cybersecurity-related topics that stood out throughout the year and analyzing what consequences they brought to different sectors of the economy.

## Attacks on Critical Infrastructure

The concern with cyber resilience in critical infrastructure elements (energy, telecommunications, water, and logistics) is not new, but the methods used to assess sector maturity and improvement proposals have advanced significantly.

In 2024, the Biden administration initiated a review of cranes used in American ports with the objective of replacing models manufactured in China. Regulators later cited the presence of undocumented electronic components with external connectivity as one of the justifications for this measure. In parallel, government security agents indicated that Chinese invaders were infiltrated in the IT systems of several companies in critical sectors, without giving specific examples.

In September 2024, the press, initially through the Wall Street Journal, reported that Chinese hackers linked to **Salt Typhoon** gained access to several telecommunications carriers. Despite the incident's severity, what marked this attack was the invaders' interest: the carriers' customers.

In 2025, we witnessed the unfolding of this campaign. Other countries began publishing notes and bulletins warning about Salt Typhoon activity in telecommunications carriers in their territory, often exploiting flaws in so-called **edge devices** from brands like Cisco, Ivanti, and Palo Alto Networks.

In August, the FBI warned that more than 80 countries were attacked by Salt Typhoon.

In the same month, the agency warned about activity from another hacker group, this time associated with Russia, which would also be focused on critical infrastructure operators.

Both China and Russia deny involvement with the attacks. Whether countries are directly involved or not, the breaches generate tensions and fears with clear consequences for the companies involved.

An example occurred after a ProPublica report denouncing the involvement of Chinese engineers in Department of Defense contracts, forcing Microsoft to promise it would no longer use these teams.

The idea of "nationalizing" services for national security ended up also reaching proposals to the American legislature. Congressmen examined rules for purchasing equipment and even for call centers, all with the potential to impose barriers to outsourcing.

At the same time, government agencies in several countries have been structuring cybersecurity assessments. In December 2024, the European Union Cybersecurity Agency (ENISA) launched its first report on the "state of cybersecurity" in the bloc.

The focus of these measures tends to be critical infrastructure and some government agencies. However, they are already being extended to companies that provide services to protected sectors.

## Expert Commentary



Sérgio Costa

Researcher at  
Axur Research Team.

When analyzing hacktivist groups in the context of the conflict involving Israel, Hamas, and Iran, the groups are increasingly united by a common cause and possibly conducting coordinated actions, with a growing tendency to target critical infrastructure.

Despite this, classic DDoS attacks are still prevalent. Some groups are citing the development of ransomware, which can serve as a source of financial support for their actions. The line between hacktivism and state-sponsored activities is becoming increasingly blurred, raising doubts about the true motivations of certain groups.

## Regional Conflicts

The war between Russia and Ukraine creates a unique situation for cyberattacks. Successful actions are even celebrated by channels that distribute news of the conflict, eliminating much of the doubt about their origin.

Notorious attacks were carried out against telecommunications carriers in Ukraine (Kyivstar) and Russia (NodeX, Lovit, Beeline, Rostelecom). Many of the incidents involve DDoS and are carried out by so-called "volunteer" hackers.

Another specific scenario is the Middle East, with tensions primarily involving Israel, Hamas, and Iran.

Iran's Minister of Intelligence even announced that country agents had infiltrated the Israeli nuclear program. Generally, admissions of this nature are rare, and the doubt is no longer about the attack's origin (as occurs in espionage operations that are not acknowledged), but rather about the veracity of the facts narrated by the attacker.

There was also an escalation in tensions between India and Pakistan, with four days of armed conflict in May. During this period, Pakistan announced a cyberattack campaign against India to bring down services and destroy files. Hostilities ended with a ceasefire agreement.



## Supply Chain Challenges

Attacks linked to geopolitical tensions are not always the only ones using a particular strategy, but it's common for them to adopt these known strategies with a different purpose or with more sophistication.

This is no different for supply chain attacks. While third-party attack campaigns carried out by criminals seek corporate data and look for a chance to extort victims, attacks on telecommunications carriers aim to collect information about targets of geopolitical interest.

In addition to attacks on telecommunications carriers in dozens of countries, there are reports that internet providers in Moscow were also attacked to facilitate espionage of embassies installed in the Russian capital.

Unlike criminals, who seek the most profitable and vulnerable targets, government-sponsored espionage attacks can study a target more calmly and find less exposed gaps.

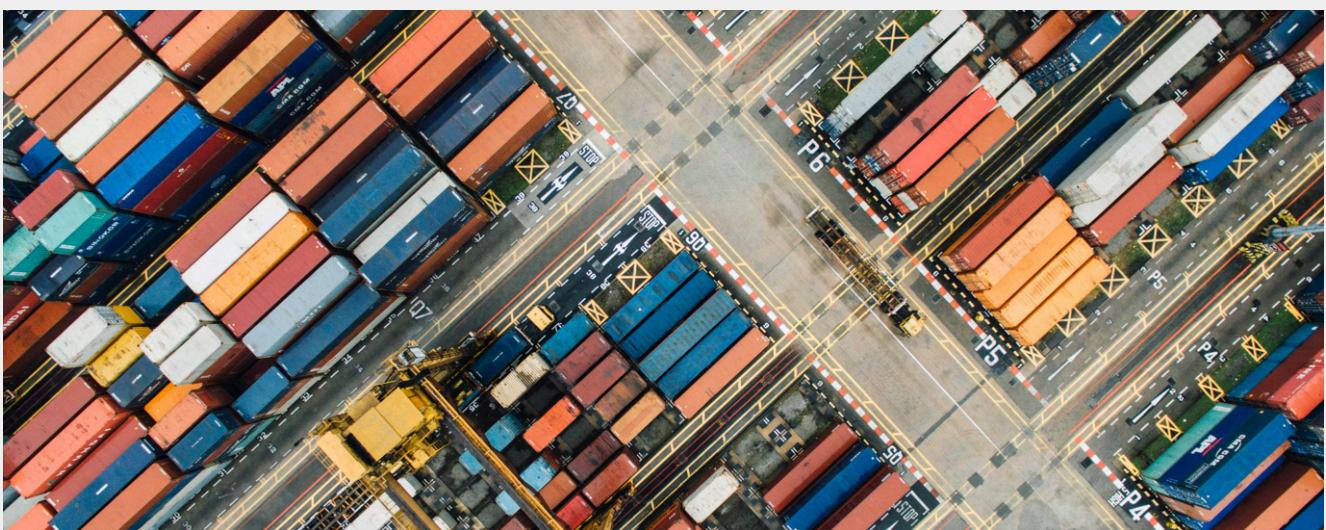
Critical infrastructure operators are a valuable target and act as a "supplier" for a large portion of companies and individuals, which helps explain these actions. However, it's worth remembering that the SolarWinds incident was also attributed to a government-sponsored group (Russia).

Therefore, it's fair to conclude that any private company providing services to targets of geopolitical interest can become a target of these attacks.

A notable development from these episodes is the imposition of trade barriers and contractual restrictions. Chinese manufacturers such as Huawei and ZTE are already prohibited from selling products in the United States, while others are under threat. Similar rules exist in Europe and Australia covering network or security devices, such as cameras.

The idea is to avoid a scenario in which authorities in these countries decide to distribute compromised software or sabotaged hardware. The operation of explosive pagers in the Middle East had already demonstrated this risk in 2024.

More recently, we have seen cases such as impediments to Chinese engineers in U.S. government contracts and Microsoft's decision to reduce Chinese access to information from the Microsoft Active Protections Program (MAPP), a platform that provides advance information about vulnerabilities that will soon be patched.



Microsoft's decision to limit Chinese access occurred after a SharePoint vulnerability shared through MAPP was exploited before the patch was distributed. With the flaw uncorrected, hackers (who would be Chinese, according to incident analyses) gained easy access to hundreds of companies.

China is the main target of these measures, but the Asian country is also working to no longer depend on American software and hardware. The Chinese government even recommended that local technology companies not purchase Nvidia's H20 chips, which were developed to circumvent AI hardware export restrictions.

There are, however, a series of more neutral measures aimed at increasing cyber resilience, such as the adoption of Software Bill of Materials (SBOMs) and other third-party risk management methodologies.

At the same time, lawsuits have been attempting to dismantle the idea that it's possible to outsource risk, holding the contractor responsible for not supervising work performed on their behalf. These measures aim to create a scenario in which companies themselves demand greater security concern from their suppliers, which contributes to cyber resilience across entire sectors of the economy.

## The \$1.5 Billion Theft

Many government-sponsored attacks are carried out for espionage purposes. However, North Korean hackers diverge from this pattern, acting primarily to obtain resources and finance the regime.

In March, cryptocurrency exchange ByBit suffered a cyberattack from Lazarus, a notorious North Korean group. The action, which was considered the largest theft in history, resulted in the diversion of \$1.5 billion in funds from the exchange.

The attack was possible because the invaders compromised a ByBit supplier, Safe {Wallet}. The first target of the attack was a Safe engineer who, according to some evidence, may have been a phishing victim. With access to this engineer's system, the invaders then obtained a key to Safe's cloud storage to tamper with JavaScript code on its platform. The code compromised a ByBit wallet.

This incident illustrates the technical complexities of supply chain attacks, the persistence of government-sponsored hackers, and how outsourcing risks often exceed the limits imagined by risk management methodologies.

## Digital Sovereignty and Resilience

The concept of "digital sovereignty" is not exactly new, but it was not mere coincidence that investments in national and sovereign data centers were announced in the same year that the U.S. government decided to acquire part of Intel.

Essentially, the idea of digital sovereignty advocates that a country has independence to handle its IT needs, both in terms of infrastructure and management and regulation.

Countries that have some cutting-edge semiconductor manufacturing capacity are taking steps to strengthen the sector's production chain or attract new investments. In the United States, this began in 2023 with the CHIPS Act.

Already in 2025, Japanese memory manufacturer Kioxia announced it would disconnect third parties that could not achieve a satisfactory score in a security assessment, possibly reflecting new demands from customers and regulators.

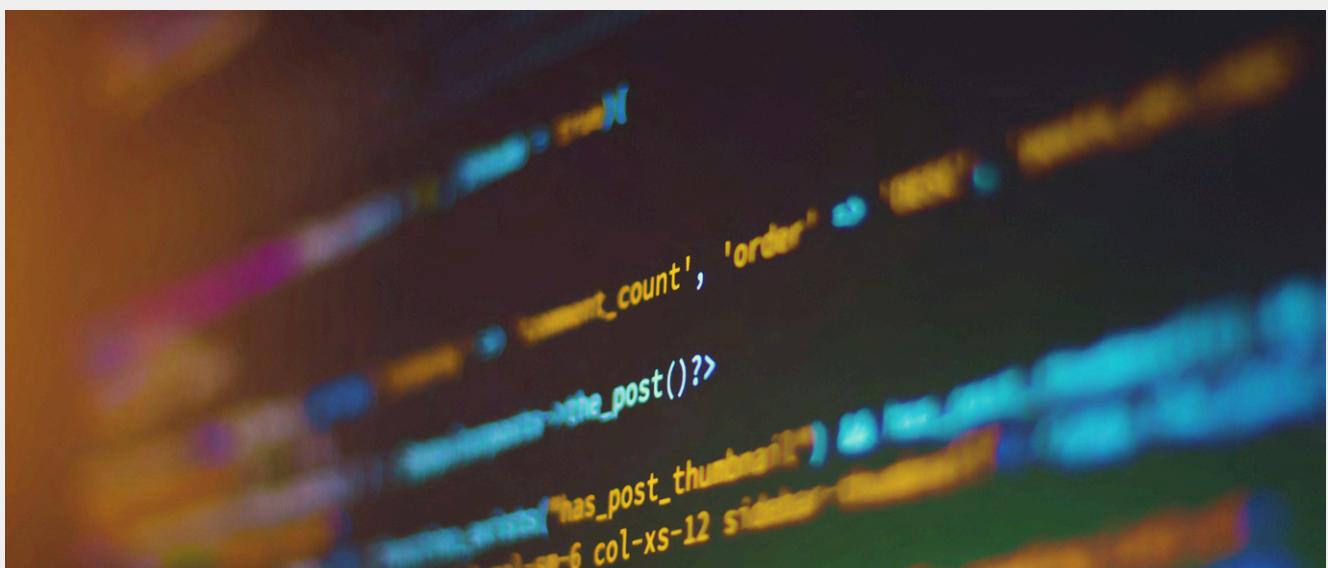
Meanwhile, the United States assumed control of 10% of processor manufacturer Intel, a rare direct intervention by the U.S. government that helped stabilize the company's market value.

But given the complexity of semiconductor manufacturing, many countries are unable to replicate the IT infrastructure production chain, even with strategic allies. Therefore, an alternative is to ensure the presence of assets on national territory and the capacity for management and regulation.

With the approval of the CLOUD Act in 2018, critics questioned the independence of American providers, pointing out that they would be forced to comply with orders and deliver information in disagreement with local legislation. With the migration to the cloud, American influence ceased to be limited to specific services such as email or chat and placed all IT infrastructure under external jurisdiction.

During the coronavirus pandemic, the cloud was the natural path for companies to continue operating with remote work and avoid purchasing hardware, which had elevated prices due to the suspension of factory operations and demand for equipment.

This consolidation reinforced concerns associated with the CLOUD Act. However, the advancement of artificial intelligence, with its high computational requirements, brought an even more urgent element to the topic.



A notable fact in 2025 was the temporary suspension of an International Criminal Court prosecutor's email address in response to a U.S. government sanction. Since the email was a Microsoft cloud service, the episode raised questions about privacy and how foreign cloud providers would respect European laws.

American providers reacted and committed to sovereign infrastructure, but could not deny that they were subject to decisions by the U.S. government and courts. This means they would indeed have to hand over data to American courts, even if the data were stored in European territory.

With this message, some companies announced new investments in sovereign infrastructure in Europe, eyeing the government market and demand for more legal certainty.

This movement is not restricted to Europe. China has similar initiatives to reduce dependence on American hardware and software.

## Consequences for Cybersecurity

Viewed in isolation, digital sovereignty seems to be a political and abstract issue. However, this topic is linked to governance, national security, and cyber resilience issues.

From a resilience standpoint, the consolidation of IT infrastructure in just a few providers brings significant risks, since all services tied to these providers can suffer interruptions or violations simultaneously. Risk management is also made more difficult, since mechanisms to compensate for this systemic risk will be more complex.

Depending on priorities and methods, mitigating the risks of a widespread cyber blackout may be more expensive than funding distributed infrastructure.

The topic of systemic risk is linked to another subject closer to companies' daily operations: the supply chain and third parties. In addition to computers and software, data centers need suppliers for cooling, energy, and connectivity services, and all of this must be factored in for reliable infrastructure.

In this sense, supply chain incidents can heat up the digital sovereignty discussion to the same extent that regulation of this topic can impact risk management tied to suppliers.

Unfortunately, there is no way to predict the future, especially given the current geopolitical instability. It's possible, for example, that the digital sovereignty topic will follow a more political path, with multilateral agreements and international collaboration mechanisms to protect each country's jurisdiction.

On the other hand, it's also possible that it will unfold into actions with direct impact on business and cybersecurity strategy. An example is the creation of incentives for adopting software, hardware, and infrastructure dedicated to improving cyber governance.

# Trends

## AI Agents

The vision of artificial intelligence performing actions autonomously has always been present. However, early products with this concept had a somewhat experimental character, both due to their limited utility and the risks of leaving AI in charge of making critical decisions.

AI agents matured throughout 2025 with the availability and improvement of dynamic products aimed at all market segments. Some of the fastest advances were observed in software development tasks, where AIs began finding bugs and vulnerabilities along with their respective reports to communicate them to developers.

**The popularization of the term "vibe coding" reflects this trend**

As expected, similar innovations emerged in attack techniques. Researchers have demonstrated ways to exploit AI interpretation that combine malicious prompt injections and APIs to produce undesired results.

The risks include vulnerabilities mapped shortly after the launch of browsers like Perplexity Comet and OpenAI's ChatGPT Atlas.

One of the attacks disclosed against Comet used steganography, invisible text embedded in web pages, which is read by the browser's OCR engine and sent directly to the AI system without validation. This enables attackers to execute unauthorized actions, such as data theft, account access, and corporate system compromise.

Meanwhile, OpenAI's browser was vulnerable to persistent injection of malicious commands into the assistant's memory, enabling arbitrary code execution and privilege escalation. Both cases show that agents also become a critical attack surface for enterprises.

**Due to the potential of AI agents, many companies may begin looking for ways to integrate them into their workflows, bringing the entire technical discussion about these agents into the corporate environment and therefore creating challenges to protect these systems.**

The adoption of agentic AI within organizations isn't just about experimentation; it represents an operational paradigm shift. As they evolve from copilots to autonomous systems with decision-making and execution capabilities, these agents directly integrate into the response cycle: detect, decide, and act.

This autonomy requires a solid governance architecture based on constraints, approvals, isolation, and audit trails that ensure traceability and reversibility of actions.

Companies intending to incorporate autonomous agents need to align machine identities, least privilege policies, and human oversight mechanisms to prevent improper executions or unauthorized escalations. The risk isn't only in model hallucinations, but in executing valid commands in wrong contexts, which demands real-time observability and audit metrics.

Furthermore, the spread of agents outside corporate control, driven by shadow IT, expands the exposure surface. Even without official integration, these agents can interact with critical systems or sensitive data, making it essential

to use dynamic identity controls, environment isolation, and continuous monitoring of interactions between agents and corporate APIs.

In 2026, security maturity will be defined by the ability to balance autonomy and control, allowing AI to act with agility, but within verifiable, auditable, and reversible limits.

Cybersecurity teams will need to stay alert to these movements to provide the necessary support, aiming for conscious and secure use of these agents to strengthen the business.



## Use by Malicious Actors

If we have "vibe coding," we also have "vibe hacking." AI models can detect vulnerabilities to make software more robust, but criminals can use the same idea to find new vulnerabilities with the intent to exploit them.

Similarly, criminals can use AIs to facilitate the development and adaptation of malicious code, or to restructure artifacts with the intent of evading detection by security tools, such as EDR, XDR, spam filters, and IDS.

AI agents and their identities can also be exploited by criminals who have gained access to the corporate network, creating a channel for lateral movement that won't necessarily be limited by traditional network segmentation.

As AI use grows among attackers and within companies, the need to adopt AI as an ally in cybersecurity becomes increasingly clear.

There are many cybersecurity tasks that don't receive proper attention today, mainly due to the difficulty of prioritizing alerts and auditing events.

This causes many alerts to be ignored or analyzed only superficially, including in SOC environments.

Only 9% of organizations monitor 100% of their attack surface (IBM) and 28% of cybersecurity professionals use AI to reduce false positives.

(ISC2 2024 Cybersecurity Workforce Study).

For this reason, many will likely begin exploring AI agents as a way to improve understanding of events in their infrastructure to speed up incident detection and response. AI's ability to link internal alerts to databases enriched with threat intelligence has the potential to significantly amplify the quality of alerts reaching cybersecurity teams.

Adopting AI agents in cybersecurity is also an opportunity to understand the requirements of this technology and the solutions to securely integrate it into IT infrastructure.

This learning can be shared with other business areas and guide AI adoption in the most varied processes.

## Platform Insight: **Axur Command**

Axur Command introduces a new paradigm of automation in cybersecurity: a command center that orchestrates specialized AI agents to correlate alerts, eliminate false positives, and execute coordinated responses in real time.

The solution connects different sources — such as SIEM, EDR, CTI, and EASM — into a single detection and response flow, reducing analysis time and the burden on security teams.

**Among its main capabilities are:**



Automation of Tier-1 tasks, with agents that triage alerts and prioritize incidents.



Real-time correlation between multiple data sources, revealing the complete context of threats.

The screenshot shows the Axur Command platform. At the top left is the logo 'AXUR command'. In the top right corner, there is a status indicator showing 'Online' with a green dot. The main area features a large orange button with three white vertical bars. Below this button, the text 'Welcome to Axur Command' is displayed. Underneath the welcome message, there is a brief description: 'Your smart ally in cybersecurity. Discover threats, investigate leaked credentials, monitor critical news, and identify data breaches.' Further down, another line of text reads: 'All the power of Axur intelligence at your fingertips, in one place.' At the bottom of the interface, there is a dark grey footer bar containing three items: 'Ask Command a question' (with a microphone icon), 'Deep Research' (with a magnifying glass icon), and a small orange square icon.

## Regulation

When something has significant social impacts, it's natural for various civil society forces to move to establish rules. This regulation can come in a law, voluntary initiatives, or self-regulatory bodies established by stakeholders.

This dynamic also applies to technology, of course. The rapid evolution of artificial intelligence broke through the tech world bubble to also attract the attention of the political world. Several laws have already been approved or are under discussion, and it's not easy to predict what new discussions may arise in 2026.

Despite AI's prominence, it's not the only thing being examined by regulators. The growing presence of insurers in the cybersecurity market has been promoting greater discussion about liability for damages resulting from security incidents. Paying ransoms in ransomware attacks may become more complicated.

Rule changes within the sector itself are also expected for 2026. An example is Google's plan to limit Android app sideloading with mandatory registration for all developers.

Any comprehensive change in how we use technology has the potential to also transform threats.

## Digital and Data Sovereignty

The theme of digital sovereignty gained considerable relevance throughout 2025, as the geopolitical climate has left many countries concerned about the independence of their technological infrastructure and the ability to maintain control over data stored in global-scale clouds.

The objectives of digital sovereignty can impact IT infrastructure and create governance and compliance challenges. These changes have a definite impact on cybersecurity, which will need to be involved throughout the process.

At least in part, this discussion can be understood as an unfolding of the disruption that international logistics and global trade suffered from the Covid-19 pandemic. At the end of the pandemic, we observed in this report that remote work and pressure on semiconductor suppliers pushed IT equipment supply chains to the limit, increasing demand for the cloud and decreasing the control companies had over their own hardware.

Digital sovereignty brings together debates about the market, access to technology, and national security. The consequences for companies appear in IT infrastructure design, which will possibly have to be segregated for clients from different countries, depending on how sovereignty conversations advance.

On the other hand, investments in infrastructure that began in 2025 should start showing results in 2026, creating opportunities for companies that are ready and secure for this challenge.

## Internet of Things and Operational Technology (OT/IoT)

The Internet of Things (IoT) and Operational Technology (OT) create constant challenges for cybersecurity teams. These devices don't always have robust software, and sometimes are abandoned by manufacturers many years before being replaced.

Unfortunately, this legacy is getting worse, as equipment is aging.

Even though manufacturers have made a much greater commitment to product security in recent years, it will take time until all equipment is replaced.

In 2025, old botnets were resurrected with new vulnerabilities in network equipment.

The telecommunications, energy, and healthcare sectors are especially vulnerable to failures in this asset category, but they are also present in retail and hotels. Some product lines, such as security cameras, are used by businesses in all sectors.

Beyond applying security patches, the main recommendation for protecting these devices is using firewalls or network configurations that prevent any type of external access.

A good External Attack Surface Management (EASM) solution can be used to detect externally accessible devices and vulnerabilities in exposed infrastructure.



## Platform Insight: External Attack Surface Management (EASM)

Axur's EASM was designed to map, monitor, and protect this external attack surface, offering a complete view of all accessible assets and their associated vulnerabilities.

The solution identifies domains, subdomains, IPs, and running services, correlating this data with known vulnerability databases (CVEs) and checking digital certificates, open ports, and protocols in use.

This continuous analysis allows teams to:



Discover unknown or forgotten assets, reducing shadow IT risks and accidental exposure.



Classify critical vulnerabilities based on context, severity, and exploitation potential.



Anticipate emerging risks through direct integration with Axur's Cyber Threat Intelligence (CTI) module.

dev.ormuspay.com 123.123.321

Added on 11/20/2023 at 10:37 AM, from ormus.com  
Last update on 09/20/2023 at 10:32 AM

2 CVEs 3 Open ports 1 Certificate

Localization  
New York, United States  
IP Organization  
Internet Assigned Numbers Authority  
IP Net range  
192.168.0.0 - 192.168.255.255  
ISP  
Cloudflare, Inc.

▼ 2 Vulnerabilities

**CVE-2024-5274** CVSS **9.9** EPSS **0.85**  
Actively exploited  
Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)  
**Affected systems:** Fedora project Fedora, version 39.

**CVE-2023-30058**  
Is the identifier assigned to the SQL injection vulnerability in novel-plus 3.6.2.

▼ 3 Open ports

21 80 **443**

▼ Vulnerabilities: CVE-2023-30058

Service: **nginx/1.10.3 (Ubuntu)**

Certificate: 31E75A5A303edcdaedc6e1540001

## Developers in the Crosshairs of Phishing and Stealers

The traditional targets of phishing are consumers and technology service users. Ransomware attacks brought phishing to various company departments, which can now receive highly contextualized messages relevant to their respective functions.

Now, however, we're observing the growth of a new type of phishing directed at software developers.

The software development environment has endorsed large repositories of libraries and components, such as npm (Node.js) and PyPI (Python), and automation of various tasks, often based on third-party code (through GitHub Actions). These points that connect various software projects have become intermediate targets for hackers interested in reaching the companies and users who use them.

In 2025, typosquatting attacks involving the websites of these repositories were observed, as well as individual packages that can compromise developers who use them. Stolen credentials were used to alter official and popular packages, and the tj-actions incident on GitHub managed to propagate malicious code to several projects.

Integrations with AI tools can create undesired situations because of prompt injection flaws, as we've already mentioned. But we can't forget that, beyond technical vulnerabilities, all these processes involve people who are susceptible to social engineering.

A tactic frequently used against programmers in 2025 was the fake job offer, where the victim is approached by a supposed recruiter to conduct an interview. The recruiter asks the victim to install programs or run specific code to participate in the supposed selection process. If the victim follows the instructions, the system will be infected with malware.

Malware attacks against programmers are concerning, as info stealers can steal tokens with permissions to access repositories. It's somewhat surprising that there aren't more recorded cases involving misuse of API keys, but perhaps that will change in 2026.

## Platform Insight: **Data Leakage Monitoring**

Axur's Data Leakage Monitoring identifies credentials, API keys, access tokens, and sensitive code snippets published in public environments like GitHub.

The solution prioritizes alerts according to risk and relevance for each organization, helping teams act before an exposure becomes an incident.

**Among the main applications are:**



Location of credentials and secrets embedded in code and automation pipelines (such as GitHub Actions).



Identification of reused or active keys, reducing the likelihood of misuse.

## Exposed secrets

### 3 Plain password

#### OCCURRENCES

Header MIIEpAIBAAKCAYVYss2sa1BWjXrp1mVXVpb

Header a1BWJAJpK6gVemjXrp1mVXVpbJRSWgVemjXrp1mVXVpb

Body p0vmgidsss梓XVpbAilBAAKC1OYVYss2sa1BWJAJpsjDFDSsSFsd39t0svms...

### 2 Private key

### 1 Password in URL

# Cybersecurity Actions for 2026

## Create Policies for AI Adoption



### In Summary:

- AI agent permissions should leverage the granularity enabled by access management in APIs and other integrations.
- AI agents can automate various analysis, detection, and response processes in cybersecurity.
- If the business demands the use of agents, security teams will have to be ready to validate their use, with policies and technologies for implementation and audit.

The creation of policies for AI agent adoption should be structured on gradual autonomy frameworks, where each stage defines the agent's operational latitude, from mere observation to execution with integrated policies and audit. For each level, the organization must determine explicit rules for scope, rollback, and observability, ensuring that automated actions are always traceable and reversible.

The RAIL model (Restrictions, Approvals, Isolation, and Auditable Logs) provides the technical foundation for these policies, aligning with practices like NIST CSF 2.0 and CTEM (Continuous Threat Exposure Management).

This means defining a unique digital identity for each agent, permissions based on the principle of least privilege, and mandatory human validation in critical actions.

Implementation must also incorporate operational trust metrics, measuring agent precision, reversibility, and mean response time, and provide for sandboxing and continuous audit, so that autonomy comes with verifiable governance. This approach positions AI adoption policies not just as ethical guidelines, but as applied security architecture, fundamental to sustaining autonomous defense safely and scalably.

Cybersecurity teams that remain pioneers in adopting agents to automate their own functions should have an easier time identifying emerging threats.

## Establish Effective and Business-Aligned Governance



### In Summary:

- Compliance shouldn't be a formal and isolated step from the cybersecurity process.
- Whenever possible, new cybersecurity solutions should contribute to established governance goals.
- Evaluate how technical measures of forensics, Threat Hunting, and Cyber Threat Intelligence can improve compliance processes.

The concept of governance gains a new dimension when incorporated into the logic of Continuous Threat Exposure Management (CTEM). Instead of treating compliance and security as isolated cycles, CTEM proposes a continuous, context-driven view, where governance is sustained by technical visibility and strategic alignment. Each stage, from scope definition to mobilization, becomes a governance mechanism itself, connecting risk data, prioritization, and response to business decisions.

This approach complements the GOVERN function of NIST CSF 2.0 by introducing an operational model that maintains real-time control over exposure, not just static policies. Instead of just identifying vulnerabilities, security teams begin defining priorities based on asset value, operational impact, and threat context, bringing risk management closer to corporate management.

CTEM also reinforces that governance needs to be observable and measurable: metrics such as scope coverage, mean validation time, and the ratio between detected and resolved exposures become maturity indicators.

In practice, it reinforces the idea that cybersecurity is responsible for the management capability of IT assets, as well as their policies and processes that ensure their compliance.

Unfortunately, compliance work often boils down to formal and time-consuming processes, with little impact on business resilience. This isn't sustainable nor is it the real interest of good regulators, especially in light of national security concerns that have motivated regulatory reforms in the technology area.

Transforming governance capability into real resilience gains will be a competitive advantage for companies. This becomes easier when cybersecurity aligns with the business, seeing the company's needs also in its market needs, in fraud combat, brand and reputation protection.

After all, combating fraud against consumers and protecting the company's reputation are also ways to avoid the wear and tear resulting from lawsuits and improper association with illegal activity that exploits the company's brand.

The ability to investigate incidents through Threat Hunting and good Cyber Threat Intelligence sources is also decisive for achieving real compliance objectives. Ideally, all the security measures we recommend, such as AI automation, credential and leak monitoring, and supply chain visibility, should also be thought through the lens of compliance, making it part of the security process and not a formal step disconnected from technical measures.

The more robust the existing controls for governance purposes, the easier it will also be to adopt AI agents.

It's important to remember that it can be difficult to predict how regulations or market needs may impact the business. Flexibility and reaction capability will be good values in 2026.

## Implement Data and Credential Monitoring



### In Summary:

- Extortion scams that threaten to expose corporate data replacing ransomware in some cases, requiring external leak monitoring.
- Monitoring leaked credentials helps prevent criminals from gaining access to data stored in the cloud and SaaS platforms.
- Monitoring data leaks facilitates governance and allows the company to adopt a firmer stance with its partners.

Traditional ransomware has been giving way to cyber extortion attacks where criminals threaten companies with exposure of data they've stolen from assets they've accessed, including those located in the cloud, outside the corporate network.

There are no ways to prevent data from being exposed if the ransom isn't paid and, even if the company pays the ransom, there's also no way to be certain that the data was discarded. It's possible that disagreements among scammers will result in a new threat or that criminals will decide to commercialize the stolen information at some point, even if the ransom was paid.

There are two important attitudes to increase resilience against these threats. The first is to protect all IT infrastructure assets, including external ones. Exposed credential monitoring is especially relevant, always considering also corporate credentials used on third-party platforms.

Any and every place that stores corporate data should be monitored and protected. In many cases, a user's credential is the only barrier preventing attackers from accessing data stored in the cloud or SaaS solutions. Since these credentials aren't used in the company's own systems, external monitoring is the best alternative.

The second attitude to take is monitoring leaks and corporate data. Monitoring the company's data exposure has benefits for governance and for quickly initiating efforts to mitigate incidents. In the case of data shared with partners or suppliers, this monitoring also signals concern about data protection, serving as a tool to indirectly detect security breaches in third parties that result in a leak.

## Seek Supply Chain Visibility



### In Summary:

- Hackers are seeking vulnerabilities throughout a target's supply chain.
- Certain cybersecurity solutions can be used to expand supply chain visibility.
- Threat intelligence and AI integrations can be thought of cooperatively with partners.

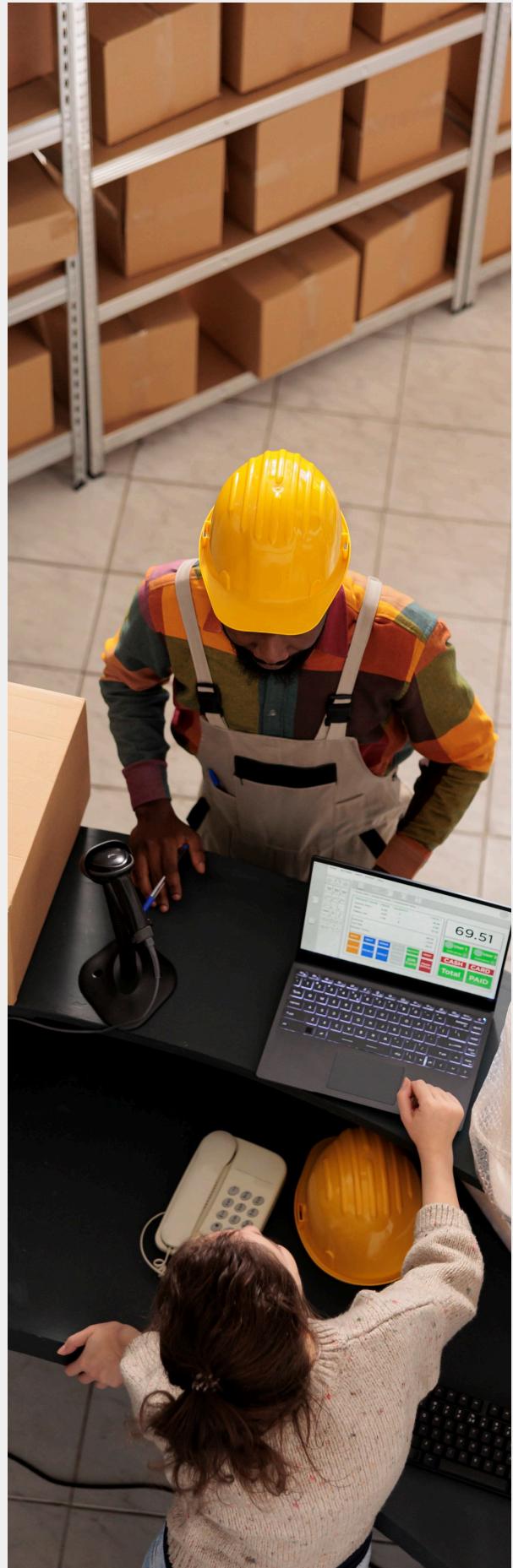
Malicious actors have been demonstrating the ability to locate vulnerabilities in third parties to reach their targets.

Therefore, it's important to seek ways to expand visibility over the entire chain of suppliers and third parties, the supply chain. It's worth mentioning that targets can be opportunistic and not previously desired; from a vulnerable supplier, one can understand what's most interesting to attackers.

Some existing security solutions can be refined to include third-party infrastructure. Axur's Cyber Threat Intelligence can be configured to search for information about asset categories used by critical third parties, alerting about events that may indicate an elevation in risk in supplier environments.

Tools like Threat Hunting and exposed data and credential monitoring can also be used to provide supply chain visibility.

Similarly, agents and other AI tools can also be used to facilitate communication with third parties and ease incident handling.



## Platform Insight: Threat Hunting

Axur's Threat Hunting allows advanced searches in the external threat database to identify exposures of credentials, cards, domains, messages on the deep & dark web, and malicious URLs and social media profiles. Beyond investigating internal incidents, the tool makes it possible to locate credentials and compromised assets of strategic suppliers, map phishing campaigns directed at partners, and anticipate shared risks in the supply chain.

### 101 THREAT HUNTING USE CASES

Threat Hunting

Date	Reference	Content type	Screenshot
18/06/2024	n/a	E-commerce	
18/06/24 at 09:25	healing-ormus.com	Financial	
18/06/24 at 09:25	ormus-holzspielzeug.de	Financial	
18/06/24 at 09:25	n/a	E-commerce	

## Raise User and Partner Awareness



### In Summary:

- Phishing attacks continue evolving, including with new primary targets in some campaigns.
- Software engineers and technical support teams have become frequent phishing targets.
- It's necessary to invest in technical measures, awareness, and training.

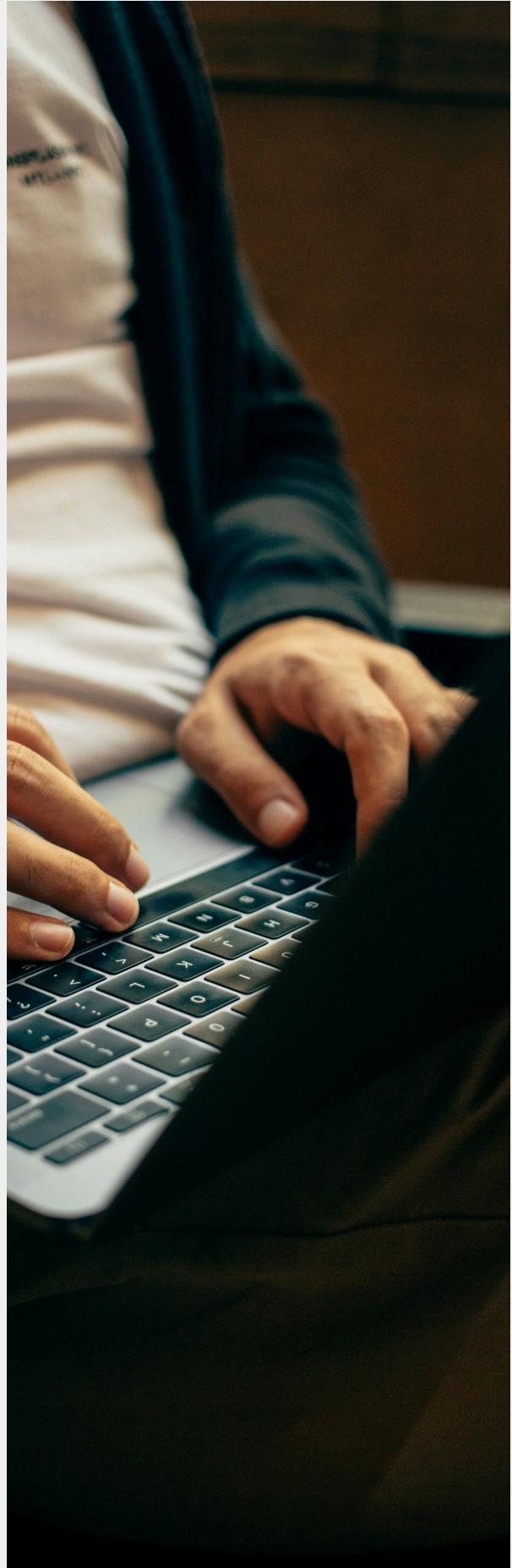
It's understandable that many see phishing as a problem mostly centered on end users from departments without IT ties. Historically, the Human Resources department is one of the most hit, as criminals can impersonate job candidates to apply scams.

The frauds in 2025 changed this scenario. Software engineers were hit through typosquatting (exploiting typing errors) in packages and their repositories.

In another situation, criminals send fake job offers and distribute malicious software under the justification that it would be necessary to take the technical test during the selection process.

If the victim believes the fraud, the result is almost always the execution of an infostealer, which will steal the developer's credentials – including corporate credentials, if they're available.

These scenarios, combined with telephone phishing attacks that targeted help desk and technical support centers, demand a possible expansion of security training and awareness campaigns.



## Threat Landscape

Produced by Axur Research Team

The Axur Research Team (ART) is Axur's intelligence and research nucleus, responsible for transforming data collected by the platform into actionable knowledge about digital threats.

The team combines technical expertise and analytical vision to map trends, correlate indicators, and identify emerging behaviors in non-indexed environments.

Throughout the year, ART conducts continuous investigations on digital fraud, data leaks, external threats, and credential exposure, among other vectors that impact organizational security. The findings result in both reports for Axur clients and strategic insights that contribute to understanding the global threat landscape.

## About Axur

Axur is a cost-effective external cybersecurity solution that empowers security teams to handle threats beyond the perimeter.

Our platform detects, inspects, and responds to brand impersonation, phishing scams, dark web mentions, threat intel vulnerabilities, and more.

With the world's best takedown, Axur removes malicious content quickly and efficiently 24×7, automatically handling 86% of detections.

Our AI-powered tools scale threat intelligence 180x, freeing your security team to focus on strategic initiatives.

[BOOK A DEMO](#)

The screenshot shows the Axur platform's user interface. At the top, there are navigation links: Brand Protection, Threat Hunting, Stats, Investigations, and a search bar. Below the navigation, there are filters for 'Filter' and 'Search ticket'. The main area displays a list of detected threats:

Category	Description	Score
Phishing	Ormus Engagement Report – Spring 2025 https://www.ormuspaly.com/analytics/engagement-report	86
Social	Ormus Pay - Performance Dashboard https://www.facebook.com/ormus-pay-performance	94
Phishing	Ormus Efficiency Metrics – 2025 http://40.86.223.188/Hormus-Energy/mobile-cibc/	72
Phishing	Original Content Releases – April Highlights https://www.ormusmedia.com/releases/may-originals	89

At the bottom right of the interface, there are navigation arrows and a page number indicator '1 - 6 de 6 resultados'.

LANDSCAPE

2025 → 2026

THREAT

MAXUR