CTM360®

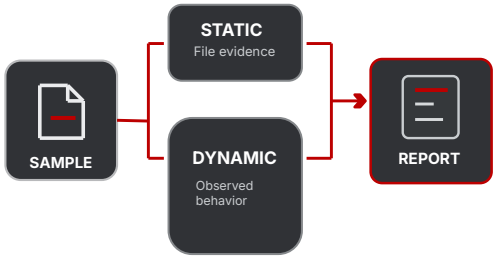
Platform Brief

MALCAGE

FILE SANDBOXING & MALWARE ANALYSIS

One file. One structured report.

Analyze suspicious files in a controlled environment. Bring file properties, runtime behavior, network activity and detection findings together in one place.



KEY CAPABILITIES

Static + Dynamic Analysis

Inspect file characteristics alongside execution behavior, system activity and network communications.

Configurable Analysis Environment

Select an operating system, observation depth and network access for the sample.

Consolidated Technical Evidence

Extract URLs, domains, IP addresses, emails, scripts, certificates, metadata and embedded resources.

Investigation Actions

Review detections and ATT&CK mappings, generate YARA, export findings or rescan a sample.

HOW MALCAGE WORKS

01
UPLOAD
Submit a supported suspicious file.

02
CONFIGURE
Choose execution, depth and network settings.

03
ANALYZE
Run static and dynamic analysis in the sandbox.

04
REVIEW & ACT
Examine the report and take follow-up actions.

CONTINUE THE INVESTIGATION

GENERATE YARA
Create a detection rule from identified characteristics and indicators to help find related samples.

DOWNLOAD PDF
Export the complete analysis report for team sharing, investigation records and evidence.

RESCAN
Run the same sample through a new analysis when a fresh examination is needed.

CTM360®

Platform Brief

THE MALCAGE ANALYSIS REPORT

BUILT FOR Malware triage / Incident investigation / Threat intelligence research

WHY MALCAGE

Reduce tool-switching by bringing technical evidence together in one structured analysis report.

One analysis workspace

Submit, observe and investigate suspicious samples from a centralized environment.

Connected technical context

View file, behavior, network, detection and AI-assisted observations together.

Evidence for the next step

Use structured findings for triage, response and threat intelligence investigations.

Investigation-ready outputs

Generate YARA rules, export a PDF report or rescan the same sample.

01 OVERVIEW
02 TIMELINE
03 FINDINGS
04 BEHAVIOR
05 NETWORK



TEN VIEWS.
ONE INVESTIGATION.

06 DROPPED FILES
07 ATT&CK
08 STATIC ANALYSIS
09 DETECTION
10 AI ANALYSIS

About Us

CTM360 is an external security platform that seamlessly integrates External Attack Surface Management, Digital Risk Protection, Third Party Risk Management, Cyber Threat Intelligence, Takedowns, and more. For any queries or assistance please contact us at **info@ctm360.com**.