说 明 书

一种语义行为链重构与 AI 引导的安全调查方法与系统

技术领域

本发明涉及网络安全与人工智能交叉领域，尤其涉及一种语义行为链重构与 AI 引导的安全调查方法与系统。

背景技术

现有的安全运营平台主要依赖 SIEM 系统进行日志汇总与事件分析 其核心模式通常基于固定规则匹配单条日志以生成告警 在实际调查过程中，分析人员需手动编写查询语句 从多源日志中定位关键信息并人工拼接行为链以推断威胁路径 此方法存在语法门槛高 日志割裂 信息遗漏 响应滞后等问题，同时，各类日志格式异构、字段不统一 ，安全设备各自为战，缺乏上下文关联能力，导致无法对攻击过程进行完整还原，并且系统告警严重依赖静态规则，对未知攻击与高隐蔽性行为缺乏检测能力，对于 APT ZERO DAY 等高级威胁往往无法提前识别和阻断。

此外，当前 SOC 调查依赖经验型人员完成行为还原与风险判断，一旦人员变动，知识与流程缺乏沉淀，调查质量易波动且缺乏可复用的知识结构，同时传统平台不支持通过自然语言提问的交互方式，分析人员仍需掌握特定语法或规则语言查询系统，数据访问与推理能力存在高门槛。

由此可以得出，现有安全运营平台普遍存在以下结构性缺陷：

一、缺乏跨设备跨维度统一主体的行为建模能力；

二、无法自动构建行为链并对角色行为做上下文解释；

三、缺少智能化问答式交互机制与语义输出能力；

四、无法将历史攻击知识沉淀形成动态可复用知识库；

五、无法摆脱对规则的依赖 对高级威胁响应能力弱。

发明内容

本发明的目的在于克服上述问题，提出了一种基于语义行为链重构的 AI 引导安全调查方法，定义为当前安全运营架构中缺失的调查层，首次实现跨日志、跨设备、跨角色的结构化调查流程与知识演进闭环。为实现上述目的，本发明采用如下技术方案：

一种语义行为链重构与 AI 引导的安全调查方法，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；