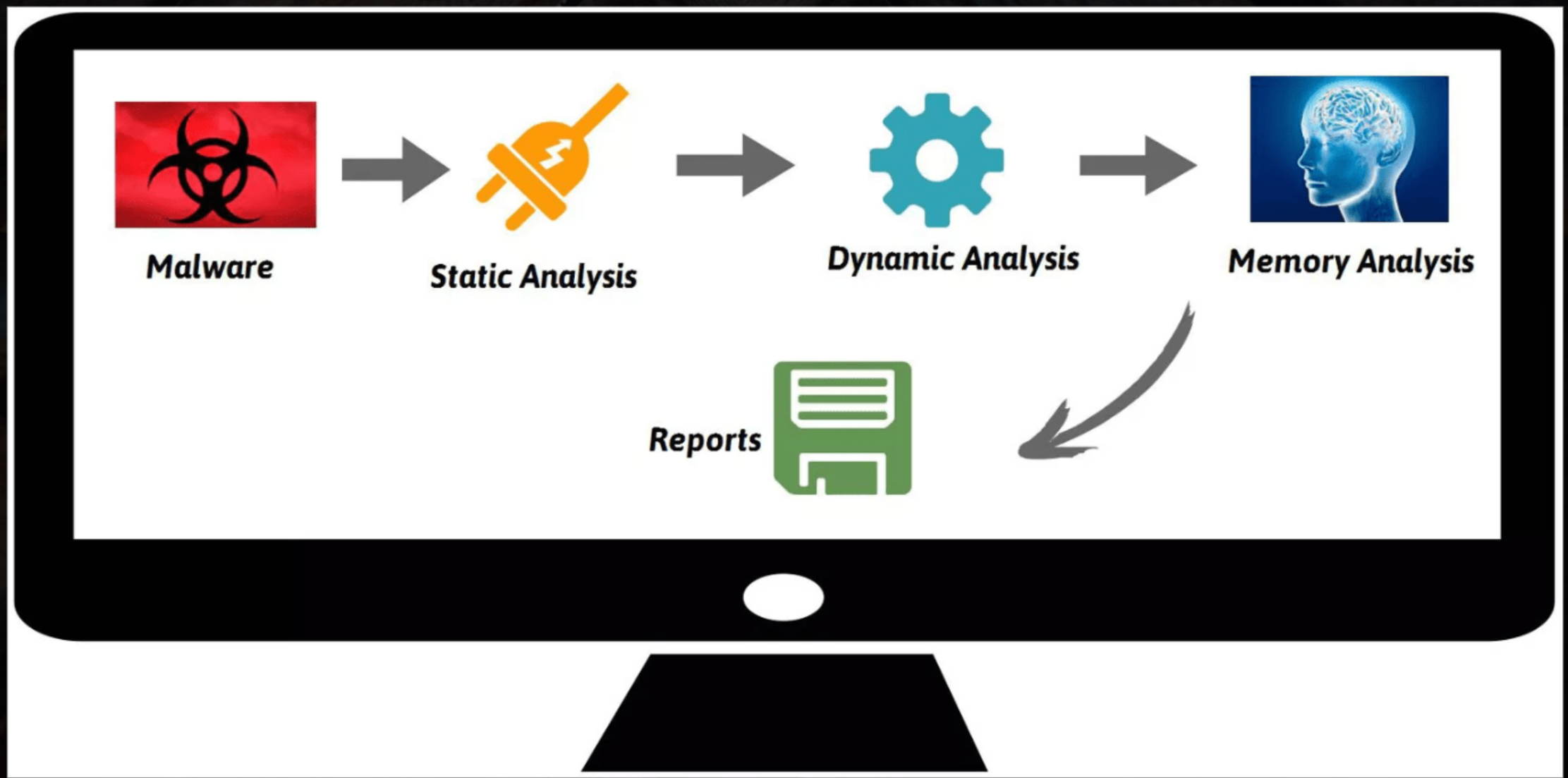
Automating Malware Analysis (Sandbox Analysis)

Sandbox Overview

- Executes malware in a controlled/monitored environment
- Monitors file system, registry, process and network activity
- Outputs the results in text format

Working of sandbox



General Features

- Can run in sandbox mode (does not allow to connect to c2). Simulates all services (like DNS, HTTP, and other protocols)
- Can run in internet mode (connects to c2
- Option to run malware for a specified time (default is 60 seconds)
- Captures desktop screenshot
- Reports on the malware behavior

Video Demo 7

Sandbox Analysis of Spyeye