Malware analysis & RE

Take a suspicious file to shared intelligence without leaving the kit

RHOMBUS SECURITY

Rhombus deploys a malware lab with a Linux reverse engineering (RE) workstation and an automated triage engine fed by files carved from traffic. Intake, verdict and intelligence all run on the kit, with no cloud service in the path.

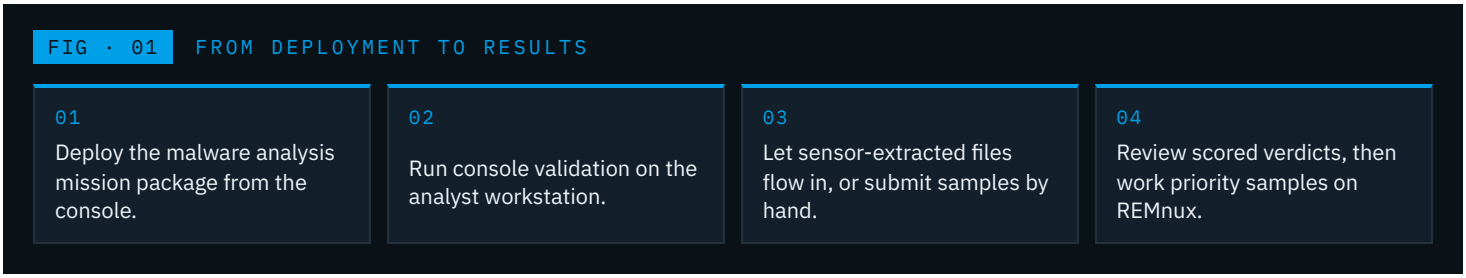
01 · WHY IT MATTERS

- Teams in the field cannot send suspect files to an internet sandbox, and often must not.
- Automated triage tells an analyst which of hundreds of files deserve hand analysis first.
- A verdict that becomes a sensor detection closes the loop between analysis and defense.

02 · HOW IT WORKS ON RHOMBUS

- REMnux deploys on a separate malware segment, reached through a browser-based analyst workspace.
- Carved files move through a governed file pipeline; the malware segment sees them read-only.
- The chosen engine, open-source Assemblyline or licensed Spectra Analyze, scores each file using antivirus and YARA content from the kit's offline mirror.
- Malicious verdicts post to team chat, become Malware Information Sharing Platform (MISP) events and return to Assemblyline as known-bad hashes.

FIG · 01 FROM DEPLOYMENT TO RESULTS



03 · DEFENSE & GOVERNMENT

- Defensive cyber operations (DCO) triage of files carved from mission network traffic.
- Incident response on a disconnected network where samples cannot leave the enclave.
- Reverse engineering training against a lab sample corpus.

04 · COMMERCIAL & ENTERPRISE

- Enterprise incident response teams that must keep suspect files inside their own boundary.
- Banks that need to triage phishing attachments without third-party upload.
- Critical infrastructure sites analyzing files where outside connectivity is restricted.

05 · OUTCOMES

- Files carved by sensors with file extraction are scored automatically, with no internet connection.
- Malicious files land in a dedicated quarantine tree, named by hash, with their verdict alongside.
- The kit's own verdicts become indicators its sensors and triage engine act on.

06 · CONSIDERATIONS

- Each kit chooses its engine — Spectra Analyze is optional and licensed separately; Assemblyline needs no license.
- Assemblyline needs a large data disk and substantial memory.
- The lab has no automated sandbox; dynamic analysis is manual.
- Automatic intake needs a sensor that extracts files, such as the optional MixMode sensors.

INTEGRATED TOOLS

Assemblyline | REMnux | YARA | ReversingLabs Spectra Analyze COMMERCIAL

Commercial products licensed separately · Trademarks of their owners; no endorsement implied