Threat status Report

2025 - 2026

Together and ahead

Together and ahead

Advens

For cyber, people & planet

Certified B Corporation

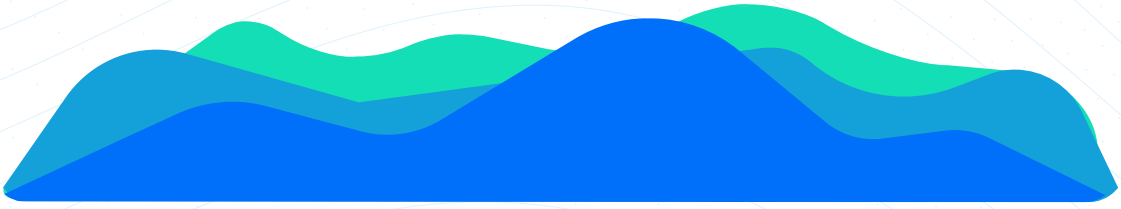
Contents

THREAT STATUS REPORT
2025 - 2026

Introduction

THREAT STATUS REPORT
2025 - 2026

The year 2025 was marked by **an increase in attacks**. Surge in data theft, surge in subcontractor breaches, surge in the use of artificial intelligence: the cyber threats have evolved in a context of ongoing crises, facing increasingly complex and unpredictable human and technological factors.



THE INCREASE IN DATA THEFT
is the result of successful attacks on organisations of various kinds, ranging from private enterprises that are leading the way in their field to central administrations, including smaller and less mature structures, as in the case of certain recently affected sports federations. Although the accuracy and recency of the data that is available for sale on the Dark Web are often challenged by CERT aDvens, the media coverage of these attacks fuels concern about cyber-related crises. This high level of media coverage highlights why it is important for each organisation to have the analytical capacity to assess its own exposure.

THE INCREASE IN ATTACKS
on the sub-contracting chain is following the trends observed in previous years. The major development concerns the importance of the affected ecosystems. Some victims, such as Harvest's software publishing industry, have a monopoly – or almost– on the solutions upon which an entire industry depends. An attack of this magnitude poses a risk to an entire segment of the economy.

THE SURGE IN THE INTEGRATION OF GENERATIVE ARTIFICIAL INTELLIGENCE
by attackers into their operations is a major factor in the recent changes affecting the cyber threat landscape. Its ability to industrialise certain types of attacks significantly increases their strike force regardless of the means they initially possess. This reduces the time between the publication of a vulnerability and the first signs of exploitation, and increases the number of exploitable vulnerabilities. Moreover, the unpredictable nature of this type of AI and its recent emergence are also creating a break with traditional defence methods, whether it is in terms of the technical aspects or the habits and good practices that were taught in the past. Finally, the ability of generative AI to quickly create links between previously unknown elements facilitates the analysis of large attack surfaces. Operations targeting industrial environments, whose technological aspects and specific protocols have required considerable research effort so far, are particularly affected.

The observed increase in attacks also resulted in **an intensification of impacts**. Repeated data theft leads to a form of discouragement among individuals, who may abandon good practices when faced with the sense that their data is already compromised. In addition, successful attacks have reached a considerable scale: the Jaguar Land Rover case is an example of the staggering cost of a successful attack on a large industrial player. This trend has also been observed by the aDvens response teams. Although the more mature structures have strengthened their capacity to deal with less complex attacks, the crisis that arises from a successful attack now lasts a long time and requires significant human and financial efforts.

Finally, **this increase in attacks has become globalised** when the cyber threat is exploited by states or opponents within conflicts. Geopolitics has strongly influenced the threats, from using cyber attacks as other attacks in hybrid warfare to using cyber as a means of destabilising, spreading disinformation or manipulating information.

These evolving threats explain the place of cyber risk in the rankings and risk matrices of many organisations such as the World Economic Forum. If necessary, this reminder highlights the need for organisations to treat cyber risks as one of the most important threats. This includes:

- **an awareness at the highest level,** if it has not already been done, the continuous and accurate reporting provided to senior management on the exposure to the threat and the understanding of the projects to be implemented to face it;

- **a permanent adjustment of the cyber defence arsenal,** through the continuous improvement of detection and response capabilities, but also through the implementation of protection adapted to new forms of threat;

- **a consideration of the cyber approach to all attack surfaces** (any type of connected environment) as well as to every aspect of information risk.

Cyber risk, a strategic priority at the heart of modern organisations...

In an environment marked by constant crises and increasingly frequent technological disruptions, our cyber strategy must be shaped by preparedness for uncertainty, and resilience must evolve into a capacity for continuous adaptation.

Enjoy reading this 2025-2026 report,

The aDvens team

Reading guide

The year 2025 saw an increase in certain trends identified in the past, including the intensification of attacks and their impacts when they succeed in particular. The most mature organisations are able to get rid of the most basic attacks. Less mature structures remain vulnerable to mass cybercrime. This gap is widening, especially with the massive use of AI, which introduces an overall acceleration. These findings call on the cybersecurity industry to adapt its initiatives to all application contexts.

01

The year 2025 in short

This publication is divided into three main sections so that it is accessible to everyone, regardless of their level of experience in cyber, type of organisation or sector of activity.

SIX MAJOR TRENDS

Before presenting our key figures, followed by the details of the analyses of our teams (CERT, SOC, offensive security, security technologies, etc.), here are the main trends observed on the ground last year.

A new boom in ransomware

New groups of attackers are making advanced use of social engineering, compromising important targets and generating strong interest from ransomware groups with more technical capabilities.

Increase in generative AI

The use of AI by attackers is now a daily occurrence. AI facilitates the generation of malicious code, but also the automation of large-scale phishing campaigns.

The supply chain in the crosshairs

2025 has been marked by major campaigns against vendors and software vendors in particular, e.g. Oracle E-Business Suite, Salesforce and the NPM package manager.

Data theft on an almost daily basis

The use of data from massive data thefts is one of the most widely used techniques this year, as is the exploitation of stolen connection data through the intensive use of infostealers.

Significant impacts

Direct and indirect attacks on critical industrial systems are spreading. The estimated figures of the losses incurred in the Jaguar Land Rover case have left their mark.

An increasingly geopolitical threat

Cybercrime is increasingly present in geopolitical actions and conflicts in states all over the world – not just in high-profile conflicts.

KEY FIGURES

+33%
RANSOMWARE ATTACKS COMPARED TO 2024
(8,145 claims)

+20%
OF PUBLISHED VULNERABILITIES
(with over 48,000 in the NVD database)

130
VULNERABILITIES PUBLISHED EVERY DAY ON AVERAGE
Common Vulnerabilities and Exposures (CVE)

60%
PRIORITY 1 ALERTS

More than 60% of the priority 1 alerts processed by the aDvens SOC (out of our hundreds of customers) come from offensive, endured (malicious acts) or controlled actions (in the case of intrusion tests in particular). This rise of almost 10 points reflects the increased effectiveness of monitoring plans: SOCs provide better protection and are less adversely affected by false positives or actions that are legitimised by cyber teams.

29.5 DAYS
OF INTERVENTIONS
average duration in 2025

Through more than 20 responses to incidents in 2025, the CSIRT team of CERT aDvens intervened on different types of threats. While the volume of interventions is lower than in 2024, the intensity and impacts of the attacks have been significant.

50%
CERT RECOMMENDATIONS
concern access and privileges

Almost one in every two actions recommended by the aDvens CERT in the case of an intervention concerns access and privilege management. This directly echoes the percentage of attacks exploiting stolen login data: 80%. This highlights delays or gaps in protecting identity security.

€2BN

The attack on Jaguar Land Rover will have cost the UK economy €2.19 billion, with £485 million in direct impacts declared by the carmaker. The scale of this attack is dramatic not only for the victim but also for the entire UK economy.

THE INTERNET, A CATALYST FOR RISK

Cyber risk is no longer a niche risk: it has become a common thread that crosses and amplifies many contemporary threats.

Cyber risk is emerging as a major and cross-sectional threat, according to the World Economic Forum's 2025 Global Risks Report. "Spying and Cyber Warfare" ranks 5th in the two-year ranking, while "Disinformation and Information Manipulation" will have taken the lead by 2027 – for the second consecutive year.

Based on a survey of more than 900 global experts, this data reveals worrying dynamics: 72% of organisations are seeing an increase in their cyber risks and, of these, 47% now identify threats powered by generative AI as their top concern.

But beyond this dominant position, the internet is a real hotbed of threats. The manipulation of information is greatly facilitated and accelerated by the overproduction of information in digital format – deepfakes, automated disinformation, alteration of content on an industrial scale. Similarly, loss of control over AI could be magnified by attacks targeting model integrity or training data poisoning.

Understanding the threat and processes of attackers is an essential and extremely valuable activity for the cybersecurity industry.

Highlights from the 2025 analysis remind us of the need to address the multiple vulnerabilities published every day and to expand the security approach to the entire ecosystem, including subcontractors.

02

Cyber threat status in 2025

2.1 OVERVIEW OF ATTACKS

This section discusses the different attack techniques that caught the attention of the aDvens teams as well as some particularly interesting malware.

2.1.1 / TTPs that marked 2025

Tactics, Techniques and Procedures (TTPs) are used to represent different aspects of an attacker's activity but are not specific to a particular attacker. These markers can be used by Cyber Threat Intelligence (CTI) to describe an attacker's processes, by the SOC to detect threats, by the Computer Emergency Response Team (CERT) to identify the chronology of an attack, and by Red Teams to simulate realistic attacks.

Perimeter and VPN equipment operations

In 2025, attackers ramped up their campaigns against perimeter devices, including Citrix Netscaler (Citrix Bleed 2), FortiWeb (CVE-2025-64446), Ivanti EPMM (CVE-2025-4427), and SharePoint (ToolShell). These attacks are based on critical vulnerabilities that provide initial access without authentication or a bypassing of security mechanisms. Observed techniques include operating exposed applications (T1190), elevating privileges (T1068), and using valid accounts (T1078). Attackers deploy implants and use encrypted tunnels through legitimate tools to mask their activities. The compromising of this equipment paves the way for rapid lateral movements and persistence in the environment.

The key recommendation is to apply patches as soon as they are released, partition management interfaces and enhance the multifactor authentication (MFA).

Compromising of software chains

Supply chain attacks marked 2025 with campaigns targeting Oracle E-Business Suite, Salesforce, Ingram Micro and NPM (Shai-Hulud). These intrusions exploit vulnerabilities that allow uploading arbitrary files and the installation of webshells (T1505.003), followed by remote command execution (T1059).

Attackers deploy malicious scripts to install persistent mining software or backdoors, thereby compromising system availability and integrity. Observables include unusual JSP/PHP files and changes in critical directories.

Preventive measures include the implementation of a web application firewall (WAF), the immediate application of patches and the proactive detection of webshells.

Advanced phishing and Adversary-in-the-Middle attacks

Phishing campaigns have evolved into more sophisticated scenarios, incorporating fake CAPTCHA and advanced social engineering techniques. Attacks like ClickFix target users via fraudulent pages mimicking legitimate services, prompting them to execute orders via Mshta or PowerShell.

These TTPs (T1566.002, T1204.002) allow attackers to bypass traditional protections and gain initial access. The mobile campaigns, including via WhatsApp, exploit automatic propagation to spread banking malware.

The defence relies on raising user awareness, blocking legitimate misused binaries (LOLbins) and activating robust anti-phishing mechanisms.

Infostealers and the theft of login details

Infostealers remain a major threat in 2025, distributed via cracks, fraudulent installers or "trojanised" games on platforms like Steam. These malwares target the theft of login details stored in browsers (T1555), modification of the registry (T1112) and exfiltration via web services (T1102). Observed campaigns exploit large archives, sideloading DLLs and malicious Chrome/Edge extensions, sometimes from official stores.

Recommendations include banning password storage in browsers, implementing strict policies on extensions and deploying EDRs to detect abnormal behaviour, and silos for personal and business use.

Ransomware and impact on critical systems

Ransomware groups continue to exploit zero-day vulnerabilities including SharePoint (ToolShell) to deploy payloads like Warlock. Techniques include command execution through PowerShell (T1059) and harmful impact data encryption (T1486). These attacks are aimed at disrupting operations and maximising the pressure on victims. Observables include encoded scripts, the use of the legitimate certutil tool and the presence of webshells.

The recommended countermeasures are immediate system updates, the activation of AMSI (Windows Antimalware Scan Interface (AMSI)) to block malicious scripts and critical key rotations.

2.1.2 The most common malware

The year 2025 saw the installation of the three malware families identified last year at the top of the ranking: SocGholish, Agent Tesla and Lumma Stealer. Here is a reminder of how they work but also, and above all, a focus on the latest developments in how cybercriminals use these malware families.

SocGholish

Also known as FakeUpdates, SocGholish is a malicious tool of the JavaScript downloader type. It appeared around 2017 and is often associated with the Evil Corp cybercriminal gang of Russian origin. The main function of this malware is to serve as an initial vector for other malware, exploiting downloads from compromised websites in order to distribute payloads.

As of 2025, SocGholish remains the most common malware because of its function: it facilitates subsequent attacks, e.g. the deployment of ransomware, that affects critical sectors like healthcare or organisations supporting Ukraine in particular.

Among its main TTPs, **SocGholish is distributed through an injection of a malicious JavaScript on compromised sites, using fake browser updates** like "Update.js" or "download.js" and employing traffic distribution systems like Parrot TDS or Keitaro TDS in order to filter and redirect victims to malicious content.

The execution **involves a "drive-by" download attack hidden as a software update**, often using ZIP archives. The names of the latter use visually similar characters like "UpdateInstall.zip" in order to bypass security filters.

Regarding persistence and exfiltration, SocGholish installs backdoors, steals data using tools like Cobalt Strike and abuses native Windows binaries like schtasks.exe to schedule tasks. In terms of evasion, it incorporates "long sleeps" delayed activation to avoid sandboxing, and partners with loaders like MintsLoader to deploy secondary loads.

LATEST NEWS

In 2025, campaigns involving SocGholish peaked in March, followed by a second wave between July and September, alongside with modifications of decoy files. The first wave, initiated in 2024 and continued in 2025, generated more than 1.5 million interactions in one week. This malware also facilitated the distribution of RansomHub ransomware in March 2025. In addition, the Russian-influenced RomCom group used it in September 2025 to target US companies by deploying the Mythic Agent loader. SocGholish also operates like a Malware-as-a-Service selling access to compromised systems to various cybercriminal customers including LockBit and Raspberry Robin.

Among **the new features or changes that occurred in 2025**, SocGholish saw changes in decoy file names from "Update.js" to "download.js" and then returning to visually similar characters. Integrations of MintsLoader or other malware like GhostWeaver and AsyncRAT were also observed. Finally, SocGholish now has an enhanced "credential harvesting" (username/password theft) capability using Outlook signatures.

Lumma Stealer

Lumma Stealer, also known as LummaC2, is an infostealer operating as a Malware-as-a-Service that emerged in 2022. Developed in C language, it is sold on underground forums via subscriptions from $250. Lumma Stealer primarily targets login data, session cookies, crypto-wallets and two-factor authentication extensions. In 2025, this malware experienced a strong resurgence, despite a partial dismantling in May. Its impact affects sectors such as healthcare, banking and telecoms, and is often used by groups such as Octo Tempest.

Among its core TTPs, Lumma Stealer delivers **through phishing emails with links to traffic distribution systems** such as Prometheus, compromised sites using EtherHiding for malicious code on blockchain, or ClickFix to broadcast false error messages prompting PowerShell commands.

The execution involves **the use of fake CAPTCHAs** intended to deceive users, e.g. by tricking them into copying and pasting malicious commands via Windows Run. Lumma uses obfuscated PowerShell scripts to ensure its persistence and exfiltrate data via HTTP POST, with a user-agent like "TeslaBrowser/5.5". When it comes to evasion, it uses the obfuscation of the code stream, the Heaven's Gate technique or the deactivation of ETWTi callbacks. In April 2025, an email campaign targeted Canada with thousands of emails using Prometheus TDS and ClickFix to deploy Lumma equipped with RAT Xworm.

LATEST NEWS

The post-dismantling resurgence in May 2025 involved stealthier methods with the use of fake CAPTCHAs on about 5,000 sites, distributing the infostealer via compromised videos or compromised KMS activators. In addition, in January, GitHub infrastructure was leveraged to deploy Lumma, followed by SectopRAT, Vidar and Cobeacon.

Among **the new features or developments in 2025**, Lumma introduced partial exfiltration, in which data is sent gradually rather than assembled in full before sending. The tool has also been equipped with a detection bypass using open-source snippets and process hollowing. Finally, it was equipped with CypherIt for the use of decoy files, e.g. Falcon Sensor updates.

Agent Tesla

Agent Tesla is a RAT (Remote Access Trojan) and keylogger based on .NET that emerged in 2014. It is available as Malware-as-a-Service on various criminal forums. Agent Tesla's function is the theft of credentials, keystrokes, screenshots and bank data. Its growing impact is marked by a 22% increase between 2024 and 2025. This RAT targets sectors such as energy, logistics and finance, mostly through spear-phishing attacks.

Agent Tesla **is distributed** through **phishing emails with** 7z or RAR archive attachments disguised as invoices, or by imitating services such as WeTransfer. The execution involves JSE or PowerShell scripts to load loaders like AutoIt or .NET, with an injection into legitimate processes, such as RegAsm.exe or RegSvcs.exe. Regarding evasion techniques, Agent Tesla uses multi-layer obfuscation, homoglyphs (similar-looking characters) and in-memory fileless execution.

LATEST NEWS

Agent Tesla was the subject of several campaigns in 2025. In October, a phishing campaign mimicking WeTransfer was used to spread the malware. Another campaign targeted Latin America in November, with the injection of Agent Tesla concealed by a RAR file disguised as an invoice. In 2025, the QuirkyLoader was used in spam emails to deploy Agent Tesla with AsyncRAT and Snake Keylogger. Fake payment emails were also sent, referring to payments made in order to induce malicious files to be opened.

Among **the new features or changes in 2025**, Agent Tesla's obfuscation techniques have been improved with advanced anti-analysis methods and an injection into the Windows RegSvcs process. Finally, its capabilities were expanded to audio and video theft.

2.2 MAJOR VULNERABILITIES

130

CVEs PER DAY

In 2025, **a total of 48,185 CVEs** (Common Vulnerabilities and Exposures) were released, indicating **a 20% increase from 2024** (40,308 CVEs). This increase reflects significant growth with an average of over 130 CVEs per day.

+32%

ADDITIONAL VULNERABILITIES

In 2025, **245 vulnerabilities were added to CISA's Known Exploited Vulnerabilities** (KEV) catalogue. This represents a 32% increase over 2024 (185 additions). Of these, 27 have been linked to ransomware attacks with a focus on network appliances and Microsoft, Cisco and Fortinet products.

Debates over CISA funding reveal the reliance on US infrastructure for listing vulnerabilities. In response to this strategic risk, **ENISA initiated the development of a European vulnerability database**, which could become a leading tool for European cybersecurity actors.

SharePoint

CVE-2025-53770/53771

These vulnerabilities bypass previous patches for the ToolShell exploits. CVE-2025-53770 allows remote code execution (RCE) by an unsecure deserialisation of unreliable data, while CVE-2025-53771 allows an authentication bypass by header spoofing.

- **Operation**: An attacker forges a referer header to bypass the authentication and then injects deserialised payloads to execute the code.
- **Impact:** total compromise of the system, deployment of backdoors by Chinese state actors, and spread of ransomware like Warlock, affecting thousands of organisations.

9.8

CRITICAL

Exploited
Execution of arbitrary code

EPSS: 0.91%

PoC: YES

EPSS: Exploit Prediction Scoring System
PoC: Proof of Concept

SAP NetWeaver®

CVE-2025-31324

A permissions vulnerability in SAP NetWeaver allows an unauthenticated attacker to execute arbitrary code or manipulate the database by uploading a specifically crafted malicious file.

- **Operation**: no permission control on the endpoint/developmentserver/metadatauploader allows an unauthenticated attacker to upload malicious JSP webshells which are executable using GET requests leading to a remote code execution (RCE).
- **Impact:** total system compromise, deployment of backdoors and ransomware (BianLian, RansomEXX), exfiltration of sensitive data affecting more than 50% of exposed NetWeaver Java systems. Operation observed from February to May 2025.

10
CRITICAL
Exploited
Execution of arbitrary code

EPSS: 0.4%

PoC: NO

FORTINET

CVE-2024-55591

Authentication bypass in the Node.js websocket module.

- **Operation**: operation relies on sending specially crafted requests to the Node.js WebSocket module allowing authentication mechanisms to be bypassed through an alternate channel or path. This vulnerability opens the way to obtaining super administrator privileges without prior authentication.
- **Impact:** changes to firewall configurations, creation of VPN accounts, credential theft and deployment of ransomware like Mora_001. Active operation since November 2024 affecting more than 50,000 exposed devices with attacks by state actors.

9.8
CRITICAL
Exploited
Authentication bypass

EPSS: 0.94%

PoC: YES

ORACLE E-BUSINESS SUITE

CVE-2025-61882/61884

The CVE-2025-61882 enables remote code execution (RCE) via XSLT injection in the concurrent processing process. The CVE-2025-61884 vulnerability allows unauthorised third parties to access sensitive configuration data.

- **Operation**: Sending forged HTTP requests to the Oracle E Business Suite BI Publisher Integration module allows an unauthenticated remote attacker to invoke internal processing and trigger remote code execution. By hijacking the XML and XSLT processing logic, these requests abuse alternative paths and internal requests (SSRF, header manipulation) to bypass access controls and gain complete control of the application.
- **Impact:** total compromise, data theft, deployment of ransomware like Cl0p since August 2025. Insufficient initial patches, requiring a final update in October. Massive exploitation by criminal groups, affecting versions 12.2.3-12.2.14.

9.8
CRITICAL
Exploited
Execution of arbitrary code

EPSS: 0.86%

PoC: YES

ivanti Connect Secure

CVE-2025-22457

This vulnerability concerns a stack buffer overflow leading to an RCE.

- **Operation**: An unauthenticated attacker sends HTTP(S) forged requests containing a forged X-Forwarded-For header, triggering an overflow buffer in the web component of the Ivanti appliance. This memory corruption allows pointers to be hijacked and arbitrary code to be executed remotely, despite mechanisms like ASR.
- **Impact:** spying by Chinese APT groups, deployment of droppers like TRAILBLAZE and backdoors like BRUSHFIRE. Active operation since March 2025 affecting versions before 22.7R2.6 with a high risk of network compromise.

9
CRITICAL
Exploited
Execution of arbitrary code
EPSS: 0.56%
PoC: YES

citrix

CVE-2025-5777

This vulnerability concerns an out-of-bounds read due to insufficient input validation.

- **Operation**: malformed requests to NetScaler appliances configured in Gateway or AAA mode cause uninitialised memory leakage exposing sensitive data such as session tokens.
- **Impact:** secret theft, MFA bypass, session hijacking to access sensitive data. Massive exploitation since June 2025, similar to Heartbleed, affecting NetScaler versions before the July 2025 patches.

7.5
IMPORTANT
Exploited
Memory leak
EPSS: 0.81%
PoC: YES

cisco

CVE-2025-20333

This vulnerability concerns an RCE in the ASA/FTD VPN web server.

- **Working**: Insufficient validation of entries in HTTPS requests allows the execution of arbitrary code in root, chained with the CVE-2025-20362 vulnerability to bypass authentication.
- **Impact:** Deployment of malware like Line Dancer and Line Runner by the Chinese group ArcaneDoor for spying. Active operation since May 2025, persistent compromise even after reboots, affecting ASA 5500-X without Secure Boot.

9.9
CRITICAL
Exploited
Execution of arbitrary code
EPSS: 0.09%
PoC: NO

React

CVE-2025-55182

This vulnerability concerns an unauthenticated RCE in React Server Components.

- **Operation**: Insecure deserialisation of malformed payloads in the Flight protocol allows the injection of arbitrary objects, leading to server-side code execution via a single HTTP request.
- **Impact: server** takeover, deployment of backdoors, XMRig cryptominers and spying tools by Iranian and Chinese groups. Widespread use since December 2025 affecting versions 19.0 to 19.2 and frameworks like Next.js.

10

CRITICAL

Exploited
Execution of arbitrary code

EPSS: 0.57%

PoC: YES

FreeType

CVE-2025-27363

This vulnerability concerns an out-of-bounds write when parsing fonts.

- **Operation**: mishandling types in the subglyph structures of TrueType GX/ variables fonts causes an integer wraparound, allocating too small a buffer and writing arbitrary data to memory.
- **Impact:** execution of arbitrary code via malicious fonts, deployment of spyware like Paragon. Active operation since March 2025, affecting versions ≤2.13.0 on Linux, Android, iOS and browsers, with a high risk of system compromise.

8.1

IMPORTANT

Exploited
Execution of arbitrary code

EPSS: 0.77%

PoC: NO

mongoDB.

CVE-2025-14847

This vulnerability concerns a memory leak in the zlib compression management.

- **Operation**: Compressed malformed messages with inconsistent lengths cause out-of-bounds reading, returning uninitialised heap memory before authentication.
- **Impact:** extraction of sensitive data such as credentials, tokens and PII. Massive exploitation since December 2025, affecting versions 3.6+, with more than 87,000 instances exposed, leading to compromises by Chinese and criminal actors.

7.5

IMPORTANT

Exploited
Memory leak

EPSS: 0.62%

PoC: YES

Find out more

In order to track major vulnerabilities year-round, you can consult the warning bulletins published by the **aDvens CERT**.
Soon, find a dedicated module for continuous monitoring.

2.3 RANSOMWARE VICTIMISATION

8,150
VICTIMS

After a question last year about a potential decline in ransomware, **significant progress was made in 2025**. The number of claimed attacks has increased significantly: more than 8,150 victims, i.e. a 33% increase compared to 2024. These attacks have intensified with a peak of over 1,000 incidents in a single month observed in February 2025.

+33%
OF ATTACKS

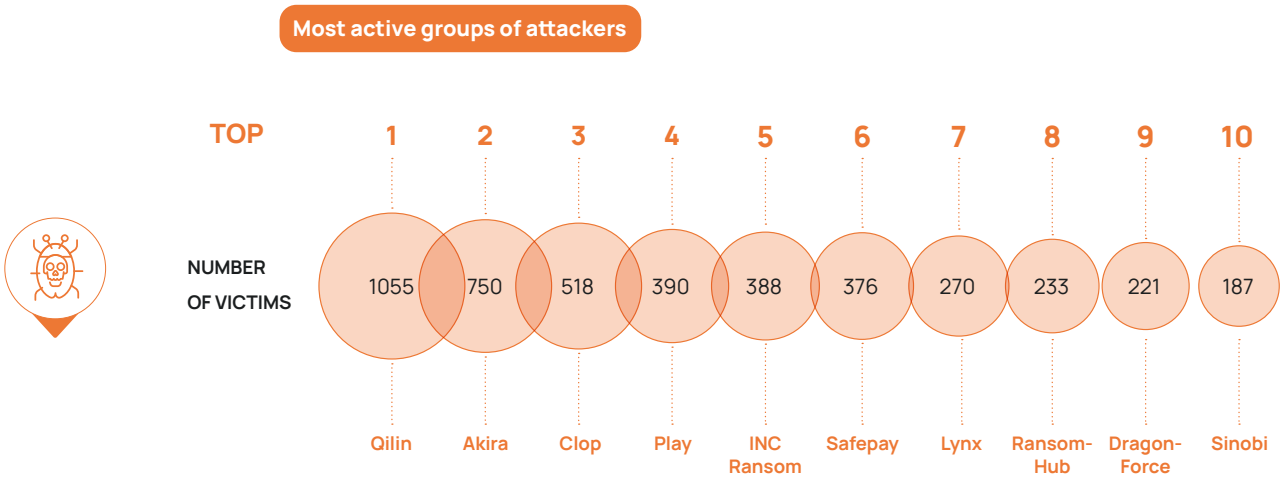
Ransomware attacks are continuing to evolve and grow despite the efforts of the authorities to dismantle the large groups. The temporary decline in Lockbit claims has led to the growth of a multitude of smaller groups and players. But this criminal market remains fairly concentrated with about a dozen groups and the dominance of the Ransomware-as-a-Service model. Technically, double extortion with a combination of encryption and data theft has become standard, sometimes supplemented by additional methods like DDoS attacks.
Ransomware actors are also adopting AI rather than being left behind. It has played an increasing role allowing cybercriminals to generate malicious code, automate certain phishing campaigns and even negotiate with victims.

1,000
INCIDENTS IN FEBRUARY

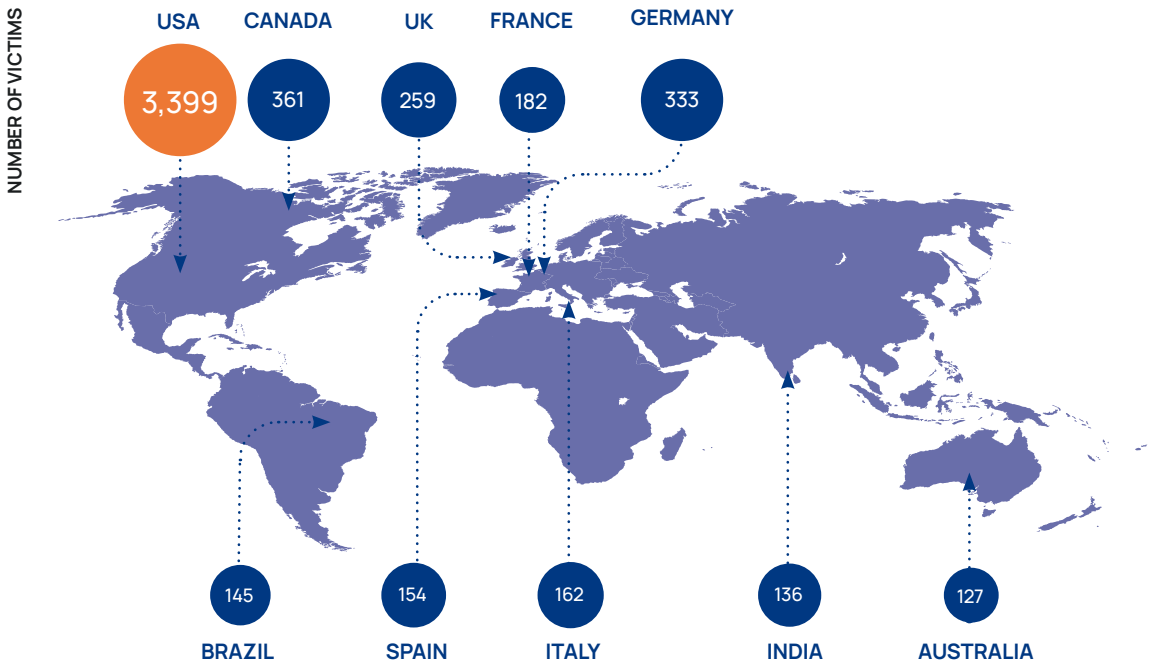
Although ransom payments are declining as are the amounts demanded, these latest developments remind us that **ransomware attacks are still massive and sophisticated** and that the arsenal of protection measures must incorporate technical and organisational measures to deal with them.

The data in this section are taken from ransomware.live.

2.3.1 / World victimology



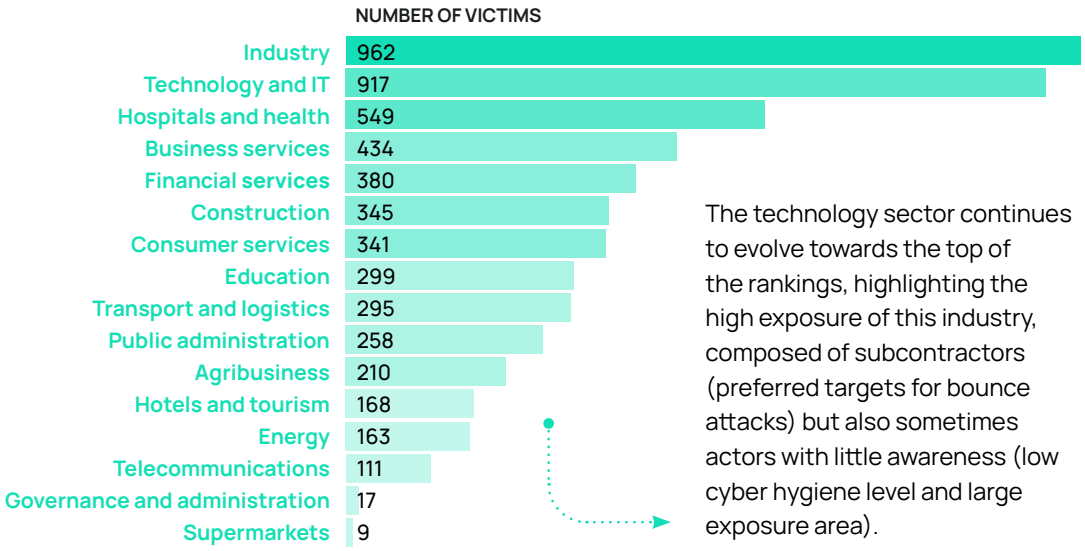
Target countries



TOP 1

Geographically, **the United States** remains the main target (47% of attacks).

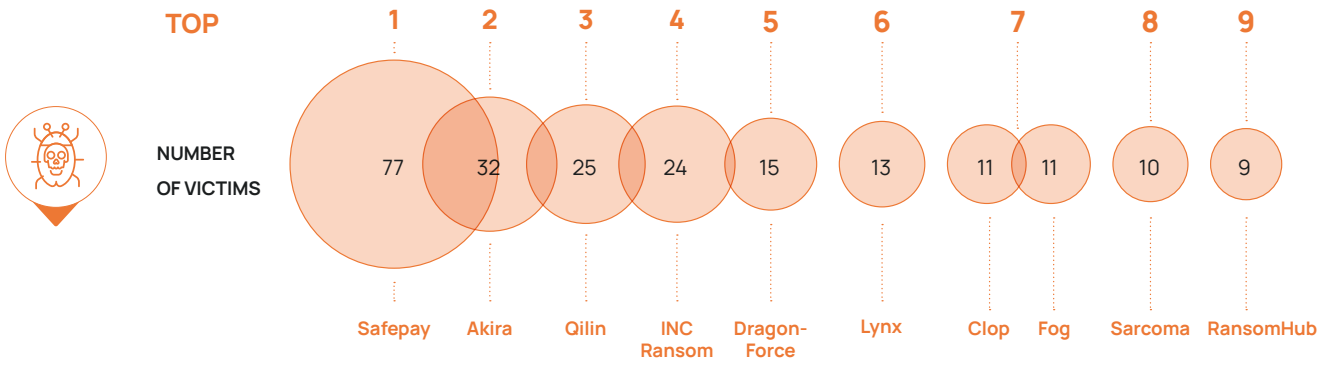
Sectors of activity targeted



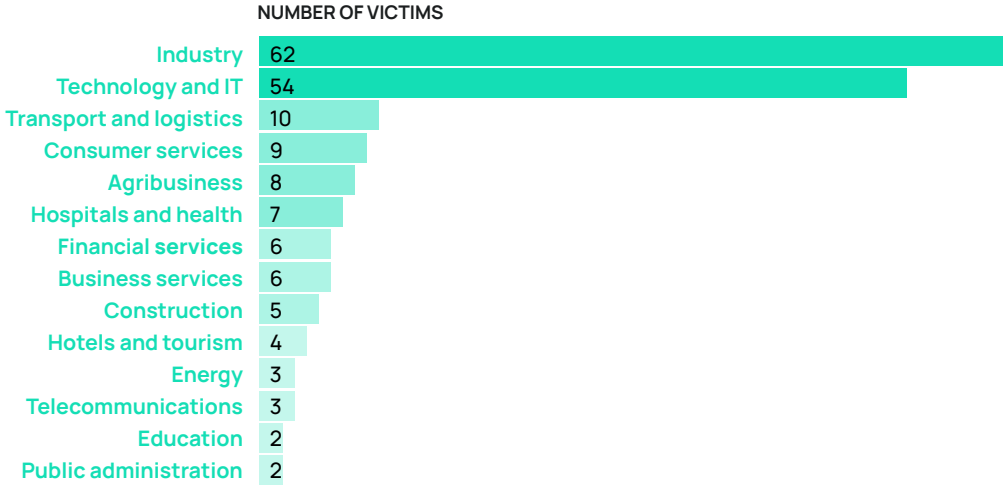
The technology sector continues to evolve towards the top of the rankings, highlighting the high exposure of this industry, composed of subcontractors (preferred targets for bounce attacks) but also sometimes actors with little awareness (low cyber hygiene level and large exposure area).

2.3.2 / Victimology in Germany

Most active groups of attackers



Sectors of activity targeted

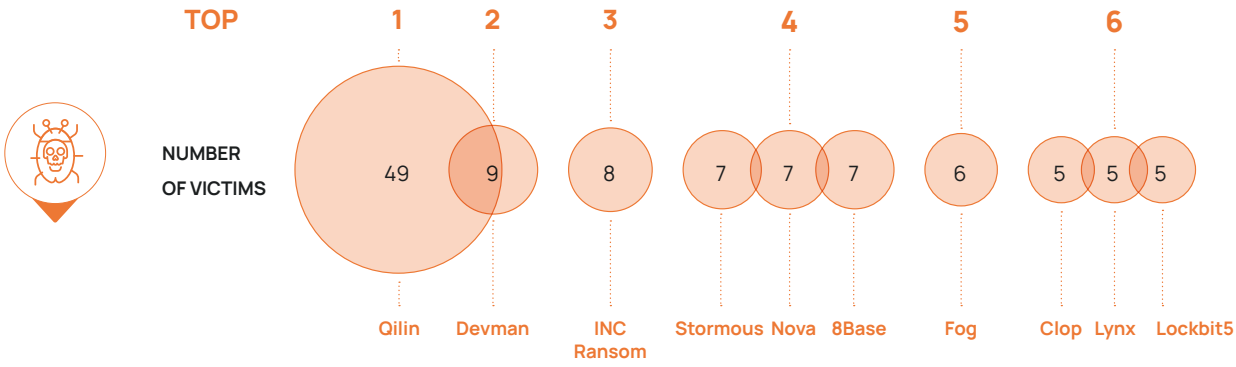


333
ATTACKS

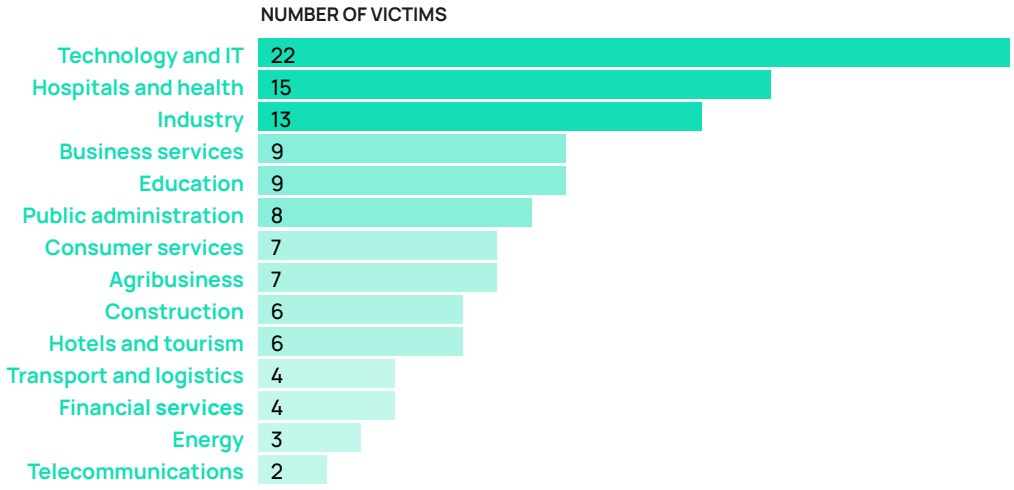
Germany is still 3rd in the world rankings with 333 attacks claimed.

2.3.3 / Victimology in France

Most active groups of attackers



Sectors of activity targeted

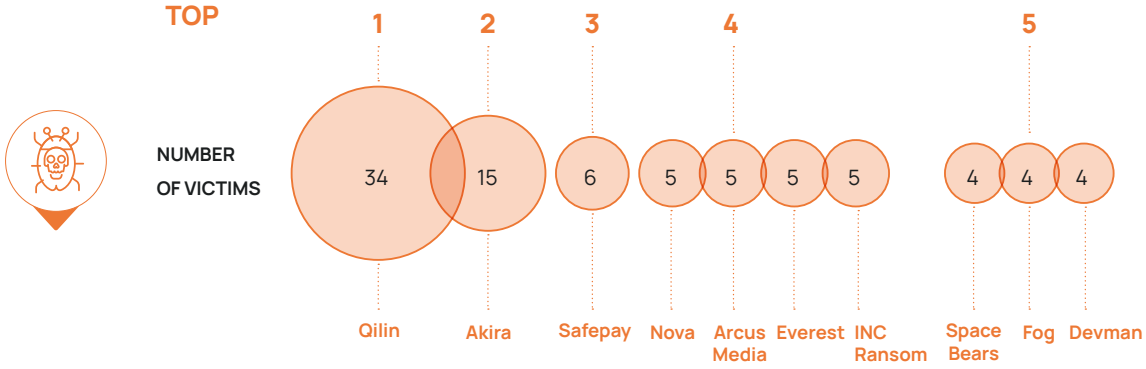


180
ATTACKS

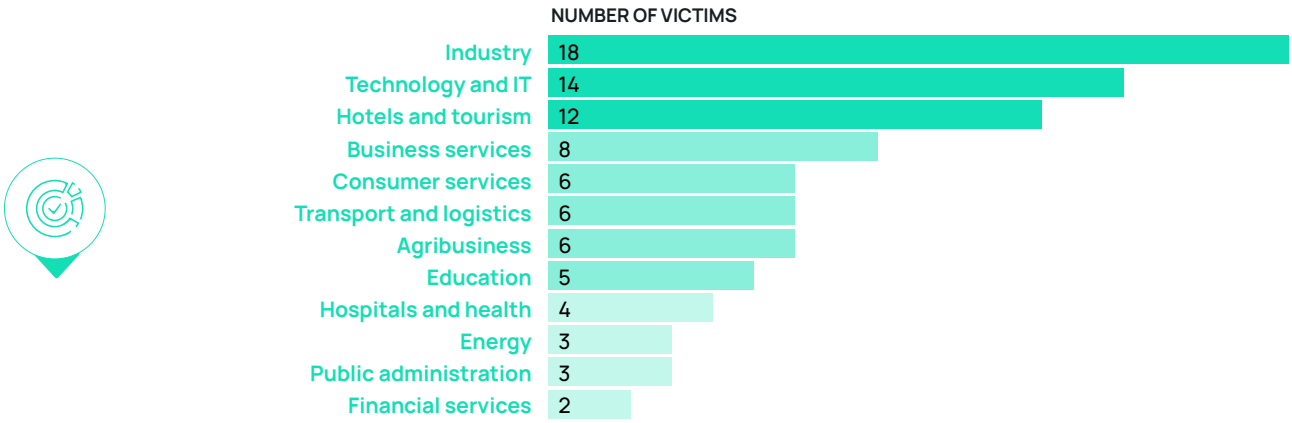
France remains the world's fifth largest ransomware target, with 180 attacks claimed last year.

2.3.4 / Victimology in Spain

Most active groups of attackers



Sectors of activity targeted

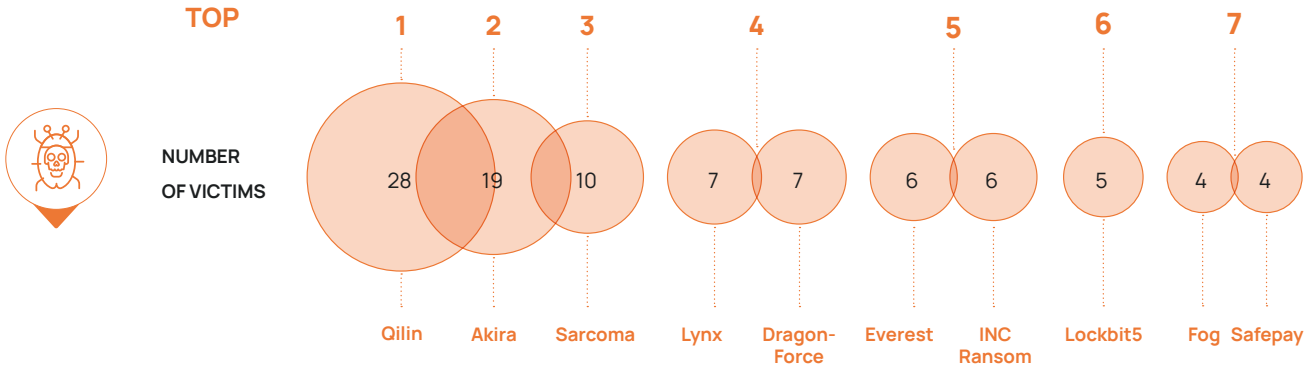


154 ATTACKS

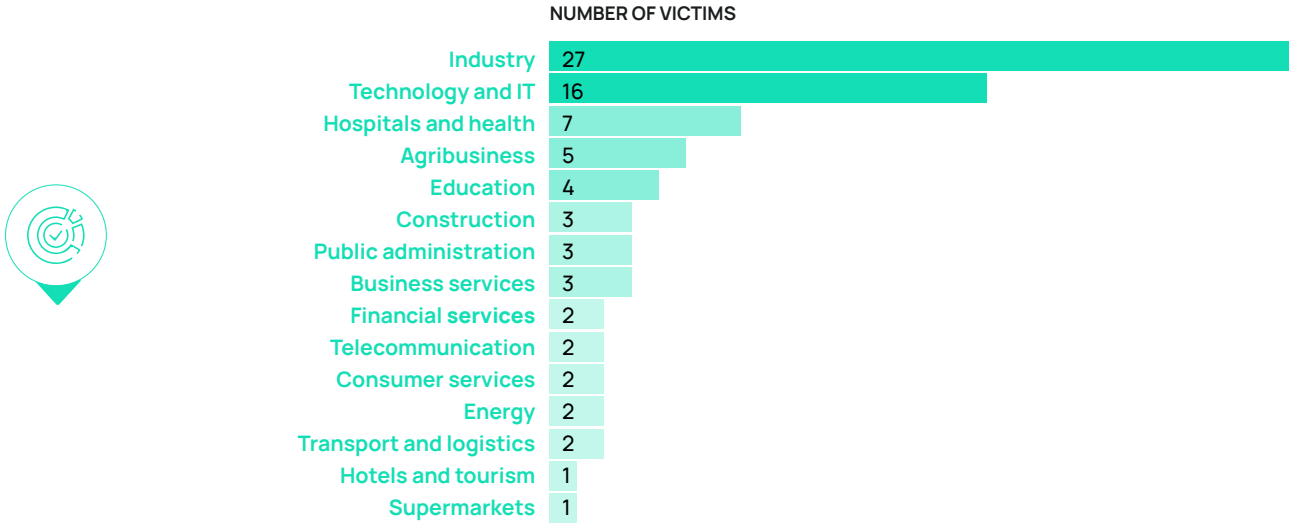
Spain improved its ranking by one spot and is now 7th in the world with an overexposure of the hospitality and tourism sector in the top three of the targeted sectors (154 attacks across all sectors).

2.3.5 / Victimology in Italy

Most active groups of attackers



Sectors of activity targeted



162
ATTACKS

Italy retained its 6th place in the world ranking with 162 attacks claimed.
The usually targeted sectors remain the most affected.

2.4 STATUS OF CYBER DEFENCE

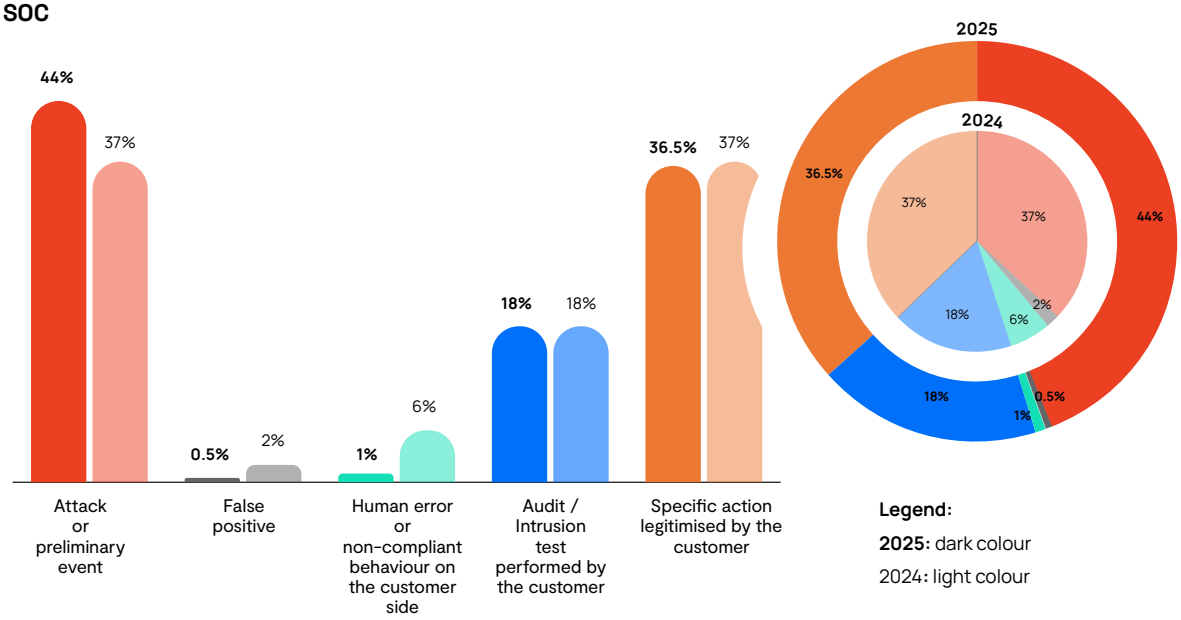
This section provides an answer to the overview of attacks from the perspective of the defenders.

This point of view was developed by consulting our experts, including the SOC teams (on incident detection), the CERT teams (on the analysis of action plans following an intervention by CSIRT or an analysis by the SOC) as well as the teams specialised in safeguarding infrastructures and implementing security technologies. Their contribution complements the viewpoints of the teams exposed to the threat with the contributions of profiles that take action using a preventive approach.

2.4.1 / Status of the SOC

This section is based on a review of the activity of the aDvens SOC which offers an outsourced SOC service used on a daily basis by several hundred customers in Europe and whose environments are deployed worldwide. Given the number of assets considered as well as the various sizes and industries of the customers concerned the figures presented illustrate trends that will apply to any type of organisation. In practice, the analysis of SOC activity is based on the review of the alerts and incidents processed by the SOC and on the analysis of the actions leading to the creation of a maximum priority ("P1") incident ticket in particular.

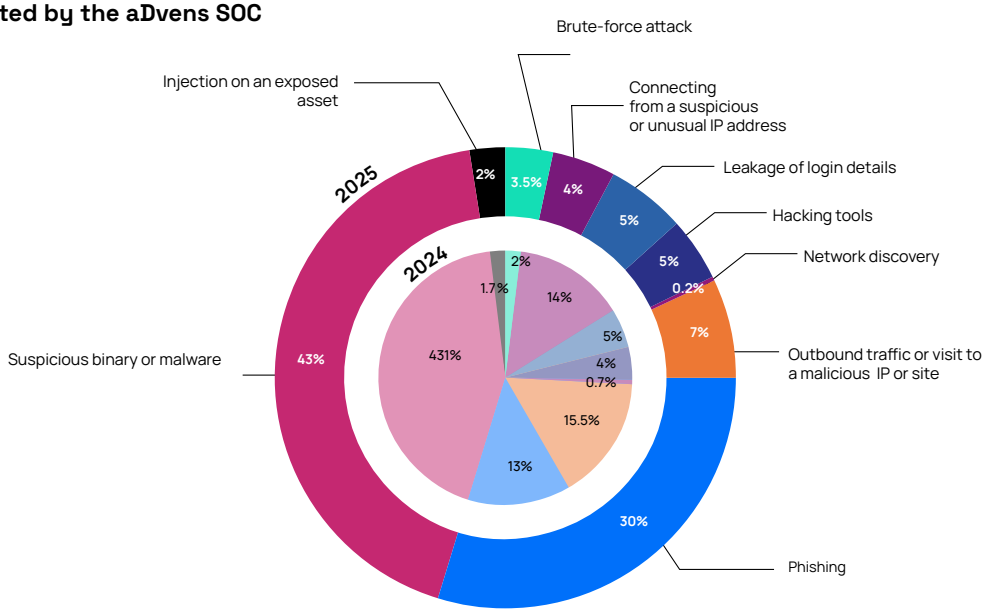
Nature of events detected by the aDvens SOC

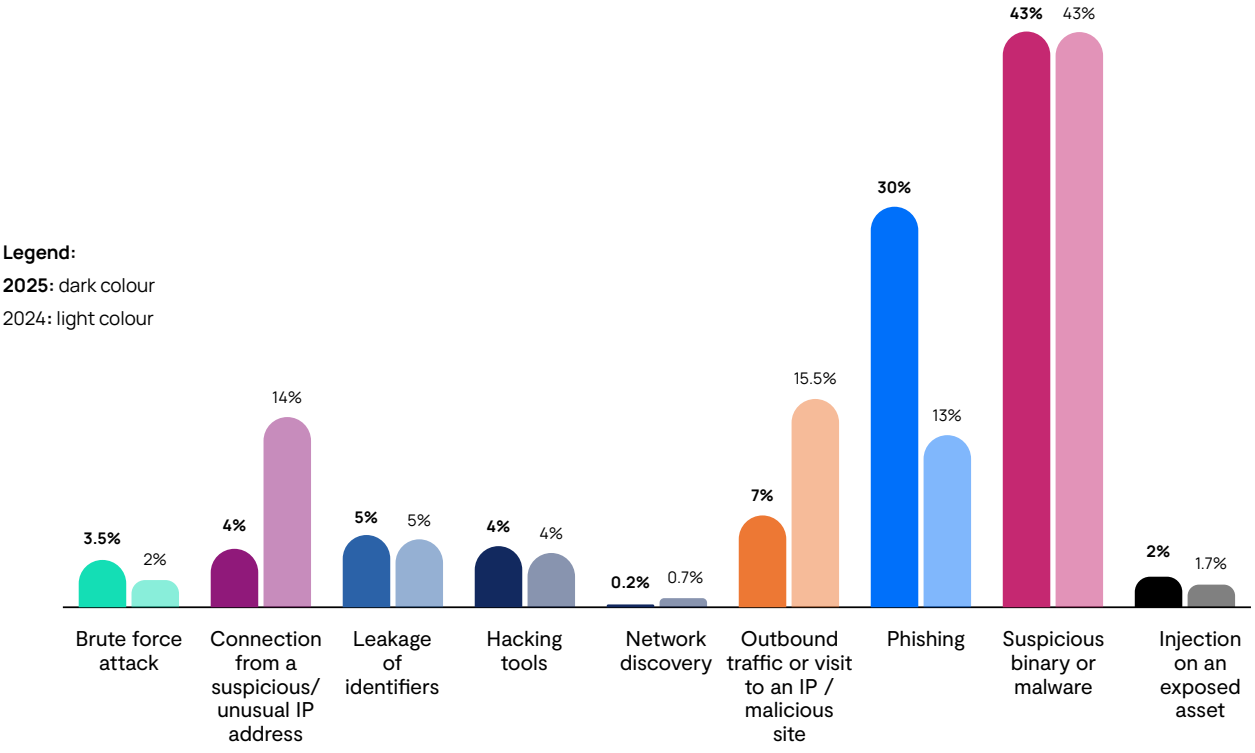


The total number of P1 tickets created by the aDvens SOC increased by 22.5%. This growth is partly related to the growth of the company's business, whose number of customers has increased, but also to the intensification of cyber activity. More and more detections result in maximum priority tickets.

Moreover, **63% of tickets are the result of offensive actions**. These actions can be controlled as in the case of 18% of the intrusion tests detected by the SOC (identified as such upon detection), but also endured. This is the case for the 44% of tickets related to an attack or an event prior to an attack (e.g. reconnaissance phase). **The percentage of alerts related to an attack increased by 7 points**. As the threat continues to escalate, detection capabilities are improving – as is the relevance of the SOC's operator analyses.

Breakdown of attacks or actions prior to a potential attack blocked or detected by the aDvens SOC





While **the number of P1s generated for malware stayed the same** in 2025, this type of threat is still one of the leading modus operandi. On the other hand, there has been **a sharp increase in phishing**. This increase has two causes. The first is linked to a review of the ticket analysis method. The second is related to the detected increase in phishing attempts. This procedure remains widespread but it has evolved as detailed in the focus above.

Logically, the exploitation of leaked login details is on the rise, as a result of the increase in infostealer attacks noted in 2024 – stolen information being used either to directly compromise accounts or to issue more sophisticated phishing. Finally, there has been an increase in attacks on an exposed asset. This trend is explained by the exponential growth of vulnerabilities on border components like Fortinet and Ivanti which were regularly announced last year and again this year.

The focus that our experts have prepared comes back to different scenarios, linked to vulnerabilities, the evolution of the technological arsenal as well as the attackers' modus operandi.

FOCUS

CVE-2025-31324

Vulnerability CVE-2025-31324, previously exposed in last year's Top 10, is an application vulnerability affecting SAP's NetWeaver module. Several aDvens customers have been victims of exploitation of this flaw targeting an ERP publisher that is extremely prevalent worldwide. The first of our compromised customers allowed the aDvens SOC to share the compromise indicators with all our customers. This request is systematically made by SOC managers to their customers. Thanks to this approach, we were able to detect many victims.

Among them was an IT provider, offering instance hosting services. It was therefore highly exposed to a major risk of spread. The joint action of its security teams and the aDvens SOC allowed this risk to be controlled. This case recalls two good practices that are essential for an effective defence.

- It is essential that the SOC provider cooperates constructively with all its customers.
- Collective intelligence is an absolute necessity for achieving an overall increase in the level of security, as highlighted in many publications such as the **2025 CESIN survey**.

CHANGING LANDSCAPE OF SECURITY SOLUTIONS

EDR spread widely and rapidly a few years ago becoming a widely deployed solution in our customers' information systems. Coupled with a SIEM (either by the organisation or not, depending on whether the SOC is internalised or outsourced), **the EDR is therefore the first step in the SOC roadmap of many organisations**. The next step is far from being as obvious! Indeed, even if it remains central, EDR alone cannot be a suitable defence in 2026 – as the example of Black Basta illustrates in the section box on phishing (next page).

- The scope of the threat has largely shifted outside of traditional network boundaries and is increasingly exploited within cloud platforms which are completely invisible to EDR. This requires the deployment of dedicated cloud solutions such as CNAPP.

- When an account is compromised that is used "on-premise" and that would be the subject of actions by legitimate tools, EDR is not enough. For example, it must be coupled with an NDR that will detect discovery and/or lateral movement actions, for example.

- The coming together of the SOC and CTI teams has proven to be effective. A CTI service is therefore key to identifying certain threats, e.g. infostealers. The CTI allows you to take action ahead of time, i.e. before the theft or operation rather than after using the compromised account. By conducting investigations and contextualising certain threats, the SOC can determine the timeline of compromise indicator activities. To identify other potential compromises, the CTI conducted 190 retro hunting campaigns corresponding to post-mortem research conducted on its customers' activity logs.

- Vulnerability management and VOC are also crucial elements for certain kinds of threat. In the case of network edge equipment events, rapid response is a success factor. You have to be able to qualify, patch and test as soon as possible.

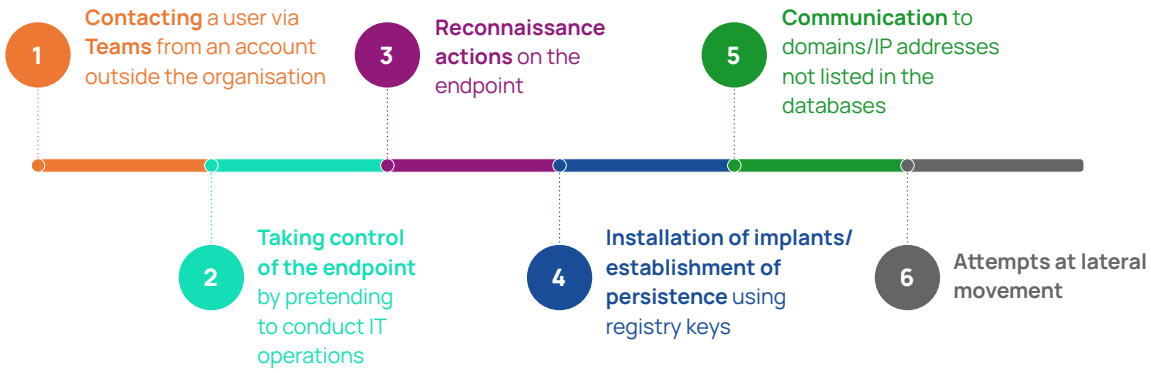
NDR, CNAPP, CTI, VOC... The right step to follow the implementation of the EDR is not the same for all organisations. Operational security teams and especially SOCs (internal and external) must therefore be able to combine flexibility, agility and agnosticity! The SOC of tomorrow will be composed in response to the threat and must embrace the perspective of attackers as well as defenders.

PHISHING – THE BLACK BASTA CASE

Far from emails full of mistakes and failed authentication pages, phishing practices are evolving to become more potent and more effective. The use of generative AI is used to make authentication pages more credible and generate messages (text messages, emails, voice messages, etc.) with a more appropriate tone. In addition, more targeted actions can be taken using stolen data and a deepening of reconnaissance phases. Another notable development is the way in which the victim is contacted.

It is no longer always a massive attack involving the sending of thousands of non-personalised mails. The modus operandi is based on direct contact with a user during a videoconference call; the user will be engaged in a most credible scenario! **Daring to make direct contact was one of the new phenomena anticipated in the previous version of this report. The trend is therefore confirmed.**
The example of events attributed to Black Basta illustrates this development in phishing practices.

The example of events attributed to Black Basta illustrates this development in phishing practices.



In a case like this, detection capabilities are quite limited because almost all the actions carried out are based on common and legitimate tools. However, it is possible to protect yourself from it through a combination of protective measures and awareness-raising:

- **Raising awareness among users on the expansion of phishing** to all communication channels;
- **Banning the use** of unofficial remote control tools;
- **Extending SOC coverage using security solutions** that detect lateral movements (such as NDR);
- **Conducting regular retro hunting** campaigns to carry out potential ex-post detections.

2.4.2 / CERT action plans

CERT aDvens intervened more than 20 times in 2025. While the volume of interventions has decreased compared to last year, their intensity has increased considerably, generating major impacts for victims and complex crisis management situations.

2,000
RECOMMENDATIONS

As part of these incident response activities (CSIRT) but also as part of threat analysis and early anticipation activities (CTI), CERT teams issued more than 2,000 recommendations related to incidents or open-source investigations ranked by scope, difficulty and priority.

1 IN 2
TO BE TREATED WITHIN TWO MONTHS

46% of the recommendations needed to be implemented in the short term (within two months) in order to quickly raise customer security posture to an acceptable level. This approach is then complemented by medium-term (P2) and long-term (P3) planned actions to enhance security on a sustainable basis. Depending on then situation surrounding the intervention and investigation, the scope of the recommendations adapts to the direction chosen whether it is to anticipate threats or respond reactively.

80%
FOR IAM

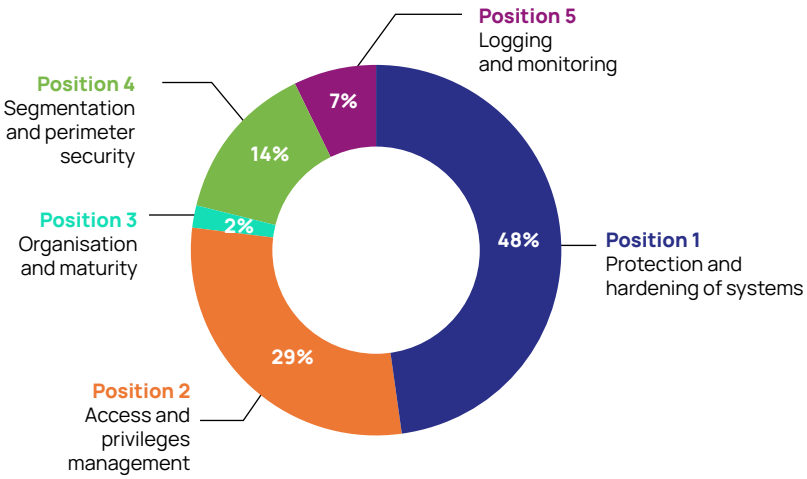
Most of the CTI analysts of CERT aDvens advocated actions related to access and privilege management. In 80% of the interventions processed by CSIRT, initial access came from the use of compromised authentication data (employees, contractors, etc.). Recommendations were also made regarding the protection and hardening of perimeter equipment, including the protection of exposed vulnerable or misconfigured services on the internet.

KNOWING YOUR DIGITAL FOOTPRINT

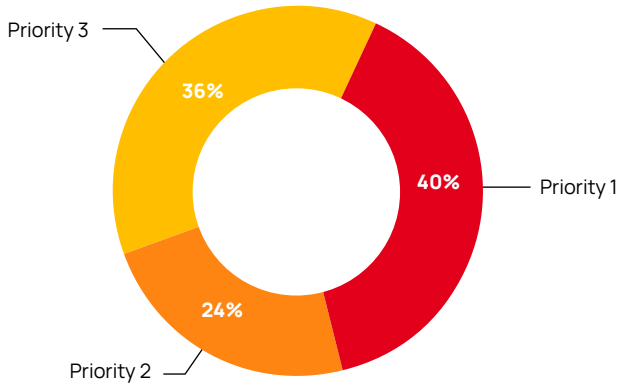
Whatever the nature of an attack, a malicious actor always begins with a passive reconnaissance phase on his target. Having an analysis of your digital exposure on the various internet media (Clear web, Deep web, Dark web) makes it possible to adopt the perspective of an attacker and thereby anticipate the risks more effectively. The aDvens CERT provides an **EASM** (External Attack Surface Management) activity to assist organisations know and master this digital exposure.

ANALYSIS OF "ANTICIPATORY" ACTIONS (CTI)

Perimeter distribution



Breakdown by implementation priority



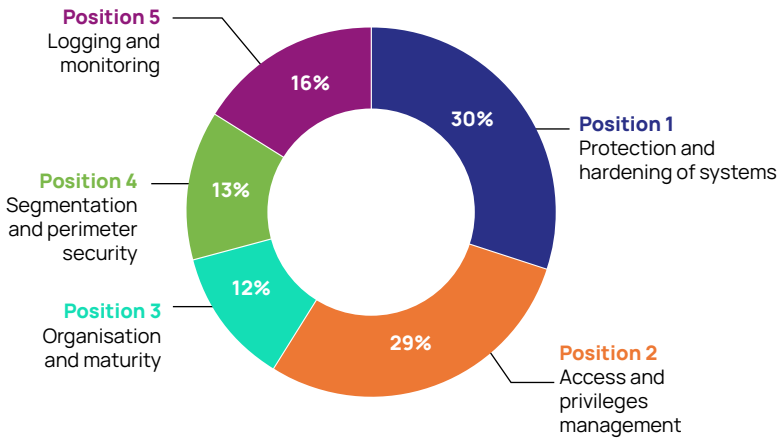
40%

PRIORITY 1 ACTIONS

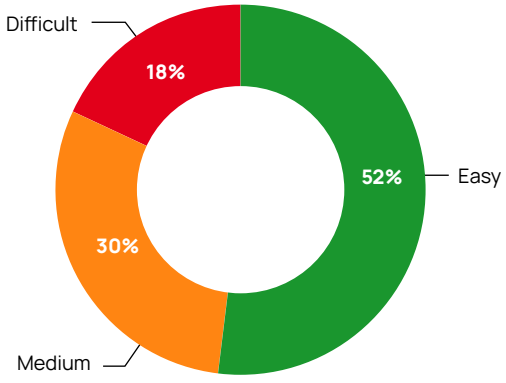
In CTI interventions, more than three-quarters of actions concern system protections, and identity and privilege management. Whatever the topic, 40% of the actions have to be carried out within a limited timeframe. Anticipatory interventions (CTI approach to threat analysis) result in specific, concrete and targeted actions (activation of MFA, closure of unnecessarily exposed services, change of password by default, etc.). They represent a leverage point for effectively improving the level of security and crisis preparedness.

ANALYSIS OF "INCIDENT RESPONSE" ACTIONS (CSIRT)

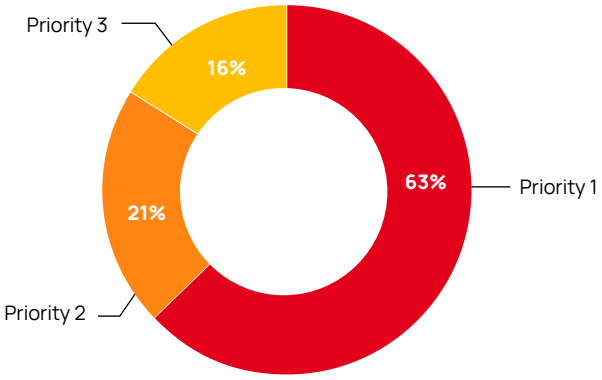
Perimeter distribution



Breakdown by difficulty in implementing recommendations



Breakdown by implementation priority



When managing a major security incident, the nature of the actions recommended is more varied with an important focus on hardening, and on identity and access management. Actions are generally considered easy but must be completed within a limited timeframe. Crisis management requires a the capacity to react very quickly but the associated efforts are not always the most important. The overall crisis context may make things more difficult but, unitarily, actions are assessed at a low level of difficulty.

2.4.3 Security-related projects

This section is the result of the work of our teams specialising in infrastructure security and the implementation of security technologies.

The contribution of these teams is one of the new features of this version of the report. It complements the points of view of teams exposed to the threat by the contributions of a team that takes action using a prevention approach outside or after the time of the incident or crisis.

NDR deployment in practice

The deployment of NDR probes has emerged as the logical follow-up to EDR for several organisations. In the field, the observation is recurrent: organisations have realised that it is no longer enough to monitor the terminals. Attackers move sideways in the network and the EDR does not provide clear visibility of the attack chain, and it is precisely this missing visibility that NDRs bring. Last year, the discussions were aimed at explaining the concept and justifying the investment. Now, it's all about deployment. Proof-of-concept (PoC) has been replaced by production and teams report actual detection cases because they are able to visualise malicious interconnections between previously isolated assets and alerts: internal recognition attempts, which result in abnormal connections to sensitive areas before sequencing on suspicious movements between servers and outwards.

Combining this vision with other SOC alerts further enhances the relevance of the SOC giving analysts a broader and more precise field of view. But this new enrichment has a price: the multiplication of the data to be processed. In this, market solutions have a strong interest in implementing agile analysis and sorting models because just as much as the EDR if not more, the NDR needs context and customisation. By giving users the opportunity to integrate the mode of operation of their IS into the tool, it will be even more able to identify deviant behaviours. This is also why these solutions require stronger support compared to EDR: NDR requires a more mature approach and an overall understanding of the monitored infrastructure in order to optimise its operation and fully exploit its capabilities.

Bastions and PAM: in addition to the deployment, the quality of implementation

Deploying a bastion is not enough: it must still be done correctly. The teams found implementations that create a false sense of security. The most difficult example still concerns the bastions with two-factor authentication by email where the second factor has the same vulnerabilities as the first. Strong authentication requires real technical solutions: mobile app authentication, physical token or biometrics.
In addition to the technical aspects, the real difficulty with PAM projects is often related to change management and team buy-in. Many users perceive the bastion as an extra layer of defence that complicates their daily access. This negative perception can hinder their cooperation, reduce the quality of deployment and even lead to dangerous work-arounds.
Moreover, the bastion cannot be thought of in isolation. Its deployment must be part of a global security roadmap, including by implementing a tiering model for the Active Directory. Without this segmentation into privilege levels (tier 0 for critical resources, tier 1 for servers, tier 2 for workstations), even the best configured bastion will not be able to prevent an attacker from escalating privileges.

The "MFA + Tiering + Bastion" triptych can be used to significantly increase the level of security and robustness in coping with an attack.

IAM and PAM: accelerating cloudification

The migration of identity and privilege management solutions to the SaaS cloud accelerated significantly this year. More and more organisations wanted to be supported to move away from their IAM and PAM on-premise infrastructures to SaaS cloud solutions. The motivations are clear: simplified management, rapid deployment of new functions and reduction of technical debt. However, this transition imposes specific requirements. SaaS cloud identity security solutions require in-depth thinking about federation architecture, resilience to vendor unavailability, and mastery of strong authentication mechanisms adapted to distributed uses.

For SaaS cloud PAM solutions, attention should be focused on network segmentation and only unidirectional on-premise access flows to SaaS cloud, to prevent a cloud compromise from opening up direct access to critical on-premise resources. "Cloudification" is not just a technical migration: it is a redesign of the control model that must anticipate failure scenarios.

Increase in attacks, globalisation, intensification: the cyber threat continues to develop into a threat of the highest order capable of impacting entire sections of society anywhere in the world.

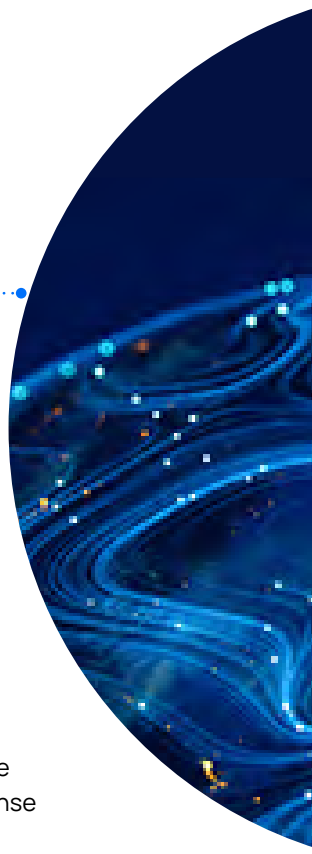
A look back at some of the highlights of the past year.

03

Highlights of 2025

3.1 A THREAT MARKED BY GEOPOLITICS

The year 2025 confirmed what observers anticipated: the cyber threat is no longer just a technical or criminal issue, it has become a geopolitical point of leverage in its own right. In every major conflict, the cyber dimension has emerged as a parallel battleground, sometimes even as the weapon of choice for hybrid warfare strategies.



3.1.1 / Russia: hacktivism, APT and hybrid warfare

The Russian-Ukrainian conflict has continued to generate a steady stream of cyber destructive operations against Ukrainian energy infrastructure. This trend, observed by aDvens as early as the summer of 2023, was clearly confirmed in 2025 in the broader context of campaigns run by players in the pro-Russian threat.

As for hacktivism, NoName057(16) has established itself as the most prolific group. Active since 2022, it led numerous large-scale DDoS attacks against governments, the media and the financial sector. The cyber group Army of Russia Reborn (CARR), suspected of being funded by GRU 74455, carried out opportunistic attacks on critical infrastructure, including in the United States, using advanced DDoS tools. Other groups such as Void Blizzard have also embarked on cyberespionage through phishing campaigns.

Priority targets in 2025 included Europe with sustained attacks on Spain, France, Italy, the Czech Republic and the United Kingdom, targeting organisations supporting Ukraine. The financial sector was particularly hard hit with a 105% increase in DDoS, including NoName057(16) which executed 98 transactions. **Israel** suffered a coordinated wave in October 2025 with spikes in DDoS attacks against the government and critical sectors in response to geopolitical events.

Operation Eastwood, coordinated by Europol and Eurojust in July 2025, targeted NoName057(16), dismantling more than 100 servers, and arrested two members.

APT groups have intensified their campaigns. APT28 (Fancy Bear), linked to the GRU, conducted multilingual credential theft campaigns using fake login portals, targeting energy, military and think tank organisations in Europe, North America and Central Asia. APT29 (Cozy Bear), associated with the SVR, focused on diplomatic espionage through watering holes campaigns and cloud compromises, targeting governments and diplomatic institutions to steal strategic information. Sandworm (APT44), another GRU affiliate, carried out destructive attacks on Ukraine's critical infrastructure, deploying wipers like ZEROLOT on the energy and logistics sectors in coordination with military operations.

ESCALATION ON OT SYSTEMS

With regard to industrial systems, attacks follow a recurring pattern: targeting SCADA systems and human-machine interfaces (HMIs) exposed over the internet through network scans, initial access via default passwords or exploitation of vulnerabilities, and manipulation and disruption of control systems without lateral movement on the victim's network. These disturbances are systematically captured in videos and published on the groups' Telegram channels.

Although rudimentary at first, TTPs are perfected. TwoNet successfully exploited the XSS vulnerability CVE-2021-26829 in OpenPLC ScadaBR in September 2025. Most importantly, the impact, hitherto limited to simple control disruptions, has recently had disastrous consequences on physical systems. Danish military intelligence officially linked Z-Pentest's activity to Russia in December 2025, following the attack on the Køge sewage treatment plant in 2024: the disruption of orders had altered the pressure of pumps causing pipes to explode and paralysing the distribution of drinking water.

Attacker: Z-PENTEST/Z-ALLIANCE

Country: Russia

Allies / Partners: NoName057 (16), sector16, CARR (cyber Army Of Russia Reborn)

Motivation: influence/disinformation, political activism, pro-Russian narrative

Capacity: Brutforce, scanning tools (nmap), exploitation of exposed VNC connections and weak default passwords to access industrial control devices (HMI, PLC), manipulation of industrial control systems.

Infrastructure: Hack-and-leak, Telegram channel, unknown C2, Telegram and X coordination, decentralised and anonymous operation and collective.

Target countries: United States and Western countries, as well as any country ally or Ukraine sympathiser.

Areas targeted: Energy, water, food, industrial infrastructure.

The forces involved are changing: Z-Pentest, renamed Z-Alliance, involves several members of the groups NNM057(16) (formerly NoName057(16)) and CyberArmy of Russia Reborn, two historical spearheads of the pro-Russia hacktivist threat. Z-Pentest's claims appear on NNM057's Telegram channel(16). Even the DDosia Project platform, developed to offer a DDoS attack kit to volunteers, has evolved into attacks on OT systems. Targets appear to be coordinated between these groups with DDoS attacks sometimes serving as a diversion.
Numerous waves of DDoS and various cyberattacks have had spillover effects in Europe with collateral effects on NATO allies, such as disruptions in Poland and Germany. Geopolitically, these attacks have magnified Russia's isolation.

3.1.2 China: spying and strategic pre-positioning

The Defence Intelligence Agency identified China as the most persistent cyber threat in 2025. The Volt Typhoon and Salt Typhoon groups, affiliated with the People's Liberation Army (PLA), **infiltrated critical US infrastructure** (pipelines, power grids) using a "pre-positioning approach" aimed at creating offensive capabilities that can be mobilised in the event of a conflict on Taiwan. A Chinese cyber threat group exploited Anthropic's Claude model **to infiltrate about 30 global organisations**, including US tech companies specialising in AI and semiconductors, by extracting sensitive data.

In the South China Sea, **cyberattacks against the Philippines** have increased: DDoS on ships and airports to contest land claims without direct confrontation. **In January 2025**, **hackers** linked to APT41 and Salt Typhoon **infiltrated the office of President Ferdinand Marcos Jr., stealing sensitive military documents** related to the territorial dispute, including defence plans and maritime patrol data around the Second Thomas Shoal.

These actions have intensified tensions with the United States, strengthened alliances like the AUKUS and accelerated the cybersecurity race in the Indo-Pacific where China is using cyber to assert its regional dominance.

3.1.3 India-Pakistan: when cyber paralyses a country

In May 2025, Pakistan, with alleged Chinese support, launched a massive cyberattack against India hitting 10 SCADA energy systems, wiping out 1,744 servers and crippling Mumbai's metro, stock exchange and Delhi's rail and gas infrastructure. **More than 150 databases were stolen, and government, media and corporate websites were disfigured**. This event exacerbated border tensions with India accusing the Pakistani ISI and pointing Chinese links via APT malware. Geopolitically, this has forced India to diversify its alliances, strengthening its partnerships with the United States and Israel for cyber defence, while Pakistan relies on China for electronic warfare and jamming capabilities.

3.1.4 / North Korea: social engineering and funding of the regime

North Korean APT **campaigns have increased their focus on long-term economic espionage and infiltration operations**, orchestrated by Lazarus (APT38), Kimsuky (APT43) and Konni (APT37), supported by the Pyongyang regime to fund nuclear programmes and gather strategic intelligence.

These players have demonstrated **advanced social engineering capabilities, leveraging artificial intelligence for more realistic and scalable attacks**: multilingual phishing campaigns using fake job offers or Google Ads redirects, targeting developers and institutions with operations that are spread multiple years.

Kimsuky has distinguished himself through stealth malware and "living-off-the-land" campaigns, hijacking Threat Intelligence platforms to identify vulnerabilities and infiltrate South Korean, American and European networks, targeting primarily the diplomatic, military and high-tech sectors for the purpose of cyberespionage.

Lazarus has continued its financial attacks using malware like Troll Stealer, integrating influence operations to undermine the trust of rival hackers while targeting critical industrial infrastructures using AI techniques and breaches of trusting relations.

Konni initiated targeted phishing via malicious VS Code projects and Android campaigns with remote removal features targeting developers and mobile users in South Korea in order to install persistent backdoors and carry out cryptocurrency mining.

Andariel exploited EtherHiding on the blockchain for espionage and financial operations focusing on the technology and financial sectors.

GRAPHITE, SPYWARE AT THE SERVICE OF THE STATES

Graphite spyware, developed by Paragon Solutions, is a mobile surveillance solution designed to allow stealthy compromise of iOS and Android devices including through zero-click capabilities for state intelligence purposes.

In 2025, several operational uses were documented. Earlier this year, a campaign exploiting a zero-click vulnerability within WhatsApp was detected and neutralised by Meta. The operation targeted approximately 90 people in more than 20 countries, mainly journalists and members of civil society, illustrating selective targeting with high information value.

At the same time, independent forensic analysis has confirmed actual compromises of iOS devices through the exploitation of zero-click vulnerabilities in iMessage, confirming the actual operational use of spyware and not limited to intrusion attempts.

3.2 ARTIFICIAL INTELLIGENCE, A CATALYST OF THREATS

3.2.1 / AI at the service of all attacker profiles

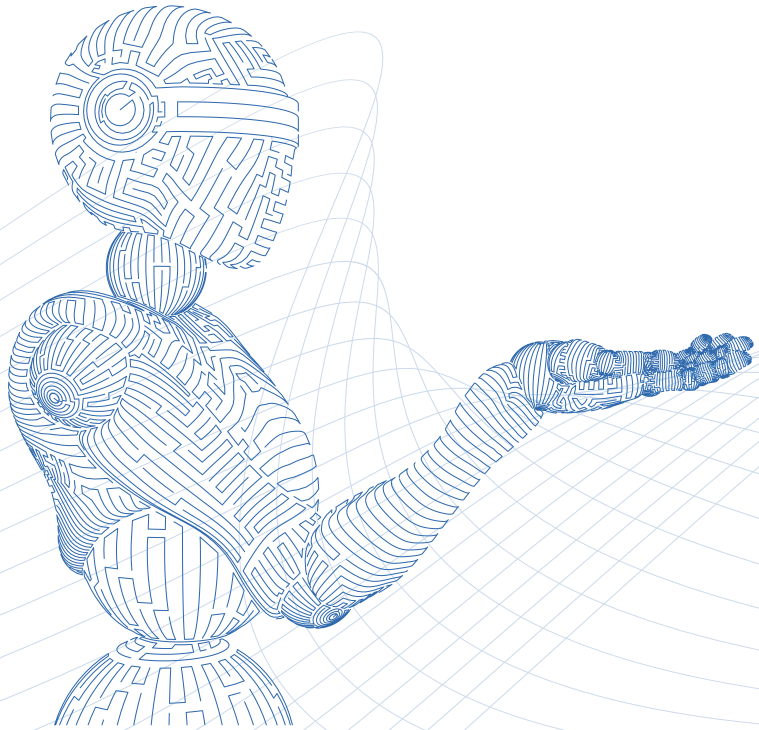
Norton's typology of cybercriminal archetypes identifies six main categories of actors: hacker, advanced and persistent threat (APT), malicious employee, "script kiddie", hacktivist and crook.

In 2025, the malicious exploitation of artificial intelligence spread across all these profiles, contributing to a widespread rise in the sophistication of cybercriminal activity.

> AI is expanding capabilities and contributing to the further industrialisation of cybercrime.

AI acts as a multiplier of capabilities, leading to the optimisation of existing techniques as well as the emergence of new modus operandi. It facilitates recognition automation, dynamic generation of malicious charges, and the real-time adaptation of attacks to target environments. This convergence between advanced automation and responsiveness produces cyberattacks and online fraud that stand out for a high level of credibility, consistency and operational precision. Analysis of malicious code developed with AI assistance reveals the growing integration of advanced techniques: sophisticated obfuscation mechanisms including steganography, exploitation of innovative attack vectors such as zero-click phishing attacks.

More broadly, **artificial intelligence is contributing to the further industrialisation of cybercrime**. It enables the large-scale production of modular, adaptable and hard-to-detect malicious tools increasing the resilience of attacks to traditional defence mechanisms. This phenomenon accentuates the imbalance between offensive and defensive capabilities posing new cybersecurity challenges.



3.2.2 / Malware that adapts on the fly

The year 2025 was marked by the emergence of experimental software capable of executing malicious actions with an unprecedented level of autonomy, reducing or eliminating the need for direct human intervention. These next-generation malware exploits generative AI to produce code on the fly,depending on their execution environment and constraints.

Prototypes like Promptlock illustrate this paradigm shift. Using large language models (LLMs), this type of software dynamically generates payloads, modifies its execution logic and adapts its behaviour in real time. This capability opens the door to unique, contextual and hard-to-replicate attacks, greatly complicating detection, analysis and remediation efforts. Unlike traditional malware, whose signatures and execution chains are relatively stable, these adaptive threats evolve continuously throughout their lifecycle.

> The year 2025 was marked by the emergence of experimental software capable of executing malicious actions with an unprecedented level of autonomy.

Although Promptlock comes from academia in an experimental and sympathetic setting, its fundamental principles were observed in malicious operational contexts. During 2025, several particularly complex malware cases were reported, illustrating a gradual appropriation of these concepts by advanced actors. Examples include PromptSteal, a tool attributed to campaigns associated with the Russian group APT28, which reportedly exploited language models such as Qwen2 to support some of its offensive features. These developments would indicate and development towards cybercriminal arsenals incorporating autonomous components, capable of "reasoning", adapting their strategies and optimising their actions without constant human supervision.

3.2.3 / North Korea: AI as a leverage point for strategic resilience

OSINT exploration by the aDvens CERT has gathered a body of information that provides insight into the development of the North Korean cyber army and its criminal use of artificial intelligence.

The results show that this development is strongly marked by the emergence of Unit 227, whose operational activity dates back to 9 March 2025. The rise of this unit, characterised by its use of state-controlled artificial intelligence (domestic AI), marks a transition from a previously decentralised and trade-dependent (democratised AI) to a new, much more resilient hybrid model. The North Korean regime can now rely on this structure, which combines democratised AI tools with locally controlled systems, to strengthen its capabilities, technological independence and efficiency. The information gathered highlights a broader transformation within the cyber army as a whole. While the use of AI once seemed decentralised and limited to a limited number of APT groups, it has now expanded, systematised and integrated across cyber forces. APTs use AI in all intrusion tactics and techniques, even implementing chains of infection and money laundering which is extorted using automated mechanisms by multiple synthetic agents.

3.2.4 / Industrialisation of attacks: a previously observed phenomenon

Some aspects of the AI-induced technological shift in cybercrime are not entirely new. The increased ease of access and efficiency offered by AI echo the phenomena observed over the past two decades.

This parallel is particularly evident in the rise of "turnkey" malware generators, such as virus and worm builders (e.g. Kalamar VBS Worm Generator), and distributed denial of service (DDoS) attack tools such as Low Orbit Ion Cannon. Designed by technically competent developers, these tools have acted as real portable and versatile cyberattack laboratories.

By significantly lowering the technical barrier to entry, these solutions have enabled individuals with limited skills, whether opportunistic hackers or inexperienced cybercriminals, to carry out complex attacks and cause significant impacts. This democratisation of the offensive capability has contributed to a quantitative and qualitative increase in security incidents, regardless of the actual level of expertise of the attackers.

Artificial intelligence is now part of a comparable dynamic, but on a much broader scale. **Where tools of the past mainly automated technical actions, AI now also automates creativity, contextual adaptation and psychological manipulation**. This paradigm shift marks a profound evolution in cybercrime: the industrialisation of the attack is no longer limited to code, but now encompasses human cognition and emotions as a vector of exploitation (e.g. "vibe hacking").

3.2.5 / Exploitation of psychological flaws

The criminal use of artificial intelligence allows attackers to significantly increase the technical credibility of their attacks. However, beyond the strictly technological dimension, psychology plays an equally decisive role. Qualitative improvements in AI also result in enhanced psychological countermeasures commonly associated with social engineering techniques.

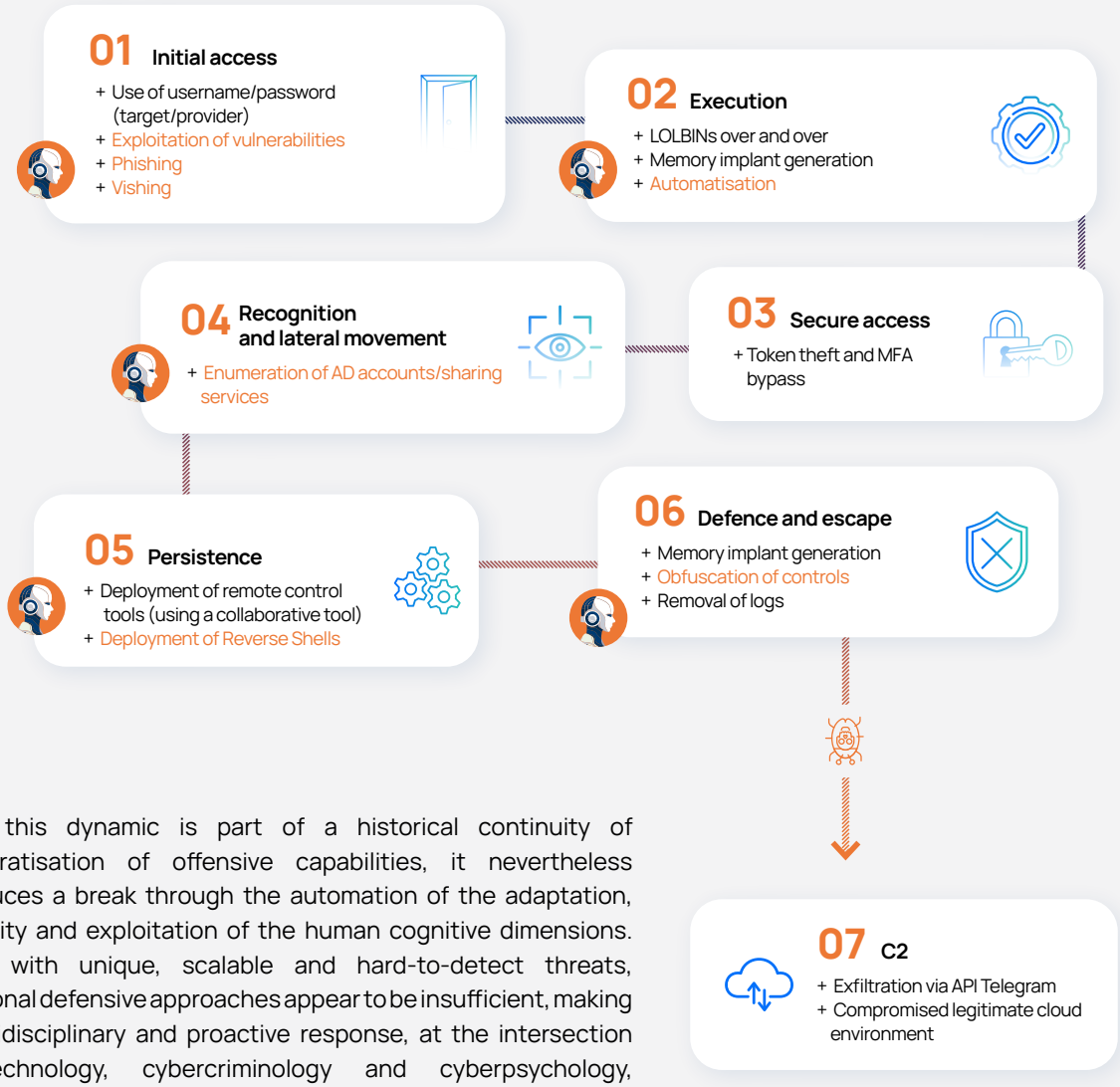
Thanks to AI, cybercriminals are now able to design and disseminate highly credible resources to fuel these psychological countermeasures: textual, visual or audio content, which is increasingly realistic and personalised.

In this context, the intersection between cyberpsychology and cybercriminology is particularly important for the following four main reasons:

1. Identifying and detecting psychological countermeasures more effectively
2. Understanding and explaining human behaviours involved in the criminal exploitation of AI
3. Anticipating cybercriminal behaviour and its development
4. Developing models of resilience based on psychological counter-countermeasures to neutralise the effectiveness of psychological countermeasures

3.2.6 / A major turning point in the evolution of cybercrime

The change observed between 2024 and 2025 marks a major turning point in the transformation of cybercrime, now deeply structured around artificial intelligence. AI is emerging as a cross-cutting capability multiplier across cybercriminal archetypes, fostering the industrialisation of attacks, the emergence of standalone malware capable of self-adapting on the fly, and the systematic integration of AI into increasingly resilient state arsenals, as illustrated by the North Korean hybrid model.



While this dynamic is part of a historical continuity of democratisation of offensive capabilities, it nevertheless introduces a break through the automation of the adaptation, creativity and exploitation of the human cognitive dimensions. Faced with unique, scalable and hard-to-detect threats, traditional defensive approaches appear to be insufficient, making a multidisciplinary and proactive response, at the intersection of technology, cybercriminology and cyberpsychology, indispensable.

Find out more

To learn more about AI security, see our **Introduction to responsible AI white paper**.

RETURN OF LAND

CERT ADVENS

AI IN PHISHING CAMPAIGNS

During its investigations, following alerts from the aDvens SOC or during response to incidents, the aDvens CERT regularly observed the use of artificial intelligence to reinforce attacks. The use of AI automates certain forms of attacks, which complicates their detection and reduces the time it takes to act on compromised infrastructure.

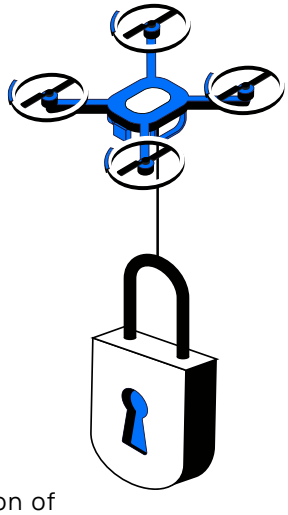
Artificial intelligence is now a major leverage point for attackers, allowing them to industrialise and perfect phishing campaigns. It significantly improves the credibility, stealth and effectiveness of attacks along the entire intrusion chain:

- **Resource Development**: AI is used for the automated generation of phishing content of very high linguistic and contextual quality (emails, web pages, attachments), combining sophistication, narrative coherence and personalisation. These resources, which are difficult to distinguish from legitimate communications, significantly increase the success rate of attacks.
- **Initial access**: attackers exploit AI to design malicious charges hidden in seemingly innocuous files, including images, using advanced steganography techniques. This approach circumvents traditional detection mechanisms by masking malicious code in media that is perceived harmless.
- **Execution**: in some scenarios, hidden code is assembled in such a way as to incorporate an exploit that can be used for automatic execution, without explicit user action. These so-called "zero-click" attacks exploit software vulnerabilities and pose a particularly critical threat because they destroy human vigilance mechanisms.
- **Defence evasion**: AI facilitates the integration of advanced obfuscation techniques, such as "junk code", false logic loops or misleading conditional structures. The goal is to disrupt both antivirus engines and human analysts, slowing down or distorting the interpretation of actual malware behaviour.

Impact

Malicious actions from an AI-enriched arsenal are characterised by their immediacy: instant redirection to a malicious URL, automatic opening of booby-trapped documents or the rapid triggering of payloads. From a cyber-psychological point of view, this speed is particularly worrying, as it drastically reduces the reaction time of the user, preventing them from reasoning, doubting or detecting the low-level signs of an attempted attack.

AI IN INTRUSION TESTING – ANOTHER RACE BETWEEN ATTACKERS AND DEFENDERS



The ecosystem of AI-assisted pentest tools is growing rapidly. PentestGPT, PentAGI, PentestAgent, HexStrike AI and Reaper illustrate the rise of autonomous agents capable of linking recognition, use and reporting. At the same time, vulnerability discovery capabilities are reaching an unprecedented level: in February 2026, Anthropic revealed that its Claude Opus 4.6 model had identified more than 500 critical vulnerabilities in open-source production projects. Some had been present for decades undetected despite years of human review and intensive fuzzing.

The difference? Unlike traditional tools that look for known patterns, Claude reasoned on the code: it tracked data streams, analysed commit history for partially fixed bug variants and identified risky execution paths that the fuzzers never explored.
These advances are of benefit to attackers as well as defenders. In this race, not integrating AI into its practices is tantamount to denying one advantage that has become strategic.

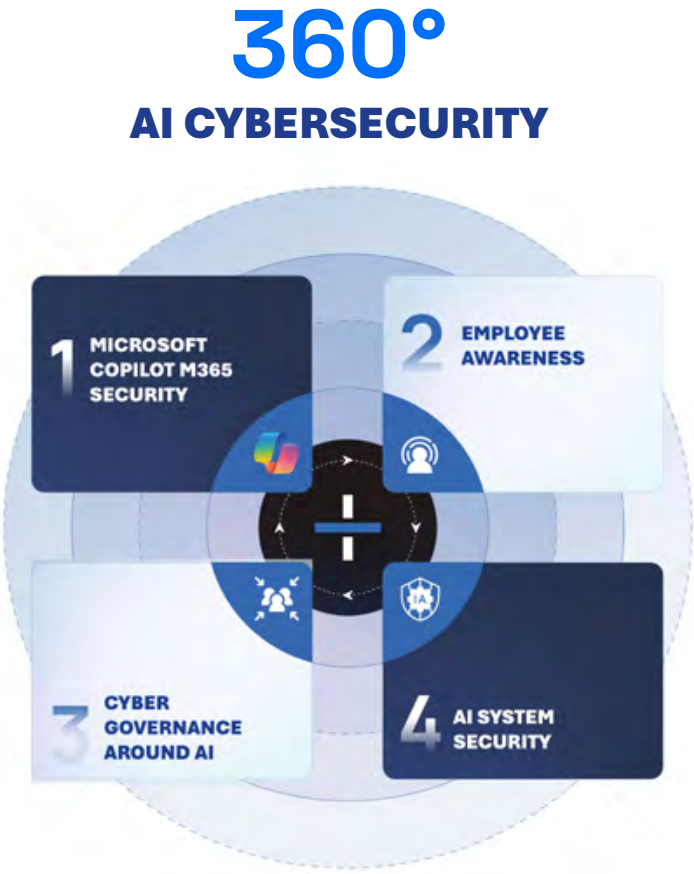
At aDvens, generative AI has become a real point of leverage for offensive teams, especially in the information search and consolidation phases. During an intrusion test, a pentester continuously manipulates heterogeneous data: define the right recommendation for each discovered vulnerability, correlate the results with the security repositories (OWASP, MITRE ATT&CK, CIS, ANSSI guides), analyse and synthesise large volumes of outputs (scans, logs, HTTP responses), enrich the analysis with internal knowledge bases.

Solutions like Ollama are used to deploy local high-performance models (Llama, Mistral, Qwen) to accelerate this synthesis and contextualisation work complementing the traditional tool chain (Nmap, Burp Suite, BloodHound, Nuclei). AI does not replace the pentester: it is always the human who guides testing, builds attack chains and adapts its approach to the customer's business challenges. It saves them time on mechanics so they can focus on what makes a difference: strategy, analysis and intuition.

The other area with high added value is the production of deliverables. aDvens is gradually integrating a local LLM directly into its reporting tool, which is a function that is continuously improving.

The use cases are practical: spelling and syntax correction, reformulation of technical passages for different levels of reading, generation of drafts of managerial syntheses or techniques, transformation of raw ratings into structured content, consolidation of recommendations based on internal benchmarks and market standards.

The approach is augmented pentester: AI as a copilot, i.e. not at the controls, with systematic human control over each deliverable. Local models are advancing rapidly and interoperability standards such as the Model Context Protocol (MCP) are opening the way for smoother orchestration between Pentester tools and AI. The aDvens teams are maintaining active monitoring and continuing their experiments to integrate these advances over time.



WHAT AI SECURITY TECHNOLOGY?

In order to control the uses of AI, the data must be protected in its entirety, including that input to generative AI. As always, this protection is based on a triptych: human / organisation / technology.

On the technological side, the market is rapidly adapting to this new demand. For example, with Purview, Microsoft offers governance and data protection features.

In addition to the classification and labelling modules for accessing the data and documents on the holder to be limited by a mastered model, new modules offer a global view of AI interactions (including Shadow AI) and carry out checks or sensitisation in the event of the presence of sensitive information in the user prompt.

The implementation of Purview DLP policies has already detected bad practices: sales teams were asking an AI to reformat files containing hundreds of prospective customers. These are strategic and personal data that could be publicly accessible.

Major cybersecurity publishers have also accelerated their acquisitions of startups specialising in AI security. SentinelOne has purchased Prompt security, a solution dedicated to detecting and preventing prompt injection attacks and securing interactions with LLMs. Similarly, Palo Alto Networks acquired Dig Security to strengthen its data protection capabilities in cloud and AI environments.

These initiatives demonstrate market awareness: securing AI is not just about protecting the model itself but requires a holistic approach that integrates data security, access governance, detection and protection from malicious manipulations.

AI, AMPLIFYING THE RISK OF MISINFORMATION

AI and AI-based attacks can amplify other risks, apart from cyber risks, including those related to misinformation and information manipulation. Generative AI can facilitate the large-scale production of ultra-realistic audiovisual content (deepfakes, voice cloning, synthetic videos) capable of deceiving even informed observers. Poisoning AI models can also lead to the mass dissemination of biased or false information through referral systems or conversational assistants.

A recent example illustrates this threat: during the European elections in 2024, several disinformation campaigns exploited deepfake audio from politicians to spread false statements on the social networks. In another case documented in 2025, malicious actors poisoned the public datasets used to train text generation patterns, introducing systematic biases aimed at discrediting certain legitimate sources of information.

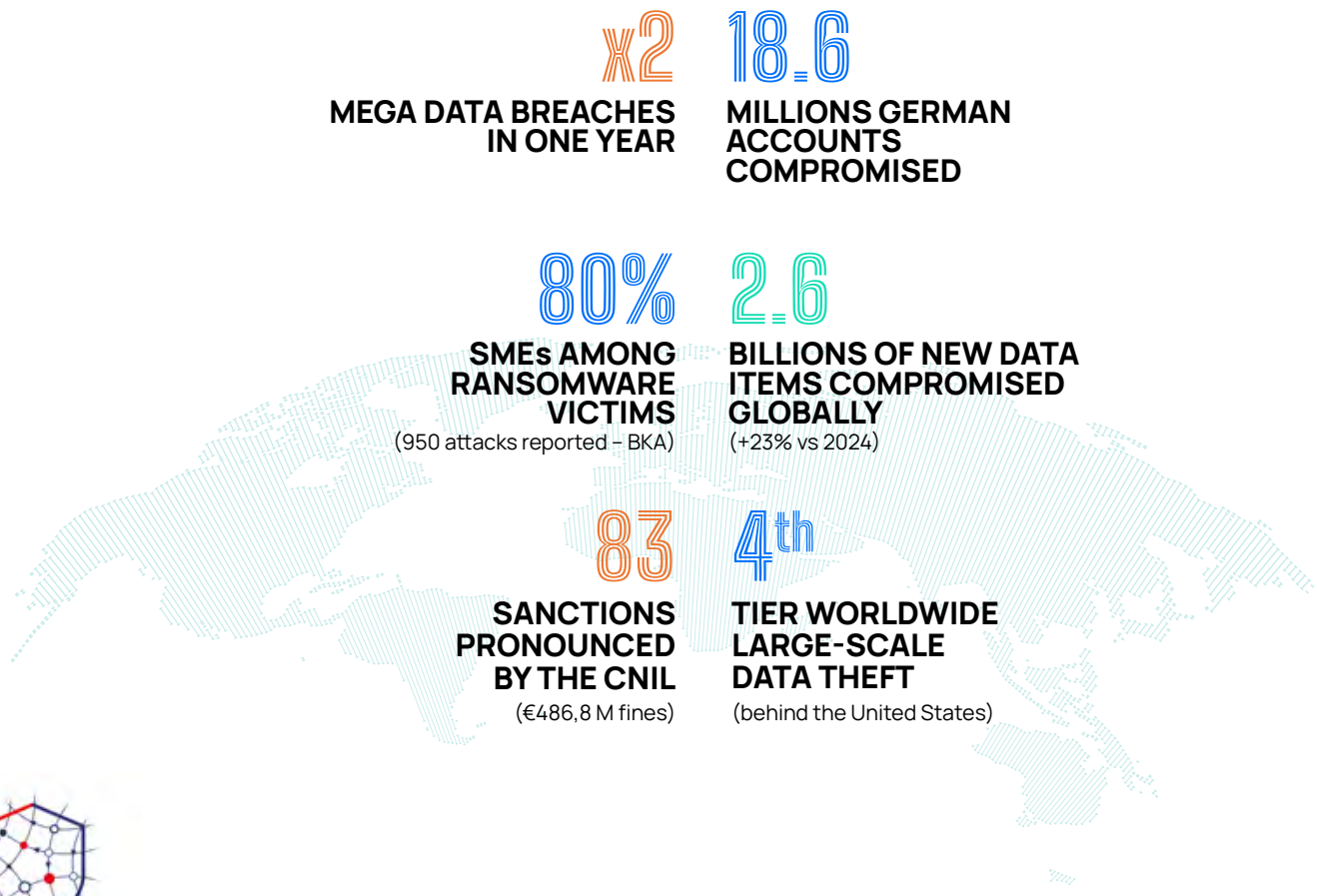
Faced with these risks, aDvens launched the cyber For Good programme through the aDvens For People and Planet endowment fund in partnership with **Viginum**, and **the vigilance and protection service against foreign** digital interference attached to the General Secretariat of Defence and National Security ("SGDSN"). The main goal of the programme is to raise awareness among independent journalists and journalists of the regional daily press about AI-assisted information manipulation techniques, synthetic content verification methods and good practices for securing their sources and communications.

3.3 EFFECTIVE AND REPEATED DATA THEFT

3.3.1 / Germany, a European epicenter of data theft

In 2025, Germany has become one of the countries most affected in the world by massive theft of personal data. According to Surfshark's annual report, 18.6 million German accounts were compromised over the year, placing Germany on place 4 in the world behind the US, France and India. Globally, more than 2.6 billion new data items were compromised, up 23% from 2024. The structural trend is particularly worrying: according to the CNIL (Commission Nationale de l'Informatique et des Libertés), the number of breaches affecting more than one million people has doubled in one year. Moreover, in 2025, 83 penalties were imposed by the CNIL, for a total amount of €486,839,500. The number of reported ransomware attacks remained largely unchanged at 950, according to the German Federal Criminal Police Office (BKA). Cybercriminals continued to rely on the successful attack strategies of recent years. As a result, an increasing number of small and medium-sized businesses were targeted (accounting for 80% of reported incidents).

In most cases, these attacks also led to data leaks—or threats of data leaks—for which victims currently have no effective mitigation strategies. While backups remain essential for defending against ransomware, they do not protect against data leaks.



VIGINUM

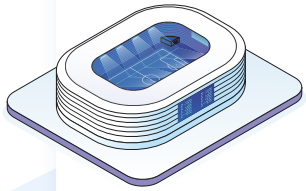
THREE ICONIC ATTACKS OF 2025

→ Bouygues Telecom (August 2025)

In the middle of the summer, Bouygues Telecom confirmed unauthorised access to the data of 6.4 million customers, including contact information, contractual information and IBAN codes. This attack is part of a systematic targeting of the telecoms sector: after Free (19.2 million accounts at the end of 2024) and SFR (3.6 million in September 2024), the entire French telecom ecosystem has been exposed. ANSSI describes this sector as "supercritical" and has documented over 150 major safety incidents since 2020. The common denominator: massive databases, insufficiently secure access and data that can be directly exploited for bank fraud.

→ Marks & Spencer and the UK retail wave (April-May 2025)

The United Kingdom was hit in the spring by a wave of cyber attacks that demonstrated that data theft is a European problem, not just a French one. In April, retail giant Marks & Spencer was the victim of a social engineering attack by the Scattered Spider group, via the compromising of accounts of an external service provider that was managing its support services. The DragonForce ransomware then encrypted virtual machines hosting customer data. The result: online sales suspended for several weeks, personal data of many stolen customers (names, addresses, dates of birth, order histories) and an estimated financial impact of €355 million. A few days later, Co-op and Harrods suffered similar attacks. The same group, the same modus operandi, three major British brands affected in a few weeks.



→ Ministry of Sport – Pass'Sport (December 2025)

A few days before Christmas, the Ministry of Sport revealed the exfiltration of data related to the Pass'Sport system, affecting nearly 3.5 million households. A 15 GB file was extracted, combining data from three separate agencies — CAF, MSA and CNOUS — aggregated in the aid management system. The attack highlighted a classic but persistent problem: insufficiently constrained interfaces for accessing data, making it possible to go from consulting a single file to the aspiration of the national database.

A SPECIAL CASE: SPORTS FEDERATIONS IN THE CROSSHAIRS

In 2025, the world of sport focused particular attention on cybercriminals with consequences that go beyond mere data theft. The attack on the French Shooting Federation (FFTir) discovered in October 2025 illustrated why this type of target is sensitive. Data from 250,000 active shooters and 750,000 former members has been leaked to the dark web, including marital status, postal addresses, emails and phone numbers. The peculiar feature of this leak: a large proportion of the persons concerned are legal owners of weapons in their homes. The postal address of a legal arms owner is precisely the type of information that interests criminal networks well beyond conventional phishing. The French Cycling Federation also reported a data leak at the end of the year, pointing out that this sector, which is poorly protected in terms of cybersecurity, presents attractive attack surfaces for attackers seeking large databases.

3.3.2 / Formative commonalities

In addition to their scale, these attacks share characteristics that make them a core trend rather than a series of isolated incidents.

The third vector is omnipresent. At Marks & Spencer, the entry point was an external IT support provider. For Pass'Sport, aggregating data from multiple agencies into a shared system created a value target. This bounce approach using the digital supply chain has become the preferred modus operandi: we reach an organisation by targeting its weakest links.

Shortcomings with the basics remain very common. Undetected social engineering, unrestricted query interfaces, data stored beyond their useful life, overly broad access rights granted to partners: in each of these cases, the incidents were made possible by deficiencies in basic security measures rather than the exceptional sophistication of the attacks.

The motivation is almost exclusively financial. Stolen data are systematically sold on the dark web or exploited for phishing, bank fraud and identity theft. France is a particularly attractive target: the available bases are large and can be cross-referenced. In addition, an active French-speaking cybercriminal community has turned French data aggregation into a structured illegal market.

3.3.3 / A threat that affects all organisations

There is still a misconception that data theft affects only the large organisations subjected to direct attacks. The reality is quite different and concerns every structure, regardless of its size.

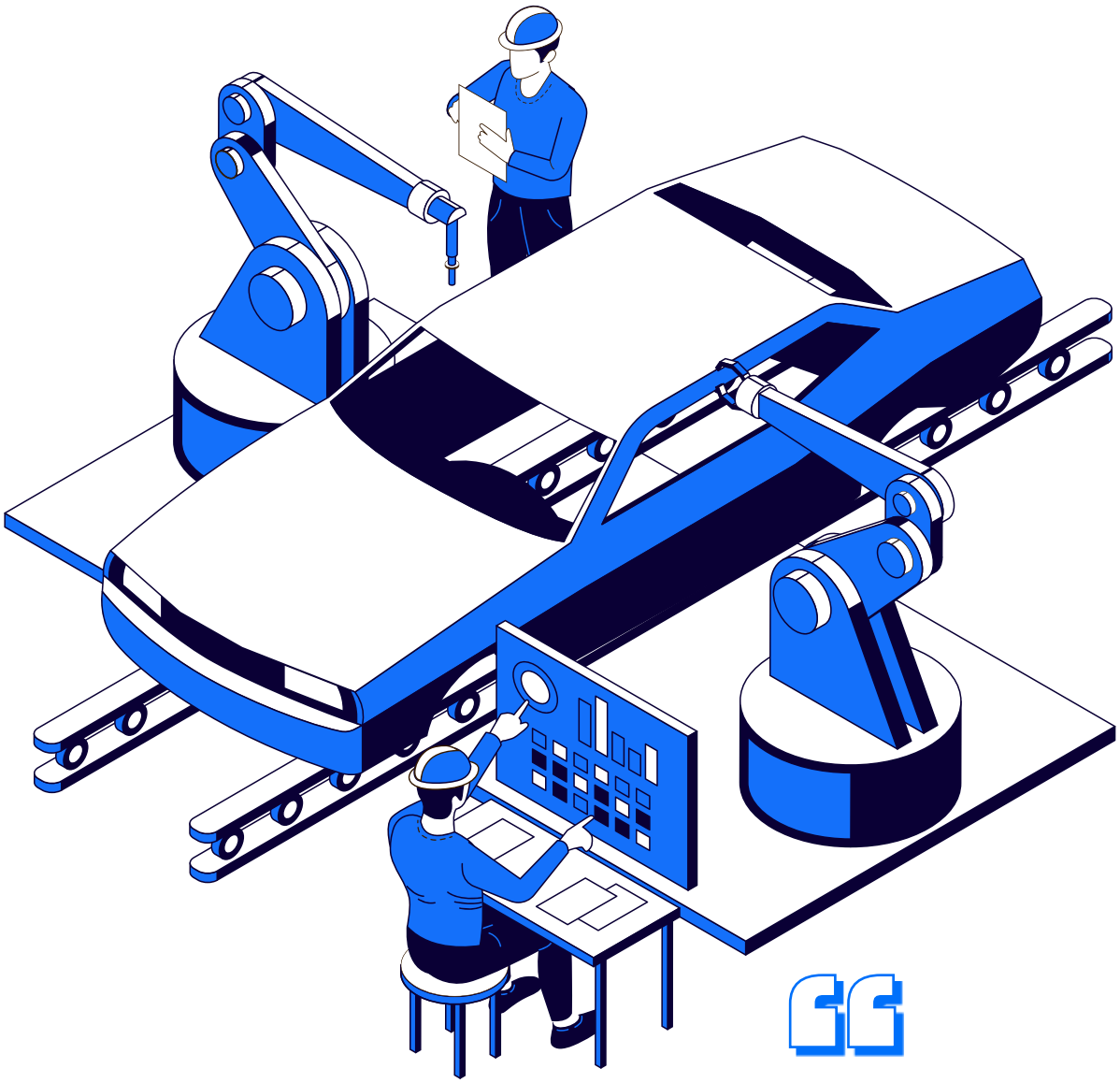
On the one hand, any entity that collects and stores personal data is a potential target. SMEs, associations and communities are not immune — they often present an attractive attack surface precisely because their defences are more limited. On the other hand, the employee data of an organisation almost inevitably finds its way into one of the major leaks of recent years (thereby maximising the chances of having complete user profiles). An employee, whose address appears in the Pass'Sport database or whose credentials have been leaked via an infostealer, becomes a prime target for a social engineering attack targeting their employer. In this sense, the aDvens For People and Planet endowment fund supports awareness-raising and support programmes for the least mature populations, either by reaching out to young people or by reaching out to certain structures neglected by the cybersecurity market such as NGOs or social and solidarity economy players.

Find out more

What if the stolen data concerns your employees but your organisation is not the victim of the attack?
Check out the advice of our CERT.

3.4 THE COLOSSAL IMPACTS OF ATTACKS ON THE INDUSTRY

Cyberattacks targeting the industrial sector are no longer limited to isolated technical disruptions. They now strike at the heart of production tools, cripple entire supply chains and generate economic impacts that go far beyond the perimeter of the affected company. When OT environments are compromised, the consequences are measured not in hours of downtime, but in weeks of production downtime, hundreds of millions of losses and thousands of jobs at risk.



> It appears to be unprecedented in the UK for a cyber or ransomware attack to cause disruptions on this scale", and he added that the fact that thousands of jobs could be at risk"represents an entirely different order of magnitude".

Jamie MacColl, Research Fellow at the Royal United Services Institute

3.4.1 / The textbook case: Jaguar Land Rover

The attack on Jaguar Land Rover on 31 August 2025 is a striking example of this new reality. It is now considered the most expensive cyber attack in British history, with a total economic impact estimated at £1.9 billion.

The methods of attack

The intrusion was not based on a sophisticated technical vulnerability or zero-day exploit, but on the exploitation of fundamental weaknesses. The attackers – a collective composed of Scattered Spider, Lapsus$ and ShinyHunters – initially conducted targeted "voice phishing" **campaigns** posing as internal employees to obtain login details. Some of these stolen login details dated back to 2021 and were still working in 2025. Once in possession of legitimate accounts, that sometimes have administrator permissions, attackers were able to log into systems using normal authentication streams.

The lack of network segmentation then facilitated lateral movements. Attackers escalated their privileges, navigated through the IT environment and reached critical infrastructure. Screenshots of internal SAP systems were released and ransomware was deployed on compromised systems. Penetration was so deep that Jaguar Land Rover had to disconnect all of its IT systems globally – from dealer platforms to production lines – rather than isolate a compromised segment.

It is important to note that this attack took place in an already fragile context: in March 2025, the HELLCAT group infiltrated JLR systems via Jira credentials stolen by infostealer, extracting hundreds of gigabytes of internal data, including source code, development logs and employee information. This first breach had already revealed significant security gaps.

Impacts for the company

Production was interrupted as of 1 September 2025 and only gradually resumed as of 8 October, i.e. more than six weeks of total shutdown. The group's 39,000 employees were temporarily laid off for operational reasons. Wholesale volumes fell 43.3% in the third quarter of the financial year while retail sales declined by 25.1%. North America was particularly hard hit with wholesale sales falling 64.4%. Production did not return to normal levels until mid-November, and the re-routing of vehicles was very gradual.

To keep the company afloat, JLR had to obtain a £2 billion emergency credit line from a banking consortium. A £500 million support package has also been deployed to support key suppliers who are themselves seriously affected by the disruption.

Impacts on the UK economy

The shock wave spread far beyond the confines of Jaguar Land Rover. More than 5,000 UK organisations have been directly affected by the shutdown. UK car production fell by 27.1% in September 2025, with the Society of Motor Manufacturers and Traders (SMMT) explicitly pointing to "stopping production at Britain's largest car employer" as the deciding factor.

The Bank of England cited the attack as one of the key factors contributing to weaker-than-expected GDP growth in the third quarter of 2025. In its November 2025 Monetary Policy Report, it said the shutdown at JLR directly contributed to a 0.17 percentage point contraction in GDP in September helping to tip the economy into decline.

The social repercussions have been massive. Liam Byrne MP described the attack as a "digital siege" referring to supply chain employees "being made redundant by the hundreds "and fearing "thousands" of redundancies if the government did not intervene. The Unite trade union confirmed that employees in the supply chain had been advised to apply for Universal Credit. In response to the scale of the disaster, the UK Government provided a £1.5 billion loan guarantee to safeguard the future of the car manufacturer and the entire automotive industry.

VIEWPOINT

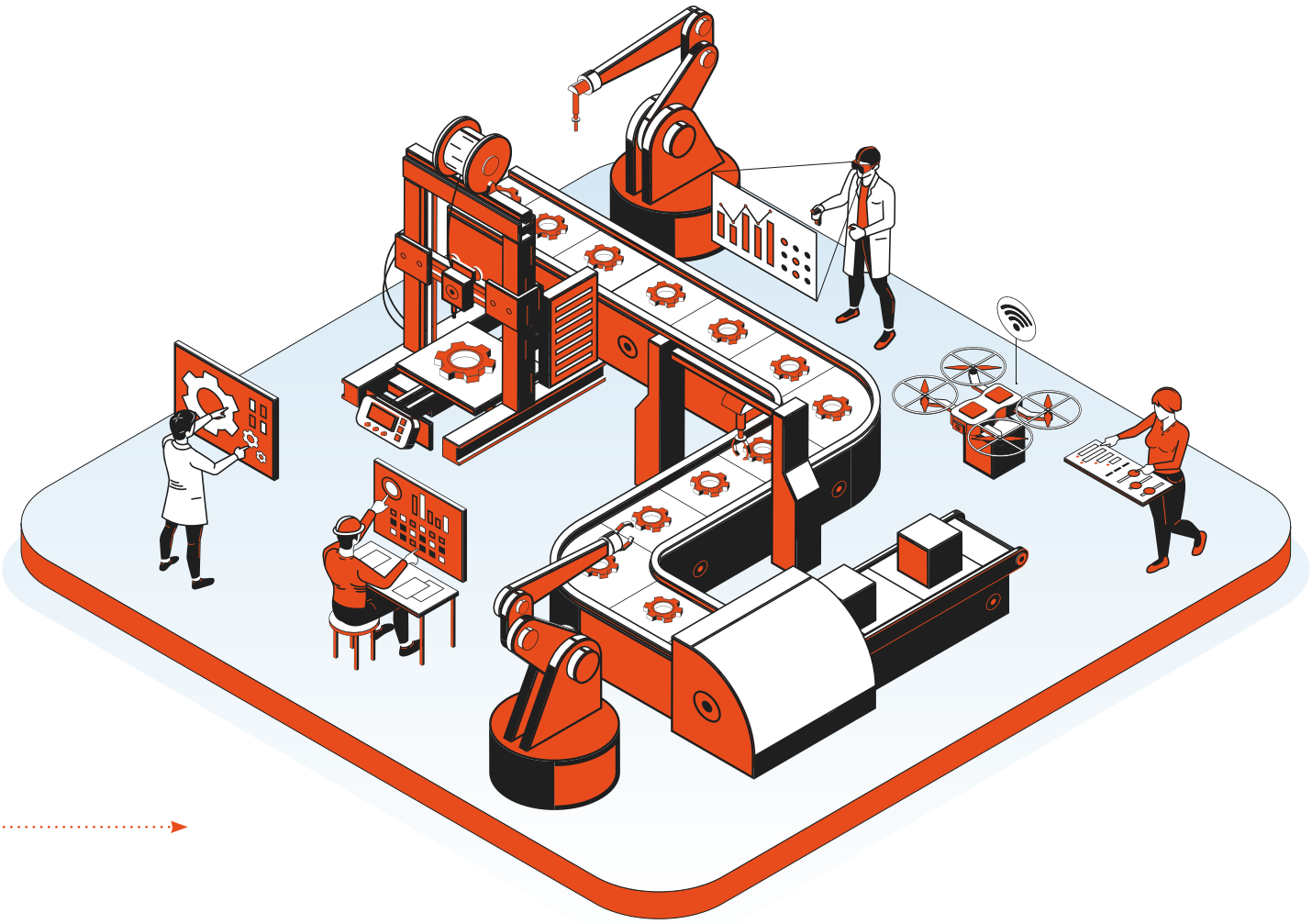
CERT ADVENS

IT for OT as a breaking point

When responding to an incident, aDvens CERT teams see a recurring pattern: the OT is usually not directly affected, but rather through the compromise of IT for OT – the IT systems that support, monitor or administer industrial environments. This distinction is critical because it reveals a snowball effect: once attackers compromise IT systems that drive or monitor OT, they can cause major operational impacts without even having to attack the PLCs or industrial control systems directly.

The attack on Matadero de Gijón in Spain, claimed by the RansomHub group in May 2024, illustrates this dynamic perfectly. The group did not directly compromise the slaughterhouse equipment but targeted the SCADA system controlling the bioenergy plant on site. The screenshots published by RansomHub show that they gained access to the digester and heating system controls of the biogas plant, demonstrating persistence on these systems until 18 May 2024. The group claimed to have encrypted and exfiltrated more than 400 GB of data. This compromise of the SCADA system – the supervisory IT layer – gave attackers the ability to disrupt all industrial processes without ever having to interact directly with the production equipment itself.

This case demonstrates the bounce approach now preferred by attackers: rather than requiring specific skills in industrial systems, it exploits classic IT vulnerabilities (weak credentials, insufficient segmentation, lack of hardening) and it generates maximum operational impact. The interventions of the aDvens CERT show that this is now the norm: the OT is hit indirectly by the compromising the IT layer that envelopes and supports it. The encryption of SCADA servers, monitoring stations (HMIs) or historical databases immediately makes it impossible to remotely monitor and control OT equipment even though it remains intact causing production to shut down completely. The interdependence between IT and OT thereby transforms a computer attack into complete industrial paralysis.



Find out more

Industrial environments are based on particular technologies and their security must take into account their specific features. This is particularly true for backups.

Check out the opinion of our OT experts on the subject.

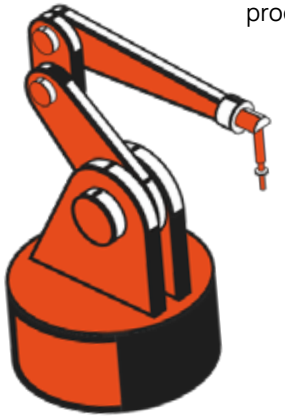
Cyber OT and IoT: protecting a mining base on the moon

VIEWPOINT

ADVENS AUDITORS

A growing maturity, persistent structural weaknesses

In recent years, the aDvens audit teams have observed an increase in the maturity of industry players in the face of cybersecurity challenges. OT environments are no longer considered out-of-bounds and concrete hardening measures are beginning to be deployed. In particular, network segmentation is making significant progress: true firewall partitioning is being implemented, which effectively limits the exposure of equipment that, for some, has no native security mechanism. This significantly reduces attack surfaces and complicates lateral movements from IT networks or less controlled areas. On the manufacturers' side, a strong awareness is also evident. Efforts made in recent years in security by design, patch release and vulnerability transparency are beginning to bear fruit. Public vulnerability discovery statistics for some major market players, e.g. Schneider Electric, show a downward trend in the number of new vulnerabilities released, reflecting an overall improvement in the robustness of products and development processes.



Persistent weaknesses

Nevertheless, several structural weaknesses remain. Industrial environments still include a large number of critical equipment, including programmable controllers (PLCs), for which firmware updates are not applied, sometimes for several years. This is often due to operational constraints but it leaves known and exploitable vulnerabilities. In addition, basic safeguards are often lacking, such as the lack of passwords for restricting access to programs, insufficient control of access to administrative interfaces or the option to directly direct control PLCs. The threat to service providers and third parties remains a significant risk in OT environments. It is still common for integrators, maintainers or managers with remote access to the industrial IS to enjoy privileges that bypass the security measures defined by the CISO and its teams. These accesses, often justified by operational needs, sometimes remain poorly regulated, with weak authentication mechanisms and password reuse between different environments or customers, which greatly increases the risk of a resurgence, especially when the segmentation between OT zones is not strict. The high dependence on service providers, which is often specific to each type of equipment, also results in numerous outbound connections that eventually increase the attack surface. In this context, supply chain attacks become a realistic scenario: the compromise of a provider or legitimate remote maintenance access can be sufficient to compromise an OT environment without directly exploiting vulnerabilities on industrial equipment.

Feedback from the field: intrusion test in industrial environment

In a recent intrusion test in the industrial environment, the audit teams chose to start on the site's office network as this is where an initial access to the OT network is most likely to occur during an actual attack. Initially, many network segmentation defects between IT and OT networks were identified. Without prior authentication, it was already possible to gain access to the HMIs (Human-Machine Interfaces) as well as equipment administration services of the industrial network. In this way, configuration files containing login details, reused on the network and on the Active Directory common to both networks, were recovered allowing initial access on the OT network. Next, login details to an MSSQL service of a machine in the OT network were also identified in network shares, for taking control of the machine, raising privileges and extracting secrets in memory, including an administrator service account for many machines in the industrial network, which is used for the backup. On other machines, the password for the VNC services, which is the same on all dedicated machines so that operators can log in to use the software used to access many HMIs, was also recovered. At this stage, it is now possible to interact with almost all industrial IS.

This intrusion test demonstrated that an attacker on the office network, without authentication, could already impact the proper working order of the production chain via accessible interfaces. As part of a more sophisticated attack, he would be able to take control of all the HMIs in the plant and alter the parameters at will, whether to affect final production and cause losses or simply shut down the plant.

Good practices for reducing these risks

These scenarios could have been avoided by applying good security practices. Maximum filtering of interconnections between the office and industrial networks via a dedicated firewall is essential: in this way, networks are segmented and if one is compromised, it does not compromise the security of the other. The use of a digital vault to store passwords and the systematic changing of default passwords when they are installed on a device are also critical. Ideally, different passwords should be used on each device in order to make it as complicated as possible for the attacker to take control.

The reduction of the attack surface is very important: it is recommended to expose only those services that are useful for the plant to operate properly. Many industrial protocols and services cannot be protected. In these cases, network partitioning remains the best option to minimise the risk of compromise. In absolute terms, it is advisable to separate the IT network from the OT network as much as possible and to minimise the dependence of each one on the other. For example, by unbundling the Active Directories and dedicating them to each environment, which also makes it possible to perform additional fine-tuning on the accounts and user rights. Physical separation between the two networks is also an option that drastically reduces the risk of totally compromising an industrial company.

While the overall maturity level of OT environments increases and the most exposed attack surfaces tend to decrease, attackers continue to benefit from fundamental weaknesses such as unmaintained equipment, inadequate access controls and operational constraints on patching. Currently, these elements remain the main leverage point for attacks in the industrial world.

The analysis of the key events of 2025 highlights some trends that will shape the cyber threat and its development in 2026. Here are some of our thoughts on attack methods as well as defender practices.

04

Outlook for 2026

4.1 OVERVIEW

4.1.1 / The widespread acceleration

Everything's speeding up. Attacks are occurring faster, new vulnerabilities are emerging at a frantic pace (several hundred per day as mentioned above) and the rate at which technological advances are made is so high that reference points become obsolete within six months. This widespread acceleration puts defence teams in a permanent race where simply keeping up with the pace becomes a challenge in itself.

As for the offensive side, the trend is clear. The average time between the discovery of a vulnerability and its active exploitation in malicious campaigns is now measured in days, sometimes hours. APT groups and cybercriminals have industrialisation capabilities that allow them to transform a zero-day vulnerability into an operational attack vector with unprecedented speed. This dynamic is amplified by generative AI: automated generation of malware variants, real-time adaptation of evasion techniques, large-scale customisation of phishing campaigns. What used to take weeks is now done within hours.

On the defensive side, this acceleration requires a profound transformation. Traditional patch management cycles, which used to be deployed on a monthly or quarterly basis, are no longer suitable. The exposure windows are narrowing, and with them, the room for action. SOC teams must handle exponentially growing alert volumes, while maintaining their ability to detect low-level events that betray sophisticated attacks.

The technical debt accumulates faster than it can be absorbed, and every new technological brick introduced to meet a threat creates new attack surfaces.

Artificial intelligence, paradoxically, is both the problem and a part of the solution. Models are changing at such a speed that it is not easy to have good practice guidelines that remain the same for a long period. Vulnerabilities specific to AI systems – prompt injection, data poisoning, model manipulation – add to the conventional risks. But AI also offers detection and analysis capabilities for processing volumes of data, that are impossible using manual approaches, automating certain responses and speeding up investigation phases. This is the approach that aDvens SOC teams have been following for some years (e.g. via neural networks to strengthen detection but also with LLM to accelerate response).

The question is no longer whether defenders can keep pace, but how they can reorganise their priorities, processes and architectures so that they do not lose their footing. The "zero trust" approach, the extensive automation of incident responses, strict prioritisation based on real business risk rather than generic CVSS and the acceptance that certain vulnerabilities are never patched in time become strategic imperatives.

> **Acceleration is not a temporary trend: it is the new cybersecurity operating regime.**

4.1.2 / The endless expansion of the perimeter

The security perimeter, which is a concept already widely challenged by digital transformation and the cloud, is experiencing a continuous expansion that seems to know no limits. Anything that connects could potentially become a gateway. Attackers know this and systematically test all available surfaces: network printers, surveillance cameras, building management systems, industrial IoT devices, connected vehicles, medical equipment. Each connected object is a potential anchor point for an intrusion.

Defenders find themselves in an impossible posture: protecting a perimeter that is expanding almost faster than they can map it. Despite being essential, the asset inventories are permanently incomplete. Equipment connects to the network without the knowledge of the IT teams. Each merger and acquisition, each new partnership, each transformation project automatically extends the attack surface. It is essential to have a means of measuring exposure and understanding the level of vulnerability.

FOCUS

CYBER RESILIENCE ACT (CRA)

The Cyber Resilience Act, implemented progressively from 2024 and whose obligations become fully binding in 2027, introduces a major regulatory transformation. For the first time, the European legislator imposes cybersecurity requirements on the entire lifecycle of products containing digital elements – from design to decommissioning. This potentially affects millions of products: computers and smartphones, of course, but also consumer connected objects, industrial equipment, medical devices, vehicles, connected toys and smart home appliances.

Manufacturers will need to integrate security by design, rigorously manage the vulnerabilities discovered throughout the lifetime of the product, provide security updates for a defined minimum duration, and notify serious security incidents within strict time frames (24 hours for preliminary notification, 72 hours for detailed reporting). Distributors and importers will also have compliance verification obligations. Failure to comply with these obligations could result in penalties of up to €15 million or 2.5% of the global annual turnover.

For user organisations, the CRA is fundamentally changing the equation. On the one hand, it should gradually improve the intrinsic level of safety of the products placed on the market. On the other hand, it imposes increased awareness on the compliance of deployed equipment, life cycle management and the monitoring of maintenance obligations. Security teams will need to integrate these criteria into their asset acquisition and management processes, verify that suppliers are meeting their obligations and maintain accurate traceability of CRA-submitted products in their infrastructure.

Find out more

4.1.3 / A double constraint that requires strategic transformation

The extension of the perimeter is not only a matter of volume, it is also a matter of diversity. Today's environments are a blend of 20-year-old legacy systems unable to receive patches, continuously evolving native cloud systems, OT equipment with absolute availability constraints and IoT objects designed without any security considerations.

These two trends – overall acceleration and perimeter expansion – reinforce each other, putting organisations under unprecedented pressure. We can no longer protect everything in the same way, and we can no longer take the time to analyse everything in depth. Defensive strategies must accept this dual constraint: strict network segmentation, the principle of least privilege applied systematically, microsegmentation to isolate critical assets and risk acceptance for certain equipment. The zero trust model, which assumes that no equipment or user is intrinsically trusted, is the only framework capable of simultaneously addressing a perimeter without defined boundaries and threats that evolve faster than defences.

Organisations that successfully navigate this environment will be those that have accepted that everything can no longer be controlled, and that have built up resilience based on the ability to quickly detect anomalies and contain compromises rather than on the illusion of tight perimeter or comprehensive protection.

4.2 ATTACKER DEVELOPMENTS

4.2.1 / Alliances of convenience

Focus #1

The year 2025 was marked by the creation of "inter-franchise" alliances between cybercriminal groups transforming the landscape into a more cooperative space. This trend can be explained by the increased pressure from law enforcement to adapt. A second factor to consider is the steady increase in the number of cybercriminal groups. With 45 new groups appearing in 2025 and a record 85 active ransomware groups in the third quarter of 2025, they are forced to be more competitive and find new ways of operating.

RANSOMWARE: moving from opportunistic model to organised cooperation

Faced with an expanding and increasingly competitive cybercriminal ecosystem, more cooperation among cybercriminal groups has been observed. Two models were identified: **the alliance between franchises** (Qilin, SafePay and WorldLeaks or Scattered Spider, LAPSUS$ and ShinyHunters) and the transformation into a **ransomware** cartel (DragonForce).

Alliance between ransomware groups

Franchises like Qilin, SafePay and WorldLeaks have teamed up to target the healthcare sector, including several European hospitals, the financial sector, retail and government institutions. Qilin was one of the most active groups in 2025 with an average of 75 victims per month.

Active since 8 August 2025, the Scattered LAPSUS$ Hunters collective has also brought together the skills of the cybercriminal groups, Scattered Spider, LAPSUS$ and ShinyHunters, to carry out attacks on various victims including Toyota, FedEx, UPS, Adidas, Disney and McDonald's.

Ransomware cartel

More than a simple coalition of different actors, DragonForce offers an attractive hybrid model that claimed 335 victims in 2025 according to Ransomware.live. In March 2025, DragonForce made its transformation into a "ransomware cartel" official with a development that goes beyond the classic Ransomware-as-a-Service (RaaS) environment. Rather than a centralised structure directly driving operations, DragonForce now functions as a coalition of affiliates. Everyone can run their own campaigns while benefiting from the infrastructure (hosting leak sites, managing secure payments, C2 servers), tools (administration panel designed as a real campaign management interface) and support provided by the group. In practice, affiliates exploit DragonForce resources while operating under their own identity. They therefore retain their name and some form of autonomy. This model appeals to profiles such as LockBit, Conti or RansomBay. Marks & Spencer, Harrods, Co-op and Belk are known to have been targeted by DragonForce.

Pooling resources

The point of setting up alliances is above all about pooling sources. Consequently, the alliance between Scattered Spider, LAPSUS$ and ShinyHunters brought together the specific skills of each group, namely:

- advanced social engineering and vishing skills for Scattered Spider;
- capitalisation in SIM swapping and multifactor authentication bypass techniques for LAPSUS$;
- specialisation in the mass exfiltration of data and monetisation on cybercriminal spaces for ShinyHunters.

As for the DragonForce cartel, its decentralised form makes operations sustainable. If an affiliate is dismantled, the cartel continues thanks to the rest of the members. Another of its strengths lies in its white label offer. The cartel has integrated two major ransomware variants – LockBit 3.0 and Conti v3 payloads (source code for which was released on 20 March 2022) – to deliver proven tools that reduce costs and time-to-market for affiliates. **These dynamics strengthen the resilience of cybercriminal groups because they can reduce their dependence on a single attack vector and ensure the continuity of their operations, despite the dismantling operations or pressure from law enforcement, by pooling infrastructure, technical skills and resources.**

Creating a dominant ecosystem

These dynamics are not limited to pooling resources, but also to the creation of a dominant ecosystem. Some groups use aggressive **communication strategies to weaken the credibility of rivals**. For example, while the RansomHub ransomware group disappeared in April 2025, DragonForce announced that the group had joined its ranks, presumably in an effort to attract former RansomHub affiliates. RansomHub's data leak site was compromised and briefly displayed the message "RansomHub R.I.P 03/03/2025", symbolically marking the end of the group. In retaliation, RansomHub defaced DragonForce's site. **Direct sabotage is a way of undermining the reputation of opposing groups**.

4.2.2 / Changes in attack methods

Focus #2

aDvens intrusion testing teams observe a transformation in attack surfaces. Attackers no longer focus solely on compromising Windows privileged accounts or exploiting Microsoft services. Their targets have evolved, and some previously neglected bricks have become formidable gateways.

DevOps channels and CI/CD pipelines are a perfect example of this trend. A simple vulnerability in these environments often allows initial access, sometimes with much higher privileges than expected. These tools often contain poorly protected secrets, i.e. in the code, in the commit histories, or directly in the pipelines. Auditors routinely compromise Azure access or ESXi hypervisor credentials using these bricks. In some cases, they don't even need to become domain administrators anymore: they extract virtual machines hosting domain controllers in the moment.

Cloud environments rarely have classic vulnerabilities (CVEs), but rather massive configuration flaws: non-compliance with the principle of least privilege, overly open file sharing containing secrets (a flaw also common on internal networks). Operating cloud services requires a much larger enumeration phase than on-premises environments, but the results are often there.
Kubernetes environments are also in the crosshairs. Vulnerabilities like IngressNightmare were widely exploited in 2025. They show that orchestration layers, which are often poorly controlled, offer particularly effective attack surfaces.

In the Windows world, Active Directory Certificate Services (ADCS) and System Center Configuration Manager (SCCM) remain prime targets. Certificate-based attacks may be less trivial than before, but they remain daunting when executed well. Other attacks that were thought to be missing are resurfacing. The recent CVE-2025-33073 on the NTLM reflective relay has made a difference in terms of its operational impact, which is far greater than its CVSS score suggests. This technique, abandoned for more than 15 years, is used to relay an authentication on the same workstation with maximum privileges. The new variant relies on maliciously creating an internal domain name and makes DNS monitoring a central challenge once again.

Kerberos relays have also become more widespread and have found practical use cases in modern environments. New weaknesses are also emerging in the architectures themselves. Tiering has become a security standard but it is often poorly implemented or difficult to maintain over time. The most commonly observed pattern is permeability between third parties 1 and 0, allowing privilege escalation from an application server administrator account. Insufficiently secure jump servers remain ideal entry points to the internal information system or directly to hypervisors.

At the same time, timeless techniques continue to work. Password attacks still provide Active Directory access, although compromised accounts are generally less privileged than before. This lengthens the attack chains without stopping them. Kerberoasting, which exploits password weaknesses in service accounts, uses the same principle. On the other hand, the LSASS process dump, that is responsible for Windows authentication, is becoming more and more complex. Modern BDUs make classical approaches ineffective and it is no longer enough to recompile Mimikatz. Attackers then turn to other sources of secrets: DPAPI, third-party software, PowerShell history, or active session spoofing via scheduled tasks.

In the longer term, new lines of attack are emerging for the coming years. Linux systems integrated with Active Directory are increasingly targeted because they are often less monitored than their Windows counterparts. Pivoting from the internal environment to the cloud is becoming common, especially through PowerShell histories on the desktops of cloud administrators. Persistence in cloud environments is also a growing priority for attackers. In addition, the use of commercial packers is very effective for bypassing EDRs including the most reputable ones. Having a good Command and Control is no longer enough: you also need to know how to properly customise your implants.

In the end, in most of the cases observed, the types of vulnerabilities exploited are still conventional: unpatched systems, overprivileged accounts used on a daily basis, lax access controls. The development of attacks lies primarily in targeted services. It's not just Windows systems anymore. Domain-integrated Linux and development solutions, often forgotten by security teams, are now prime targets.

More than ever, it is the poorly applied fundamentals that pave the way for the most effective attacks.

4.3 CHANGES AMONG DEFENDERS

As the threats evolve and intensify, the defenders do not stand still. The year 2026 promises to be marked by three major developments that are redefining practices, tools and the organisation of cybersecurity teams.

4.3.1 / The psychosocial risks in cyber defence

Focus #1

The consideration of psychosocial risks when managing cybersecurity teams is no longer an option, it is an operational necessity. Operational security teams, including the CERT teams in particular, operate under chronic conditions of stress that have direct effects on their performance and health.

The Club des Experts de la Sécurité de l'Information et du Numerique (CESIN) and aDvens have played a pioneering role in this area with the publication in 2021 of the first study on the stress of CISOs in France, as part of an initiative led by aDvens. The second edition, published in December 2024, shows a relative improvement but the levels remain worrying: 51% of cybersecurity managers report moderate to high stress, 7% are close to burnout, and 73% perceive a significant gap between their organisation's expectations and their ability to take real action.

InterCERT France, an association that is made up of more than 120 CERT and CSIRT teams in France, published in 2025 a specific study on psychosocial risks in cyber incident response centres. Conducted with 234 respondents, the study found that 72% of professionals report a lack of protection against psychosocial risks. Even more worrying, 86% report regular exposure to psychologically difficult content (illegal, violent or sensitive), and only 2% have received medical or psychological support related to their activity. Managers, who are often technically trained, are generally not trained to take into account psychosocial risks. The intense stress of the teams in case of attack, verbal abuse and post-traumatic stress exist but remain largely ignored. The study recommends that "decompression airlocks" be set up within teams, where everyone can lower adrenaline and stress levels. Counseling should be systematised and organisations should recognise that the CERT and SOC teams operate under conditions similar to emergency service roles which have long had post-intervention stress management protocols. The treatment of psychosocial risks is not just a welfare issue, it is an operational performance and talent retention issue.

4.3.2 / The ambient noise surrounding the cyber threat

Focus #2

The cyber threat is the subject of regular media outbursts that create "background noise" that is particularly problematic for cyber defence teams. The number of articles in the mainstream media on cyber incidents and data leaks skyrocketed in 2025. Some actors speak out to raise the alarm in an extreme way, communications are made about unproven data leaks or old recycled data and the ransomware groups fuel this noise by sometimes claiming fictitious attacks.

The direct impact on cyber defence teams is considerable. CISOs must provide ongoing justification to their hierarchy: "Are we affected by this leak?, why hasn't this attack been detected?" These constant requests represent a considerable waste of time when it comes to contradicting a sensationalist article or an alarmist tweet based on erroneous information.

Faced with this hubbub, the need for a real structured Cyber Threat Intelligence (CTI) capability is imperative. aDvens experts advocate a CTI that can **filter the noise** signal with reliable sources, **tailor content to different targets** (senior management does not need the same level of detail as SOC teams), and **respond quickly to internal queries** when an alert circulates. This CTI capability can be internalised, outsourced or hybridised. The key is that it exists and is operational to prevent cyber teams from being overwhelmed by the noise.

Find out more

For more information on the first CISO stress study, see our French **Cyberstress White Paper: the situation in 2024.**

4.3.3 / Technological arsenal in the age of AI

Focus #3

The defence technology arsenal will have to change significantly in response to AI, in the following three areas:

Integrate solutions dedicated to specific AI risks

The risks inherent in generative AI – prompt injection, data exfiltration via prompts, shadow AI – require specialised tools. Several solutions emerge: Prompt Security (purchased by SentinelOne) to secure interactions with LLM, Microsoft Azure Prompt Shields to detect prompt injections, advanced CASB platforms to detect shadow AI. The 2025 OWASP LLM Top 10 standard ranks prompt injection as the #1 risk for generative AI applications.

Upgrading detection and response tools

SOC platforms need to integrate generative AI to improve detection (analysis of log volumes that go beyond human capacity, identification of emerging patterns), speed up investigations (automatic event correlation, suggested attack hypotheses) and automate the response for low-ambiguity scenarios. The challenge is not to replace human analysts but to augment them.

Using AI to boost AI team productivity

In addition to detection, AI can transform other areas of security: automatic generation of incident reports and technical documentation, modelling and simulation of risk scenarios, creation of customised training content, automation of intelligence and synthesis of technical reports. This increased productivity frees up time for higher value-added activities: strategic thinking, proactive threat hunting, continuous improvement of the security architecture.

The development of the technological arsenal in the age of AI is not an option: it is a necessary condition for surviving against attackers that already master these technologies.

Find out more

To learn more about securing Microsoft 365 Copilot, **see the following article**:

4.3.4 Post-quantum cryptography: transitioning from 2026

Focus #4

The year 2026 marks a tipping point in preparation for the post-quantum era. ANSSI has set clear deadlines: as of 2027, it will no longer accept security products without post-quantum cryptography in qualification, and from 2030, it will no longer be reasonable to acquire solutions that do not fight against it. Faced with the "store now, decrypt later" threat (where data encrypted today could be decrypted tomorrow by quantum computers), the transition becomes a security imperative.

For the majority of organisations, the first priority is to become aware of the subject and its business implications. It is then a question of identifying what has been really mastered in cryptography: what algorithms are used, where, and what data does it protect? This mapping must be designed according to the criticality of the activities; data to be protected over several years or decades are given priority.

For organisations that don't have control over their cryptography, which involves a large share of the market, the approach is to survey suppliers and subcontractors on their post-quantum roadmaps and ensure that transition plans are documented and credible. This is a classic supplier compliance review but on an emerging technical topic.

For actors in sensitive sectors (OVI, OES, defence) and for those who develop or commercialise solutions integrating cryptography under their control, the challenge is different: we must integrate the post-quantum transition into the roadmaps produced from 2026, anticipate the cycles of renewal of systems and provide hybrid architectures for conducting a gradual migration. Cryptoagility (the ability to replace an algorithm without recasting the architecture) becomes a must-have design criterion.

In an environment where threats can evolve rapidly and where attackers combine automation, stealth and the exploitation of human and technical vulnerabilities, it is crucial to build defensive capabilities in a comprehensive and consistent manner.

Campaigns over the past few years have shown that successful intrusions often make use of conventional yet optimised vectors: compromised accounts, poor segmentation, misconfigurations or lack of visibility into critical activities. All within moving environments, between on-premise and cloud, between IT and OT.

The following recommendations are based on feedback from aDvens experts in the field. They apply to the **following five pillars**:

PILLAR 1 **Protection and hardening of systems**

PILLAR 2 **Access and privileges management**

PILLAR 3 **Logging and monitoring**

PILLAR 4 **Segmentation and perimeter security**

PILLAR 5 **Organisation and maturity**

05

Recommendations

PILLAR 1

Protection and hardening of systems

Hardening workstations/servers against malicious execution

BACKGROUND

The dominant execution techniques in 2025 rely heavily on PowerShell (T1059) and process injection (T1055).

ACTIONS

+ Enable PowerShell constrained language mode and mandatory script signing;
+ Block untrusted executables via AppLocker/WDAC;
+ Forbid dynamic loading and the injection of unsigned DLLs.

Priority patch management on exposed surfaces

BACKGROUND

The exploitation of vulnerabilities or configuration errors on exposed services (T1190) remains one of the main attack vectors. In 20% of cases handled by the aDvens CSIRT, this type of exploitation was used for initial access.

ACTIONS

+ Adapt a patch management policy to the criticality of assets within your organisation especially those exposed (patch application in less than 72 hours);
+ Perform periodic configuration scans on web and API servers;
+ Harden the configurations of the IS components.

Reduction of the attack surface and system hardening

BACKGROUND

Camouflage and evasion techniques (obfuscation, T1036 masquerading) remain common in 2025.

ACTIONS

+ Disable legacy services and binaries (MSHTA, WMI not required, restrictive rundll32);
+ Enable Attack Surface Reduction (ASR) to block suspicious executions;
+ Harden hypervisors and VMs (T1059.012, T1673).

PILLAR 2

Access and privilege management

Strong anti-phishing authentication

BACKGROUND

For 80% of the incidents supported by the aDvens CERT, initial access is obtained through the use of compromised accounts, mainly acquired during phishing campaigns (T1566).

ACTIONS

+ Enable MFA by default (ideally with U2F, Universal Second Factor);
+ Deploy link-protection measures before users access URLs (sandboxing, browser isolation);
+ Implement a typosquatting detection watch (domain name theft).

Strict control of privileged accounts

BACKGROUND

As in previous years, malicious actors make extensive use of credential dumping (T1003) and steal access tokens.

ACTIONS

+ Implement a privileged access management (PAM) solution including the systematic recording of sessions (for complete traceability of administrative actions and detecting any abnormal or non-compliant behaviour);
+ Enable automatic and regular password rotation of administrator accounts (ensuring that sensitive credentials never remain valid for too long and cannot be reused after a potential compromise);
+ Conduct account reviews and systematically delete dormant or unused accounts (to eliminate entry doors which are often exploited by attackers to initialise discreet access or bypass security controls).

Privilege Segmentation via Zero Trust

BACKGROUND

The attacks in 2025 reveal the massive exploitation of compromised legitimate accounts (Valid Accounts – T1078) which imposes stricter access mechanisms to limit the possibilities for bypassing and lateral movement.

ACTIONS

+ Implement context-based conditional access, including the posture of the equipment, the location, the connection risk level and type of resource requested (to ensure that even a compromised valid account cannot be used outside of strictly controlled conditions);
+ Systematically remove local administrator rights on user devices (to reduce the ability of a compromised account to perform privileged actions, deploy malicious tools or perform endpoint privilege escalation).

PILLAR 3

Logging and monitoring

Advanced command and script monitoring

BACKGROUND

Investigations conducted in 2025 demonstrate the consistent use of interpreters, especially PowerShell (T1059), in the execution phases of attacks, requiring a higher level of logging and behavioural analysis to detect malicious usage.

ACTIONS

+ Enable all the PowerShell (Event ID 4104), Script Block Logging and AMSI logs (to gain complete visibility into executed scripts, their content and associated behaviours including those that attempt to escape analysis);
+ Deploy advanced behavioural analysis within the EDR and User and Entity Behaviour Analytics engine (to identify abnormal executions, interpreter strings and patterns characteristic of scripted attacks).

Detection of C2 communications via web protocols

BACKGROUND

Command and control (C2) infrastructures mostly use HTTP/HTTPs (T1071) to blend in with legitimate traffic, making deep visibility into encryption and network behaviour essential.

ACTIONS

+ Implement targeted TLS inspection combined with JA3/JA3S fingerprint analysis (to identify abnormal communications, atypical certificates and TLS customer profiles associated with malicious implants);
+ Detect characteristic C2 flow anomalies, including "beaconing" signals (frequency, low data volume, etc.) and unusual variations in the size or frequency of exchanged packets – statistical data remains a metric of interest in this exercise, that is all too often neglected by security teams.

Strengthening multi-source correlation and detection of persistence mechanisms

BACKGROUND

Persistence techniques, including start-up mechanisms (T1547), are among the most commonly observed techniques in the incidents handled by the aDvens CERT.

ACTIONS

+ Enable and exploit Sysmon logs (to detect changes in Run/RunOnce keys, services and startup items so as to quickly detect malicious implants or configurations);
+ Actively supervise the creation and modification of scheduled tasks (in order to identify Scheduled Tasks added or altered by an attacker to maintain persistent access to the system),
+ Enhance the SOC from different possible sources and not rely solely on EDR for detection and response capability.

PILLAR 4

Segmentation and perimeter security

Strict microsegmentation and separation of environments

BACKGROUND

The use of compromised valid accounts allows malicious actors to perform lateral movement on the victim's infrastructure: network and business segmentation is therefore essential.

ACTIONS

+ Strictly segment production, administration and user environments (to limit lateral movement and prevent compromised accounts from accessing critical areas without justification);
+ Prohibit any RDP or SMB connections between segments (to reduce the attack surface that can be exploited by malicious actors seeking to use these common protocols to extend their hold on the network).

Harden cloud environments and isolate "workloads"

BACKGROUND

The MITRE ATT&CK 2025 reports highlight a significant increase in attacks targeting cloud environments including through groups like Scattered Spider that exploit MFA bypasses and vulnerabilities in cloud service configuration.

ACTIONS

+ Deploy Zero Trust Network Access (ZTNA) to fine-tune access to cloud resources taking into account context and identity (to limit exposure and prevent privilege exploitation via MFA bypass);
+ Isolate workloads using native mechanisms such as VPC, NSG or Security Groups and reinforce posture using a CSPM (to ensure strict separation, limit exposure of sensitive components and detect misconfigurations that can be exploited).

Enhanced inspection of encrypted traffic

BACKGROUND

C2 communications using HTTPS (T1071
dominate exfiltration and attack control operations in 2025 making visibility into encrypted flows indispensable.

ACTIONS

+ Implement a TLS inspection or intelligent proxy for the identification of cryptographic anomalies, atypical certificates or patterns characteristic of C2 infrastructures hidden behind legitimate traffic;
+ Deploy behavioural beaconing detection mechanisms which analyse the regularity of connections, volumes exchanged or network signatures typical of implants seeking to communicate discreetly with their control servers.

PILLAR 5

Organisation and maturity

Awareness and communication

BACKGROUND

Awareness must continue and adapt to the AI era. In addition, senior management must be fully informed about cyber risks.

ACTIONS

+ Organise regular phishing simulation campaigns, adapted to the most common attack typologies and new social engineering modes observed in the threat reports;
+ Train employees to recognise weak signals of modern attacks, including identity spoofing, voice or video compromise attempts (deepfake), and enhanced persuasion methods used by malicious actors (vishing);
+ Inform management of threats to the organisation's (and sector's) business to reinforce the strategic vision.

Conduct continuous testing and detection exercises

BACKGROUND

The modus operandi of malicious actors is evolving and requires monitoring on TTPs. It must be translated into a number of tests and controls over time.

ACTIONS

+ Organise Purple Team exercises based on the identified TTPs - to assess detection capability and verify the actual behaviour of controls in the face of representative scenarios);
+ Conduct continuous validation of controls using BAS (Breach & Attack Simulation) solutions or regular Red Team tests (to ensure that security mechanisms remain operational in the face of tactics observed in 2025 and the constant developments of attackers);
+ Conduct regular retrohunting campaigns (to verify that systems are healthy and have not been infected with new undetected malicious components).

Continuously enriching threat intelligence

BACKGROUND

The 2025 version of the ATT&CK MITRE matrix (v18) introduces new objects, thoroughly reviews detection strategies and enriches data components making it necessary to update the internal mapping to maintain an accurate and operational view of risk.

ACTIONS

+ Update the whole internal ATT&CK mapping to v18 in order to integrate new detection logics, enriched techniques and structural changes made to the knowledge base;
+ Implement a Continuous Threat Exposure Management system to regularly measure coverage, detect blind spots and direct hardening and investment efforts;
+ Raise awareness among decision-making bodies (COMEX) about threats to the organisation via the CTI.

> The past year has confirmed many of the trends observed in the past in terms of the intensification, generalisation and geopoliticisation of cyber threats. With the rise of generative artificial intelligence and its constant acceleration, the time factor is changing some of the analyses. The threat is even more global, attackers go even faster and the work of defenders is even more complex.

But it is even more valuable. Given the pervasiveness of the cyber threat and its involvement in several common threats around the world, protection is crucial. The cyber community continues to adapt at all times, specialises in its expertise and, in turn, makes the most of AI. It must now face up to a series of large permanent gaps.

+ **Develop the cyber resources of small businesses**... and help the experts of large groups to further strengthen the resilience of their organisations;
+ **Master the specifics of securing technical infrastructures**... and know how to protect the most vulnerable populations from information manipulation;
+ **Resolve a critical incident that could shut down a plant**... and plan the three-year SOC roadmap of a hospital.

To do this, cyber specialists and defenders need to stand together more than ever, not only to combat threats, but also to help combat the digital vulnerabilities of our society.

Conclusion

Threat Status Report 2025 - 2026

This report is the result of the work of the aDvens threat monitoring teams, as well as the findings from field missions in cyber crisis management, security incident response, attack response, security oversight, audits and security assessments.

In preparing this publication, the services of the following entities were required:

→ **CERT,** the cyber threat intelligence (CTI) as well as the Computer Security Incident Response Team (CSIRT);

→ **SOC,** including the teams of analysts that observe daily alerts and attempted attacks on the information systems of aDvens customers;

→ **Audit**, especially "pentesters" who replicate attacker behaviour in order to test the robustness of our customers' defences;

→ **Architecture and Integration**, including architects and security technology specialists who protect our customers' infrastructures.

This information is also enhanced by third-party sources, organisations and companies that produce cyber-relevant intelligence with the analysis of our teams.

Find out more...

aDvens CERT

Newsletters

Newsletters (monthly and alerts) published by the **aDvens CERT** are available on the aDvens website.

- https://www.advens.com/en/media/bulletins-cert-en/

aDvens CERT Newsletters

Incident response reference sheets

with the Societe Generale CERT

aDvens collaborated with Societe Generale's CERT and also contributed to InterCERT's work to produce documents that help in responding to attacks.

- https://github.com/certsocietegenerale/IRM
- https://github.com/cert-advens/IRM

Incident response methodology

aDvens publications

aDvens experts, from all our teams, regularly publish articles on technical analysis, feedback or prospective studies on cybersecurity and related threats.

- Advens Media: Discover, Understand, Decide

Which managed SOC provider should you choose?

ABOUT ADVENS

aDvens is a leading independent and sovereign European cybersecurity company. Our 650 experts are present throughout France, Spain, Italy, Germany, as well as in Montreal and Papeete.

Our mission is to protect public and private organisations, 24 hours a day, 365 days a year, that are increasingly dependent on digital technology and that are increasingly exposing their resources to ever more professional attackers. This mission guides and drives us on a daily basis. But this is not enough for us.

If our daily business is focused on your protection and security, we pursue a business model guided by overall performance. We want to put our financial performance at the service of people and the planet. Through the **aDvens For People and Planet** endowment fund, we fight against digital vulnerabilities that affect the company and support projects such as **the Cybercitizens' Fresco** (to raise awareness among young people), **CyberSup** (to train future experts and future Cyber experts), **Cyber for Good** (to develop the cyber-maturity of certain exposed populations such as actors in the social and solidarity economy or independent journalists).

Operational security 24/7

+ **Sovereign SOC** leader in **France, 300 experts, 1m protected endpoints**, PDIS qualified
+ **PRIS qualified CERT, 40 CSIRT interventions, 197 CTI qualifications** in 2024
+ Rated **4th European MSSP**, data hosted in France, 100% European teams

Governance, Risk and Compliance

+ **For 25 years**, aDvens has been structuring and driving the CRM approaches of CISOs
+ **200+ certifications** accompanied each year, **50+ regulatory texts** and **45 mastered** ISO standards

Technological expertise

+ In-house designed SOC platform, **open and scalable** architecture
+ Support throughout the lifecycle of security technologies and the security of your technologies (OT, Cloud, AI, etc.)
+ Fruitful and dynamic partnerships:

CROWDSTRIKE SentinelOne NOZOMI NETWORKS CybelAngel Microsoft HarfangLab

Offensive approach

+ **1,200+ offensive campaigns/year** (Pentests, Red Team, complex audits, etc.)
+ Certified teams (**PASSI, OSCP, CEH, GPEN**...)

ADVENS CERT

Created in 2020 to respond to internal and external incidents, the aDvens CERT consists of an incident response team (CSIRT) and a cyber threat intelligence (CTI) team. The aDvens CERT is PRIS qualified by ANSSI (France) and also **APT response service provider** qualified by BSI (Germany). It was recognised as a leader by ISG in its ISG Provider Lens report for France.

Finally, CERT is strongly integrated into the French cyber community by being a member of Intercert but also internationally by contributing to FIRST.

ADVENS SOC

mySOC offers a managed detection and response service 24/7 provided by aDvens. mySOC has been providing a comprehensive range of detection and response activities, from run and security operations, vulnerability management, threat analysis and incident response, to more than 500 customers in Europe since 2016. mySOC is PRIS qualified by ANSSI (France), ISO/IEC 27001:2023 certified and is part of the SOC Red Nacional of the CCN-CERT (Spain).

We are recognised as a leader in the managed SOC for mid-market and large organisations in the Markess by exaegis blueprint. We are also supported by ISG in its ISG Provider Lens "Next-Gen Soc Services" report, mySOC is the 4th European MSSP in the Top 250 maintained by MSSP Alert.

aDvens

For cyber, people & planet

www.advens.com