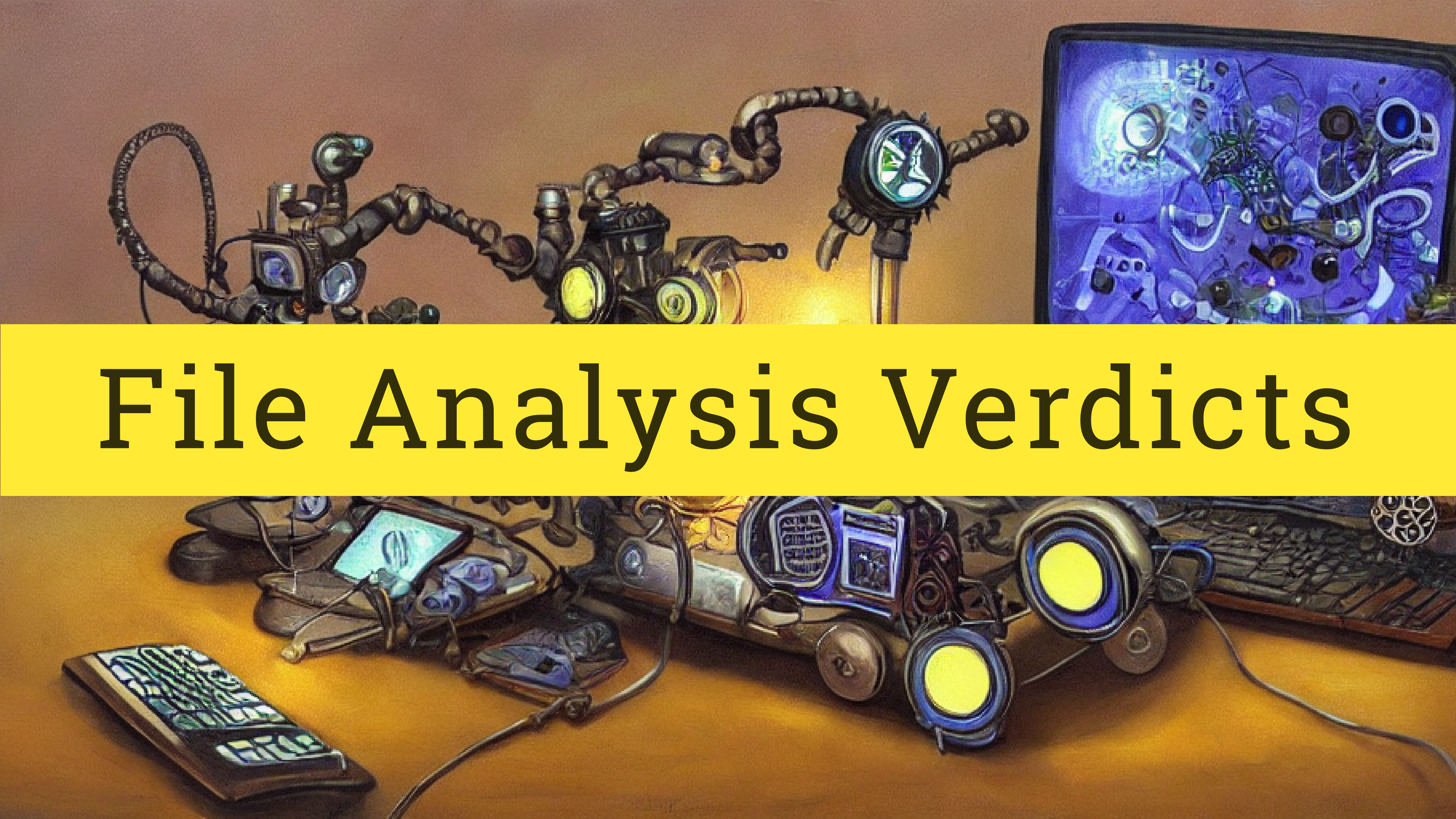

File Analysis Verdicts

Purpose of File Analysis Verdicts

SUMMARIZE ANALYSIS RESULT

- the tl;dr of the report in one word

COMMUNICATE POTENTIAL DANGER

- can the file cause harm or damage?

COMMUNICATE RELEVANCE

- should I even look into this?

CLASSIFY SAMPLES

- collect statistical data
- use for AI training
- use for security product tests

File Analysis Verdicts

MALWARE

RISKWARE

GRAYWARE

PUP

CORRUPTED OR JUNK

CLEAN

Malware

DEFINITION

Programs that are designed to cause damage or harm or unintenionally do so.

KINDS OF DAMAGE/HARM

- financial
- physical
- mental
- systemic

Malware

CONTEXT MATTERS

Whether something is malware can depend on context!

Example: Program that downloads a file and executes it.

If the downloaded file is clean, e.g., an update or a patch, then the program is also clean.

But the downloaded file is an external component that can change. If the program downloads malware at some point, it suddenly becomes malware too.

Malware

WHY THIS VERDICT

The malware verdict communicates that the sample is dangerous and undoubtedly has to be detected by antivirus software.

PUP - Potentially Unwanted Program

DEFINITION

Non-malicious, legal programs that are **usually** not wanted by the user.

They often use **psychological tactics** to manipulate users into accepting or paying for the installation.

PUP - Potentially Unwanted Program

TYPICAL SYMPTOMS

- suddenly new advertisments, pop-ups
- changed browser settings: default page, search settings, toolbars, changes can be hard to remove
- newly installed programs, unknown to user

USELESS PROGRAMS

- user was tricked into payment of a useless program
- often via exaggerated warnings, problems with a promise to repair

PUP - Potentially Unwanted Program

REMARKS

- illegal programs are never PUP but grayware or malware
- malware may show same symptoms, but usually arrives without consent whereas PUP tricks into consent

PUP - Potentially Unwanted Program

WHY THIS VERDICT

Some people love their PUP software and want to keep using it.

For other people it is akin to an infection.

PUP is the best verdict to describe that a program is legal but still annoying.

Riskware

DEFINITION

Programs that pose a serious security risk or indicate a compromised system or network.

Riskware

EXAMPLES

- password recovery or credential dumping tools
- vulnerable drivers
- so called "hacking tools" used by attackers to invade systems or move in the network

Riskware

WHY THIS VERDICT

Presence of riskware on company systems may indicate a serious compromise. The underlying issue can be more severe than the presence of "just" one malware.

Sometimes administrators use riskware to test and secure their systems, so whether the presence of these programs is a problem depends on **who** used these tools and **why**

Corrupted or Junk

DEFINITION CORRUPTED

Programs that are damaged to a point that they do not execute.

Documents that are damaged so that they cannot be opened anymore.

DEFINITION JUNK

Files that serve no purpose. For example empty files, zero filled files or files filled with data that cannot be determined and seems random.

Corrupted or Junk

REMARKS

Junk and corrupted cannot always be clearly distinguished nor does it make sense to do so.

Junk files may actually serve a purpose in context but for the analyst this context is not known and cannot be determined.

Caution: If a program executes and then exits with an error message, it is **not** corrupted. It still runs.

Corrupted or Junk

WHY THIS VERDICT

With corrupted files there is often missing information to create a verdict of their original state because the files cannot be viewed or executed.

At the same time the verdict of their original state is not that important because they cannot be run anyways.

The verdict communicates that the sample is irrelevant.

Grayware

DEFINITION

Samples that are not malicious but **illegal** or for other reasons **not okay** to be used.

Grayware

WHY THIS VERDICT

Clean carries the association that a file is perfectly fine to be used and not associated with anything shady, illegal or phishy.

So in communication with others it should be made clear when this is not the case even though a file is "technically" clean.

Furthermore, it is optional for certain samples that they are quarantined by antivirus software. Such samples may also get the verdict grayware.

Grayware

EXAMPLES

- software cracks, keygens
- child abuse material
- ransom notes

Clean

DEFINITION

The clean verdict is given by **exclusion of all other verdicts.**

Clean samples are:

- legal
- free of serious security risks
- do not use shady tactics for installation
- somewhat useful / no junk

Clean

WHY THIS VERDICT

In colloquial terms his verdict is given whenever it is *okay to use this program or file*.

There are no doubts and no considerable security risks involved.

A clean verdict communicates that nothing else needs to be done.