MalwareLab.ai

Quick Start Guide

AI Investigation Assistant for Information Technology Professionals

Getting Started

MalwareLab.ai helps Information Technology and security professionals analyze suspicious evidence, build investigative context, and produce structured findings using one consistent workflow.

Step	Action	Description
1	**Launch**	Sign in and select **Launch Analyzer**.
2	**Submit Evidence**	Upload a binary, PowerShell script, CSV/logs, paste IOCs, or describe suspicious behavior.
3	**Review Findings**	Review severity, confidence, IOCs, MITRE ATT&CK; mappings when applicable, and recommended actions.
4	**Build Context**	Add evidence or ask follow-up questions to refine the investigation.
5	**Document**	Copy or export results into incident documentation or ticketing.

Supported Evidence

- Binary executables (static analysis)
- PowerShell scripts
- CSV datasets and security logs
- IP addresses, domains, URLs, and file hashes
- Plain-English descriptions of suspicious activity

Best Practices

Provide as much context as possible. Use MalwareLab.ai as an investigation assistant alongside your existing workflow and professional judgment. Validate important findings using your organization's established procedures.