权 利 要 求 书

1、一种语义行为链重构与 AI 引导的安全调查方法，其特征在于，包括以下步骤：

步骤 S11：采集来自多个安全设备或系统的日志数据，以统一行为主体建模为目的字段标准化；

步骤 S12：构建与实体相关联的行为链结构，所述行为链结构为时间序列、图结构、标签链式结构或其等效路径结构；

步骤 S13：接收用户输入的自然语言安全调查问题；

步骤 S14：利用人工智能引擎将自然语言问题映射至与行为链结构相关的查询目标；

步骤 S15：基于行为链结构对查询目标执行语义推理、路径搜索或上下文分析操作；

步骤 S16：输出结构化或非结构化的查询结果，包括路径图、节点列表、行为片段、风险提示、专家反馈信息或提示式结果。

2、根据权利要求 1 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：在步骤 S11 中，所述日志数据在采集过程中进行字段标准化、实体统一、平台对齐、标识聚合，进行跨平台、跨系统日志行为链整合。

3、根据权利要求 2 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：在步骤 S12 中，所述行为链结构基于日志时间顺序、操作关联、标签联动、因果依赖或知识图谱路径建立，支持行为节点的图形化展现与实时或持久化存储；所述行为链结构嵌入增强信息包括节点风险评分、结构路径权重、行为意图标签、异常置信度；跃迁点标识，所述跃迁点标识用于标记行为链中攻击阶段变化的关键节点；行为坐标，所述行为坐标记录每一行为在链路径中的阶段位置、角色归属、时间位次；阶段跃迁强度评分，所述阶段跃迁强度评分用于度量节点间跃迁的可信度，综合考虑时间连续性、角色一致性与行为模式偏移度；所述增强信息用于优化人工智能模型的路径排序、异常识别与阶段跃迁推理能力。

4、根据权利要求 3 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：在步骤 S12 中，所述行为链结构为预先构建的结构或在查询过程中基于用户指定的实体标识、时间范围或行为特征条件所动态聚合形成的事件片段集合；所述事件片段集合在语义层面具有关联性或逻辑顺序；所述行为链结构作为构建基础，触发结构化事件调查流程，包括特定 IP 或用户的行为链重建、相似攻击路径比对、行为归因、协同分析任务；行为链节点构成包括通信动作、登录行为、文件操作、配置变更、进程调用、URL 访问、API 请求或其它可识别的安全行为事件。

5、根据权利要求 4 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：在步骤 S14 中，所述人工智能引擎包括大语言模型、NLP，图神经网络、规则-学习混合引擎或其等效语义推理系统；所述人工智能引擎将自然语言问题转化为结构化查询模板、图结构遍历请求或 SQL 语句，并结合 Prompt 工程进行自然语言与结构化查询的高效映射，支撑语义推理过程。

6、根据权利要求 5 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：用户以自然语言方式进行连续提问，人工智能基于行为链上下文状态维持语义会话，支持上下文缩放、链结构焦点切

换、逆向提问生成与交互式行为路径演化，并支持跨轮次上下文记忆与专家反馈驱动的对话演化能力。

7、根据权利要求 6 所述的一种语义行为链重构与 AI 引导的安全调查方法，其特征在于：在步骤 S16 中，输出结果包括攻击路径图、结构节点列表、时间窗口内行为轨迹、匹配片段、风险说明、推理失败提示或需人工确认的半结构结果。

8、一种语义行为链重构与 AI 引导的安全调查系统，其特征在于：包括字段归一化模块、行为链建模模块、AI 语义推理模块、微模型评分模块以及专家反馈与知识回写模块；所述字段归一化模块、行为链建模模块、AI 语义推理模块、微模型评分模块以及专家反馈与知识回写模块构成逻辑反馈闭环，支撑行为链构建、攻击路径重构与人工智能语义分析过程；

所述字段归一化模块对采集的多源日志数据进行字段标准化、实体归一化、平台对齐与关键字段映射；

所述行为链建模模块基于时间顺序、语义一致性与角色一致性构建行为链结构，作为 AI 推理与路径重建的输入基础；

所述 AI 语义推理模块对行为链进行路径推理、阶段跃迁识别与风险评估，支持自然语言接口调用；

所述微模型评分模块对标准化日志字段执行多维度模型评分，生成威胁评分字段，支撑行为链建模与 AI 推理；

所述专家反馈与知识回写模块将经人工专家确认的行为链与阶段标签反馈至知识库，形成可持续演进的 AI 知识记忆层。

9、根据权利要求 8 所述的一种语义行为链重构与 AI 引导的安全调查系统，其特征在于：在微模型评分模块中，日志数据处理与评分分析方法对结构化日志字段进行外部分析处理并统一写入数据库，包括以下步骤：

步骤 S21：日志预处理，接收原始日志数据后，利用本地脚本程序、应用程序或等效模块执行字段提取、数据清洗及标准化操作；

步骤 S22：接口调用，将预处理后的日志字段以结构化格式通过 API 接口发送至一个或多个外部分析服务；

步骤 S23：服务处理，外部分析服务包括微观模型服务、评分引擎、特征提取器、标签分类器或基于规则的评估器，用于执行行为评估、威胁打分、字段统计、上下文解析的处理操作；

步骤 S24：结果接收与封装，统一接收分析服务返回的结构化结果并进行封装处理；

步骤 S25： 数据库写入，将处理后的结果数据写入至数据库的预定义字段，供行为链建模、攻击阶段识别、可视化呈现或知识库更新使用。

10、根据权利要求 8 所述的一种语义行为链重构与 AI 引导的安全调查系统，其特征在于：在字段归一化模块中，基于三元字段映射对安全日志进行处理，包括以下步骤：

步骤 S31：采集来自安全设备的日志数据，提取原始字段 srcip 与 dstip；

步骤 S32：构建 external_ip → srcip → dstip 的三元结构，当日志来源为可直接接收公网访问的边界设备时，将原始 srcip 映射为 external_ip，将原始 dstip 映射为逻辑 srcip，并保留原始 srcip 字段内容不用于行为链建模。

11、根据权利要求 8 所述的一种语义行为链重构与 AI 引导的安全调查系统，其特征在于：所述专家反馈与知识回写模块包括结构化行为链知识库，所述结构化行为链知识库将已验证的攻击行为链及其关联信息写入知识库，并基于知识库的自动语义判断与行为链相似性检索；

所述专家反馈与知识回写模块中，专家通过人工智能辅助调查流程对安全事件进行判定并反馈知识，手动触发比对流程，将当前待排查的行为链与知识库中已存的历史行为链进行相似性比对，辅助判断为相似攻击路径或阶段跃迁风险，所述比对流程独立于 AI 自动推理流程运行；

所述知识库包括行为链复现库、字段语义解析库、风险标签与意图库、图谱关系数据库、路径语义坐标库及其他优化信息知识库；所述路径语义坐标库存储行为链中各节点的结构位次、阶段标签、行为坐标、跃迁点标识与跃迁强度评分；

所述结构化行为链知识库利用结构向量、语义标签或图结构重叠度进行相似性匹配，基于历史行为链进行高置信度攻击路径比对与阶段跃迁推理，匹配结果作为人工智能模型输入或安全分析师辅助参考；

所述结构化行为链知识库与人工智能模型形成闭环交互机制，在人工智能模型的训练阶段、更新阶段及推理阶段，所述人工智能模型动态依赖知识库中的结构化行为链数据、路径语义坐标、跃迁点标识与阶段跃迁强度评分信息。