TECHNICAL BRIEF

Swarm Hunter

Review reports and activity records in one case workspace.

In development · local review build 0.6.0
Brief revision 1.0 | October 3, 2026

Swarm Hunter helps an analyst organise supplied activity records and public report leads, review related events, and save an assessment. Its findings are advisory: a person must review the evidence, its source and what may be missing.

What it does

Start a target case, import a log or browse a labeled test scenario. Keep the source of each record visible throughout the investigation.

How the reviewed workflow works

- Choose a case and evidence source. Incoming activity requires a source you explicitly make available; Hunter does not discover hidden traffic or scan an unknown target.
- Review records, findings and coverage limits. Inspect related events in a 2D or 3D map and step through time replay. Map positions are conceptual, not physical locations.
- Add an assessment, save the case or export it for review. The tested exports retain source labels, settings, notes, record identifiers and original input.

Supported evidence in this build

Imported records	Supported structured event logs. JSONL means one JSON record per line; JSON is a common structured text format.
Incoming activity	An explicitly selected local JSONL source. Event time, collection time, delays and reported coverage are kept distinct.
Reported leads	Public reports and bounded public metadata, including the reviewed URLhaus source. Metadata describes a report; malware payloads are not fetched.
Test scenarios	15 labeled datasets: 11 synthetic, three report reconstructions and one historical public metadata sample with 60 records.

What the warnings mean

Narrow advisory rules flag recorded denied relays, restricted handoff/export contradictions and a qualified sequence of denied logins. Connections or shared resources alone do not prove hostile coordination. Source claims do not authenticate an AI agent or establish harmful intent.

TECHNICAL BRIEF

Swarm Hunter / Technical brief

In development · local review build 0.6.0
Brief revision 1.0 | October 3, 2026

Setup and information use

Use only records you are permitted to review. Keep prompts, credentials, payloads and unrelated personal content out of the incoming metadata format.

Reviewed setup

Portable workspace	Asupplied HTML file supports local import, inspection, maps and export without a launcher session.
Local launcher	The supplied Windows PowerShell launcher requires Python 3.10 or newer with SQLite, a local database. It serves the app at an address on the same computer.
Source connection	Incoming collection and Pattern Review require the browser session created when the launcher is first used. Only a source path selected at launch can be observed.
Platform limits	Desktop browser workflows were checked. Awider list of supported operating systems and browsers, minimum hardware and throughput guarantees are not established.

Storage, exports and external requests

Native browser cases use browser storage where available. The local service uses SQLite for retained cases and evidence. Storage belongs to the selected browser, address and data folder; changing them does not automatically move saved cases.

External cases can retain raw records, source history, warnings, coverage gaps and reviewer notes. Exports can contain original input and should be treated as sensitive case files. Local storage is not a guarantee of encryption or independent evidence authenticity.

Pattern Review lets a person compare repeated action sequences across supplied logs. Its comparison workspace lasts only for the launcher session; export its review record before closing it. A match is a lead to review, not proof of a threat.

A public report connector may make bounded requests to its configured public source. Selecting a source reference in an imported record does not fetch that reference. Offline imports do not establish complete visibility of external activity.

Control boundary

The investigation workspace does not execute imported commands or automatically block agents. Optional developer controls affect fixed local test tools only. They are not general computer protection or a working Agent Defender integration.

TECHNICAL BRIEF

Swarm Hunter / Technical brief

In development · local review build 0.6.0
Brief revision 1.0 | October 3, 2026

Evidence, limits and next steps

The review checks the supplied application and controlled examples. It does not measure accuracy at detecting threats in real use.

What has been checked

Recorded checks cover the event and graph models, advisory transitions, labeled dataset loading, source classification, settings of saved cases and export consistency. Desktop browser reviews cover case selection, maps, replay, notes, save/reopen/export and manual pattern comparison.

The 15 test datasets include invented scenarios and reconstructed incidents with invented timing and roles. The historical public sample contains real revision metadata; its public handles are not authenticated AI agents. These examples do not provide a estimate of accuracy in real use.

What remains unverified

- Detection of unknown targets, live customer/provider connections and rates of false alarms or missed threats in real use remain unvalidated.
- The final mobile pixel appearance and physical speaker output were not verified. Responsive layout and checks of audio controls do not substitute for those observations.
- Record hashes check internal consistency, not authorship. Missing records, inaccurate timestamps or false source claims can limit an assessment.
- There is no security certification, production hosting claim or automatic agent blocking. Swarm Hunter and Agent Defender remain separate products.

Before evaluating it with your team

- Start with a labeled test scenario, then a permitted sample log. Check its format, source identity, missing intervals and event times.
- Review every warning against the supporting records and possible ordinary explanations. Save and reopen a case, then check the exported original input and source labels.
- Agree on access, retention and secure sharing of case files. Confirm the exact build, required platform and source connection before broader use.

Review basis: Swarm Hunter 0.6.0 workspace guide, security boundary, evidence contract and review records available October 3, 2026.
Public details: Read the technical details online
Typography updated October 4, 2026. Product evidence and review date unchanged.