aDvens

For cyber, people & planet

Threat Status Report 2024 - 2025

Table of Contents

THREAT STATUS REPORT
2024-2025

Introduction

THREAT STATUS REPORT
2024 - 2025

2024 was a year of dangers for the Cyber France team, with the Olympic and Paralympic Games being held in France in a highly tense geopolitical context that is conducive to large-scale actions.

The risk could come from all sides: groups of state attackers in a context where Russian athletes were deprived of the Olympic Games, groups of private attackers looking for global stunts to attract new members or even groups of hacktivists wishing to defend a cause.

Thanks to the Cyber France collective, and despite numerous attempts before and during the Paris 2024 Games, defence held up and contributed to the success of this event, which amazed the whole world and made the vast majority of French people proud.

Under the leadership of ANSSI, aDvens contributed to this success by carrying out numerous Red Team exercises. These tested the feared attack scenarios, as well as deploying and managing the protection of 13 major Olympic sites, with a particular focus on industrial environments (OT).

The first lesson to be learnt is that with significant resources, it is possible to contain even the most extreme threats. The resources put in place were commensurate with the event: off the scale. We now need to adapt these best practices and make them sustainable in a context of tighter budgets and human resources, for both public and private companies. Absolute protection against all threats is impossible, given the limited resources of each organisation, so the challenge is to identify the major risks and take the most effective action to mitigate them.

Away from the Games, in 2024, cybercriminals have refined their tactics and enhanced their arsenal to maximise the effectiveness of their attacks. In particular, they are exploiting critical vulnerabilities affecting perimeter security equipment such as Fortinet and Ivanti. The use of legitimate access, acquired on cybercriminal markets or sometimes freely available, has become a preferred method. Such access often comes from data exfiltrated by infostealers such as Lumma Stealer, or from sophisticated phishing campaigns orchestrated using kits sold or rented on clandestine channels. These techniques enable attackers to infiltrate systems discreetly and carry out their initial actions while remaining under the radar.

2024 marked a significant turning point with cybercriminals increasingly leveraging artificial intelligence, whether by ransomware operators or state actors (APTs) seeking to weaponise their cyberattacks.

Specifically, AI has revolutionised social engineering, making spoofing attempts more convincing and harder to detect. Cybercriminals are also using deepfakes to simulate the voice or face of trusted individuals, making it easier to extort, defraud or gain unauthorised access to sensitive systems.

AI is also being used to design malicious implants with advanced mechanisms, making them ever more complex to detect and analyse.

Another notable trend is the rise of attacks involving direct contact with victims via collaborative communication platforms such as Microsoft Teams. Assuming the identity of members of the IT department, cybercriminals are able to convince employees to install utilities (hidden backdoors), thereby giving them access to the targeted infrastructures.

Faced with this situation, companies must continue the efforts they have made in the past. However, they must also:

→ **Intensify preventive measures,** using Cyber Threat Intelligence data to better manage their attack exposure, and prioritise the most relevant vulnerabilities in terms of the impact and criticality of their businesses.

→ **Prioritise security** across their industrial supply chain, to be able to compete with attackers who use them themselves.

→ **Use new tools** (or choose service providers capable of doing so) provided by the rise of generative AI, to be able to compete with attackers who use them themselves..

The years to come promise to be just as eventful...

Cybersecurity teams are going to be hard-pressed, particularly with NIS 2 compliance plans (but also with DORA, the Cyber Resilience Act and other applicable regulatory frameworks). On the geopolitical front, it would be hard to predict the consequences of the new US administration's decisions.

Like many people, the end of monitoring of malicious Russian activities came as a great surprise. As well as trying to understand the logic behind it, we need to consider the impact on Europe. One thing is certain: we will have to be ready and prepare our cyber defences to protect our businesses, our public institutions and our way of life.

Enjoy reading this 2024-2025 report.

The aDvens team

> 2024 was another year rich in information and lessons for the Cyber community. It is essential to have precise, quantified knowledge of the state of Cyber threat in order to adapt defence strategies. This is especially crucial considering the rapid evolution of attacks and the growing number of vulnerabilities. There are many security measures available, and all these factors need to be taken into account to make the right decisions.

01

2024 in Review: Key Cyber Trends and Statistics

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

5 MAJOR TRENDS

Before looking in detail at the figures for the past year, here are **5 major trends** that our teams have observed in the field, whether CERT (CTI and CSIRT), SOC or Audit (Red Team, Purple Team, etc.).

Artificial intelligence

Highly publicised in 2024, it is everywhere, including on the attackers' side, whether they are preparing a simple scam or phishing message, or contributing to the development of adaptive and evolving malware.

An exponential number of public vulnerabilities

This has exploded, with attackers taking a worrying (but logical given the associated impact) interest in vulnerabilities affecting security products, particularly perimeter security or access control vulnerabilities affecting security products, particularly perimeter security and access control products.

Data theft increasingly massive

They target all sectors of activity and all types of organisation, with a particular focus on the theft of credentials, notably via infostealers.

The cloud threatened

It has been the target of a large number of malicious actions, including the deletion or transfer of entire tenants, following the theft of administration credentials or the exploitation of a configuration error in the targeted outsourced service.

Industry on alert

Attacks are increasingly targeting industrial environments (OT), which can support activities that are highly critical to a company, a community or even the general public.

Added to this is **a particularly unstable geopolitical context**, which has given rise to opportunistic attacks, exacerbated by certain world events or certain tensions between major powers.

KEY STATISTICS

+14%
MORE CYBER ATTACKS THAN IN 2023*

+38.6%
MORE VULNERABILITIES PUBLISHED
(40,291 compared with 29,066 in 2023)

244
VULNERABILITIES EXPLOITED BY BY MALICIOUS GROUPS

80%
OF ATTACKS RE-USE STOLEN DATA

Data theft has direct consequences. Attackers use accounts and passwords that they have stolen in a previous attack or purchased from other cybercriminals on the Web or Dark Web to gain legitimate access to the target organisation's information system and commit illegitimate acts. This is why it is so important to keep a close eye on cases of data theft: even if the direct victims are third-party organisations, they may possess data from other organisations, which are then indirectly affected.

TOP 4
VECTORS OF COMPROMISES

The four most common attack vectors are still phishing and its derivatives (SMShing, Vishing, etc.), the malicious use of leaked accounts, the exploitation of unaddressed vulnerabilities and the abuse of a misconfigured component. This top 4 is likely to persist, but the ways in which attackers exploit these weaknesses are likely to evolve.

3
TARGETED SECTORS

The 3 most targeted sectors: manufacturing, healthcare and agri-food. The manufacturing and agri-food industries are targeted by cybercriminals because an attack on this type of organisation has an immediate impact on production capacity and therefore turnover. These structures represent profitable targets for attackers. The health sector, for its part, is targeted because it enables destabilisation operations to be carried out against a State, an administration or a population.

NEW FIGURES ANALYSED THIS YEAR

Action plans resulting from interventions by aDvens's CERT ;

→ aDvens's CTI teams recommended **1,249 actions for 253 analyses,** i.e. less than 5 actions per request when the intervention is carried out in an anticipatory dynamic;

→ As for the actions recommended by the CSIRT, during an invident response and/or crisis, **50 % them must be carried out quickly**, within two months of the attack. To ensure that the occurrence of a new cyber crisis is greatly reduced, an action plan must be carried out that may include several dozen actions.

* based on attacks claimed by attacker groups.

> 2024 was an exceptionally productive year for threat actors. With new methods of operation, facilitated by AI or adapted to cloud environments, malicious groups were able to innovate and enrich their arsenal.

Additionally, published vulnerabilities increased by 38%, some of which are being used by attackers of all levels. Only ransomware seems to have suffered a drop in activity - which reflects the effectiveness of the measures put in place by security teams.

After presenting the attack techniques and tactics that caught the attention of aDvens's teams in 2024, a review of defence measures is also proposed, in order to adjust the action plans for 2025.

02 / Threat Intelligence Analysis: Attack Patterns and Vulnerabilities

2.1 OVERVIEW OF ATTACKS

This section looks at the different attack techniques (TTP, for Tactics, Techniques and Procedures) that have caught the attention of aDvens's teams, as well as some particularly interesting malware.

2.1.1 / The TTPs that made their mark on 2024

A TTP typically represents one stage of an attack, not the attack as a whole. Complete attacks consist of sequences of TTPs that enable attackers to achieve their objectives.

These TTPs are sometimes the marker of a group of attackers: spotting them enables us to know how to react by placing the TTP observed in the context of the attack chain of a given group.

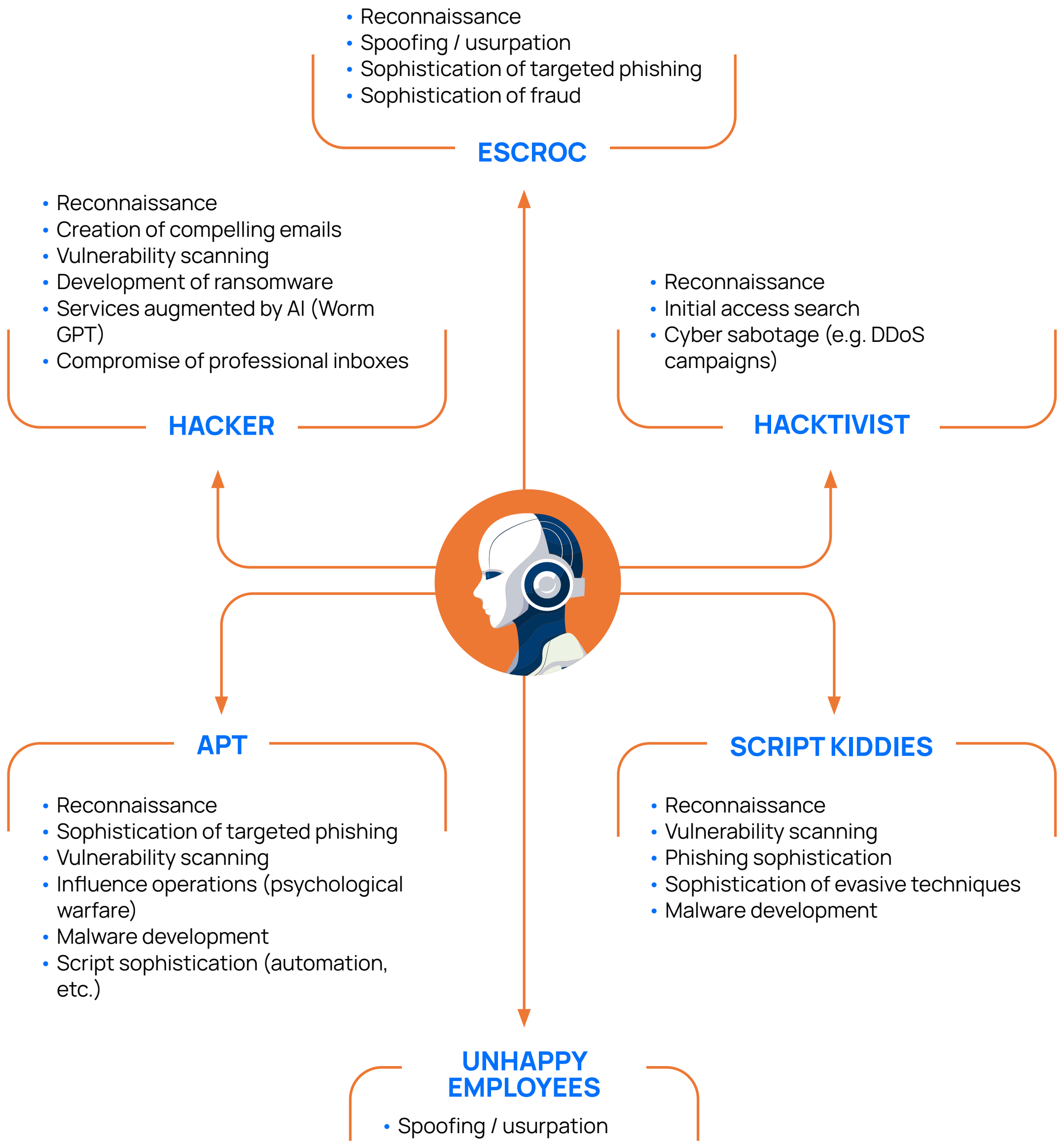
Artificial Intelligence

The use of artificial intelligence in scams and phishing attacks was a recurring topic in 2024, especially in efforts to raise awareness and educate the public. However, AI has also played an increasing role in the development of other cybercriminal activities this year. A survey by security firm SoSafe found that **87 % of cyber security professionals surveyed had encountered AI-driven cyber attacks in 2024**.

> AI was massively used in 2024 in the development of **adaptive and evolving malware**, capable of modifying its behaviour in real time, in order to avoid detection by traditional security tools. This new risk was the subject of a specific publication by the FBI in May 2024. Another little-another little known usage of AI was its use in automation and development of attacks, leading to increasingly rapid execution.

White paper on AI

The uses of AI by malicious actors


ESCROC
• Reconnaissance
• Spoofing / usurpation
• Sophistication of targeted phishing
• Sophistication of fraud
HACKER
• Reconnaissance
• Creation of compelling emails
• Vulnerability scanning
• Development of ransomware
• Services augmented by AI (Worm GPT)
• Compromise of professional inboxes
HACKTIVIST
• Reconnaissance
• Initial access search
• Cyber sabotage (e.g. DDoS campaigns)
APT
• Reconnaissance
• Sophistication of targeted phishing
• Vulnerability scanning
• Influence operations (psychological warfare)
• Malware development
• Script sophistication (automation, etc.)
SCRIPT KIDDIES
• Reconnaissance
• Vulnerability scanning
• Phishing sophistication
• Sophistication of evasive techniques
• Malware development
UNHAPPY EMPLOYEES
• Spoofing / usurpation

Malicious actions in the cloud: deletion or transfer of a tenant

In 2023, the focus was on the deployment of malware via cloud providers.

This year highlights the appropriation of victims' cloud infrastructures by attackers.

aDvens's CERT's interventions have highlighted modus operandi based on the transfer of the victim organisation's data from its legitimate tenant to a malicious tenant controlled by the attacker (after gaining access to the victim's tenant). In some cases, the attacker simply deletes a tenant in order to destabilise the target.

Tenants protected by strong authentication (MFA) are not immune. A tenant can be attacked by compromising a workstation or an administrator account, from which the attacker will use applications on the victim's tenant. It is also possible to capture the token generated after the authentication stage, using MFA bombing techniques for example.

On occasion, during an attack, the attackers were unable to return to the correct cloud administration/configuration page as, in the cloud, this location can change rapidly. The attacker then had to navigate from page to page to transfer the data to a tenant under his control, thereby recovering all the victim's data. This makes a ransom demand possible, and also offers a guarantee of controlled access to recover the data without leaving any trace in the logs of the tenant of the organisation attacked.

Regular changes to the management interfaces of cloud providers not only make administration more complex, but also make intrusions more likely. An attacker was seen attempting to access an obsolete administration page that had changed location following an update.

Credential theft

In 2024, infostealers consolidated their position **as a major threat, with a significant increase in credential theft** (3.9 billion shared passwords according to Forbes). Malware families such as LummaC2, RisePro, and Stealc dominate this activity, often distributed via Malware-as-a-Service (MaaS) models at affordable prices ($10 per piece of malware).

Their modus operandi is based on initial infections via phishing or malicious downloads, followed by theft of sensitive data, which is then exploited for larger-scale attacks (as in the case of the Snowflake breaches, for example). A large parallel market in stolen connection data flourished in 2024, with a sharp increase in the amount of data shared free of charge or as a sample, reflecting the volume of data stolen and shared on a daily basis. It is also worth noting the use of loaders by infostealers. The loader makes it possible to launch the attack based on certain characteristics specific to the targeted organisations. For example, HijackLoader has frequently been used to to load various types of malware (Danabot, SystemBC and RedLine Stealer).Credential theft, linked to almost a quarter of attacks in 2024, is the primary means of initial access, ahead of vulnerability exploitation. The main strength of this technique lies largely in the human factor: the absence of MFA and the reuse of passwords from one account to another, for example.

VIEWPOINT

CERT ADVENS

In 2023, **80 % of incident responses were caused by stolen credentials.** the figure for 2024 is the same.

Infostealers can hide in a wide variety of software and know how to keep up with the times. For example, one of them suggests that users download *ChatGPT* onto their computer. This empty shell then displays only a pseudo Internet browser but requests (and retrieves !) the user's real password to connect to ChatGPT. For more personal use, for well-known video games such as Minecraft, infostealers create a fake *launcher* that retrieves all the victim's credentials.

Very often, these are still valid on the service where they were stolen and/or they are used identically on another service accessed by the victim (same password used on several accounts or between professional and personal spheres).

VIEWPOINT

SOC ADVENS

In addition to the infection vectors mentioned above, 2024 saw the widespread use of **Captcha hijacking as a means of infection**. Malicious websites invite users to execute commands on their workstations in order to verify that they are indeed human and not an automated mechanism. As the command is encoded in base64, the unwary user will not suspect that it is actually a command executing the download of a malicious payload from a third-party site. This modus operandi was widely used by the Lumma infostealer in 2024.

Organisations must adopt a dual approach to combating information-stealing malware:

- Leaked credentials enable malicious actors to gain access to various services, sometimes with elevated rights, making the organisation particularly vulnerable (and sometimes turning the victim into a proxy for attacks on other organisations);
- Users who store private identifiers on their browsers or workstations also become victims of private credential leaks, the consequences of which can be significant (for example in the event of theft of banking credentials).

Phishing as a service (PhaaS)

In 2024, a new type of service, hitherto in its infancy, developed and succeeded in creating a new market in cybercriminal circles: **phishing as a service kits and tools,** transforming the ability to carry out this type of attack into a commercial service, accessible even to novice cybercriminals.
These tools, which are often sold on the darknet, include HTML templates for creating fake login pages and scripts for stealing information such as passwords and bank details.

Specific cases illustrating the scale of the phenomenon emerged throughout the previous year. For example, the dismantling of the PhaaS LabHost platform in April 2024 led to the arrest of 37 suspects. Similarly, Darcula, also discovered in 2024, had deployed more than 20,000 phishing domains, targeting postal and financial services in more than a hundred countries. Darcula stood out for its use of iMessage and RCS (Rich Communication Services) to bypass SMS firewalls, as well as its infrastructure of almost 11,000 IP addresses distributed worldwide.
This type of offer is available on a subscription basis, with prices ranging from a few dozen dollars for simple models to several hundred, like the Darcula platform and its 250 dollars per month.

Adversary-in-the-middle

While this is not a new modus operandi, there was a resurgence in 2024. In this type of "*adversary-in-the-middle*" (AiTM) attack, the attacker intercepts data sent by a sender to its recipient, and then from the recipient to the sender, without the latter noticing. This form of eavesdropping and data theft makes it possible to obtain a wide range of information (personal data, passwords, intellectual property or business secrets).

The black markets of the Web or Darkweb offer "*phishing-as-a-service*" (PhaaS) kits that make it easy to set up an AiTM phishing attack, such as Sneaky 2FA or GreatNess. These attacks can go as far as bypassing strong authentication mechanisms (2-factor authentication, 2FA, or multi factor authentication, MFA). Although MFA has become commonplace, it remains essential to monitor the effectiveness of this authentication method over time.

VIEWPOINT

SOC ADVENS

Several MFA bypass attacks were observed in 2024. These attacks are particularly difficult to detect because the attackers can use the compromised account to usurp the user's identity (for example, as part of RIB fraud or president attacks). Their primary objective is not necessarily to gain technical access (which ends up generating detectable events), but to be able to perform actions "in the name of" the compromised user in order to achieve lucrative objectives or gain access to higher-value data.

Vulnerabilities

Exploiting vulnerabilities in components exposed on the Internet is a popular activity for malicious actors of all sizes (from cybercriminals to APTs). 2024 was a *landmark* year for several vendors, including Ivanti and Fortinet.

These vulnerabilities on perimeter equipment are being actively used by attackers, as are those on hypervisors. Here are some of these attacker groups and the vulnerabilities they have exploited.

APT28: multiple vulnerabilities (CVE-2022-38028/CVE-2023-23397/CVE-2021-1675) for deploying the GosseEgg post-exploitation tool. The latter is used to execute arbitrary code, deploy backdoors and perform lateral movement;

North Korean group Citrinel Sleet: Chrome vulnerability CVE-2024-7971 to deploy the FudModule rootkit. The cryptocurrency sector is specifically targeted;

Chinese APT group Volt Typhoon: zero day (CVE 2024-39717) affecting Versa to compromise ISPs;

Salt Typhon Chinese Group: GhostSpider backdoor and vulnerabilities affecting Fortinet EMS (CVE-2024-48788), Sophos firewall (CVE-2022-3236), Ivanti Connect Secure (CVE-2023-46805 and 21887) finally Microsoft Exchange (proxylogon);

Blackbasta (Darkgate) and Akira ransomware groups: common vulnerabilities affecting Windows (CVE-2024-26169/21412/38213) and VMWARE ESXi (CVE-2024-37085);

Clop ransomware group: CVE-2024-50623 vulnerability affecting Cleo (file transfer tool). The latter reportedly claimed more than 50 victims at the end of December (19 to 25 December 2024).

ivanti

Among the most notable vulnerabilities is **CVE-2024-21887**, which, when exploited in conjunction with **CVE-2023-46805**, allowed an unauthenticated user to execute arbitrary commands via malicious requests.
In January 2024, another major flaw, **CVE-2024-21893**, a **Server-Side Request Forgery (SSRF)** vulnerability, was widely exploited, accentuating the cybersecurity challenges for the company.
A second wave of attacks hit Ivanti in September 2024, this time targeting **Ivanti CSA 4.6**. This crisis was exacerbated by a flawed patch of **CVE-2024-8963**, which unintentionally led to the emergence of new critical **Remote Code Execution (RCE)** vulnerabilities: **CVE-2024-9379** and **CVE-2024-9380**.

FORTINET

The **CVE-2024-21762** vulnerability affected the **SSL VPN (SSLVPN** component of **Fortinet's FortiOS** and **FortiProxy** products. This buffer overflow vulnerability (**CWE-787**) allows a remote, unauthenticated attacker to execute arbitrary code via specially crafted HTTP requests.

On **8 February 2024**, Fortinet issued a security advisory **PSIRT (FG-IR-24-0151** reporting a potential exploit. This alert was quickly confirmed by the addition of the CVE to the CISA's **Known Exploited Vulnerabilities (KEV) database on 9 February 2024**.

The impact was significant, with around **150,000 machines exposed on the Internet** likely to be affected. In response, Fortinet released a number of mitigation measures detailed in its initial security bulletin, as well as providing an update tool to secure vulnerable systems.

VIEWPOINT

CERT ADVENS

In August, aDvens's CERT noted the frequent targeting of ESXi :

- It is recommended that ESXi not be integrated into the Active Directory domain supporting users;
- A dedicated authentication system can be set up;
- It must not be visible from zones T2, T1 and T0, but only from infrastructure zone T-1 or backup zone T-2.

2.1.2 / The most widespread malware

In 2024, aDvens teams observed the prevalent use of SocGholish, Agent Tesla, and Lumma Stealer malware across the cybercriminal ecosystem.

SocGholish

SocGholish, also known as **FakeUpdates,** is malware commonly used as a primary infection vector for the deployment of other malware, including ransomware. Identified in 2017, it is attributed to the **Mustard Tempest** cybercrime group (aka **TA569**), which specialises in Initial Access Broker (IaB).

The malware relies primarily on **social engineering** techniques, tricking victims into downloading fake software updates via *malvertising* campaigns. It can also be distributed via compromised legitimate websites, where injected scripts cause a **stealthy** *(drive-by download*), and infection without user interaction.

Once executed on a system, SocGholish establishes persistence by downloading additional payloads, such as **remote access tools** *(RATs*), *infostealers* or **ransomware**.

It acts as a gateway for attackers to exfiltrate sensitive data and extend their access to compromised infrastructures.

In 2024, the TA569 group used SocGholish in a massive campaign targeting a thousand companies worldwide. That same year, a change in modus operandi was observed with the download from legitimate repositories of the Python installer needed to carry out additional operations. Downloading from the publisher's site and the democratisation of the programming language within companies make detection more complex.

Agent Tesla

Agent Tesla is a Remote Access Trojan(RAT), which appeared in 2014 and was developed to **exfiltrate sensitive information** on **Windows** systems. Operating on a **Malware-as-a-Service** *(MaaS)* model, it is marketed on underground forums, often accompanied by a **support service** for cybercriminals.

This malware has a wide range of features that enable advanced compromise of targeted systems:

- **Password theft**: extraction of identifiers stored in browsers, email clients and password managers;
- **Keylogging**: real-time capture of data entered by the user;
- **Screenshots** : record images of the desktop and running applications ;

WELCOME TO AGENT TESLA

Create an account and buy now.

- **Interception of communications**: monitoring exchanges via messaging and remote desktop software ;
- **Exfiltration of data** to a command and control server *(C2)*, via SMTP, FTP or HTTP / HTTPS.

Phishing remains the primary method of distributing Agent Tesla. Attackers send **fraudulent emails** containing malicious attachments in the form of **Office documents**,**password-protected ZIP archives** or **disguised executables**. These files often exploit **VBA macros** or **known vulnerabilities** to execute the malware on the target machine.

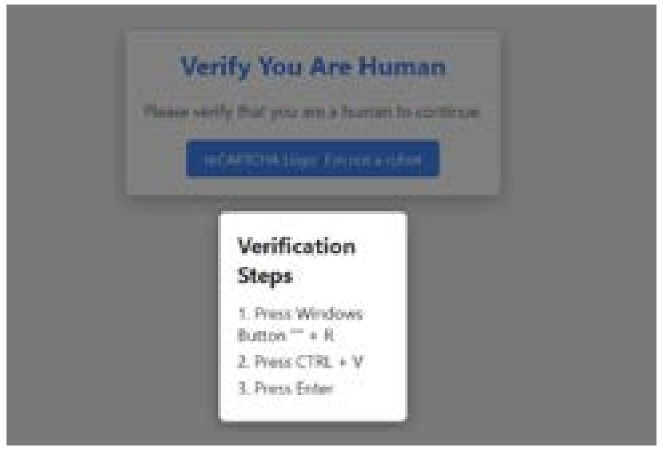
Lumma stealer

Lumma, also known as **LummaStealer** or **Lumma C2 Stealer**, is a **data exfiltration malware** designed specifically for stealing sensitive information. The malware primarily targets **cryptocurrency wallets, browser passwords** and **other credentials** stored on compromised machines.

Lumma, which first appeared in **August 2022** on **Russian underground forums**, operates on a Malware-as-a-Service *(MaaS)* model, giving cybercriminals access to a centralised platform to generate variants of the malware, recover stolen data and manage their attack campaigns.

Lumma Stealer offers a wide range of functions:

- **Theft of credentieals and sensitive information**: extraction of passwords stored in the Chromium and Firefox browsers, as well as authentication tokens;
- **Targeting cryptocurrency wallets** : detection and exfiltration of private keys from software such as MetaMask, Trust Wallet and Exodus;
- **Capture system information** : collect IP addresses, hardware configurations and details of the Windows environment;
- **Download and run additional payloads**: additional malware can be installed on the infected machine;
- **Advanced evasion techniques** : encryption of communications with the C2 server, execution in memory to avoid detection by antivirus software, and deactivation of Windows Defender protections.



Verify You Are Human

Please verify that you are a human to continue.

Verification Steps

1. Press Windows Button ⊞ + R
2. Press CTRL + V
3. Press Enter

Lumma is distributed mainly via :

- **Phishing campaigns**, often in the form of fraudulent e-mails containing infected files (Office documents, password-protected ZIP archives, disguised executable files);
- **Fake Captcha fraud**, in which victims are tricked into downloading a file on the pretext of checking that they are not robots. This technique has been massively exploited and recently adapted to make the victim execute the file directly.

> While the ingenuity of cybercriminals allows them to develop their arsenal to make it more effective in terms of impact and speed, there are certain behaviours that allow analysts to detect the three malwares in order to react as quickly as possible:

- → Connection from or to servers hosting anonymised infrastructures (TOR, proxies);
- → Communication to domains or IP addresses identified as C2 ;
- → Executing PowerShell or JavaScript script from the victim's environment;
- → Registry key modification to maintain persistence ;
- → Changing and/or deactivating system security settings.

Late 2024 and early 2025 saw the start of the EpiBrowser campaign, a subject likely to be of interest to all security teams.

2.2 MAJOR VULNERABILITIES

TOP 10

VULNERABILITIES

The remediation action plans provided by CERT highlight area 4 - **Perimeter Security and Isolation**. In 2024, the number of public reports of vulnerabilities increased considerably, with a strong focus on perimeter security components. A small number of these vulnerabilities are exploited by criminals, so resolving them can quickly limit the risks. Our TOP 10 of 2024 is designed to highlight the vulnerabilities that need to be addressed as a priority.

+38.6%

VULNERABILITIES PUBLISHED

(40,291 compared with 29,066 in 2023)

The number of published **vulnerabilities has increased dramatically**. This staggering figure raises the question of how to monitor, analyse, qualify, evaluate and react to such a vast amount of information. We need to reinvent the way in which we prioritise the vulnerabilities that need to be dealt with - so as not to exhaust ourselves and guarantee a level of maintenance that is consistent with the business risks. Focusing on the vulnerabilities most used by attacker groups can be a good starting point.

244

VULNERABILITIES EXPLOITED BY RANSOMWARE GROUPS

Attackers concentrated on using 244 main vulnerabilities. It is important to be aware of these vulnerabilities and to assess their potential impact on the organisation. It then becomes easier to prioritise remediation efforts by taking an impact and business criticality view. Some vulnerabilities are critical for everyone, when they affect perimeter elements or security components.

ivanti

CVE-2024-21887

A command injection vulnerability in the web components of Ivanti Connect Secure and Ivanti Policy Secure was discovered by Volexity security researchers. The exploitation of this vulnerability by a remote and authenticated attacker allows, by sending a specifically crafted request, to execute arbitrary code. Volexity observed the exploitation of this vulnerability and attributed it to the APT group UTA0178.

9.1

CRITICAL

-

Exploited
Remote code
execution

EPSS: 97.32 %

PoC: YES

ivanti

CVE-2023-46805

A flaw in the authentication checks in the web components of Ivanti Connect Secure and Ivanti Policy Secure has been discovered by security researchers at Volexity. Exploitation of this vulnerability by a remote, unauthenticated attacker can bypass security controls and gain access to web service information. Volexity observed the exploitation of this vulnerability and attributed it to the APT group UTA0178.

8.2

IMPORTANT

-

Exploited
Authentication
bypass

EPSS: 96.63 %

PoC: YES

FORTINET

CVE-2024-47575

Exploiting this vulnerability allows an unauthenticated remote attacker, using a valid FortiGate certificate, to register unauthorised devices in FortiManager. The attacker would then be able to view and modify files, such as configuration files, to obtain sensitive information and execute arbitrary code.

According to Mandiant, the first attempt to exploit this vulnerability was observed on 27 June 2024 by the UNC5820 group.

9.8

CRITICAL

-

Exploited
Remote code
execution

EPSS: 87.15%

PoC: YES

paloalto NETWORKS

CVE-2024-3400

On 12 April 2024, Palo Alto published a security bulletin concerning the critical vulnerability CVE-2024-3400, affecting GlobalProtect.

A command injection vulnerability in the GlobalProtect module of Palo Alto PAN-OS allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

According to Volexity researchers, exploitation of the vulnerability by UTA0218 was observed from 26 March 2024.

10

CRITICAL

-

Exploited
Remote code
execution

EPSS: 96.26 %

PoC: YES

paloalto NETWORKS

CVE-2024-0012

On 8 November 2024, Palo Alto Networks published a security bulletin PAN-SA-2024-0015 to report a vulnerability exploited in the administration interfaces of its firewalls.

On 18 November 2024, Palo Alto confirmed that this vulnerability allows an unauthenticated attacker to obtain administrator privileges, modify configurations or exploit other elevation-of-privilege vulnerabilities such as CVE-2024-9474.

9.8

CRITICAL

-

Exploited
Privilege
escalation

EPSS: 97 %

PoC: YES

CISCO

CVE-2024-20359

A file control flaw in the flash memory of Cisco Adaptative Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) allows an authenticated local attacker, by copying a file specifically forged in the disk0:file system, to execute arbitrary code and gain root privileges.

6

MODERATE

-

Exploited Remote code execution

EPSS: 0.13 %

PoC: NO

Citrix NetScaler

CVE-2023-6548

This vulnerability allows an attacker with access to the NetScaler management interface to execute arbitrary code on it.

8.8

IMPORTANT

-

Exploited Remote code execution

EPSS: 1.79 %

PoC: NO

GitLab

CVE-2023-7028

On 11 January 2024, GitLab published an alert concerning critical vulnerabilities in the Community Edition (CE) and Enterprise Edition (EE). CVE-2023-7028, considered to be the most critical, allows an attacker, by sending forged requests to the Rest API, to reset a user's password and log in.

10

CRITICAL

-

Exploited Authentification bypass

EPSS: 93.22 %

PoC: YES

ssh COMMUNICATIONS SECURITY

CVE-2024-6387

A security measure implemented to protect OpenSSH against CVE-2006-5051 was removed in OpenSSH version 8.5p1. This security regression allows a remote, unauthenticated attacker to execute arbitrary code with root privileges or to cause a denial of service.

8.1

IMPORTANT

-

Exploited Remote code execution

EPSS: 0.28 %

PoC: YES

ScreenConnect

CVE-2024-1709

An access control flaw allows an unauthenticated attacker to access the ScreenConnect installation wizard, which is normally restricted to authenticated users. This access allows the attacker to create an administrator account and access confidential data. Exploiting this vulnerability is not very complex.

10

CRITICAL

-

Exploited Security bypass

EPSS: 95.72 %

PoC: YES

Microsoft

CVE-2024-21412

This vulnerability is due to a link control flaw in Windows. By persuading a victim to open a specially crafted file containing Internet Shortcut links, an attacker can exploit this flaw, bypassing security controls, in order to execute arbitrary code. This vulnerability has reportedly been exploited since December 2023. Trend Micro researchers have observed at least two campaigns exploiting this vulnerability. One of these campaigns, associated with the Water Hydra group (DarkCasino), targets the financial sector (traders). The second is thought to be associated with Darkgate operators. The attackers are believed to have used phishing emails containing a link to a malicious jpeg image or PDF to exploit this vulnerability. When the user clicks on the image, the warning dialogue window is no longer displayed, and malicious files are executed until the DarkMe Remote Access Trojan is deployed.

8.1

IMPORTANT

-

Exploited Security bypass

EPSS: 2.87 %

PoC: YES

Cleo

CVE-2024-55956

A defect in the Autorun directory of Cleo's Harmony, VLTrader and LexiCom software allows an attacker to execute arbitrary Bash or PowerShell code on the system. This vulnerability is due to an incomplete patch against CVE-2024-50623. It was actively exploited by the Cl0p ransomware group.

9.8

CRITICAL

-

Exploited Remote code execution

EPSS: 96.9 %

PoC: YES

> Vulnerability management requires more than simply calculating universal risk scores. **It is important to put in place a process to have a business/impact view and the level of exposure**. By combining different elements of the environment, certain vulnerabilities with a high score could have a much lower rating for the entity under consideration.
> Critical vulnerabilities, like the one affecting CLEO, are being used by cybercriminals who have a financial interest in exploiting them quickly, such as the Cl0p ransomware group.

2.3 VICTIMOLOGY OF RANSOMWARE

Ransomware groups are still active in 2024, despite law enforcement operations (see 3.4). After years of overactivity by these groups, it would appear that 2024 will be a "*quieter*" year. The groups appear to have reorganised following the various police operations, forcing them to rebuild their infrastructures and alliances and regain the trust of affiliates and users of Ransomware as a Service (RaaS).

Even so, the business remains lucrative. It continues to attract new players, who are taking over the market share vacated by competitors shut down by law enforcement agencies. RansomHub takes the top spot, dethroning the famous Lockbit.

An overview of the activities and demands of the various groups is presented. It is important to analyse these figures with hindsight. Many of the claims made are not true, as has been the case in the past when Lockbit were falsely implicated. The marketing of a criminal group can take liberties with reality, with the aim of attracting new recruits or new members to their service... "*Business is business* !"

But isn't business in decline?
After years of explosive growth in encryption ransomware, has a turning point been reached? The increase compared with 2023 is only 11 %.

Here is a global overview of ransomware activity, with a focus on certain European countries.

2.3.1 / World victimology

Most active criminal groups

1	2	3	4	5	6	7	8	9	10
RansomHub	Lockbit 3.0	PLAY	Akira	Hunters International	Medusa	BlackBasta	Qilin	BianLian	INC Ransom
530 victims	519 victims	359 victims	300 victimes	226 victimes	214 victimes	188 victimes	181 victims	166 victimes	158 victims

Target countries

1	2	3	4	5	6	7	8	9	10
USA	UNITED KINGDOM	GERMANY	CANADA	FRANCE	ITALY	AUSTRALIA	SPAIN	INDIA	BRAZIL
1 821 victims	216 victims	154 victims	128 victims	119 victims	118 victims	73 victims	62 victims	60 victims	57 victims

3RD GERMANY

Compared with 2023, the change in the top 3 countries is the arrival of Germany in 3rd position.

Targeted business sectors

1	2	3	4	5	6	7	8	9	10
Construction	Hospitals and Health	Services and IT consul-tancy	Law firms	Government - Administration	Services	Retail	Accounting and Management	Software development	Medical practices
350 victims	210 victims	195 victims	146 victims	134 victims	133 victims	126 victims	119 victims	109 victims	104 victims

In terms of business sectors, IT services and consultancy have moved into the world's top 3 compared with 2023.

2.3.2 / Victimology in France

Most active criminal groups

1	2	3	4	5
Lockbit 3.0	8BASE	RansomHub	Qilin	Hunters International
26 victims	16 victims	12 victims	10 victims	8 victims

Targeted business sectors

1	2	3	4	5
Construction	Archirecture	Public administration	Services and IT consultancy	Pharmacy
7 victims	6 victims	6 victims	4 victims	4 victims

119 ATTACKS

France is ranked 5th in the world for ransomware attacks.
In 2024, 119 ransomware attacks targeted the region.

2.3.3 / Victimology in Germany

Most active criminal groups

1	2	3	4	5
Lockbit 3.0	BlackBasta	RansomHub	Cloak	Akira
17 victims	15 victims	11 victims	10 victims	9 victims

Targeted business sectors

1	2	3	4	5
Construction	Services and IT advice	Electronic industries	Industries machine	Food industry
12 victims	10 victims	6 victims	6 victims	5 victims

154 ATTACKS

Germany ranks 3rd in the world for ransomware incidents, having been the target of 154 attacks. The sectors most frequently targeted in 2024 were **construction and IT services**.

2.3.4 / Victimology in Italy

Most active criminal groups

1	2	3	4	5
RansomHub	Lockbit 3.0	8Base	BlackBasta	Akira
18 victims	14 victims	12 victims	10 victims	7 victims

Targeted business sectors

1	2	3	4	5
Services and IT advice	Industries manufacturing	Retail distribution Textiles	Electronic industries	Restaurant ser-vices
11 victims	11 victims	7 victims	4 victims	7 victims

118 ATTACKS

Italy is ranked 6th worldwide for ransomware attacks, with 118 known attacks. The main sectors targeted in 2023 are **IT services and manufacturing.**

2.3.5 / Victimology in Spain

Most active criminal groups

1	2	3	4	5
Lockbit 3.0	RansomHub	Hunters International	Cactus	8BASE
20 victims	15 victims	7 victims	5 victims	5 victims

Targeted business sectors

1	2	3	4	5
Administration public	Apparel industry	Real estate	Industries	Services and IT advice
5 victims	5 victims	5 victims	4 victims	4 victims

62 ATTACKS

Spain ranks 8th worldwide for ransomware attacks, with 62 claims.

2.4 DEFENCE ASSESSMENTS

This section contrasts with the previous attacker-focused analysis by examining the perspective of defense teams. For aDvens, this comes from the SOC teams, whose main lessons in terms of detection and protection are shared below, and from the CERT teams.

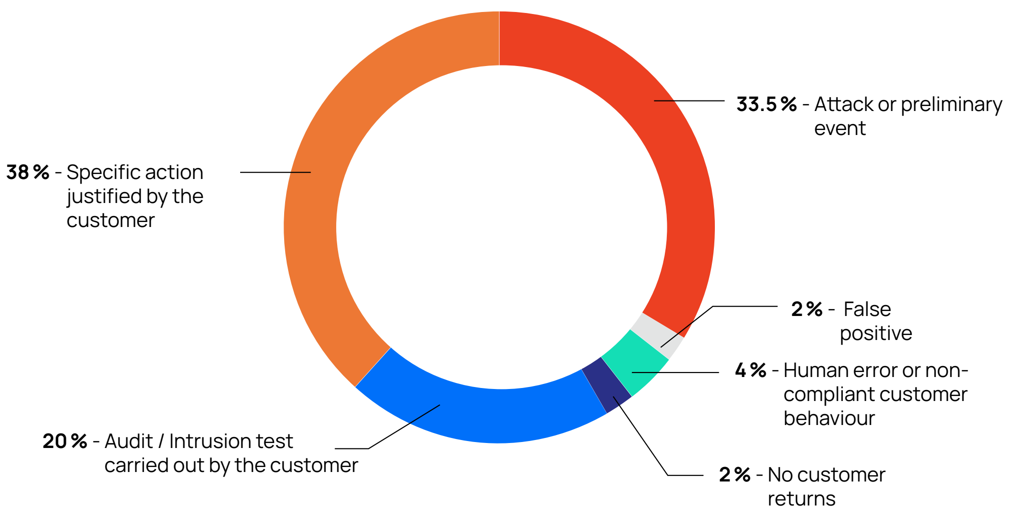
This year, the report includes an analysis of the action plans formulated by CERT teams following anticipation activities (such as CTI) or incident response and crisis management activities. This new analysis highlights the most advantageous actions to reduce the occurrence of a crisis and its impact.

2.4.1 / SOC status report

Including the defence point of view in a threat report puts the figures for successful attacks into perspective, compared with attempted or blocked attacks.

This is an opportunity to take a step back and look at our cyber defence systems and how well they are adapted to a changing threat. This summary is based on a review of alerts and incidents handled by aDvens's SOC teams in 2025.

Nature of events detected by aDvens's SOC



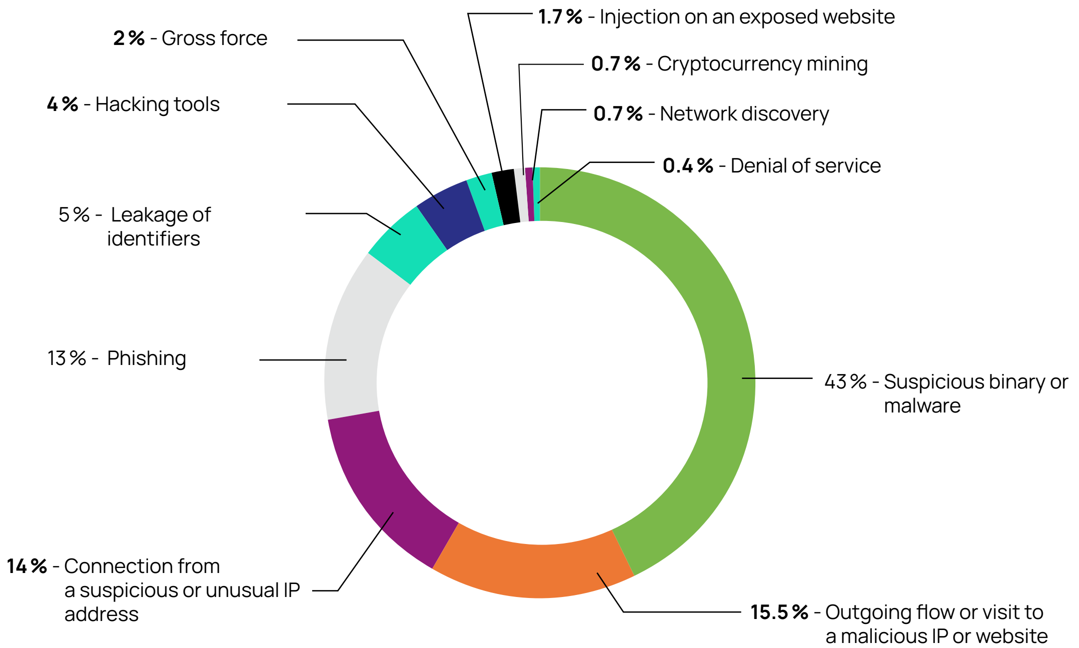
External malicious actions comprised approximately 33% of all critical priority events (+6 points vs. 2023), confirming an improvement in the relevance of the aDvens SOC's detection and an increase in actual attacks on information systems.

Although internal risk behaviours do not account for a large proportion of events (4 %), they are still sensitive events because employees have direct access to data or infrastructure **.**

These events may reflect malicious intent or handling errors / lack of knowledge of good practice within the organisation. They highlight:

- The need to continue efforts to raise awareness, including among technical teams;
- The need to maintain a good level of supervision over the infrastructure, including areas or perimeters not directly exposed to the outside world;
- Theimportance of continuously improving processes and documentation to ensure the safe use of the information system.

Breakdown of attacks or preliminary actions to a potential attack blocked or detected by aDvens's SOC



Malware is the most common modus operandi (43 %). The percentage of malware in critical incidents is up compared with 2023 (+6 points).
The most common strain identified is Raspberry Robin. This is a worm whose markers are well identified by security solutions. Its prevalence reflects a lack of computer hygiene, with these detections resulting from the connection of removable media whose origin is not controlled. During the remediation phase of incidents, it is often the case that the media is not clearly identified, opening up the possibility of further contagion attempts. The level of EDR coverage, the activation of security policies enabling blocking and the very regular review of these configurations are therefore critical to avoid contamination in contexts where blocking USB ports is not compatible with the activity.
Uncontrolled network flows, whether outbound to malicious sites or inbound from an unusual or suspicious IP, account for almost 30 % of alerts (16 % + 14 %), a sharp increase compared with 2023. **Phishing, for its part, accounts for 13 % of alerts, representing a fall of more than 15 % compared with 2023**. This fall is partly the result of improved tools and greater awareness among teams.

In addition, **almost 20 % of high-priority tickets correspond to intrusion tests to assess the SOC's performance** or meet compliance requirements. **This number is up by 8 % compared with 2023**, which clearly highlights the continuing growth of the threat and the need for customers to be reassured about the effectiveness of their protection system. The regular launch of SOC and information system audits is relevant if the report is shared in detail and exhaustively with the defence teams and if it is supplemented by 3-handed exercises (Auditor, Defender, Customer) known as the "*Purple team*". Now, if the percentage of alerts handled by the SOC is too high for audits, this could lead to a bias towards underestimating high-priority alerts. The security analyst must constantly expect to receive alerts relating to real attacks.

Another interesting figure is that **almost 30 % of high-priority tickets are ultimately classified as legitimate actions after validation with the customer**. This could, for example, be an action carried out by a member of the customer's Cyber team in order to test a security tool. Declaring this type of action in advance or carrying it out on dedicated environments would reduce the proportion of tickets of this nature, while optimising everyone's time and effort.
Generally speaking, the more the SOC and its customer communicate, the more relevant the data is.

EDR remains a central element of detection, but it cannot be the only source. In fact, although behavioural algorithms are becoming more and more effective, there are many ways of circumventing EDRs. The correlation of information between different sources collected from a customer makes it possible to identify behaviours based on unitary events that could be described as weak signals.

What's more, with attacks on EDR consoles in the cloud on the rise, it is essential to monitor these perimeters, in addition to implementing best security practices. This also highlights the need to evolve detection strategies. **Real-time detection is no longer the only way of identifying threats, but *threat hunting* now plays a major role in detection**:

- When an IOC is identified, an analysis of past events is used to assess the risk of a compromise already in progress;
- Thanks to the collective intelligence offered by a pooled SOC, an indicator or technique that is the subject of an incident at one customer site will directly benefit all customers, for whom a retroactive indicator search will also be carried out.

There has been a sharp increase in MFA bypass attacks, due in particular to the use of the Tycoon2FA phishing kit. In one case detected by the aDvens SOC, the attacker gained access to a company employee's account via a phishing attack, enabling him to recover the login details and the MFA token. He then requested a change of direct debit from a customer, taking advantage of an ongoing email exchange to make this request. Initial analysis showed that the connection had been made using MFA. Following these discoveries, the analysts improved the surveillance plans to include these new techniques. Observation of a change in behaviour compared to normal enables detection. Authorising the use of commercial VPNs (Windscribe, NordVPN or others) on organisations' machines increases the difficulty of detecting such behaviour.

2.4.2 / CERT action plans

aDvens's CERT develops remediation action plans during interventions to contain security incidents, mitigating its impact and avoiding any recurrence of the incident. These measures should be analysed from two complementary angles:

→ **Anticipation and prevention**
through threat intelligence;

→ **Crisis management and incident response**
to a threat that has achieved its strategic objective.

In order to optimise the implementation of these measures, aDvens's CERT has a database of actions structured according to different levels of priority and complexity. This base is organised by axis corresponding to action perimeters:

Axis 1	Protection & Hardening
Axis 2	Access & privilege management
Axis 3	Organisation of safety
Axis 4	Perimeter & Insulation
Area 5	Logging & Monitoring

In addition, each action is linked to a priority level to ensure optimum organisation of the remediation plan:

Priority 1

Concerns actions carried out during the incident response, of a level of difficulty deemed easy and medium to achieve in the short term (less than 2 months).

Priority 2

Actions carried out after the incident response, at a level of difficulty deemed easy, medium and difficult to achieve in the medium term (between 2 and 6 months).

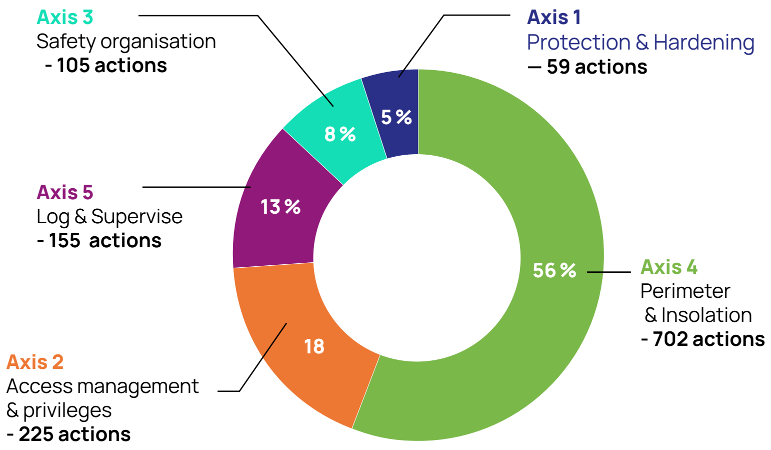
Priority 3

Actions carried out after the incident response, of a level of difficulty considered to be medium and difficult to achieve in the long term (between 6 months and 1 year).

→ Anticipating and preventing

The CTI team draws up remediation plans for monitoring requests on the various Internet channels ("clear", "deep" and "dark web"), following detection by the SOC or as part of crisis management with the CSIRT team.

Breakdown of actions resulting from analyses in 2024



In terms of prevention and anticipation, the recommendations focus mainly on **the perimeter protection of equipment and the partitioning of the information system** (Axis 4). These recommendations are the result of investigations that have revealed data leaks of authentication elements (credentiales/passwords) as well as the exploitation of vulnerabilities affecting equipment exposed on the Internet.

In addition, controlling the separation between the Internet and internal entities must be an absolute priority. This boundary is not limited to the physical equipment providing the interconnection; it also encompasses messaging services and cloud service providers. A pragmatic, risk-based approach, in line with the business challenges, is essential if this prioritisation is to be effective.

Breakdown of priority levels for actions

Priority 1	Priority 2	Priority 3
729 actions	405 actions	112 actions

Prevention and anticipation requires rapid implementation of corrective actions, with almost 60 % of recommended measures to be implemented within two months. Some actions, such as resetting passwords, can be carried out immediately.
Although **Axis 1 - Protection and hardening** is the least represented (59 actions), the level of priority of the associated actions is high (49 priority 1 actions).

Figures based on the processing of +400 000 Deep & Dark surveillance alerts and +200 CTI qualification requests from SOC and CSIRT.

3 priorities for action

Axis 1 - Protection & Hardening - **59 actions**

Priority 1	Priority 2	Priority 3
49 actions	9 actions	1 action

Axis 2 - Access & Privilege Management - **225 actions**

Priority 1	Priority 2	Priority 3
211 actions	14 actions	0 action

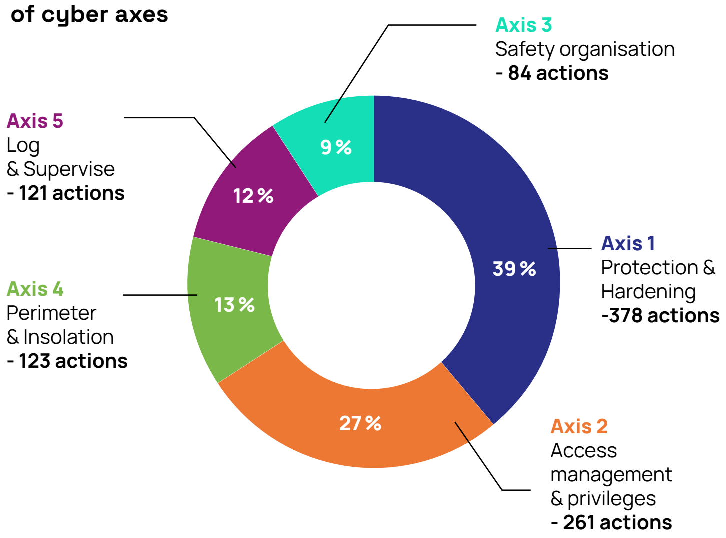
Axis 4 - Perimeter & Insolation - **702 actions**

Priority 1	Priority 2	Priority 3
402 actions	257 actions	43 actions

Responding to crises and incidents

The CSIRT team intervenes in crisis management and incident response, not only for its beneficiaries, but also for other structures as required. A remediation plan must be drawn up to ensure that the crisis is brought under control. This plan also ensures that corrective actions are aligned with management's strategic objectives, thereby ensuring an effective response to cybersecurity issues.

Breakdown by function of cyber axes



As part of its missions, aDvens's CERT, through the remediation action plans it provides and sometimes implements, recommends the implementation of important corrective measures in three areas:

Axis 2 – Access and privilege management :

- Implementation of a physical MFA;
- Deployment of a physical tiering model;
- Use of certificates on smart cards or physical tokens;
- Monitoring of entity information leaks.

Axis 4 – Perimeter and isolation :

- Implementation of a vulnerability management process specific to edge equipment (firewall, VPN, cloud, proxy, etc.);
- Diversification of technologies - if possible ;
- Correlation between physical architecture and tiering model at network level.

Axis 1 - Protection and hardening :

- Deployment and control of hardening measures on workstations and servers;
- Enhanced security based on business criticality;
- Proactive vulnerability management (patch management).

More recommendations: → Chapter 5

POINT OF VIEW

LOGGING & MONITORING

This year, recommendations relating to logging and supervision were less frequently suggested during incidents than in previous years. The deployment of EDRs and the implementation of SOCs are helping to limit the need for emergency supervision.
On the other hand, action plans aimed at improving the architecture and best practices for supervision and logging were more frequently recommended. These actions, which are more complex and structuring, require a longer implementation period of more than two months.

In addition, 30 % of the actions must be carried out within 6 months, to allow time for reflection after the incident. However, it is the full implementation of the action plan, followed by regular checks via audits and preventive measures, that will reduce the risk of another cyber crisis.

In 2024, the action plans developed by the CSIRT mainly concern the protection and hardening of infrastructures and information systems. The actions implemented include

- Resetting accounts;
- Reinstalling workstations and servers;
- Applying cyber hygiene and security measures

This approach highlights a critical point: when the threat has broken through the first defence barriers, protection in depth has failed and needs to be significantly reinforced.
This observation is directly linked to the degree of compromise of the entities that required intervention. In most of the crises we have dealt with, the attackers have managed to take full or partial control of the most privileged and strategic access points, exposing critical assets and impacting business continuity.

Approximately 50% of all corrective actions require immediate implementation. However, the complexity of organisations - be they businesses, local authorities or associations - combined with the resources and skills available, does not always allow for immediate implementation. In such cases, remediation becomes a major project, aimed at regaining control of the information system and requiring long-term monitoring.

Axis 2 - Managing access and privileges, although in second place, has the highest proportion of actions to be carried out quickly.
The other areas are security management, supervision and logging, where the majority of actions are rated as important.

Figures based on more than 70 CSIRT requests, 25 major incidents and 12 major crises.

Breakdown of priority levels for actions

Priority 1	Priority 2	Priority 3
471 actions	291 actions	205 actions

3 priorities for action

Axis 1 - Protection & Hardening - **378 actions**

Priority 1	Priority 2	Priority 3
187 actions	122 actions	69 actions

Axis 2 - Access & Privilege Management - **261 actions**

Priority 1	Priorité 2	Priority 3
161 actions	64 actions	36 actions

Axis 4 - Perimeter & Insolation - **121 actions**

Priority 1	Priority 2	Priority 3
69 actions	26 actions	28 actions

POINT OF VIEW

THE CONTRIBUTION OF PHYSICAL MEDIA

Security solutions based on physical media or incorporating physical models may seem anachronistic in an era of rapid migration to the cloud. However, in many cases of attack, a return to the physical world makes it possible to ensure a robust core of trust. Controlling all the technological layers involved in authentication, for example, means that attackers have a number of essential points of passage. This makes it possible to concentrate surveillance efforts in a single place to control access and input/output, and thus considerably increase the level of protection of this nerve centre of the information system. This solution makes it possible to strictly limit who can access the most critical perimeters by requiring the highest level of privilege.

In addition, physical smart cards and tokens make it possible to compensate for the failings of TOTP or MFA software suppliers, who are increasingly "*bypassed*" thanks to the Sneaky 2FA kit, for example.

POINT OF VIEW

DENIAL OF SERVICE

Denial of service (DoS) & Distributed denial of service (DDoS)

DoS or DDoS incidents rarely require direct CERT team intervention. Protection relies mainly on technical solutions that need to be highly responsive. In addition to increasing the capacity of the targeted resources (malicious actors are mobilising ever greater resources), it is possible to put in place specific anti DoS/DDoS protections that rely in particular on learning and anomaly detection (abnormal flow variation for example). In addition, CERT-SG has created Incident Response Methodology (IRM) sheets, to which aDvens's CERT has contributed. IRM-04 deals with DDoS[1/2]. It is useful to familiarise yourself with it in order to prepare for this type of attack. France's interCERT and the Fiche Réflexe working group have also produced documents on denial of service attacks to qualify and contain them, in addition to IRM[3].

[1] files CERT-SG IRM

[2] files aDvens RMI cards

[3] files InterCERT France RMI cards

> Whatever the action plan, it will be optimal (in terms of time and resources) when management validates the identification and prioritisation of critical business assets. This approach enables teams to put in place the right security measures and, above all, to deploy the right business continuity and recovery solutions.
>
> In addition, the aDvens's CERT and SOC teams were involved in several incidents and crises involving third parties. In 2023, this represented a significant proportion of the incidents handled, and this trend continued in 2024. All the actions envisaged must take into account the numerous interconnections with external players and also reflect on the most critical third parties, by means of contractual commitments if necessary.

> 2024 was characterised by significant advances in both offensive and defensive cybersecurity.
>
> A look back at some of the year's highlights.

03

Critical Incidents of 2024: High-Impact Events and Case Studies

3.1 PARIS 2024 OLYMPIC AND PARALYMPIC GAMES

The Paris 2024 Olympic Games were a global event, bringing together millions of spectators, thousands of athletes and colossal logistical organisation. Just like sporting performances involving years of training for just a few minutes of performance, the various cybersecurity professions worked for months on end to be ready for the event.

Anticipation

The preparatory phase

PILLAR 1

Optimal protection begins with identifying potential threats targeting the relevant companies and public organisations, based on their activities and the associated risks. As part of this preparatory process, ANSSI has shared its assessment of the threats, classifying them by criticality: cybercrime, sophisticated attacks (APT) and hacktivism.

Turning to operational teams

Anticipating the threat means not only identifying malicious actors, but also providing operational teams with actionable intelligence. This involves analysing TTPs (using the MITRE ATT&CK matrix), which enables surveillance plans to be adapted and the associated detection rules to be optimised.

Defining priorities

Given the intensity of the threat, it was necessary to classify the areas to be protected and assign priority levels. This approach made it possible to adapt the levels of protection. This adaptation was fed by the work of all the aDvens teams involved, from the SOC (which carried out several Purple Team campaigns) to the CERT (CSIRT and CTI) and the Audit teams. Each piece of information highlighting a weakness or an indicator of compromise was used to define the right levels of protection for each level of risk.

Making the most of community information

The preparatory phase included taking into account indicators of compromise (IOCs) and indicators of attack (IOAs) discovered during incident responses, monitoring or during shares within the cyber community (as was the case for this event with the ANSSI and the Cyber community in France).

Taking advantage of threat hunting

As part of a proactive approach, well in advance of the game's opening, post-mortem or "*hunting*" campaigns were carried out by the CTI teams to identify possible compromises, in conjunction with threat mapping. Some malicious actors infiltrate a system of interest weeks or even months beforehand, in order to carry out stealthy activities and be able to carry out actions that are just as stealthy - or only visible when the time is right. This knowledge of the threat has been enhanced by the sharing of information and the joint work of the SOC and the CTI. During the Olympic Games, this *Task* Force monitored just over 300,000 indicators.

> In addition to the games, the CERT was involved in crisis management in May. This intervention brought to light a possible actor who had been pre-positioned for many months.
> This intervention reinforced the preventive actions underway and the search for pre-positioned players prior to the event.

VIEWPOINT

ADVENS'S AUDITORS

The Audit teams were asked to carry out an audit campaign and Red Team missions at the heart of various Olympic sites. The aim was to assess the scenarios in which an on-site attacker could be compromised by discovering and exploiting vulnerabilities in real-life conditions, both on office networks and, above all, on industrial networks.

Industrial environments are traditionally associated with factories and heavy industrial infrastructures. However, in an arena or on a site open to the public, you will find a range of industrial systems, such as PLCs used for technical management of the building, the physical access control system, and the information and broadcasting systems (giant screens, IPTV, public address systems, etc.). The auditors carried out audits of IT and OT environments, as well as industrial IoT systems.

The audits enabled us to assess an attacker's ability to carry out a scenario that could have led to destabilisation during the event, for example. This work led to the development of a security plan aimed at correcting the vulnerabilities identified, such as :

- → The possibility of accessing sensitive networks from areas accessible to the public;
- → Possibilities of bouncing between IT and OT networks due to lack of filtering;
- → Ease of access and control on a giant screen system;
- → The obsolescence of industrial systems and the poor robustness of administration access security;
- → The poor physical security of installations providing access to applications critical to the operation of the competition site;
- → Bypassing physical security systems dedicated to access control to the competition site (copying access badges, opening closed doors and accesses...).

VIEWPOINT

SOC ADVENS

In the run-up to the Games, aDvens's SOC prepared to provide a level of commitment commensurate with this global event. To achieve this, a dedicated team was set up for the Olympic Games, enabling the right resources to be mobilised, while guaranteeing supervision of the other organisations benefiting from the SOC's services. Circles of "*level of exposure to threats and level of commitment to the Olympic Games (sponsor, host city, critical support infrastructure, etc.)*" were created.

The organisations at the heart of the system were supervised by a dedicated team. This team followed specific procedures (extended working hours, closer proximity to all the aDvens centres of expertise, etc.). For example, close proximity to the CTI team meant that indicators could be shared very quickly. This was crucial for carrying out targeted threat research or adapting detection rules with a very high level of responsiveness.

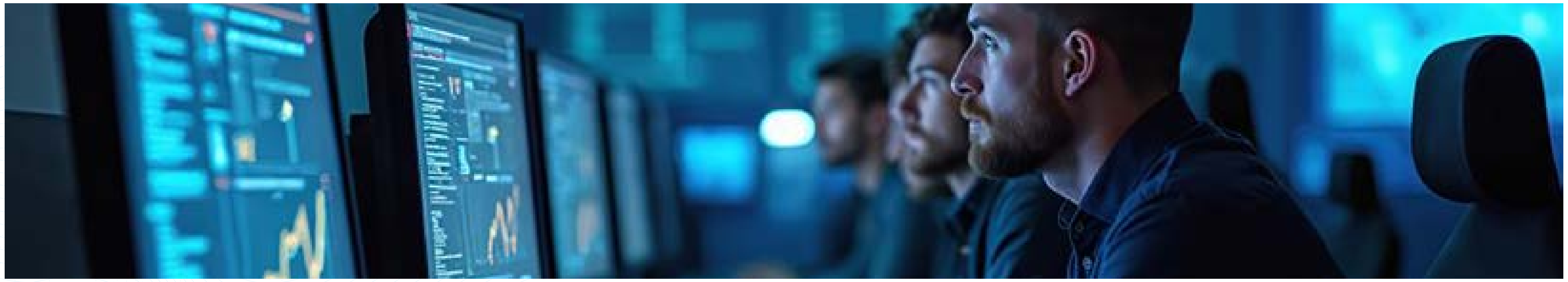
The Purple Team exercises carried out upstream tested the defence systems and supervision, providing very practical input for the continuous improvement process.

FOCUS

SOC OT

Industrial environments have also been the subject of specific preparation:

- Training analysts and the Blue Team in the specific features of the businesses concerned (not just OT technologies, but the use of these technologies in the business teams concerned);
- Definition of response procedures adapted to a variety of industrial contexts (to optimise the effectiveness of the response and its appropriateness to industrial constraints, but also to ensure that alerts are qualified by Cyber experts and OT experts);
- Adaptation of collection infrastructures (in particular via network probes dedicated to OT) according to physical constraints (power supply, bandwidth, etc.).



Detection and Reaction

The execution phase

PILLAR 2

An exceptional organisational structure, commensurate with the Games themselves, was implemented both nationally in France and within aDvens's teams. Large-scale sharing channels within the Cyber community in France (under the aegis of the ANSSI, with the OCOPG but also InterCERT-France, numerous SOCs and CERTs from companies, administrations and cybersecurity service providers), enabled a high level of proactivity to be developed.

This sharing, initiated in the preparatory phase, strengthened the security of the Games as a whole. Large-scale attacks would have been more difficult; the first to be hit would have warned the entire ecosystem so that protective measures could be taken.

The community was expecting massive attacks during this period. It would appear that the preparations were equal to the event. The Paris 2024 Olympic Games were not marred by a cyber crisis. The attacks were kept under control. The expected threats did not succeed in jeopardising this global event. aDvens's teams detected threats linked to cybercriminal groups and hacktivists.

- The CTI team carried out around thirty specific hunting campaigns during the games. These campaigns led to the detection of around ten attempted compromises on SOC clients.
- During this period, the CSIRT team was involved in 5 incidents, including 1 crisis management incident and 4 proven security incidents unrelated to the Games. Their interventions were carried out while maintaining a high level of commitment and availability: several interventions were refused (and passed on to peers).

VIEWPOINT

SOC ADVENS

During the Games, the SOC teams were faced with a variety of alerts. For example, VPN connections from an unauthorised country led to the detection of a compromised account used for these malicious accesses. Immediate blocking, following the alert issued by aDvens's SOC, brought the situation under control, without any consequences for the targeted entity. The alerts did not only concern IT perimeters and "classic" situations. Given the perimeters protected, some alerts concerned OT perimeters. An attempt was made to exploit a vulnerable industrial component. This was detected after analysis of suspicious network frames, made possible by Nozomi network security probes adapted to industrial protocols.

Learning and capitalising

After the Olympic and Paralympic Games

PILLAR 3

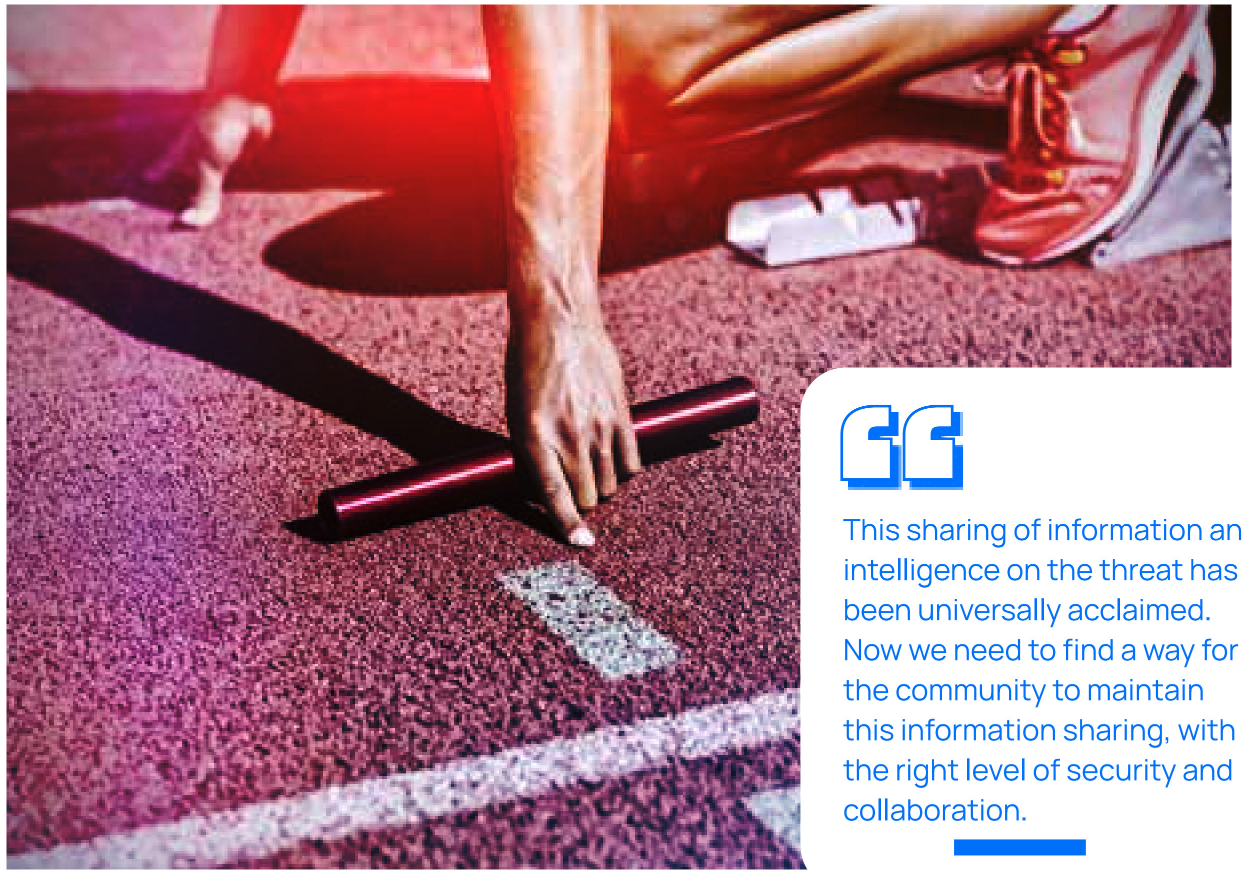
The whole community was aware of the exceptional nature of this event. But it also emphasised an essential point: good, thorough preparation (technical and organisational) is the key to controlled safety, reducing the occurrence of a crisis and the impact of any incident.

Another, more surprising lesson: activity wasmore intense after the Olympic Games than during them! It is likely that malicious actors realised how difficult it would be to carry out successful attacks during the phase of total mobilisation... they might as well take advantage of the "*aftermath*", when attention will be less intense and some of the teams will be resting. The incidents that may have been put to one side during the Games came back with a vengeance between September and November.

Be that as it may, the overall assessment of the Paris 2024 Olympic and Paralympic Games is very positive, since neither the ceremonies nor the competitions were marred by Cyber incidents. The Organising Committee for the Olympic and Paralympic Games (OCOPG), ANSSI and all the stakeholders have hailed this success, and in particular stressed the importance of working together to meet this challenge.

This collaboration went beyond the strict framework of the official bodies involved (OCOPG, police forces, etc.). Cybersecurity players from the sponsors and key structures surrounding the event were also involved. Everyone was delighted with this sharing of information and intelligence on the threat. We now need to find a way for the community to maintain this information sharing, with the right level of security and collaboration. These issues are being addressed by the CERT community, and in particular CERT-FR and InterCERT France.

We need to capitalise on this success, which has been facilitated by motivation commensurate with the event, but also by extraordinary investment. It is important that these budgetary efforts are maintained, because they represent a level of commitment adapted to a high threat. And the level of threat at the end of 2024 and the beginning of 2025 has not diminished.



> This sharing of information and intelligence on the threat has been universally acclaimed. Now we need to find a way for the community to maintain this information sharing, with the right level of security and collaboration.

3.2 ATTACKS ON INDUSTRIAL ENVIRONMENTS

In 2023, threat analysis warned of risks to industries and their supply chains. The year 2024 saw an explosion in threats targeting industry and industrial equipment (PLCs, SCADA, connected objects, etc.).

Various threats are targeting industrial sectors. For example, hacktivists have been targeting OT environments supporting water treatment and distribution. The ANSSI published a threat assessment for this sector, confirming the actions of hacktivists linked to the Ukrainian conflict, who have allegedly taken control of small water management units.

Securing industrial environments, through preventive or supervisory measures, is now a necessity given the associated risks. To continue with the example of water, if attackers succeeded in taking control of a key dam or wastewater treatment plant, the impact could be extreme for the populations concerned.

The motivations of the attackers have broadened. In addition to the desire for profit and espionage, they are now seeking to destabilise or sabotage, as a result of the tense geopolitical context. The result is a coalition between hacktivists and groups attached to states. This alignment of interests, which began in 2023, is confirmed over time.

The profit motive has not waned, however. This explains why the manufacturing and agri-food industries are at the top of the list of the most targeted sectors: in the event of a successful attack, stopping this type of production has a financial impact that is as rapid as it is substantial. Attackers and defenders alike are well aware that more and more threats are targeting industrial IoT and OT environments.

Industry is also a mine of information for anyone wishing to copy or reproduce European innovations. That's why the APTs have specifically targeted this sector and the subcontractors involved.

FOCUS

CERT ADVENS

Focus on aDvens's CERT's interventions in an OT context in 2024:
aDvens's CERT has assisted industrial companies that have been victims of cyber attacks:

- Bringing several production plants back into service with an acceptable level of risk in the face of a ransomware attack, with no ransom demand;
- Setting up a dedicated zone for critical business activities, with differentiated authentication and business continuity for all other activities;
- Switching from a compromised Active Directory to the user zone (linked to the authentication of certain critical factory applications) in less than 8 days, for more than 15,000 users and with physical tiering.

Key points for responding effectively to a cyber incident in an industrial context:

- A very detailed knowledge of the industrial environment and of the local teams;
- The right technical skills for industrial networks, so that they can be successfully *"enclosed" in* a short space of time;
- Rapid decision-making to validate the business priorities to be re-established;
- Easier synchronisation between teams thanks to an adapted organisation;
- The ability to mobilise different teams and players despite a degraded or inaccessible information system.

> The main actions implemented during crisis management in the industrial world concern system isolation and network segmentation, with differentiated access controls for the user zone. The separation of zones with a controlled point of entry simplifies the detection of an intrusion from the IT world to the OT world. And this principle simplifies supervision.

FOCUS

AUDIT

Focus on aDvens' Audit interventions in an industrial context in 2024 :

aDvens has had the opportunity to carry out Red team exercises in conditions as close as possible to those that would be encountered by an attacker "*in real life*".

- Using access to a plant's information system, the auditor was able to retrieve and modify the control program for a fleet of PLCs managing a critical system. The consequences of an attack could have been major for the site's security.
- The auditor was able to connect a malicious device capable of recovering all the scanned cheques from a cheque reader kiosk's maintenance access.
- From a factory car park, he was able to take control of the PLCs via a WiFi access point, and regain control of the management system and the entire factory supply chain.
- By taking control of a warehouse network, an attacker could gain the control over all the company's cash registers worldwide.

The vulnerabilities identified in the industrial environment remain the same as in previous years :

- The partitioning of plants and warehouses is too permissive and does not comply with the best practices of the PURDUE model. This means that all industrial equipment can be damaged very quickly;
- Communication between IT and OT environments are still possible due to the lack of flow filtering and the use of a shared directory for all environments;
- Technologies are still obsolete, and updates are not systematically applied. For example, there are still operator workstations running Windows XP ;
- The protocols used in OT networks are not encrypted, making it possible to alter their content or obtain accounts.

The issues that caused a stir in 2024 and how to react :

In 2024, water treatment systems were the target of numerous cyber attacks. The ANSSI has published a report dedicated to the cyber threat in this sector (find out more). The "*Typhoon*" network, affiliated to the Chinese state, has also targeted critical infrastructures by the back door. For example, the Volt Typhoon group targets small structures that provide services to more strategic organisations. Flax Typhoon operated a network of botnets around the world.

> Currently, attacks against industrial organisations still primarily exploit IT systems rather than OT infrastructure. However this proportion is set to change, as attackers realise that they can do more damage by targeting OT. What's more, these attacks will be facilitated by the use of AI, which will make it easier to understand and develop exploits that require the use of industrial protocols.

3.3 MASSIVE DATA LEAKAGE

In 2023, an initial trend towards not encrypting and instead stealing data was reported. Attackers realised that they could gain more by remaining as discreet as possible to maintain the right level of pressure, and then by monetising the value of this data.

2024 was a record year for data theft : no fewer than 5,629 data breaches were notified to the CNIL, 20 % more than the previous year[1].

Millions of accounts[2] have been hacked, and the chair of the body, Marie-Laure Denis, has even spoken of "*half the french people whose personal data have been compromised*."[3]

Among the most high-profile attacks were those targeting the operator Free, the third-party payment service providers Viamedis and Almerys and the *France Travail* agency. What these organisations have in common is that they have large databases of information on many individuals whose "*account*" (login/password) is now circulating in the wild, and more likely on the Dark or Deep Web.

The numerous data thefts have facilitated access to potentially valid accounts, with which attackers can penetrate the information systems of their target organisations.

What's more, analysing the data from several thefts enables it to be enriched and, consequently, enhanced. The sum of all the leaks makes it possible to create consolidated databases containing a wide range of information.

This enrichment offers the attacker a wide variety of solutions for deceiving his target by using personal details (physical address, social security number, identity of a bank adviser, etc.).

[1] article cnil.fr
[2] items 01net.com
[3] item rtl.fr

A Universal Threat: No Organisation is Safe

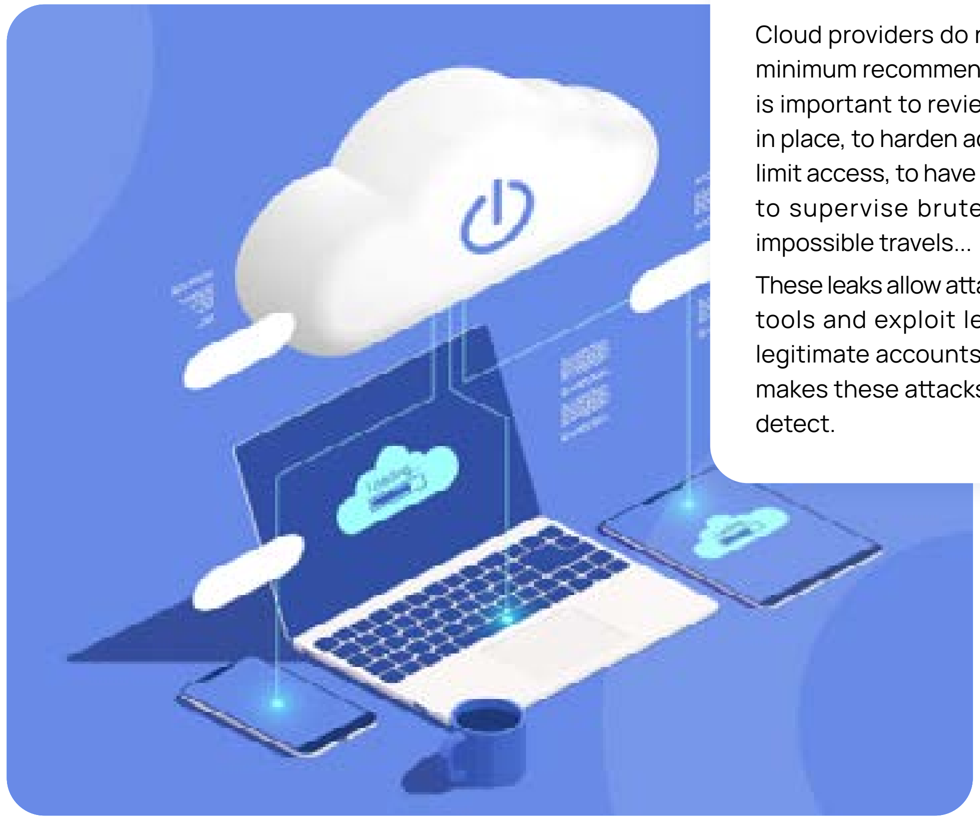
In early 2024, hundreds of HPE's (Hewlett Packard Entreprise) O365 accounts were compromised by APT29. The attack targeted the accounts of management teams as well as the teams in charge of cybersecurity at these organisations. Companies like these have the resources to invest in their cybersecurity. This episode proves that no one is safe from data theft.

A new modus operandi for stealing information, which had not yet been encountered by the aDvens CERT teams, is the transfer of tenants to a tenant controlled by the attacker.

After successfully recovering a valid account on the tenant, the attacker took control of the global administrator account. He then changed the telephone number for the MFA, while he created a valid access and deployed an application linked to this account, then restored the MFA telephone number of the account to the highest privilege. With the application in place, he was able to retrieve the tenant's information and transfer it.

All the data was transferred to a tenant controlled by the latter. After numerous requests to the supplier, it was possible to repatriate the elements and cancel the transfer. This took around a week, during which time the data was no longer under the control of the client.

Following this remediation, the main countermeasures put in place were "*geo-filtering*" (the attack came from a different geographical area to that of the sponsor), the strengthening of security measures for the global admin account (strong password, use of the application MFA rather than SMS), the introduction of supervision of impossible travels, and supervision of brute force password attempts on the tenants.



Cloud providers do not always provide the minimum recommended level of security. It is important to review the level of security in place, to harden administrator access, to limit access, to have a good level of logging, to supervise brute force attempts and impossible travels...

These leaks allow attackers to use legitimate tools and exploit legitimate assets with legitimate accounts. This modus operandi makes these attacks even more difficult to detect.

RECOMMENDATIONS

- SG's (Société Générale) CERT provides methodological sheets sheets to help you prepare and take the first steps in the event of an information leak[4];
- For organisations that have been the victim of an attack on their databases : as data leaks are increasingly publicised in the media, it is essential to prepare and handle crisis communications across all channels, including social media, and to quickly inform those affected by the data theft;
- Implement a process for lodging complaints and making declarations to regulators and to the country's RGPD entity.
- Have the ability to reinitialise compromised credentials, detect attempts to use stolen credentials (connection times, origin of connections, etc.), monitor information leaks relating to your company or entity, etc. ;.
- For companies whose employees are affected by data theft: redouble their vigilance and include this risk in your SOC monitoring plan.

[4] article aDvens media

3.4 A LOOK BACK AT SOME LAW ENFORCEMENT OPERATIONS

In 2024, law enforcement agencies achieved some very significant victories.

Cronos operation

against Lockbit, a ransomware "*giant*"

At the beginning of 2024, authorities in 10 countries dismantled one of the world's largest ransomware groups in an international operation called Cronos. Two people were arrested and thirty-four servers were seized.

Endgame operation

against several droppers including Pikabot

In May 2024, several droppers were targeted by another international operation. They included IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot. The operation led to four arrests and the seizure of more than 100 servers, a way for the authorities to set the tone ahead of the Olympic and Paralympic Games.

Kraken operation

against Ghost messaging

In September 2024, Europol announced the arrest of 51 people after dismantling the Ghost messaging service with the help of authorities in nine countries. Encrypted from end to end using three different standards, the service had become a preferred communication tool for criminal groups.

These operations are the result of a long period of work, made possible and crowned with success thanks to cooperation between police forces on an international scale. They were also made possible thanks to the victims who agreed to lodge complaints and to the information received from the field by the security incident response service providers (PRIS).

POINT OF VIEW

CERT ADVENS

A complaint is the start of an investigation: without a complaint, there is no investigation. Without an investigation, operations are not possible. The rate of complaints filed is close to 90 % for aDvens's CERT interventions.
All our sponsors who filed complaints contributed to the success of these operations. It is true that some victims are afraid to use this lever for image reasons. However, it can help them to obtain information at the end of investigations, to recover data (if possible) and to participate in protecting themselves and others.

aDvens's CERT highlights this possibility every time it intervenes, and if a complaint is refused, offers to share the information collected anonymously, which could supplement ongoing investigations.

Of course, the groups that have been brought down know how to get back up again, but these victories are real brakes on cybercrime : they damage the psychology of the attackers by showing that the police can weaken them. The groups affiliated to the dismantled group can also be impacted, as in some cases they may face payment defaults that contribute to their weakening.

Anticipating resurgence of a cybercriminal group : the 5 key factors

aDvens's CTI team launched a new indicator in 2024 to assess a cybercriminal group's ability to reorganise after a disruption/ dissolution. This indicator is based on five key elements:

1 A solid foundation

A group with a large number of members and technological resources can reassemble quickly, sometimes almost instantaneously.

2 Structured recruitment

Whether through recruitment campaigns, the hiring of volunteers or an internal organisation designed to ensure the succession, these groups adapt and are reborn with method.

3 A permissive environment

When law enforcement agencies are unable to intervene effectively (because of a lack of international cooperation or judicial leverage), impunity strengthens their ability to survive. A cybercriminal operating from a "*tolerant*" country will be able to continue his activities without fear of arrest.

4 An ability to adapt

Far from being set in stone, these groups learn from their mistakes, analyse the tactics of the forces of law and order and constantly adjust their methods to remain operational.

5 State support

When a government turns a blind eye (or worse, actively supports these cybercriminals) their longevity and impact are considerably amplified.

Cybercrime does not disappear, it evolves. Understanding these mechanisms makes it possible to anticipate the regeneration of groups and adapt the security response accordingly.

Law enforcement pressure has led to some unexpected outcomes : the group behind BlackCat is said to have disbanded out of fear of the police, leaving with the ransom money of its affiliates. They reportedly staged an FBI seizure and disappeared with the cash !

04

Forecast 2025: Emerging Threats and Strategic Defense Priorities

4.1 OVERVIEW

VULNERABILITY

Vulnerability disclosures will continue to accelerate, with projections exceeding 50,000 published vulnerabilities - including an ever-increasing number in security products.

SAFETY OF THIRD PARTIES

Continued rise in supply chain compromises - through the weakest link or the link of greatest interest (notably outsourcing and outsourced security providers).

AI

- Attackers are increasingly using artificial intelligence on a daily basis, not only to enhance their techniques, but also to target AI systems themselves.;
- A concern shared by defenders, who will increasingly use AIs in their defence and who will also have to protect AIs.

AI will also be integrated into broader issues that do not exclusively concern cyber security, but that cyber teams will gradually have to embrace: disinformation, power games between major powers, technological independence, etc.

All this is taking place against the backdrop of an unprecedented geopolitical climate, particularly following the US presidential election in November 2024, which has led to fears of an upsurge in complex state attacks from APT (Advanced Persistent Threat) groups. added to this is the Pentagon-ordered pause in cyber operations against Russia, a recent development that is bound to have an impact, particularly on Europe.

4.2 DEVELOPMENTS TO BE EXPECTED AMONG ATTACKERS

Attack methodologies (TTPs) will continue to evolve throughout 2025 in response to technological advances and geopolitical developments.

AI as an accelerator

The use of AI for malicious purposes is growing rapidly, whether for the generation of stealthy malicious files, the creation of fake content impersonating identities, the automation of campaigns, the creation of malicious infrastructures, or even the acceleration of the training of junior malicious actors. All attacker groups are taking the time to analyse what AI can do for them and what they can gain from it.

At present, it is still possible to differentiate AI-generated content from real-world content. This boundary will become increasingly tenuous. More and more disinformation campaigns facilitated by the rise of AI and deepfakes will continue to be implemented in the current geopolitical context. These actions were conducted not only by state actors but by all categories of threat actors.

APT

Certain countries, such as China and Russia, are regularly associated with computer attacks, particularly complex APT-type attacks. Delicate to detect, these attacks sometimes incorporate highly sophisticated devices. The US cyber defence agency CISA has provided a very detailed analysis of an attack on Microsoft in 2023, which clearly demonstrates its complexity. Given the geopolitical unrest and tensions between the major powers, an upsurge in these state attacks is likely in 2025.

In 2024, the Chinese APT group Volt Typhoon used a vulnerability in Versa's SD-WAN platform to target ISPs, MSPs and IT companies, particularly in the United States. The technology sector was a prime target for China in 2024. With developments in both AI and computer components, this sector will remain a target for Chinese interests in 2025, whatever the continent.

On the Russian side, the war in Ukraine is still not over, and combined physical, informational and cyber actions are set to continue.

Hacktivism

This type of malicious activity was already significant in 2024 and will remain so in 2025 ! The evolution of conflicts and geopolitical structures will always bring its share of DDoS campaigns.

The coalitions between certain hacktivist groups and state groups give rise to fears that they will increase their capacity by learning or gaining access to more effective tools. These actions can have an impact in both the information and cyber fields. The use of state-level tools and procedures by other groups could also create confusion and destabilise the lines of defence, which could be exploited by state sponsored groups to carry out other actions. Diversions have always made it possible to take action in unexpected areas.

Ransomware

An increase of at least 10% in claims from ransomware groups is expected by 2025. As was the case in 2024, the sectors expected to be mostly targetted are the healthcare and manufacturing sectors. The technology and cybersecurity sectors will also be targets of interest in the current geopolitical context. Groups will continue to capitalise on existing vulnerabilities and find new ones to increase their effectiveness.

These groups will continue to target backup servers and virtualisation systems (such as ESXI or Hyper-V) to ensure that the victim organisation is brought to a standstill. By impacting the entire information system, the attacker prevents a rapid resumption of activity or recovery of data that could have been encrypted. It should be noted that encryption will no longer be systematic in the case of ransomware attacks.

Finally, it cannot be ruled out that some ransomware attacks will have the sole aim of destabilisation.

Supply chain

Attempts to compromise technology supply chains are rising steadily. In 2024, for example, the open source XZ Utils project running on Linux was used to introduce a backdoor with the aim of weakening OpenSSH. These technological building blocks, which enable access to a large number of information systems at once, will be increasingly targeted and will no longer remain within the bounds of state groups. Discovering a vulnerability in a component used by a large number of tools and software applications means that the environments of a large number of potential victims can be rapidly taken over.

The use of deepfakes to recruit for companies around the world is becoming increasingly common. North Korean groups have used deepfakes to impersonate IT workers in online interviews, increasing their chances of infiltrating technology companies. This sophisticated tactic allows them to bypass identity verification processes and compromise the security of targeted companies. These techniques are likely to become increasingly common and used by all types of attackers.

The increase in 2024 in the targeting of subcontractors both for reasons of lesser protection (opportunism) and to reach a target of greater interest will continue in 2025. Physical disruption of supplies through ransomware or sabotage will also become a reality.

> Information sharing during the Olympic Games significantly enhanced collective resilience against diverse threat vectors. The anticipation and information shares between teams were key factors.
>
> In the future, it will be important to put in place global knowledge-sharing and anticipation resources that will considerably increase the level of protection for all companies, administrations and entities, while taking into account the issue of sovereignty.

4.3 CHANGES TO BE EXPECTED ON DEFENDERS' SIDE

As attackers continue to upgrade their tools and processes, defensive teams will need to adapt their arsenal.

Supply chain

The sector CERT initiative in France is fundamental to sharing information with the entire chain. Sharing the protection capabilities of major players to strengthen their supply chains and partners should help achieve greater resilience.

It will be important not to neglect our VSE and SME partners and suppliers in the overall protection of our business. The provision of resources, tools, skills and the centralisation of knowledge should enable us to see an increase in protection or awareness among these players by 2025.

APT

Managed security service providers will have an important role to play in dealing with APTs. It will be necessary to ensure that their infrastructures are secure to guarantee that it is not possible to obtain the information available on these groups.

Enabling vital and essential entities to have action plans in line with the capabilities of these APT groups will also be a challenge.

In addition, the security of the anticipation, detection and reaction systems of these same service providers will have to be exemplary if they are not to become a source of threat. The guides are there, the people are motivated. We must continue to invest in and strengthen our protection systems. To achieve this, secure sharing between entities will be an absolute necessity. We must not underestimate the ability of APT groups to manipulate other actors (for example hacktivists) to achieve their objective.

AI for defence

AI has long been used in defence solutions. A new use is necessary to detect the use of AI by attackers, as AI-generated content becomes increasingly complex to detect. The first AIs to detect such content will emerge. Law enforcement agencies will also face a major challenge in certain areas in differentiating between AI generated content, content generated from realcontent (from a real photo, for example) and real content..

Data quality and characterisation will be key for defenders to avoid compromising the models used to detect other AI.

Ransomware

The action plans and solutions provided over the last few years offer a real prospect of putting in place measures to slow down ransomware groups. These groups, motivated by financial gain, give priority to the poorly protected companies or administrations in order to maximise their return on investment. Implementing the measures recommended in this report and the various best practice guides will help to reduce the number of crises.

Cooperation between cybersecurity teams, business teams and management committees will be essential to anticipate, detect and respond to threats targeting a business sector.

Hacktivism

In the face of hacktivists, DDoS protection has evolved considerably and effective solutions exist. They will need to be put in place. As tools evolve, anticipation and the sharing of information between players on these threats should make it possible to limit the impact of hactivist's actions. On the other hand, in the sphere of influence, we need to be particularly vigilant about what could trigger reprisals through mass manipulation.

Sharing information during the Olympic and Paralympic Games helped to build resilience in the face of different types of threat, and anticipation and sharing of team detections was key.

In the future, it will be important to put in place global knowledge-sharing and anticipation resources that will considerably increase the level of protection for all companies, administrations and entities, while taking into account the issue of sovereignty.

05 / Recommendations

aDvens
For cyber, people & planet

05

Strategic Defenses: Actionable Recommendations for Organisations

The aDvens teams have developed pragmatic, operational recommendations with three primary objectives:

1. **Reducing the occurrence of a crisis;**
2. **Minimising impact;**
3. **Managing and closing accounts.**

They are the result of action plans proposed and implemented by the teams in charge of **threat assessment** (CTI), **security level assessment** (Audit), **supervision** (SOC) and **crisis and incident management** (CSIRT).

Furthermore, the recommendations proposed in this report do not include the various requirements arising from the applicable regulatory framework. This regulatory framework is becoming increasingly structured, richer and more specialised, in particular with NIS 2 and its counterpart DORA, or the CRA (Cyber Resilience Act).

TARGET

DECISION-MAKERS AND MEMBERS OF THE MANAGEMENT TEAMS (COMEX, CODIR, ETC.)

PREPARING FOR THE CRISIS

When a crisis occurs, the response must be based on the organisation's most critical activity. This criticality may be linked to the proportion of the organisation's turnover represented by this activity, but also to its media exposure or the applicable regulatory framework. This criticality assessment must be carried out quickly but calmly, so that the right decisions can be taken to manage the crisis.

RESTART PRIORITY ACTIVITY

The main question to ask yourself is this : "*If one day, the entire organisation comes to a standstill, which activity should be restarted in priority to save the company ?*". This crucial question is asked by aDvens's CSIRT team during crisis management interventions. Without an answer to this question, it is much more difficult to react quickly and effectively.

IDENTIFY CRITICAL ACTIVITIES

Identifying the criticality of activities and sequencing the restart in the event of a total shutdown can be carried out using *BIA* (Business Impact Analysis). This methodological tool identifies priority activities and the information systems that support them. It can also be used to define the restart sequences (what to restart and in what order) for a given crisis situation.

> These recommendations apply equally to "*on premises*" systems and to cloud environments. The implementation of security measures must be accompanied by an evaluation process, via an audit carried out by a third party, in order to determine the organisation's cybersecurity posture. The implementation of measures can be based on the best practice guides published by ANSSI.

TARGET

TEAMS IN CHARGE SET UP THE SECURITY MEASURES (CISO, SOM, CIO, ETC.)

Perimeter security and component isolation

- + **Management of vulnerabilities** specific to edge equipment (firewalls, VPNs, proxies, cloud access gateways, etc.): a vulnerability in one of these components could render the entire IS vulnerable from its "*entry point*": it is therefore necessary to define a management process dedicated to these vulnerabilities and to vary the technologies and suppliers if possible. In addition, the network must reflect physical security measures and tiering principles;
- + **Review of the remote access policy:** remote access via VPN and access to Tier 2 components do not always need to be available 24/7. Depending on the users and their activities, the implementation of a time slot can be studied. This can be accompanied by simplified monitoring when no access is authorised (non-working hours, for example).

Managing access and privileges

- + **Implementation of strong authentication (MFA) with physical support** : TOTP and software solutions are increasingly being circumvented by attackers. The use of physical media (certificates on smart cards, physical tokens such as USB dongles, etc.) provides an additional level of protection against by-pass MFA;
- + **Implementation of a physical tiering model for central authentication components**: physical access to Tier 0 resources must not be neglected. The tiering methodology recommended by Microsoft must integrate the physical layer in order to increase the robustness of the authentication architecture and Active Directory servers;
- + **Monitoring information leaks affecting the organisation** : the threat from infostealers is growing steadily: every information leak, even a one-off, must be the subject of an action plan and accompanied by immediate measures to contain it;
- + **In-depth monitoring of privileged user accounts and groups**: any user, account or group with access to a critical function (in terms of business activities and administrative rights over IS components) must be included in an enhanced monitoring plan.

Protection and system hardening

- + **Setting up a component hardening process** : a component, whether it's a workstation, a server, a network device or an application, cannot be installed "*by default*". Its configuration (and that of the underlying operating system) must be adapted to suit the role of the component for the organisation and the potential vulnerabilities. Many guides exist, by technology family, for defining a suitable security foundation;
- + **Tighter control over back-ups** : the "*3-2-1*" principle (consisting of having 3 copies of data, stored on 2 different media, 1 of which is offline) must be implemented. Backups must be subject to regular validity and integrity tests.

> The events of 2024 decisively proved the effectiveness of collaborative cybersecurity approaches. The Olympic and Paralympic Games, in particular, were a full-scale laboratory demonstrating the effectiveness of a coordinated national programme in the face of high-intensity threats. The mobilisation of all stakeholders enabled a global event to take place without major incidents.

This model of multi-dimensional collaboration, structured around rigorous procedures and effective communication channels, represents a promising basis for tackling the challenges ahead.

The experience gained during this period of exceptional intensity provides a proven operational framework, adaptable to rapid changes in the threats anticipated for 2025 and beyond. In a context where threats ignore borders, where geopolitics generate instability, where technology demultiplies the capacity of attackers to cause harm, this collaborative approach deserves to be shared and repeated.

Conclusion

Threat status report 2024 - 2025

This report is the fruit of the work of aDvens's teams in terms of threat monitoring, but also the findings from field missions in Cyber crisis management, security incident response, attack response, security supervision or security audits and assessments.

The following organisations were asked to contribute to this publication:

- → **CERT**, both the threat intelligence team (CTI) and the team in charge of crisis management and incident responses (CSIRT) ;
- → **The SOC**, in particular the teams of analysts, who observe alerts and attempted attacks on customers' information systems (IS) on a daily basis ;
- → **Audit,** in particular the "*pentesters*" who reproduce the behaviour of attackers to test the robustness of our customers' defences.

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

For more information...

The CERT

aDvens bulletins

The advisories (monthly and alerts) published by **aDvens's CERT** are available on aDvens's website.

- https://media.aDvens.com/bulletins-cert/

Bulletins
CERT aDvens

Incident response reflex cards

before the CERT Société Générale

Working together for several months between SG's (Société Générale) CERT and aDvens's CERT has made it possible to propose **methodologies** updated **Incident Response Managers (IRM)** now available in English and French.

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

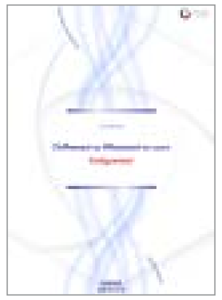
Incident response
methodology

Incident response procedures

InterCERT France

InterCERT France, through working groups, has published **reflex sheets** to which aDvens's CERT has contributed, alongside many other CERTs.

- https://github.com/intercert-france/publications/

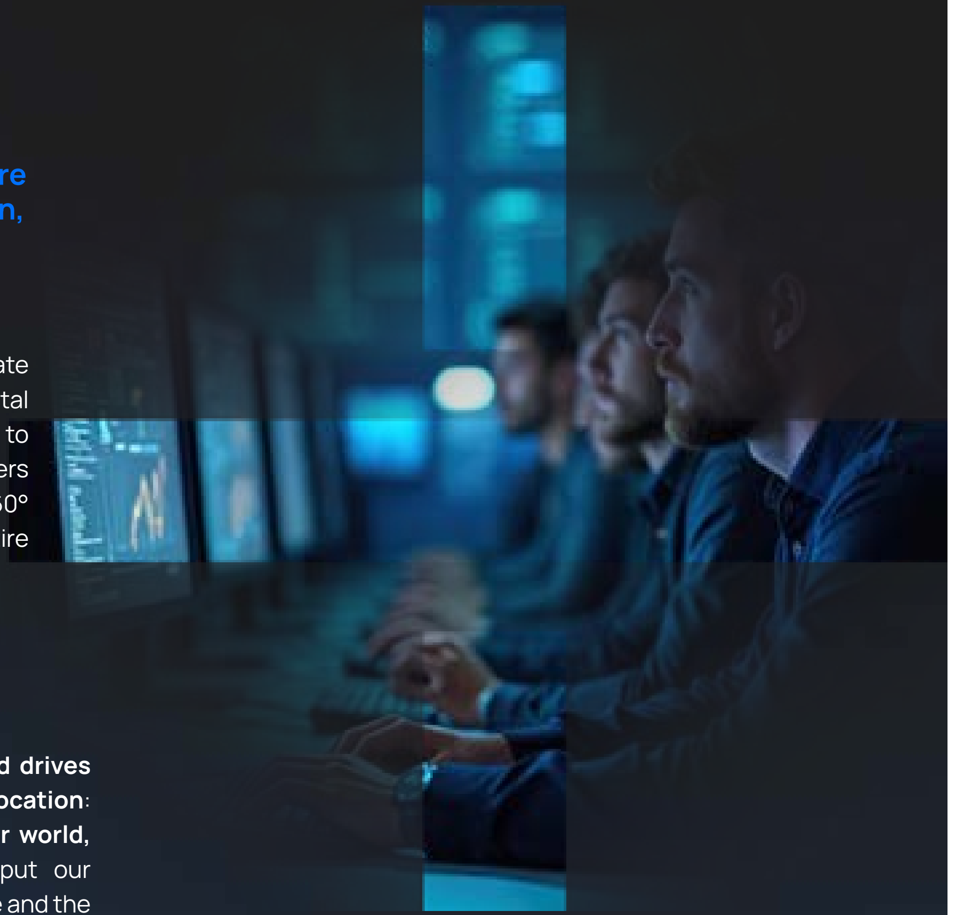


Incident response
methodology

> aDvens is a European leader in Cybersecurity, independent and sovereign.

About aDvens

INTRODUCING ADVENS



ADvens is an independent, sovereign European leader in cybersecurity. Our 650 experts are present throughout France, Spain, Italy and Germany, as well as in Montreal and Papeete.

Our mission: protecting public and private organisations facing increasing digital dependency and increasingly exposed to formidable attackers. We offer our customers a global, unified experience as well as a 360° service with close proximity across the entire cybersecurity value chain.

Our mission to protect guides and drives us every day. But it's not our only vocation: we **want to have an impact on our world, our society and our lives.** We put our performance at the service of people and the planet: 50 % of aDvens's Group's capital, and therefore the financial profits derived from it, are devoted to action in favour of people and the planet through the aDvens for People & Planet endowment fund.

about aDvens

Expertise

Strategy & Organisation

Operations & Animation

Detection & Response

Compliance

IoT & OT security

Cloud security

AI security

Sectors

Service public

Food industry

Industry

Energy

Health

Finance Insurance

Distribution

Tech & Digital

Transport

FOCUS ON ADVENS'S CERT

myCERT aDvens

Created in 2020 to respond to internal and external incidents, the aDvens's CERT comprises an Incident Response Team (CSIRT) and a Cyber Threat Intelligence Team (CTI).

In 2024, aDvens's CERT produced nearly forty incident responses, including several on ransomware cases. No fewer than 2,000 cyber intelligence bulletins were also published.

To carry out incident response missions, the CSIRT team can draw on aDvens' internal resources. This agility means that we can offer appropriate skills across the entire spectrum of cyber security.

For example, in the event of an incident involving a client with a SOC, the team works in conjunction with the client's operational security teams.

To carry out cyber intelligence missions, the CTI team gathers information and uses specific data feeds. They analyse all the information so that only the most relevant elements are reported. By monitoring over 700 cybercriminal channels, the CTI team can anticipate threats.

In support of aDvens's SOC, and in response to requests to qualify indicators of compromise, it capitalises on information, so that each incident becomes a source of information for all our clients.

The PRIS qualification, initiated in 2021 with ANSSI (France's national cybersecurity agency), was obtained for the 2 CERT teams. As a result, our investigation and OSINT processes have been validated and qualified, enabling us to offer the same level of requirements for both qualified and non-qualified services.

In 2024, aDvens's CERT was recognised as a leader by ISG in its Provider Lens for France.

SUMMARY OF ACTIVITIES

- The CSIRT team carried out around 40 interventions, including 12 crisis management operations. Among the victims, 4 infrastructures had their data exfiltrated and/or encrypted;
- The CTI team has carried out over 250 assessments and more than a dozen Open Source Intelligence (OSINT) investigations into potential data leaks, in close collaboration with the CSIRT and clients. This enabled us to confirm and validate hypotheses in the context of data exfiltration with clients;
- In addition, aDvens CERT has continued to develop and industrialise;
- We share our experience with ANSSI on an ongoing basis, whether through feedback, exchanges on incident response methodologies or the management of TLP/PAP indicators;
- There is constant sharing with ANSSI, whether through feedback, exchanges on incident response methodologies or the management of TLP/PAP indicators;
- Likewise, there are regular exchanges with the police, both to deal with incidents involving clients and to improve our synergies;
- aDvens's CERT is a member of the board of directors of the InterCERT-France association, which works to promote strong sharing between French CERTs. It will be at the heart of our desire to share with the community. This will enable the association to produce reflex sheets based on the work of a large number of French CERTs.

about aDvens

THE CERT'S KEY FIGURES

+40

CSIRT INTERVENTIONS

197

CTI QUALIFICATIONS

+90 %

OF SUCCESS ON TAKE-DOWNS

400 000

ALERTS ALERTS EASM / CTEM

leading to 620 contextualised alert bulletins

40 291

PUBLIC VULNERABILITIES ANALYSED

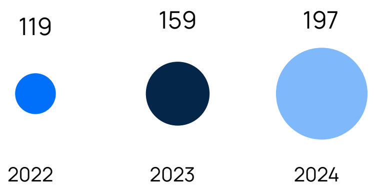
leading to more than 1,500 alert bulletins

73

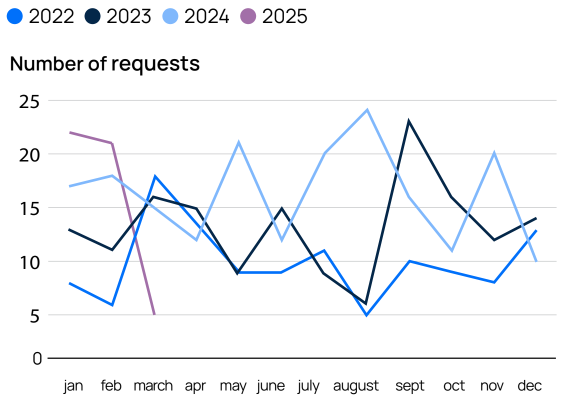
THREAT HUNTING CAMPAIGNS

detecting more than 20 proven compromises

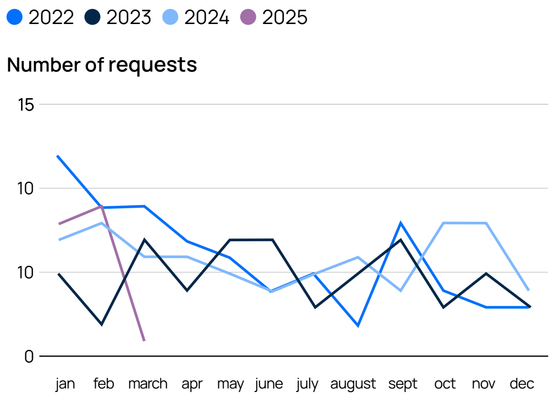
Total number of CTI qualifications



Number of applications for CTI qualification



Number of requests for assistance CSIRT



PRESENTATION OF THE SOC

mySOC® by aDvens

mySOC is aDvens' 24/7 managed detection and response offer. Since 2016, mySOC has been providing detection and response, MCO / MCS, vulnerability management, threat analysis and incident response activities for more than 500 customers in Europe.

Convinced of the need to protect all our customers' digital activities, whatever their environment, we work with them on an **operational security** trajectory that covers **all perimeters (IT, endpoints, cloud, OT/IoT) without compromising security**.

To protect our customers every day from an increasingly rapid and discreet threat, mySOC by aDvens relies on the best latest-generation technologies (EDR/NDR/IDR) orchestrated and enriched within an augmented AI/ML platform and operated by a team of over 300 multidisciplinary experts. To effectively protect our customers by offering a total understanding of our service, it is built around three axes:

→ We place **customer and aDvens collaboration and transparency** at the heart of our service: the cybercentre, operational 24/7, mobilises pooled and dedicated resources for each customer (SOC Manager, Lead Security Analysts and Technology Specialist). The mySOC portal enables our customers to manage their operational security in real time by accessing security incidents and the structuring elements of their service, such as the surveillance plan and the communication pact.

→ We are turning **collective intelligence** into an asset for our customers: by pooling our knowledge, we can ensure that every customer benefits from what we learn, and we can continuously improve all our monitoring points. New detection rules and threat markers are instantly deployed across the entire community, protecting all our customers. The AI/ML algorithms are trained on all the customer data to improve their accuracy in detecting the weakest signals through behavioural analysis.

→ We control **the entire detection and response chain** through our SOC platform. To enable us to protect new perimeters or integrate new technologies, we have designed an end-to-end agnostic security orchestrator that can connect to any security technology or data type. The SOC platform, fed continuously by threat analysis data (CTI), enables correlated multisource detection and orchestration of the response as close as possible to the equipment.

In 2024, SOC aDvens was recognised as a leader by ISG in its Provider Lens for France.

PRESENTATION OF THE AUDIT SERVICE

Audit aDvens
Security for the greater good

→ **In 2024, aDvens carried out more than 1,700 audits.**

aDvens supports you in managing and carrying out your audit campaigns across all your scopes, and integrates agilely into every stage of your projects.

Successful audits depend primarily on selecting the appropriate approach based on specific security challenges within the targeted perimeter. This approach may involve one or more audit scopes. Our offer covers all the services needed to assess the level of security from an organisational, logical and physical point of view.

- **Organisational and functional audit**: assess the general level of security and validate compliance with best practices and internal or regulatory requirements (ISO 2700x, PCI-DSS, GDPR, etc.);
- **Architecture audit**: to validate the level of technical security of an IS or infrastructure and the compliance of implementations with standards or regulations;
- **Configuration audit**: validate the level of security or compliance of components against internal or regulatory standards;
- **Source code audit**: using the source code to identify security risks and development practices that could be improved;
- **Penetration testing**:to test the level of security of a system or an application and assess the risk associated with the presence of a vulnerability through its full and concrete exploitation;
- **Social engineering**: measuring employee awareness through attacks targeting the human element: phishing, phoning or physical campaigns.

All our skills can be applied to specific themes and offers, such as:

- **Audit cloud** : Azure, AWS, GCP, O365 architecture and configuration audit ;
- **Audit IoT** : Hardware intrusion testing on connected objects, communication channels, firmware analysis, etc.
  Examples of solutions already audited: Connected buoy, box connected to a vehicle, electric charging stations, data security box via TPM chip, etc.
- **Industrial environment audit / OT** : Maturity diagnosis and review of industrial IS architecture, intrusion tests in warehouses or factories targeting key components (production line, access control, etc.), audit of biomedical equipment, etc.;
- **Audit Ransomware** : Carrying out a realistic Ransomware campaign to measure the effectiveness of detection solutions in place and to assess the ability to restore encrypted data;
- **Internet exposure audit** : Mapping of equipment and applications exposed on the Internet, collection of information about your company available on the Internet and the Darkweb (leakage of strategic information, theft of passwords, etc.);
- **Audit DevSecOps** : On-demand penetration testing during each sprint, code review support, etc.

All of this can be achieved on a stand-alone basis or via a Pentest-as-a-Service offering.

We also help our customers to secure their information systems and challenge their defence mechanisms through real-life exercises.

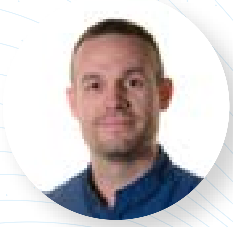
- **Redteam**: realistic intrusion campaign inspired by scenarios already carried out by criminal groups, targeting the most critical elements of the business. This service combines Internet, social engineering and physical attacks;
- **Purpleteam**: carrying out a series of attacks by the Red Team, and analysing the Blue Team's monitoring, detection and response capabilities, right through to actually blocking the attacks. This service allows us to improve the monitoring plan and all defence processes.

> Throughout the audit, we aim to be as close as possible to your teams, right from the preparatory stages. The results are then presented at different levels to meet individual needs : from the presentation of high-level risks for managers / decision-makers and with regard to your feared events to the most technical details enabling a perfect understanding of the audit findings and the action plans to be implemented.

aDvens is qualified as an Information Security Audit Service Provider (PASSI) for all audit and penetration test scopes by ANSSI, France's national cybersecurity agency. This qualification enables us to carry out the audits required by the *Référentiel Général de Sécurité* (RGS) and the *Loi de Programmation Militaire* (LPM).

Contributors

Fabian Cosset
CERT aDvens



David Quesada
CERT aDvens
and the CSIRT and CTI teams

Erwan Blanchon
SOC aDvens

Julien Reisdorffer
SOC aDvens DACH

Sébastien Calba
Audit

Stéphane Potier
OT cybersecurity

aDvens

For cyber, people & planet

LILLE
aDvens
32 Rue Faidherbe
59800 Lille
Tel: +33 3 20 68 41 81

www.aDvens.com

Credits: Shutterstock, Freepik, Flaticon
Design: Agence La nageuse