AVLAB
CYBERSECURITY FOUNDATION

CYBER TRANSPARENCY AUDIT
AVLAB
CYBERSECURITY FOUNDATION
★ Q3 – 2024 ★
CERTIFIED

# Transparency First Then Trust

Q3 24

## CYBER TRANSPARENCY AUDIT OF XCITIUM BACKEND DATA

Cyber Transparency Audit – a review of cybersecurity vendor Xcitium and their endpoint workstations protection

Range of the audit: 1 July 2024 – 30 September 2024 (Q3 2024)

2024

Q3 24

# Table of contents

# Transparency First

## Then Trust

The world needs **more transparency** in the cybersecurity

One of the cornerstones of cybersecurity is to ensure that data and systems are protected from serious consequences. It is difficult to choose a product if a customer does not have the opportunity to check whether the software meets certain standards. Endpoint cybersecurity is a multibillion-dollar industry that lacks standardized policies, yet it impacts businesses around the world.

Endpoint security software is designed to minimize risk. A good way to make it clear for a user that a developer helps to mitigate that risk is to be transparent about how the application works and the processes in the developer's infrastructure. By disclosing certain statistical information, it is possible to know and understand strengths of a product. This may lead to the resolution of the basic problem, that is the elimination of all remaining gaps. On the other hand, developers who are taking the difficult path of disclosing statistical data from end devices may face public criticism and control, but it is beneficial for all companies and institutions.

In an interpersonal relationship, clear rules are needed to build mutual trust. Transparency should be the cybersecurity industry's motto to strengthen the end customer's trust in the people who are responsible for the brand's image. This is the only way to improve collective thinking about cybersecurity.

I

# What is this audit?

## Definition of "Cyber Transparency Audit"

As part of the "Cyber Transparency Audit", the testing body as the Auditor checks data from a provider of a cybersecurity solution for historical compliance.

The audit is an independent assessment of a given system, organization, process, or entire project. The data is examined for compliance with specific guidelines that must be met. The main advantage of the audit is the participation of an external Auditor who is able to thoroughly check, and objectively indicate areas that need to be improved.

Obtaining the "Cyber Transparency Audit – Certified" certificate by a provider means that its effectiveness regarding historical data is confirmed.

The methodology and policy are available to anyone who meets the criteria, therefore anyone can join the project as the Auditor or Developer.

## Security incidents in telemetry data

This report contains analyzed and anonymized telemetry data that originated from devices protected against malicious software by a product called Xcitium Advanced. The presented data show a correlation between potentially malicious activity on a Windows device, and actually confirmed malware. This is important because unknown files on employees' computers that are not confirmed malware yet, can be a backdoor to serious threats such as ransomware or spyware.

## New standards for the endpoint protection industry

One of the overarching challenges currently facing the cybersecurity industry is the development of standards that will ultimately visualize the real effectiveness of modern security products installed on hundreds of thousands of end devices. Transparency of specific statistics, among others, malware data, as well as the information collected about cyberattacks, is fundamental from the point of view of building trust. After meeting this condition we, as the Auditor of historical data in the Xcitium infrastructure, can confirm that at the end of this chain there is an effective protection of the end customer's work environment which undoubtedly inspires trust, and builds a good opinion about a developer and its solutions.

## Nowadays transparency means more

The priority task of Endpoint Protection software is to minimize the risk of incidents. This is not entirely possible if the public does not receive information about the real functioning of the software. Well implemented protection in real time can relieve administrators who can start patching vulnerabilities, and thus better protect systems and data. Therefore, making incidents and threats publicly available (or lack thereof) from the point of view of fairness and transparency allows for a better assessment of the developer's technologies – whether they work well in real scenarios or not. In addition, auditing such statistical data allows to practically assess whether the applied configuration of protection settings is sufficient for the majority of end customers.

## The myth of closed source code

Open source solutions of Endpoint Protection are not popular in this industry, but developers can use certain libraries, frameworks, or share their code. It is a misconception that closed source code is more secure than open source – as shown by the examples of numerous incidents. Hackers do not need access to a source code to understand how it works. Through trial and error, they are able to find weaknesses, vulnerabilities of the application to various types of attacks that were not discovered in the process of creating an application. In addition, the disclosure of the source code may occur as a result of a cyberattack on the developer's servers or one of its partners (supply-chain attack). The unavailability of the code does not mean that we will not hear about incidents of critical vulnerabilities of the RCE (Remote Command Execution) class.

***Based on the analyzed historical data, we confirm that from 1 July 2024 to 30 September 2024, among 1 166 139 unknown 0-day files, no malware infection was recorded on systems that at this time were protected by Xcitium Advanced.***

## Key audit insights

- **Audited period:** 1 July 2024 – 30 September 2024
- **Purpose of the audit:** Confirmation of compliance with data from the audited period, indication of key information about malware and data leaks.
- **Scope of the conducted audit:** Audit of telemetry data concerns devices protected by the developer's software and file metadata as part of access to its static threat infrastructure.
- **Name of the audited developer:** Xcitium
- **Data comes from software of the class:** EDR, XDR, MDR Xcitium. The developer did not disclose which operating systems the audited period covers. Based on the audited file extensions for malware and clean samples, we conclude that this is a Windows environment.
- Public Data:
  https://www.xcitium.com/resources/threat-labs/data-statistics/
  https://verdict.xcitium.com/

## The audit was prepared taking into account the following data set

1. Devices with potentially malicious activity (virtualized files).
2. Devices with confirmed malware status (virtualized files).
3. The number of 0-day files classified as secure.
4. Number of 0-day files classified as PUAs.
5. Number of 0-day files classified as malware.
6. Potential data leaks and active infections.

**We used several malware samples to determine the compliance and authenticity of the audited data.
Those were run in the Auditor's network on a test machine with Windows 11 on the following days:**

Fille checksums (SHA1) together with machine and expert analysis were included in the audited data which we treat as confirmation of the authenticity of the data.

**SHA1: 9ea31c9c9f4d878f804fe5e24521bf831028a82f** 2024-07-03 08:11:14
https://verdict.xcitium.com/get_info?sha1=9ea31c9c9f4d878f804fe5e24521bf831028a82f
Malware Type: **Trojan Generic**

**SHA1: 496594c30db2456816e1acf7de35082c654be99a** 2024-07-23 12:19:42
https://verdict.xcitium.com/get_info?sha1=496594c30db2456816e1acf7de35082c654be99a
Malware Type: **Trojan Generic**

**SHA1: 1d78518cc76abf62a24da3c94f1f349191ae702f** 2024-09-11 11:51:09
https://verdict.xcitium.com/get_info?sha1=1d78518cc76abf62a24da3c94f1f349191ae702f
Malware Type: **Spyware**

**Transparency of statistical data is one of the fundamental arguments in favor of the honesty of the developer for the end customer.
That way it is easier to decide which solution to choose by comparing one product with competitive solutions.**

1. Without disclosing certain telemetry data, the end customer has no way to know about the real effectiveness of endpoint device security in practice.
2. Closed source code does not guarantee better protection against malware and hacker attacks.
3. Regular monitoring and auditing of statistical information about incidents from endpoint devices by external auditors can improve trust in the developer.
4. Early identification of problems in the audited project and neutralization of potential risk increases the effectiveness of security.

II

# Audit Summary

CYBER TRANSPARENCY AUDIT
AVLAB
CYBERSECURITY FOUNDATION
★ Q3 – 2024 ★
CERTIFIED

This part of the report is a summary of the statistics collected from devices protected by Xcitium where potentially malicious activity has been detected in relation to confirmed malware as a result of uploading a file from a device for the analysis in the cloud. The risk of unknown files on employees' computers can lead to infections with ransomware, spyware, or other malicious software. Employees may accidentally download unknown files from the Internet, bring them to the company on their mobile devices, or download them from an email. These files can damage operating systems which consequently leads to loss of important data, and even encryption of infrastructure and deletion of backups.

From 1 July 2024 to 30 September 2024, out of 1 166 139 unknown 0-day files, not a single system infection with malware or potentially unwanted software (PUA) was detected that could contribute to data leakage.

## Q3 2024 audit summary in numbers

| Total audited devices | Devices with potential malicious activity | Devices with malware (in containment) |
|---|---|---|
| 5 467 135 | 659 769 | 17 707 |

| Total unknown files | Number of files with malware status | Number of files with PUA, PUP status |
|---|---|---|
| 1 166 139 | 23 935 | 5 767 |

| | |
|---|---|
| Number of unresolved malware issues | 0 unresolved |
| Number of infected systems | 0 infected |
| Number of data leaks | 0 data leaks |

# Devices with confirmed malware (virtualized files)

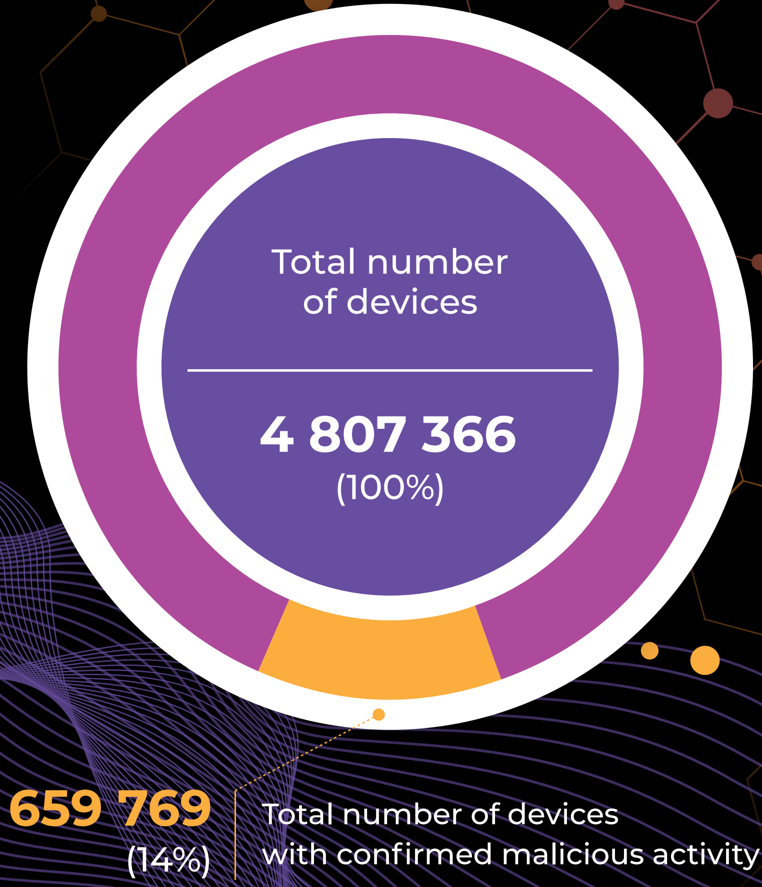
This part of the telemetry data concerns devices running unknown 0-day software, and which in the initial phase of machine analysis could have been characterized by potential malicious activity, significantly increasing the risk of an incident.

This is the first and most important stage for the security of the entire organization due to the introduction of an unknown file into one of the systems. According to the principle that 100% detection of dangerous 0-day files cannot be scientifically confirmed, Xcitium uses virtualization of access to system resources for an unknown file to isolate potentially malicious file activity from the real operating system at an early stage. As a result of this patented technology, a file is virtualized on the employee's device, then it is analyzed by machine, as well as it is analyzed manually by an employee of Xcitium Threat Lab*.

The final verdict about a file is determined by machine and human analysis. The file then becomes safe and trusted, or classified as malware or potentially unwanted software (PUP). Interestingly, 6.8% of all files were immediately classified by machine learning, while 93.2% of files were verified again by a human to minimize the occurrence of false positives.

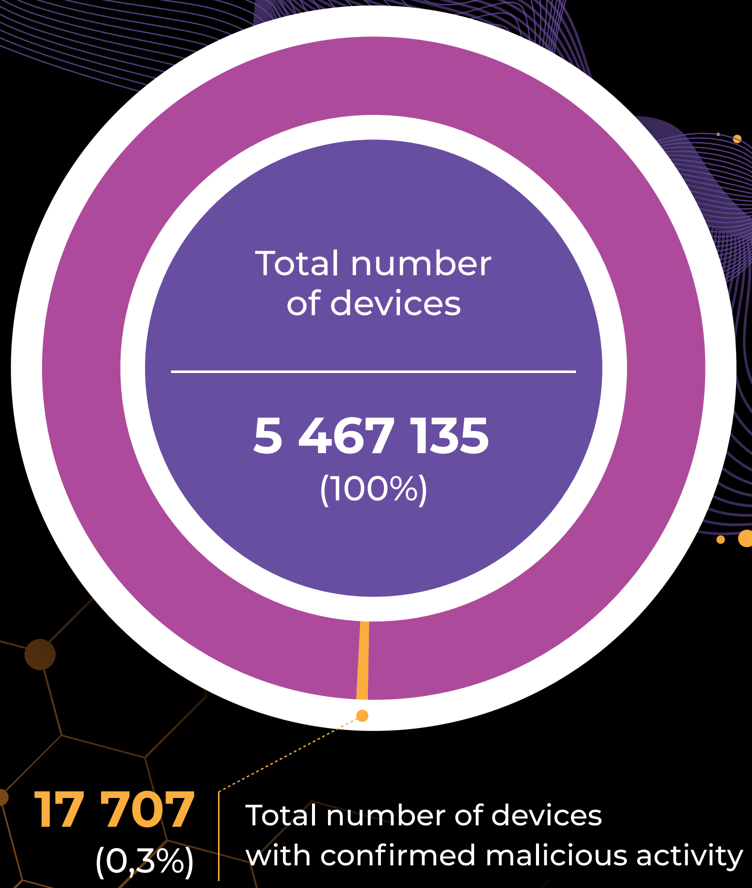
From 1 July 2024 to 30 September 2024 (the last day of the audit), the number of safe devices in relation to the number of devices with potentially suspicious activity (virtualization) is presented in the chart.

*https://enterprise.xcitium.com/what-we-do-for-detection-in-the-cloud



Number of devices without security incidents in relation to devices with 0-day files

## Devices with confirmed malware (virtualized files)



**Number of secure devices in relation to devices with malware files subjected to virtualization**

This part of the telemetry data applies to the Windows devices where the 0-day file is treated as a potential security incident in the initial phase of analysis, then there is machine and expert analysis where it finally turns out to be 100% malware or not. This process is invisible to the end user, while their workstation remains secure until a verdict is provided, as well as after the analysis is completed.

Regardless of the analysis outcome, a potentially unknown file has no way of infecting the operating system. From the perspective of the organization's security officer, this incident information is revealed in the admin console. It is possible to view detailed logs to learn more about the verdict from file analysis in Xcitium Verdict Cloud.

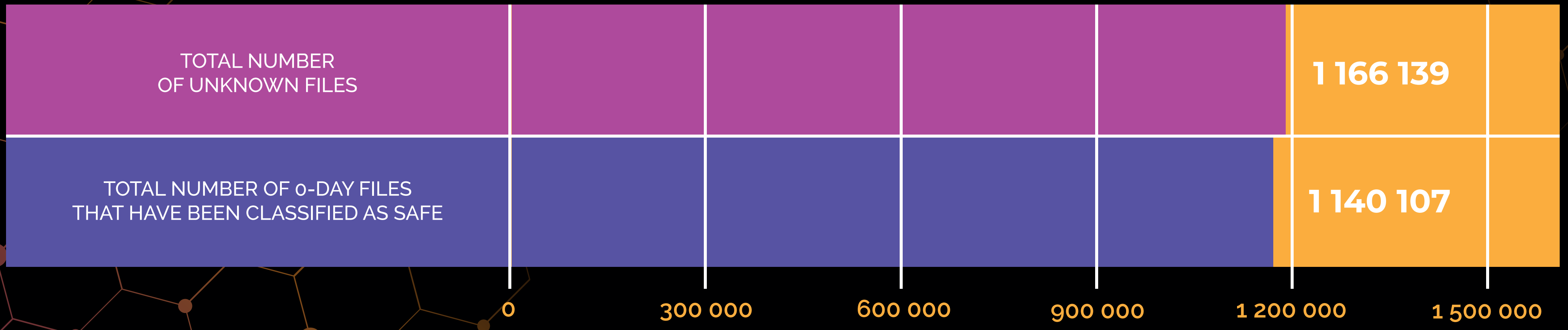
Machine analysis quickly classifies an unknown file by assigning it a status of malware if activity resembling the behavior of malware using Windows API is detected. Next, the file is analyzed by an expert from Xcitium Threat Lab, so it is subjected to double verification. This is an added value for any organization that receives additional opinion about the security provided by human.

## 0-day files classified as safe

This part of the telemetry data concerns files unknown in the initial phase of intrusion into the system which after machine and human analysis turned out to be clean and safe.

Audited data showed that on average 98% percent of unknown files turn out to be safe. The strategy that Xcitium has chosen towards the potential risk seems to be right in the end where the probability of infecting the device with malware by running an unknown file is crucial. With appropriate preventive measures, human risk is reduced to a minimum or eliminated altogether.

## Number of unknown files in relation to files classified as safe



## 0-day files classified as PUAs

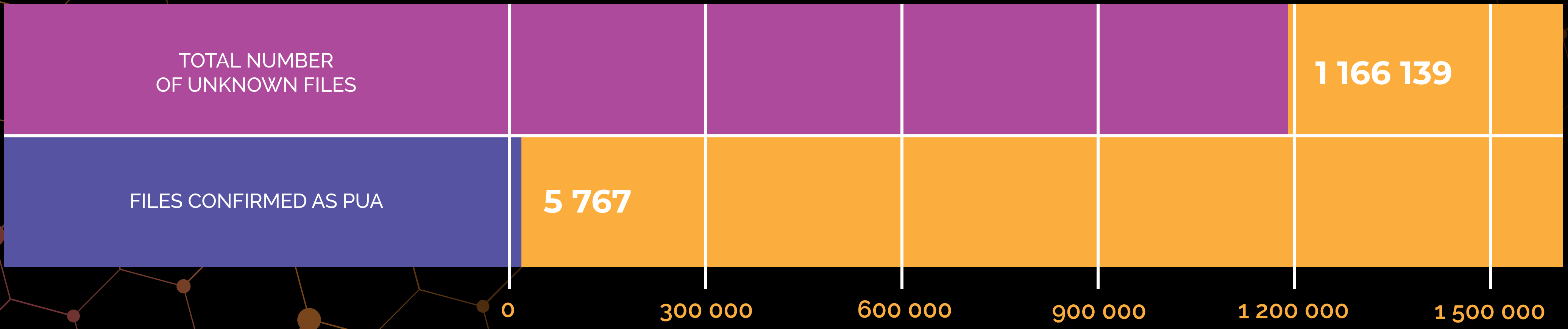
This part of telemetry data concerns initially unknown files and later classified in the developer's infrastructure as potentially unwanted software (PUAs) installed on a computer, often without explicit user consent. Such software can run in the background, collecting data, or causing other damage.

The audit has shown that PUA threats had a small share in the statistics as fake programs pretending to be antiviruses, applications supposedly cleaning the system, applications allegedly taking care of updating drivers. A large percentage of these types of applications have got advanced mechanisms that make it difficult to both detect and remove them from the system.

Thanks to the triple verification of files (static, dynamic, and human analysis), it is possible to better understand the operation of an unknown file in its initial phase, and to classify it later. PUAs usually come bundled with installers for main software, and thus users may not be aware of installing unwanted applications, potentially posing a greater risk to an organization's security.

The number of PUAs detected among unknown files is marginal, and it is only 0.4%.

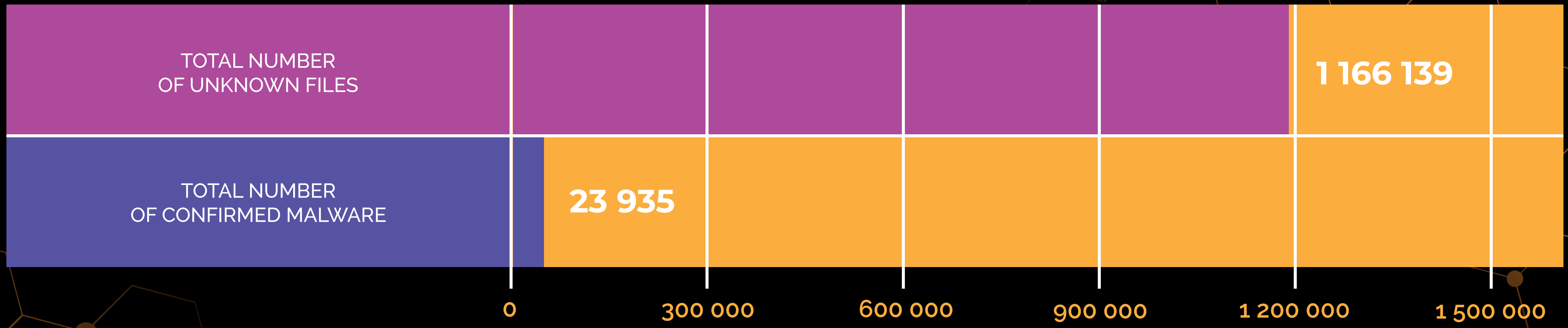
## Number of unknown files in relation to files classified as PUA



## 0-day files classified as malware

This is the last part of the telemetry data that has been checked for historical compliance with the data provided by the developer. It concerns files initially unknown, and later confirmed as malware as a result of machine analysis, and the analysis by Xcitium Threat Lab experts.

## Number of unknown files in relation to files with confirmed malware status



## TOP 8 general malware families

| | | | |
|---|---|---|---|
| 88.26% | 5.92% | 2.24% | 1.94% |
| TROJAN GENERIC | VIRUS | SPYWARE | WORM |
| 1.09% | 0.5% | 0.04% | 0.01% |
| TROJAN DOWNLOADER | TROJAN DROPPER | PUA | BACKDOOR |

It can be observed that on average 2% of unknown files turn out to be malware. Rounding up, every 50 file that was in the developer’s audited static infrastructure was classified as malware. Applying these numbers to third-party software, it can be theorized that 2% of all unknown files could be allowed to run after the first contact with antivirus software which drastically increases the risk of infecting the work environment. Please note that in fact, only one malware file is enough for a real disaster to occur for the organization to suffer financial and reputational losses.

## Potential Data Leaks and Active Infections

Initially, 0-day and later files classified as malware did not cause any harmful changes to devices with Xcitium protection installed due to the system resource access virtualization technology used.

The patented technology is designed to prevent any damage by detonating the file in a secure environment so that we do not need to rely on faulty static and partly dynamic threat detection.

Data Leaks

**0**

(0%)

Potentially infected devices

**0**

(0%)

Number of unresolved malware issues

**0**

(0%)

III

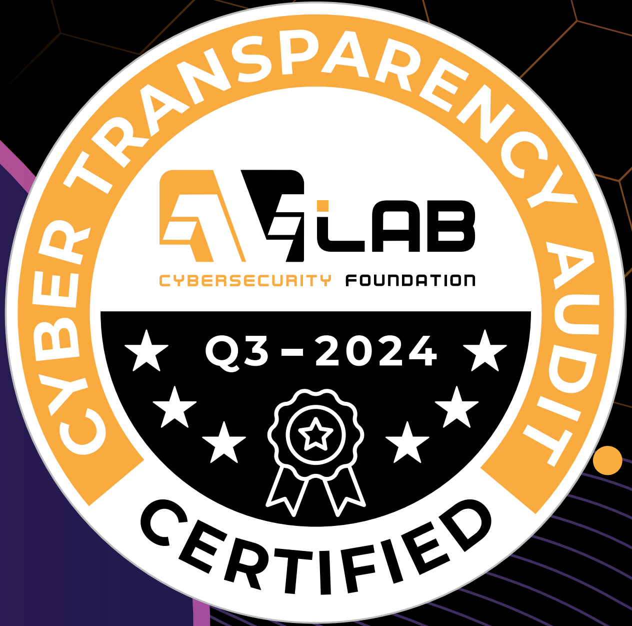
# Audit methodology in the third quarter of 2024

The testing organization plugs into the static infrastructure of the cybersecurity solution provider.
It does additional work, and obtains permission to validate the results.
It issues a certificate confirming compliance with the methodology.

## General description and requirements for joining the audit

The methodology will change as often as it is available to all who want to participate in the discussion on its development. The methodology for the audited developer in the third quarter of 2024 has been prepared in cooperation with the Cyber Transparency Forum group, and may change in the future with the participation of other developers which we will inform about in subsequent audits.

The changes are necessary because, depending on the data that can be provided to us by developers, we want to adapt the methodology to all protective solutions as best as possible in order to extract the maximum benefit from the statistics for end customers and developers.



## Requirements for Developers

The Cyber Transparency Forum invites any developer that has telemetry data from at least 100 000 (one hundred thousand) devices to participate.

The testing organization will require access to data that will match at least the recommended settings of the protection policy. They may include the so-called hardened settings. It is not allowed to audit data from devices with disabled security modules, for examples, antivirus, SSL scanning, unless it is a recommended policy.

It is allowed to participate in the audit of a device with the following settings:

1. **Recommended Policy:** These are the required settings for workstation protection to meet the minimum security measures proposed by the developer. The IT solution provider must recognize these settings in the provided static infrastructure so that the Auditor does not check data from devices with policy of key product features disabled.

2. **Hardened Policy:** Protection settings have been increased by the administrator, or have been switched on maximum security using a predefined hardened policy prepared by the developer.

The developer will create access to statistical data via API or graphic panel. Access to data should be possible in time intervals:

1. access to data from the last 1-3 hours,
2. last 24h,
3. last week,
4. last month,
5. last full quarter.

The developer agrees to publish the results online. Transparency enables a better understanding of the product's strengths, and the development of ways to detect and fix product weaknesses that may pose a high risk.

The developer must prepare the data in accordance with section "2A" below with at least the recommended telemetry data that will be part of the overall analysis performed by the Auditor.

Other requirements are listed in the rules of the Cyber Transparency Forum.

# Requirements for Auditors

Any entity that tests IT solutions,
the so-called test laboratory,
can become an auditor.

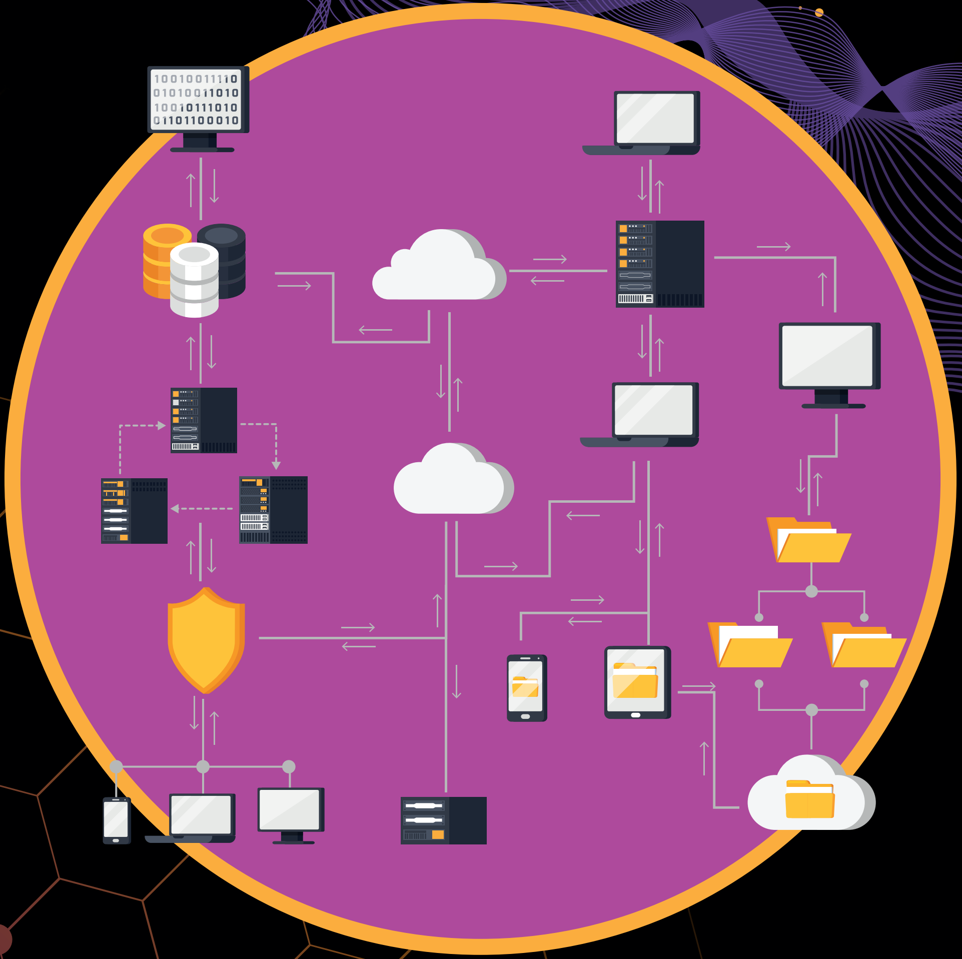
Auditor at the auditing stage will communicate with the Developer and,
if possible, will indicate errors that falsify or prevent performing a full audit.
The developer is obliged to repair them immediately,
no later than 2 weeks before the end of the audit.

Auditor may propose adding new feature
and data To the static infrastructure,
and using new data in the same
or subsequent edition of the audit.

IV

# Audit Test Components

This is general information that must be met by the Developer, and the Auditor in order to effectively validate the data.



## Minimum Requirements Data for Endpoint Security

To conduct a transparency audit, we have set ourselves the goal of validating data from at least 100 000 (one hundred thousand) end devices, regardless of the operating system. It is not required to include all devices in the statistics, as this may constitute a trade secret or may be technically difficult for the Auditor to isolate.

**Therefore, in order to properly conduct the audit, we require:**

1. Telemetry data from a minimum of 100 000 endpoints.

2. Taking into account only those endpoints that are secured by a security agent with at least a default (predefined by the Producer) or hardened (enhanced) security policy.

Developer should care about making its customers aware of the protection settings used. In specific situations, the system administrator can reduce the level of security, so we want to exclude devices with a reduced level of protection from the audit.

## File information and metadata from endpoints

We include file telemetry in the audit. The data provided by the Developer should be anonymized to not reveal confidential information.

1. The total number of unknown files that were found to be clean.
2. The total number of unknown files that turned out to be malware.
3. Total number of unknown files that turned out to be PUAs/PUPs.

Obtaining information about files and metadata will allow to better interpret the audited data, which can contribute to:

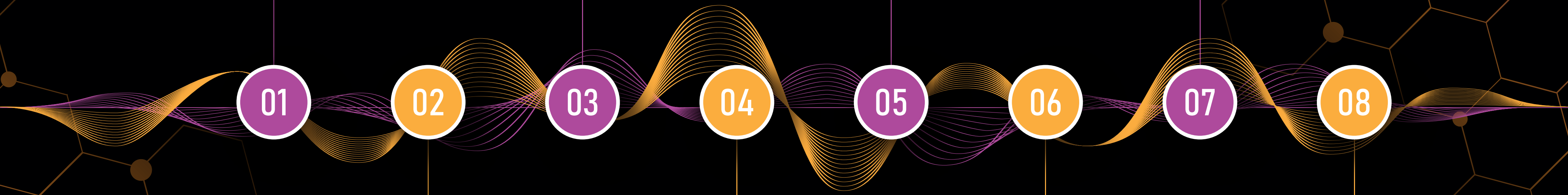
1. Search for trends over time to better understand whether a threat or cyberattack is growing or decreasing in statistics.
2. See the severity of threats over time, such as the type of malware detected or the number of malicious domains blocked.
3. Remediation so that the developer’s end customers can receive recommendations to improve their security fundamentals, such as increasing the use of SSL certificates or strengthening email security.
4. Compare data with industry averages or other sources to see how the vendor and its customers are vulnerable to, and how they deal with them.

## Required data from the Developer about devices

Endpoints secured with developer software must provide the following telemetry data to the central system to prepare for the audit:

1. Total number of devices.
2. The number of devices that contain potential malicious activity.
3. The number of devices with confirmed malicious activity.
4. The number of devices that meet security standards not infected).

# Audit Test Process – Step by step



01
A cybersecurity service provider provides an API or graphical interface with anonymized telemetry data for the testing organization.

02
The required data must have the possibility to be sorted according to a specific time schedule, for example, last hour, week, month, quarter.

03
Telemetry data should include basic information about devices and files.

04
Developer will create a process whereby testing organizations will have access to this data at any time during the audit. Data must be updated on an ongoing basis, at least once a day. The auditor can use malware sample to make sure the data is authentic.

05
Developer will provide the same set of data through the software API or proposed data format (JSON, XML, CSV, etc.), so that the testing organization can connect to the back-end of the developer's statistical infrastructure, and download this data for further analysis.

06
The time of the audit depends on the schedule agreed upon between the Developer and the Auditor. During this time, both sides cooperate, and any aspects that require clarification are urgently resolved. There may be "spot checks" or additional questions to the Developer about the data provided by the testing organization.

07
The testing organization will publish an audit report. The report will be available at the end of the reporting period.

08
Finally, the testing organization issues a certificate confirming the successful validation of the audited telemetry data.

# VI FAQ - questions & answers

## How do we collect data from a developer?

We obtain data from a developer’s static infrastructure via API or graphical interface. The scope of this data and its detail is discussed during the initial audit preparation. The auditor can verify the percentage data using malware samples which should be included in a developer’s telemetry data.

## How to obtain the data compliance certificate?

In order to obtain the transparency certificate, it is necessary to meet all data compliance requirements in the audited period. During the audit, a developer must cooperate with the Auditor, and answer all his questions.

## How long is the certificate valid and why?

The certificate is valid for one year from the date of its granting. Historical telemetry data after such a long time may differ significantly from the initial state, so further use of the certificate will require data validation to be performed again.

## Why it is worth joining?

The Cyber Transparency Forum working group brings together leading security software vendors who work together to increase transparency, and share telemetry data in the entire Internet community. Together, we create new security standards for cybersecurity software vendors.

## How to join the Cyber Transparency Audit program?

If you are a provider of security software, please contact the Cyber Transparency Forum group.
Onboarding requires meeting certain conditions, including 100 000 protected devices, and sharing telemetry data from them.

AVLAB
CYBERSECURITY FOUNDATION

# Transparency First
# Then Trust

CYBER TRANSPARENCY AUDIT OF XCITIUM BACKEND DATA

**The AVLab Cybersecurity Foundation** is an independent organization dedicated to protecting privacy and security on the Internet.
We are part of the CTF (Cyber Transparency Forum), and provide independent assessments of cybersecurity vendors' systems.
We are a member of AMTSO (Anti-Malware Testing Standards Organization) which works to improve the transparency, objectivity, and quality of testing.

We build awareness of users in the field of digital protection.
We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity. Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation, please refer to our full offer and contact us: kontakt@avlab.pl

CYBER TRANSPARENCY AUDIT
FORUM MEMBER

amtso
The cybersecurity industry's testing standard community
MEMBER

www.avlab.pl