CLAIMS

1. A method for semantic behavior chain reconstruction and AI-driven security investigation, including the following steps:

step S11: collecting log data from multiple security devices or systems, performing field standardization for the purpose of unified behavior subject modeling;

step S12: constructing a behavior chain structure associated with an entity, and the behavior chain structure is a time series, graph structure, tag chain structure, or equivalent path structure;

step S13: receiving a user-input natural language security investigation question;

step S14: mapping the natural language question to a query target related to the behavior chain structure using an artificial intelligence engine;

step S15: performing semantic reasoning, path search, or context analysis operations on the query target based on the behavior chain structure;

step S16: outputting a structured or unstructured query result, including path diagrams, node lists, behavior segments, risk prompts, expert feedback information, or suggestive results.

2. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 1, wherein in step S11, the log data undergoes field standardization, entity unification, platform alignment, and identifier aggregation during the collection process, achieving cross-platform and cross-system log behavior chain integration.

3. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 2, wherein in step S12, the behavior chain structure is established based on log chronological order, operational association, tag linkage, causal dependency, or knowledge graph paths, supporting graphical display and real-time or persistent storage of behavior nodes; the behavior chain structure embeds enhancement information including node risk scores, structural path weights, behavior intent tags, anomaly confidence levels; transition point identifiers: the transition point identifiers are used to mark key nodes indicating changes in attack phases within the behavior chain; behavior coordinates: the behavior coordinates record the phase position, role attribution, and temporal sequence of each behavior within the chain path; phase transition intensity scores: the phase transition intensity scores are used to measure the credibility of transitions between nodes, comprehensively considering temporal continuity, role consistency, and behavior pattern deviation; the enhancement information is used to optimize the artificial intelligence model's path ranking, anomaly identification, and phase transition reasoning capabilities.

4. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 3, wherein in step S12, the behavior chain structure is either a pre-constructed structure or a dynamically aggregated collection of event segments formed during a query process based on user-specified entity identifiers, time ranges, or behavior characteristic conditions; the collection of event segments has relevance or logical sequence at the semantic level; the behavior chain structure serves as the foundation for triggering a structured event investigation process, including behavior chain reconstruction for specific IPs or users, comparison of similar attack paths, behavior attribution, and collaborative analysis tasks; behavior chain node composition includes communication actions, login behaviors, file operations, configuration changes, process invocations, URL accesses, API requests, or other identifiable security behavior events.

5. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 4, wherein in step S14, the artificial intelligence engine comprises a

large language model, NLP, a graph neural network, a rule-learning hybrid engine or an equivalent semantic reasoning system; the artificial intelligence engine converts the natural language question into a structured query template, graph structure traversal request, or SQL statement, and combines Prompt engineering to achieve efficient mapping between natural language and structured queries, supporting the semantic reasoning process.

6. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 5, wherein the user continuously asks questions in natural language, and the artificial intelligence maintains a semantic session based on the behavior chain context state, supporting context zooming, chain structure focus switching, reverse question generation, and interactive behavior path evolution, and supporting cross-turn context memory and expert feedback-driven dialogue evolution capabilities.

7. The method for semantic behavior chain reconstruction and AI-driven security investigation of claim 6, wherein in step S16, the output result includes attack path diagrams, structural node lists, behavior trajectories within a time window, matching segments, risk explanations, reasoning failure prompts, or semi-structured results requiring manual confirmation.

8. A system for semantic behavior chain reconstruction and AI-driven security investigation, comprising: a field normalization module, a behavior chain modeling module, an AI semantic reasoning module, a micro-model scoring module, and an expert feedback and knowledge write-back module; the field normalization module, behavior chain modeling module, AI semantic reasoning module, micro-model scoring module, and expert feedback and knowledge write-back module form a logical feedback loop, supporting the behavior chain construction, attack path reconstruction, and artificial intelligence semantic analysis process;

the field normalization module performs field standardization, entity normalization, platform

alignment, and key field mapping on collected multi-source log data;

the behavior chain modeling module constructs a behavior chain structure based on chronological order, semantic consistency, and role consistency, serving as the input foundation for AI reasoning and path reconstruction;

the AI semantic reasoning module performs path reasoning, phase transition identification, and risk assessment on the behavior chain, supporting natural language interface invocation;

the micro-model scoring module performs multi-dimensional model scoring on standardized log fields, generating threat scoring fields to support behavior chain modeling and AI reasoning;

the expert feedback and knowledge write-back module feeds back behavior chains and phase tags confirmed by human experts to a knowledge base, forming a sustainably evolving AI knowledge memory layer.

9. The system for semantic behavior chain reconstruction and AI-driven security investigation of claim 8, wherein in the micro-model scoring module, the log data processing and scoring analysis method performs external analysis processing on structured log fields and uniformly writes them to a database, including the following steps:

step S21: log preprocessing: upon receiving raw log data, utilizing local script programs, applications, or equivalent modules to perform field extraction, data cleaning, and standardization operations;

step S22: interface invocation: sending the preprocessed log fields in a structured format via an API interface to one or more external analysis services;

step S23: service processing: the external analysis services includes micro-model services, scoring engines, feature extractors, tag classifiers, or rule-based evaluators, used to perform processing operations such as behavior evaluation, threat scoring, field statistics, and context parsing;

step S24: result reception and encapsulation: uniformly receiving structured results returned by the analysis services and performing encapsulation processing;

step S25: database writing: writing the processed result data to predefined fields in the database for use in behavior chain modeling, attack phase identification, visual presentation, or knowledge base updates.

10. The system for semantic behavior chain reconstruction and AI-driven security investigation of claim 8, wherein in the field normalization module, processing security logs based on a ternary field mapping includes the following steps:

step S31: collecting log data from security devices and extracting raw fields srcip and dstip;

step S32: constructing a ternary structure external_ip→srcip→dstip, wherein when the log source is a border device directly accessible from the public network, mapping the original srcip to external_ip, mapping the original dstip to a logical srcip, and retaining the original srcip field content without using it for behavior chain modeling.

11. The system for semantic behavior chain reconstruction and AI-driven security investigation of claim 8, wherein the expert feedback and knowledge write-back module comprises a structured behavior chain knowledge base; the structured behavior chain knowledge base writes verified attack behavior chains and their associated information into

the knowledge base, and performs automatic semantic judgment and behavior chain similarity retrieval based on the knowledge base;

in the expert feedback and knowledge write-back module, the expert determines a security event through an AI-driven investigation process and feeds back knowledge, manually triggers a comparison process to compare the current behavior chain under investigation with historical behavior chains stored in the knowledge base for similarity, assisting in judging as a similar attack path or phase transition risk; the comparison process operates independently of the AI automatic reasoning process;

the knowledge base comprises a behavior chain reproduction library, a field semantic parsing library, a risk tag and intent library, a graph relationship database, a path semantic coordinate library, and other optimization information knowledge bases; the path semantic coordinate library stores the structural position, phase tag, behavior coordinates, transition point identifier, and transition intensity score of each node in the behavior chain;

the structured behavior chain knowledge base utilizes structural vectors, semantic tags, or graph structure overlap for similarity matching, performs high-confidence attack path comparison and phase transition reasoning based on historical behavior chains, and uses the matching results as input to the artificial intelligence model or as auxiliary reference for security analysts;

the structured behavior chain knowledge base and the artificial intelligence model form a closed-loop interaction mechanism; during the training, update, and inference stages of the artificial intelligence model, the artificial intelligence model dynamically depends on structured behavior chain data, path semantic coordinates, transition point identifiers, and phase transition intensity scoring information within the knowledge base.