METHOD AND SYSTEM FOR SEMANTIC BC (BEHAVIOR CHAIN) RECONSTRUCTION AND AI-DRIVEN SECURITY INVESTIGATION

TECHNICAL FIELD

The invention relates to the cross-field of network security and artificial intelligence, and particularly to a method and system for semantic BC (behavior chain) reconstruction and AI-driven security investigation.

BACKGROUND ART

Existing security operation platforms primarily rely on SIEM systems for log aggregation and event analysis. Their core mode typically involves matching single logs based on fixed rules to generate alerts. During actual investigation processes, analysts need to manually write query statements to locate key information from multi-source logs and manually piece together BCs to infer threat paths. This method suffers from problems such as high syntax barriers, fragmented logs, information omission, and delayed response. Simultaneously, various log formats are heterogeneous, fields are inconsistent, security devices operate independently, and there is a lack of contextual correlation capability, resulting in an inability to fully reconstruct attack processes. Moreover, system alerts heavily rely on static rules, lacking detection capabilities for unknown attacks and highly covert behaviors, often failing to identify and block advanced threats like APT and ZERO DAY in advance.

Furthermore, current SOC investigations rely on experienced personnel to complete behavior reconstruction and risk judgment. Once personnel change, knowledge and processes lack accumulation, investigation quality fluctuates easily, and reusable knowledge structures are lacking. Traditional platforms also do not support interactive methods using natural language questioning. Analysts still need to master specific syntax or rule languages to query the system, creating a high barrier to data access and reasoning capabilities.

Therefore, it can be concluded that existing security operation platforms generally have the following structural defects:

1. lack of capability for unified subject behavior modeling across devices and dimensions;